FERDINAND PORSCHE
FERNFH

Einsatzmöglichkeiten der Blockchain-Technologie an der Ferdinand Porsche FernFH

Bachelorarbeit

eingereicht von: **Jürgen WIELÄNDNER**
Matrikelnummer: 51807282

im Fachhochschul-Bachelorstudiengang Wirtschaftsinformatik (0470)
der Ferdinand Porsche FernFH

zur Erlangung des akademischen Grades eines

Bachelor of Arts in Business

Betreuung und Beurteilung: Prof. (FH) DI Dr. Martin STAUDINGER

Wiener Neustadt, Juni 2024

Ehrenwörtliche Erklärung

Ich versichere hiermit,

1. dass ich die vorliegende Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle Inhalte, die direkt oder indirekt aus fremden Quellen entnommen sind, sind durch entsprechende Quellenangaben gekennzeichnet.
2. dass ich diese Bachelorarbeit bisher weder im Inland noch im Ausland in irgendeiner Form als Prüfungsarbeit zur Beurteilung vorgelegt oder veröffentlicht habe.

Batschuns, 06.06.2024

Unterschrift

Die Kapitel 2 bis 5 der vorliegenden Bachelorarbeit wurden im Rahmen der Lehrveranstaltung „Bachelor Seminar 1“ eingereicht und am 23.05.2024 als Bachelorarbeit 1 angenommen.

Kurzzusammenfassung: Einsatzmöglichkeiten der Blockchain-Technologie an der Ferdinand Porsche FernFH

Im Rahmen dieser Arbeit wird die Einführung der Blockchain-Technologie an der Ferdinand Porsche FernFH (FERNFH) hinsichtlich technischer, organisatorischer und rechtlicher Aspekte auf ihre Machbarkeit überprüft. Zunächst werden durch eine umfassende Literaturrecherche die Grundlagen der Blockchain-Technologie erläutert und mögliche Problemfelder identifiziert. Aufbauend auf diesen Erkenntnissen und einem ausführlichen Gespräch mit der IT-Leitung der FERNFH wird eine detaillierte Machbarkeitsanalyse für den spezifischen Anwendungsfall „Blockchain-basiertes Zeugnis an der FERNFH“ durchgeführt. Die Analyse der technischen Infrastruktur zeigt, dass die bestehenden Systeme der FERNFH in der Lage sind, die Anforderungen der Blockchain-Technologie zu erfüllen. Organisatorisch werden Schulungsprogramme als notwendig erachtet, um die Akzeptanz und erfolgreiche Implementierung der neuen Technologie sicherzustellen. Rechtlich wird die Einhaltung der Datenschutz-Grundverordnung (DSGVO) durch geeignete Maßnahmen wie Anonymisierung und Pseudonymisierung gewährleistet. Die Ergebnisse der Machbarkeitsanalyse zeigen, dass die FERNFH gut positioniert ist, diese innovative Technologie zu implementieren und somit die Authentizität und Integrität digitaler Zeugnisse zu gewährleisten. Die Zusammenarbeit mit anderen Hochschulen könnte das volle Potenzial dieser Technologie im Bildungssektor ausschöpfen und ihre Akzeptanz weiter fördern. Diese Kooperation würde nicht nur die Interoperabilität und Datensicherheit erhöhen, sondern auch den gemeinsamen Nutzen maximieren.

Schlagwörter:

Blockchain, Bildung, Ferdinand Porsche FERNFH, Zeugnis, Machbarkeitsanalyse

Abstract: Applications of blockchain technology at Ferdinand Porsche FernFH

As part of this study, the feasibility of implementing blockchain technology at the Ferdinand Porsche FernFH (FERNFH) is examined from technical, organizational, and legal perspectives. Initially, the fundamentals of blockchain technology are explained, and potential problem areas are identified through comprehensive literature research. Building on these insights and an in-depth discussion with the IT management of FERNFH, a detailed feasibility analysis is conducted for the specific use case of "blockchain-based certificates at FERNFH." The analysis of the technical infrastructure reveals that FERNFH's existing systems can meet the requirements of blockchain technology. Organizationally, training programs are deemed necessary to ensure the acceptance and successful implementation of the new technology. Legally, compliance with the General Data Protection Regulation (GDPR) is ensured through measures such as anonymization and pseudonymization. The results of the feasibility analysis indicate that FERNFH is well-positioned to implement this innovative technology, thereby ensuring the authenticity and integrity of digital certificates. Collaboration with other universities could fully exploit the potential of this technology in the education sector and further enhance its acceptance. This cooperation would not only increase interoperability and data security but also maximize the mutual benefits.

Keywords:

Blockchain, Education, Ferdinand Porsche FERNFH, Certificate, Feasibility Analysis

Inhaltsverzeichnis

1. Einleitung

1.1 Kurzportrait der Ferdinand Porsche FERNFH

Die Ferdinand Porsche FERNFH wurde im Jahr 2006 durch die Humboldt Bildungsgesellschaft m.b.H. und die Fachhochschule Wiener Neustadt für Wirtschaft und Technik GmbH gegründet. Ihr offizieller Studienbetrieb begann im Jahr 2007 mit dem ersten Bachelorstudiengang "Wirtschaftsinformatik". Seitdem hat sich die FERNFH als Vorreiterin im Bereich des Distance-Learnings in Österreich etabliert. Sie ist spezialisiert auf akademische Online-Lehre, Fernstudium und Blended-Learning und nimmt eine Vorreiterrolle in diesem Bereich ein.[1]

Im Zeitraum vom 1. April 2015 bis zum 1. Oktober 2016 erwarb die Fachhochschule Wiener Neustadt die Eigentümerschaft an der FERNFH. Danach wurde die FERNFH Management & Service GmbH gegründet, die die FERNFH von der Fachhochschule Wiener Neustadt übernommen hat. Im Jahr 2020 beteiligte sich auch das Land Niederösterreich mit einem Anteil von 26%. In den Jahren seit der Gründung expandierte die FERNFH in Österreich durch die Eröffnung eines weiteren Studienzentrums in Wien sowie eines neuen Campus in Wiener Neustadt und nahm weitere Bachelor- und Masterstudiengänge in das Studienangebot auf. Seit ihrer Gründung hat die FERNFH zahlreiche Auszeichnungen, Zertifizierungen und Preise erhalten, darunter den Titel "Familienfreundlichster Betrieb NÖ 2017", das "Staatliche Gütezeichen für familienbewusste Studien- und Arbeitsbedingungen" und den 3. Platz beim Staatspreis für "Familie & Beruf", um nur einige zu nennen.[2]

In Tabelle 1 werden die Daten und Fakten über Studierendenzahlen an der FERNFH übersichtlich dargestellt:

[1] Vgl. Ferdinand Porsche FERNFH, 2023a

[2] Vgl. Ferdinand Porsche FERNFH, 2023b

Studiengänge	Betriebswirtschaft & Wirtschaftspsychologie		Wirtschafts-informatik		Aging Services Management		Gesamt
	Bachelor	Master	Bachelor	Master	Bachelor	Master	
Studierende	193	82	257	112	102		746
Absolvent*innen	750	403	611	286	166		2.216

Lehrgänge	Gesamt
Studierende	10
Absolvent*innen	89
Studierende gesamt	**1.003**
Absolvent*innen gesamt	**2.305**

Tabelle 1: Daten und Fakten zur FERNFH (Stand: November 2023)[3]

1.2 Ausgangslage und Problemstellung

Unter dem Begriff „Blockchain“ wird in der Informatik eine bestimmte Art und Weise der Strukturierung und Weitergabe von Daten verstanden.[4] Der anhaltende Hype um Kryptowährungen hat in den letzten Jahren zunehmend das Interesse an der zugrunde liegenden Blockchain-Technologie geweckt. Diese Technologie wird als Teil der „Distributed Ledger Technologie“ (DLT, dt. „Verteilte Datenbank-Technologie“) bezeichnet. Der Grundgedanke der DLT ist eine sichere Datentransaktion zwischen zwei Parteien zu ermöglichen, ohne auf einen vertrauenswürdigen Intermediären (Vermittler*in) angewiesen zu sein, indem Daten unveränderbar gespeichert werden.

Diese grundlegende Funktionalität eröffnet völlig neue Möglichkeiten im Umgang mit Daten und Transaktionen im Internet, sowie im Geschäftsumfeld verschiedener Geschäftsbereiche. Dazu zählen beispielsweise Branchen, wie die Finanz- und Immobilienindustrie, öffentliche Verwaltung, sowie das Bildungswesen.

In den vergangenen Jahren wurde vermehrt in verschiedenen Medien darüber berichtet, dass Zeugnisse, Prüfungsergebnisse und Lerninhalte künftig digital mithilfe der Blockchain zugänglich gemacht werden sollen. Meike Laaff von "Zeit Online" berichtet über die Bemühungen der Bundesdruckerei in Deutschland, Zeugnisse mithilfe der Blockchain zu digitalisieren. In ihrem Bericht erläutert sie nicht nur die praktischen

[3] Vgl. Ferdinand Porsche FERNFH, Ferdinand Porsche FERNFH - Österreichs führende Distance-Learning-Hochschule, 2023b

[4] Vgl. Laurence, 2017, S. 23

Vorteile dieser Initiative, sondern weist auch auf die damit verbundenen Herausforderungen hin.[5] Ein Artikel im "Journal of Teacher Education for Sustainability" von Merija Jirgensons und Jānis Kapenieks gibt Einblicke in die Vorteile des Einsatzes der Blockchain im Bildungssektor und zeigt experimentelle Anwendungsfälle, die bereits von verschiedenen höheren Schulen erforscht werden.[6]

Bestimmte Abläufe in Bildungseinrichtungen, wie der Ferdinand Porsche FernFH, erfordern nach wie vor einen erheblichen administrativen Aufwand im Zusammenhang mit der Verwaltung von Prüfungsergebnissen und der Ausstellung von Zeugnissen und Bestätigungen. Diese Prozesse basieren größtenteils auf zentralen Datenbanksystemen, die einen hohen Aufwand und Kosten erfordern, um Manipulationen zu verhindern. Aktuell werden an der FERNFH Zeugnisse klassisch in Form von Papier als Ausdruck und zusätzlich als PDF-Datei ausgestellt. Diese PDF-Datei wird mittels elektronischer Unterschrift digital signiert. Somit wird zwar eine Validierung des Dokuments auf Echtheit ermöglicht, allerdings besteht eine Abhängigkeit zum Aussteller des Zertifikats. Sollte dieser aus irgendwelchen Gründen nicht mehr zur Verfügung stehen, besteht die Möglichkeit eines Vertrauensverlustes in die Gültigkeit und Authentizität des Zertifikats. Folge dessen wird eine Überprüfung der PDF-Datei auf Echtheit schwierig bis unmöglich.

1.3 Motivation und Ziel der Arbeit

Seit dem Hype um Kryptowährungen im Jahr 2017 beschäftige ich mich mit der zugrundeliegenden Blockchain-Technologie und ihren Potenzialen im alltäglichen Leben und der Wirtschaft. Die Distributed Ledger Technology (DLT) im Kontext von Kryptowährungen verdeutlicht, wie Daten manipulationssicher gespeichert und Transaktionen ohne vertrauenswürdige Intermediäre nachvollziehbar durchgeführt werden können. Dies löst ein zentrales Problem im Internet: den sicheren Austausch von Daten und Werten zwischen zwei Parteien, ohne auf Vermittler*innen wie eine Bank angewiesen zu sein. Viele Expert*innen betrachten diesen Fortschritt als bahnbrechend, und ich schließe mich dieser Einschätzung an. Die Vielfalt der Anwendungsmöglichkeiten in unterschiedlichen Geschäftsbereichen wie dem Finanzsektor, der Immobilienbranche oder der Logistik begeistert mich nach wie vor.

Von Anfang an haben mich die ersten Projekte zur Anwendung der Blockchain-Technologie im Bildungsbereich fasziniert. Als Student an der Ferdinand Porsche FernFH (FERNFH) interessiere ich mich besonders für den Einsatz der Blockchain-Technologie für einen spezifischen Anwendungsfall. Konkret geht es um die Online-

[5] Vgl. Laaff, 2022

[6] Jirgensons & Kapenieks, 2018

Verfügbarkeit von Zeugnissen, deren Echtheit problemlos überprüft werden kann. Durch die Implementierung dieser Lösung könnten potenzielle Arbeitgeber*innen die Richtigkeit und Authentizität der Abschlusszeugnisse von Bewerber*innen ohne die Einbindung der FERNFH-Verwaltung überprüfen, was Kosten und Aufwand reduzieren würde.

Derzeit werden digitale Zeugnisse mit einer digitalen Signatur ausgestellt, die jedoch einen Intermediär (CA - Certificate Authority) erfordert, um die Echtheit eines öffentlichen Schlüssels zu gewährleisten. Wenn eine CA kompromittiert wird, könnten die vorhandenen Schlüssel nicht mehr verwendet werden. Ein weiteres Risiko stellen zentrale IT-Systeme dar, die zwar aufwendig abgesichert werden müssen, aber dennoch einen Single-Point-of-Failure darstellen. Die Vergangenheit hat gezeigt, dass selbst sorgfältig abgesicherte IT-Systeme großer Unternehmen und öffentlicher Institutionen böswillig gehackt wurden, wie zum Beispiel die „Frankfurter Uniklinik", „Südwestfalen-IT", deutsche Flughäfen und Ziele im Finanzsektor.[7] Durch die Nutzung der Blockchain-Technologie könnten technische Schwachstellen minimiert oder sogar beseitigt werden. Es ist jedoch zu beachten, dass bestimmte technische Voraussetzungen für die Einführung der Blockchain-Technologie erforderlich sind, was mit entsprechenden Kosten für Hardware, Software und Schulungen des vorhandenen Personals oder der Einbeziehung von Fachpersonal verbunden ist. Schließlich müssen auch rechtliche Rahmenbedingungen erfüllt und eingehalten werden. Dies kann die Einhaltung der Datenschutzgrundverordnung (DSGVO) für die Speicherung personenbezogener Daten, sowie die Berücksichtigung von Anforderungen des Studienrechts umfassen.

Das Ziel dieser Arbeit besteht darin, die Machbarkeit der Implementierung eines spezifischen Anwendungsfalles an der FERNFH zu untersuchen: die Ausstellung digitaler Zeugnisse mithilfe von Blockchain-Technologie. Die Machbarkeit wird auf technische, organisatorische und rechtliche Aspekte hin untersucht.

1.3.1 Forschungsfrage

Ist die Ausstellung von Blockchain basierten Zeugnissen an der Ferdinand Porsche FernFH in Bezug auf technische, organisatorische und rechtliche Aspekte machbar?

1.3.2 Hypothese

Die Ausstellung von Blockchain basierten Zeugnissen an der Ferdinand Porsche FernFH ist in Bezug auf technische, organisatorische und rechtliche Aspekte machbar.

[7] Vgl. Müller, 2024

1.4 Abgrenzung des Themenbereichs

Die Arbeit fokussiert sich auf eine spezifisches Anwendungsszenario an der FERNFH, die auf Blockchain-Technologie basiert. Dabei wird der Begriff „Blockchain“ genauer erklärt und die verschiedenen Typen und deren Funktionsweise näher erläutert. Es wird bewusst auf eine detaillierte Behandlung der technischen Aspekte, wie den Aufbau der Blockchain (Blöcke, Konsensmechanismus, etc.), oder andere Technologien, wie beispielsweise der Tangle-Technologie von IOTA, verzichtet.

1.5 Methodisches Vorgehen

Um die vorangegangene Forschungsfrage beantworten zu können, werden unter Berücksichtigung relevanter Literatur die grundlegenden Prinzipien der Blockchain-Technologie dargestellt und erläutert. Die Anwendbarkeit dieser Technologie an der Ferdinand Porsche FernFH wird im Rahmen einer Machbarkeitsstudie anhand eines spezifischen Anwendungsfalles eingehend untersucht. Dabei orientiert sich die Untersuchung an aktuellen Initiativen von Hochschulen im Bereich Blockchain und dem "Digitalen Zeugnis" der Bundesdruckerei Deutschland. Basierend auf sämtlichen Ergebnissen erfolgt eine kritische Bewertung des Potenzials und der Herausforderungen des Blockchain-Einsatzes unter Berücksichtigung technischer, organisatorischer und rechtlicher Aspekte.

1.6 Aufbau der Arbeit

Kapitel 1 stellt die Ferdinand Porsche FERNFH in einem Kurzportrait vor und führt Leser*innen in die Ausgangslage und Problemstellung, sowie Motivation und Ziel der Arbeit ein. Daraus werden die Forschungsfrage und Hypothese abgeleitet. Es erfolgt eine Abgrenzung des Themenbereichs und eine Erläuterung des methodischen Vorgehens. Abschließend wird der Aufbau der Arbeit skizziert, um den Leser*innen einen Überblick zu verschaffen.

Kapitel 2 erläutert die Grundlagen der Blockchain-Technologie, um den Leser*innen ein fundiertes Verständnis für die nachfolgenden Themengebiete zu vermitteln. Hierbei werden relevante Begriffe erklärt und die grundlegenden Eigenschaften der Blockchain näher beleuchtet. Das Kapitel schließt mit einer Beschreibung über die Stärken und Schwächen der Blockchain-Technologie sowie deren Bedeutung für die Beantwortung der Forschungsfrage.

Kapitel 3 vertieft das Verständnis der verschiedenen Typen von Blockchains und ihrer Funktionsweise. Dabei liegt ein besonderes Augenmerk auf den angewandten kryptografischen Verfahren und dem Konsensmechanismus. Durch die Zusammenführung der einzelnen Komponenten entsteht ein Gesamtbild des Blockchain-Prozesses.

Kapitel 4 widmet sich den Aspekten, die vor der Einführung der Blockchain-Technologie im Bildungssektor zu berücksichtigen sind. Hierbei werden technische, organisatorische und rechtliche Gesichtspunkte beleuchtet, um eine fundierte Entscheidungsgrundlage zu schaffen.

Kapitel 5 beschreibt bedeutende Projekte, bei denen die Blockchain-Technologie zum Einsatz kommt. Dabei werden wichtige Erkenntnisse gewonnen, die für die potenzielle Einführung der Blockchain-Technologie bei der FERNFH von Relevanz sein könnten.

Kapitel 6 widmet sich der Machbarkeit der Einführung von Blockchain basierter Zeugnisse an der FERNFH. Die durchgeführte Machbarkeitsanalyse orientiert sich dabei an den dafür notwendigen Prozessschritten und beleuchtet diese aus technischer, organisatorischer und rechtlicher Sicht.

Kapitel 7 fasst die gewonnen Ergebnisse aus der Machbarkeitsanalyse zusammen, beantwortet die Forschungsfrage und gibt einen Ausblick auf das zukünftige Potential es Einsatzes von Blockchain-Technologie im Bildungssektor.

