Bachelorarbeit - Wirtschaftsinformatik

Bachelor-Thesis:

Blockchain – Potentiale einer disruptiven Technologie im Gesundheitswesen

Departement:	School of Management and Law
Modul:	Bachelorarbeit
Dozent:	Dr. Stefan Koruna
Semester:	FS 2018
Abgabedatum:	24. Mai 2018

Autor:	Andreas Bächli, WIN15VZa, baechand@students.zhaw.ch andi.b90@gmx.ch
Matrikelnummer:	12-299-236

Management Summary

Die Blockchain-Technologie ist eine der vielversprechendsten technologischen Entwicklungen der letzten Jahre. Insbesondere durch die hohe Volatilität der kryptographischen Währung Bitcoin, wurde die zugrundeliegende Technologie popularisiert. Trotz des grossen Interesses mangelt es häufig an Wissen über die Funktionsweise der Technologie und das Potential bleibt oft unentdeckt oder wird missverstanden. Zahlreiche Start-Ups und etablierte Unternehmen arbeiten an Blockchain-basierten Applikationen, um bestehende Geschäftsmodelle zu revolutionieren. Dabei hat die Blockchain-Technologie das Potential bestehende Prozesse durch den Ausschluss von Intermediären komplett umzugestalten.

Neben einer umfassenden Erklärung der technischen Funktionsweise der Blockchain-Technologie, untersucht die vorliegende Bachelorarbeit die möglichen Anwendungsgebiete von Blockchain-basierten Applikationen im Gesundheitswesen. Diese Bachelorarbeit hat das Ziel, die Funktionsweise der Blockchain-Technologie für Personen ohne fachspezifischen Hintergrund verständlich zu vermitteln und die Anwendungspotentiale im Gesundheitswesen aufzuzeigen.

Zur Beantwortung der vorgestellten Forschungsfragen wurde deduktiv vorgegangen. Basierend auf der bestehenden Literatur wurde die Erklärung der Blockchain-Technologie ausgearbeitet und das Anwendungspotential im Gesundheitswesen analysiert. Bei der Literaturrecherche wurden auch die bestehenden Problemfelder der Blockchain-Technologie oder ähnlichen distributed-ledger-Technologien und deren Auswirkungen auf mögliche Anwendungen in der Praxis berücksichtigt.

Aus der Analyse konnten fünf Anwendungsmöglichkeiten der Blockchain-Technologie im Gesundheitswesen abgeleitet werden. Der erste Anwendungsbereich umfasst die elektronische Erfassung und den Austausch von Patientendaten über die Blockchain. Weiteres Potential konnte in der Abwicklung von Versicherungsansprüchen und der Nachverfolgbarkeit von Medikamenten entlang der Supply Chain identifiziert werden. Weitere Bereiche sind E-Health in Government und die medizinische Forschung. In einer weiteren detaillierten Analyse lag der Fokus auf der Umsetzung des erstgenannten Anwendungsbereichs, dem Erfassen und Teilen von Patientendaten mithilfe der Blockchain-Technologie. Insgesamt konnten drei Hauptproblemfelder für eine nachhaltige Anwendung der Blockchain-Technologie identifiziert werden. Dabei handelt es sich um die mangelnde Skalierbarkeit und Performance, die hohen Kosten

des Proof-of-Work-Konsensmechanismus und die Aufrechthaltung einer nachhaltigen Dezentralisierung des Netzwerks.

Aus den Ergebnissen der Analyse konnte die Schlussfolgerung gezogen werden, dass die Blockchain-Technologie im Anwendungsbereich zur elektronischen Erfassung von Patientendaten eine disruptive Wirkung aufweist. Obwohl die Auswirkung der mangelnden Skalierbarkeit und Performance in diesem Bereich eher gering sein könnten, lassen die Kosten des Proof-of-Work Skepsis aufkommen. Bietet die Applikation in diesem Bereich eine Very-Different-Value-Proposition, wie es mit alternativen Technologien nicht möglich wäre.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einführung

1.1 Ausgangslage und Problemstellung

Der Begriff «Blockchain» war ursprünglich eine Bezeichnung für die Art und Weise, wie Daten strukturiert und gespeichert werden (Laurence, 2017, S. 7). Im Jahr 2008 verlieh ein White Paper mit der Bezeichnung «Bitcoin: A Peer-to-Peer Electronic Cash System» dem Begriff Blockchain eine neue Bedeutung (Nakamoto, 2008). Bitcoin war die erste Kryptowährung und Blockchain die zugrundeliegende Technologie (Swan, 2015, S. 1). Interessanterweise verwendete der Autor des Bitcoin White Paper ein Pseudonym und es ist bis heute nicht klar, welche Person oder Gruppe dafür verantwortlich ist (Tapscott & Tapscott, 2016, S. 22).

Das Ziel von Bitcoin war das Kreieren eines elektronischen Peers-to-Peer Zahlungssystems, welches direkte Onlinezahlungen ohne den Einbezug von Drittparteien ermöglichen sollte (Nakamoto, 2008, S. 1). Dies mag sich unspektakulär anhören, doch dabei muss berücksichtigt werden, dass bis anhin für jede getätigte Überweisung immer vertrauenswürdige Intermediäre vonnöten waren (Tapscott & Tapscott, 2016, S. 22-23). Intermediäre wie zum Beispiel Banken, Kreditkartenunternehmen oder PayPal müssen als Drittparteien hinzugezogen werden, um die Integrität der Daten zu gewährleisten oder in diesem Fall eine Transaktion zu bestätigen (Tapscott & Tapscott, 2016, S. 29-30). Dies ist eine besonders wichtige Aufgabe, da es das sogenannte «Problem des doppelten Ausgebens» verhindern soll (Tapscott & Tapscott, 2016, S. 52-53). So stellt beispielsweise eine Bank als Intermediär sicher, dass eine Person nicht mehr Geld beziehen oder überweisen kann, als sich auf dem Konto befindet. Das gleiche Prinzip gilt zum Beispiel beim Verkauf einer Immobilie (Drescher, 2017, S. 50). Ein Verkäufer soll ein Haus nicht gleichzeitig an zwei unterschiedliche Personen verkaufen können, deshalb gibt es Unternehmen oder staatliche Organisationen, die ein zentrales Register führen und eine solche Situation verhindern (Drescher, 2017, S. 50). In anderen Worten soll es also nicht möglich sein, eine Geldeinheit mehrfach auszugeben, daher der Begriff «Problem des doppelten Ausgebens». Fallen diese Intermediäre jedoch weg, würde eine Transaktion auf dem Vertrauen in die andere Partei basieren. Die Blockchain ist eine technische Lösung für das Problem des doppelten Ausgebens, indem die Validierung der Transaktionen über ein dezentralisiertes Netzwerk, basierend auf dem Proof-of-Work Konsensalgorithmus, stattfindet (Davidson, De Filippi & Potts, 2016, S. 2).

Seit der Einführung im Jahr 2009 hat sich die digitale Währung «Bitcoin» zur weitverbreitetsten Anwendung der Blockchain-Technologie entwickelt (Olnes, Ubacht & Janssen, 2017, S. 356), gemäss Tapscott und Tapscott (2016, S. 394) geht die revolutionäre Wirkung der Blockchain-Technologie weit über Bitcoin hinaus und hat das Potential, bestehende Geschäftsmodelle, Regierungen und sogar die Gesellschaft grundlegend zu verändern.

1.2 Forschungsfrage

Im Zuge des Bitcoin-«Hypes» wird in der gehobenen Tagespresse immer wieder auf das Potential der Blockchain-Technologie für Unternehmen hingewiesen. Dabei wird auch immer wieder anhand von Beispielen dargestellt, wo diese Transaktions-Technologie überall Anwendung finden kann. Häufig bleiben die Darstellungen über die Anwendung der Blockchain-Technologie in den Unternehmen jedoch sehr oberflächlich. Das hat insbesondere damit zu tun, dass die Blockchain-Technologie selbst relativ komplex ist. Die Komplexität der Blockchain-Technologie hat auch zur Folge, dass viele Fachleute kaum etwas von dieser Technologie verstehen und deren Potential deshalb sowohl nicht erkennen und damit auch vernachlässigen.

Im Rahmen der vorliegenden Bachelorarbeit geht es deshalb darum, die «Black Box» Blockchain «aufzubrechen» und Managern ohne IT-Hintergrund aufzuzeigen, wie die Blockchain-Technologie funktioniert. Neben der grundsätzlichen Forschungsfrage geht es insbesondere darum, das Anwendungspotential der Blockchain-Technologie im Gesundheitswesen aufzuzeigen.

1.3 Abgrenzung

Bei der Erklärung der Funktionsweise der Blockchain-Technologie beschränkt sich diese Bachelorarbeit auf das Konzept der Bitcoin-Blockchain. Andere Blockchain-Technologien wie zum Beispiel IOTA, die auf einer «tangle-based» Blockchain basieren, werden in dieser Arbeit nicht abgedeckt.

1.4 Methodisches Vorgehen

Bei der Beantwortung der zwei vorgestellten Forschungsfragen wurde deduktiv vorgegangen. Basierend auf der bestehenden Literatur wurde die Erklärung der Blockchain-Technologie ausgearbeitet und das Anwendungspotential im Gesundheitswesen analysiert. In einem ersten Schritt wurde eine extensive Literaturrecherche in Datenbanken wie SpringerLink, Nebis, Web of Science und Google Scholar durchgeführt. Die Themenbereiche der Literaturrecherche umfassen neben den zentralen Begriffen wie Blockchain und distributed ledger technologies auch die zahlreichen Nebenbereiche der Technologie wie Smart Contract, Decentralized Autonomous Organizations, Kryptowährungen, Kryptographie und Konsensmechanismen. Zur Analyse des Anwendungspotentials im Gesundheitswesen wurden in einem ersten Schritt die Limitationen der Technologie recherchiert. In Kombination mit der Literaturrecherche bezüglich der Anwendungsmöglichkeiten der Blockchain-Technologie im Gesundheitswesen wurden die fünf vielversprechendsten Bereiche zur weiteren Analyse ausgewählt. Bei der Auswahl der Bereiche wurden die Limitationen der Technologie und die Anzahl der Publikationen und des vorhandenen Proof of Concepts berücksichtigt. Basierend auf den Ergebnissen einer zusätzlichen und detaillierteren Literaturanalyse in den ausgewählten Bereichen wurde ein spezifischer Anwendungsfall ausgewählt und die Funktionsweise eines Proof of Concepts genauer erläutert. Die erarbeiteten Artefakte umfassen einerseits die ausführliche und vollständige Erklärung der Blockchain-Technologie inklusive der Visualisierung von besonders komplexen Abläufen und Beispielen, um Personen ohne spezifische Vorkenntnisse den Einstieg in das Thema zu erleichtern. Andererseits umfassen die Artefakte auch verschiedene Anwendungsmöglichkeiten im Gesundheitsbereich und eine detaillierte Erläuterung der Funktionsweise einer ausgewählten Applikation.

1.5 Relevanz der Arbeit

Die Literaturanalyse im Zuge dieser Arbeit hat ergeben, dass obwohl diverse wissenschaftliche Publikationen über die Funktionsweise der Blockchain-Technologie existieren, handelt es sich dabei entweder um nur oberflächliche Erläuterungen der Technologie oder beziehen sich nur auf vereinzelte Aspekte der Funktionsweise. Die im ersten Teil bearbeitete Forschungsfrage, die Erklärung der Blockchain-Technologie

für Personen ohne fachspezifisches Vorwissen, liefert somit eine umfassende Erläuterung der Funktionsweise und den angrenzenden Themengebieten. Basierend auf dem im ersten Teil der Arbeit vermittelten Wissenstand, werden im zweiten Teil die Anwendungsmöglichkeiten der Blockchain-Technologie untersucht und mögliche Problemfelder aufgezeigt. Damit liefert diese Bachelorarbeit eine umfassende Einleitung in die Blockchain-Technologie und soll dem Leser die möglichen Anwendungsbereiche im Gesundheitswesen verständlich erklären.

1.6 Aufbau der Arbeit

Kapitel 1 führt die Arbeit ein. Dabei werden zunächst die Ausgangslage und die Problemstellung erläutert. Darauf folgen die Formulierung der Forschungsfrage, welche es in der vorliegenden Bachelorarbeit zu beantworten gilt, sowie die Abgrenzung des Themenbereichs. Im weiteren Verlauf des Kapitels wird das methodische Vorgehen formuliert und der aktuelle Stand der Forschung aufgezeigt. Das Kapitel endet mit der Beschreibung des Aufbaus der Arbeit.

Kapitel 2 befasst sich mit der theoretischen Grundlage des Themas. Dieses Kapitel beinhaltet den Hauptteil der grundsätzlichen Forschungsfrage und erklärt die Funktionsweise der Blockchain-Technologie.

Kapitel 3 führt im Kontext der Ethereum-Blockchain in die Themen Smart Contract und Decentralized Autonomous Organizations ein.

Kapitel 4 bietet eine kurzgefasste Erläuterung der branchenunabhängigen Folgen der Blockchain-Technologie. Im Fokus stehen das Problem des doppelten Ausgebens und die Frage, wieso die Blockchain-Technologie die Intermediäre ersetzen kann.

Kapitel 5 befasst sich mit dem zweiten Teil der Aufgabenstellung und erläutert verschiedene Anwendungsgebiete der Blockchain-Technologie im Gesundheitswesen. Das Kapitel beinhaltet eine Beschreibung von insgesamt fünf unterschiedlichen Anwendungsbereichen, wobei der Austausch von Patientendaten über die Blockchain im Zentrum steht.

Kapitel 6 stellt einen Use Case für den Austausch von Patientendaten über die Blockchain vor. Der Use Case basiert auf einem Proof of Concept für eine Applikation, die einen einheitlichen und schnellen Zugriff auf Patientendaten ermöglichen, Kompati-

bilität zwischen unterschiedlichen Systemen gewährleisten, dem Patienten die Kontrolle über die eigenen Daten ermöglichen und zusätzlich die Quantität und Qualität von medizinischen Daten für die Forschung erhöhen soll.

Kapitel 7 zeigt die grössten Problemfelder auf, die einen weitreichenden Einsatz der Blockchain-Technologie beeinträchtigen könnten. Dabei stehen vor allem die Probleme im Fokus, welche die Blockchain-Technologie im Allgemeinen betreffen und nicht auf spezifische Applikationen oder Anwendungsbereiche beschränkt sind.

Kapitel 8 liefert einen Ausblick in ein mögliches Anwendungsgebiet der Blockchain-Technologie in der Zukunft. Konkret befasst sich dieses Kapitel mit der Kombination der Blockchain-Technologie und des Internet of Things.

Kapitel 9 fasst die gewonnenen Erkenntnisse bezüglich der Blockchain-Technologie im Allgemeinen und bezüglich des Anwendungspotentials im Gesundheitswesen zusammen.

2 Theoretische Grundlagen zur Blockchain-Technologie

Der Begriff «Blockchain» war ursprünglich eine Bezeichnung für die Art und Weise, wie Daten strukturiert und gespeichert werden (Laurence, 2017, S. 7). Im Jahr 2008 verlieh ein White Paper mit der Bezeichnung «Bitcoin: A Peer-to-Peer Electronic Cash System» dem Begriff Blockchain eine neue Bedeutung (Nakamoto, 2008). Bitcoin war die erste Kryptowährung und Blockchain die zugrundeliegende Technologie (Swan, 2015, S. 1).

Seit der Einführung der digitalen Währung «Bitcoin» im Jahr 2009 hat sich Bitcoin zur weitverbreitetsten Anwendung der Blockchain-Technologie entwickelt (Olnes, Ubacht & Janssen, 2017, S. 356), doch gemäss Tapscott und Tapscott (2016, S. 394) geht die revolutionäre Wirkung der Blockchain-Technologie weit über Bitcoin hinaus und hat das Potential, bestehende Geschäftsmodelle, Regierungen und sogar die Gesellschaft grundlegend zu verändern. Da die Auswirkungen der Blockchain-Technologie so weitreichend sind, wird gemäss Swan (2015, S. XI) dabei bereits von der fünften Evolution des Computing gesprochen (Abbildung 1).

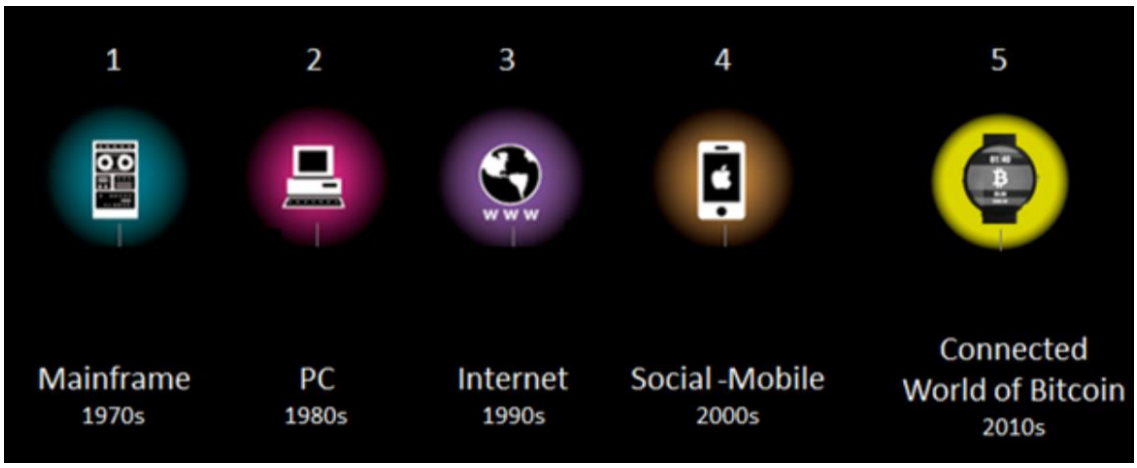


Abbildung 1: Evolution des Computing (Swan, 2015, S. XI)

Blockchains können als ein neuer Ansatz einer dezentralisierten beziehungsweise verteilten Datenbanken angesehen werden, wobei die Innovation in einer neuen Art der Nutzung von bereits existierenden Technologien besteht (Laurence, 2017, S. 7).

Die Blockchain-Technologie ist eine potentiell revolutionäre Innovation, was Tapscott und Tapscott (2016, S. 90) damit begründen, da es die Blockchain-Technologie erstmals ermöglicht, Transaktionen durchzuführen, ohne der Gegenpartei vertrauen oder einen Intermediär hinzuziehen zu müssen. Die Blockchain-Technologie ist eine technische Lösung für das Problem des doppelten Ausgebens (Davidson et al.,

2016, S. 2). Das Problem des doppelten Ausgebens beschreibt die Problematik, dass eine einzelne, in diesem Sinne einzigartige, Werteinheit mehrfach ausgegeben werden könnte (Tapscott & Tapscott, 2016, S. 52-53). Ohne zentrale Kontrollinstanz, würde eine Transaktion zwischen unterschiedlichen Parteien auf dem Vertrauen basieren, dass keine Partei diese Problematik ausnutzt (Morabito, 2017, S. 22). Traditionell haben Intermediäre, wie zum Beispiel eine Bank, die Aufgabe der zentralen Kontrollinstanz übernommen (Morabito, 2017, S. 22).

Die Blockchain-Technologie löst das Problem des doppelten Ausgebens und schafft ein sogenanntes fälschungssicheres «trustless network», in welchem keine Intermediäre eine Transaktion bestätigen müssen (Morabito, 2017, S. 22). Dies hat zur Folge, dass die Transaktionskosten gesenkt, der zeitliche Aufwand für die Durchführung einer Transaktion von Tagen auf Minuten minimiert (Tapscott & Tapscott, 2016, S. 92) und durch die Dezentralisierung der Single-Point-of-Failure, welcher durch Hacker ausgenutzt werden könnte, eliminiert werden (Olnes et al., 2017, S. 356).

2.1 Begriffsdefinition

Stark vereinfacht, ist eine Blockchain ein öffentliches Register (ledger) von Transaktionen (Kewell, Adams & Parry, 2017, S. 431). Diese Transaktionen beinhalten folgende Informationen: Wem gehört was, wer transferiert was, woher wird etwas transferiert und wann wurde es transferiert (Kewell et al., 2017, S. 431). Die Technologie basiert auf dem von Nakamoto (2008, S. 1-8) beschriebenen Konzepts zur Ermöglichung von Werttransfers zwischen zwei unbekannten Entitäten, ohne dabei zusätzliche Intermediäre (zum Beispiel eine Bank oder eine Clearinggesellschaft) zwischenzuschalten (Kewell et al., 2017, S. 431). Die erfassten Transaktionen sind – im Gegensatz zu konventionellen Transaktionssystemen - jedoch nicht in einer zentralen Datenbank gespeichert, sondern auf den Computern aller User (Nodes), welche zusammen ein dezentralisiertes Netzwerk bilden (Kewell et al., 2017, S. 431). Daher spricht man bei Blockchain ebenfalls von einer «distributed ledger technology» (DLT), da alle Transaktionsinformationen in den verschiedenen «Nodes» des Netzwerks gespeichert sind (Olnes et al., 2017, S. 355). Dadurch entfällt die Abhängigkeit von einer zentralen Schnittstelle und das Risiko wird reduziert, dass Daten manipuliert werden oder das ganze System zusammenbricht, da alle Nodes im Netzwerk alle Transaktionsinformationen besitzen (Olnes et al., 2017, S. 355).

Die Blockchain-Technologie oder DLT ist allerdings keine neue technische Erfindung, sondern entspricht eher einer Zusammenführung verschiedener Technologien wie der Kryptographie, den digitalen Währungen, Hashing und dem Prinzip der Buchführung in einem Register (Laurence, 2017, S. 42). Die Kombination all dieser Technologien in einer online verfügbaren, dezentralisierten Datenbank macht die DLT nach Ansicht von Laurence (2017, S. 42) revolutionär.

Obwohl häufig von *der* Blockchain gesprochen wird, wäre es falsch anzunehmen, dass es sich dabei um ein einziges Konstrukt handelt (Tapscott & Tapscott, 2016, S. 23). Tatsächlich gibt es diverse Adaptionen der von Nakamoto (2008, S. 1-8) beschriebenen Blockchain, welche sich jeweils in deren Grösse, Funktionsweise und Zweck unterscheiden können (Tapscott & Tapscott, 2016, S. 23-24). Dennoch haben die meisten Blockchains laut Tapscott und Tapscott (2016, S. 23-24) drei markante Gemeinsamkeiten: Sie sind *verteilt, öffentlich* und *verschlüsselt*.

Verteilt bedeutet, dass die Blockchain dezentralisiert ist, also nicht auf einem zentralen Server einer Institution, sondern auf den Rechnern von freiwilligen Teilnehmern verteilt auf der ganzen Welt läuft (Tapscott & Tapscott, 2016, S. 23-24).

Öffentliche Blockchains sind für jeden zugänglich, die Überprüfung und Dokumentation der Transaktionen werden vom Netzwerk durchgeführt und können eingesehen werden (Tapscott & Tapscott, 2016, S. 24).

Bei Blockchains kommt eine fortgeschrittene Form der *Verschlüsselung* zum Einsatz, um Transaktionen über die Blockchain zu verifizieren (Tapscott & Tapscott, 2016, S. 24).

Zum besseren Verständnis und zur Übersicht des in den folgenden Kapiteln behandelten Sachverhalts folgt als erstes eine kurze Beschreibung der wichtigsten Begriffe im Bereich der Blockchain-Technologie. Vereinzelte Begriffe werden zu einem späteren Zeitpunkt nochmals aufgegriffen und in einem höheren Detaillierungsgrad erläutert.

Blockchain	Eine Blockchain ist eine Datenstruktur, welche es ermöglicht, ein digitales Register (ledger) gefüllt mit Daten herzustellen und sie in einem Netzwerk von unabhängigen Parteien zu teilen (Laurence, 2017, S. 7)

DLT	DLT steht für distributed ledger technology und kann als Synonym für die Blockchain-Technologie angesehen werden (Olnes et al., 2017, S. 355).
Kryptowährung	Kryptowährung ist digitales Geld, welches wie eine reguläre Währung als Zahlungsmittel genutzt werden kann, jedoch nicht von einer Zentralbank überwacht und herausgegeben wird (Vranken, 2017, S. 1).
Transaktionen	Eine Transaktion ist eine in der Blockchain aufgezeichnete Datenreihe mit Informationen zu einem getätigten Transfer (Kewell et al., 2017, S. 431).
Block	Ein Block einer Blockchain ist eine Liste von aufgezeichneten Transaktionen in einem bestimmten Zeitraum (Laurence, 2017, S. 10).
Chain	Die Chain oder Kette ist das Bindeglied zwischen zwei aufeinanderfolgende Blöcke einer Blockchain (Laurence, 2017, S. 10). Die Verknüpfung von zwei Blöcken basiert auf einer kryptographischen Hash-Funktion (Laurence, 2017, S. 10).
Netzwerk	Das Netzwerk einer Blockchain besteht aus einer Vielzahl von unabhängigen und verteilten Nodes (Kewell et al., 2017, S. 431).
Node	Ein Node ist Teil des Blockchain-Netzwerks, dabei handelt es sich um ein Computer eines Nutzers, welcher mittels eines Algorithmus die Sicherheit des Netzwerks gewährleistet (Laurence, 2017, S. 10). Ein Node, der eine Kopie der vollständigen Blockchain hält, wird als «Full-Node» bezeichnet (Laurence, 2017, S. 10)
Miner	Ein Miner ist der Betreiber eines Nodes. Er prüft die in einem Block enthaltenen Transaktionen auf deren Validität in einem Prozess, welcher «mining» genannt wird (Nofer, Gomber, Hinz & Schiereck, 2017, S. 184). Für die Validierung des Blockes erhalten die Miner eine Belohnung, im Falle der Bit-

coin-Blockchain besteht diese Belohnung aus einer bestimmten Anzahl Bitcoins und den Transaktionskosten (Nofer et al., 2017, S. 184).

Mining — Das Mining ist die Aufgabe eines Miners, es besteht in den meisten Blockchains darin, ein rechenintensives Rätsel zu lösen (Proof-of-Work) und bei erfolgreicher Lösung den überprüften Block der Blockchain anzuhängen (Pazaitis, De Filippi & Kostakis, 2017, S. 109).

Blockchain-Protokoll — Software, welche Transaktionen auf der Blockchain zwischen verschiedenen Parteien ermöglicht, ohne einen Intermediär zu benötigen (Swan, 2015, S. 21).

2.2 Struktur und Netzwerk-Architektur einer Blockchain

Dieses Kapitel erläutert den strukturellen Aufbau einer Blockchain und zeigt auf, wie sich das Blockchain-Netzwerk von zentralisierten Systemen unterscheidet. Hierbei ist zu vermerken, dass sich die in diesem und den folgenden Kapiteln erläuterten technischen Eigenschaften mehrheitlich auf die Funktionsweise der Bitcoin-Blockchain beziehen. Obwohl die verschiedenen Weiterentwicklungen der Bitcoin-Blockchain auf dem gleichen Grundprinzip beruhen, ist es wichtig zu differenzieren, da sie sich in der Art des verwendeten Konsens-Mechanismus, der kryptographischen Verschlüsselung oder bezüglich des Einsatzes von Kryptowährungen unterscheiden können (Tapscott & Tapscott, 2016, S. 23-24).

2.2.1 Struktur von Blockchains

Eine Blockchain ist im Prinzip ein Register, ähnlich einer Datenbank, in dem alle getätigten Transaktionen in einer chronologisch geordneten Reihenfolge festgehalten und auf eine Art gespeichert werden, welche es erlaubt, Änderungen und nachträgliche Manipulationsversuche automatisch zu erkennen und zu verhindern (Drescher, 2017, S. 112). Bei den getätigten Transaktionen kann es sich um eine Vielzahl von unterschiedlichen Einträgen handeln. So kann eine Transaktion beispielsweise eine simple Überweisung eines Vermögenswertes (beispielsweise 10 Bitcoins) repräsentieren, jedoch aber auch jede andere Art von digitalisierten Informationen (Olnes et

al., 2017, S. 355). Gemäss Olnes et al. (2017, S. 355) handelt es sich typischerweise um transaktionale Daten wie Grundbucheintragungen, Geburts- und Heiratszertifikate, Geschäftslizenzen und Fahrzeugzulassungen. Die Blockchain-Technologie beschränkt sich jedoch nicht nur auf die Erfassung simpler Transaktionen (Laurence, 2017, S. 52-54). In Kapitel 3.1 wird die Funktionsweise von Smart Contracts erläutert, welche es erlauben, komplexe Vorgänge über die Blockchain zu steuern (Laurence, 2017, S. 52-54).

Um die Funktionsweise einer Blockchain verstehen zu können, kann als erstes der Begriff «Blockchain» herangezogen werden. Eine Blockchain besteht aus «Blöcken», welche sequentiell miteinander «verkettet» sind und somit, wie in Abbildung 2 dargestellt, eine Kette bilden (Asharaf & Adarsh, 2017, S. 11).