2. Grundlagen der Blockchain-Technologie

In der Informatik wurde der Begriff Blockchain ursprünglich für eine bestimmte Art der Strukturierung und Weitergabe von Daten verwendet. Weltweit werden viele verschiedene Arten von Blockchains eingesetzt.[8] Einer der bekanntesten Anwendungsfälle wird durch das Zahlungsmittel „Bitcoin“ vertreten, welcher in den letzten Jahren einen gewissen Hype erlebte. Im Jahr 2008 publizierte ein Autor unter dem Pseudonym „Satoshi Nakamoto“ ein Whitepaper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“[9], in welchem auf weniger als zehn Seiten die Funktionsweise des digitalen Zahlungsmittels „Bitcoin“ beschrieben wurden. Nakamoto entwickelte ein Zahlungssystem, welches völlig unabhängig von zentralen Instanzen für die Geldausgabe, Abrechnung und Validierung von Transaktionen war und auf der Blockchain basierte[10]. Anhand von objektiven Statistiken auf Google oder subjektiven Ansichten von Menschen lässt sich feststellen, dass Bitcoin wesentlich bekannter ist als die Blockchain selbst. Die Leute reden offensichtlich lieber über Dinge, die sie verstehen, anfassen oder kaufen können.[11] Diverse Pressemitteilungen unterstützen Bitcoin dabei, seinen Bekanntheitsgrad entsprechend zu erhöhen. Beispielsweise von einem Briten, der seine Festplatte auf einer Müllkippe sucht, die Bitcoins mit einem Gegenwert von mehreren hundert Millionen Euros gespeichert hat.[12] Heute gibt es weitaus mehr Anwendungsfälle für die Blockchain. Genauer wird in den folgenden Kapiteln darauf eingegangen.

Das Hauptmerkmal von Blockchains ist die Speicherung von Daten bzw. Datenstrukturen aus verschiedenen Blöcken auf unveränderbare und manipulationssichere Art und Weise.[13] Die Blockchain-Technologie wird im Gabler Wirtschaftslexikon als „dezentrale, chronologisch aktualisierte Datenbank mit einem aus dem Netzwerk hergestellten Konsensmechanismus zur dauerhaften digitalen Verbriefung von Eigentumsrechten“[14] erläutert.

---

[8] Vgl. Laurence, 2017, S. 23

[9] Vgl. Nakamoto, 2008

[10] Vgl. Antonopoulos, 2018, S. 4

[11] Vgl. Hosp, 2018, S. 32

[12] Vgl. Bild.de, 2017

[13] Vgl. Wittenberg, 2020, S. 18

[14] Mitschele, 2018

2.1 Definition und Terminologie

Für ein besseres Verständnis des Sachverhalts in den folgenden Abschnitten, werden in diesem Kapitel einige wichtige Begriffe beschrieben, die im Kontext der Blockchain gerne verwendet werden. Manche dieser Begriffe werden in nachfolgenden Kapiteln nochmals aufgegriffen und genauer erläutert.

DLT

Da die Regeln zur Aktualisierung, sowie die Lese- und Schreibrechte der Daten durch Software-Code geregelt sind, wird bei der Blockchain-Technologie auch häufig von einer Distributed-Ledger-Technologie (DLT) gesprochen.[15] Die beiden Begriffe werden oftmals synonym verwendet. Wesentlich bei einer DLT ist die Art der Datenverarbeitung und -speicherung auf einer dezentralen Datenbank, auf der die Teilnehmer*innen des Netzwerks gemeinsame Schreib- und Leseberechtigungen haben. Es bedarf keiner zentralen Instanz, die die Datenbank kontrolliert und steuert.[16]

Knoten (Node)

Ein Knoten beschreibt einen Computer in einem Netzwerk, der bestimmten Regeln folgt und Informationen mit anderen Teilnehmer*innen im Netzwerk teilt.[17]

Distributed Ledger

Im Kontext der Blockchain-Technologie ist der Ledger analog mit einem verteilten Kassenbuch zu vergleichen. Dieses Kassenbuch ist redundant auf allen Nodes gespeichert.[18] Man spricht auch von einem Register mit Transaktionen, die über viele Nodes gespeichert sind.[19]

Blockchain

Eine Blockchain ist eine Datenstruktur, die es ermöglicht, ein verteiltes Kontenbuch (Ledger) mit Datenbeständen redundant in einem dezentralen Netzwerk auf vielen Knotenpunkten zu speichern und zu teilen.[20] Sie wird auch als technisches Konzept beschrieben, welches einzelne Transaktionen zu Blöcken zusammenfasst und mittels kryptografischer Verfahren die Integrität der Daten sicherstellt.[21]

---

[15] Vgl. Wittenberg, 2020, S. 19

[16] Vgl. Metzger, 2018

[17] Vgl. Bitpanda, 2024

[18] Vgl. Wittenberg, 2020, S. 19

[19] Vgl. Kirstein, Lämmel, & Altenbernd, 2021, S. 8

[20] Vgl. Laurence, 2017, S. 23

[21] Vgl. Burgwinkel, 2016, S. 5

Chain

Die Blöcke einer Blockchain werden mittels Hash-Schlüssel, welche mathematisch berechnet werden, verkettet.[22] Ein vereinfachtes Prinzip wird in „Abbildung 1: Blockchain Prinzip - vereinfacht“ veranschaulicht.

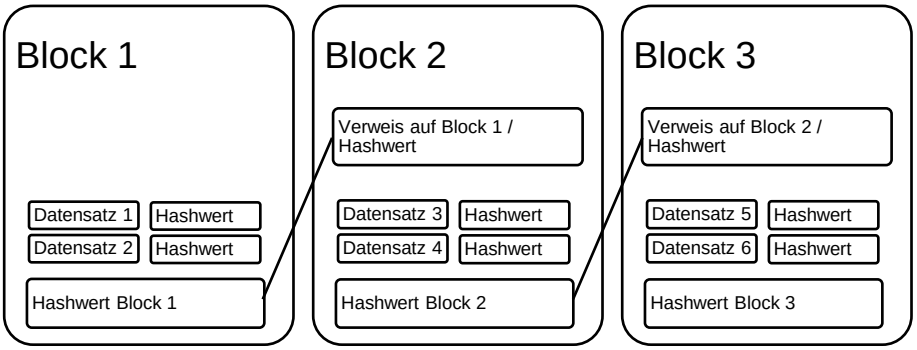

Abbildung 1: Blockchain Prinzip - vereinfacht[23]

Für jeden Datensatz innerhalb eines Blocks (Datensatz 1, Datensatz 2, …) wird ein individueller Hashwert erzeugt. Alle diese Hashwerte dienen wiederum als Grundlage für den Hashwert des Blocks (Block 1). Der Hashwert des Blocks (Block 1) wird wiederum als Referenz im nachfolgenden Block (Block 2) gespeichert, wodurch eine fortlaufende Kette, die sogenannte „Chain“, entsteht. Dieses Prinzip gewährleistet die Fortsetzung der Datenkette mit jedem weiteren Block, sowie auch dessen Integrität. Es bildet die Grundlage für die Unveränderlichkeit der Informationen in der Blockchain und der Dezentralisierung.

Transaktion

Eine Transaktion ist die Übertragung von Daten, signiert mit einem eigenen privaten Schlüssel. Anhand der Signatur wird sichergestellt, dass die Nachricht nicht verändert wurde.[24] Transaktionen werden in Blöcken zusammengefasst.

Block

Ein Block in einer Blockchain beinhaltet Transaktionen, die in einem bestimmten Zeitraum getätigt wurden.[25] Die einzelnen Blöcke werden mittels Hash-Schlüssel miteinander verkettet.

---

[22] Vgl. Laurence, 2017, S. 26

[23] Vgl. Burgwinkel, 2016, S. 6

[24] Vgl. Wittenberg, 2020, S. 33

[25] Vgl. Laurence, 2017, S. 26

2.2 Distributed Ledger Technologie (DLT)

Der Begriff „Blockchain“ wird oftmals mit der Distributed Ledger Technologie (DLT) synonym verwendet, obwohl für den Betrieb eines Distributed Ledger die Blockchain nicht zwingend eine Voraussetzung ist.[26] Da bei der Blockchain-Technologie dennoch alle Transaktionsinformationen im Netzwerk verteilt auf Nodes (Peer-to-Peer System) gespeichert werden, wird ebenfalls von einer DLT gesprochen.[27] Die DLT ist mit einer Buchhaltung vergleichbar, in der ein Hauptbuch (Ledger) existiert und auf verteilten Nodes gespeichert wird. Transaktionen werden, nicht wie in einer herkömmlichen Datenbank gespeichert, sondern sequenziell zu Datenblöcken zusammengefasst, durch ein kryptografisches Verfahren miteinander verknüpft und in das verteilte Hauptbuch eingetragen.

Der Vorteil besteht darin, dass eine öffentliche, nachvollziehbare und transparente Übertragung zwischen unbekannten Parteien möglich wird, ohne dass dafür eine vertrauenswürdige zentrale Instanz (Intermediär) erforderlich ist.[28] Das Risiko einer Datenmanipulation oder der Zusammenbruch des Systems wird reduziert, da alle im Netzwerk vorhandenen Nodes im Besitz der Transaktionsinformationen sind.[29]

2.3 Eigenschaften der Blockchain

Eine Blockchain zeichnet sich im Wesentlichen durch mehrere Eigenschaften aus:

2.3.1 Dezentral und belastbar

Es handelt sich um ein dezentral organisiertes Netzwerk, bei dem es keinen Intermediären benötigt, stattdessen sind alle Knoten in ihrer Funktion gleichberechtigt. Es kann jederzeit ein neuer Knoten dem Netzwerk beitreten oder es verlassen. Mit der Anzahl der Knoten steigt die Sicherheit des Netzwerks, wodurch es weitgehend vor Eingriffen eines einzelnen Individuums, aber auch vor politischen und organisatorischen Angriffen geschützt ist.[30]

2.3.2 Verifizierbar und transparent

Sämtliche Transaktionsinformationen sind auf jeder Node gespeichert. Das bedeutet, dass für alle Teilnehmer*innen ein Zugriff auf sämtliche Transaktionen ermöglicht wird.

---

[26] Vgl. Mitschele, 2018

[27] Vgl. Olnes, Ubacht, & Janssen, 2017, S. 355

[28] Vgl. Schacht & Lanquillon, 2019

[29] Vgl. Olnes, Ubacht, & Janssen, 2017, S. 355

[30] Vgl. Schacht & Lanquillon, 2019, S. 5

Mittels verschiedener Algorithmen, den sogenannten Konsens-Algorithmen, werden Transaktionen von freiwilligen, und sich immer wieder wechselnden Knoten verifiziert. Einer der bekanntesten Konsens-Algorithmen ist als „Proof-of-Work“ bekannt und arbeitet auf Basis von Rechenleistung. Der Zugriff aller Netzwerkteilnehmer*innen auf die Transaktionen und der Konsensmechanismus sind die Basis für eine hohe Belastbarkeit und Nachvollziehbarkeit der Daten.[31]

2.3.3 Unveränderlich

Alle Daten und Transaktionen in der Blockchain sind aufgrund ihres Designs unveränderlich. Jede Transaktion wird in einem Block gespeichert und durch ein kryptografisches Hash-Verfahren mit dem nachfolgenden Block verknüpft. Diese verbundenen Blöcke werden wiederum auf alle Teilnehmer*innen des Netzwerks dezentral gespeichert. Sollte sich eine Transaktion auf einem Knoten verändern, bedeutet dies eine Verletzung der Datenkonsistenz auf diesem einen Knoten, da die berechneten Hashwerte der Blöcke nicht mehr mit den Kopien auf allen anderen Teilnehmern übereinstimmen würde. Die manipulierte Transaktion würde als ungültig angesehen werden und als Konsequenz wäre ein Ausschluss des Knotens aus dem Netzwerk. „Unveränderlichkeit“ bedeutet im Kontext der Blockchain nicht, dass überhaupt keine Daten geändert werden können, sondern lediglich manipulierte Änderungen erkannt und aus dem Netzwerk entfernt werden.[32]

Es wäre falsch zu glauben, dass es sich bei der Blockchain um eine einzelne Datenstruktur handelt. Tatsächlich gibt es diverse Abwandlungen der von Nakamoto beschriebenen Blockchain, die sich in Zweck, Größe und Funktionsweise unterscheiden können.

Die meisten Blockchains haben dennoch folgende Gemeinsamkeiten:[33]

2.3.4 Verteilt

Die Blockchain ist im Gegensatz zu einer herkömmlichen zentralen Datenbank auf vielen verschiedenen Knoten weltweit verteilt und daher nicht zentral organisiert.[34] In der Abbildung 2 werden die drei wichtigsten Netzwerkarchitekturen grafisch dargestellt:

---

[31] Vgl. Schacht & Lanquillon, 2019, S. 5

[32] Vgl. Schacht & Lanquillon, 2019, S. 6

[33] Vgl. Tapscott & Tapscott, 2016, S. 23-24

[34] Vgl. Tapscott & Tapscott, 2016, S. 24

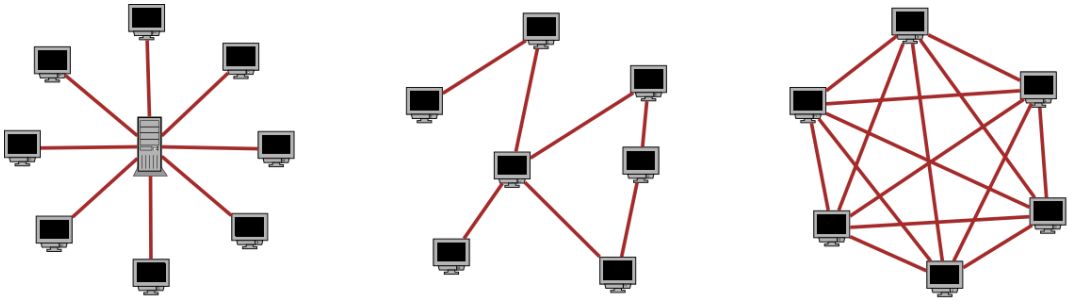

Abbildung 2: Netzwerkarchitekturen[35]

In **zentralisierten** Netzwerken sind die Netzwerkteilnehmer*innen nicht direkt untereinander vernetzt, sondern lediglich mit einer zentralen Instanz verbunden. Diese Netzwerkstruktur ist besonders für Kommunikationszwecke geeignet. Hierbei übernimmt die zentrale Instanz die Rolle, Regeln durchzusetzen und die Aktionen der einzelnen Teilnehmer zu koordinieren. Das Vertrauen der Teilnehmer*innen in die zentrale Instanz ist dabei essenziell. Wird dieses Vertrauen jedoch missbraucht, kann das gesamte System zusammenbrechen.[36] Im Gegensatz dazu müssen in **dezentralisierten** Netzwerken die Teilnehmer*innen selbst die Koordination übernehmen, um gemeinsam interagieren zu können. Ein wesentlicher Nachteil eines solchen Systems liegt darin, dass zwischen den Teilnehmer*innen kein vorab vorhandenes Vertrauen besteht, da sie einander nicht kennen. Aus diesem Grund ist es unabdingbar, ein solches System vor möglichen Manipulationen zu schützen. Bislang existiert noch keine etablierte Lösung für diese Herausforderungen. Dies erklärt auch, warum das heutige Internet größtenteils zentral organisiert ist. Die Blockchain-Technologie unterscheidet sich somit vom herkömmlichen Internet, da sie weder zentral noch dezentral organisiert ist, sondern auf einem **verteilten** Modell basiert. Sie setzt sich aus zahlreichen unabhängigen Teilnehmer*innen zusammen, die direkt miteinander kommunizieren können, ohne auf eine zentrale Instanz angewiesen zu sein. Die Datenintegrität wird durch redundantes Speichern auf jedem einzelnen Knotenpunkt (Node) sichergestellt. Ein Ausfall einer individuellen Teilnehmer*in beeinträchtigt das Netzwerk in keiner Weise.[37]

2.3.5 Öffentlich

Eine öffentliche Blockchain ist für alle zugänglich, da sie nicht Bestandteil einer Institution, sondern eines Netzwerks ist. Alle Transaktionen können jederzeit von

[35] Vgl. Bartek & Goudz, 2019, S. 39

[36] Vgl. Bartek & Goudz, 2019, S. 39-40

[37] Vgl. Bartek & Goudz, 2019, S. 40

Netzwerkteilnehmer*innen überprüft werden.[38] Es existieren noch weitere Arten der Blockchain, die in einem späteren Abschnitt näher beschrieben werden.

2.3.6 Verschlüsselt

Um virtuelle Sicherheit gewährleisten zu können, werden kryptographische Verschlüsselungsverfahren unter Verwendung von öffentlichen und privaten Schlüsseln eingesetzt. Dabei ist keine Netzwerk-Firewall oder eine ähnliche Maßnahme erforderlich.[39]

2.4 Stärken und Schwächen der Blockchain-Technologie

In den vorherigen Abschnitten wurden die verschiedenen Typen von Blockchains und ihre Funktionsweise näher erläutert. Auf dieser Grundlage werden in diesem Kapitel die Vor- und Nachteile skizziert. Mithilfe einer SWOT-Analyse werden die Stärken und Schwächen der Blockchain-Technologie laut Hosp[40] in sieben Kategorien eingeteilt. Diese Analyse bildet die Basis für verschiedene Anwendungsszenarien auf der Blockchain. Dabei fokussiert sich ein Anwendungsfall hauptsächlich auf eine der Stärken und zieht dabei auch andere Vorteile mit ein.[41]

2.4.1 Sieben Stärken

Unveränderbarkeit

In Abschnitt 2.3.2 17 wurde die Unveränderbarkeit der Blockchain bereits erläutert, wobei betont wurde, dass Unveränderbarkeit nicht bedeutet, dass Daten nicht geändert werden können, sondern vielmehr darauf hindeutet, dass manipulierte Änderungen erkannt und aus dem Netzwerk entfernt werden. Bei jeder Eintragung von Daten in die Blockchain entstehen Kosten aufgrund des Konsensmechanismus (PoW, PoS usw.). Eine nachträgliche Änderung bereits gespeicherter Daten würde erneut dieselben Kosten verursachen. Insbesondere bei älteren Daten müssten nicht nur der aktuelle Block mit den gespeicherten Informationen, sondern auch alle nachfolgenden Blöcke geändert werden. Diese Kosten würden schnell den eigentlichen Wert der zu ändernde Information übersteigen und machen daher aus wirtschaftlicher Sicht keinen Sinn. Infolgedessen gilt die Blockchain als unveränderbar, da eine Änderung von Informationen zu erheblichen wirtschaftlichen Verlusten führen würde. Auf der Bitcoin-

---

[38] Vgl. Tapscott & Tapscott, 2016, S. 24

[39] Vgl. Tapscott & Tapscott, 2016, S. 24

[40] Vgl. Hosp, 2018

[41] Vgl. Hosp, 2018, S. 70

Blockchain wurden bisher keine Änderungen vorgenommen, da dies unmittelbar zu Milliardenverlusten führen würde.[42]

Vertrauen und Integrität

Integrität ist ein nichtfunktionaler Aspekt eines Computer- oder Softwaresystems, das sich auf seine Einheitlichkeit, Korrektheit, Vollständigkeit und Fehlerfreiheit bezieht. Im Kontext von Vertrauen im Computer- und Softwareumfeld handelt es sich um die menschliche Überzeugung in die Zuverlässigkeit eines Systems, ohne notwendigerweise über Beweise oder eine umfassende Untersuchung zu verfügen. Vertrauen wird oft im Voraus gewährt und spielt eine entscheidende Rolle dabei, dass Menschen an Interaktionen im Netzwerk, insbesondere in Bezug auf die Blockchain, teilnehmen. Die Integrität ist entscheidend, um das gewährte Vertrauen zu rechtfertigen.[43] In der Geschäftswelt bedeutet Vertrauen, dass alle Beteiligten sich an grundlegende Prinzipien der Integrität halten: Transparenz, Gegenleistung, Ehrlichkeit und Rechenschaftspflicht.[44] Ein herausragendes Beispiel für Vertrauen, das unabhängig von Kultur, Rasse, Religion und Geschichte besteht, ist die Mathematik. In der Welt der Berechnungen herrscht Einigkeit darüber, dass 1+1 gleich 2 ergibt. Die Mathematik stellt ein universelles Regelwerk dar, dem überall gleichermaßen vertraut wird. Dieses Vertrauen in die Mathematik und Kryptographie bildet den Grundstein für das Vertrauen in die Blockchain-Technologie.[45]

Transparenz

Sämtliche Transaktionsinformationen sind auf allen Nodes gespeichert. Das bedeutet, dass für einen Teilnehmerkreis ein Zugriff auf sämtliche Transaktionen ermöglicht wird (siehe Kapitel 2.3.2). Jeder Mensch kann sich selbst davon überzeugen, dass Behauptungen auch wahr sind.[46] Allerdings ist wichtig zu beachten, dass die Zugriffsart je nach Blockchain-Typ variieren kann. In nicht öffentlichen Blockchains gibt es Unterschiede zwischen Nodes und deren Zugriffsrechte.[47]

Privatsphäre

Die meisten Internetdienste erfordern die Erstellung eines Accounts, der durch E-Mail-Adresse und Handynummer verifiziert wird. Dies steht im Kontrast zur Blockchain, die auf Kryptografie basiert. Es genügt die Erstellung eines Private Keys ohne weitere

---

[42] Vgl. Hosp, 2018, S. 71

[43] Vgl. Drescher, 2017, S. 49-50

[44] Vgl. Tapscott & Tapscott, 2016, S. 28

[45] Vgl. Hosp, 2018, S. 72

[46] Vgl. Hosp, 2018, S. 73

[47] Vgl. Espich, 2019, S. 57

Verifizierung. In einer Blockchain kann daher anonym teilgenommen werden, da niemand weiß, wer oder was den Private Key besitzt. Obwohl Transaktionen auf öffentlichen Blockchains transparent sind, könnten Rückberechnungen gewisse Rückschlüsse auf die Identität der beteiligten Parteien ermöglichen. Aus diesem Grund gelten viele Blockchains als pseudoanonym. [48]

Kompatibilität

Viele Regierungen erforschen die Blockchain, um verschiedene Prozesse abzubilden, obwohl dies nicht unbedingt erforderlich ist. Der Hauptgrund liegt in der Interoperabilität zwischen verschiedenen Blockchains und der Möglichkeit des vertrauenslosen Datenaustauschs. Zum Beispiel könnte eine Blockchain für Immobilien automatisch eine Identitätsprüfung eines Individuums durchführen, indem sie mit einer Identitäts-Blockchain interagiert.[49]

Offenheit

Öffentliche Blockchains sind so gestaltet, dass sie allen offenstehen, unabhängig davon, ob es sich um Menschen oder Maschinen handelt. Dies steht im Gegensatz zu zentralisierten Diensten, die einem elitären Prinzip folgen. In diesen Hierarchien haben es diejenigen leichter, die weiter oben stehen, während diejenigen, die weiter unten stehen, erschwerten oder gar keinen Zugang haben. Die Blockchain hingegen macht keinerlei Unterschiede aufgrund von Rasse, Religion, Hautfarbe, Alter oder Geschlecht. Alle Teilnehmer*innen werden gleichberechtigt behandelt. Viele Initiativen nutzen diesen Vorteil und entwickeln Blockchain-Anwendungen für eine breite Nutzerschaft.[50]

Redundanz

Die Blockchain ist per Definition dezentral, was zu einer umfangreichen Redundanz von Daten führt. Es wäre theoretisch auch möglich, eine Datenredundanz mit herkömmlichen Systemen zu schaffen; dafür müssten die Daten jedoch weit genug verteilt sein. Eine hohe Datenredundanz bringt einerseits hohe Ineffizienz mit sich, andererseits wird es nahezu unmöglich, Daten zu zerstören. Aufgrund dieser Redundanz sind die Daten selbst vor praktisch jeder Naturkatastrophe geschützt.[51]

---

[48] Vgl. Hosp, 2018, S. 72

[49] Vgl. Hosp, 2018, S. 73

[50] Vgl. Hosp, 2018, S. 74

[51] Vgl. Hosp, 2018, S. 74

2.4.2 Sieben Schwächen

Wenn es darum geht, eine Herausforderung in Bezug auf die Blockchain-Technologie zu bewältigen, ist es unabdingbar, sich auch eingehend mit den Schwächen auseinanderzusetzen. Schließlich hat jede Medaille, wie allgemein bekannt, zwei Seiten.

Kosten

Die Kosten einer Blockchain können aufgrund diverser Faktoren entstehen. Hierbei handelt es sich nicht nur um direkte Transaktionsgebühren, sondern auch um Aufwendungen, die durch den gewählten Konsensmechanismus (PoW, PoS, etc.) bedingt sind.[52] Die Kosten im Zusammenhang mit der Umsetzung eines Blockchain-Projekts schließen den initialen Start, Forschung & Entwicklung, Implementierung sowie den laufenden Betrieb und schließlich die spätere Stilllegung mit ein – den gesamten Lebenszyklus eines Projekts.[53]

Starrheit

Einerseits stellt es einen bedeutenden Vorteil dar, dass eine Blockchain nicht von einer einzelnen Partei übernommen werden kann. Andererseits resultiert daraus eine gewisse Starrheit, da für Updates und Upgrades der Blockchain die Zustimmung beziehungsweise der Konsens innerhalb der Blockchain-Gemeinschaft erforderlich ist. Das Finden eines solchen Konsenses kann mitunter äußerst schwierig oder sogar unmöglich sein. Eine einst erfolgreiche Blockchain kann somit veralten und durch eine andere ersetzt werden. Um solche Situationen zu vermeiden, empfiehlt es sich, sogenannte Smart Rules einzuführen. Diese „schlauen Regeln“ regulieren die Blockchain unabhängig von den Knoten, die am Netzwerk teilnehmen. Ein Beispiel hierfür ist der „Mining-Schwierigkeitsgrad“ im Bitcoin-Netzwerk.[54]

Eigenverantwortung

Im Zusammenhang mit Blockchains ist ein ausgeprägtes Maß an Eigenverantwortung erforderlich. Bei Vergessen oder Verlust eines Passworts oder des privaten Schlüssels (Private Key) wird der Zugriff auf die Blockchain unmöglich. Es existiert keine verantwortliche Instanz, die in der Lage wäre, den Zugriff wiederherzustellen. Im Gegensatz dazu ermöglicht ein zentralisiertes System das Zurücksetzen oder erneute Anfordern eines Passworts, da dieses in der Regel zentral in einer Datenbank gespeichert ist. Genau aus diesem Grund könnte es in Zukunft vorstellbar sein, dass eine hybride Lösung aus dezentralen und zentralen Systemen entsteht. Diese könnten

---

[52] Vgl. Hosp, 2018, S. 78

[53] Vgl. Wittenberg, 2020, S. 137

[54] Vgl. Hosp, 2018, S. 82-83

sich gegenseitig ergänzen und die Schwächen des jeweils anderen Systems ausgleichen. Dabei ist von Bedeutung, dass die Systeme nicht miteinander vermischt werden, sondern lediglich kooperieren.[55]

Nutzerunfreundlichkeit

Im Vergleich zur Entwicklung des Internets befindet sich die Blockchain noch in ihren Anfängen. Die meisten Unternehmen oder Akteur*innen im Bereich der Blockchain konzentrieren sich hauptsächlich auf die technischen Aspekte, oft auf Kosten der Benutzerfreundlichkeit. Genauso wie das Internet, das mit einem einfachen Datenmodem und komplizierten Einstiegsschritten begonnen hat. Die Bedienung eines Wallets ist beispielsweise nicht immer intuitiv. Da es keine klare Verantwortlichkeit für die Blockchain gibt, steht auch kein Kundensupport im Falle von Problemen zur Verfügung. Diese Situation wird sich jedoch im Laufe der Zeit kontinuierlich verbessern.[56]

Skalierungslimitierung

Wenn von einer Limitierung der Skalierung einer Blockchain gesprochen wird, ist damit die Verarbeitung mehrerer Transaktionen innerhalb einer Zeiteinheit gemeint. Damit vollständiger Konsens herrschen kann, müssen alle Netzwerkteilnehmer*innen im Besitz der vollständigen Informationen sein. Damit dies auch während eines Updates der Informationen gewährleistet werden kann, müssen alle Teilnehmenden die technischen Voraussetzungen erfüllen, da die Limitierung von der jeweiligen Blockgröße abhängig ist. Wenn ein Update 250 Byte groß ist und ein Block 1 Megabyte an Speicherplatz benötigt, dann könnten innerhalb einer bestimmten Zeiteinheit maximal 4.000 Updates/Block umgesetzt werden. Einhergehend mit einem erhöhten Verbrauch an Datenmenge könnte alternativ die Blockgröße erhöht werden. Bis dato gibt es noch keine perfekte Skalierungslösung, allerdings gute Ansätze, wie beispielsweise die Off-Chain- oder 2nd-Layer-Möglichkeiten.57 In Layer-2-Lösungen wird eine zusätzliche Ebene auf die bestehende Blockchain implementiert. Diese zweite Schicht bearbeitet zahlreiche Transaktionen außerhalb des Hauptnetzes und fasst sie in einer einzigen Transaktion auf dem Hauptnetz zusammen. Dadurch wird die Belastung des Hauptnetzes verringert, während gleichzeitig die Aspekte der Dezentralisierung, Verfügbarkeit und Sicherheit gewährleistet werden.[58]

---

[55] Vgl. Hosp, 2018, S. 84-86

[56] Vgl. Hosp, 2018, S. 77-78

[57] Vgl. Hosp, 2018, S. 80-82

[58] Vgl. Haqshanas, 2023

Ressourcenverschwendung

Im Abschnitt über „Kosten“ wurde bereits auf die Abhängigkeit der Kosten vom gewählten Konsensmechanismus hingewiesen. Insbesondere beim Konsensmechanismus Proof-of-Work (PoW) müssen Rätsel mithilfe von Rechnerkapazitäten gelöst werden. Der dadurch verursachte Stromverbrauch wird zu Recht von Umweltschützer*innen kritisiert. In Island wird mittlerweile die Hälfte des Stromverbrauchs für Miningaktivitäten (Bitcoin) benötigt.[59] Das „Cambridge Centre for Alternative Finance“ schätzt den Stromverbrauch von Bitcoin auf 112 Terrawattstunden pro Jahr, was einem höheren Verbrauch als in den Niederlanden entspricht und nur etwas unter dem Verbrauch von Saudi-Arabien liegt.[60] Andere Konsensmechanismen, wie beispielsweise Proof-of-Stake (PoS) versuchen dieses Problem zu lösen, weisen jedoch entsprechende Nachteile im Vergleich zu PoW auf.

Privatsphäre

Dieser Punkt wurde bereits im Abschnitt zu den Stärken der Blockchain angesprochen. Als Nachteil wird hier gesehen, dass ein hohes Maß an Transparenz dazu führen kann, dass eine Person praktisch "gläsern" wird. In der Regel werden Informationen auf einer Blockchain dauerhaft gespeichert und können von allen Teilnehmer*innen bei öffentlichen Blockchains eingesehen werden. Durch die erwähnte Pseudoanonymität könnten beispielsweise Rückschlüsse auf die Identität gezogen werden, indem festgestellt wird, welche Investments eine Person getätigt hat. Es ist wahrscheinlich, dass nur wenige Menschen möchten, dass solche Informationen öffentlich zugänglich sind.[61] In Anbetracht der Gesetze in vielen Ländern, die die Privatsphäre als grundlegendes Menschenrecht verankern, ergeben sich weitere Herausforderungen im Kontext der Blockchain. In Europa haben alle Menschen gemäß der Datenschutzgrundverordnung (DSGVO) das Recht, die Einwilligung zur Verarbeitung persönlicher Daten zu widerrufen und die Löschung von Daten zu verlangen. Dies stellt viele Projekte vor erhebliche Herausforderungen, insbesondere im Umgang mit dauerhaft gespeicherten Daten, und beeinflusst teilweise auch das Design der Blockchain. Ein konkretes Beispiel hierfür ist die Universität von Nikosia, die als erste Bildungseinrichtung Bitcoin als Zahlungsmittel für Online-Kurse akzeptierte und Abschlusszertifikate in der Blockchain speicherte.[62]

---

[59] Vgl. Hosp, 2018, S. 79-80

[60] Vgl. Pramer, 2021

[61] Vgl. Hosp, 2018, S. 83-84

[62] Vgl. Moiseev, 2018

2.4.3 Zusammenfassung

Die verschiedenen Schwächen verdeutlichen, dass der Einsatz der Blockchain-Technologie nicht nur Vorteile, sondern auch Nachteile mit sich bringt und nur dann sinnvoll ist, wenn sie ein Problem besser lösen kann als ein zentrales System.[63]

Für den Anwendungsfall an der FERNFH ergeben sich jedoch wesentliche Vorteile hinsichtlich Transparenz und Vertrauen. Zeugnisse könnten von jeder Person jederzeit auf Echtheit und Richtigkeit überprüft werden, ohne auf das Vertrauen in die Unverfälschtheit angewiesen zu sein. Sicherheitsbedenken spielen generell eine wichtige Rolle beim Einsatz der Blockchain-Technologie im Bildungsbereich. Insbesondere besteht die Herausforderung darin, sensible Daten wie Zeugnisse sicher zu speichern und vor Manipulation zu schützen. Traditionelle Systeme, die auf zentralen Datenbanken basieren, sind anfällig für Hackerangriffe und unbefugten Zugriff. Die Blockchain bietet hier eine vielversprechende Alternative, da sie durch ihre dezentrale Natur und ihre Kryptographie basierte Sicherheit eine höhere Widerstandsfähigkeit gegenüber solchen Bedrohungen bietet. Dennoch ist es wichtig, die spezifischen Anforderungen und potenziellen Risiken sorgfältig zu prüfen, um sicherzustellen, dass die Implementierung der Blockchain-Technologie im Bildungsbereich effektiv und sicher ist.

Die Einführung und der Betrieb eines Blockchain-Netzwerks können mit beträchtlichen Kosten verbunden sein, insbesondere im Vergleich zu herkömmlichen Datenbank-Systemen. Während bei klassischen Systemen nur wenige Server benötigt werden, um Datenbanken und Anwendungen zu betreiben, erfordert ein Blockchain-Netzwerk eine redundante Infrastruktur, was zu erhöhten Anschaffungs- und Betriebskosten für Hardware und Software führt. Darüber hinaus müssen alle Nodes im Netzwerk dieselben Daten speichern, was zu einem zusätzlichen Bedarf an Speicherplatz und entsprechenden Kosten führt. In einigen Fällen können auch Transaktionsgebühren anfallen, je nach Art der Blockchain.[64] Für die FERNFH ist es daher von entscheidender Bedeutung, die passende Art von Blockchain für die geplanten Anwendungsfälle auszuwählen, denn nicht alle Arten von Blockchains erheben zwangsläufig Transaktionsgebühren. Diese Eigenschaft sollte daher bei der Auswahl unbedingt mitberücksichtigt werden. Auf die verschiedenen Blockchain-Typen wird an dieser Stelle auf Kapitel 3.1 verwiesen. Darüber hinaus ist es wichtig, sicherzustellen, dass der Nutzen der Einführung der Blockchain-Technologie die möglichen wirtschaftlichen und organisatorischen Nachteile aufwiegt.

---

[63] Vgl. Hosp, 2018, S. 76

[64] Vgl. Wittenberg, 2020, S. 112

Ein weiterer wichtiger Aspekt ist der Schutz der Privatsphäre, insbesondere wenn personenbezogene Daten im Spiel sind, wie es bei Zeugnissen der Fall ist. Es muss eine Lösung gefunden werden, um die Anforderungen der DSGVO zu erfüllen, einschließlich des Rechts auf Löschung von Daten.

3. Blockchain-Systeme: Typen und Funktionsweise

Die dynamische Entwicklung der Blockchain-Technologie in den letzten Jahren erschwert eine präzise Definition der Blockchain-Systeme. Oft wird der Begriff „Blockchain“ synonym für verschiedene Systeme oder Typen verwendet,[65] und bisher konnte keine einheitliche Definition etablieren werden. Eine Beschreibung der Blockchain als Multi-Party Consensus System (Mehrparteien-Konsenssystem) ermöglicht bereits eine präzise Definition, von der mögliche Anwendungsfälle abgeleitet werden können. Im Blockchain-Kontext haben sich zusätzliche Begriffe und Terminologien etabliert (siehe Kapitel „Definition und Terminologie“), die eine genauere Unterscheidung ermöglichen.[66]

3.1 Typen der Blockchain-Technologie

Bei der Blockchain-Technologie können verschiedene Varianten unterschieden werden, die auf zwei wesentlichen Aspekten beruhen. Auf der einen Seite wird die Teilnahme am Netzwerk durch den spezifischen Blockchain-Typen festgelegt, während auf der anderen Seite der Konsensmechanismus bestimmte Restriktion bezüglich der Teilnahme aufweist. Bei „permissioned“-Restriktionen ist die Teilnahme am Konsensmechanismus auf einen speziellen Teilnehmerkreis eingeschränkt, während bei „permissionless“-Restriktionen alle Teilnehmerkreise daran teilnehmen dürfen.[67]

In Abbildung 3 werden drei unterschiedliche Blockchain-Typen grafisch dargestellt und in den nachfolgenden Kapiteln 3.1.1 bis 3.1.3 beschrieben.