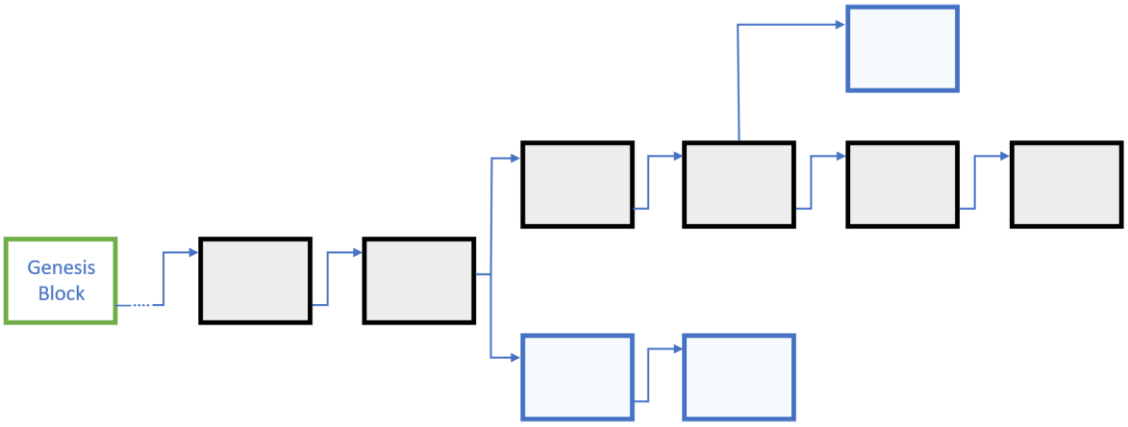


Abbildung 2: Struktureller Aufbau einer Blockchain (Wright & De Filippi, 2015, S. 8)

Im Kontext dieses Kapitels genügt es zu verstehen, dass die Blöcke Informationen zu den getätigten Transaktionen eines bestimmten Zeitraums enthalten (Laurence, 2017, S. 10) und jeweils mittels einer kryptografischen Hash-Funktion mit dem vorangehenden Block verknüpft sind (Asharaf & Adarsh, 2017, S. 11). Dies hat zur Folge, dass für den Datenbestand der gesamten Blockchain sowohl die zeitliche Reihenfolge als auch die Datenintegrität sichergestellt ist (Burgwinkel, 2016, S. 5-6).

Aus Abbildung 2 sind verschiedene Informationen zu entnehmen. Der erste Block in der Kette (grün) ist der sogenannte «Genesis Block» (Morabito, 2017, S. 65-66). Dieser Block steht immer am Anfang einer Blockchain und kann eine wichtige Rolle bei der Identifizierung von Blöcken spielen, da in jedem späteren Block immer auch die Distanz (Anzahl Blöcke bis zum Genesis Block) zum Genesis Block gespeichert ist

(Morabito, 2017, S. 65-66). Ebenfalls dargestellt sind die Blau eingefärbten «forks» oder Gabelungen der Blockchain, welche Auftreten können, wenn aufgrund von Unstimmigkeiten gleichzeitig mehrere Blöcke an einen Block angehängt werden (Olnes et al., 2017, S. 356). Dieses Problem wird gelöst, indem immer die längste Kette mit der grössten Distanz zum Genesis Block priorisiert wird (Nakamoto, 2008, S. 3).

2.2.2 Netzwerk-Architekturen

Ein fundamentaler Bestandteil der Blockchain-Technologie ist nicht nur die Speicherung von Informationen in Blöcken und deren Verknüpfung, sondern auch das weltweit verteilte Netzwerk von Nodes (Laurence, 2017, S. 10). Nodes sind Systemkomponenten (Drescher, 2017, S. 11), beziehungsweise einzelne Computer von Nutzern, welche zusammen das Netzwerk bilden (Laurence, 2017, S. 10).

Grundsätzlich kann (Abbildung 3) zwischen drei verschiedenen Netzwerk-Architekturen unterschieden werden (Baran, 1962, S. 3). In einem zentralisierten Netzwerk sind alle Nodes mit einem einzigen Server verbunden, einer zentralen Autorität (Asharaf & Adarsh, 2017, S. 1-2). Zentralisierte Systeme (centralized) haben den Vorteil, dass sich deren Wartung relativ einfach gestaltet, da sich der zentrale Server an einem Punkt befindet (Asharaf & Adarsh, 2017, S. 2). Dem gegenüber stehen allerdings Schwierigkeiten mit der Skalierbarkeit, weiter sind zentralisierte Netzwerke anfällig für Hacker-Angriffe und Netzwerkausfälle, da sie einen Single-Point-of-Failure besitzen (Drescher, 2017, S. 12).

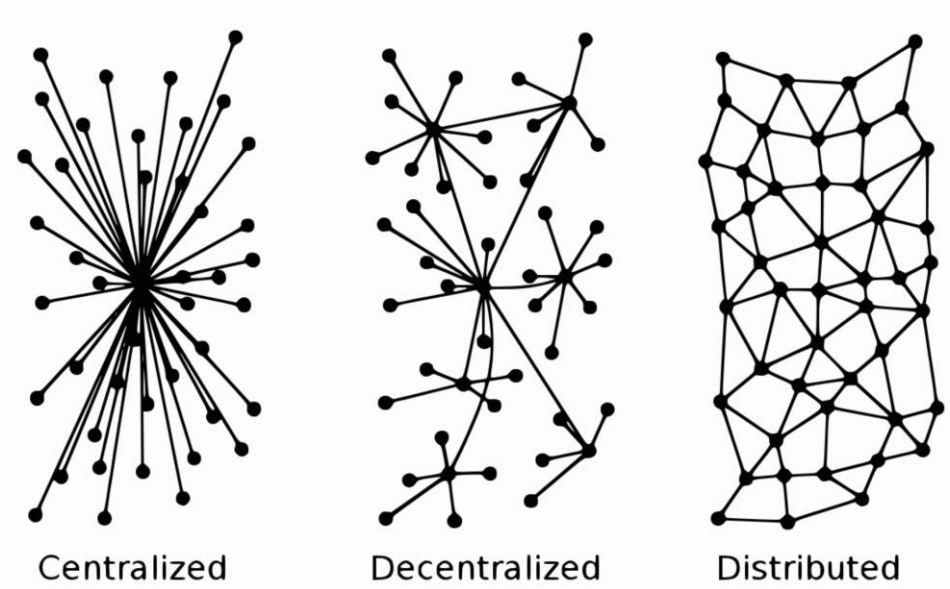


Abbildung 3: Unterschiedliche Netzwerk-Architekturen (Baran, 1962, S. 4)

Bei einem verteilten (distributed) Netzwerk ist die Rechenkapazität des gesamten Netzwerks auf die einzelnen Nodes verteilt (Drescher, 2017, S. 12). Es ist zusätzlich darauf hinzuweisen, dass ein Service gleichzeitig verteilt, aber auch zentralisiert sein kann und sich diese beiden Architekturen nicht gegenseitig ausschliessen (Drescher, 2017, S. 15-16). Ein Beispiel hierfür ist die Steuerung eines Netzwerks von einem zentralen Punkt aus, wobei die Leistung des Netzwerks über verschiedene Nodes verteilt ist (Drescher, 2017, S. 15-16). Vorteile einer verteilten Netzwerkarchitektur sind die geringeren Wartungskosten, eine höhere Rechenleistung aufgrund der Vielzahl der Nodes, bessere Stabilität des Netzwerks, da das System nicht von einem zentralen Punkt abhängig ist, und eine einfachere Skalierbarkeit der Netzwerkkapazität (Drescher, 2017, S. 12-13).

Die Haupteigenschaft eines dezentralisierten (decentralized) Netzwerks ist, dass es keine zentrale Autorität und somit auch keinen Single-Point-of-Failure besitzt (Olnes et al., 2017, S. 356). Laut Asharaf und Adarsh (2017, S. 3) können durch Dezentralisierung Sicherheit, Redundanz, Vertrauen, Zugänglichkeit und Kongruenz des Netzwerks verbessert werden, indem Kopien der Informationen auf dem Netzwerk über alle Nodes verteilt werden statt auf einem einzigen Server. Die Nutzer eines dezentralisierten Netzwerks, auch «Peers» genannt, können direkt miteinander interagieren und Daten oder Rechenkapazitäten teilen (Asharaf & Adarsh, 2017, S. 5). Einer der entscheidenden Vorteile eines dezentralisierten Netzwerks ist die Stabilität beziehungsweise der Schutz vor Ausfällen und Datenverlusten (Asharaf et al., 2017, S. 5). Die Stabilität kommt daher, dass der Ausfall einzelner Nodes nicht das gesamte Netzwerk beeinträchtigt, da jeder Node eine Kopie aller Daten besitzt, gehen beim Ausfall einzelner Nodes keine Daten verloren (Asharaf & Adarsh, 2017, S. 5).

Im Kontext dieses Kapitels wird auf eine der zentralen Eigenschaften der Blockchain-Technologie zurückgekommen, dem verteilten Netzwerk von Peers (P2P Netzwerk). Die Bitcoin-Blockchain ist ein Beispiel für ein Netzwerk, welches sowohl verteilt als auch dezentralisiert ist (Olnes et al., 2017, S. 356). Es ist verteilt, da jeder Node im Netzwerk eine Kopie der gesamten Blockchain besitzt und dezentralisiert, da keine zentrale Autorität vorhanden ist und das System auch bei einem Ausfall von mehreren Nodes nicht zusammenbricht (Olnes et al., 2017, S. 356). Diese Eigenschaften der Blockchain-Architektur tragen zur Sicherheit und Unveränderbarkeit der aufgezeichneten Transaktionen bei (Olnes et al., 2017, S. 356). Die Sicherheit und Unveränder-

barkeit der Transaktionen wird im folgenden Kapitel im Zusammenhang mit der Anwendung von digitalen Unterschriften genauer erläutert. Zusätzlich trägt der Konsens-Mechanismus (siehe Kapitel 2.3.3) zur Datenintegrität der Transaktionen bei (Olnes et al., 2017, S. 356). Die Aufzeichnung der Transaktionen und die Überprüfung ihrer Authentizität durch das gesamte Netzwerk von Peers mittels eines Konsens-Mechanismus macht die Blockchain zu einer «trustless technology» (Morabito, 2017, S. 22). Morabito (2017, S. 22) spricht von einer vertrauenslosen Technologie, da über die Blockchain Transaktionen durchgeführt werden können, auch wenn die beteiligten Parteien sich gegenseitig nicht vertrauen. Trotzdem muss kein vertrauenswürdiger Intermediär hinzugezogen werden, da das Blockchain-Netzwerk die Aufgaben des Intermediäres übernimmt, die Transaktion zu verifizieren, aufzuzeichnen und auszuführen (Morabito, 2017, S. 22).

2.3 Technische Funktionsweise einer Blockchain

Dieses und die folgenden Kapitel befassen sich mit der Validierung der Transaktionen und beschreiben den Prozess des «Minings», bei welchem es darum geht, einen neuen Block an die Blockchain anzuhängen. Als erstes folgt eine Einführung in den Bereich der «digital signatures» (digitale Unterschriften) und der dafür verwendeten Public-Key Kryptographie.

2.3.1 Digitale Unterschriften

Um den Prozess der Validierung von Transaktionen besser veranschaulichen zu können, wird das Vorgehen anhand einer beispielhaften Überweisung von 10 Bitcoins (Kryptowährung) von der Person A zur Person B beschrieben.

Abbildung 4: Transaktion von A nach B

Damit eine Transaktion zwischen A und B (siehe Abbildung 4) stattfinden kann, müssen beide Personen eindeutig identifizierbar sein, sodass A sicher sein kann, dass die

10 Bitcoins bei der richtigen Person ankommen. Andererseits soll niemand ausser A selbst seine/ihre Bitcoins versenden können. Bei der Bitcoin-Blockchain basiert diese Identifikation auf der Public-Key Kryptographie und digitalen Unterschriften (Courtois, Grajek & Naik, 2014, S. 132). Für die Personen A und B bedeutet das, dass beide einen sogenannten «Bitcoin wallet» besitzen müssen, um mit Bitcoins handeln zu können (Laurence, 2017, S. 26). Bei der Erstellung eines Wallets (Brieftasche für Bitcoins) wird zugleich eine einzigartige Wallet-Adresse erstellt, die das Senden und Empfangen von Bitcoins erlaubt (Laurence, 2017, S. 26). Damit sich Person A sicher sein kann, dass B die 10 Bitcoins erhält, kann A also die Wallet-Adresse von B verwenden. Allerdings würde eine solche Transaktion vom Netzwerk abgelehnt werden, da der Sender A die Transaktion noch mittels einer digitalen Unterschrift unterzeichnen muss, um seine Identität zu bestätigen (Krombholz, Judmayer, Gusenbauer & Weippl, 2016, S. 557). Eine digitale Unterschrift ist eine sichere Methode, um eine Transaktion durchzuführen (Courtois et al., 2014, S. 132). In Abbildung 5 ist dargestellt, wie eine Transaktion zwischen A und B mit den zusätzlichen Informationen visualisiert werden könnte.

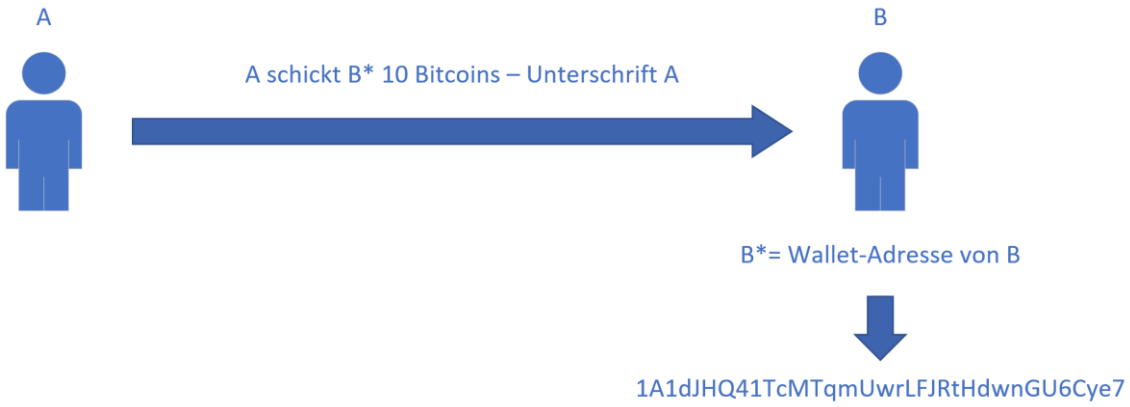


Abbildung 5: Autorisierung der Transaktion von A nach B

Eine digitale Unterschrift kann mit einer physischen Unterschrift verglichen werden, allerdings ist eine digitale Unterschrift deutlich sicherer (Katz, 2010, S. 3). Für die Erstellung einer digitalen Unterschrift wird ein Public-/Private-Key-Paar vorausgesetzt (wobei der Privat Key auch häufig als Secret Key bezeichnet wird) (Katz, 2010, S. 3), was im Beispiel von A und B bereits gegeben ist. Mittels eines Unterzeichnungs-Algorithmus wird die Unterschrift erstellt und durch einen Verifikations-Algorithmus kann der Empfänger die Unterschrift überprüfen (Katz, 2010, S. 3). Der generierte Output der kryptographischen Funktion «Sign(Message, Secret Key)» ist nicht nur vom Secret Key, sondern auch von der gesendeten Mitteilung abhängig (Katz, 2010,

S. 9-10). Dadurch wird für jede Transaktion eine neue Unterschrift generiert. Die Funktion «Vrfy(Message, Unterschrift, Public Key)» prüft die Validität der Unterschrift und gibt einen Output von 1 für «accept» oder 0 für «reject» zurück (Katz, 2010, S. 10). Die Funktionsweise des verwendeten Algorithmus (Elliptic Curve Digital Signature Algorithm im Falle von Bitcoin) wird an dieser Stelle nicht genauer erläutert, jedoch ist es wichtig zu verstehen, dass eine Transaktion vom Sender mit einer digitalen Unterschrift autorisiert werden muss (Gennaro, Goldfeder & Narayanan, 2016, S. 157).

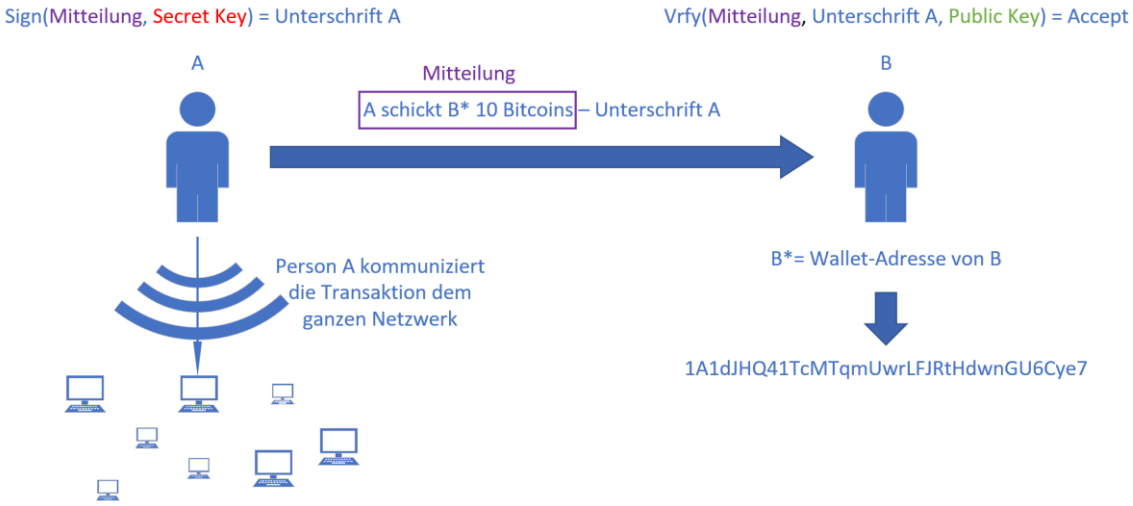


Abbildung 6: Transaktion von A nach B (erweitert)

Abbildung 6 stellt den Ablauf in einem erweiterten Format nochmals dar, daraus ist ebenfalls ersichtlich, dass die Transaktion, sobald die Person A unterzeichnet hat, an alle Nodes im Netzwerk der Blockchain gesendet wird (Krombholz et al., 2016, S. 557).

2.3.2 Einführung in den Mining-Prozess

Dieses Kapitel enthält eine kompakte Formulierung des Mining-Prozesses und dient als Basis für das darauffolgende Kapitel.

Mit der Übermittlung der Transaktion an das P2P-Netzwerk der Blockchain werden ausstehende Transaktionen von Bitcoin-Minern in einem neuen Block zusammengetragen und durch einen Konsens-Mechanismus validiert (Olnes et al., 2017, S. 356). Der angewandte Konsens-Mechanismus der Bitcoin-Blockchain nennt sich Proof-of-Work, also eine Art Arbeitsnachweis (Kewell et al., 2017, S. 432). Die Validierung

der Transaktionen mittels des Proof-of-Work Algorithmus ist ein Prozess, welcher als «Mining» bezeichnet wird (Pazaitis et al., 2017, S. 109). Das Ziel ist das Erreichen eines Konsenses, in dem Sinne, dass sich alle Teilnehmer des Netzwerks über den aktuellen Stand der Blockchain einig werden (Laurence, 2017, S. 12-13).

Im Prozess zur Validierung und Bestätigung von ausstehenden Transaktionen («Mining»), werden Transaktionen, wie zum Beispiel die Überweisung von 10 Bitcoins von Person A zu Person B, von der Person A an das gesamte Netzwerk übermittelt (Olnes et al., 2017, S. 356). Die Miner sammeln diese Transaktionen und fassen sie in einem neuen Block zusammen, welcher am Ende des Mining-Prozesses an die Blockchain angehängt werden soll (Olnes et al., 2017, S. 356). Damit ein Miner einen neuen Block an die bestehende Blockchain anhängen darf, muss er nachweisen können, dass er Ressourcen in die Erstellung des Blockes investiert hat (Kewell et al., 2017, S. 432). Im Falle der Bitcoin Blockchain handelt es sich dabei um einen Arbeitsnachweis, den Proof-of-Work (Tapscott & Tapscott, 2016, S. 54). Der Proof-of-Work Algorithmus stellt den Minern eine Aufgabe, welche es zu lösen gilt (Drescher, 2017, S. 92). Das Ziel ist das Finden einer bestimmten Zahl, welche auch Nonce genannt wird (Drescher, 2017, S. 90). Der Wert dieser Zahl wird dadurch bestimmt, indem ein SHA-256 (Secure Hash Algorithm) auf den gesamten Inhalt des Block Headers (Abbildung 7) und der Nonce angewendet wird, sodass das Ergebnis gewissen Bedingungen entspricht (Krombholz et al., 2016, S. 557).

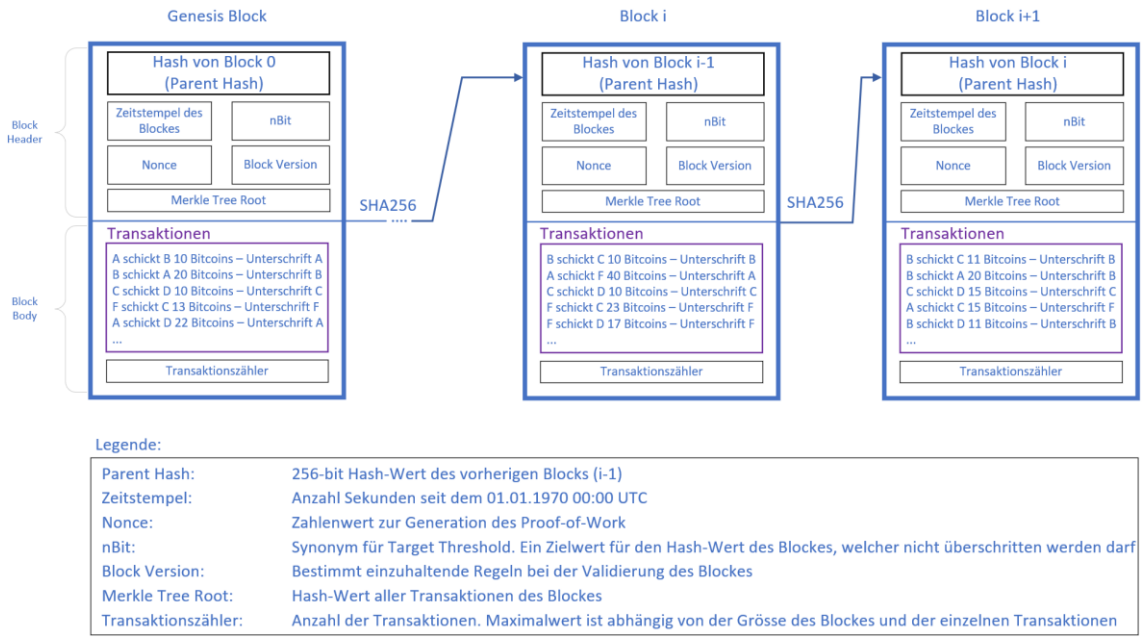


Abbildung 7: Bestandteile eines Blockes in der Blockchain (Zheng, Xie, Dai, Chen & Wang, 2016, S. 4-5)

Miner versuchen, den Wert dieser Nonce durch ein Trial-and-Error Verfahren herauszufinden, wobei sie in Konkurrenz mit den restlichen Minern des Netzwerks stehen, da nur der erste Miner, welcher eine gültige Nonce gefunden hat, den Block erstellen darf (Vranken, 2017, S. 2-3). Sobald eine gültige Nonce gefunden wurde, ca. alle zehn Minuten, wird das Ergebnis zur Verifikation an das gesamte Netzwerk gesendet und muss bestätigt werden (Kewell et al., 2017, S. 432). Da für die Berechnung der Nonce Zeit, Strom und Geld in Hardware investiert werden muss, wird die Erstellung eines neuen Blockes mit Bitcoins belohnt (Kewell et al., 2017, S. 432).

Die Anwendung des Proof-of-Work Konsensmechanismus trägt zur Datenintegrität der Transaktionen bei (Olnes et al., 2017, S. 356). Datenintegrität bedeutet, dass die gespeicherten Daten in einem System dem entsprechen, was sie in der Realität repräsentieren und kann sich auf eine Vielzahl von Aspekten wie Datenkonsistenz, Sicherheit, Verlässlichkeit, Aktualität und Originalität beziehen (Olnes et al., 2017, S. 357).

Im folgenden Abschnitt wird der Mining-Prozess im Detail beschrieben.

2.3.3 Bitcoin-Mining

Wie im vorherigen Abschnitt bereits beschrieben, werden ausstehende Transaktionen von Minern in einem Block zusammengetragen und durch einen Prozess, der «Mining» genannt wird, an die bestehende Blockchain angehängt (Pazaitis et al., 2017, S. 109). Ein zentraler Bestandteil des Proof-of-Work und der Blockchain ist die Kryptographie, im Falle von Bitcoin insbesondere der 256-Bit Secure Hash Algorithm (SHA-256) (Courtois et al., 2014, S. 131-133).

SHA-256 ist eine kryptographische Hash Funktion (Abbildung 8), welche einen beliebigen Input, in einen 256-Bit-Output umwandelt, welcher auch als «Digest» oder «Hash» bezeichnet wird (Chaves, Kuzmanov, Sousa & Vassiliadis, 2006, S. 3). Mittels Hashing lassen sich Daten von beliebiger Grösse in einen Hash mit einer fixen Länge umwandeln (Laurence, 2017, S. 42).

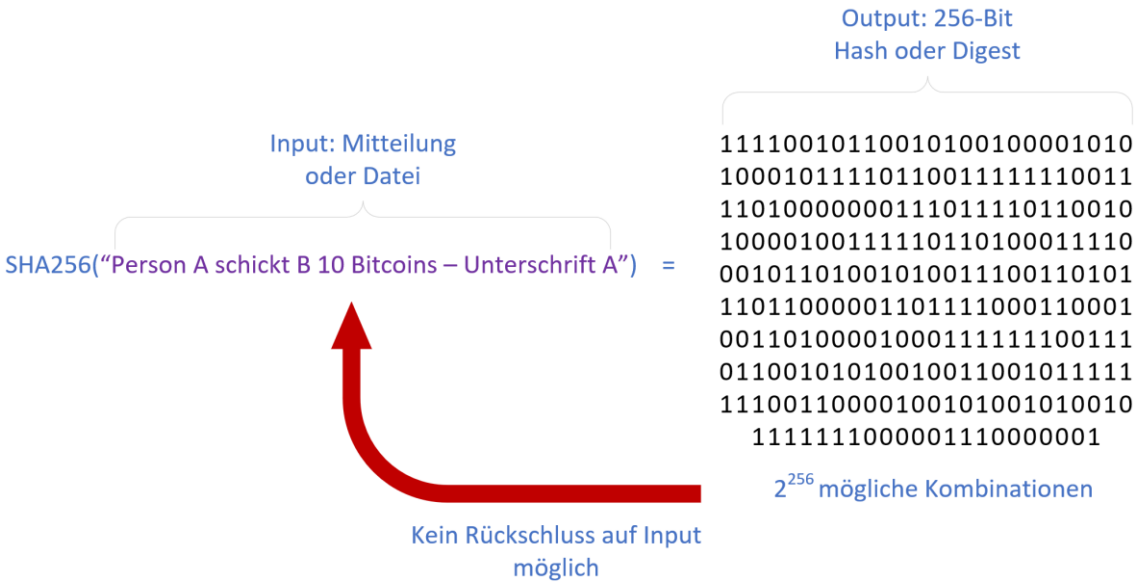


Abbildung 8: Einseitigkeit des SHA-256

Der Hash ist eine Binärzahl aus 256 Nullen oder Einsen, was 2^{256} unterschiedliche Kombinationen ermöglicht. Ein kryptographischer Hash ist einseitig und kollisionsresistent (Vranken, 2017, S. 2). Einseitig bedeutet, dass ein Hash mit gegebenen Input schnell zu berechnen ist, jedoch gibt es nach heutigem Wissensstand keine Möglichkeit, von einem Hash auf den Input zu schliessen (Vranken, 2017, S. 2).

Kollisionsresistenz bezieht sich auf die Wahrscheinlichkeit, dass zwei unterschiedliche Inputs denselben Hash ergeben, wie dies in Abbildung 9 dargestellt ist (Vranken, 2017, S. 2).

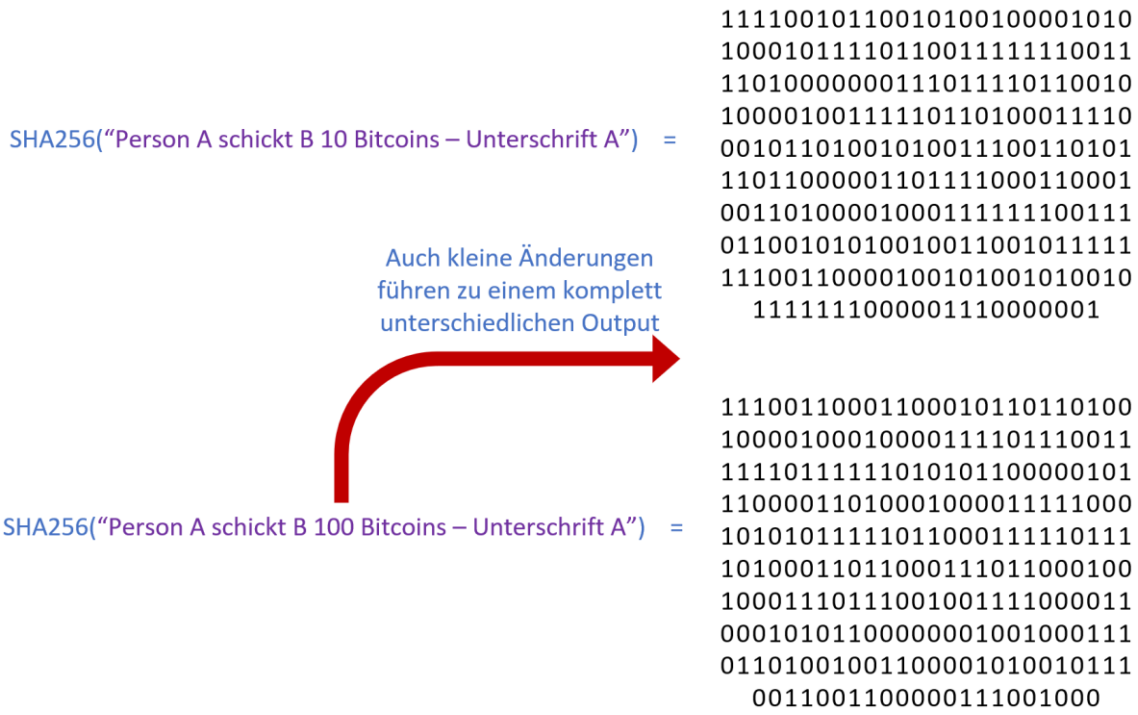


Abbildung 9: Kollisionsresistenz des SHA-256

Die einzige Option, einen Input für einen gegebenen Hash zu finden, ist durch Raten (Vranken, 2017, S. 2). Dies ist die Aufgabe der Miner (Vranken, 2017, S. 2).