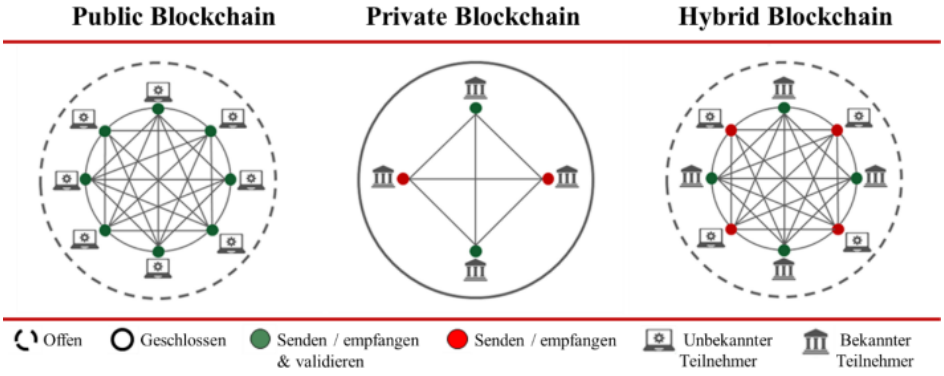

Abbildung 3: Unterschiedliche Typen der Blockchain-Technologie[68]

[65] Vgl. Kirstein, Lämmel, & Altenbernd, 2021, S. 5

[66] Vgl. Kirstein, Lämmel, & Altenbernd, 2021, S. 8

[67] Vgl. Bogensperger, et al., 2021, S. 13

[68] Quelle: Espich, 2019

3.1.1 Öffentliche Blockchains

Öffentliche Blockchains ähneln dem Internet, da sie in der Regel „permissionless“ sind. Das impliziert, dass jede beliebige Person an diesem Typ der Blockchain-Technologie teilnehmen und Teil des Netzwerks werden kann. Infolgedessen kann auch jede Person am Konsensmechanismus mitwirken und somit an der Verifizierung der Transaktionen beteiligt sein.[69] Folglich fungieren öffentliche Blockchains als P2P-Netzwerke und erfordern keine zentrale Autorität (Intermediär), die den Datenfluss verwaltet.[70]

3.1.2 Private Blockchains

Private Blockchains sind ausschließlich einer bestimmten Gruppe an Benutzer*innen zugänglich. Sie sind in der Regel gegenüber einer öffentlichen Blockchain kleiner und benötigen einen Intermediär (Autorität), der die Mitgliedschaft streng kontrolliert.[71] In der Regel sind private Blockchains im Gegensatz zu den öffentlichen Blockchains „permissioned“. Durch die vorhandene Autorität wird das Recht zum Lesen und Schreiben an bestimmte Netzwerkteilnehmer*innen vergeben. Eine Validierung der Transaktionen erfolgt normalerweise von einer einzigen Person, während die Konsensfindung von der Mehrheit der berechtigten Benutzer*innen erfolgt.[72]

3.1.3 Hybride Blockchains

Eine hybride Blockchain ist eine Kombination der beiden zuvor genannten Typen. Sie bestehen aus einem öffentlichen und privaten Zustand, die miteinander verbunden sein können. Spezielle Rechte sind üblicherweise an bestimmte Teilnehmer*innen vergeben, die wiederum verschiedenen Mitgliedern des Netzwerks unterschiedliche Rechte zuweisen können. Bei diesem Typ von Blockchain werden Transaktionen zuerst im privaten Bereich abgehandelt und von definierten Teilnehmern validiert.[73] Im Anschluss werden diese Transaktionen im öffentlichen Zustand als dauerhafter Nachweis gespeichert, nachdem sie mittels Konsensmechanismus genehmigt wurden.

3.2 Funktionsweise der Blockchain-Technologie

Im folgenden Abschnitt wird die grundlegende Funktionsweise der Blockchain erläutert. Um dies genauer zu verstehen, werden bekannte Basistechnologien in der Informatik,

---

[69] Vgl. Bogensperger, et al., 2021, S. 13f.

[70] Vgl. Laurence, 2017, S. 24

[71] Vgl. Laurence, 2017, S. 24

[72] Vgl. Bogensperger, et al., 2021, S. 14

[73] Vgl. Bogensperger, et al., 2021, S. 15

wie Hash-Funktionen, Kryptographie und digitale Signaturen kurz vorgestellt, wobei technische Details nur oberflächlich behandelt werden. Diese Technologien sind entscheidend für die Erstellung der erforderlichen Datenstrukturen und Funktionen in Blockchains.[74]

3.2.1 Hash-Funktionen

In einem dezentralen Peer-to-Peer-Netzwerk werden umfangreiche Daten und Informationen gespeichert. Um diese effizient und präzise identifizieren sowie vergleichen zu können, kommen in der Blockchain-Technologie Hash-Funktionen zum Einsatz.[75] Bei Hash-Funktionen handelt es sich um mathematische Funktionen, die auf Grundlage bestimmter Eingabewerte eine eindeutige Zahl (Hash-Wert) erzeugen. Anhand dieser Zahl kann kein Rückschluss auf die ursprünglichen Eingabewerte gezogen werden. Wird ein Eingabewert geringfügig geändert, ändert sich auch der Hash-Wert. Zur Veranschaulichung könnte man den Hash-Wert mit einem Fingerabdruck eines Menschen vergleichen, da er eine einzigartige Identifikation ermöglicht.[76] In Abbildung 4 wird schemenhaft veranschaulicht, wie die einzelnen Blöcke mithilfe der Hash-Werte miteinander verknüpft werden.

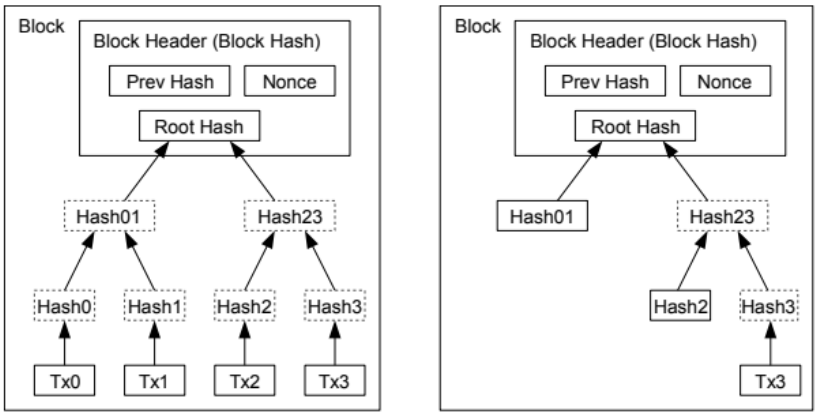

Abbildung 4: Verkettung der Blöcke mittels Hash-Werten[77]

Mithilfe von Hash-Funktionen wird für jede einzelne Transaktion (Tx) ein eindeutiger Hash-Wert berechnet. Diese Hash-Werte der Transaktionen werden paarweise kombiniert und dienen als Basis zur Berechnung des nächsten Hash-Wertes. Dieser Prozess wiederholt sich, bis alle Transaktionen zu einem einzelnen Hash-Wert, dem

---

[74] Vgl. Fill & Meier, Blockchain - Grundlagen, Anwendungsszenarien und Nutzungspotenziale, 2020, S. 5

[75] Vgl. Drescher, 2017, S. 89

[76] Vgl. Drescher, 2017, S. 89

[77] Quelle: Nakamoto, 2008, S. 4

sogenannten Block-Hash oder Block-Header, zusammengeführt wurden. Der übergeordnete Hash-Wert wird auch als Merkle Root oder Root-Hash bezeichnet. Zusammen mit einem Zeitstempel, dem Hash-Wert des vorherigen Blocks in der Kette und der Nonce (eine zufällige Zahl), wird dieser im Block gespeichert.[78]

3.2.2 Digitale Signaturen und Kryptographie

Neben der Anwendung von Hash-Funktionen kommt in der Blockchain-Technologie auch asymmetrische Kryptographie zum Einsatz. Diese Methode ermöglicht in einer Blockchain die eindeutige Identifikation von Nutzer*innen, die Autorisierung von Transaktionen und schützt das Eigentum der Anwender*innen vor unbefugtem Zugriff Dritter.[79] Digitale Signaturen, die auf asymmetrischer Kryptographie basieren, sind bereits heute ein weit verbreiteter Standard zur Sicherstellung der Authentizität von Informationen. Bei der asymmetrischen Kryptographie wird immer ein Schlüsselpaar benötigt, bestehend aus einem privaten, geheimen Schlüssel und einem öffentlichen Schlüssel, der allen bekannt ist. Der entscheidende Punkt ist, dass ein mit einem Schlüssel erzeugter Geheimtext nur mit dem jeweils anderen Schlüssel entschlüsselt werden kann und umgekehrt.[80] In Abbildung 5 wird die Funktionsweise der asymmetrischen Kryptographie schematisch dargestellt.

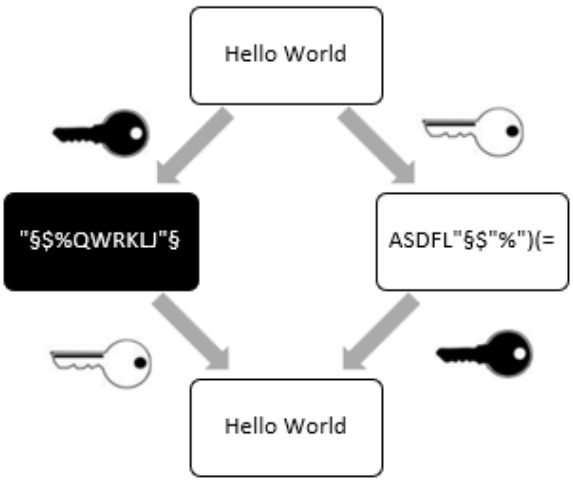

Abbildung 5: Schematische Darstellung der asymmetrischen Kryptographie[81]

Es gibt hier einen schwarzen (privaten) und einen weißen (öffentlichen) Schlüssel, die gemeinsam ein Schlüsselpaar bilden. In der oberen Hälfte wird die Nachricht „Hello

[78] Vgl. Espich, 2019, S. 14

[79] Vgl. Drescher, 2017, S. 112

[80] Vgl. Drescher, 2017, S. 114

[81] Vgl. Drescher, 2017, S. 114

World“ mit einem der beiden Schlüssel verschlüsselt (schwarzer Kasten mit weißer Schrift bzw. weißer Kasten mit schwarzer Schrift) und in der unteren Hälfte mit dem jeweils anderen Schlüssel wieder entschlüsselt.

In Abbildung 6 wird der Prozess der Signaturerstellung schematisch dargestellt.

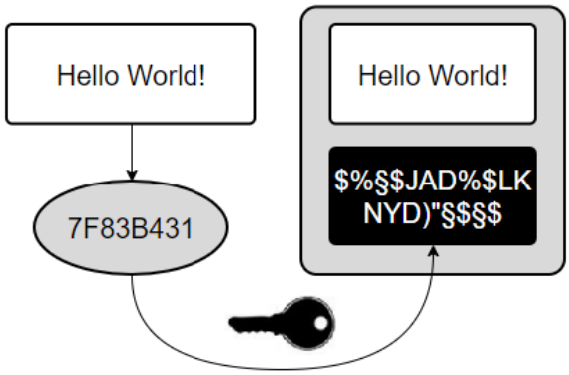

Abbildung 6: Erstellung einer digitalen Signatur[82]

Um eine Transaktion digital zu signieren, wird der Inhalt der Transaktion an eine Hashfunktion übermittelt. Der erhaltene Hash-Wert wird im Anschluss mithilfe des privaten Schlüssels verschlüsselt, wodurch die Signatur entsteht. Diese Signatur dient als Bestätigung der Transaktion und gewährleistet, dass der Ursprung der Transaktion authentifiziert und unverändert bleibt.[83] In Abbildung 7 wird schematisch das Überprüfen einer Nachricht dargestellt.

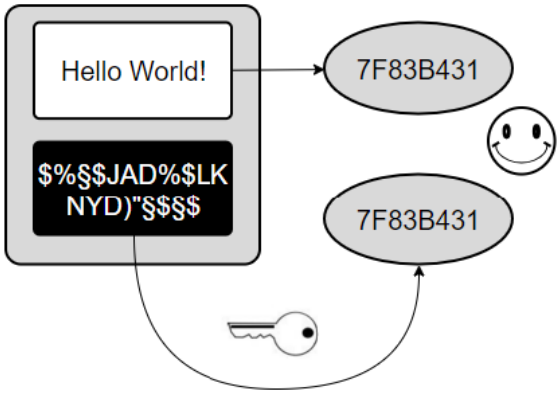

Abbildung 7: Überprüfen einer digitalen Signatur[84]

---

[82] Vgl. Drescher, 2017, S. 123

[83] Vgl. Drescher, 2017, S. 121

[84] Vgl. Drescher, 2017, S. 124

Bei Empfang wird die Nachricht mithilfe des öffentlichen Schlüssels entschlüsselt und erhält dabei den Hashwert 7F83B431. Ebenso erfolgt die Entschlüsselung der digitalen Signatur unter Verwendung des öffentlichen Schlüssels. Der dabei erhaltene Hashwert wird anschließend mit dem ersten Hashwert verglichen. Wenn die beiden Werte übereinstimmen, wie in Abbildung 7 dargestellt, kann davon ausgegangen werden, dass die ursprüngliche Nachricht "Hello World!" unverändert geblieben ist. Im Falle einer Manipulation der Nachricht würde ein anderer Hashwert als Nachweis erzeugt.

3.2.3 Konsensmechanismus

In P2P-Netzwerken fehlt eine Zwischeninstanz oder zentrale Autorität, die eine Transaktion, vergleichbar mit einer Bank, als gültig bestätigen könnte. Daher ist es von entscheidender Bedeutung, dass ein bestimmter Prozess oder Mechanismus sicherstellt, dass Einigkeit (Konsens) über die Gültigkeit einer Transaktion erzielt wird. Der sogenannte Konsensalgorithmus gewährleistet, dass die festgelegten Regeln der Blockchain konsequent durchgesetzt werden und somit ein Eintrag im Ledger erfolgt.[85] In Abbildung 8 wird schematisch eine Einigung innerhalb der Blockchain dargestellt.

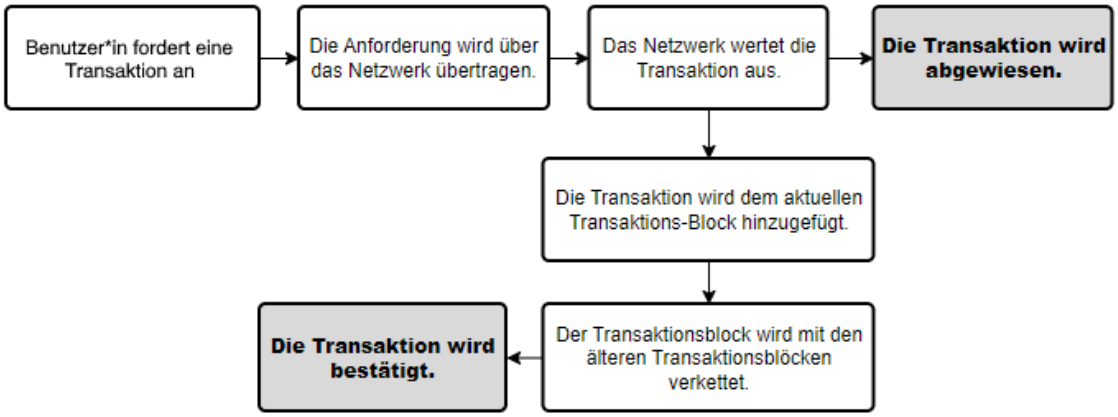

Abbildung 8: Einigung in einer Blockchain[86]

Da jede Blockchain andere Einträge erzeugt, setzt sie auch ihre eigenen Mechanismen ein, um einen Konsens zu erreichen. Zwei der am häufigsten verwendeten Konsensmechanismen sind Proof-of-Work (PoW) und Proof-of-Stake (PoS).[87]

---

[85] Vgl. Laurence, 2017, S. 28

[86] Vgl. Laurence, 2017, S. 28

[87] Vgl. Espich, 2019, S. 19

3.2.4 Gesamtbild des Blockchain-Prozesses

Die verschiedenen Komponenten der Funktionsweise von Blockchains, wie Hash-Verfahren, kryptographische Methoden und Konsensmechanismen, wurden in den vorherigen Abschnitten näher beleuchtet und können nun zu einem umfassenden Gesamtbild zusammengefügt werden.

In Abbildung 9 wird exemplarisch die Übertragung einer Transaktion in der Bitcoin-Blockchain veranschaulicht. Die Teilnehmerin Alice, die als Senderin fungiert, überträgt zehn Bitcoins an Teilnehmer Bob, den Empfänger. Beide verfügen bereits über einen privaten Schlüssel und die entsprechende öffentliche Adresse.

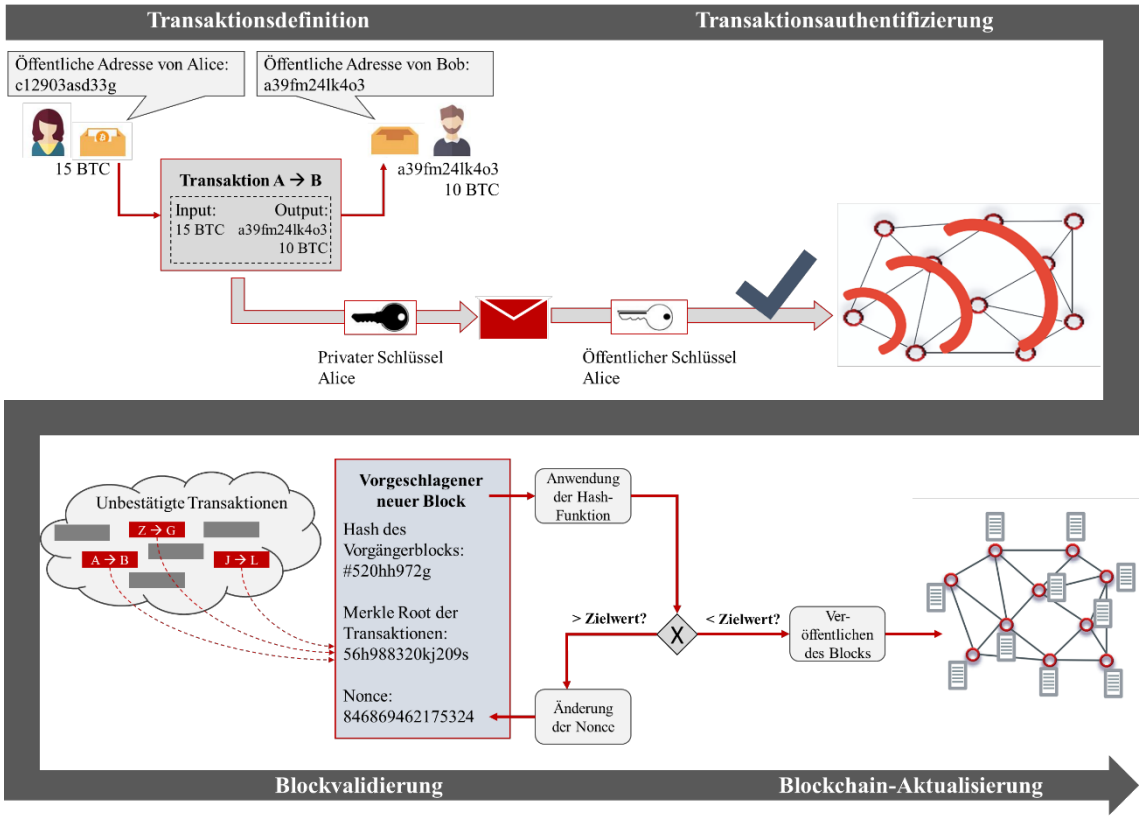

Abbildung 9: Gesamtprozess einer Blockchain[88]

Die Transaktion von Alice, bestehend aus verschiedenen Werten, wird mithilfe ihres privaten Schlüssels digital signiert und an das Netzwerk übermittelt. Die Authentizität der Nachricht wird von den Netzwerkteilnehmer*innen überprüft, indem die digitale Signatur mit dem öffentlichen Schlüssel entschlüsselt und die Nachricht in einen Hash-Wert umgewandelt wird. Wenn die beiden Hash-Werte übereinstimmen, wird die Transaktion

88 Quelle: Espich, 2019, S. 24

in einem Datenblock konsolidiert. Da die Transaktion noch nicht als gültig betrachtet wird, wird im Anschluss der Konsensmechanismus gestartet. In diesem Beispiel kommt der PoW-Mechanismus zum Einsatz. Das Ergebnis wird im gesamten Netzwerk veröffentlicht und von den Teilnehmer*innen überprüft. Wenn der neue Block als gültig bestätigt wird, wird er an die Blockchain angehängt.[89]

3.2.5 Kurzer Ausflug: Smart Contracts

Smart Contracts (dt. „intelligente Verträge“) nehmen einen beachtenswerten Platz im Blockchain-Bereich ein. Hierbei handelt es sich um Computercode auf der Blockchain, der einen Vertrag auf digitale Weise repräsentiert. Diese intelligenten Verträge können die Vertragserfüllung aller beteiligten Parteien sicherstellen, indem sie automatisch Maßnahmen ergreifen, sollte eine Partei sich nicht an die objektiven Vertragsbedingungen halten. Zudem können sie gewünschte Aktionen initiieren, sobald bestimmte Bedingungen erfüllt sind. Dies geschieht durch die automatische Ausführung von Anweisungen nach dem Prinzip "wenn X eintritt, dann führe Y aus" oder "wenn X nicht eintritt, dann führe Y aus". Ein Beispiel hierfür könnte sein, dass bei einem Autokredit die Nutzung des Fahrzeugs unterbrochen wird, sobald Kreditnehmer*innen mit Zahlungen in Verzug geraten.[90]

In Bezug auf Smart Contracts ist zu betonen, dass es sich dabei nicht um rechtlich bindende Verträge im Sinne des Bürgerlichen Gesetzbuches (ABGB) handelt. Smart Contracts teilen rechtliche Herausforderungen in Bezug auf die Unveränderlichkeit von Vertragsinhalten mit herkömmlichen Blockchain-Strukturen, insbesondere hinsichtlich einer möglichen Rückabwicklung bereits abgeschlossener Transaktionen.