Um den Mining-Prozess auf eine möglichst verständliche Art und Weise zu beschreiben, werden im folgenden Abschnitt die elementaren Aussagen der kurzgefassten Erklärungen aus dem Kapitel 2.3.2 genauer erläutert.

«..., werden Transaktionen [...] an das gesamte Netzwerk übermittelt, die Miner sammeln diese Transaktionen und fassen sie in einem neuen Block zusammen, ...»

Ausstehende Transaktionen werden über das Netzwerk an die Miner gesendet, jedoch können die Miner selbst entscheiden, welche Transaktionen sie in einen neuen Block aufnehmen wollen (Courtois et al., 2014, S. 136). Da die Miner allerdings bei einer erfolgreichen Erstellung eines neuen Blockes die Transaktionskosten erhalten, besteht ein finanzieller Anreiz, alle ausstehenden Transaktionen zu berücksichtigen (Courtois et al., 2014, S. 136). Die vom Miner ausgewählten Transaktionen werden jedoch nicht als einzelne Datenreihen im Block-Header gespeichert, sondern werden in einem einzelnen Hash zusammengefasst, der sogenannten Merkle Tree Root (Courtois et al., 2014, S. 135-136). Ein Merkle Tree (Abbildung 10) dient dazu, mehrere Hashes in einem einzelnen Hash zusammenzufassen (Laurence, 2017, S. 42). Dadurch können

unterschiedliche Daten mittels eines einzigen Hash-Werts zugänglich gemacht werden (Drescher, 2017, S. 88).

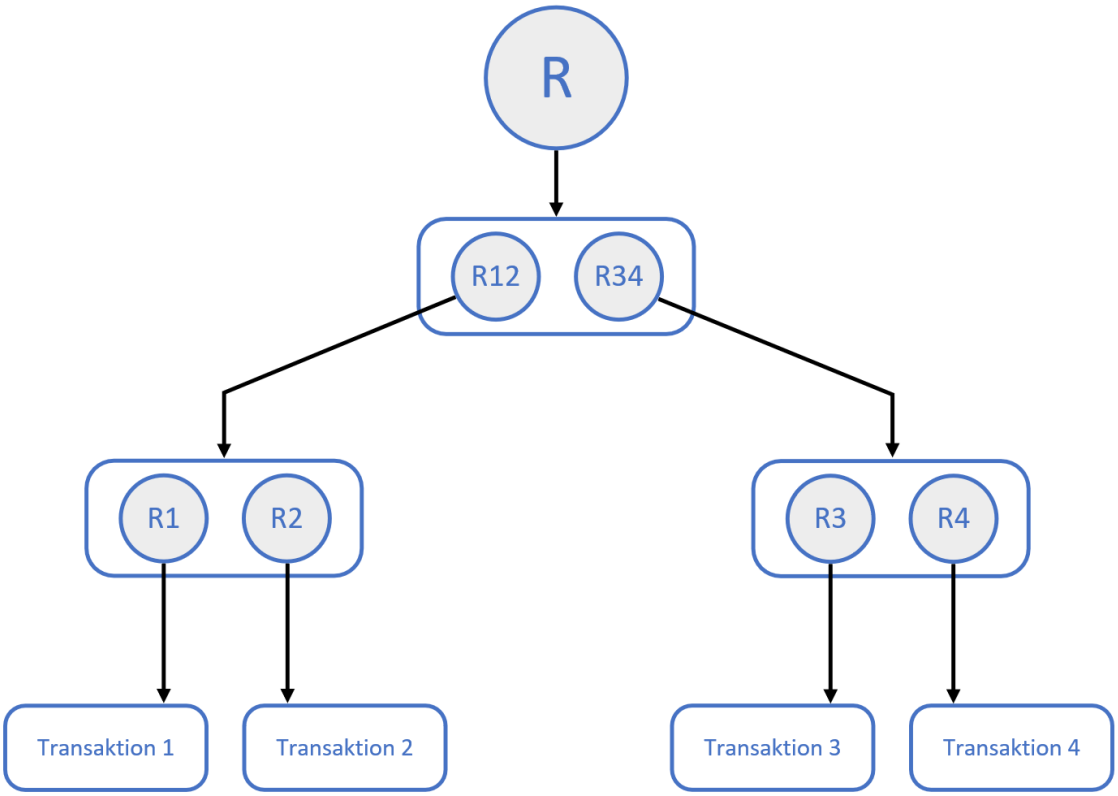


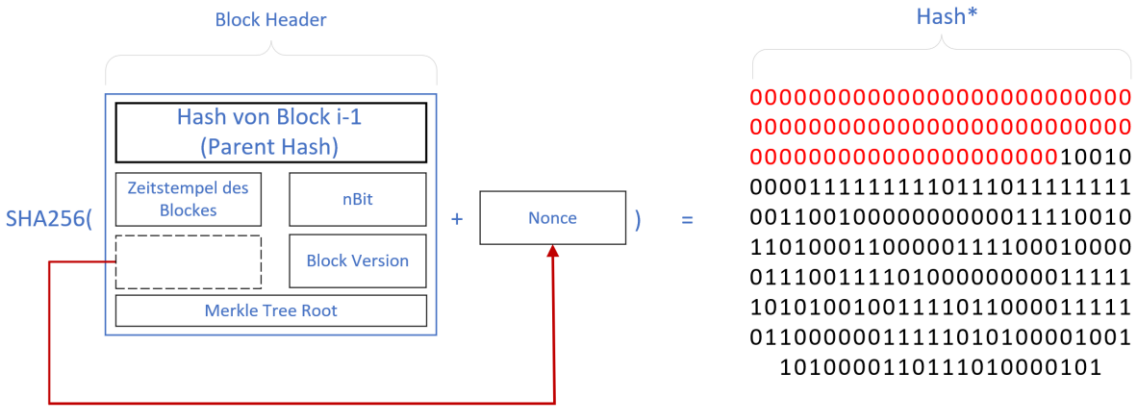
Abbildung 10: Merkle Tree (Drescher, 2017, S. 88)

Merkle Trees wurden entwickelt, um Transaktionsdaten auf eine sichere Art zu speichern (Drescher, 2017, S. 123). In Abbildung 10 wird jeweils ein Hash aus den vier Transaktionen gebildet und als R1-R4 betitelt. Die dargestellten Pfeile zeigen auf den Wert, auf den der respektive Hash referenziert (Drescher, 2017, S. 121). Als nächstes wird ein zusätzlicher Hash für die Kombination von R1 und R2 gebildet, woraus R12 entsteht (Drescher, 2017, S. 121). Transaktion 3 und 4 durchlaufen diesen Prozess ebenfalls, mit dem Resultat R32 (Drescher, 2017, S. 121). Bei der Hash-Referenz R handelt es sich um den Merkle Tree Root, der Root-Hash, oder auch Wurzel genannt, bezieht sich nun auf alle Transaktionen, obwohl es sich nur um einen einzelnen Hash handelt (Drescher, 2017, S. 88). Dies bedeutet, dass sobald eine Transaktion nachträglich manipuliert wird, sich der Root-Hash ebenfalls ändert (Drescher, 2017, S. 88).

«Der Proof-of-Work Algorithmus stellt den Minern eine Aufgabe, welche es zu lösen gilt. Das Ziel ist das Finden einer bestimmten Zahl, welche auch Nonce genannt wird. […] Ergebnis gewissen Bedingungen entspricht.»

Beim Proof-of-Work Algorithmus handelt es sich um eine spezifische Art eines Konsens-Mechanismus, einen Prozess, der Konsens unter den Netzwerkteilnehmern schaffen soll, was von Laurence (2017, S. 12) wie folgt beschrieben wird: «In the blockchain world, consensus is the process of developing an agreement among a group of commonly mistrusting shareholders». Der Grund für die Verwendung eines Konsens-Mechanismus ist das Misstrauen zwischen den Netzwerkteilnehmern und die Annahme, dass die Blockchain entweder von externen oder internen Quellen angegriffen werden könnte (Laurence, 2017, S. 13). Um einen Angriff auf die Blockchain zu verhindern, müssen Miner für die Erstellung eines neuen Blockes zuerst ein aufwendiges kryptographisches Rätsel lösen, welches auf Hash-Funktionen basiert (Courtois et al., 2014, S. 131-132). Der Miner, welcher das Rätsel als erstes lösen kann, darf den neuen Block erstellen (Vranken, 2017, S. 2). Um eine Blockchain nachhaltig zu manipulieren, müssten die Angreifer mindestens 51 Prozent der gesamten Rechenkapazität des Netzwerks besitzen, um langfristig schneller neue Blöcke erstellen zu können als die konkurrierenden Miner (Tapscott & Tapscott, 2016, S. 340-341). Ein solches Unterfangen wäre jedoch nur mit enormen Schwierigkeiten und finanziellem Investment möglich (Courtois et al., 2014, S. 132).

Beim kryptographischen Rätsel gilt es eine spezielle Zahl (Nonce) zu finden, welche in Kombination mit dem restlichen Header des Blockes einen Hash produziert, welcher bestimmte Bedingungen erfüllt (Zheng et al., 2016, S. 8). Einfach formuliert handelt es sich bei dieser Bedingung um die Vorschrift, dass der berechnete 256-Bit Hash (eine Binärzahl mit 256 Stellen), per 10. April 2018, mit mindestens 73 Nullen (Abbildung 11) beginnen muss (Courtois et al., 2014, S. 137).



* Der Hash des gesamten Blockes darf einen vordefinierten Wert nicht überschreiten, dieser Wert wird auch als Schwierigkeitsstufe des Proof-of-Work bezeichnet und bedeutet, dass der Hash mit einer bestimmten Anzahl von 0 beginnen muss (Krombholz et al., 2016, S. 557).

Abbildung 11: Proof-of-Work

Je höher die Anzahl von Nullen, desto anspruchsvoller ist das Rätsel (Bowden, Keeler, Krzesinski & Taylor, 2018, S. 2). Mit wie vielen Nullen der berechnete Hash mindestens beginnen muss, ist kein fixer Wert, sondern wird alle 2016 erstellten Blöcke angepasst, um die durchschnittlich benötigte Zeit für das Finden der Lösung und somit die benötigte Zeit für die Erstellung eines neuen Blockes bei 10 Minuten zu halten (Bowden et al., 2018, S. 2). Die Anpassung der Schwierigkeit ist notwendig, um mit den Fortschritten der Mining-Hardware mitzuhalten, da sich dadurch die Geschwindigkeit, ausgedrückt in berechneten Hashes pro Sekunde, stetig erhöht (Vranken, 2017, S. 2). Die Definition der Schwierigkeit anhand der Anzahl benötigter Nullen ist jedoch nur eine Approximation, die allerdings einfach zu verstehen ist. Tatsächlich handelt es sich bei dem Maximalwert des Hashes um eine Zahl, die als Target bezeichnet wird, welche unter Berücksichtigung der aktuellen Schwierigkeit und des von der Bitcoin-Blockchain gesetzten höchstmöglichen Target-Werts von 2^{224} (höher bedeutet einfacher) berechnet werden kann (Bowden et al., 2018, S. 2). Mit der in Abbildung 12 dargestellten Formel von Bowden et al. (2018, S. 2) und dem aktuellen (10. April 2018) Schwierigkeitsgrad der Bitcoin-Blockchain von 3'511'060'552'899 (Bitcoinwisdom, 2018), kann der maximal erlaubte Wert des Hashes (Target) berechnet werden: $7.678576391*10^{54}$.

$$D_i = \frac{2^{224}}{L_i}$$

Abbildung 12: Berechnung des Schwierigkeitsgrads (D) und Targets (L) (Bowden et al., 2018, S. 2)

Zu Beginn dieses Abschnitts wurde die Bedingung für den Hash-Wert des gesamten Block-Headers so formuliert, dass der 256-Bit Hash mit 73 Nullen beginnen muss. Durch die Umwandlung des berechneten Targets in eine Binärzahl (Abbildung 13) wird ersichtlich, dass diese Aussage im Grunde korrekt ist, jedoch missverstanden werden kann.

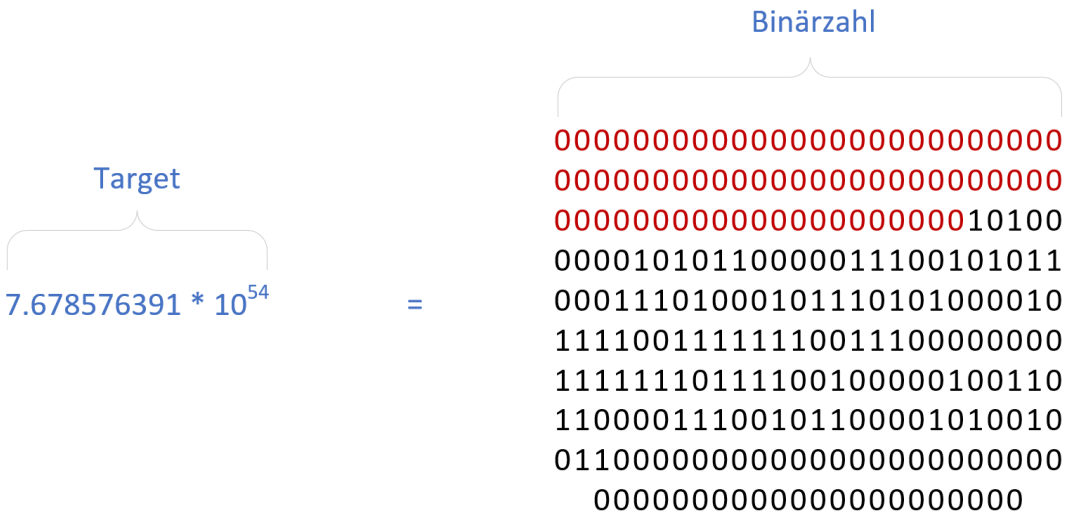


Abbildung 13: Target als Binärzahl

«Miner versuchen, den Wert dieser Nonce durch ein Trial-and-Error Verfahren herauszufinden, wobei sie in Konkurrenz mit den restlichen Minern des Netzwerks stehen, da nur der erste Miner, welcher eine gültige Nonce gefunden hat, den Block erstellen darf.»

Obwohl den Minern die Anforderungen an den Output (Anzahl Nullen) und den grössten Teil des Inputs (alles bis auf die Nonce) bekannt ist, können sie diese Informationen nicht zu ihrem Vorteil nutzen, um die gesuchte Nonce zu finden. Dies liegt an den beiden bereits in Abbildung 8 und 9 beschriebenen Eigenschaften des 256-Bit Hash-

Algorithmus (Vranken, 2017, S. 2). Erstens führen auch kleinste Änderungen des Inputs zu komplett unterschiedlichen Outputs und zweitens ist es unmöglich, anhand eines vordefinierten Outputs auf einen bestimmten Input rückzuschliessen (Vranken, 2017, S. 2). Somit bleibt Minern nichts anderes übrig, als die gesuchte Nonce zu erraten (Vranken, 2017, S. 2). Je mehr Hashwerte ein Miner pro Sekunde (Hash-Rate) berechnen kann, desto schneller kann die gesuchte Nonce gefunden werden (Vranken, 2017, S. 2). Aus diesem Grund verwenden Miner speziell für Aufgabe geeignete Hardwarekomponenten, um eine möglichst hohe Hash-Rate zu erreichen (Vranken, 2017, S. 2).

Unter Berücksichtigung des aktuellen Schwierigkeitsgrads kann berechnet werden, wie viele Anläufe durchschnittlich benötigt werden, um den Hash zu finden. So ist die Wahrscheinlichkeit, berechnet anhand der Formel von Courtois et al. (2014, S. 136), per Zufall im ersten Anlauf eine passende Nonce zu finden, bei $6.631347997*10^{-21}$ Prozent. Mit einer totalen Hashrate von 25'133'150’415$*10^9$ pro Sekunde im gesamten Bitcoin-Netzwerk (Bitcoinwisdom, 2018) werden für einen neuen Block durchschnittlich $1.508*10^{22}$ Versuche benötigt, was ungefähr 10 Minuten dauert.

«Sobald eine gültige Nonce gefunden wurde, ca. alle zehn Minuten, wird das Ergebnis zur Verifikation an das gesamte Netzwerk gesendet und muss bestätigt werden.»

Sobald ein Miner eine Nonce gefunden hat, mit der sich ein gültiger Hash generieren lässt, muss er das Ergebnis an die restlichen Miner im Netzwerk schicken, da der neue Block nur Teil der Hauptkette (Schwarze Blöcke in Abbildung 14) werden kann, wenn das Ergebnis und somit der neue Block weit verbreitet ist (Courtois et al., 2014, S. 132-133). Obwohl es sich bei der Berechnung der Nonce um einen arbeitsaufwändigen Prozess handelt, ist der resultierende Hash sehr einfach zu validieren, da dazu nur eine einzige Hash-Berechnung (Input: Block Header und zu überprüfende Nonce) benötigt wird (Kewell et al., 2017, S. 432). Damit ein neuer Block und somit die darin enthaltenen Transaktionen endgültig bestätigt und der Transaktionshistorie hinzugefügt werden können, reicht das Finden der Nonce und das Kommunizieren des Ergebnisses nicht aus (Drescher, 2017, S. 174-175). Damit die Transaktionen der Blockchain hinzugefügt werden, muss der entsprechende Block Teil der Hauptkette sein

(Drescher, 2017, S. 174-175). Dies ist ein weiterer Aspekt des Proof-of-Work Konsens-Mechanismus, wobei sich die Mehrheit der Teilnehmer des Netzwerks einig werden, also Konsens darüber erreichen, welche Blöcke zur Hauptkette gehören und welche nicht (Drescher, 2017, S. 168). Wie sich ein Mehrheitsentscheid in der Bitcoin-Blockchain bilden kann, erklärt Nakamoto (2008, S. 3): «Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.». Konsens bedeutet, dass sich alle Miner einig darüber werden, was der aktuelle Stand der Blockchain ist (Laurence, 2017, S. 12-13). Dies ist ein entscheidender Aspekt der Blockchain-Technologie, da es durchaus vorkommen kann, dass gleichzeitig mehr als ein Block an die bestehende Kette angehängt wird, dies wird in Abbildung 14 nochmals dargestellt (Olnes et al., 2017, S. 356).

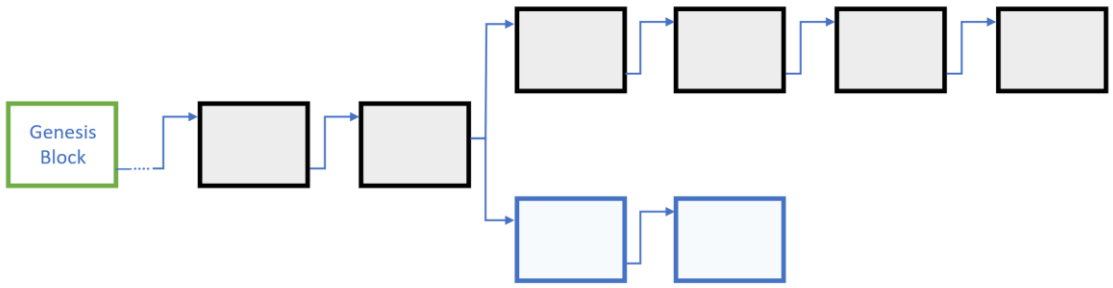


Abbildung 14: Struktureller Aufbau einer Blockchain (Wright & De Filippi, 2015, S. 8)

Eine Gabelung kann aus unterschiedlichen Gründen auftreten; so argumentiert Drescher (2017, S. 169-171), dass das Versenden eines neuen Blockes im Netzwerk Zeit in Anspruch nimmt und wegen Verzögerungen, oder wenn zwei Miner fast zeitgleich das Proof-of-Work lösen, die restlichen Teilnehmer des Netzwerkes unterschiedliche Blöcke empfangen können. Um dies in einem Beispiel zu veranschaulichen (Abbildung 15), wird angenommen, dass 60 Prozent (Teil A) des Netzwerks den Block #4a empfängt und die restlichen 40 Prozent (Teil B) den Block #4b.

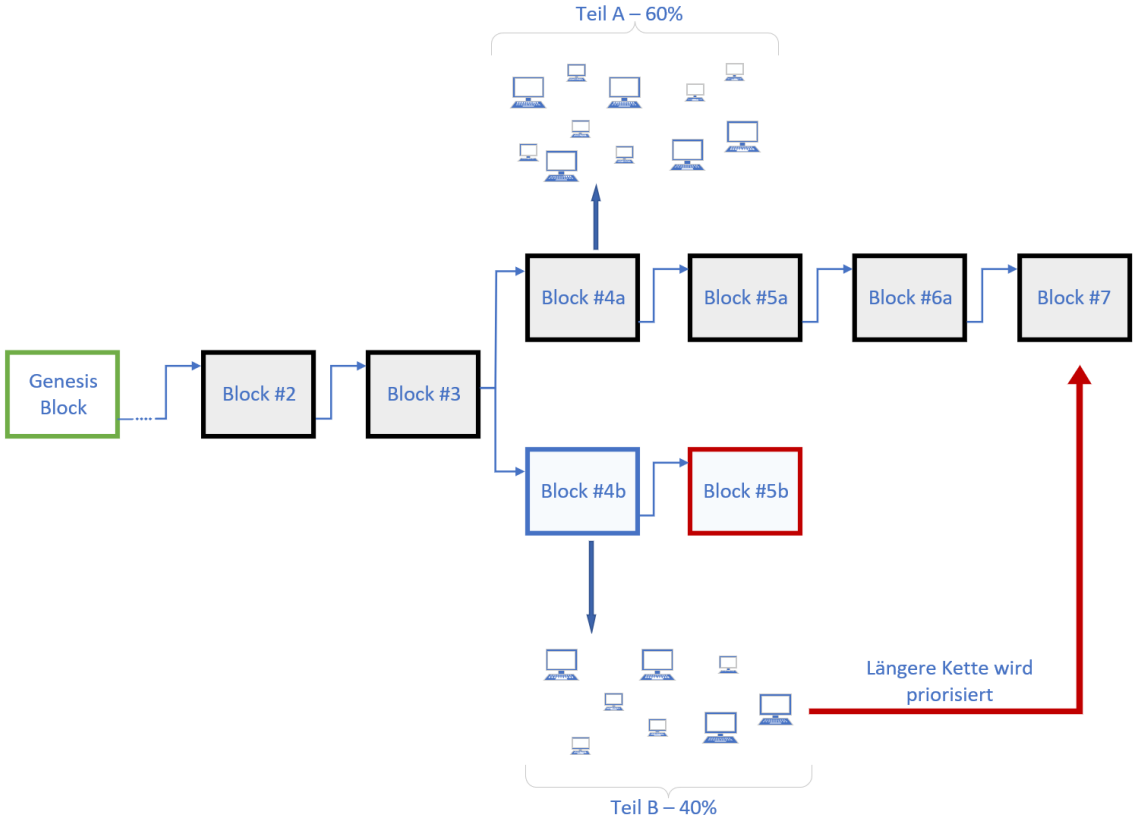


Abbildung 15: Priorisierung der längeren Kette

Das Netzwerk ist nun in zwei Gruppen gespalten, die jeweils versuchen, auf Basis des neusten Blockes, die (nun aber unterschiedliche) Blockchain zu erweitern. Wie von Nakamoto (2008, S. 3) beschrieben, wird immer die längste Kette priorisiert. Da zum jetzigen Zeitpunkt beide der neu entstandenen Ketten die gleiche Länge aufweisen, ist noch kein Konsens möglich. Allerdings verfügt Teil A des Netzwerks, deren Miner am Proof-of-Work des Blockes #5a arbeiten, über mehr rechnerische Kapazitäten als Teil B. Folglich wird die Kette von Teil A schneller wachsen und wird als Hauptkette definiert.

Die Folge eines solchen Ereignisses ist, dass alle Blöcke, die nicht Teil der Hauptkette sind, als invalide deklariert werden (Drescher, 2017, S. 174-175). Die als invalid erklärten Blöcke werden auch als «orphan blocks» oder Waisenblöcke bezeichnet (Drescher, 2017, S. 174-175). Diese Waisenblöcke, inklusive der darin enthaltenen Transaktionen, werden nicht in die Transaktionshistorie der Blockchain aufgenommen und behandelt, als würden sie nicht existieren (Drescher, 2017, S. 175). Für die Miner, welche die Waisenblöcke ursprünglich erstellt haben, bedeutet dies, dass die ausbezahlte Belohnung rückgängig gemacht wird und die Transaktionen beim nächsten Block der Hauptkette nochmals berücksichtigt werden (Drescher, 2017, S. 175).

«Da für die Berechnung der Nonce Zeit, Strom und Geld in Hardware investiert werden muss, wird die Erstellung eines neuen Blockes mit Bitcoins belohnt.»

Die Belohnung für die Arbeit des Miners besteht aus zwei Teilen (Vranken, 2017, S. 2). Einerseits aus den Transaktionskosten und andererseits aus einem «block reward», einer Belohnung von aktuell 12.5 Bitcoins, für die erfolgreiche Erstellung eines neuen Blockes (Vranken, 2017, S. 2). Die Block-Belohnung ist eine sogenannte «coinbase transaction» (Krombholz et al., 2016, S. 558). Das Spezielle daran ist, dass die ausbezahlten Bitcoins keinen Vorbesitzer haben, sondern neu generiert werden (Krombholz et al., 2016, S. 558). Dadurch vergrössert sich die Anzahl der im Umlauf befindlichen Bitcoins mit jedem neuen Block (Vranken, 2017, S. 2). Dennoch ist das Angebot begrenzt, denn alle 210'000 Blöcke wird die Block-Belohnung halbiert, bis zu einem Minimum von 10^{-8} Bitcoins pro Block (Vranken, 2017, S. 2). Dadurch werden bis ins Jahr 2140 (Vranken, 2017, S. 2) insgesamt 21 Millionen Bitcoins in Umlauf gebracht (Bheemaiah, 2017, S. 57).

«Die Anwendung des Proof-of-Work Konsensmechanismus trägt zur Datenintegrität der Transaktionen bei.»

In den bisherigen Abschnitten wurde der Mining-Prozess und der Proof-of-Work Konsensalgorithmus genauer erklärt. Es wurden auch die Eigenschaften des SHA-256 Hash-Algorithmus erläutert und anhand eines Beispiels die Vorgehensweise beim Auftreten von mehreren Ketten dargelegt. Ein wichtiger Aspekt der Blockchain-Technologie wurde jedoch noch nicht behandelt: Die Unveränderbarkeit der Transaktionen durch das Verketten von aufeinanderfolgenden Blöcken.

Wie bereits erwähnt, trägt die Peer-to-Peer-Netzwerkarchitektur zur Sicherheit und Unveränderlichkeit der Transaktionen bei und zusätzlich gewährleistet der Konsensmechanismus die Datenintegrität (Olnes et al., 2017, S. 356). Ein entscheidender Faktor ist auch die Verkettung der Blöcke, dies geschieht durch die Weitergabe des Parent-Hashs an den nächsten Block (Courtois et al., 2014, S. 135). Der Parent-Hash ist eine Art Zusammenfassung des vorangehenden Blockes in Form eines kryptographischen Hashs (Courtois et al., 2014, S. 135). Dies führt dazu, dass eine nachträgliche Änderung oder Manipulation früherer Transaktionen sofort erkannt werden kann, da

sich auch bei der kleinsten Änderung der Output Hash ändern würde und somit alle darauffolgenden Blöcke (Courtois et al., 2014, S. 132).

2.4 Klassifikation der Blockchains

Im Kapitel 2.3 zur Funktionsweise wurde die Blockchain-Technologie anhand der Bitcoin-Blockchain erklärt. Jedoch gibt es unterschiedliche Arten von Blockchains, die in verschiedene Kategorien unterteilt werden können (Laurence, 2017, S. 21). Gemäss Olnes et al. (2017, S. 360) können Blockchains, wie in Tabelle 1 dargestellt, in private, public, permissioned und permissionless unterteilt werden.

	Permissioned	Permissionless
Public	No restricted data access or transactions. Only a restricted set of nodes can participate in the consensus mechanism.	No restriction on access, transaction (data writing) or validation.
Private	Restricted access, data writing and validation. Only the owner determines who can participate.	Restrictions on access and who can transact. No restriction on participation in the consensus mechanism.

Tabelle 1: Arten von Blockchains (Olnes et al., 2017, S. 360)

Ob eine Blockchain public oder private (öffentlich oder privat) ist, wird dadurch bestimmt, wer Zugriff auf die Kopien des Registers und die darin enthaltenen Daten hat und wer nicht (Olnes et al., 2017, S. 360). Die Eigenschaften permissioned und permissionless (beschränkt und unbeschränkt) beziehen sich darauf, wer Teil des Netzwerks sein und am Konsensmechanismus teilnehmen kann (Olnes et al., 2017, S. 360). Olnes et al. (2017, S. 360-361) liefern in Tabelle 2 eine Übersicht zu den Unterschieden zwischen öffentlichen und privaten Blockchains

Öffentliche Blockchains sind gross und dezentralisiert, jeder kann freiwillig daran teilnehmen (Laurence, 2017, S. 21). Zusätzlich sind öffentliche Blockchains sicherer als private oder Blockchains mit Zugriffsrechten, jedoch auch langsamer und teurer im Unterhalt (Laurence, 2017, S. 21).

.

	Public Blockchains	Private Blockchains
Who can update	Everybody	Appointed entities
Who can produce data	All users	Customers and/or partners
Incentive to follow rules	Economic	Reputation
Storage	Distributed	Centralized
Trust central actors	No	Yes
Transaction costs	Varies from low to high	Low
Capacity/throughput	Low/slow	High/fast
Immutability	Strong	Unclear
Currency/token	Yes	No
Examples	Bitcoin, Ethereum	HyperLedger, Corda

Tabelle 2: Unterschiede zwischen öffentlichen und privaten Blockchains (Olnes et al., 2017, S. 361)

Private Blockchains erlauben der Öffentlichkeit keinen Einblick in das Register, sondern nur einer ausgewählten Gruppe von Teilnehmern (Laurence, 2017, S. 21). Vorteile von privaten Blockchains sind unter anderem die hohe Geschwindigkeit und die geringe Latenz (Laurence, 2017, S. 21). Im Gegensatz zu öffentlichen Blockchains benötigen private Blockchains nicht zwingend Tokens in Form einer Kryptowährung, da kein zusätzlicher finanzieller Anreiz für die Instandhaltung der Blockchain benötigt wird (Laurence, 2017, S. 21). Private Blockchains haben allerdings auch den Nachteil, dass sie nicht von den Sicherheitsvorteilen dezentralisierter Netzwerke profitieren können (Laurence, 2017, S. 21).

3 Ethereum

Das Ethereum-Projekt besitzt eine der am weitesten entwickelten und zugänglichsten Blockchains und ist industrieführend im Bereich der Blockchain Innovation- und Use Case-Entwicklung (Laurence, 2017, S. 51). Bei der «Ethereum Blockchain» handelt es sich nicht um eine normale Blockchain, sondern eher um eine universelle Kryptowährungsplattform (Swan, 2015, S. 21). Swan (2015, S. 21) beschreibt die Ethereum Plattform wie folgt: «Rather than being a blockchain, or a protocol running over a blockchain, or a metaprotocol running over a protocol like other projects, Ethereum is a fundamental underlying infrastructure platform that can run all blockchains and protocols, rather like a unified universal development platform.». Ethereum kann als eine Erweiterung der Bitcoin-Blockchain angesehen werden und ermöglicht eine vielseitigere Anwendung der Technologie (Nofer et al., 2017, S. 185). Ermöglicht wird diese Vielseitigkeit durch Smart Contracts, welche in den folgenden Abschnitten genauer erklärt werden.

3.1 Smart Contracts

Smart Contracts können als Verträge angesehen werden, allerdings ohne eine zentrale Einheit, welche die Erfüllung des Vertrages vollstreckt (Laurence, 2017, S. 58). In einem Smart Contract werden von den beteiligten Parteien die Bedingungen formuliert, zu denen ein Vertrag durchgeführt werden soll (Olnes et al., 2017, S. 356). Wenn die definierten Bedingungen erfüllt sind, wird der Vertrag vollautomatisch ausgeführt (Olnes et al., 2017, S. 356). Im White Paper von Ethereum beschreibt Buterin (2014, S. 1) Smart Contracts als Mittel, um digitale Vermögenswerte zu verschieben, gesteuert mittels vorbestimmte Regeln. Weiter beschreibt Buterin (2014, S. 13) Smart Contracts als kryptographische Boxen, die einen Wert beinhalten, sich jedoch nur öffnen lassen, wenn bestimmte Bedingungen erfüllt sind.

Die Idee von Smart Contracts ist jedoch nicht erst mit der Entwicklung der Blockchain entstanden, sondern stammt von Szabo (1997, S. 2), der das Konzept des Smart Contracts vorstellte, welches Computerprotokolle und User-Interfaces kombinierte, um Verträge zu vollstrecken. In Kombination mit der Blockchain-Technologie lassen sich Smart Contracts in einer Vielzahl von Bereichen einsetzen (Nofer et al., 2017, S. 185). Der innovative Einsatz von Smart Contracts trägt weiter zur Disintermediation

bei, bei der nicht nur Banken als Intermediär von Transaktionen, sondern auch Anwälte bei der Durchführung von Verträgen ausgeschlossen werden können (Fairfield, 2014, S. 39). Einfach formuliert können Smart Contracts als Computercode angesehen werden, welcher Teil der Blockchain ist und prinzipiell aus «if this then do that» Statements besteht (Morabito, 2017, S. 103).

Um die Funktionsweise von Smart Contracts verständlich aufzeigen zu können, wird im folgenden Abschnitt das Anwendungspotential von Smart Contracts im Bereich des Managements von geistigen Eigentumsrechten anhand eines Beispiels erklärt, welches auf dem Artikel von Meitinger (2017, S. 372-375) basiert.

Die Ausgangslage des Beispiels befasst sich mit den rechtlichen Aspekten beim Erwerb und Erhalt von geistigen Eigentumsrechen (IPR), bei welchen die bestehenden Gesetze einzuhalten sind, gesetzliche Fristen beachtet und Gebühren zu bestimmten Zeiten bezahlt werden müssen (Meitinger, 2017, S. 372). Dies erfordert ein funktionierendes Fristenüberwachungssystem, welches häufig von Patentanwaltskanzleien und spezialisierten Rechtsanwälten als Dienstleistung angeboten wird (Meitinger, 2017, S. 372). Die Patentanwaltskanzleien agieren, wie in Abbildung 16 dargestellt, als Intermediäre zwischen Anmelder und Patentamt (Meitinger, 2017, S. 372).

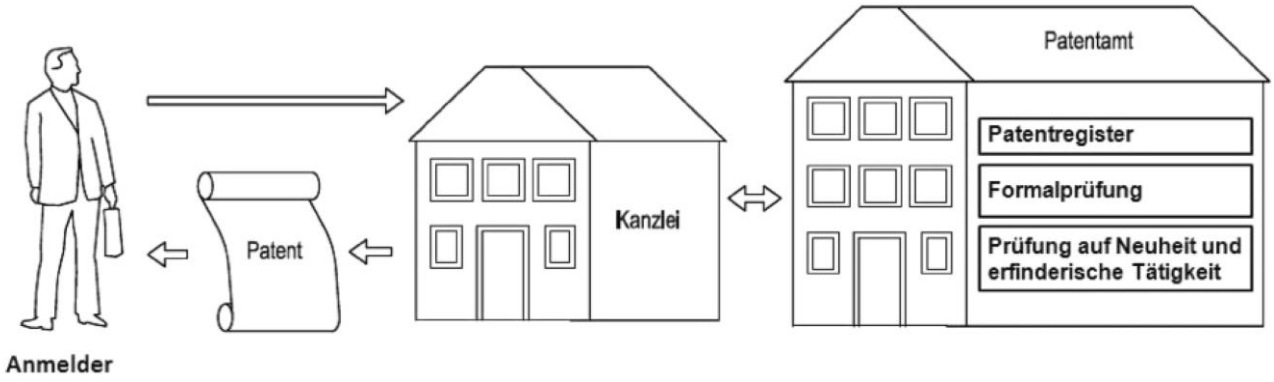


Abbildung 16: Verwaltung von IPRs mit einer Kanzlei (Meitinger, 2017, S. 373)

Gemäss Meitinger (2017, S. 372) können die Bestimmungen des Patentgesetzes als If-then-Beziehung in einem Smart Contract implementiert werden. Als Beispiel nennt er die Überprüfung der formalen Voraussetzungen für eingereichte Patentanträge und die Bewertung der thematischen Einordnung der Erfindung, inklusive automatischer Korrekturen bei formalen Fehlern und des Hinweisens auf Mängel bei der thematischen Einordnung durch einen Smart Contract. Folglich wären Smart Contracts in der Lage, die Einreichung beim Patentamt und die darauffolgende Korrespondenz bis zur

Erteilung des Schutzrechts zu übernehmen (Meitinger, 2017, S. 372-373). Abbildung 19 stellt die Anwendung von Smart Contracts im Kontext von IPR dar.

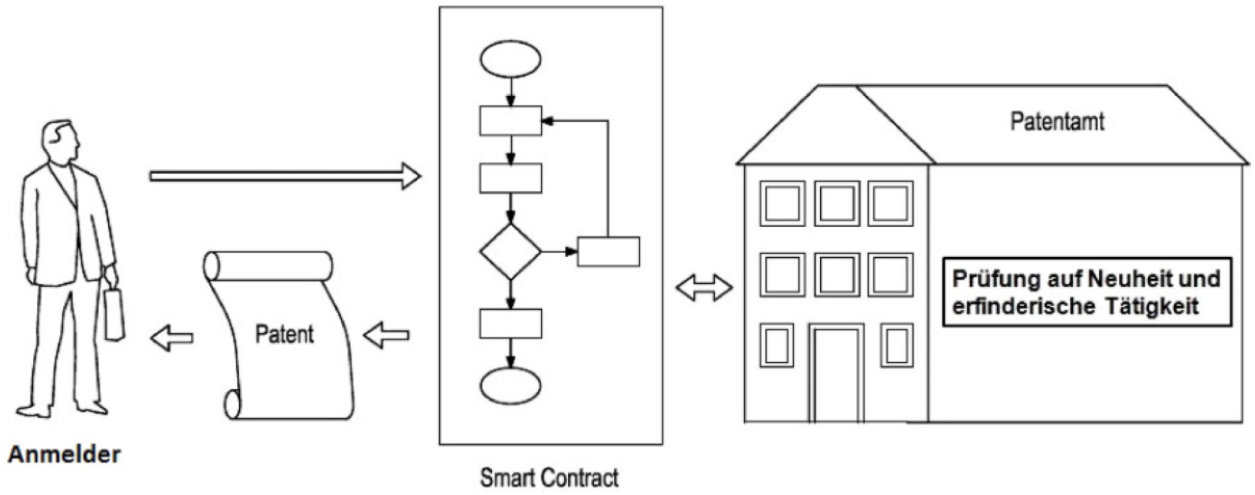


Abbildung 17: Verwaltung von IPRs mit Smart Contracts (Meitinger, 2017, S. 373)

Wie in Abbildung 17 ersichtlich, übernehmen Smart Contracts die Kommunikation zwischen Schutzrechtinhabern und Patentamt (Meitinger, 2017, S. 373). Laut Meitinger (2017, S. 373) werden in dem Patentregister, welches online zugänglich ist, verschiedene Prozesse als eine Abfolge von Transaktionen dargestellt:

- Einreichung der Patentanmeldung
- Erstellung eines Prüfbescheids durch das Patentamt
- Vollautomatische Erwiderung auf den Bescheid
- Patenterteilung
- Lizenzvergabe
- Verkauf des Patents
- Zahlung von Jahresgebühren
- Inanspruchnahme von Prioritäten
- Nichtigkeitsverfahren

Gemäss Meitinger (2017, S. 373) kann diese Folge von Ereignissen durch die Sequenz einer Blockchain innerhalb eines Smart Contracts dargestellt werden und somit das Patentregister des Patentamts ersetzen. Hierbei kann der Prozess der Zahlung von Jahresgebühren (Abbildung 18) als Beispiel für die logische Funktionsweise eines Smart Contracts herangezogen werden (Meitinger, 2017, S. 374).

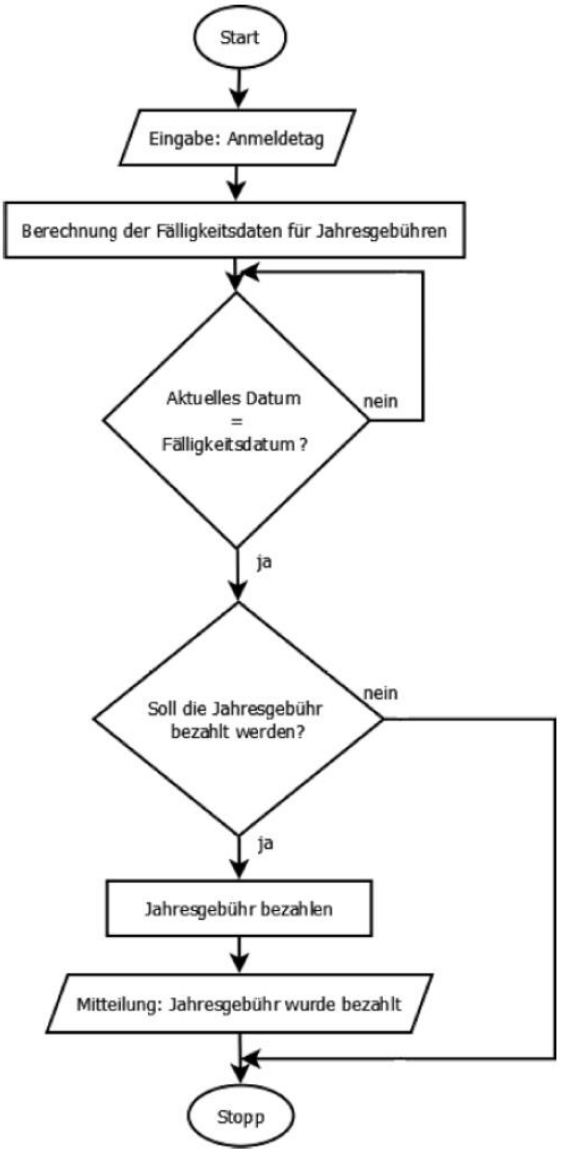


Abbildung 18: Flussdiagramm für die Bezahlung von Jahresgebühren (Meitinger, 2017, S. 374)

Der in Abbildung 18 veranschaulichte logische Ablauf eines Smart Contracts basiert auf einer Patentanmeldung mittels Anmeldetag und könnte die Fälligkeit der Jahresgebühren überwachen und dessen Bezahlung selbsttägig vornehmen (Meitinger, 2017, S. 374). Ein Kritikpunkt an dem von Meitinger (2017, S. 374) visualisierten Prozess ist, dass nicht überprüft wird, ob das abgefragte Patent überhaupt noch Gebührenpflichtig ist.

Ein Patentamt befasst sich im Wesentlichen mit drei Hauptaufgaben (Abbildung 16), dem Führen eines öffentlichen Patentregisters, der Kontrolle der formalen Erfordernisse und der Prüfung auf Neuheit und erfinderische Tätigkeit (Meitinger, 2017, S. 374). Meitinger (2017, S. 374) legt nahe, dass die ersten zwei Aufgaben, das Führen

des Patentregisters und die Formalprüfung, durch den Einsatz der Blockchain-Technologie und Smart Contracts hinfällig werden.

3.2 Decentralized Autonomous Organizations

DOAs sind langfristige Smart Contracts, welche Wirtschaftsgüter und kodierte Statuten eines ganzen Unternehmens beinhalten (Buterin, 2014, S. 1). Eine DAO ist, anders formuliert eine Organisation, welche weder einen Geschäftsführer noch eine andere zentrale Führungsinstanz besitzt (Meinel, Gayvoronskaya & Schjakin, 2018, S. 74). Stattdessen basiert eine DAO auf einer dezentralen Struktur mit festgelegten Regeln, welche automatisierte Entscheidungsfindungen ermöglicht (Meinel et al., 2018, S. 74). So können auf der Ethereum-Plattform selbstausführende Smart Contracts eingebunden werden, sodass sie eine ganze Organisation repräsentieren (Asharaf & Adarsh, 2017, S. 82). Innerhalb dieser Smart Contracts ist die gesamte Businesslogik programmiert, welche ausgeführt wird, sobald bestimmte Ereignisse eintreten (Asharaf & Adarsh, 2017, S. 82). Das Konzept einer DAO ist in Abbildung 19 dargestellt.

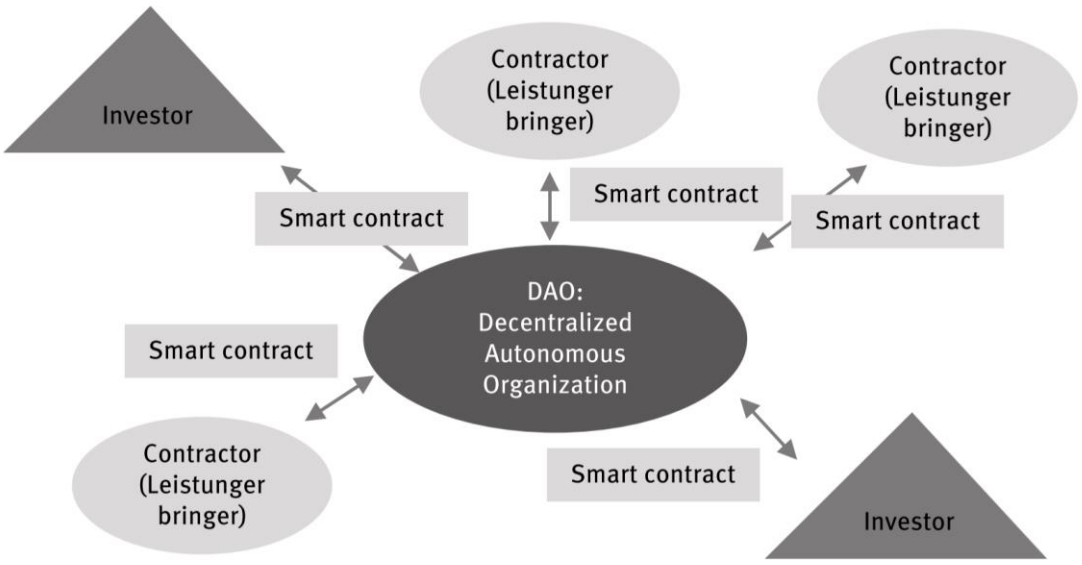


Abbildung 19: Konzept einer DAO (Tosovic, 2016, S. 161)

Im Zentrum des Konzepts steht die DAO, welche über Smart Contracts mit der Umwelt, Investoren und externen Leistungserbringern in Verbindung steht (Tosovic, 2016, S. 161). Investoren können an Projekten der DAO teilnehmen, indem sie Tokens (meist in Form einer Kryptowährung) kaufen (Tosovic, 2016, S. 161). Abhängig von

der DAO kann es sich bei den Tokens zum Beispiel um eine kryptographische Währung handeln, und erhalten im Gegenzug Stimmrechte für die Projekte der DAO (Tosovic, 2016, S. 161). Die mit Stimmanteilen verknüpften Tokens können von den Investoren dazu genutzt werden, um über die Finanzierung einzelner Projekte abzustimmen, wobei sie in Relation zum Stimmrechtsanteil an den zukünftigen Erträgen des Projekts beteiligt sind (Tosovic, 2016, S. 161).

Gemäss Tosovic (2016, S. 161-162) sind die besonderen Eigenschaften einer DAO die Anonymität, die Integrität und der Automatismus. Investoren bleiben sowohl beim Kauf der Tokens als auch bei der Ausübung ihres Stimmrechts anonym (Tosovic, 2016, S. 161). Die Integrität wird dadurch gewährleistet, da alle Prozesse, wie zum Beispiel die Abstimmung und die Verteilung der Einkünfte, über die Blockchain laufen (Tosovic, 2016, S. 161-162). Dies stellt ebenfalls die notwendige Transparenz sicher und reduziert den Aufwand einer Revision (Asharaf & Adarsh, 2017, S. 33). Da sich eine DAO auf einer Blockchain befindet, kann der vorprogrammierte Code nur geändert werden, wenn mindestens 51 Prozent des Netzwerks zustimmen (Asharaf & Adarsh, 2017, S. 82).

4 Folgen der Blockchain-Technologie

Einer der grössten Durchbrüche der Blockchain-Technologie ist die Lösung eines Problems, welches als «double-spending problem» oder Problem des doppelten Ausgebens bezeichnet wird (Tapscott & Tapscott, 2016, S. 52-53). In der Informatik wird dieses Problem auch als «Byzantine General's problem» bezeichnet wird (Davidson et al., 2016, S. 2). Das Problem des doppelten Ausgebens (Abbildung 20) beschreibt die Problematik, dass eine einzelne, in diesem Sinne einzigartige, Werteinheit (zum Beispiel 100 Schweizer Franken auf einem Bankkonto) mehrfach ausgegeben werden könnte (Tapscott & Tapscott, 2016, S. 52-53).

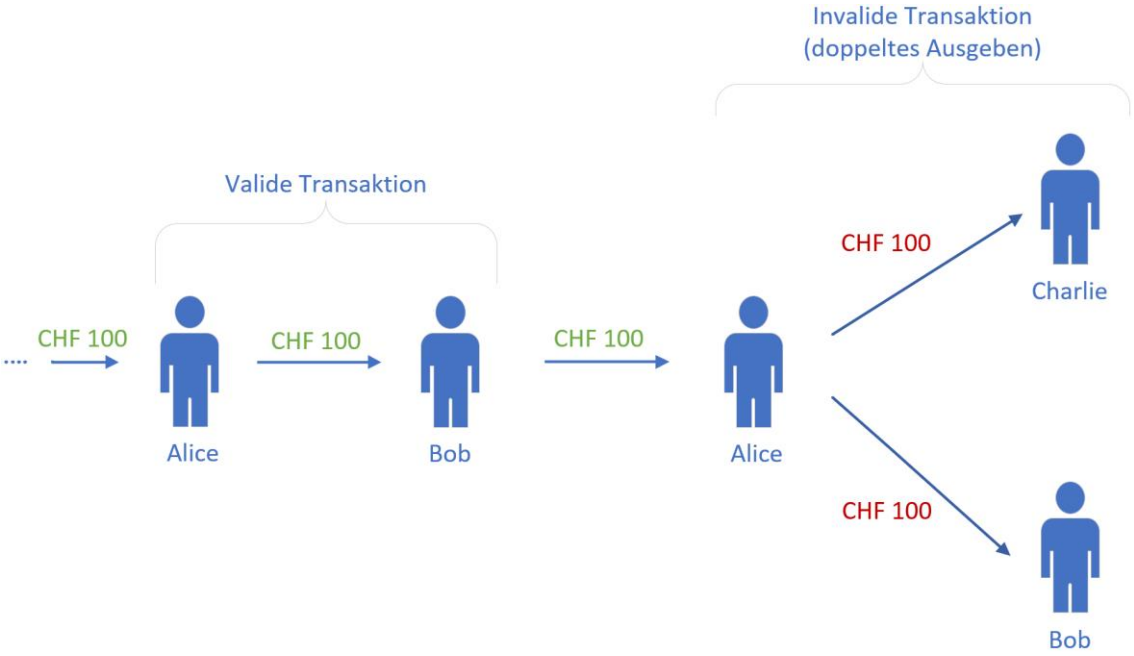


Abbildung 20: Problem des doppelten Ausgebens (Kuo, Kim & Ohno-Machado, 2017, S. 1212)

Ohne zentrale Kontrollinstanz, würde eine Transaktion zwischen unterschiedlichen Parteien auf dem Vertrauen basieren, dass keine Partei diese Problematik ausnutzt (Morabito, 2017, S. 22). Bis anhin wurde dieses Problem gelöst, indem Intermediäre für die Transaktion dieser 100 Schweizer Franken hinzugezogen wurden, welche als eine zentrale Instanz agiert haben und sicherstellten, dass sich diese 100 Franken nicht an mehreren Orten gleichzeitig befinden können (Tapscott & Tapscott, 2016, S. 52-53). Bei den Intermediären für Transaktionen kann es sich beispielsweise um einen Überweisungsdienst (Western Union), eine Geschäftsbank (Citicorp), eine staatliche Stelle (Commonwealth Bank of Australia), ein Kreditkartenunternehmen (VISA) oder um einen Online-Zahlungsplattform wie Paypal handeln (Tapscott & Tapscott, 2016,

S. 53). Die Involvierung von Intermediären in den Abwicklungsprozess führt allerdings zu höheren Transaktionskosten (Tapscott & Tapscott, 2016, S. 30) und längeren Transaktionsabwicklungsdauer (Tapscott & Tapscott, 2016, S. 53).

Die Blockchain ist eine technische Lösung für das Problem des doppelten Ausgebens, indem die Validierung der Transaktionen über ein dezentralisiertes Netzwerk, basierend auf dem Proof-of-Work-Konsensalgorithmus, stattfindet (Davidson et al., 2016, S. 2). Somit ist die Blockchain-Technologie die erste Lösung, welche Vertrauen in einer unsicheren Umgebung schafft, ohne auf Drittparteien zurückgreifen zu müssen (Olnes et al., 2017, S. 356).

Gemäss Olnes et al. (2017, S. 359) sind die grundsätzlichen Vorteile der Blockchain-Technologie die verbesserte Datenintegrität und, weil jede Transaktion und deren Änderungen nachverfolgt werden können, die erhöhte Transparenz. Dies führt, so argumentieren Olnes et al. (2017, S. 359), zur Reduktion von Korruption und Betrug. Zusätzlich erhöhen Smart Contracts (Kapitel 3.1) die Geschwindigkeit und Effizienz bei der Abwicklung von Verträgen und garantieren den beteiligten Parteien, dass die Verträge wie vereinbart ausgeführt werden (Kewell et al., 2017, S. 433).

5 Anwendungspotential in der Gesundheitsbranche

In diesem Kapitel wird das mögliche Anwendungspotential der Blockchain-Technologie in der Gesundheitsbranche analysiert. Dabei werden die unterschiedlichen Einsatzgebiete genauer erläutert und verschiedene Projekte im Bereich der Gesundheitsbranche vorgestellt, welche die Blockchain-Technologie nutzen können, um die operationelle Effizienz und die Sicherheit des Datenaustausches zu verbessern.

5.1 Einleitung

Neben der Finanzbranche gilt das Gesundheitswesen als eine der vielversprechendsten Branchen zur Anwendung der Blockchain-Technologie, insbesondere deswegen, weil die Vertraulichkeit und Richtigkeit der gespeicherten Informationen von höchster Bedeutung sind (Asharaf & Adarsh, 2017, S. 88). Jedoch verlangsamen die starke Regulierung der Branche und bürokratische Ineffizienz den Innovationsprozess im Bereich der elektronischen Erfassung von Patientendaten (Azaria, Ekblaw, Vieira & Lippman, 2016, S. 25). Gemäss Azaria et al. (2016, S. 25) hat der Mangel an innovativen Lösungen im Datenmanagement-Bereich zur Folge, dass Patientendaten nicht über ein einzelnes System zugänglich sind, sondern dass die Daten über verschiedenste Bereiche verteilt sind. Dadurch bilden sich etliche Datensilos, welche den einfachen Zugang zu vergangenheitsbezogenen Patientendaten stark erschweren (Azaria et al., 2016, S. 25). Zusätzlich führt der Anstieg von chronischen Erkrankungen, eine Folge der stetig älter werdenden Bevölkerung, zu einer höheren Komplexität der Koordination von medizinischen Dienstleistungen (Dhillon, Metcalf & Hooper, 2017, S. 125).

Die heutzutage genutzten Technologien stehen allerdings im Kontrast zur wachsenden Komplexität und sind nicht dazu geeignet, alle Aspekte der modernen Gesundheitsversorgung abzudecken, was im Gegenzug die Qualität der erbrachten Dienstleistungen beeinträchtigt (Dhillon et al., 2017, S. 125). Laut Dhillon et al. (2017, S. 125) sind Gründe hierfür, dass zahlreiche Dienstleister in der Gesundheitsbranche noch mit Altsystemen arbeiten, ein Mangel an Integrationsmöglichkeiten für nicht-verkäuferspezifische Technologien besteht, Patientenakten papierbasiert dokumentiert werden und nicht genügend Daten beziehungsweise Informationen auf horizontaler Ebene mit anderen Dienstleistern geteilt werden. Gleichzeitig investieren Spitäler beträchtliche

Summen in die Abwicklung von Versicherungsansprüchen und die administrative Dokumentation, deren Aufwand durch den Einsatz von fortgeschrittenen Technologien eliminiert werden könnte (Dhillon et al., 2017, S. 125). Eine zusätzliche Herausforderung stellt die Kompatibilität zwischen den verschiedenen Systemen unterschiedlicher Anbieter dar (Azaria et al., 2016, S. 25).

Die Blockchain-Technologie hat drei zentrale Grundfunktionen, welche für eine Anwendung in der Gesundheitsbranche entscheidend sein können (Burgwinkel, 2016, S. 13):

- Nachweis der Integrität von Daten
- Registrierung und Beurkundung
- Abwicklung von Transaktionen

Ein auf der Blockchain basierendes System verbessert die Authentizität und Transparenz der Daten im Gesundheitswesen (Angraal, Krumholz & Schulz, 2017, S. 1) und eliminiert den Intermediär zwischen den elektronisch erfassten Patientendaten und den Patienten selbst (Kshetri, 2017a, S. 1031). Die Patienten haben die Kontrolle über ihre Daten und können Doktoren, Apothekern, Versicherungen und anderen Drittparteien den Zugang zu ihren Daten erlauben (Swan, 2015, S. 59). Gemäss Morabito (2017, S. 30) hat die Blockchain-Technologie das Potential, Vertrauen zu schaffen, die Sicherheit zu erhöhen und gleichzeitig Kosten, Zeit und Ressourcenverbrauch, die bei konventionell betriebenen Systemen entstehen, einzusparen. Gleichzeitig kann die Blockchain eine Vereinheitlichung der erfassten elektronischen Gesundheitsdaten herbeiführen, was bis anhin für Gesundheitsdienstleistungsanbieter ein grosses Problem dargestellt hat, da die uneinheitliche Erfassung der Daten einen effizienten Austausch unmöglich macht (Swan, 2015, S. 59-60). Eine einheitliche Erfassung von medizinischen Daten liegt nicht nur im Interesse von Spitälern und anderen Anbietern, sondern ist auch ein kritischer Faktor für die medizinische Forschung, die auf möglichst grosse Datenquellen angewiesen ist und mit den erbrachten Leistungen die Qualität der medizinischen Betreuung nachhaltig verbessern kann (Azaria et al., 2016, S. 25).