---

[89] Vgl. Espich, 2019, S. 23-24

[90] Vgl. Fill & Meier, 2019, S. 120

4. Einführung von Blockchain-Technologie – was ist zu beachten?

Die derzeitige Auseinandersetzung und Erprobung der Blockchain-Technologie erstrecken sich über diverse Branchen. Eine effektive Umsetzung erfordert eine gründliche Analyse unterschiedlicher Aspekte, darunter technische, organisatorische sowie rechtliche Vorgaben und Rahmenbedingungen. Technische Aspekte stellen sicher, dass die Infrastruktur robust und sicher ist, organisatorische Maßnahmen fördern die Akzeptanz und Nutzung der Technologie, und rechtliche Überlegungen gewährleisten die Einhaltung gesetzlicher Vorschriften und den Schutz personenbezogener Daten. Eine genauere Untersuchung dieser Bereiche ermöglicht der FERNFH die Vorteile der Blockchain-Technologie voll auszuschöpfen und gleichzeitig potenzielle Risiken zu minimieren.

In den folgenden Abschnitten werden technische, organisatorische und rechtliche Aspekte beschrieben, die zum Teil auch für den Anwendungsfall an der FERNFH relevant sein können.

4.1 Technische Aspekte

In den vorangegangenen Abschnitten wurden die technischen Grundlagen näher erläutert, um die komplexe Funktionsweise der Blockchain zu verdeutlichen. Es wurde bereits aufgezeigt, vor welchen technischen Herausforderungen man bei der praktischen Umsetzung stehen könnte. Es ist entscheidend zu betonen, dass die reine Anwendung dieser Technologie allein nicht ausreicht, um IT-Sicherheitsprobleme zu lösen. Zusätzliche Angriffsvektoren, wie etwa Schnittstellen zu externen Datenquellen, können zu Herausforderungen führen. Berichte in den Medien über erfolgte Angriffe bestätigen, dass es sich hierbei keineswegs nur um theoretische Szenarien handelt.[91]

4.1.1 Technische Herausforderungen

Sicherheitsbedrohungen und Angriffsvektoren

Blockchain-Technologie ist nicht immun gegen Sicherheitsbedrohungen. Angriffe auf Schnittstellen zu externen Datenquellen, wie APIs und Datenbanken, können die Integrität des Systems gefährden. Es ist entscheidend, Sicherheitsmaßnahmen wie Firewalls und Intrusion Detection Systems (IDS), sowie regelmäßige Sicherheitsaudits zu implementieren.

[91] Vgl. Berghoff, Gebhardt, Lochter, & Maßberg, 2019, S. 2

Kryptografische Sicherheit

Die Anwendung starker kryptografischer Algorithmen ist notwendig, um die Integrität und Vertraulichkeit der Daten zu gewährleisten. Dies beinhaltet die Nutzung von Public-Key-Infrastrukturen (PKI) für digitale Signaturen und die Verschlüsselung sensibler Daten (vgl. Kapitel 3.2.2).

Netzwerkinfrastruktur

Eine robuste und skalierbare Netzwerkinfrastruktur ist notwendig, um eine hohe Verfügbarkeit und Leistung der Blockchain sicherzustellen. Dies umfasst die Bereitstellung redundanter Netzwerkverbindungen und verteilte Serversysteme, idealerweise an unterschiedlichen Standorten (vgl. Kapitel 2.3.4).

Transaktionsverarbeitung

Die Blockchain muss unter Umständen in der Lage sein, eine große Anzahl von Transaktionen in kurzer Zeit zu verarbeiten. Dies erfordert effiziente Konsensmechanismen und möglicherweise Layer-2-Lösungen wie Side-Chains oder Off-Chain-Transaktionen, um die Skalierbarkeit zu verbessern.

Datenmanagement

Da die Blockchain kontinuierlich wächst, muss das System ausreichend Speicherkapazität bieten, um alle Daten langfristig zu speichern. Strategien zur Datenkomprimierung und zur Aufbewahrung von nur wesentlichen Daten können hilfreich sein.

4.1.2 Integration in bestehende Systeme

Systemintegration/Interoperabilität

Die Blockchain muss nahtlos in bestehenden IT-Systeme der FERNFH integriert werden, um die Verwaltung von Studierendendaten und akademischen Leistungen effizient zu unterstützen, ohne bestehende Prozesse zu stören. Dies erfordert die Entwicklung robuster Schnittstellen (APIs). Unter Umständen muss die Blockchain mit verschiedenen Systemen und Plattformen interoperabel sein, um eine reibungslose Datenübertragung und -synchronisation zu gewährleisten.

Redundanz und Ausfallsicherheit

Die Blockchain-Infrastruktur sollte redundant ausgelegt sein, um Ausfälle zu vermeiden. Dies umfasst die Implementierung von Backup- und Wiederherstellungsmechanismen, sowie die Nutzung von Cloud-basierten Lösungen für zusätzliche Redundanz.

Monitoring und Wartung

Ein kontinuierliches Monitoring der Netzwerkverfügbarkeit und Leistung ist notwendig, um potenzielle Probleme frühzeitig zu erkennen und zu beheben. Regelmäßige

Wartungs- und Update-Zyklen sind entscheidend, um die Sicherheit und Effizienz der Blockchain-Lösung zu gewährleisten.

4.1.3 Entscheidung für den richtigen Blockchain-Typ

Öffentliche vs. private Blockchain

Eine öffentliche Blockchain bietet größere Transparenz und Sicherheit durch Dezentralisierung und ein umfangreiches Netzwerk von Teilnehmer*innen. Ideal für Anwendungen, die maximale Transparenz und Sicherheit erfordern. Eine private Blockchain bietet mehr Kontrolle und höhere Geschwindigkeit, da sie auf eine begrenzte Anzahl von Teilnehmer*innen beschränkt ist. Geeignet für Anwendungen, die eine kontrollierte Umgebung und schnelle Transaktionsverarbeitung erfordern (vgl. Kapitel 3.1).

Permissioned vs. permissionless Blockchain

Nur autorisierte Teilnehmer*innen können dem „permissioned“ Netzwerk beitreten und Transaktionen validieren. Es bietet mehr Kontrolle und Sicherheit in regulierten Umgebungen. Hingegen kann einem „permissionless“ Netzwerk jede*r beitreten und Transaktionen validieren. Es fördert Dezentralisierung und Transparenz, kann jedoch anfälliger für Angriffe sein (vgl. Kapitel 3.1).

4.1.4 Sicherheit, Datenschutz und DSGVO-Konformität

Datenschutzmaßnahmen

Maßnahmen zur Anonymisierung und Pseudonymisierung personenbezogener Daten sind notwendig, um die Privatsphäre der Studierenden zu schützen und die DSGVO-Konformität sicherzustellen. Strategien zur Bewältigung des Widerspruchs zwischen dem Recht auf Löschung personenbezogener Daten und der Unveränderlichkeit der Blockchain müssen entwickelt werden. Diese Maßnahmen sind jedoch nur erforderlich, wenn personenbezogene Daten auf der Blockchain gespeichert werden sollen. Alternativ könnten beispielsweise Hashwerte gespeichert werden, die keine Rückschlüsse auf personenbezogene Daten zulassen.

End-to-End-Verschlüsselung

Implementierung fortschrittlicher Verschlüsselungstechnologien zur Sicherstellung der Datenintegrität und Vertraulichkeit.

Zugriffskontrollen

Einrichtung von Zugangskontrollen und Authentifizierungsmechanismen, um unbefugten Zugriff auf die Blockchain-Daten zu verhindern.

4.2 Organisatorische Aspekte

Die Einführung der Blockchain-Technologie erfordert zumeist umfassende organisatorische Maßnahmen, um eine erfolgreiche Implementierung sicherzustellen. Hier sind einige wichtige Punkte, die dabei berücksichtigt werden sollten:

Grundlagenschulungen

Zunächst sind Schulungsprogramme für alle Beteiligten essenziell, um die Akzeptanz und Nutzung zu fördern. Diese Programme sollten Mitarbeiter*innen und Studierende mit den Grundlagen der Blockchain-Technologie, spezifischen Anwendungsfällen und Best Practices vertraut machen.

Technische Schulungen

Fortlaufende Schulungen und Workshops sind unter Umständen notwendig, um die Kenntnisse aktuell zu halten und sicherzustellen, dass IT-Mitarbeiter*innen über die erforderlichen Kompetenzen verfügen und praktische Fähigkeiten verbessern. Dies kann durch interne Schulungen oder durch externe Experten erfolgen.

Change-Management-Strategie

Ein effektives Change-Management kann ebenfalls entscheidend sein. Eine gut durchdachte Change-Management-Strategie unterstützt die Akzeptanz der neuen Technologie innerhalb der Organisation. Dies umfasst die Kommunikation der Vorteile der Blockchain-Technologie, sowie die Unterstützung bei der Überwindung von Widerständen.

Projektmanagement

Ein effektives Projektmanagement mit klaren Meilensteinen und regelmäßiger Überprüfung des Fortschritts gewährleistet, dass die Implementierung der Blockchain-Technologie strukturiert und effizient erfolgt.

Durch diese Maßnahmen kann die FERNFH sicherstellen, dass die Einführung der Blockchain-Technologie möglichst reibungslos verläuft und die zahlreichen Vorteile dieser Technologie voll ausgeschöpft werden.

4.3 Rechtliche Aspekte

Die Implementierung der Blockchain-Technologie wirft eine Reihe teilweiser komplexer rechtlicher Fragen auf, die in mehrere Schlüsselbereiche untergliedert werden können. Diese umfassen das Datenschutzrecht gemäß DSGVO, sowie spezifische Rechtsgebiete, abhängig vom jeweiligen Einsatzgebiet. Die Beachtung dieser rechtlichen Bestimmungen ist entscheidend, da sie wesentlichen Einfluss auf die Gestaltung technischer Lösungen haben und die Umsetzung eines Projekts beeinträchtigen oder sogar verhindern können. Daher ist eine umfassende Prüfung der

rechtlichen Rahmenbedingungen vor Projektbeginn unerlässlich, um potenzielle Hindernisse frühzeitig zu erkennen und zu umgehen.[92]

4.3.1 Datenschutzrecht (DSGVO)

Anonymisierung und Pseudonymisierung

Die DSGVO verlangt, dass personenbezogene Daten anonymisiert oder pseudonymisiert werden, um die Privatsphäre der Nutzer zu schützen. Die Implementierung solcher Maßnahmen auf einer Blockchain, die per Definition unveränderlich ist, stellt eine Herausforderung dar. Die FERNFH muss also sicherstellen, dass die Speicherung und Verarbeitung eventuell vorhandener personenbezogener Daten auf der Blockchain den DSGVO-Vorschriften entspricht.

Recht auf Löschung

Die DSGVO gewährt das Recht auf Löschung personenbezogener Daten. Dies steht im Konflikt mit dem Konzept der Blockchain, das die dauerhafte Speicherung von Daten vorsieht. Es müssen Lösungen gefunden werden, um das Recht auf Löschung personenbezogener Daten zu gewährleisten, obwohl die Blockchain per Definition unveränderlich ist. Mögliche Ansätze sind die Speicherung von Hashes anstelle der eigentlichen Daten oder die Nutzung von Off-Chain-Datenbanken.

4.3.2 Einfluss auf technische Lösungen

Technische Lösungen müssen so gestaltet werden, dass sie den rechtlichen Anforderungen entsprechen. Dies kann die Integration von Funktionen zur Datenanonymisierung und -pseudonymisierung, sowie Mechanismen zur Sicherstellung der Datenintegrität und -sicherheit umfassen.

4.3.3 Prüfung der rechtlichen Rahmenbedingungen

Eine umfassende rechtliche Beratung ist vor Beginn eines Blockchain-Projekts empfehlenswert. Dies hilft, potenzielle rechtliche Hindernisse frühzeitig zu erkennen und geeignete Maßnahmen zu deren Umgehung zu entwickeln und Risiken zu minimieren.

4.3.4 Anpassung interner Richtlinien

Die internen Richtlinien der FERNFH müssen überprüft und gegebenenfalls angepasst werden, um die Nutzung der Blockchain-Technologie zu legitimieren. Dies umfasst die

[92] Vgl. Wittenberg, 2020, S. 147

Anpassung der Datenschutzrichtlinien, IT-Sicherheitsrichtlinien und Compliance-Richtlinien.

Die Berücksichtigung dieser rechtlichen Aspekte ist entscheidend, um die erfolgreiche Implementierung der Blockchain-Technologie an der FERNFH sicherzustellen. Durch eine sorgfältige Planung und umfassende rechtliche Prüfung können potenzielle Hindernisse frühzeitig erkannt und geeignete Maßnahmen zur Risikominderung entwickelt werden. Dies gewährleistet, dass die Nutzung der Blockchain-Technologie rechtskonform erfolgt und die Vorteile dieser Technologie voll ausgeschöpft werden können.

4.4 Zusammenfassung

Das Kapitel behandelt eine breite Palette von Aspekten im Zusammenhang mit der Blockchain-Technologie und ihrer potenziellen Anwendung an der FERNFH. Es wird betont, dass die Implementierung dieser Technologie eine gründliche Prüfung technischer, organisatorischer und rechtlicher Überlegungen erfordert. Insbesondere wird auf die Bedeutung der Auswahl des geeigneten Blockchain-Typs vor Beginn des Projekts hingewiesen, da dies wesentliche Auswirkungen auf die Funktionalität und Effizienz der Lösung haben kann. Es wird zudem deutlich gemacht, wie wichtig organisatorische Maßnahmen bei der Einführung und im laufenden Betrieb sind, um eine hohe Akzeptanz bei allen Stakeholdern zu erreichen. Diese Akzeptanz bildet die Grundlage für eine möglichst reibungslose Implementierung und den Betrieb des Blockchain-Netzwerks, sowie dessen Integration in bestehende Systeme und Prozesse. Ein weiterer wichtiger Gesichtspunkt ist die Berücksichtigung rechtlicher Vorgaben, insbesondere der Datenschutz-Grundverordnung (DSGVO), da die Blockchain-Technologie potenziell im Widerspruch dazu stehen könnte. Daher ist es unerlässlich, vor Beginn eines Projekts eine umfassende rechtliche Prüfung durchzuführen, um mögliche Hindernisse zu identifizieren und zu vermeiden. Ein besonderer Fokus liegt auch auf der Kompatibilität von Privatsphäre und Blockchain, da das zugrunde liegende Konzept dieser Technologie möglicherweise nicht vollständig mit den Anforderungen der DSGVO im Einklang steht.

Insgesamt wird deutlich, dass die Einführung der Blockchain-Technologie an der FERNFH eine sorgfältige Planung und Analyse erfordert, um potenzielle Vorteile gegenüber den Herausforderungen und Risiken abzuwägen und eine erfolgreiche Implementierung sicherzustellen.

5. Anwendungsfälle rund um den Einsatz der Blockchain-Technologie im Bildungsbereich

In den bisherigen Kapiteln wurde die Blockchain-Technologie und deren Herausforderungen beim Einsatz in der realen Welt erläutert. Im Rahmen dieser Arbeit soll der Anwendungsfall „Ausstellung von digitalen Zeugnissen mithilfe der Blockchain“ an der FERNFH geprüft werden. Daher werden Anwendungsfälle vorgestellt, die bereits initiiert oder umgesetzt wurden.

5.1 Digitales Zeugnis (Bundesdruckerei Deutschland)

Im Rahmen des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) wurde im Jahr 2021 das OZG-Umsetzungsprojekt "Digitales Schulzeugnis" in Deutschland von Sachsen-Anhalt ins Leben gerufen. Das Ziel war die Einführung eines fälschungssicheren und datenschutzkonformen digitalen Schulzeugnisses. Der Pilotbetrieb startete im Sommer 2021 in den Bundesländern Berlin, Nordrhein-Westfalen und Rheinland-Pfalz. Alle interessierten Bundesländer hatten die Möglichkeit, sich dem Probebetrieb bis Ende 2022 anzuschließen. Ab 2023 war ein Echtbetrieb geplant, der es Schüler*innen ermöglicht, ihre eigenen Zeugnisse zu verwalten und zu überprüfen.[93]

Der Einsatz der Blockchain-Technologie bietet eine Sicherheitslösung für Zeugnisse, indem lediglich eine Prüfsumme gespeichert wird, ohne die eigentlichen Zeugnisse direkt auf der Blockchain abzulegen. Die verwendete Blockchain wird von der govdigital eG in zertifizierten Rechenzentren betrieben und öffentliche Dienstleister des Bundes, der Länder und Kommunen können daran teilnehmen, indem sie als Node auftreten. Schüler*innen erhalten neben dem herkömmlichen Papierzeugnis eine zusätzliche PDF-Datei, die von der Bundesdruckerei digital signiert wird. Der Hash-Wert oder die Prüfsumme dieser Zeugnisdatei wird als digitaler Fingerabdruck in der Blockchain hinterlegt. Zur Überprüfung der Echtheit des Zeugnisses kann über ein Portal der Bundesdruckerei online eine Abgleichung der Prüfsummen zwischen der PDF-Datei und der Blockchain durchgeführt werden. Etwaige Manipulationen können so zügig erkannt werden, ohne dass auf den Inhalt der PDF-Datei oder des Zeugnisses selbst geschlossen werden kann. Es werden keine personenbezogenen Daten in der Blockchain gespeichert, was eine wichtige Voraussetzung für die DSGVO-Konformität darstellt. Die Lösung wurde insgesamt so konzipiert, dass die Kosten und der Personalbedarf für Bildungseinrichtungen sinken. Durch eine standardisierte Schnittstelle können Verwaltungssysteme problemlos integriert werden, ohne dass

[93] Vgl. Chibber, 2021

zusätzliche Schulungen notwendig sind. Bisher mussten Papierzeugnisse für eine Hochschulbewerbung amtlich beglaubigt werden, was die Überprüfung ihrer Echtheit für die Hochschulen erschwert hat. Die vorgeschlagene Lösung schafft hier mehr Sicherheit und Fälschungsschutz.[94] Trotz dieser Vorteile bestehen jedoch Bedenken hinsichtlich der Einhaltung der DSGVO-Vorgaben. Insbesondere wenn Zeugnisse zentral im jeweiligen Bundesland oder dezentral an Bildungseinrichtungen archiviert werden müssen, können IT-Sicherheitsprobleme auftreten, da diese oft nicht über angemessene Sicherheitssysteme verfügen. Selbst auf Landes- oder Bundesebene kann der Schutz dieser Daten nicht uneingeschränkt gewährleistet werden, wie uns der Hackerangriff auf den Deutschen Bundestag im Jahr 2015 gezeigt hat.[95]

Im Februar 2022 wurde der Test aufgrund von Sicherheitsmängeln abgebrochen, nachdem Sicherheitsforscher*innen eine Schwachstelle im System entdeckten, die es ihnen ermöglichte, fiktive PDF-Zeugnisse auszustellen. Die Bundesdruckerei betonte in einer offiziellen Stellungnahme, dass die Ausstellung echter Zeugnisse zu keinem Zeitpunkt möglich war und verwies auf den frühen Entwicklungsstand des Projekts, das noch mit Fehlern behaftet war.[96] Wittmann, einer der Sicherheitsforscher, kritisiert die Verantwortlichen bezüglich fehlender Digitalkompetenz in der Verwaltung und einer ausgeprägten „Beratergläubigkeit“. Man habe sich für technische Fragen zu wenig interessiert.[97] Zu guter Letzt wurde das Lösungskonzept mittels Blockchain-Technologie vom Auftraggeber eingestellt.

Für die FERNFH bedeutet dies, dass die Einführung der Blockchain-Technologie für die Ausstellung von digitalen Zeugnissen eine vielversprechende Lösung sein könnte, um Sicherheitsprobleme zu minimieren und die Authentizität von Bildungsdokumenten zu gewährleisten. Die Nutzung von Blockchain könnte Studierenden ermöglichen, ihre Zeugnisse sicher zu verwalten und zu überprüfen, während gleichzeitig die Integrität der Daten gewährleistet wird. Allerdings sollten bei der Einführung der Blockchain-Technologie auch die potenziellen Herausforderungen und Bedenken berücksichtigt werden, insbesondere in Bezug auf die Einhaltung der Datenschutzbestimmungen und die Sicherheit der IT-Systeme. Es ist wichtig, dass angemessene Sicherheitsmaßnahmen implementiert und sichergestellt wird, dass die Technologie den rechtlichen Anforderungen entspricht.

---

[94] Vgl. Thylmann, Digitales Zeugnis, einfach und sicher, 2021

[95] Vgl. Chibber, 2021

[96] Vgl. Thylmann, 2022

[97] Vgl. Laaff, 2022

Darüber hinaus sollten Entwicklungen und Erfahrungen anderer Bildungseinrichtungen und Projekte im Zusammenhang mit der Blockchain-Technologie sorgfältig beobachten und analysieren werden, um von deren Erfahrungen zu lernen und mögliche Fallstricke zu vermeiden. Insgesamt bietet die Einführung der Blockchain-Technologie für die FERNFH die Möglichkeit, die Verwaltung von Bildungsnachweisen effizienter und sicherer zu gestalten und den Studierenden mehr Kontrolle über ihre eigenen Bildungsdaten zu geben.

5.2 Bewertung und Verwaltung von digitalen Lernnachweisen

Der Anwendungsfall beschreibt den Einsatz der Blockchain-Technologie im Bildungswesen zur Bewertung und Verwaltung von Lernnachweisen. Diese Technologie bietet dauerhafte, transparente und nachhaltige Lösungen, die Nutzer*innen direkten Zugang ermöglichen. Durch persönlich verschlüsselte Zertifikate können Lernende lebenslange Lernwege gestalten und ihre Bildung individuell anpassen. Die Nutzung von digitalen Badges, insbesondere durch offene Standards wie Mozilla's „digital badges“, war ein erster Schritt in der Online-Zertifizierung. Sollten die Herausgeber*innen der Zertifikate die Badges nicht mehr hosten, würden die Zertifikate automatisch ungültig werden. Die Blockchain-Technologie bietet dahingehend eine verbesserte Lösung, die eine dauerhafte und sichere Infrastruktur für Lernprotokolle schafft. Beispiele hierfür sind die „Blockcerts“ des MIT Media Lab und die Ethereum Smart Contracts der Open University, UK. Die Blockchain-Technologie wird von vielen EU-Ländern im Bildungsbereich getestet und bietet eine effiziente Möglichkeit zur Dokumentation und Verwaltung von Qualifikationen sowie zur Reduzierung von Verwaltungskosten in Universitäten. Es wird beschrieben, wie die Blockchain-Technologie eine permanente Authentifizierung und Speicherung für den wachsenden Markt alternativer Bildungsnachweise bietet, wobei Nutzer*innen direkte Kontrolle und Verwaltung über ihre Zertifikate haben. Diese alternativen Zertifikate ergänzen oft die Bildung älterer Lernender, die wenig oder keine IT-Schulung als Teil ihrer formellen Ausbildung erhalten haben. Die Blockchain könnte dazu beitragen, die Kompetenzlücke zu verringern und bietet zugleich ein hohes Maß an Sicherheit aufgrund der verteilten Ledger-Technologie. Es werden jedoch auch Herausforderungen wie Skalierbarkeit, Datenschutz und Speicherkapazität diskutiert. Obwohl die Blockchain teilweise noch experimentell ist, zeigt sie Potenzial für die Bildung, indem sie eine permanente, sichere und flexible Aufzeichnung von Lernerfolgen ermöglicht. Diese Entwicklung steht im Einklang mit den Standards und Richtlinien für Qualitätssicherung im europäischen Hochschulraum sowie den Zielen der EU zur Förderung nachhaltiger Entwicklung durch Bildung.[98]

[98] Vgl. Jirgensons & Kapenieks, 2018

Für die FERNFH könnte die Einführung der Blockchain-Technologie im Bildungsbereich bedeuten, dass sie ihre Zertifizierungs- und Verwaltungsprozesse für Bildungsnachweise verbessern und modernisieren kann. Der Einsatz der Blockchain könnte eine dauerhafte und sichere Aufzeichnung von Zertifikaten und anderen Bildungsnachweisen ermöglichen, wodurch sie die Authentizität und Integrität dieser Dokumente gewährleisten kann. Dies könnte dazu beitragen, das Vertrauen in die Bildungsnachweise zu stärken und den Verwaltungsaufwand zu reduzieren. Darüber hinaus könnte die Blockchain-Technologie helfen, den steigenden Bedarf an flexiblen Bildungswegen und alternativen Bildungsnachweisen besser zu bewältigen. Lernende könnten direkten Zugang zu ihren Zeugnissen und anderen Bildungsnachweisen erhalten und diese auf sichere Weise verwalten. Dies könnte die Zufriedenheit der Lernenden erhöhen und ihre Bindung an die FERNFH stärken. Allerdings müsste bei der Einführung der Blockchain-Technologie auch Herausforderungen wie Skalierbarkeit, Datenschutz und Speicherkapazität berücksichtigt werden. Es wäre wichtig, sicherzustellen, dass die technische Infrastruktur der FERNFH diesen Anforderungen gerecht wird und angemessene Sicherheitsmaßnahmen implementiert werden, um die Privatsphäre der Lernenden zu schützen, sowie die Integrität der Bildungsnachweise zu gewährleisten.

5.3 Bildung und Blockchain – UNESCO Publikation

Die Publikation "Bildung und Blockchain" von UNESCO und dem Commonwealth of Learning[99] untersucht tiefgehend die Anwendung der Blockchain-Technologie im Bildungssektor. Sie zielt darauf ab, politischen Entscheidungsträger*innen und Bildungs-Expert*innen einen umfassenden Überblick über die Möglichkeiten und Herausforderungen dieser Technologie zu vermitteln. Besonders hervorgehoben werden spezifische Anwendungsfälle wie die Speicherung digitaler Zertifikate und die Automatisierung administrativer Prozesse durch intelligente Verträge. Die Publikation betont das transformative Potenzial der Blockchain, stellt jedoch auch klar, dass eine umsichtige Bewertung technologischer, rechtlicher und ethischer Aspekte entscheidend ist, um eine verantwortungsbewusste Integration in die Bildungslandschaft zu gewährleisten.

Trotz des erkennbaren Nutzens der Blockchain gibt es bedeutende Limitationen und Herausforderungen, die im Bildungsbereich berücksichtigt werden müssen. Diese Limitationen verdeutlichen, dass, obwohl die Blockchain-Technologie das Potenzial hat, den Bildungssektor zu transformieren, erhebliche Überlegungen und Entwicklungen

[99] Vgl. Grech, Balaji, & Miao, 2022

notwendig sind, um ihre Herausforderungen zu meistern und eine effektive und verantwortungsbewusste Integration an der FERNFH zu gewährleisten:

Skalierbarkeit

Die Blockchain-Technologie kann in kleineren, kontrollierten Umgebungen effizient funktionieren, aber es gibt ernsthafte Bedenken hinsichtlich ihrer Skalierbarkeit, besonders wenn es um die Implementierung in umfangreichen Bildungssystemen geht. Die Verarbeitungsgeschwindigkeit und Kapazität der Blockchain könnten bei einer hohen Anzahl von Transaktionen eingeschränkt sein, was zu signifikanten Verzögerungen führen kann.

Datenschutz

Die unveränderliche Natur der Blockchain stellt eine Herausforderung für den Datenschutz dar, insbesondere im Hinblick auf die Speicherung sensibler persönlicher Daten wie Bildungsnachweise. Probleme entstehen daraus, dass einmal auf der Blockchain gespeicherte Daten schwierig zu modifizieren oder zu löschen sind, selbst wenn dies aus rechtlichen oder datenschutzrechtlichen Gründen erforderlich wäre.

Komplexität und Benutzerfreundlichkeit

Die Technologie kann für Nicht-Expert*innen kompliziert und schwer zu verstehen sein. Das erschwert die breite Akzeptanz und Anwendung von Blockchain-Lösungen in der Bildung, da umfassendes technisches Verständnis und fortlaufende Schulungen erforderlich sind.

Energieverbrauch

Die für die Aufrechterhaltung der Blockchain notwendige Rechenleistung ist erheblich und führt zu einem hohen Energieverbrauch. In einer Zeit, in der globale Anstrengungen zur Reduzierung von CO2-Emissionen und zur Förderung der Nachhaltigkeit zunehmen, ist dies eine bedeutende Einschränkung.

Regulatorische und rechtliche Herausforderungen

Die Gesetzgebung hinkt oft der technologischen Entwicklung hinterher, was zu einem Mangel an Klarheit und Sicherheit führt, der die Implementierung und Akzeptanz der Blockchain-Technologie behindern kann.

6. Blockchain-Technologie an der FERNFH

In diesem Kapitel wird eine Machbarkeitsanalyse für die Implementierung von Blockchain basierten Zeugnissen an der FERNFH durchgeführt. Diese Analyse berücksichtigt technische, organisatorische und rechtliche Aspekte, um die Machbarkeit dieses innovativen Anwendungsfalles umfassend zu bewerten. Die Nutzung der Blockchain-Technologie an der FERNFH bietet das Potenzial, die Sicherheit und Authentizität von Zeugnissen erheblich zu verbessern. Durch die Dezentralisierung und die kryptografische Absicherung könnten technische Schwachstellen traditioneller zentraler IT-Systeme, die anfällig für Hackerangriffe sind, minimiert oder sogar beseitigt werden. Dies würde dazu beitragen, die Integrität und Verifizierbarkeit von Zeugnissen langfristig sicherzustellen. Organisatorisch stellt die Einführung von Blockchain-Technologie hohe Anforderungen an die Infrastruktur und das IT-Personal der FERNFH. Es bedarf einer robusten Netzwerkinfrastruktur, umfassender Schulungsmaßnahmen für Mitarbeiter*innen der FERNFH und Studierende, sowie einer durchdachten Change-Management-Strategie, um die Akzeptanz und effektive Nutzung der neuen Technologie sicherzustellen. Rechtlich gesehen bringt die Implementierung der Blockchain-Technologie an der FERNFH Herausforderungen mit sich, insbesondere im Hinblick auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO). Die unveränderliche Natur der Blockchain steht im Konflikt mit dem Recht auf Löschung personenbezogener Daten, was eine innovative technische Lösungen erfordert, um rechtliche Konformität zu gewährleisten.

Das Ziel dieser Machbarkeitsanalyse anhand des genannten Anwendungsfalles ist es, die Potenziale und Herausforderungen einer Blockchain basierten Lösung für digitale Zeugnisse an der FERNFH zu identifizieren und zu bewerten. Dabei wird untersucht, ob die technischen Voraussetzungen vorhanden sind, wie organisatorische Hürden überwunden werden können und inwieweit rechtliche Rahmenbedingungen eingehalten werden müssen. Diese umfassende Betrachtung soll als Grundlage für eine fundierte Entscheidungen zur Implementierung der Blockchain-Technologie an der FERNFH dienen.

6.1 Anwendungsfall „Blockchain basiertes Zeugnis“

Die folgenden Prozessschritte orientieren sich an den Erfahrungen der Bundesdruckerei Deutschland (vgl. Kapitel 5.1) und passen sich an die spezifischen Anforderungen und Rahmenbedingungen der FERNFH an. Durch die systematische Berücksichtigung technischer, organisatorischer und rechtlicher Aspekte wird sichergestellt, dass die Implementierung der digitalen Zeugnisse sowohl effizient als auch konform mit den relevanten Vorschriften erfolgt. In der folgenden Abbildung 10 werden die einzelnen Prozessschritte schematisch dargestellt:

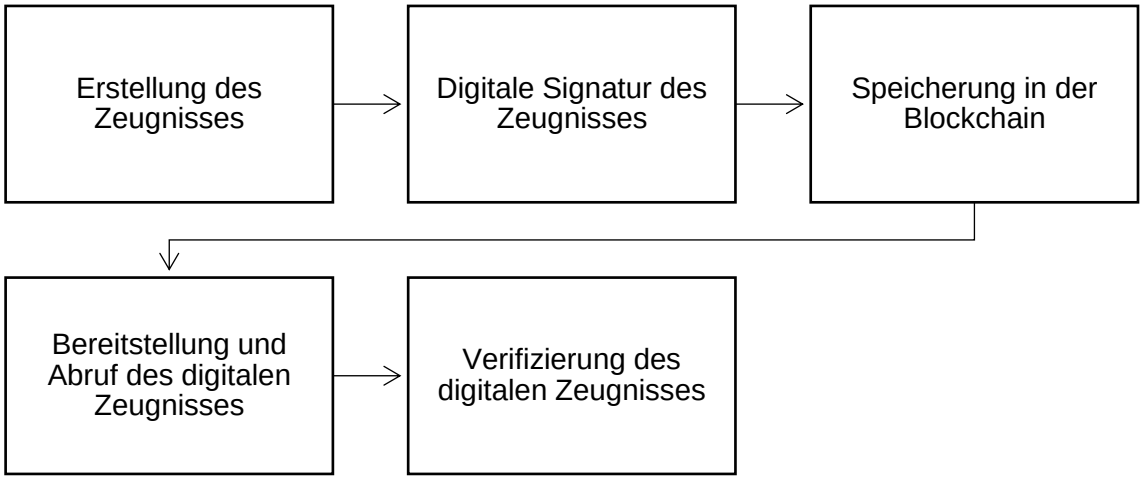

Abbildung 10: Schematische Darstellung der Prozessschritte

1. Erstellung des Zeugnisses

Technische Aspekte:

- Die Zeugnisdaten werden digital erfasst und in einem sicheren, zugangsbeschränkten System gespeichert.
- Einsatz von Software zur Erzeugung des Zeugnisses im PDF-Format.
- Generierung eines Hash-Wertes für das digitale Zeugnis, um die Integrität und Authentizität sicherzustellen.

Organisatorische Aspekte:

- Identifizierung und Schulung der Mitarbeiter*innen der FERNFH, die für die Erstellung und Verwaltung der Zeugnisse zuständig sind.
- Definition der Prozesse zur Dateneingabe und Qualitätssicherung.
- Einrichtung eines Workflows zur systematischen Zeugniserstellung.

Rechtliche Aspekte:

- Sicherstellung, dass die Datenerfassung und -verarbeitung den Datenschutzbestimmungen (DSGVO) entspricht.
- Einholung der Einwilligung der Studierenden zur digitalen Verarbeitung ihrer Daten.

2. Digitale Signatur des Zeugnisses

Technische Aspekte:

- Anwendung einer digitalen Signatur auf das PDF-Dokument mithilfe eines Zertifikats einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) oder einer entsprechenden Hash-Funktion zur Erstellung des Zeugnis-Hashes
- Speicherung des Hash-Wertes des signierten Dokuments in der Blockchain.

Organisatorische Aspekte:

- Festlegung und Dokumentation der Verantwortlichkeiten für die digitale Signatur der Zeugnisse.
- Schulung der Mitarbeiter*innen der FERNFH im Umgang mit der Signatur-Software und der Blockchain-Technologie.

Rechtliche Aspekte:

- Sicherstellung, dass die verwendete Signaturtechnologie den rechtlichen Anforderungen entspricht.
- Dokumentation und Archivierung der digitalen Signaturprozesse zur Nachweisbarkeit.