In den folgenden Abschnitten wird das Anwendungspotential der Blockchain-Technologie in den verschiedenen Bereichen der Gesundheitsbranche genauer untersucht. Anhand von Beispielen wird der Einsatz einer Blockchain verdeutlicht und es werden

Projekte vorgestellt, welche das Datenmanagement in der Gesundheitsbranche nachhaltig verändern könnten.

5.2 Austausch von Patientendaten über die Blockchain

Ein mögliches Anwendungsgebiet der Blockchain-Technologie ist das Datenmanagement von Gesundheitsdaten, insbesondere der Austausch von Patientendaten. Bei Daten aus dem medizinischen Bereich, beispielsweise Forschungsdaten zu Medikamenten, Diagnosen und andere Patientendaten, ist die Datenintegrität von hohem Interesse, damit nachgewiesen werden kann, dass die erfassten Daten nicht nachträglich manipuliert wurden (Burgwinkel, 2016, S. 14). In Abbildung 21 wird der Ablauf dargestellt, welcher zum Nachweis der Datenintegrität bei einer Blockchain zum Einsatz kommt.

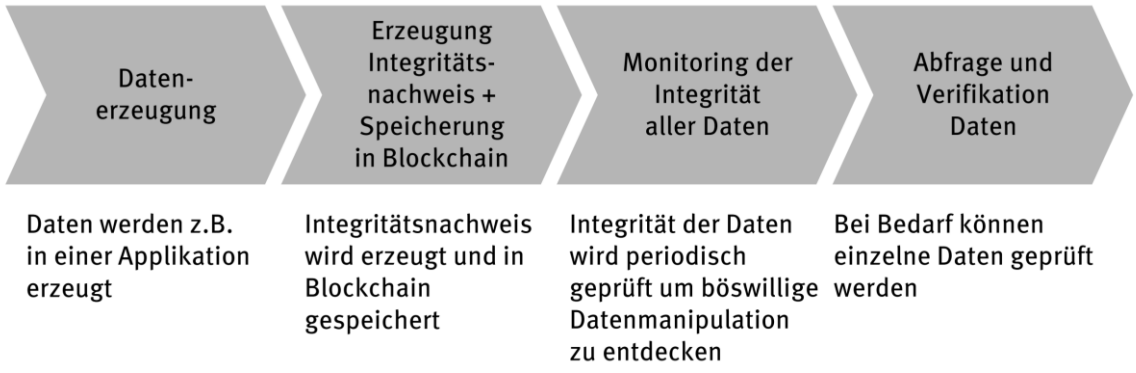


Abbildung 21: Blockchains zum Nachweis der Datenintegrität (Burgwinkel, 2016, S. 14)

In einem ersten Schritt werden die Daten ausserhalb der Blockchain erzeugt, dabei kann es sich beispielsweise um den Besuch eines Patienten beim Arzt handeln. Im zweiten Schritt wird für die erfassten Daten ein Integritätsnachweis erzeugt und in der Blockchain gespeichert (Burgwinkel, 2016, S. 14). Eine häufig verwendete Methode zur Erstellung eines Integritätsnachweises ist die Verwendung eines Hashverfahrens (Burgwinkel, 2016, S. 14), beispielsweise durch einen Merkle Tree (siehe Kapitel 2.3.3). Das Monitoring der Integrität aller Daten kann je nach Art der Blockchain (siehe Kapitel 2.4) und dem verwendeten Konsens-Mechanismus (siehe Kapitel 2.3.3) unterschiedlich ablaufen. Burgwinkel (2016, S. 14) verweist hierbei darauf, dass das Intervall der Überprüfungen von den Sicherheitsbedürfnissen und der Sensitivität der

gespeicherten Daten abhängig ist. Je nach Bedarf können als letztes auch einzelne Datenbestände auf ihre Echtheit überprüft werden (Burgwinkel, 2016, S. 14).

Bei der Umstellung auf ein Blockchain-basiertes Datenmanagementsystem würde der Patient die Kontrolle über die eigenen Daten erhalten (Mandl, Szolovits & Kohane, 2001, S. 284). Dies bedeutet, dass der Patient bestimmen kann, welche Drittparteien (Ärzte, Spitäler, Versicherungen etc.) neue Daten erstellen, zusammentragen, modifizieren, weiterverarbeiten, nutzen, löschen oder kommentieren dürfen (Mandl et al., 2001, S. 284). Mandl et al. (2001, S. 284-285) weisen darauf hin, dass ein Datenmanagementsystem, welches den Patienten die Kontrolle über die Daten erteilt und die Daten in einem dezentralisierten Netzwerk speichert, folgende Eigenschaften aufweisen sollte:

Vollständigkeit: Alle Daten müssen vollständig erfasst werden, da die Patienten nicht immer vom gleichen Anbieter (Arzt, Spitalpersonal, Apotheker etc.) betreut werden und jederzeit ersichtlich sein soll, was andere involvierte Parteien bereits unternommen haben (Mandl et al., 2001, S. 284). Dies umfasst ebenfalls alle vergangenen Ereignisse, sodass die komplette medizinische Geschichte der Patienten erfasst ist und gegebenenfalls retrospektiv analysiert werden kann (Mandl et al., 2001, S. 284).

Zugänglichkeit: Patientendaten sollen sowohl bei Routineuntersuchungen als auch bei Notfällen jederzeit zur Verfügung stehen (Mandl et al., 2001, S. 284). Laut Mandl et al. (2001, S. 284) bedarf es zusätzlich einer Regelung für den Fall, dass ein Patient den Zugriff auf die Daten aus medizinischen Gründen nicht bewilligen kann (zum Beispiel bei Bewusstlosigkeit).

Systemkompatibilität: Es soll unabhängig vom verwendeten System möglich sein, auf die Daten der Patienten zugreifen zu können (Mandl et al., 2001, S. 284).

Vertraulichkeit: Patienten sollen über die Weitergabe der Daten entscheiden können (Mandl et al., 2001, S. 284). Es soll aber auch möglich sein, kategorienspezifische Freigaberechte bestimmen zu können und je nach Empfänger unterschiedlich zu definieren (Mandl et al., 2001, S. 284).

Integrität: Bei Zugriffen auf die Patientendaten und deren Änderungen soll für die Patienten ersichtlich sein, was und von wem etwas geändert wurde (Mandl et al., 2001, S. 285).

Flexibilität: Bei der Erteilung von Rechten an Drittparteien sollen Patienten genügend Flexibilität in der Bestimmung dieser haben (Mandl et al., 2001, S. 285). Dies bedeutet, dass es zum Beispiel möglich sein sollte, zeitliche Fristen zu setzen oder einem Anbieter nur die Erstellung neuer Daten zu bewilligen, jedoch die Einsichtnahme in bestehende Daten zu verweigern (Mandl et al., 2001, S. 285).

5.2.1 Erster Besuch des Patienten bei einem Arzt

In diesem Abschnitt wird ein auf der Blockchain basierender Workflow anhand eines simplen Beispiels erläutert. Wie in Abbildung 22 dargestellt, beruht der Austausch von Informationen und Patientendaten auf der Verwendung eines Public/Private-Key Verfahrens, wie dies in Kapitel 2.3.1 für die Funktionsweise einer Transaktion über die Bitcoin Blockchain bereits beschrieben wurde. Der aufgezeigte Prozess startet mit dem Besuch des Patienten beim Arzt, wobei folglich eine Probe an das Labor zur Untersuchung geschickt wird und der Patient letztlich an einen Spezialisten weitergeleitet wird, welcher den finalen Behandlungsplan aufstellt (Dhillon et al., 2017, S. 127-131).

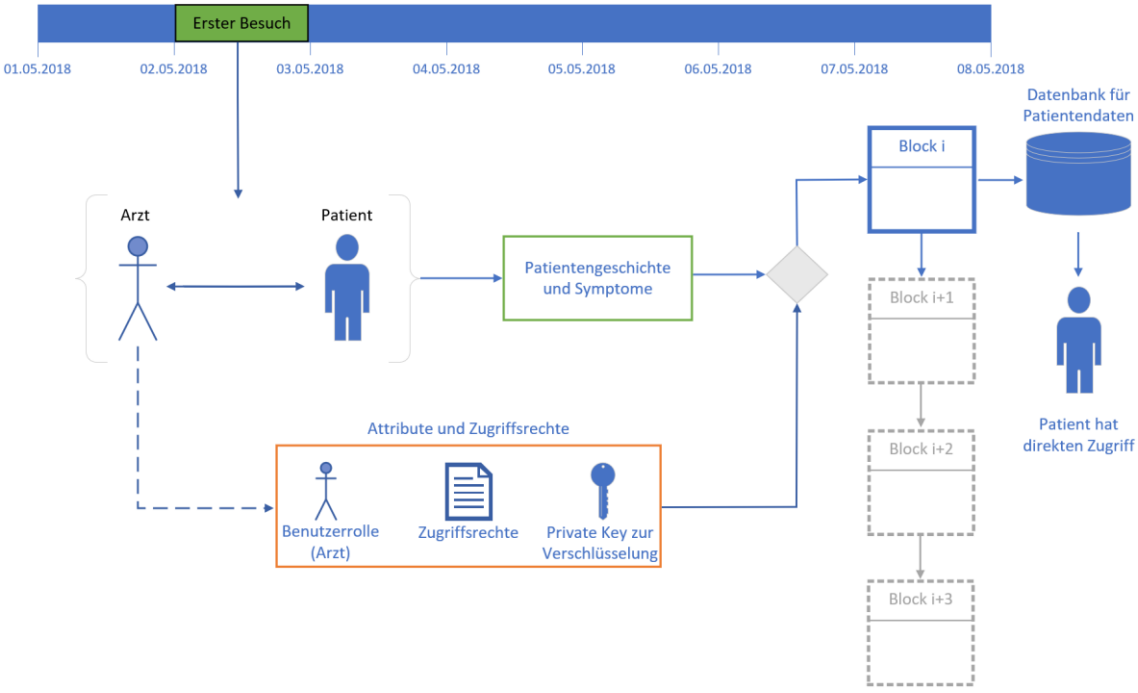


Abbildung 22: Erster Besuch des Patienten (Dhillon et al., 2017, S. 128)

Das Ziel dieses Beispiels ist aufzuzeigen, wie über eine Blockchain die Zugriffsrechte für Patientendaten und das Teilen von Daten mit Drittparteien gehandhabt werden.

Abbildung 22 stellt den Ablauf des ersten Besuchs des Patienten bei seinem Arzt dar. Um den dargestellten Prozess besser verstehen zu können, kann dieser in vier Teilprozesse unterteilt werden. Der erste Teilprozess ist die Untersuchung des Patienten durch den Arzt (Dhillon et al., 2017, S. 129). Es wurden zu diesem Zeitpunkt noch keine Daten in der Blockchain erfasst (Dhillon et al., 2017, S. 129). In einem zweiten Zwischenschritt erfasst der Arzt die gestellte Diagnose, Symptome und die Patientengeschichte (Dhillon et al., 2017, S. 129). Der dritte Teilprozess befasst sich mit den Zugriffsberechtigungen («Attribute und Zugriffsrechte»). Darin sind die Zugriffsrechte und Benutzerrollen (zum Beispiel Patient, Arzt, Spezialist etc.) definiert. In einem letzten Schritt wird die SOAP Note mit den Patientendaten verschlüsselt (Hash) und zusammen mit den Zugriffsrechten und Benutzerrollen der Blockchain hinzugefügt (Dhillon et al., 2017, S. 129). Das Hinzufügen dieser Daten wird durch den Arzt mittels seiner digitalen Unterschrift (Private Key) durchgeführt, wodurch garantiert wird, dass die Daten nicht verändert worden sind (Dhillon et al., 2017, S. 129). Sobald die Daten in der Blockchain eingetragen sind, hat auch der Patient selbst Zugriff auf seine Daten (Dhillon et al., 2017, S. 129).

5.2.2 Labor-Tests

In diesem Beispiel wird davon ausgegangen, dass beim ersten Besuch des Patienten ein zusätzlicher Labortest angeordnet wurde, welcher von einer Pflegekraft (als Beispiel einer zusätzlich involvierten Partei bei gleichbleibendem Anbieter) durchgeführt werden soll (Abbildung 23).

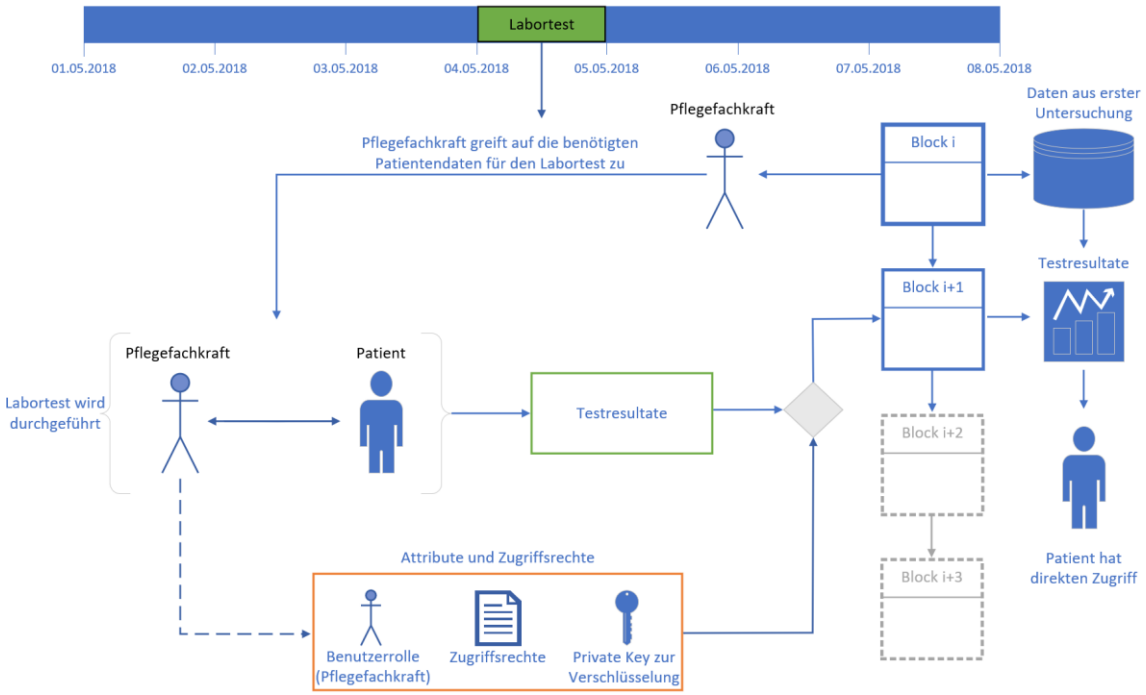


Abbildung 23: Labortest durch Pflegekraft (Dhillon et al., 2017, S. 129)

Beim ersten Besuch des Patienten wurde die Anordnung des Labortests zusammen mit den neu erfassten Patientendaten in der Blockchain gespeichert und gleichzeitig dem Pflegepersonal die entsprechenden Rechte erteilt, um auf die Daten zugreifen und neue Daten (Testresultate) hinzufügen zu können (Dhillon et al., 2017, S. 130). In einem ersten Schritt greift die Pflegefachkraft auf die Patientendaten zu, bespricht den Ablauf des Tests mit dem Patienten und führt den Test durch (Dhillon et al., 2017, S. 130). Ähnlich wie im vorherigen Beispiel bei der erstmaligen Erfassung der Patientendaten, werden nun die Testresultate einem neuen Block auf der Blockchain hinzugefügt (Dhillon et al., 2017, S. 130).

5.2.3 Miteinbezug eines Spezialisten

In diesem abschliessenden Beispiel wird der Einbezug eines Spezialisten (als Beispiel einer zusätzlich involvierten Drittpartei) simuliert (Abbildung 24). Dies soll den Prozess aufzeigen, der eintritt, wenn der Patient seine Daten mit einer zusätzlichen Partei teilen will.

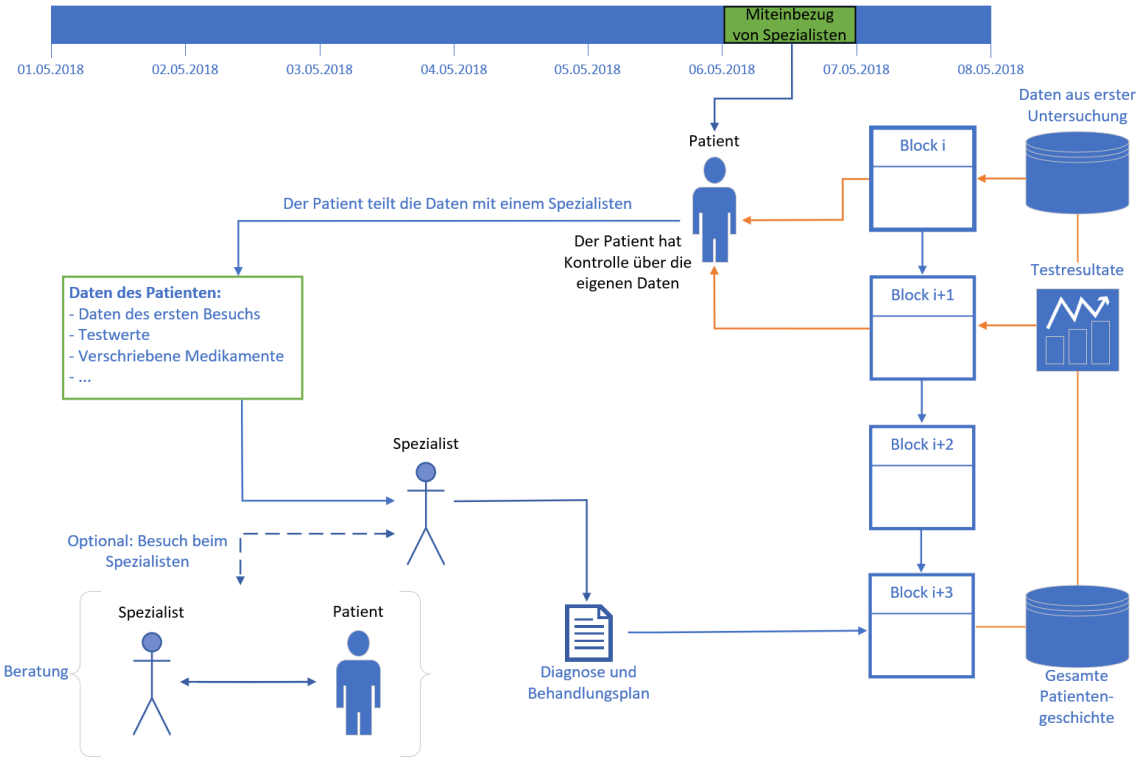


Abbildung 24: Miteinbezug eines Spezialisten (Dhillon et al., 2017, S. 130)

Als erstes erteilt der Patient dem Spezialisten die Rechte, um auf die Patientendaten zugreifen zu dürfen (Dhillon et al., 2017, S. 130). Laut Dhillon et al. (2017, S. 130) hat der Spezialist nun zwei Möglichkeiten, entweder liefert der Spezialist eine Ferndiagnose, welche ausschliesslich auf den erhaltenen Daten beruht, oder es findet ein Besuch des Patienten beim Spezialisten statt. Die erste Option könnte eine Möglichkeit sein, um die Kosten des gesamten Prozesses zu senken (Dhillon et al., 2017, S. 130). In beiden Fällen werden die Daten (Diagnose und Behandlungsplan) einem neuen Block der Blockchain hinzugefügt (Dhillon et al., 2017, S. 130).

5.3 Abwicklung von Versicherungsansprüchen über die Blockchain

Dhillon et al. (2017, S. 125) beschreiben mittels des Payer-Provider-Patient-Modells (Abbildung 25) die Beziehung zwischen den beteiligten Parteien (Versicherungsgesellschaft, Anbieter und Patient) beim Prozess zur Abwicklung von Versicherungsansprüchen.

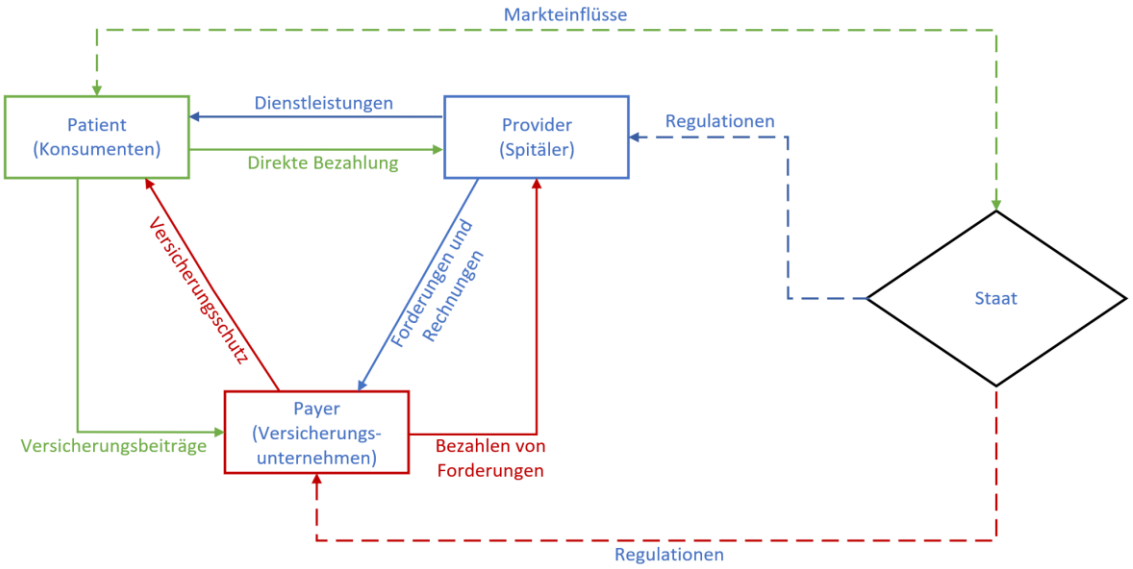


Abbildung 25: Payer-Provider-Patient-Modell (Dhillon et al., 2017, S. 126)

In diesem Modell bezahlt der Patient der Versicherungsgesellschaft eine Prämie, um im Gegenzug eine Versicherung zu erhalten (Dhillon et al., 2017, S. 126). Diese Versicherung tritt in Kraft, wenn der Patient Dienstleistungen von einem Anbieter in Anspruch nimmt und die Versicherung die Kosten für die Behandlung übernimmt (Dhillon et al., 2017, S. 126). In zahlreichen Ländern hat ein Patient aber auch die Möglichkeit, direkt für eine Behandlung zu bezahlen (Dhillon et al., 2017, S. 126). Der Anbieter unterhält ein Register mit allen Ausgaben bezüglich eines Patienten (beispielsweise die Kosten für einen Spitalaufenthalt, eine Behandlung oder Medikamente) und sendet diese Daten an die Versicherungsgesellschaft, welche die Ausgaben entweder annimmt oder zurückweist (Schumacher, 2017, S. 11). Dabei führt die Versicherungsgesellschaft in vielen Fällen eine manuelle Überprüfung der Kostenteilung durch, welche die patientenspezifischen Bedingungen, die Validierung der beanspruchten Behandlungen und eventuell geltende regulatorische Vorschriften berücksichtigt (Schumacher, 2017, S. 11).

Dieser Prozess kann gemäss Schumacher (2017, S. 11) in einen Smart Contract eingebunden werden. Wie bereits in Kapitel 3.1 erläutert, sind Smart Contracts autonome, selbstregulierende und dezentralisierte Verträge (Swan, 2015, S. 16). Diese Verträge können in Echtzeit durchgeführt werden, reduzieren die Wahrscheinlichkeit eines menschlichen Fehlers oder Betrugs und erhöhen den Datenschutz und die Glaubwürdigkeit (Morabito, 2017, S. 112). Einfach formuliert können Smart Contracts als Computercode angesehen werden, welcher Teil der Blockchain ist und prinzipiell aus

«if this then do that»-Statements besteht (Morabito, 2017, S. 103). Somit können Verträge zwischen unterschiedlichen Anspruchsgruppen im Gesundheitswesen als Smart Contract formuliert werden (Schumacher, 2017, S. 11). Damit lassen sich Zahlungen automatisch abwickeln, der Datenschutz erhöhen und die zur Abwicklung von Versicherungsansprüchen benötigte Zeit und die Kosten des Prozesses reduzieren (Schumacher, 2017, S. 11-12).

5.4 Nachverfolgbarkeit von Medikamenten entlang der Supply Chain

Gefälschte Medikamente stellen besonders in Entwicklungsländern ein enormes Problem dar, wobei Schätzungen davon ausgehen, dass es sich insgesamt bei 15 Prozent aller verkauften Medikamente um Fälschungen handelt, in Teilen von Afrika und Asien steigt dieser Anteil sogar bis auf 50 Prozent an (Cockburn, Newton, Agyarko, Akunyili & White, 2005, S. 302). Dies hat zu einem wachsenden Misstrauen gegenüber der Pharmaindustrie geführt und hat Behörden, wie zum Beispiel die Food and Drug Administration (FDA) in den USA, dazu veranlasst, eine Verordnung zu erlassen, die Pharmaunternehmen dazu zwingt, ihre Produkte entlang der Supply Chain nachverfolgbar zu machen (Archa, Alangot & Achuthan, 2017, S. 189). So fordert der «Drug Quality and Security Act» in den USA, dass verschreibungspflichtige Medikamente, die innerhalb der USA vertrieben werden, durch ein System nachverfolgbar gemacht werden müssen (Archa et al., 2017, S. 189). Bei der Umsetzung eines solchen Systems wird häufig von einer sogenannten «chain of custody» gesprochen, in der alle Änderungen, Phasen oder Besitzer eines Gutes entlang der Supply Chain vermerkt sind (Mainelli & Smith, 2015, S. 12). Dieses Prinzip wird zum Beispiel auch zur Nachverfolgung von Diamanten genutzt, um den Vertrieb von Blutdiamanten zu verhindern (Mainelli & Smith, 2015, S. 12).

BlockVerify ist ein Unternehmen, welches sich auf eine Blockchain-basierte Lösung zur Bekämpfung von Fälschungen konzentriert, indem sie es Unternehmen erlauben, ihre Produkte entlang der Supply Chain zu verfolgen (Bheemaiah, 2017, S. 68). Dies ermöglicht es, den Ursprungsort von gekauften Produkten zu bestimmen, deren Authentizität zu verifizieren und ein Produkt von der Produktion bis zum Verkaufsregal nachzuverfolgen (Morabito, 2017, S. 139). Blockchains können die Sicherheit von Transaktionen erhöhen und die dadurch effizient gestaltete Buchführung kann die Wahrscheinlichkeit von Betrugsfällen reduzieren (Asharaf & Adarsh, 2017, S. 77).

Nicht nur im Gesundheitswesen, sondern auch in anderen Industrien hat die Blockchain-Technologie das Potential, das Supply Chain Management zu revolutionieren (Bheemaiah, 2017, S. 98-99). Der Grund dafür ist, dass das Supply Chain Management, welches sich mit dem Warenfluss vom Produzenten bis hin zum Konsumenten befasst, zahlreiche Prozesse zur Überwachung der Produktion, des Lagermanagements und der Qualitätskontrolle beinhaltet (Bheemaiah, 2017, S. 98). Dadurch wird auch eine grosse Anzahl von Intermediären involviert und die Interaktionen mit diesen Intermediären müssen dokumentiert werden, um die Integrität des gesamten Prozesses zu gewährleisten (Bheemaiah, 2017, S. 98). Dies hat hohe Gebühren, komplexe Prozesse und grosse Zeitverzüge als Folge, da die Dokumentation häufig papierbasiert abläuft (Bheemaiah, 2017, S. 98). Die Blockchain-Technologie zielt darauf ab, diese Intermediäre von den Prozessen auszuschliessen, da die Blockchain deren Aufgabe übernehmen kann und für eine direkte Verbindung zwischen den unterschiedlichen Anspruchsgruppen sorgt (Asharaf & Adarsh, 2017, S. 77).

Im Kontext der Gesundheitsbranche soll die Blockchain-Technologie genutzt werden, um die verschiedenen Entitäten zu verknüpfen (Archa et al., 2017, S. 190). Dabei soll es einzelnen Entitäten nicht möglich sein, die auf der Blockchain aufgezeichneten Transaktionen zu ändern, ohne dass die anderen involvierten Parteien von der Änderung in Kenntnis gesetzt werden (Archa et al., 2017, S. 190). Archa et al. (2017, S. 195) beschreiben den Einfluss der Blockchain-Technologie auf das Supply Chain Management bezüglich Medikamenten wie folgt: «The blockchain by design imparts transparency, authentication, auditability to trace the origins of a product. Using the blockchain distributed design reduces the data tampering risks further providing a unique identity to the blockchain makes it a cheap but error free operation.».

5.5 E-Health in Government

In Estland wird die Blockchain-Technologie bereits als Lösung für den sicheren Zugriff auf elektronisch erfasste Gesundheitsdaten und zur Sicherstellung deren Datenintegrität verwendet (Ojo & Abebayo, 2017, S. 287-288). Das auf der Blockchain basierte Framework kommt auch bei der Validierung der Patientenidentität zur Anwendung (Angraal et al., 2017, S. 2). Die Einwohner verfügen über eine persönliche Smart Card, auf der ihre elektronisch erfassten Gesundheitsdaten mit ihrer Blockchain-basierten Identität verlinkt sind (Angraal et al., 2017, S. 2). Das nationalweite System

integriert die Daten von vielen verschiedenen Dienstleistungsanbietern aus dem Gesundheitswesen in ein einziges Portal (Bheemaiah, 2017, S. 81). Dadurch haben die Bürger vollen Einblick in ihre gespeicherten Gesundheitsdaten und können einsehen, wie diese Informationen genutzt werden (Bheemaiah, 2017, S. 81). Zusätzlich wurde in Estland ebenfalls ein System zur Verwaltung von digitalen Identitäten erstellt, womit sich der Datenaustausch zwischen unterschiedlichen System immens vereinfachen lässt und Funktionalität und Effektivität gesteigert werden (Bheemaiah, 2017, S. 81).