3. Speicherung in der Blockchain

Technische Aspekte:

- Implementierung der Blockchain-Technologie zur sicheren und unveränderlichen Speicherung der Zeugnis-Hashes.
- Einrichtung eines Netzwerks aus Nodes, die an der Blockchain teilnehmen und die Daten verifizieren.

Organisatorische Aspekte:

- Festlegung der beteiligten Benutzer*innen und deren Rolle im Blockchain-Netzwerk.
- Implementierung von Backup- und Wiederherstellungsmechanismen.

Rechtliche Aspekte:

- Sicherstellung, dass keine personenbezogenen Daten direkt in der Blockchain gespeichert werden, sondern nur die Hash-Werte.
- Einhaltung der gesetzlichen Vorgaben zur Datenaufbewahrung und -löschung.

4. Bereitstellung und Abruf des digitalen Zeugnisses

Technische Aspekte:

- Entwicklung eines Portals, über das Studierende ihre digitalen Zeugnisse abrufen können.
- Implementierung von Schnittstellen für potenzielle Arbeitgeber*innen und andere Institutionen zur Überprüfung der Zeugnisse.

Organisatorische Aspekte:

- Schulung der Studierenden im Umgang mit dem digitalen Portal. Alternativ könnten detaillierte Informationen auf dem vorhandenen Online-Campus der FERNFH publiziert werden.
- Festlegung der Prozesse für den Abruf und die Überprüfung der Zeugnisse.

Rechtliche Aspekte:

- Sicherstellung, dass der Zugang zum Zeugnisportal sicher und datenschutzkonform ist.
- Implementierung von Authentifizierungsmechanismen zur Verhinderung unbefugter Zugriffe.

5. Verifizierung des digitalen Zeugnisses

Technische Aspekte:

- Nutzung der Blockchain zur Verifizierung des Hash-Wertes des digitalen Zeugnisses.
- Bereitstellung einer Benutzeroberfläche zur einfachen Überprüfung der Zeugnisauthentizität für potenzielle Arbeitgeber*innen und sonstige Institutionen

Organisatorische Aspekte:

- Einrichtung von Helpdesk- und Support-Strukturen zur Unterstützung bei der Verifizierung.
- Dokumentation der Verifizierungsprozesse und -protokolle.

Rechtliche Aspekte:

- Sicherstellung, dass die Verifizierungsprozesse transparent und nachvollziehbar sind.
- Einhaltung aller rechtlichen Anforderungen an die Nachweisführung und Dokumentation.

6.2 Machbarkeitsanalyse

Die Machbarkeitsanalyse orientiert sich an den Erfahrungen des Projekts "Digitale Zeugnisse" der Bundesdruckerei Deutschland (vgl. Kapitel 5.1) und passt diese an die spezifischen Rahmenbedingungen und Anforderungen der FERNFH an. Die Untersuchung gliedert sich in mehrere Prozessschritte, die jeweils unter technischen, organisatorischen und rechtlichen Gesichtspunkten betrachtet werden. Dabei werden theoretische Erkenntnisse aus den vorherigen Kapiteln sowie ein Gespräch mit der Leitung der IT-Abteilung an der FERNFH einbezogen.

Kategorisiert nach den zu untersuchenden Aspekten, wurden folgende Fragen an die IT-Leitung gerichtet:

Technische Sicht

- Welche Datenbanksysteme sind aktuell im Einsatz?
- Welche Software zur Erstellung eines PDF-Dokuments ist im Einsatz?

- Können kryptografische Hash-Funktionen (z.B. SHA256) verwendet bzw. implementiert werden?
- Könnte eine Blockchain-Infrastruktur eingerichtet werden? Wird extern Unterstützung benötigt oder ist das Fachwissen bereits vorhanden? Ist die Implementierung weiterer Server möglich? Gibt es eine favorisierte Plattform?
- Kann grundsätzlich eine Blockchain-Infrastruktur zur Speicherung der Hash-Werte implementiert werden?
- Ist es vorstellbar, eine eigene Blockchain zu betreiben oder sich einer Plattform wie Hyperledger Fabric anzuschließen? Sind technischen Kenntnisse vorhanden oder müsste externe Unterstützung angefordert werden?
- Welche Infrastruktur/Netzwerke (z.B. ein Hochschulnetzwerk) gibt es? Können Server an verteilten Standorten zur Verfügung gestellt werden?
- Ist die Entwicklung eines Online-Portals technisch machbar oder bereits vorhanden? (für Studierende und Arbeitgeber*innen/Institutionen)
- Können APIs zwischen Blockchain und Online-Portal entwickelt und implementiert werden?
- Kann eine Weboberfläche zur Überprüfung des Zeugnisses erstellt werden, indem ein Hashwert eines hochgeladenen PDF-Dokuments (Zeugnis) erzeugt und dieser gegen die Blockchain und eine Datenbank überprüft?

Organisatorische Sicht

- Ist die Durchführung von internen Schulungen (Mitarbeiter*innen und IT-Personal) durchführbar bzw. von wem werden sie organisiert?
- Gibt es Prozessbeschreibungen zur Dateneingabe, um die Richtigkeit von Zeugnissen zu gewährleisten?
- Gibt es einen Workflow zur Erstellung eines Zeugnisses bzw. könnte ein solcher eingerichtet bzw. adaptiert werden?
- Gibt es einen Organisationsplan, der Verantwortlichkeiten definiert und dokumentiert? Könnte ein solcher organisatorisch umgesetzt werden?
- Müssten andere Institutionen zur Teilnahme am Netzwerk mitberücksichtigt werden? Wenn ja, müssten Verträge/Vereinbarungen erstellt oder adaptiert werden?
- Können Wiederherstellungsmechanismen organisatorisch implementiert werden oder sind bereits vorhanden (z.B. Notfallwiederherstellungsplan)?
- Können neue Prozesse, die den Abruf und die Überprüfung der Zeugnisse regeln, organisatorisch umgesetzt werden?
- Gibt es einen Help-Desk/Support der bei Fragen zur Verfügung steht oder kann ein solcher eingerichtet werden?
- Können Protokolle von Verifizierungsprozessen zur Dokumentation erstellt und gespeichert werden?

Rechtliche Sicht

- Wie wird die rechtmäßige Verarbeitung personenbezogener Daten gewährleistet? …Pseudonymisierung, Zugriffskontrollen…
- Werden Einwilligungen von Studierenden zur Verarbeitung personenbezogener Daten eingeholt? …wie wird dieses Verfahren umgesetzt?
- Gibt es rechtliche Anforderungen an die digitale Signatur? Muss ein Zertifikat einer vertrauenswürdigen Stelle verwendet werden oder würde eine interne Hash-Funktion ausreichen?
- Gibt es eine Art Dokumentationssystem, welches alle Signaturprozesse zur Dokumentation erfasst und speichert bzw. ist das überhaupt notwendig?
- Hash-Werte (Blockchain) und personenbezogene Daten (klassische Datenbank) müssten getrennt gespeichert werden. Gibt es Prozesse, die eine sichere Löschung von Daten gemäß gesetzlicher Anforderungen (DSGVO) sicherstellen?
- Ist die Implementierung von Authentifizierungs- und Autorisierungsmechanismen (z.B. 2FA) für den Zugriff auf das Zeugnisportal möglich oder bereits vorhanden (z.B. Online-Portal)?
- Können Sicherheitsfunktionen, die den unbefugten Zugriff verhindern implementiert werden oder sind bereits vorhanden? …z.B. durch Verwendung von Authentifizierungsprotokollen wie OAuth 2.0 oder Sicherheitsfunktionen, wie IP-Whitelisting und Captchas?
- Ist die Transparenz und Nachvollziehbarkeit von Verifizierungsprozessen rechtlich notwendig und könnte sie organisatorisch umgesetzt werden?
- Gibt es Datenschutzbeauftragte und/oder rechtliche Berater*innen, um die rechtliche Konformität zu gewährleisten? Können regelmäßige Audits durchgeführt werden oder werden durchgeführt?

Diese systematische Vorgehensweise ermöglicht es, die Potenziale und Herausforderungen der Einführung Blockchain basierter Zeugnisse fundiert zu bewerten. Durch die umfassende Berücksichtigung technischer, organisatorischer und rechtlicher Aspekte wird eine solide Entscheidungsgrundlage für die Implementierung dieser innovativen Technologie an der FERNFH geschaffen.

Die folgenden Prozessschritte werden detailliert analysiert:

1. Erstellung des Zeugnisses

Hierbei werden die technischen Anforderungen an die Zeugnisgenerierung, die organisatorischen Strukturen zur Datenerfassung, sowie die rechtlichen Rahmenbedingungen zur Einhaltung der Datenschutzgrundverordnung (DSGVO) betrachtet.

2. Digitale Signatur des Zeugnisses

Dieser Schritt umfasst die Anwendung digitaler Signaturen zur Sicherstellung der Echtheit der Zeugnisse, die Schulung der Mitarbeiter*innen der FERNFH im Umgang mit der Signatursoftware und die rechtliche Absicherung der Signaturverfahren.

3. Speicherung in der Blockchain

Die Analyse beleuchtet die technische Implementierung der Blockchain zur sicheren Speicherung von Zeugnis-Hashes, die organisatorische Einbindung der Blockchain-Technologie und die rechtlichen Vorgaben zur Datenaufbewahrung und -löschung.

4. Bereitstellung und Abruf des digitalen Zeugnisses

Es wird untersucht, wie Studierende ihre digitalen Zeugnisse sicher abrufen können, welche organisatorischen Prozesse zur Unterstützung dieser Bereitstellung notwendig sind und wie rechtliche Anforderungen an den Datenschutz erfüllt werden können.

5. Verifizierung des digitalen Zeugnisses

Dieser Schritt analysiert die technischen Lösungen zur Verifizierung der Zeugnisse über die Blockchain, die organisatorischen Maßnahmen zur Unterstützung der Verifizierung und die rechtlichen Aspekte zur Sicherstellung der Transparenz und Nachvollziehbarkeit.

6.2.1 Prozessschritt 1: Erstellung des Zeugnisses

6.2.1.1 Technische Aspekte

Erfassung und Speicherung der Zeugnisdaten

Anforderung	Die Daten müssen sicher und zuverlässig erfasst und gespeichert werden. Dies erfordert eine robuste Datenbanklösung, die sowohl strukturiert als auch skalierbar ist.
Lösung	Einsatz einer relationalen Datenbank (z.B. MySQL, MS-SQL, PostgreSQL) für strukturierte Datenspeicherung. Alternativ könnte eine NoSQL-Datenbank (z.B. MongoDB) verwendet werden, wenn Flexibilität bei der Datenspeicherung gefordert ist.
Bewertung	Die FERNFH betreibt aktuell einen SQL-Server von Microsoft für die Verwaltungssoftware. Somit ist die zuverlässige Erfassung und Speicherung von Zeugnisdaten, sowie Performance bereits sichergestellt. Diese Anforderung wird als machbar eingestuft.

Erzeugung des digitalen Zeugnisses im PDF-Format

Anforderung	Ein Tool zur Erstellung von PDF-Dokumenten muss integriert werden. Es sollte in der Lage sein, die Zeugnisdaten in ein standardisiertes Format zu überführen.
Lösung	Einsatz von Bibliotheken wie Apache PDFBox oder iText zur PDF-Erstellung. Diese Tools können in bestehende Systeme integriert werden.
Bewertung	Grundsätzlich hat sich die Erstellung von PDF-Dokumenten technisch gut etabliert und wird in vielen Softwareprodukten bereits als Standardfunktionalität angeboten. Die FERNFH verwendet aktuell ein Tool zur Generierung von PDF-Dokumenten der FH-Krems, welche anschließend mit einer Amtssignatur von der Firma A-Trust[100] signiert werden. Diese Anforderung wird daher als machbar eingestuft.

Generierung eines Hash-Wertes für das Zeugnis

Anforderung	Ein eindeutiger Hash-Wert muss generiert werden, um die Integrität des Zeugnisses sicherzustellen.
Lösung	Verwendung von kryptografischen Hash-Funktionen wie SHA-256 zur Erzeugung des Hash-Wertes.
Bewertung	Die Implementierung kryptografischer Hash-Funktionen ist technisch gut etabliert und sicher (vgl. Kapitel 3.2.2). Es muss sichergestellt werden, dass der Hash-Wert zusammen mit dem Zeugnis gespeichert wird, um spätere Verifizierungen zu ermöglichen. Aus Sicht der IT-Leitung der FERNFH steht dem ebenfalls nichts im Wege, da bereits kryptografische Verfahren problemlos eingesetzt werden. Diese Anforderung wird als machbar eingestuft.

6.2.1.2 Organisatorische Aspekte

Identifikation und Schulung der Mitarbeiter*innen der FERNFH

Anforderung	Mitarbeiter*innen der FERNFH, die für die Erstellung und Verwaltung der Zeugnisse verantwortlich sind, müssen identifiziert und geschult werden.

[100] A-Trust, 2024

Lösung	Durchführung von Workshops und Schulungen, um die Mitarbeiter*innen der FERNFH mit neuen Tools und Prozessen vertraut zu machen.
Bewertung	Schulungsprogramme sind organisatorisch gut umsetzbar, erfordern jedoch Zeit und Ressourcen. Es ist wichtig, frühzeitig Schulungen zu planen und durchzuführen, um einen reibungslosen Übergang sicherzustellen (vgl. Kapitel 4.2). Erfahrungsgemäß werden Schulungsprogramme im Rahmen von IT-Projekten zumeist von der IT-Abteilung selbst durchgeführt. Diese Schulungsprogramme können auch von der IT-Abteilung der FERNFH durchgeführt werden. Diese Anforderung wird als machbar eingestuft.

Definition der Prozesse zur Dateneingabe und Qualitätssicherung

Anforderung	Es müssen klare Prozesse zur Dateneingabe und Qualitätssicherung definiert werden, um die Richtigkeit und Vollständigkeit der Zeugnisse zu gewährleisten.
Lösung	Erstellung von Prozessdokumentationen und Checklisten, die die Schritte zur Dateneingabe und Überprüfung detailliert beschreiben.
Bewertung	Die Definition und Dokumentation von Prozessen sind organisatorische Aufgaben, die sorgfältige Planung erfordern. Durch klare Anweisungen kann die Fehlerquote minimiert und die Effizienz gesteigert werden. Dieser Schritt ist insbesondere in Bezug auf die Unveränderlichkeit der Blockchain wichtig (vgl. Kapitel 2.3.3). Die IT-Leitung der FERNFH bestätigt ebenfalls einen bereits vorhandenen Prozess, der eventuell entsprechend adaptiert werden müsste. Diese Anforderung wird als machbar eingestuft.

Einrichtung eines Workflows zur systematischen Zeugniserstellung

Anforderung	Ein automatisierter Workflow sollte eingerichtet werden, um die Zeugnisse systematisch zu erstellen und zu verwalten.
Lösung	Implementierung eines Workflow-Management-Systems, das die Erstellung, Überprüfung und Freigabe von Zeugnissen automatisiert.
Bewertung	Die Implementierung eines Workflow-Systems kann die Effizienz und Konsistenz bei der Zeugniserstellung erheblich verbessern. Dies erfordert jedoch eine sorgfältige Planung und möglicherweise Anpassungen der bestehenden Systeme. Die Implementierung von

	Workflows und Dokumentationssystemen gehört in vielen Unternehmen und Organisationen zu Routineaufgaben, um eine hohe Datenqualität zu erreichen oder Prozesse zu unterstützen (z.B. Anlage von Stammdaten eines Artikels oder Kundenauftrags). Die IT-Leitung der FERNFH beurteilt die Einführung eines solchen Systems als machbar.

6.2.1.3 Rechtliche Aspekte

Einhaltung der Datenschutzgrundverordnung (DSGVO)

Anforderung	Die Erfassung und Verarbeitung personenbezogener Daten muss den Anforderungen der DSGVO entsprechen.
Lösung	Durchführung einer Datenschutz-Folgenabschätzung (DSFA), um die Risiken der Datenverarbeitung zu identifizieren und zu minimieren. Implementierung von Datenschutzmaßnahmen wie Pseudonymisierung und Zugriffskontrollen.
Bewertung	Die Einhaltung der DSGVO erfordert detaillierte Planung und fortlaufende Überwachung. Die Durchführung einer DSFA ist ein eventuell notwendiger Schritt, um die Rechtmäßigkeit der Datenverarbeitung sicherzustellen. Die Einhaltung von DSGVO-Vorgaben steht besonders im Fokus und kann eine große Herausforderung darstellen, die aber mit entsprechenden technischen Lösungsansätzen umgangen bzw. eingehalten werden können (vgl. Kapitel 4.1.4). Die IT-Leitung der FERNFH bestätigt bereits vorhandene Zugriffskontrollen und die Einhaltung der gesetzlichen Vorschriften, und beurteilt diese Anforderung daher als machbar.

Einholung der Einwilligung der Studierenden

Anforderung	Vor der digitalen Verarbeitung ihrer Daten müssen die Einwilligungen der Studierenden eingeholt werden.
Lösung	Entwicklung und Implementierung eines Verfahrens zur Einholung und Dokumentation der Einwilligungen.
Bewertung	Die Einholung der Einwilligungen ist rechtlich notwendig und organisatorisch umsetzbar. Es muss jedoch sichergestellt werden, dass die Einwilligungen korrekt dokumentiert und aufbewahrt werden. Die IT-Leitung der FERNFH bestätigt, dass die Einwilligungen bereits

	im Zuge der Unterzeichnung des Ausbildungsvertrages eingeholt werden. Diese Anforderung wird als machbar eingestuft.

6.2.1.4 Zusammenfassung der Machbarkeitsanalyse für den 1. Prozessschritt

Die Erstellung eines digitalen Zeugnisses unter Berücksichtigung technischer, organisatorischer und rechtlicher Aspekte ist technisch machbar, organisatorisch umsetzbar und rechtlich durchführbar. Es erfordert jedoch eine sorgfältige Planung und die Bereitstellung entsprechender Ressourcen. Die technische Infrastruktur muss teilweise angepasst werden, und es sind Schulungsmaßnahmen sowie detaillierte Prozessdokumentationen erforderlich. Rechtlich ist die Einhaltung der DSGVO von zentraler Bedeutung, wofür entsprechende Datenschutzmaßnahmen bereits implementiert wurden.

6.2.2 Prozessschritt 2: Digitale Signatur des Zeugnisses

6.2.2.1 Technische Aspekte

Anwendung einer digitalen Signatur auf das PDF-Dokument

Anforderung	Die digitalen Zeugnisse müssen mit einer digitalen Signatur versehen werden, um deren Echtheit zu gewährleisten.
Lösung	Einsatz von Softwarelösungen wie Adobe Acrobat, DocuSign oder Open Source Alternativen wie OpenSSL, die die Signierung von PDF-Dokumenten unterstützen.
Bewertung	Es muss sichergestellt werden, dass die gewählte Software kompatibel mit den vorhandenen IT-Systemen ist und die Anforderungen an Sicherheit und Benutzerfreundlichkeit erfüllt. Die Integration solcher Software in bestehende Systeme der FERNFH ist technisch machbar und sogar teilweise bereits vorhanden. Bei vielen Unternehmen und Institutionen ist beispielsweise das Signieren von Rechnungen aufgrund von rechtlichen Vorgaben ein fester Bestandteil und hat sich als Prozess etabliert. Zudem gibt es auf dem Markt unzählige Bibliotheken und Softwarelösungen, die eine digitale Signatur von PDF-Dokumenten problemlos ermöglichen. Diese Anforderung wird daher als machbar eingestuft.