5.6 Daten für die medizinische Forschung

Gemäss Benchoufi und Ravaud (2017, S. 335) stellen Probleme mit der Vorgehensweise in der medizinischen Forschung eine der grössten Herausforderung in diesem Bereich dar. Diese Probleme beziehen sich vor allem auf die mangelhafte Reproduzierbarkeit von Studien und Experimenten, stammen aus einer Reihe von unterschiedlichen wissenschaftlichen Fehlverhalten und reichen von simplen Fehlern bis hin zu Betrug (Benchoufi & Ravaud, 2017, S. 335). Dies beeinträchtigt die Aussagekraft von klinischen Studien und hat einen negativen Einfluss auf die Qualität der Forschung (Benchoufi & Ravaud, 2017, S. 335).

Die Blockchain-Technologie kann die Qualität der Forschung verbessern, indem einerseits die Reproduzierbarkeit erhöht wird und die Forscher eine Möglichkeit erhalten, Daten auf eine sichere Art und Weise zu teilen, und andererseits die Privatsphäre der Patienten garantiert werden kann (Benchoufi & Ravaud, 2017, S. 335). Unterschiedliche Eigenschaften der Blockchain-Technologie ermöglichen das Erreichen dieser Ziele einerseits durch die Anonymisierung der Daten mittels kryptographischer Verfahren, wobei dies auch mit anderen Anwendungen möglich wäre, die nicht auf einer Blockchain basieren (Engelhardt, 2017, S. 28-29). Die Blockchain-spezifischen Vorteile beziehen sich vor allem auf die Unveränderbarkeit der Daten, die Transparenz und die Ermächtigung der Patienten über die eigenen Daten (Engelhardt, 2017, S. 28-29). Die Unveränderbarkeit bedeutet für die Forschung, dass die Daten, sobald sie gespeichert und auf der Blockchain referenziert sind, nicht verändert werden können, ohne dass die Änderung für jeden ersichtlich wäre (Engelhardt, 2017, S. 28). Somit wird das Manipulieren von Daten verunmöglicht (Engelhardt, 2017, S. 28). Die Transparenz trägt vor allem zum Problem der mangelhaften Reproduzierbarkeit von Studien bei, da klar ersichtlich ist, welche Daten für die Studie berücksichtigt wurden

und welche nicht (Engelhardt, 2017, S. 28). Damit können die Ergebnisse leichter überprüft werden (Engelhardt, 2017, S. 28). Der dritte Vorteil, die Ermächtigung der Patienten über die eigenen Daten, nutzt die Eigenschaften von Smart Contracts, welche es den Patienten ermöglichten, Rechte zur Nutzung ihrer Daten für die medizinische Forschung zu erteilen oder zurückzuziehen (Engelhardt, 2017, S. 28-29).

Ein Anwendungsbeispiel der Blockchain-Technologie bezüglich der Verbesserung von Qualität und Quantität von Daten für die medizinische Forschung wird in Kapitel 6 anhand eines detaillierten Proof of Concept genauer erläutert. Ein anderes Beispiel ist die Plattform Healthbank (Morabito, 2017, S. 30).

Healthbank hat ihren Sitz in der Schweiz und ist eine Plattform zum Teilen von Gesundheitsdaten (Riso et al., 2017, S. 13). Die Applikation ist international zugänglich und ermöglicht es den Nutzern, von den von ihnen zur Verfügung gestellten medizinischen Daten zu profitieren, wenn sie diese der medizinischen Forschung zugänglich machen (Riso et al., 2017, S. 13-14). Kurz formuliert funktioniert das Geschäftsmodell von Healthbank wie folgt: User bezahlen für die Registrierung und Speicherung von persönlichen Informationen eine Gebühr, im Gegenzug werden die Daten an Forschungsinstitute zur Analyse weiterverkauft und die erwirtschafteten Erlöse werden unter den Teilnehmern aufgeteilt (Riso et al., 2017, S. 13). Wie hoch der Anteil am Erlös der einzelnen User ausfällt, ist abhängig von der Qualität und Quantität der zur Verfügung gestellten Daten (Riso et al., 2017, S. 13). Gleichzeitig haben die User aber die Autorität über die eigenen Daten und können definieren, mit welchen Institutionen und zu welchem Zweck ihre Daten geteilt werden dürfen (Riso et al., 2017, S. 14).

Tabelle 3 beinhaltet eine Übersicht aller behandelten Anwendungsgebiete.

Tabelle 3: Anwendungsbereiche der Blockchain-Technologie im Gesundheitswesen

Anwendungsbereich	Beschreibung	Value Proposition	Proof of Concepts	Quelle
Elektronische Erfassung von Patientendaten	Eine der grössten Herausforderungen im Gesundheitswesen ist die einheitliche elektronische Erfassung von Patientendaten. Obwohl traditionelle Lösungsansätze (ohne Blockchain) für diesen Bereich existieren, bleiben in vielen Fällen akute Probleme bestehen. Mittels der Blockchain-Technologie kann ein einheitliches System geschaffen werden, was die Interaktion zwischen unterschiedlichen Systemen ermöglicht, die Datenintegrität sicherstellt, den Zugriff auf Daten effizienter gestaltet und den Patienten mehr Kontrolle über die eigenen Daten verspricht. Verschiedene Lösungsansätze berücksichtigen ebenfalls die erhöhte Generation von qualitativ hochwertigen Datenquellen für die medizinische Forschung als erstrebenswertes Ziel.	1) Einheitlicher und schneller Zugriff auf medizinische Daten 2) Kompatibilität zwischen verschiedenen Systemen 3) Kontrolle der Patienten über die eigenen Daten 4) Erhöhte Qualität und Quantität von Daten für die medizinische Forschung	MedRec Medicalchain Healthcoin Factom GemOS BurstIQ	Angraal et al., 2017, S. 1-3 Azaria et al., 2016, S. 25-30 Dhillon et al., 2017, S. 126 Engelhardt, 2017, S. 25-27
Abwicklung von Versicherungsansprüchen	Einbindung des Prozesses zur Abwicklung von Kostenbeteiligungen der Versicherungsgesellschaften in einen Smart Contract. Interaktion zwischen Patient, Anbieter und Versicherung soll schneller abgewickelt und somit Kosten eingespart werden.	1) Automatisierung der Zahlungsabwicklung 2) Verbesserter Datenschutz beim Umgang mit sensitiven Daten 3) Reduzierung der administrativen Kosten 4) Zeiteinsparungen bei der Prozessabwicklung	GemHealth Pokitdok Simply Vital-Health	Dhillon et al., 2017, S. 126 Engelhardt, 2017, S. 29-30 Mainelli & Smith, 2015, S. 12 Schumacher, 2017, S. 11
Nachverfolgbarkeit von Medikamenten entlang der Supply Chain	Nutzen der Blockchain-Technologie um den Vertrieb von gefälschten Medikamenten zu verhindern. Umgesetzt wird dies durch die Erstellung eines Registers aller Medikamente, welches jeden Schritt durch die Supply Chain dokumentiert, um den Ursprung eines Medikaments eindeutig verifizieren zu können.	1) Vertrieb von gefälschten Medikamenten verhindern 2) Manipulation des Verfallsdatums verunmöglichen 3) Echtheit von Medikamenten kann verifiziert werden 4) Rückverfolgung des Medikaments entlang der Supply Chain 5) Transparenz der Supply Chain wird erhöht und die Revision erleichtert	Block Verify Pokitdok iSolve	Archa et al., 2017, S. 189-195 Asharaf & Adarsh, 2017, S. 77 Bheemaiah, 2017, S. 68 Engelhardt, 2017, S. 29-30 Mainelli & Smith, 2015, S. 12 Morabito, 2017, S. 139
eHealth in Government	In Estland wird die Blockchain-Technologie bereits als Lösung für den sicheren Zugriff auf elektronisch erfasste Gesundheitsdaten und zur Sicherstellung deren Datenintegrität verwendet. Das auf der Blockchain basierte Framework kommt ebenfalls bei der Validierung der Patientenidentität zum Zuge. Die Einwohner verfügen über eine persönliche Smart Card, auf der ihre elektronisch erfassten Gesundheitsdaten mit ihrer Blockchain-basierter Identität verlinkt sind.	1) Verwaltung von elektronischen Gesundheitsdaten auf nationaler Ebene 2) Identitätsmanagement über die Blockchain 3) Verbesserung der Interoperabilität zwischen unterschiedlichen Systemen 4) Bürger haben Einsicht die eigenen Daten über ein zentrales Portal	Guardtime Hashed Health Nuco	Angraal et al., 2017 Bheemaiah, 2017, S. 80-81 Engelhardt, 2017, S. 29 Morabito, 2017, S. 30 Ojo & Abebayo, 2017, S. 287-288 Schumacher, 2017, S. 39-40
Medizinische Forschung	Die mangelhafte Reproduzierbarkeit von klinischen Studien stellt eines der grössten Probleme in der medizinischen Forschung dar. Die Blockchain-Technologie liefert eine mögliche Lösung für dieses Problem. Erreicht wird dies durch die Anonymisierung der Daten mittels kryptographischen Verfahren, die Unveränderbarkeit der Daten, die Transparenz und durch die Ermächtigung der Patienten über die eigenen Daten.	1) Erhöhte Qualität und Quantität von Daten für die medizinische Forschung 2) bessere Reproduzierbarkeit von klinischen Studien durch erhöhte Transparenz 3) Gewährleistete Integrität von klinischen Studien, da die verwendeten Daten nicht manipuliert wer-den können 4) Erhöhte Kontrolle über die für Studien zur Verfügung gestellten Daten von Privatpersonen 5) Anonyme Teilnahme an klinischen Studien (nicht zwingend Blockchain-spezifisch)	MedRec Healthbank Data Lake	Azaria et al., 2016, S. 2 Benchoufi & Ravaud, 2017, S. 335-339 Engelhardt, 2017, S. 28-29 Morabito, 2017, S. 30 Riso et al., 2017, S. 13-14 Schumacher, 2017, S. 13-17

6 Use Case: MedRec

In diesem Kapitel wird der Use Case von MedRec, einem System zur Verwaltung von elektronischen Patientendaten, genauer analysiert.

6.1 Einleitung

MedRec und die zugrundeliegende Idee zur Verwaltung von elektronischen Patientendaten wurde 2016 an der zweiten International Conference on Open and Big Data von Azaria et al. (2016, S. 25) vom Massachusetts Institute of Technology vorgestellt. Es ist eine Antwort auf die nur langsam voranschreitende Innovation im Gesundheitsbereich und soll gleichzeitig den Patienten die Möglichkeit geben, ihre Daten selber zu verwalten (Azaria et al., 2016, S. 25). MedRec ist ein neuartiges, dezentralisiertes Dokumentenmanagement-System für Patientendaten im Gesundheitswesen, welches auf der Blockchain-Technologie basiert (Azaria et al., 2016, S. 25). Ähnlich wie bei dem in Kapitel 5.2.1 beschriebenen Workflow, erstellen Azaria et al. (2016, S. 25) mit MedRec ein umfassendes und unveränderliches Register, welches den Patienten den Zugriff auf die eigenen medizinischen Informationen, unabhängig davon, von welcher Quelle diese Daten stammen, stark vereinfachen soll. Gemäss Azaria et al. (2016, S. 26) gibt es im Gesundheitsbereich vier Problemfelder, welche durch die Implementation des Blockchain-basierten Dokumentenmanagement-Systems gelöst werden können:

1) Uneinheitlicher und langsamer Zugriff auf medizinische Daten
2) (In-)Kompatibilität zwischen verschiedenen Systemen
3) Kontrolle der Patienten über die eigenen Daten
4) Qualität und Quantität von Daten für die medizinische Forschung

6.2 Funktionsweise

An dieser Stelle ist es essentiell zu verstehen, dass die eigentlichen Patientendaten nicht auf der Blockchain gespeichert werden (Azaria et al., 2016, S. 26). Stattdessen besteht ein Block der Blockchain aus drei unterschiedlichen Arten von Informationsquellen (Azaria et al., 2016, S. 27). Dabei handelt es sich um die von Azaria et al. (2016, S. 26-27) als *Registrar Contract*, *Summary Contract*, und *Patient Provider Relationship* bezeichneten Bestandteile (Abbildung 26).

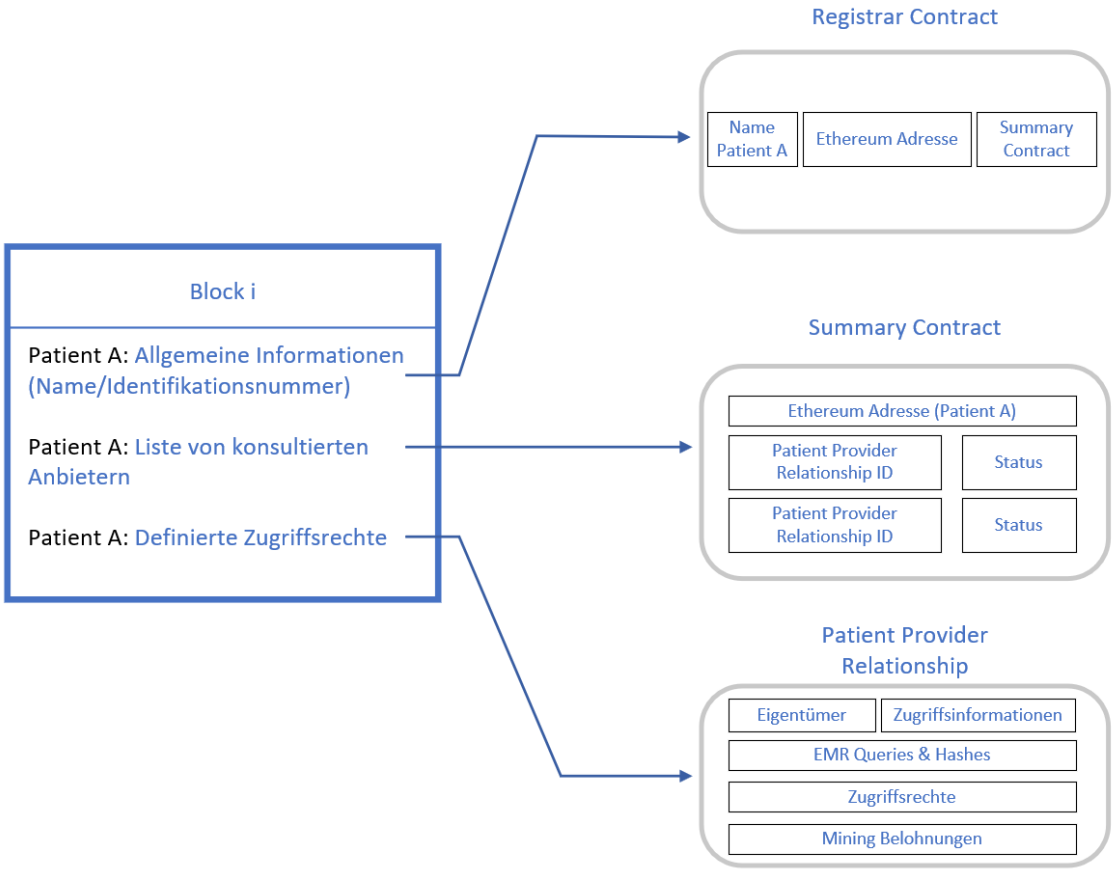


Abbildung 26: Bestandteile eines Blockes (MedRec) (Azaria et al., 2016, S. 27)

Bei diesen drei Bestandteilen handelt es sich um Smart Contracts, welche unter bestimmten Bedingungen ausgeführt werden, zum Beispiel um einen neuen Datensatz zu erfassen oder die Einsichtsrechte eines Anbieters zu ändern (Azaria et al., 2016, S. 26). Mittels diesen Smart Contracts können Anbieter neue Patientenakten erstellen (Registrar Contract) und Patienten können ihre Daten verwalten, indem sie ihre Beziehung zu einem bestimmten Anbieter spezifizieren (Patient Provider Relationship) und dessen Zugriffsrechte definieren (Azaria et al., 2016, S. 26). Der Summary Contract agiert als zentrale Einheit, welche alle Interaktionen zwischen einem Patienten und den mit dem Patienten in Verbindung stehenden Anbietern zusammenfasst (Azaria et al., 2016, S. 26). Dadurch entspricht der Summary Contract einem zentralen Referenzpunkt, durch den auf die gesamte medizinische Geschichte eines Patienten zugegriffen und diese auf Updates überprüft werden kann (Azaria et al., 2016, S. 26).

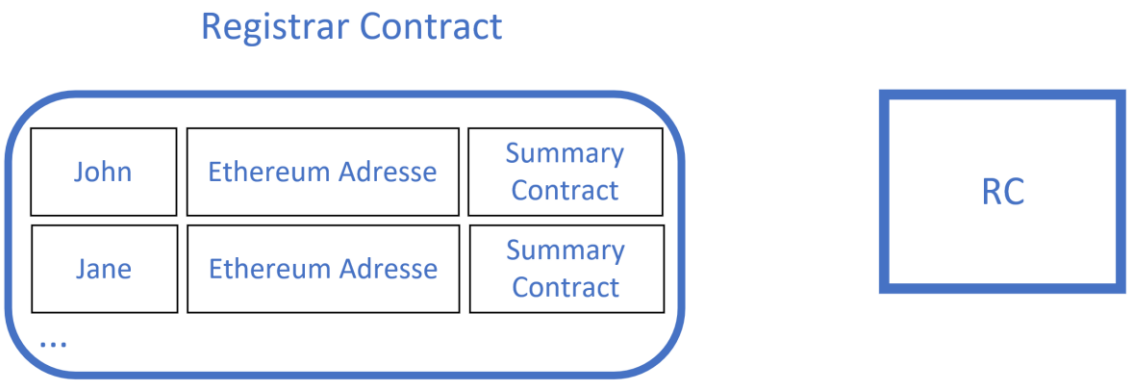


Abbildung 27: Registrar Contract (Azaria et al., 2016, S. 27)

Laut Azaria et al. (2016, S. 27) verknüpfen Registrar Contracts (RC) einen Patienten mit einer auf den Patienten lautenden, einzigartigen Ethereum-Adresse und den entsprechenden Summary Contracts (Abbildung 27). Das Verknüpfen von Daten wird als Mapping bezeichnet, ein Begriff der Informatik, der eine Technik für die Herstellung einer Beziehung zwischen unterschiedlichen Datenpunkten beschreibt. In diesem Beispiel wird durch das Mapping definiert, dass der Beispielpatient John mit einer spezifischen Ethereum-Adresse in Verbindung steht. Dies vereinfacht beispielsweise Datenbankabfragen oder das Erfassen von neuen Daten, da für die Identifikation des Patienten John seine Ethereum-Adresse verwendet werden kann und nicht sein realer Name, was gleichzeitig zu mehreren Treffern für alle Patienten mit dem Namen John führen könnte. Eine Ethereum-Adresse ist das Äquivalent zu einer Bitcoin-Adresse (Kapitel 2.3.1), für das Verständnis ist allerdings nur wichtig zu verstehen, dass es sich dabei um eine einzigartige Folge von Zeichen handelt. Zusätzlich können Registrar Contracts mit Bedingungen ergänzt werden, welche beispielsweise regulieren, dass nur bestimmte zertifizierte Institutionen neue Patienten registrieren können (Azaria et al., 2016, S. 27).

Azaria et al. (2016, S. 27) bezeichnen die Funktion des Summary Contracts (SC) als «bread crumb trail» für die Teilnehmer des Systems, um die Daten der Patientengeschichte zu lokalisieren (Abbildung 28). Der Summary Contract beinhaltet eine Liste von Referenzen auf alle Patient-Provider Realtionship Contracts (PPR), was einer Übersicht über alle vergangenen und aktuellen Interaktionen zwischen Systemteilnehmern bezüglich des Patienten entspricht (Azaria et al., 2016, S. 27).

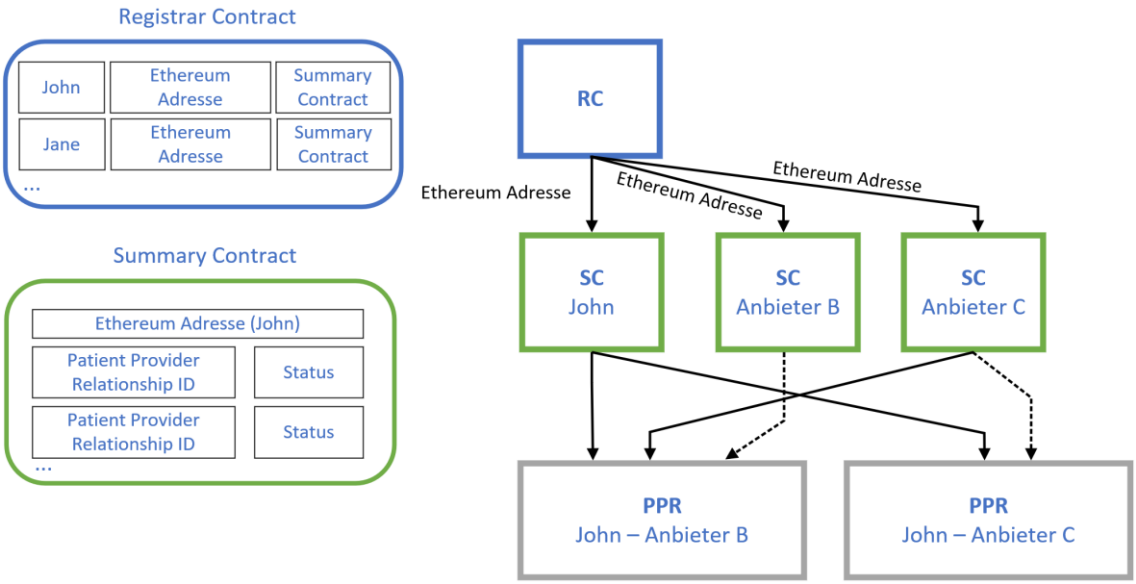


Abbildung 28: Summary Contract (Azaria et al., 2016, S. 27)

Neben den Patienten haben Anbieter ebenfalls einen eigenen Summary Contract, der eine Übersicht über ihre Patienten und alle Drittparteien liefert, für welche die Anbieter die Berechtigung der Patienten zum Datenaustausch erhalten haben Azaria et al., 2016, S. 27).

Der Patient-Provider Relationship Contract (Abbildung 29) ist ein Smart Contract zwischen zwei Systemteilnehmern, welcher zustande kommt, wenn eine Partei für eine zweite Partei Patientendaten verwaltet (Azaria et al., 2016, S. 27). Ein PPR Contract widerspiegelt die Beziehung zwischen zwei Teilnehmern in diesem System (Azaria et al., 2016, S. 27). In dem Beispiel, welches in Abbildung 29 dargestellt wird, werden zwei solcher Beziehungen gezeigt: Eine Patient-Provider-Relationship zwischen dem Patienten John und dem Anbieter B und eine zweite zwischen John und dem Anbieter C. Zwischen John und dem Anbieter B besteht ein PPR Contract, da der Anbieter B medizinische Daten über John in deren Datenbank gespeichert hat (Azaria et al., 2016, S. 27). Mittels des PPR Contracts «John – Anbieter B» kann John genau definieren, auf welche Daten zusätzliche Drittparteien Zugriff haben (Azaria et al., 2016, S. 27). In Abbildung 29 ist ersichtlich, dass die Beziehung «John – Anbieter B» vom Anbieter B verwaltet wird (Daten sind bei B in einer Datenbank gespeichert) und gleichzeitig dem Anbieter C Einsichtsrechte in diese Daten gewährt wurden. John kann die Einsichtsrechte von C einschränken, indem er nur vordefinierte Datenbankabfragen zulässt (Azaria et al., 2016, S. 27).

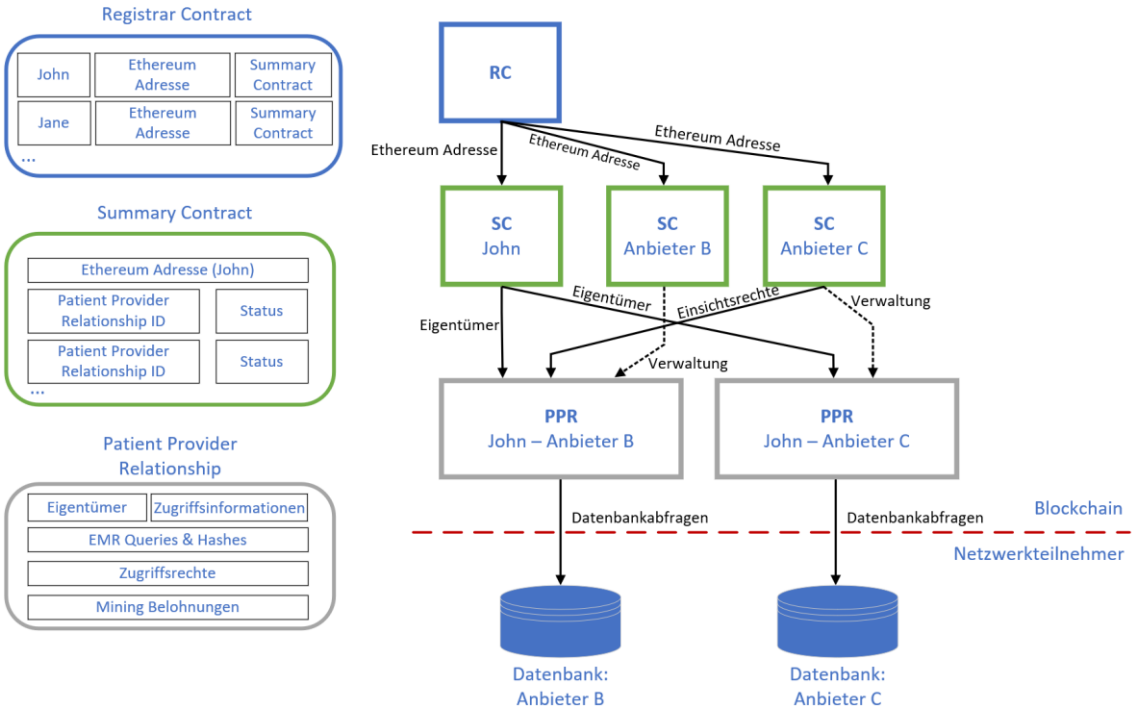


Abbildung 29: Patient-Provider Relationship (Azaria et al., 2016, S. 27)

Abbildung 29 vervollständigt das von Azaria et al. (2016, S. 25-30) vorgestellte Modell zur Anwendung der Blockchain-Technologie für die Verwaltung von Patientendaten.

Da es sich bei Patientendaten um sensible Daten handelt, wird der Zugriff auf die Blockchain eingeschränkt und nur autorisierte Parteien dürfen am Konsensmechanismus teilnehmen (Azaria et al., 2016, S. 25). Somit handelt es sich bei der vorgeschlagenen Blockchain gemäss der in Kapitel 2.4 vorgestellten Definitionen um eine Private-Permissioned-Blockchain (Olnes et al., 2017, S. 360). Wie auch bei der Bitcoin Blockchain, basiert das beschriebene Dokumentenmanagement-System für Patientendaten auf dem Proof-of-Work Konsensmechanismus (Azaria et al., 2016, S. 25). Da es sich jedoch um eine Private-Permissioned-Blockchain handelt, können nur autorisierte Stakeholder aus dem Gesundheitsweisen am Mining-Prozess teilnehmen (Azaria et al., 2016, S. 29). Trotzdem sollen sich aber möglichst viele Stakeholder am Mining-Prozess beteiligen, da das Netzwerk umso sicherer ist, desto mehr Miner am Konsensprozess teilhaben (Olnes et al., 2017, S. 356). Daher sollen durch das System zwei unterschiedliche Anreize geschaffen werden (Azaria et al., 2016, S. 29). Der erste Anreiz besteht darin, dass die Miner mittels Kryptowährungen entlohnt werden und dies im Gegenzug für die Finanzierung der Unterhaltskosten des Systems nutzen können (Azaria et al., 2016, S. 29). Die Unterhaltskosten bestehen aus administrativen

Aufgaben rund um die Verwaltung des Systems, beispielsweise dem Aktualisieren der Patient-Provider-Relationship oder der manuellen Annahme von Zugriffsrechten für Drittparteien (Azaria et al., 2016, S. 29). Der zweite Aspekt des Anreizmodells involviert medizinische Forschungsinstitute und die Gesundheitsbehörde (Azaria et al., 2016, S. 29). Diese beiden Stakeholder können am Mining-Prozess teilnehmen und erhalten als Belohnung anonymisierte Patientendaten (Azaria et al., 2016, S. 29). Dabei fügt beispielsweise ein Arzt die aggregierten Eisenwerte aller durchgeführten Bluttests der letzten Woche als Belohnung für den Miner einer neuen Transaktion an (Azaria et al., 2016, S. 29). Somit haben medizinische Forschungsinstitute und die Gesundheitsbehörden die Möglichkeit, medizinische Daten in hoher Quantität und Qualität zu sammeln und müssen als Gegenleistung eigene Ressourcen in Form von Rechenkapazität bereitstellen (Azaria et al., 2016, S. 29).

6.3 Disruptive Wirkung

Die aufgezeigte Anwendungsmöglichkeit der Blockchain-Technologie im Gesundheitswesen verspricht eine revolutionäre Änderung im Umgang mit Patientendaten. Der von Azaria et al. (2016, S. 25-30) entwickelte Prototyp nimmt auch Bezug auf die von Mandl et al. (2001, S. 284-285) definierten Standards zur Handhabung von elektronisch erfassten Patientendaten, insbesondere der im Kapitel 5.2 beschriebener Vollständigkeit, Zugänglichkeit, Systemkompatibilität, Vertraulichkeit, Integrität und Flexibilität. Das Ziel von Azaria et al. (2016, S. 26) war das Entwickeln eines auf der Blockchain-Technologie basierenden, neuartigen und dezentralisierten Dokumentenmanagement-Systems für Patientendaten, um vier Problemfelder der Patientendaten im Gesundheitswesen zu lösen. Diese Probleme umfassen den uneinheitlichen und langsamen Zugriff auf medizinische Daten, die Inkompatibilität zwischen aktuell genutzten Systemen, die mangelnde Kontrolle der Patienten über die eigenen Daten und die Erhöhung der Quantität und Qualität der Daten für die medizinische Forschung (Azaria et al., 2016, S. 26).

Die in diesem Use Case beschriebene Anwendung der Blockchain-Technologie gibt den Patienten die Kontrolle über ihre eigenen Daten. Es wird ein umfassendes, einfach zugängliches und verlässliches Register gebildet, welches die gesamte medizinische Patientengeschichte abbildet und der Patient wird über jede Änderung informiert (Azaria et al., 2016, S. 29). Durch das Management der User-Rechte kann der Patient

selbst darüber entscheiden, wie mit seinen Daten umgegangen werden soll (Azaria et al., 2016, S. 29). Dies beinhaltet insbesondere den Austausch seiner Daten zwischen verschiedenen Anbietern von Dienstleistungen im Gesundheitswesen und die Definition unterschiedlicher Zugriffsrechten für spezifische Daten (Azaria et al., 2016, S. 29). So kann der Patient detaillierte Restriktionen festlegen, wodurch beispielsweise nur bestimmte Testresultate mit einem anderen Anbieter geteilt und deren Zugriff auf diese Daten, falls gewünscht, ebenfalls zeitlich begrenzt werden kann (Azaria et al., 2016, S. 29). Die erhöhte Kontrolle über die Patientendaten bietet auch Anbietern und der Gesundheitsbehörde Vorteile, da eine aufgezeichnete Geschichte aller medizinischen Interaktionen zwischen Patienten und Anbietern geschaffen wird (Azaria et al., 2016, S. 29). Dies ermöglicht eine einfachere Überprüfung der Geschehnisse im Falle von Rechtsstreitigkeiten (Azaria et al., 2016, S. 29).

Die einfach gestaltete Integration des entwickelten Prototyps in bestehende Systeme sorgt für bessere Kompatibilität zwischen unterschiedlichen Systemen und vereinfacht den Zugriff auf die relevanten Daten (Azaria et al., 2016, S. 29). Darüber hinaus weisen die Autoren (Azaria et al., 2016, S. 29) darauf hin, dass neu erfasste Patientendaten gleichzeitig aus unterschiedlichen Quellen kommen können, was ihren eigentlichen Transfer stark vereinfacht. Obwohl ein neues System geschaffen wird, welches gemeinsam von einer Vielzahl von unterschiedlichen Anbietern genutzt werden soll, wird aufgrund der dezentralen und verteilten Eigenschaften der genutzten Blockchain-Technologie kein neuer zentraler Angriffspunkt für Hacker gebildet (Azaria et al., 2016, S. 29).

Die Datenintegrität soll durch einen Mining-Prozess sichergestellt werden, der das Proof-of-Work als Konsensmechanismus nutzt (Azaria et al., 2016, S. 30). Dabei werden medizinische Forschungsinstitute in den Prozess integriert, indem anonymisierte medizinische Daten als Belohnung für das Proof-of-Work dienen (Azaria et al., 2016, S. 29). Dadurch erhalten die Forschungsinstitute eine zentrale Quelle für anonymisierte Daten im grossen Umfang (Azaria et al., 2016, S. 30). Dies eröffnet die Möglichkeit zur weitreichenden Analyse von Mustern in der medizinischen Behandlung und dem Auftreten bestimmter Erkrankungen, wobei gleichzeitig die Privatsphäre der Patienten geschützt wird und die Kosten reduziert werden können, welche mit traditionellen Studien einhergehen (Azaria et al., 2016, S. 30). Das Resultat ist eine Erhöhung der Quantität und Qualität der Daten, welche der medizinischen Forschung zur Verfügung stehen (Azaria et al., 2016, S. 26).

7 Problemfelder bei der Integration der Blockchain-Technologie

Dieses Kapitel befasst sich mit den möglichen Problemen und offenen Fragen bezüglich der weitverbreiteten Anwendung der Blockchain-Technologie in der Praxis.

7.1 Skalierbarkeit und Performance

Im eigentlichen Sinne dient eine Blockchain zur Erreichung von zwei Zielen: Einerseits soll ermöglicht werden, dass jeder Teilnehmer neue Transaktionsdaten einem gemeinsam unterhaltenen Register hinzufügen kann (Drescher, 2017, S. 207). Andererseits soll die Transaktionsgeschichte gegen Manipulations- und Fälschungsversuche abgesichert werden (Drescher, 2017, S. 207). Eine Blockchain erreicht diese Ziele durch eine «append-only» Datenstruktur (Daten können nur hinzugefügt, jedoch nicht geändert oder gelöscht werden), welche das Lösen eines kryptographischen Rätsels (Proof-of-Work) verlangt, bevor ein neuer Block angehängt werden kann (Drescher, 2017, S. 207). Dieses Verfahren ist absichtlich zeitaufwändig, was ein Manipulationsversuch der Transaktionsgeschichte untragbar kostenintensiv machen würde (Drescher, 2017, S. 207). Laut Drescher (2017, S. 207) haben diese Sicherheitsmassnahmen jedoch Auswirkungen auf die Skalierbarkeit und Performance der Blockchain.

Im Kontext der Blockchain-Technologie wird die Skalierbarkeit als die Anzahl von Nodes und User im Blockchain-Netzwerk definiert (Vukolic, 2016, S. 117). Die Performance bezieht sich auf die Latenz, das heisst die Zeit, die verstreicht, bis eine Transaktion als definitiv valide erachtet werden kann, und auf die Durchsatzleitung (Vukolic, 2016, S. 117-118). Die Durchsatzleistung entspricht der Anzahl an Transaktionen pro Zeiteinheit, welche durch die Blockchain verarbeitet werden können (Vukolic, 2016, S. 118).

Ein Problem der Bitcoin Blockchain ist die mangelnde Skalierbarkeit und Performance, welche auf sieben Transaktionen pro Sekunde und auf eine Latenzzeit von einer Stunde beschränkt ist (Vukolic, 2016, S. 113). Die Latenzzeit von einer Stunde beruht auf der Annahme, dass für eine eindeutige Bestätigung eines neu erstellten Blockes (und somit den Transaktionen), sechs weitere Blöcke abgewartet werden sollen, bis eine Gabelung der Blockchain sicher ausgeschlossen werden kann (Kapitel 2.3.3) (Vukolic, 2016, S. 113). Vukolic (2016, S. 113) bezeichnet dies als die «6-block transaction confirmation», wobei die einstündige Latenzzeit daraus abgeleitet

wird, dass für die Erstellung der sechs Blöcke je zehn Minuten benötigt werden, was einer Gesamtdauer von 60 Minuten entspricht. Dass es sich dabei um einen sehr hohen Wert handelt, wird besonders dann ersichtlich, wenn die 60 Minuten mit den Latenzzeiten des Kreditkartenunternehmens VISA verglichen werden, die höchstens wenige Sekunden betragen (Swan, 2015, S. 82). Mit nur sieben Transaktionen pro Sekunde kann die Bitcoin-Blockchain allerdings nicht die Anforderungen von vielen möglichen Anwendungsszenarien in der Praxis erfüllen (Vukolic, 2016, S. 117). So wickelt VISA durchschnittlich 2000 Transaktionen pro Sekunde ab (Zohar, 2015, S. 111-112) und kann gemäss Vukolic (2016, S. 113) bis zu 10'000 Transaktionen pro Sekunde bewältigen.

Eine Möglichkeit, die Transaktionsrate zu steigern, wäre eine Erhöhung der Speicherkapazität der einzelnen Blöcke, was eine höhere Transaktionszahl pro Block ermöglichen würde (Swan, 2015, S. 82). Dies würde gemäss Swan (2015, S. 82) allerdings zu einem neuen Problem bezüglich der Grösse der Blockchain führen, welches als «bloat» bezeichnet wird und auf das Aufblähen der Blockchain referenziert. Dabei besteht das Problem darin, dass die sogenannten «full nodes» stets eine aktuelle Kopie der gesamten Blockchain halten und das Aufblähen der Blockchain dazu führt, dass der dafür benötigte Speicherplatz exzessiv ansteigt (Swan, 2015, S. 82). Wie stark der benötigte Speicherplatz für die komplette Blockchain angewachsen ist, wird in Abbildung 30 dargestellt.

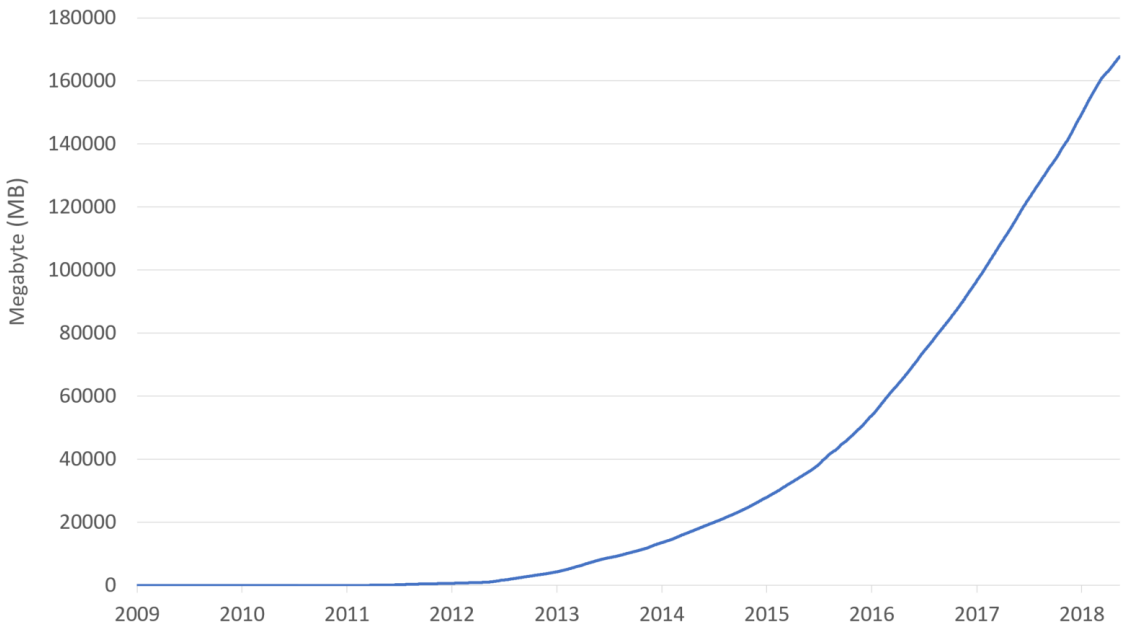


Abbildung 30: Benötigter Speicherplatz der Bitcoin Blockchain (Blockchain, 2018a)

Anfang Mai 2018 betrug die Grösse der Blockchain 163 GB, wobei diese innerhalb eines Jahres um 51.5 GB angewachsen war (Blockchain, 2018a). Obwohl 163 GB bereits eine gewisse Zeitspanne für den Download und eine signifikante Menge an Speicherplatz in Anspruch nimmt, würde eine Skalierung auf Transaktionsraten in der Grössenordnung von VISA (oder möglicherweise auf noch viel höhere Werte, damit eine weitverbreitete Anwendung der Blockchain realistisch erscheint), die Blockchain auf mehrere Petabytes (1 Petabyte = ~10^6 Gigabytes) aufblähen (Swan, 2015, S. 82). Swan (2015, S. 82) ist jedoch der Ansicht, dass sich Blockchains in Zukunft in diese Grössenordnungen entwickeln werden, beziehungsweise müssen, um sich zu einer etablierten Technologie entwickeln zu können.

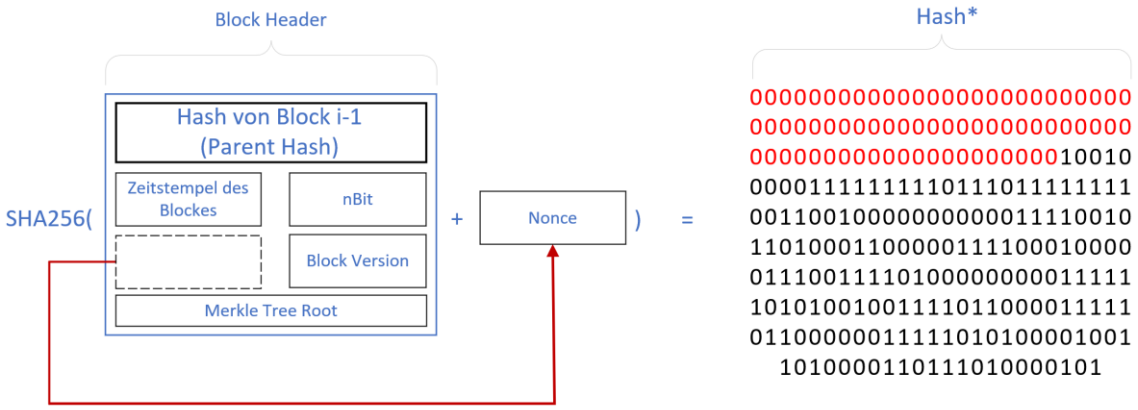
7.2 Hohe Kosten des Proof-of-Work

Wie beim Problem der limitierten Skalierbarkeit und Performance, liegt dem Problem der hohen Kosten ebenfalls der Proof-of-Work zugrunde (Drescher, 2017, S. 207). Das Finden der Lösung für das gestellte kryptographische Rätsel zur Erstellung eines neuen Blockes ist absichtlich mit hohem Aufwand und damit Kosten verbunden, um Manipulationsversuche möglichst unattraktiv zu machen Drescher, 2017, S. 207). Wie bereits in Kapitel 2.3.3 genauer erläutert, ist das Lösen dieses Rätsels mit dem Erraten einer Zahl verbunden, um einen geeigneten Hash zu generieren. Je mehr Hashes pro Sekunde berechnet werden können, desto höher ist die Chance für den Miner, rechtzeitig eine Lösung zu finden. Um eine möglichst hohe Hash-Rate zu erreichen, bedienen sich Miner speziell dafür geeigneter Hardware, die mit zusätzlichen Kosten verbunden ist (Vranken, 2017, S. 2-3). Diese mit dem Proof-of-Work einhergehenden Kosten beinhalten gemäss Drescher (2017, S. 207) beispielsweise Zeit, Energie und Geld.

Ein von Fachexperten häufig beachteter und im öffentlichen Interesse stehender Aspekt des Proof-of-Work ist dessen Energieverbrauch (Vranken, 2017, S. 1-2). Dabei gilt es zu beachten, dass der Energieverbrauch zwei hauptsächliche Ursachen besitzt (Tapscott & Tapscott, 2016, S. 331). Einerseits handelt es sich dabei um den benötigten Strom für den Betrieb der Mining-Hardware und andererseits um die erforderliche Energie zu ihrer Kühlung (Tapscott & Tapscott, 2016, S. 331). Laut Vranken (2017, S. 1-3) ist der tatsächliche Energieverbrauch, welcher für das Proof-of-Work der Bitcoin Blockchain benötigt wird, ein schwierig zu bestimmender Wert, da die Miner

geographisch weit verteilt sind und somit von unterschiedlichen Einflussfaktoren betroffen sind. Einer dieser möglichen Einflussfaktoren ist zum Beispiel das Klima, so können sich Miner in kälteren Regionen die natürlich kalte Luft zu Nutze machen, um die Kosten für die Kühlung zu reduzieren (Vranken, 2017, S. 3). Vranken (2017, S. 6-7) berücksichtige bei der Schätzung zum Energieverbrauch der Bitcoin Blockchain unterschiedliche Studien, wobei die Ergebnisse teilweise stark voneinander abwichen. Entscheidend bei der Berechnung des Energieverbrauchs ist die Effizienz der Mining-Hardware, ausgedrückt in Hashes pro Joule (Vranken, 2017, S. 5-6). Vranken (2017, S. 7) schätzt den Energieverbrauch auf 100 bis 500 Megawatt, was 3 bis 16 Petajoules pro Jahr entspricht. Gemäss Tapscott und Tapscott (2016, S. 330) entspricht dies am oberen Ende dem jährlichen Energieverbrauch von Zypern.

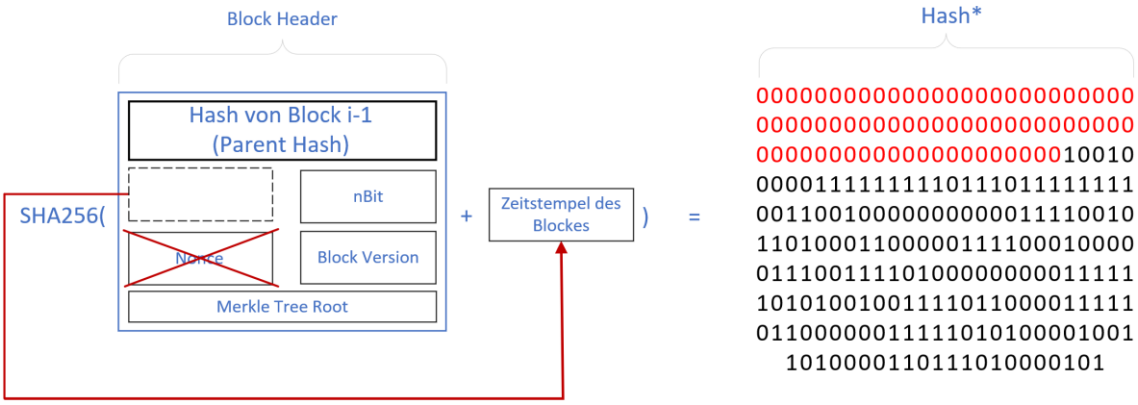
Die Aspekte des hohen Energieverbrauchs, die Skalierungsprobleme und die mangelnde Performance haben dazu geführt, dass vermehrt nach alternativen Verfahren zur Verifikation und Erstellung von neuen Blöcken gesucht wurde (Kewell et al., 2017, S. 432). Eine mögliche Alternative ist der sogenannte Proof-of-Stake Konsensmechanismus (Vranken, 2017, S. 7). Das Proof-of-Stake basiert auf dem Besitznachweis der vom Miner gehaltenen Kryptowährung, wobei eine einzelne Einheit der Kryptowährung als «Coin» bezeichnet wird (Vranken, 2017, S. 7). Das Ziel beim Mining-Prozess ist ähnlich wie beim Proof-of-Work (Vranken, 2017, S. 7). Beim Proof-of-Work versuchen die Miner möglichst schnell, die gesuchte Nonce zu erraten, um einen Hash zu finden, welcher kleiner als der vom Schwierigkeitsgrad definierte Wert ist (Abbildung 31) (Zheng et al., 2016, S. 8). Da die Miner mit dem restlichen Netzwerk konkurrieren, haben sie einen Anreiz, möglichst viele Berechnungen pro Sekunde durchzuführen (Vranken, 2017, S. 2-3). Dies führt allerdings zu den in diesem Abschnitt beschriebenen Nachteilen.



* Der Hash des gesamten Blockes darf einen vordefinierten Wert nicht überschreiten, dieser Wert wird auch als Schwierigkeitsstufe des Proof-of-Work bezeichnet und bedeutet, dass der Hash mit einer bestimmten Anzahl von 0 beginnen muss (Krombholz et al., 2016, S. 557).

Abbildung 31: Funktionsweise des Proof-of-Work

Beim Proof-of-Stake Konsensmechanismus gibt es dagegen keine Nonce, die es zu finden gilt (Vranken, 2017, S. 7). Stattdessen ist der generierte Hash abhängig vom aktuellen Zeitstempel (Abbildung 32), welcher sich jede Sekunde ändert (Vranken, 2017, S. 7).



* Der Schwierigkeitsgrad des Hashs ist unterschiedlich für jeden Miner.

Abbildung 32: Funktionsweise des Proof-of-Stake

Da sich der Input der Hash-Funktion im Sekundentakt ändert, können Miner nur einen Hash pro Sekunde berechnen, was den Energiebedarf massiv einschränkt (Vranken, 2017, S. 7). Ein Miner kann seine Chancen vergrössern, indem er sich mittels einer «coinstake transaction» selbst Coins überweist (Vranken, 2017, S. 7). Da alle Miner denselben Input zum Lösen des Proof-of-Stake haben und alle auf einen Hash pro Sekunde beschränkt sind, gibt es stattdessen einen persönlichen Schwierigkeitsgrad für jeden Miner (Vranken, 2017, S. 7). Wie beim Proof-of-Work definiert der Schwierigkeitsgrad die maximale Grösse des Outputs (Krombholz et al., 2016, S. 557). Umso

kleiner diese Zahl ist, desto schwieriger ist das Rätsel (Krombholz et al., 2016, S. 557). Der Schwierigkeitsgrad des Proof-of-Stake wird aus der Coinstake Transaktion berechnet: Anzahl Coins der Coinstake Transaction multipliziert mit der Zeitdauer seit der Coinstake Transaktion (Vranken, 2017, S. 7). Das Ergebnis dieser Berechnung wird als «Coin Age» bezeichnet und der Schwierigkeitsgrad ist umgekehrt proportional dazu (Vranken, 2017, S. 7). Dies bedeutet, dass die Chancen für das erfolgreiche Lösen des Rätsels umso höher werden, desto mehr Coins die Transaktion beinhaltet und desto älter die Transaktion ist (Vranken, 2017, S. 7). Nachdem ein Miner erfolgreich einen Block erstellen konnte, wird das Coin Age der Coinstake Transaktion wieder zurückgesetzt (Vranken, 2017, S. 7).

Neben dem Proof-of-Stake gibt es zahlreiche andere Konsensmechanismen, welche einen deutlich geringeren Energiebedarf als das Proof-of-Work haben oder den Minern andere Aufgaben als das Lösen von kryptographischen Rätseln stellen (Kewell et al., 2017, S. 432). Kewell et al. (2017, S. 432) nennen als Beispiel SolarCoin, bei dem Miner für die Generierung von Solarstrom belohnt werden, oder Gridcoin, die einen Algorithmus verwenden, um Anreize für die Teilnahme an wissenschaftlichen Projekten zu schaffen.

7.3 Keine nachhaltige Dezentralisierung

Das dezentralisierte Netzwerk von Minern und somit die Eliminierung einer zentralen Autorität ist eine der fundamentalen Eigenschaften der Blockchain-Technologie (Laurence, 2017, S. 10). Die Eigenschaften eines solchen dezentralisierten Netzwerks tragen zur Sicherheit und zur Unveränderlichkeit der aufgezeichneten Transaktionen bei und in Kombination mit dem Konsensmechanismus wird ebenfalls die Datenintegrität gewährleistet (Olnes et al., 2017, S. 356). Der Proof-of-Work Konsensmechanismus sorgt für einen Konkurrenzkampf zwischen den Minern und liefert ihnen den Anreiz, möglichst hohe Hashraten zu erreichen (Drescher, 2017, S. 208).

Wie im vorherigen Abschnitt beschrieben, spielt der Energieverbrauch beim Lösen des kryptographischen Rätsels eine wichtige Rolle, da der Mining-Prozess nur kosteneffizient ist, wenn der erwirtschaftete finanzielle Ertrag in Form von Bitcoins die notwendigen Investitionen (Kosten für Hardware und Strom) übersteigt (Vranken, 2017, S. 2-3). Produzenten von Computerhardware haben den Bedarf nach energieef-

fizienter Hardware für Miner erkannt und Komponenten entwickelt, die ausschliesslich auf das Lösen des kryptographischen Rätsels spezialisiert sind (Vranken, 2017, S. 3-4). Laut Drescher (2017, S. 208) hat diese Entwicklung allerdings dazu geführt, dass das Minen von Bitcoins ohne darauf spezialisierte Hardware in vielen Fällen ein Verlustgeschäft ist und vor allem kleinere Miner dazu zwingt, aus dem Netzwerk auszutreten. Dies hatte zur Konsequenz, dass sich im einst stark diversifizierten Bitcoin-Netzwerk eine kleine Anzahl von Gruppen (Pools) mit jeweils sehr hoher Rechenkapazität gebildet hat, die sich die hohen Kosten der Spezialhardware leisten kann (Drescher, 2017, S. 208). Daraus folgt eine hohe Konzentration der gesamten Hashrate in wenigen Pools (Swan, 2015, S. 83). Abbildung 33 stellt die geschätzte Verteilung der Rechenkapazität (Hashrate) unter den grössten Mining-Pools im Bitcoin-Netzwerk basierend auf den im Zeitraum vom 8. bis 11. Mai 2018 586 erstellten Blöcke dar. Es ist ersichtlich, dass sich eine kleine Gruppe von Pools die Mehrheit der gesamten Rechenkapazität des Netzwerks teilt. Hierbei ist nochmals zu erwähnen, dass eine Kontrolle von mindestens 51 Prozent der gesamten Computerpower ausreichend ist, um die gesamte Blockchain zu kontrollieren und Transaktionen zu manipulieren (Tapscott & Tapscott, 2016, S. 340-341).

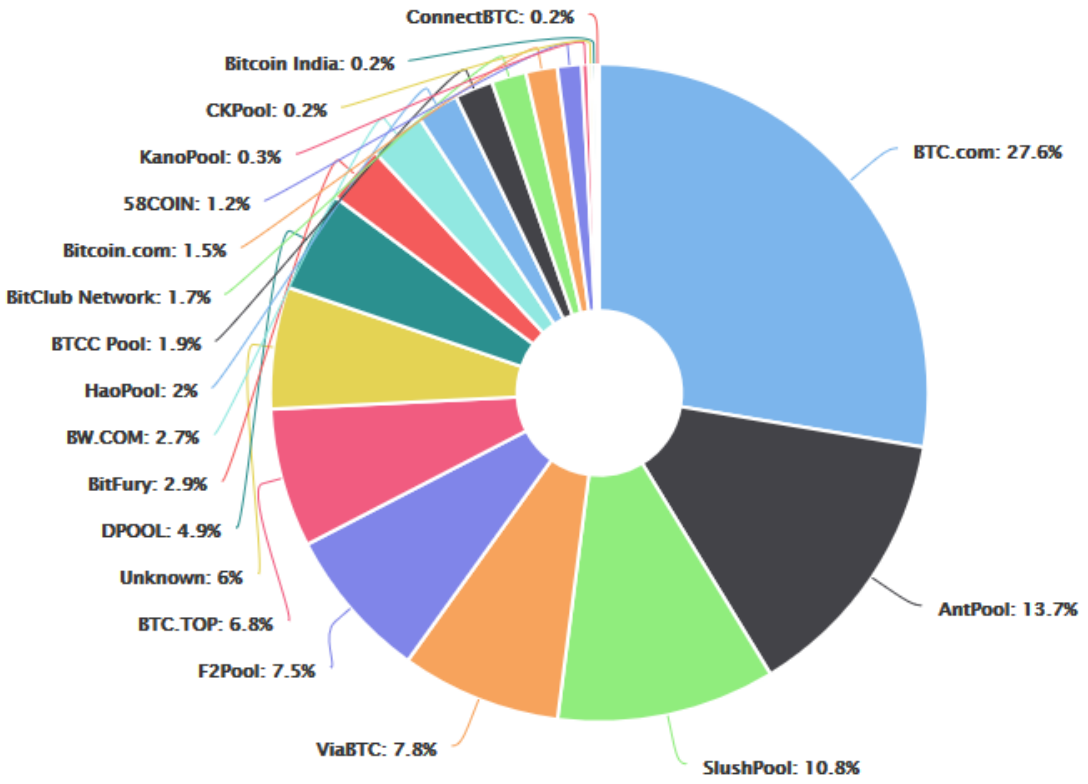


Abbildung 33: Verteilung der Computerpower von Pools im Bitcoin-Netzwerk (Blockchain, 2018b)

Das ursprünglich stark diversifizierte Netzwerk von Peers, welche die Integrität des Systems sicherstellten, wird nun hauptsächlich von einer geringen Anzahl von Gruppen kontrolliert, die zusammen ein Oligopol bilden (Drescher, 2017, S. 208). Gemäss Drescher (2017, S. 208) verhält sich dieses Oligopol wie auch in anderen Industrien, in denen eine kleine Gruppe von dominierenden Anbietern ihre Machtstellung missbräuchlich ausnutzen könnten. Aus einer technischen Perspektive handelt es sich zwar weiterhin um ein dezentralisiertes und verteiltes System, jedoch wird der ursprüngliche Ansatz der Dezentralisierung untergraben (Drescher, 2017, S. 208).

8 Ausblick – Blockchains in Kombination mit dem Internet of Things

Das Internet of Things (IoT) hat sich zu einem der populärsten Schlagwörter der letzten Jahre im technischen Bereich entwickelt (Di Martino, Li, Yang & Esposito, 2018, S. 3). Im Grunde handelt es sich bei der Technologie um das Verknüpfen von mehreren intelligenten Geräten, die untereinander Informationen und Daten austauschen können (Di Martino et al., 2018, S. 3). Di Martino et al. (2018, S. 3) beschreiben die Technologie wie folgt: «IoT represents the ability of network devices to sense, collect and sometimes even analyse in loco data from the world around us, and then share that data across the Internet». Die theoretischen Anwendungsmöglichkeiten von IoT-Geräten sind breit und beinhalten beispielsweise tragbare Geräte zur Messung und Analyse von Daten bei sportlicher Betätigung oder die Erhebung von Vitalwerten (Di Martino et al., 2018, S. 3). Weiteres Potential gibt es im Bereich von Smart Homes mit dem Einsatz von intelligenten Geräten zur Steuerung der Temperatur oder dem automatischen Bestellen von Nahrungsmittel (Di Martino et al., 2018, S. 3). Laut Crosby, Pattanayak, Verma und Kalyanaraman (2016, S. 16) handelt es sich bei dem IoT um eine Technologie, welche sowohl bei den Konsumenten als auch bei Unternehmen zunehmend populärer wird. Aktuell basiert der Datenaustausch zwischen den angeschlossenen Geräten bei einer grossen Mehrheit der IoT-Plattformen auf einem zentralen Verteiler (Crosby et al., 2016, S. 16). Dieser Cloud-basierte zentrale Aspekt der Datentransaktion zwischen IoT-Geräten stellt insbesondere ein Risiko dar, da es einen Single-Point-of-Failure gibt, also einen zentralen Punkt, von dem eine grosse Anzahl von Geräten abhängig ist und bei eventuellen Attacken oder technischen Problemen alle damit verbundenen Geräte ebenfalls betroffen sein können (Huckle, Bhattacharya, White & Beloff, 2016, S. 463). Li, Xu und Zhao (2015, S. 256) gehen ausserdem davon aus, dass es im Bereich von IoT fünf technische Probleme existieren, welche noch gelöst werden müssen: Erstens fehlt eine klare Definition von Datensicherheit und Privatsphäre im Kontext der Gesellschaft, des Gesetzes und der Kultur, zweitens fehlt ein verlässlicher Vertrauensmechanismus (Datenintegrität) bezüglich der Transaktionen zwischen den Endgeräten, ein dritter Bereich ist die Sicherheit der Kommunikation zwischen diesen Geräten, das vierte bestehende Problem bezieht sich auf den Datenschutz bei der Kommunikation und den Userdaten und der fünfte Punkt ist die Sicherheit der Applikationen. Kshetri (2017a, S. 1032) argumentiert, dass die Blockchain-Technologie besonders vielversprechend sei, diese Probleme der Sicherheit und des Datenschutzes zu lösen.

Kshetri (2017b, S. 68-72) identifiziert vier Herausforderungen (Tabelle 4) im Bereich von IoT, welche durch die Blockchain-Technologie gelöst werden könnten.

Challenge	Explanation	Potential blockchain solution
Costs and capacity constraints	It is a challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1,000 times the level of 2016 will be needed.	No need for a centralized entity: devices can communicate securely, exchange value with each other, and execute actions automatically through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck or point of failure and disrupts the entire network; vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists.	Secure messaging between devices: the validity of a device's identity is verified, and transactions are signed and verified cryptographically to ensure that only a message's originator could have sent it.
Cloud server downtime and unavailability of services	Cloud servers are sometimes down due to cyberattacks, software bugs, power, cooling, or other problems.	No single point of failure: records are on many computers and devices that hold identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses.	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: if one device's blockchain updates are breached, the system rejects it.

Tabelle 4: Internet of Things und Blockchain (Kshetri, 2017b, S. 70)

Dabei handelt es sich einerseits um die Bedenken bezüglich der Kosten und der Kapazität von zentralisierten Cloud-Lösungen, die bei dem prognostizierten exponentiellen Wachstum von IoT-Geräten an ihre Grenzen stossen könnte (Kshetri, 2017b, S. 70). Andererseits bezeichnet Kshetri (2017b, S. 70) die Cloud-basierte Architektur als mangelhaft, da sich im Falle von Ausfällen oder Angriffen auf einzelne IoT-Geräte das Problem auf das gesamte Netzwerk ausbreiten könnte. Zusätzlich kann die Blockchain-Technologie beispielsweise als Basis für ein Identitäts- und Bewilligungsmanagementsystem genutzt werden, um die Sicherheit von IoT zu stärken (Kshetri, 2017a, S. 1032).

Das Grundproblem beim Datenschutz bezüglich IoT-Geräte besteht darin, dass in vielen Fällen sensitive Daten des Users von den Geräten gespeichert oder übermittelt werden (Di Martino et al., 2018, S. 5). Dabei kann es sich beispielsweise um den physischen Standort des Users oder dessen Daten zu seinem Gesundheitszustand wie das Gewicht oder den Blutdruck handeln (Di Martino et al., 2018, S. 5). Das Sicherheitsrisiko besteht darin, dass diese Daten abgefangen oder dass die Geräteeinstellungen manipuliert werden könnten, sodass mehr Informationen aufgezeichnet oder geteilt werden, als vom User vorgesehen (Kshetri, 2017a, S. 1033). Um eine Manipulation der Einstellungen zu verhindern oder zumindest sofort entdecken zu können, kann die Blockchain-Technologie genutzt werden (Kshetri, 2017a, S. 1033). So könnte ein kryptographischer Hash der Firmware (Software für ein spezifisches Gerät) auf einer

privaten Blockchain gespeichert werden und somit ein permanentes Register aller Geräte und deren Konfigurationen zu erstellen (Kshetri, 2017a, S. 1033). Damit lassen sich die Geräte eindeutig identifizieren und es besteht eine Garantie, dass die Geräte nicht manipuliert wurden, da sich ansonsten der kryptographische Hash des Gerätes ändern würde (Kshetri, 2017a, S. 1033). So könnte ein System designt werden, das das Verbinden der Geräte nur erlaubt, wenn diese Geräte jeweils über einen gültigen Hash verfügen (Kshetri, 2017a, S. 1033). Dabei kann die Blockchain-Technologie auch für das sichere Übermitteln von Informationen genutzt werden, indem die versendeten Transaktionen (Daten/Informationen übermittelt von einem IoT-Gerät) mittels Public Key Kryptographie signiert werden und somit eine automatische Überprüfung der Validität der Transaktion durch das empfangende Gerät ermöglicht (Kshetri, 2017a, S. 1033). Dies entspricht dem gleichen Prinzip wie dem der digitalen Unterschriften, welche zur Signatur von Transaktion in der Bitcoin Blockchain genutzt werden (Kapitel 2.3.1).

Die präsentierten Anwendungsmöglichkeiten zeigen auf, wie die dezentralen, eigenständigen und vertrauenslosen Eigenschaften der Blockchain-Technologie dazu genutzt werden können, um einige der grössten Probleme anzugehen, welche mit einem Cloud-basierten IoT-System in Verbindung stehen (Kshetri, 2017a, S. 1036).

9 Schlussfolgerung und Implikation

Im Zuge dieser Bachelorarbeit wurde die Funktionsweise der Blockchain-Technologie erklärt und die möglichen Anwendungspotentiale im Gesundheitswesen aufgezeigt. In diesem abschliessenden Kapitel werden die wichtigsten Aspekte der Blockchain-Technologie und deren Implikationen für die praxisorientierte Anwendung nochmals zusammengefasst.

Der im Jahr 2008 von Nakamoto (2008, S. 1-2) geprägte Begriff Blockchain wurde in den vergangenen Jahren von vielen Managern in den Wortschatz aufgenommen. Trotz des grossen Interesses mangelt es häufig an Wissen über die Funktionsweise der Technologie und das Potential bleibt unentdeckt oder wird missverstanden. Das ursprüngliche Ziel der Bitcoin Blockchain war die Entwicklung einer technischen Lösung für das Problem des doppelten Ausgebens, um finanzielle Transaktionen ohne Intermediäre zu ermöglichen (Nakamoto, 2008, S. 1). Seither hat sich die Technologie weiterentwickelt und zahlreiche Unternehmen und Start-Ups arbeiten an eigenen Lösungen. Trotz zahlreicher Innovationen in diesem Bereich handelt es sich bei einer Blockchain im eigentlichen Sinne nicht um eine neue Technologie, viel eher ist es eine Kombination von verschiedenen älteren Technologien (Laurence, 2017, S. 42). Der wohl wichtigste Bestandteil der Blockchain-Technologie ist der Konsensmechanismus, welcher es einem verteilten Netzwerk von Peers erlaubt, sich über den aktuellen Stand der Blockchain einig zu werden (Laurence, 2017, S. 12). Sobald das Netzwerk einen Konsens erreicht hat, kann ein neuer Block an die Kette von Blöcken angehängt werden, wobei der neue Block mit dem vorangehenden Block kryptographisch verknüpft wird (Courtois et al., 2014, S. 135). Die Kombination eines verteilten Netzwerks mit dem Konsensmechanismus und der kryptographischen Sicherheit macht die Blockchain zu einer revolutionären Innovation (Laurence, 2017, S. 42). Es sind diese Eigenschaften, welche zur Unveränderbarkeit und Sicherheit von Transaktionen beitragen und die Datenintegrität der gesamten Blockchain gewährleisteten (Olnes et al., 2017, S. 356).

Im zweiten Teil der Arbeit wurde das Anwendungspotential in der Gesundheitsbranche untersucht und die Problemfelder der Blockchain-Technologie analysiert. Insgesamt konnten fünf unterschiedliche Anwendungsfelder identifiziert werden, welche als realistisch und ökonomisch relevant bezeichnet werden können. Alle Anwendungsgebiete liefern durch die erhöhte Sicherheit und Unveränderbarkeit der Daten einen Mehrwert. Insbesondere die im Detail behandelte Anwendung im Bereich der

elektronischen Datenerfassung von Gesundheitsdaten, gemäss Azaria et al. (2016, S. 25) ein durch eine starke Innovationsträgheit gekennzeichneter Bereich, könnte möglicherweise eine disruptive Wirkung auf bestehende Modelle haben. So werden bei dem von Azaria et al. (2016, S. 25-30) präsentierten Proof of Concept «MedRec» nicht nur die von Mandl et al. (2001, S. 284) definierten Standards zur Verwaltung von digitalen Patientendaten eingehalten, sondern auch die Patienten werden ins Zentrum der Kontrolle über die Daten gerückt. Die elektronische Erfassung von Patientendaten und die Definition von Zugriffsrechten über die Blockchain könnteen vier bestehende Problemfelder im Bereich des Datenmanagements im Gesundheitswesen lösen (Azaria et al., 2016, S. 26). Sowohl der uneinheitliche und langsame Zugriff auf Patientendaten als auch die Inkompatibilität zwischen verschiedenen Systemen, beides verursacht durch die Vielzahl von unterschiedlichen genutzten Systemen, haben hohe Effizienzeinbussen beim Austausch von Patientendaten und über mehrere Systeme hinweg fragmentierte Patientenakten zur Folge (Azaria et al., 2016, S. 25). Beide Aspekte können mittels einer zentralen Blockchain-Plattform angegangen werden und die Effizienz beträchtlich steigern. Hierbei ist zu erwähnen, dass die Applikation zwar wie erwähnt im Zentrum des Datenaustauschs steht, die Anwendung selbst jedoch eine dezentrale und verteilte Netzwerkarchitektur aufweist (Azaria et al., 2016, S. 29). Dies bedeutet, dass keine neue zentrale Entität geschaffen wird, welche mögliche Risiken eines Single-Point-of-Failure beinhalten könnte (Azaria et al., 2016, S. 29). Ein weiteres von Azaria et al. (2016, S. 26) identifiziertes Problemfeld ist die Kontrolle über die Daten. Durch ein in die Applikation eingebautes Berechtigungsmanagement haben die Patienten die Autorität über die eigenen Daten und können entsprechende Zugriffsrechte erteilen (Azaria et al., 2016, S. 27).

Das letzte Problemfeld behandelt die für die medizinische Forschung zur Verfügung gestellten Daten (Azaria et al., 2016, S. 26). Hierfür werden in dieser Arbeit zwei unterschiedliche Lösungsansätze präsentiert. Einerseits ist es ein Bestandteil des Proof-of-Concept «MedRec» von Azaria et al. (2016, S. 25-30), andererseits wurde es in einem separaten Anwendungsfall in Kapitel 5.6 zur Erhöhung der Qualität und Quantität der Daten für die medizinische Forschung diskutiert. Zusätzlich behandelte Anwendungsmöglichkeiten betreffen die Abwicklung von Versicherungsansprüchen, die Nachverfolgbarkeit von Medikamenten entlang der Supply Chain zur Eindämmung des Vertriebs von gefälschten Medikamenten und die Einführung der Blockchain-Technologie im Gesundheitswesen auf staatlicher Ebene. In allen vorgestellten

Anwendungsgebieten stehen primär die Datenintegrität und die Sicherheit im Zentrum. Die Analyse hat gezeigt, dass, obwohl alle aufgezeigten Beispiele Potential haben, die Anwendung der Blockchain-Technologie zur elektronischen Erfassung der Patientendaten den grössten Einfluss auf bestehende Geschäftsmodelle haben könnte.

Mangels aussagekräftiger Quellen zur Schätzung der möglichen Kosteneinsparungen durch die verbesserte Kompatibilität zwischen verschiedenen Systemen und dem Effizienzgewinn durch die Vereinheitlichung des Datenzugriffs, kann das Kosteneinsparungspotential nicht genau quantifiziert werden. Dennoch könnte die Blockchain-Technologie im Bereich der elektronischen Erfassung von Patientendaten im Vergleich zu den traditionellen Technologien eine «very different value proposition» haben.

Dies lässt sich insbesondere damit begründen, dass aus der Perspektive von Anbietern im Gesundheitswesen die Kosten gesenkt werden können, indem der Zugriff auf die Daten einheitlich gestaltet und Kompatibilität zwischen Systemen geschaffen wird. Ergänzend dazu reduziert die garantierte Datenintegrität den finanziellen Aufwand von Audits. Ein weiterer Grund ist die Involvierung des Patienten. Die Möglichkeit für Patienten, die komplette Kontrolle über die eigenen Daten zu erhalten, war mit bisherigen Technologien nicht umsetzbar. Dies könnte den Umgang mit sensitiven Daten revolutionieren.

Ein noch nicht berücksichtigter Faktor in Bezug auf die unterschiedlichen Anwendungsmöglichkeiten sind die in der Arbeit identifizierten Problemfelder der Blockchain-Technologie. Dabei handelt es sich um die mangelnde Skalierbarkeit und Performance, die hohen Kosten des Proof-of-Work und die anstehenden Probleme bezüglich einer nachhaltigen Dezentralisierung des Netzwerks. Es kann argumentiert werden, dass die drei Aspekte die Value Proposition der vorgestellten Anwendung (Digitalisierung der Patientendaten) negieren könnten.

Skalierbarkeit und Performance: Hierbei sind drei Faktoren relevant: die Anzahl möglicher Transaktionen pro Sekunde, die Latenz und die Grösse der Blockchain (Vukolic, 2016, S. 117; Swan, 2015, S. 82). Diese drei Faktoren haben je nach Anwendungsbereich unterschiedliche Implikationen. In Bezug auf den Austausch von Patientendaten kann argumentiert werden, dass in den meisten Fällen eine erhöhte Latenz (Zeit, bis die Datenintegrität garantiert werden kann) keine entscheidende Rolle spielt.

Wie stark die beschränkte Anzahl von Transaktionen pro Sekunde (sieben pro Sekunde im Falle der Bitcoin Blockchain) die Umsetzbarkeit beeinträchtigt, ist vom benötigten Transaktionsvolumen abhängig. Bei der Beschreibung des Problems wurde hierzu ein Vergleich mit dem Kreditkartenunternehmen VISA gemacht. Im Kontext von Transaktionen von Patientendaten könnte sich der Wert jedoch in den meisten Situationen (ausser eventuell bei internationaler Nutzung) als ausreichend erweisen. Die letzte Problemstellung in Bezug auf die Skalierbarkeit bezieht sich auf die Grösse der Blockchain. Ein ausschlaggebendes Argument für die Nutzung der Blockchain-Technologie ist, dass eine Datei und jede Änderung an dieser entlang der Blockchain bis zum Ursprungspunkt zurückverfolgt werden kann. Eine Voraussetzung dafür ist jedoch, dass die Full-Nodes im Netzwerk stets eine Kopie der gesamten Blockchain halten. Eine logische Folge davon ist, dass das benötigte Speichervolumen über die Zeit zunimmt und besonders bei Blockchains mit hohem Transaktionsvolumen in relativ kurzer Zeit exzessive Werte erreichen kann (Swan, 2015, S. 82). Doch auch in diesem Bereich lässt sich die Auswirkung dieses Problems im Kontext der vorgestellten Anwendung relativieren. Ein entscheidender Unterschied zwischen der Bitcoin Blockchain und einer Blockchain-basierten Lösung für ein Patientendatenmanagementsystem ist, dass es sich aufgrund der Sensitivität der Daten um eine Private-Permissioned-Blockchain handelt. Dies bedeutet, dass nur ausgewählte Parteien Full-Nodes betreiben dürfen. Mit hoher Wahrscheinlichkeit handelt es sich dabei um Institutionen (beispielsweise Spitäler, Gesundheitsbehörden und Forschungsinstitute), die bereits die nötige Infrastruktur besitzen, um mit hohen Datenvolumina umgehen zu können.

Hohe Kosten des Proof-of-Work: Im dazugehörigen Kapitel 8.2 «Hohe Kosten des Proof-of-Work» wurden die Nachteile des Proof-of-Work beschrieben. Wie bereits beschrieben, ist dieser Prozess absichtlich mit hohem Aufwand verbunden, um Manipulationsversuche zu verhindern (Drescher, 2017, S. 207). Die Kosten beziehen sich hauptsächlich auf den hohen Energieverbrauch der Computer, die zur Berechnung der gesuchten Nonce benötigt werden und auf die durch den Konkurrenzkampf zwischen den Miner hervorgerufenen hohen Investitionen in Hardwarekomponenten (Vranken, 2017, S. 1-3). Hierbei sind die Auswirkungen auf die Nachhaltigkeit einer Anwendung im Gesundheitswesen etwas schwieriger einzuschätzen. Obwohl es sich um eine Private-Permissioned-Blockchain handelt und somit die Anzahl der Miner beschränkt

ist, haben diese trotzdem einen finanziellen Anreiz, möglichst hohe Rechenkapazitäten zu haben, um einen Vorteil gegenüber den anderen Miner zu erhalten. Natürlich handelt es sich beim Konkurrenzkampf um ein wichtiges Prinzip des Proof-of-Work, dennoch könnten zu hohe Kosten des Proof-of-Work dazu führen, dass eine Blockchain-basierte Lösung unattraktiv wird.

Keine nachhaltige Dezentralisierung: Bei diesem Problem handelt es sich zum Teil um eine Folgeerscheinung der hohen Kosten des Proof-of-Work (Drescher, 2017, S. 208). Aufgrund des hohen Investitionsbedarfs in Mining-Hardware, werden vermehrt kleinere Parteien aus dem Wettbewerb verdrängt (Drescher, 2017, S. 208). Dies führte bereits in der Bitcoin Blockchain zur Bildung eines Oligopols (Drescher, 2017, S. 208). Jedoch wird ein möglichst verteiltes und dezentrales Netzwerk benötigt, um die Sicherheit, die Unveränderbarkeit und die Integrität der Daten zu garantieren (Olnes et al., 2017, S. 356). Solange ein Konkurrenzkampf zwischen den Miner besteht, werden auch Applikationen im Gesundheitswesen von diesem Problem betroffen sein.

Wie bereits zu Beginn dieses Kapitels erläutert wurde, handelt es sich bei einer Blockchain-basierten Applikation zur Erfassung und zum Teilen von Patientendaten möglicherweise um eine disruptive Innovation, die eine *very different value proposition* bietet. Werden die aktuellen Problemfelder der Blockchain-Technologie in Betracht gezogen, müssen eventuell manche Vorteile etwas relativiert werden. Obwohl die Anwendung eher gering von der mangelnden Skalierbarkeit und Performance betroffen sein könnte, lassen die Kosten des Proof-of-Work und dessen Auswirkungen Skepsis aufkommen. Allerdings handelt es sich hierbei nicht um branchenspezifische Nachteile der Blockchain-Technologie und es kann, wie in diesem Kapitel erläutert, sogar davon ausgegangen werden, dass die Gesundheitsbranche in einem geringeren Ausmass davon betroffen ist. Um nachhaltig anwendbare Applikationen und Systeme entwickeln zu können, sind weitere Fortschritte (wie zum Beispiel das Proof-of-Stake) in der Blockchain-Technologie nötig.

10 Literaturverzeichnis

Angraal, S., Krumholz, H. M. & Schulz, W. L. (2017). Blockchain Technology Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9), 1-3. https://doi.org/10.1161/CIRCOUTCOMES.117.003800

Archa, Alangot, B. & Achuthan, K. (2017). Trace and Track: Enhanced Pharma Supply Chain Infrastructure to Prevent Fraud. In N. Kumar & A. Thakre (Hrsg.), *Ubiquitous Communications and Network Computing* (S. 189-195). Cham: Springer.

Asharaf, S. & Adarsh, S. (2017). *Decentralized computing using blockchain technologies and smart contracts: Emerging research and opportunities.* doi:10.4018/978-1-5225-2193-8

Azaria, A., Ekblaw, A., Vieira, T. & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. In I. Awan & M. Younas (Hrsg.), *2016 2nd International Conference on Open and Big Data*. (S. 25-30). Wien: IEEE.

Baran, P. (1964). On distributed communications networks. *IEEE Transactions on communication systems*, 12(1), 1-9. doi:10.1109/TCOM.1964.1088883

Benchoufi, M. & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials*, 18, 335-339. https://doi.org/10.1186/s13063-017-2035-z

Bheemaiah, K. (2017). *The Blockchain Alternative – Rethinking Macroeconomic Policy and Economic Theory*. doi:10.1007/978-1-4842-2674-2

Bitcoinwisdom (2018). Bitcoin difficulty vom 23.5.2017 bis 1.4.2018. Abgerufen am 10. April 2018 von https://bitcoinwisdom.com/bitcoin/difficulty

Blockchain (2018a). Entwicklung des benötigten Speichervolumens für die Bitcoin Blockchain vom 3.1.2009 bis 8.5.2018. Abgerufen am 8. Mai 2018 von https://blockchain.info/charts/blocks-size?timespan=all

Blockchain (2018b). Verteilung der Hash-Rate unter den grössten Mining-Pools vom 8.5.2018 bis 11.5.2018. Abgerufen am 11. Mai 2018 von https://blockchain.info/pools

Bowden, R., Keeler, H. P., Krzesinski, A. E., & Taylor, P. G. (2018). *Block arrivals in the Bitcoin blockchain*. (Cryptography and Security Working Paper 1801.07447) Abgerufen von der Cornell University Library Webseite: https://arxiv.org/abs/1801.07447

Burgwinkel, D. (2016). Blockchaintechnologie und deren Funktionsweise verstehen. In D. Burgwinkel (Hrsg.), *Blockchain Technology – Einführung für Business- und IT Manager* (S. 3-50). Berlin & Boston: Walter de Gruyter.

Buterin, V. (2014). *A next-generation smart contract and decentralized application platform* (White Paper). Abgerufen von https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Chaves, R., Kuzmanov, G., Sousa, L. & Vassiliadis, S. (2006). Improving SHA-2 Hardware Implementations. In L. Goubin & M. Matsui (Hrsg.), *Cryptographic Hardware and Embedded Systems – CHES 2006* (S. 298-310). Berlin: Springer.

Cockburn, R., Newton, P. N., Agyarko, E. K., Akunyili, D. & White, N. J. (2005). The Global Threat of Counterfeit Drugs: Why Industry and Governments Must Communicate the Dangers. *PLoS Medicine*, 2(4), 302-308. https://doi.org/10.1371/journal.pmed.0020100

Courtois, N. T., Grajek, M. & Naik, R. (2014). Optimizing SHA256 in Bitcoin mining. In Z. Kotulski, B. Ksiezopolski & K. Mazur (Hrsg.), *Cryptography and Security Systems* (S. 131-144). Heidelberg, New York, Dordrecht & London: Springer.

Crosby, M., Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation Review*, 2, 6-19.

Davidson, S., De Filippi, P. & Potts, J. (2016). *Economies of Blockchain*. (SSRN Working Paper 2744751) Abgerufen von der SSRN Webseite: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751

Dhillon, V., Metcalf, D. & Hooper, M. (2017). *Blockchain Enabled Applications – Understanding the Blockchain Ecosystem and How to Make it Work for You*. doi: 10.1007/978-1-4842-3081-7

Di Martino, B., Li, K., Yang, L. T. & Esposito, A. (2018). Trends and Strategic Researches in Internet of Everything. In B. Di Martino, K. Li, L. T. Yang & A. Esposito (Hrsg.), *Internet of Everything – Algorithms, Methodologies, Technologies and Perspectives* (S. 1-12). https://doi.org/10.1007/978-981-10-5861-5

Drescher, D. (2017). *Blockchain Basics – A non-technical introduction in 25 steps*. doi:10.1007/978-1-4842-2604-9

Engelhardt, M. A. (2017). Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. *Technology Innovation Management Review*, 7(10), 22-34.

Fairfiled, J. A. T. (2014). Smart Contracts, Bitcoin Bots, and Conusmer Protection. *Washington and Lee Law Review Online*, 71(2), 35-50.

Gennaro, R., Goldfeder, S. & Narayanan, A. (2016). Threshold-Optimal DSA/ECDSA Signatures and an Application to Bitcoin Wallet Security. In M. Manulis, A. Sadeghi & S. Schneider (Hrsg.), *Applied Cryptography and Network Security* (S. 156-174). Cham: Springer.

Huckle, S., Bhattacharya, R., White, M. & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, 98, 461-466. http://dx.doi.org/10.1016/j.procs.2016.09.074

Katz, J. (2010). *Digital Signatures*. https://doi.org/10.1007/978-0-387-27712-7

Kewell, B., Adams, R. & Parry, G. (2017). Blockchain for good?*. *Strategic Change*, 26(5), 429-437. https://doi.org/10.1002/jsc.2143

Krombholz, K., Judmayer, A., Gusenbauer, M. & Weippl, E. (2016). The other side of the coin: User experiences with Bitcoin security and privacy. In J. Grossklags & B. Preneel (Hrsg.), *Financial Cryptography and Data Security* (S. 555-580). Berlin: Springer.

Kshetri, N. (2017a). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Kshetri, N. (2017b). Can Blockchain Strengthen the Internet of Things? *IT Professional*, 19(4), 68-72. doi: 10.1109/MITP.2017.3051335

Kuo, T. T., Kim, H. E. & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211-1220. doi: 10.1093/jamia/ocx068

Laurence, T. (2017). *Blockchain for dummies*. Hoboken, NJ: John Wiley & Sons.

Li, S., Xu, L. D. & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, 17(2), 243-259. https://doi.org/10.1007/s10796-014-9492-7

Mainelli, M. & Smith, M. (2015). Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology). *Journal of Financial Perspectives*, 3(3), 1-47.

Mandl, K. D., Szolovits, P. & Kohane, I. (2001). Public standards and patients' control: how to keep electronic medical records accessible but private. *The BMJ*, 322, 283-287. https://doi.org/10.1136/bmj.322.7281.283

Meinel, C., Gayvoronskaya, T. & Schnjakin, M. (2018). *Blockchain: Hype oder Innovation* (113. Aufl.). Potsdam: Universitätsverlag Potsdam.

Meitinger, T. H. (2017). Smart Contracts. *Informatik-Spektrum*, 40(4), 371-375. https://doi.org/10.1007/s00287-017-1045-2

Morabito, V. (2017). *Business Innovation through Blockchain – The B3 Perspective*. doi: 10.1007/978-3-319-48478-5

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Abgerufen von https://bitcoin.org/bitcoin.pdf

Nofer, M., Gomber, P., Hinz, O. & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, 59(3), 183-187. doi:10.1007/s12599-017-0467-3

Ojo, A. & Abebayo, S. (2017). Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries. In A. Ojo & J. Millard (Hrsg.), *Government 3.0 – Next Generation Government Technology Infrastructure and Services* (S. 283-298). Cham: Springer.

Ølnes, S., Ubacht, J. & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3), 355-364. https://doi.org/10.1016/j.giq.2017.09.007

Pazaitis, A., De Filippi, P. & Kostakis, V. (2017). Blockchain and value systems in the sharing economy: The illustrative case of Backfeed. *Technological Forecasting & Social Change*, 125, 105-115. https://doi.org/10.1016/j.techfore.2017.05.025

Riso, B., Tupasela, A., Vears, D. F., Felzmann, H., Cockbain, J., Loi, M., Kongsholm, N. C. H., Zullo, S. & Rakic, V. (2017). Ethical sharing of health data in online platforms – which values should be considered? *Life Science, Society and Policy*, 13(12), 1-27. https://doi.org/10.1186/s40504-017-0060-z

Schumacher, A. (2017). *Blockchain & Healthcare – 2017 Strategy Guide*. doi: 10.13140/RG.2.2.12162.48327

Swan, M. (2015). *Blockchain – Blueprint for a new economy.* Sebastopol, CA: O'Reilly Media.

Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1-25. http://dx.doi.org/10.5210/fm.v2i9.548

Tapscott, D. & Tapscott, A. (2016). *Die Blockchain Revolution* (3. Aufl.). Kulmbach: Börsen Medien.

Tosovic, V. (2016). Der DAO-Hack – und die Konsequenzen für die Blockchain. In D. Burgwinkel (Hrsg.), *Blockchain Technology – Einführung für Business- und IT Manager* (S. 159-165). Berlin & Boston: Walter de Gruyter.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current Opinion in Environmental Sustainability*, 28, 1-9. https://doi.org/10.1016/j.cosust.2017.04.011

Vukolic, M. (2016). The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In J. Camenisch & D. Kesdogan (Hrsg.), *Open Problems in Network Security* (S. 112-125). Cham: Springer.

Wright, A. & De Filippi, P. (2015*). Decentralized blockchain technology and the rise of lex cryptographia.* (SSRN Working Paper 2580664). Abgerufen von der SSRN Webseite: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. (2016). *Blockchain Challenges and Opportunities: A Survey*. (International Journal of Web and Grid Services Working Paper). Abgerufen von der ResearchGate Webseite: https://www.researchgate.net/publication/319058582_Blockchain_Challenges_and_Opportunities_A_Survey

Zohar, A. (2015). Bitcoin: Under the Hood. *Communications of the ACM*, 58(9), 104-113. doi: 10.1145/2701411