Speicherung des Hash-Wertes in der Blockchain

Anforderung	Der Hash-Wert des signierten Dokuments muss in einer Blockchain gespeichert werden, um die Integrität des Zeugnisses sicherzustellen.

Lösung	Implementierung einer Blockchain-Infrastruktur (z.B. Ethereum, Hyperledger[101]) zur Speicherung der Hash-Werte.
Bewertung	Die Einrichtung einer Blockchain ist laut IT-Leitung der FERNFH technisch anspruchsvoll, aber mit den richtigen Ressourcen und Fachkenntnissen durchführbar. Es muss eine geeignete Blockchain-Plattform ausgewählt werden, die die Anforderungen an Sicherheit und Skalierbarkeit erfüllt (vgl. Kapitel 3.1 und 4.1.3). Einige Projekte, nicht nur im Bildungssektor, haben bereits bewiesen, dass diese Anforderung aufgrund der vorhandenen Vielfalt an Blockchain-Typen und -Plattformen als machbar eingestuft werden kann (vgl. Kapitel 5).

6.2.2.2 Organisatorische Aspekte

Festlegung und Dokumentation der Verantwortlichkeiten

Anforderung	Klare Zuordnung der Verantwortlichkeiten für die Erstellung, Signierung und Verwaltung der digitalen Zeugnisse.
Lösung	Erstellung eines Organisationsplans, der die Verantwortlichkeiten definiert und dokumentiert.
Bewertung	Die Festlegung von Verantwortlichkeiten ist organisatorisch gut umsetzbar und erfordert klare Kommunikationsstrukturen (vgl. Kapitel 4.2). Es ist wichtig, dass alle Beteiligten ihre Rollen und Aufgaben verstehen. Die IT-Leitung der FERNFH bestätigt einen bereits vorhandenen Organisationsplan, in dem Verantwortlichkeiten klar definiert sind. Diese Anforderung gilt daher als machbar.

Schulung der Mitarbeiter*innen der FERNFH im Umgang mit der Signatursoftware und der Blockchain-Technologie

Anforderung	Mitarbeiter müssen im Umgang mit der Signatursoftware und der Blockchain-Technologie geschult werden.
Lösung	Durchführung von Schulungen und Workshops, um das technische Wissen und die praktischen Fähigkeiten der Mitarbeiter*innen der FERNFH zu erweitern.

[101] Hyperledger Foundation, 2015

Bewertung	Schulungsprogramme sind notwendig und organisatorisch gut durchführbar. Es ist wichtig, regelmäßige Schulungen anzubieten, um sicherzustellen, dass die Mitarbeiter*innen auf dem neuesten Stand der Technologie bleiben. Diese Schulungsprogramme können von der IT-Abteilung der FERNFH durchgeführt werden. Diese Anforderung gilt als machbar.

6.2.2.3 Rechtliche Aspekte

Sicherstellung, dass die verwendete Signaturtechnologie den rechtlichen Anforderungen entspricht

Anforderung	Die digitale Signatur muss den rechtlichen Anforderungen entsprechen.
Lösung	Auswahl und Implementierung von Signaturtechnologien, die rechtskonform sind. Zusammenarbeit mit rechtlichen Experten zur Überprüfung der Konformität.
Bewertung	Die Auswahl einer rechtskonformen Signaturtechnologie ist eventuell rechtlich notwendig und technisch machbar. Es erfordert jedoch eine sorgfältige Prüfung und Auswahl der geeigneten Technologie. Aus Sicht der IT-Leitung ist diese Anforderung technisch gut umsetzbar und daher machbar.

Dokumentation und Archivierung der digitalen Signaturprozesse zur Nachweisbarkeit

Anforderung	Alle Schritte im Signaturprozess müssen dokumentiert und archiviert werden, um die Nachweisbarkeit zu gewährleisten.
Lösung	Implementierung eines Dokumentationssystems, das alle Signaturprozesse erfasst und speichert.
Bewertung	Die Dokumentation und Archivierung sind notwendig und organisatorisch gut umsetzbar. Es erfordert jedoch die Implementierung geeigneter Systeme und Prozesse zur Erfassung und Speicherung der Daten. Die IT-Leitung ist sich nicht sicher, ob eine rechtliche Notwendigkeit besteht, sieht aber in der technischen Umsetzung keine Hürden. Eine Rechtsberatung würde Klarheit schaffen. Diese Anforderung gilt daher als machbar.

6.2.2.4 Zusammenfassung der Machbarkeitsanalyse für den 2. Prozessschritt

Die Anwendung einer digitalen Signatur auf das Zeugnis und die Speicherung des Hash-Wertes in der Blockchain sind technisch machbar, organisatorisch umsetzbar und rechtlich durchführbar. Technisch erfordert dies die Integration von Signatursoftware und die Implementierung einer Blockchain-Infrastruktur. Organisatorisch müssen Verantwortlichkeiten klar definiert und Mitarbeiter*innen der FERNFH entsprechend geschult werden. Rechtlich ist sicherzustellen, dass die verwendete Signaturtechnologie den gesetzlichen Anforderungen entspricht und alle Prozesse dokumentiert und archiviert werden. Mit einer sorgfältigen Planung und Umsetzung können diese Anforderungen erfüllt werden, was die Echtheit und Integrität von digitalen Zeugnissen gewährleistet.

6.2.3 Prozessschritt 3: Speicherung in der Blockchain

6.2.3.1 Technische Aspekte

Implementierung der Blockchain-Technologie zur Speicherung von Zeugnis-Hashes

Anforderung	Es muss eine Blockchain-Infrastruktur implementiert werden, um die Zeugnis-Hashes sicher und unveränderlich zu speichern.
Lösung	Auswahl einer geeigneten Blockchain-Plattform (z.B. Ethereum, Hyperledger Fabric[102]) und deren Implementierung. Ethereum ist bekannt für seine Contract-Funktionalität, die sich hervorragend für die Erstellung und Verwaltung von digitalen Zeugnissen eignen würde, hat zudem eine große Entwicklergemeinschaft und viele vorhandene Tools und Bibliotheken, die den Entwicklungsprozess erleichtern. Als Nachteil sind hohe Transaktionskosten und die Skalierbarkeit anzuführen. Bei Hyperledger Fabric handelt es sich um eine permissioned Blockchain und bietet somit mehr Kontrolle und Datenschutz, da nur autorisierte Teilnehmer*innen Transaktionen durchführen und validieren können. Als Nachteil ist eine hohe Komplexität anzuführen.
Bewertung	Die Implementierung einer Blockchain-Technologie erfordert fundierte technische Kenntnisse und eine sorgfältige Auswahl der Plattform. Es ist technisch machbar, wenn die erforderlichen Ressourcen und das Fachwissen vorhanden sind. Die Sicherheit und Skalierbarkeit der

[102] Hyperledger Foundation, 2015

	Plattform müssen gewährleistet sein. Diese Anforderung ist aus Sicht der IT-Abteilung der FERNFH mithilfe von externen Experten machbar.

Einrichtung eines Netzwerks aus Nodes

Anforderung	Ein Netzwerk aus Nodes muss eingerichtet werden, die die Blockchain-Daten speichern und verifizieren.
Lösung	Konfiguration und Verteilung der Nodes auf verschiedene Serverstandorte zur Erhöhung der Redundanz und Sicherheit.
Bewertung	Die Einrichtung eines Netzwerks aus Nodes ist technisch machbar, erfordert jedoch eine gründliche Planung der Infrastruktur und der Sicherheitsmaßnahmen. Eine verteilte Netzwerkarchitektur erhöht die Zuverlässigkeit und Sicherheit (vgl. Kapitel 2.3.4). Laut der IT-Leitung der FERNFH werden Cloud-Infrastrukturen von IT-Partnern genutzt, die eine verteilte Server-Infrastruktur erlauben. Diese Anforderung wird als machbar eingestuft.

6.2.3.2 Organisatorische Aspekte

Festlegung der beteiligten Institutionen und deren Rolle im Blockchain-Netzwerk

Anforderung	Die Rolle und Verantwortung der beteiligten Institutionen müssen klar definiert werden.
Lösung	Erstellung eines Konsortialvertrags oder einer Vereinbarung, die die Zusammenarbeit und die Rollen der beteiligten Institutionen regelt.
Bewertung	Laut IT-Leitung der FERNFH sind und wären keine weiteren Institutionen an der Erstellung von digitalen Zeugnissen beteiligt. Es besteht daher kein weiterer Handlungsbedarf. Diese Anforderung wird als machbar eingestuft.

Implementierung von Backup- und Wiederherstellungsmechanismen

Anforderung	Es müssen Mechanismen zur Sicherung und Wiederherstellung der Blockchain-Daten implementiert werden.
Lösung	Einrichtung von regelmäßigen Backups und die Entwicklung eines Notfallwiederherstellungsplans.
Bewertung	Die Implementierung von Backup- und Wiederherstellungsmechanismen ist organisatorisch umsetzbar und

	notwendig, um die Datenintegrität und Verfügbarkeit sicherzustellen. Die IT-Leitung der FERNFH bestätigt bereits vorhandene Mechanismen zur Sicherung und Wiederherstellung von Daten, sowie einem IT-Notfallplan. Diese Anforderung wird als machbar eingestuft.

6.2.3.3 Rechtliche Aspekte

Sicherstellung, dass keine personenbezogenen Daten direkt in der Blockchain gespeichert werden

Anforderung	Die Speicherung von personenbezogenen Daten in der Blockchain muss vermieden werden, um DSGVO-Konformität zu gewährleisten.
Lösung	Speicherung von Hash-Werten anstelle von personenbezogenen Daten in der Blockchain. Zusätzliche personenbezogene Daten werden in einer separaten, sicheren Datenbank gespeichert.
Bewertung	Die rechtlichen Anforderungen zur Vermeidung der Speicherung personenbezogener Daten in der Blockchain sind umsetzbar. Dies erfordert eine klare Trennung der Daten und die Implementierung sicherer Datenbanklösungen (vgl. Kapitel 4.3.1). Die IT-Leitung der FERNFH sieht diese Anforderung als machbar an. Mögliche technische Lösungen (z.B. durch Speichern einer Prüfsumme oder Hash-Wertes auf der Blockchain, anstatt personenbezogener Daten) unterstreichen die Machbarkeit der Anforderung.

Einhaltung der gesetzlichen Vorgaben zur Datenaufbewahrung und -löschung

Anforderung	Es müssen Mechanismen zur Einhaltung der gesetzlichen Vorgaben zur Datenaufbewahrung und -löschung implementiert werden.
Lösung	Entwicklung von Prozessen zur Verwaltung der Datenlebenszyklen, einschließlich der sicheren Löschung von Daten gemäß den gesetzlichen Anforderungen.
Bewertung	Die Einhaltung der gesetzlichen Vorgaben zur Datenaufbewahrung und -löschung erfordert rechtliche Beratung und die Implementierung entsprechender Prozesse und Technologien. Es ist organisatorisch und technisch machbar, erfordert jedoch sorgfältige Planung und Überwachung, sowie eine strikte Trennung von Zeugnisdaten und personenbezogener Daten (vgl. Kapitel 4.3.1). Ein entsprechendes Mapping der Daten auf einer klassischen Datenbank ermöglicht somit die Löschung von Daten. Die IT-Leitung der FERNFH löscht bereits

	personenbezogene Daten im Rahmen der gesetzlichen Vorgaben der DSGVO. Diese Anforderung wird daher als machbar eingestuft.

6.2.3.4 Zusammenfassung der Machbarkeitsanalyse für den 3. Prozessschritt

Die Speicherung der Zeugnis-Hashes in der Blockchain ist technisch machbar, organisatorisch umsetzbar und rechtlich durchführbar. Technisch erfordert dies die Implementierung einer geeigneten Blockchain-Plattform und die Einrichtung eines Netzwerks aus Nodes. Organisatorisch müssen Backup- sowie Wiederherstellungsmechanismen eventuell erweitert werden. Rechtlich ist sicherzustellen, dass keine personenbezogenen Daten direkt in der Blockchain gespeichert werden und alle gesetzlichen Vorgaben zur Datenaufbewahrung und -löschung eingehalten werden. Mit einer sorgfältigen Planung und Umsetzung können diese Anforderungen erfüllt werden, wodurch die Sicherheit und Integrität von digitalen Zeugnissen gewährleistet wird.

6.2.4 Prozessschritt 4: Bereitstellung und Abruf des digitalen Zeugnisses

6.2.4.1 Technische Aspekte

Entwicklung eines Portals für den Abruf der digitalen Zeugnisse

Anforderung	Ein sicheres und benutzerfreundliches Online-Portal muss entwickelt werden, über das Studierende ihre digitalen Zeugnisse abrufen können.
Lösung	Einsatz von Webentwicklungstechnologien wie HTML, CSS, JavaScript für die Frontend-Entwicklung und sichere Backend-Technologien wie Node.js, Python/Django oder Ruby on Rails. Integration von Datenbanklösungen für die Verwaltung der Daten von Studierenden.
Bewertung	Die Entwicklung eines Portals ist lt. IT-Leitung der FERNFH technisch machbar und kann mit den richtigen Ressourcen und Fachkenntnissen innerhalb eines angemessenen Zeitrahmens durchgeführt werden. Sicherheitsmaßnahmen wie HTTPS, SSL/TLS-Verschlüsselung und regelmäßige Sicherheitsüberprüfungen sind notwendig. Der bereits vorhandene Online-Campus der FERNFH erfüllt die notwendigen Anforderungen und kann somit als machbar eingestuft werden.

Implementierung von Schnittstellen für Arbeitgeber*innen und Institutionen

Anforderung	Es müssen Schnittstellen (APIs) oder ein Webportal entwickelt werden, über die Arbeitgeber*innen und andere Institutionen die Echtheit der Zeugnisse verifizieren können.
Lösung	Entwicklung von RESTful APIs, die den sicheren Zugriff auf die Zeugnisdaten ermöglichen. Verwendung von OAuth 2.0 oder anderen Authentifizierungsprotokollen zur Sicherstellung der Zugriffskontrollen. Implementierung eines Webportals, ähnlich dem Zeugnisportal für Studierende.
Bewertung	Die Entwicklung von APIs ist laut IT-Leitung der FERNFH technisch gut umsetzbar und ermöglicht eine flexible Integration in verschiedene Systeme von Drittanbietern. Ein Webportal, ähnlich dem Zeugnisportal für Studierende, stellt technisch keine große Herausforderung dar. Die Sicherheit der Schnittstellen muss durch geeignete Authentifizierungs- und Autorisierungsmechanismen gewährleistet werden. Diese Methoden sind bereits im Online-Campus implementiert. Diese Anforderung wird als machbar eingestuft.

6.2.4.2 Organisatorische Aspekte

Schulung der Studierenden und potenziellen Zeugnisprüfer*innen im Umgang mit dem digitalen Portal

Anforderung	Alle Nutzergruppen müssen im Umgang mit dem digitalen Portal geschult werden, um eine reibungslose Nutzung zu gewährleisten. Alternativ müssen entsprechende Anleitungen (z.B. Online über ein Webportal) zur Verfügung gestellt werden.
Lösung	Durchführung von Schulungen, Workshops und Erstellung von Anleitungen und Tutorials für Studierende und Zeugnisprüfer*innen.
Bewertung	Schulungsmaßnahmen und das zur Verfügung stellen von Anleitungen sind organisatorisch gut umsetzbar und notwendig, um sicherzustellen, dass alle Nutzer*innen die Funktionen des Portals verstehen und effektiv nutzen können. Die Schulungen und Anleitungen können kontinuierlich angeboten bzw. aktualisiert und von der IT-Abteilung der FERNFH durchgeführt werden. Diese Anforderung wird als machbar eingestuft.

Festlegung der Prozesse für den Abruf und die Überprüfung der Zeugnisse

Anforderung	Es müssen klare Prozesse definiert werden, die den Abruf und die Überprüfung der Zeugnisse regeln.
Lösung	Erstellung von Prozessdokumentationen und Checklisten, die die Schritte für den Abruf und die Überprüfung detailliert beschreiben.
Bewertung	Die Definition und Dokumentation der Prozesse sind laut IT-Leitung der FERNFH organisatorisch gut durchführbar. Es ist wichtig, klare Anweisungen und Verantwortlichkeiten festzulegen, um die Effizienz und Zuverlässigkeit der Prozesse zu gewährleisten. Diese Anforderung wird als machbar eingestuft.

6.2.4.3 Rechtliche Aspekte

Sicherstellung des sicheren und datenschutzkonformen Zugriffs auf das Zeugnisportal

Anforderung	Der Zugang zum Zeugnisportal muss sicher und datenschutzkonform gestaltet sein.
Lösung	Implementierung von Authentifizierungs- und Autorisierungsmechanismen, z.B. Zwei-Faktor-Authentifizierung (2FA) und rollenbasierte Zugriffskontrollen. Einhaltung der Datenschutzbestimmungen der DSGVO.
Bewertung	Die Implementierung von Sicherheits- und Datenschutzmaßnahmen ist rechtlich notwendig und technisch machbar. Es erfordert kontinuierliche Überwachung und Anpassung an aktuelle Sicherheitsstandards. Die IT-Abteilung der FERNFH hat bereits Authentifizierungs- und Autorisierungsmaßnahmen in Form einer 2FA im Bereich der Mitarbeiter*innen implementiert. Der Bereich für Studierende wird aktuell umgesetzt. Diese Anforderung wird als machbar eingestuft.

Implementierung von Authentifizierungsmechanismen zur Verhinderung unbefugter Zugriffe

Anforderung	Es müssen Mechanismen implementiert werden, die unbefugte Zugriffe auf das Zeugnisportal verhindern.

Lösung	Nutzung von modernen Authentifizierungsprotokollen wie beispielsweise OAuth 2.0 und die Implementierung von Sicherheitsfunktionen wie IP-Whitelisting und Captchas.
Bewertung	Die Implementierung von Authentifizierungsmechanismen ist laut IT-Leitung der FERNFH technisch machbar und notwendig, um die Sicherheit der Zeugnisdaten zu gewährleisten (vgl. Kapitel 4.1.1). Es muss darauf geachtet werden, dass diese Mechanismen den Nutzer*innen eine gute Balance zwischen Sicherheit und Benutzerfreundlichkeit bieten. Aktuell sind diese Mechanismen in allen möglichen Ausprägungen implementiert. Diese Anforderung wird als machbar eingestuft.

6.2.4.4 Zusammenfassung der Machbarkeitsanalyse für den 4. Prozessschritt

Die Bereitstellung und der Abruf der digitalen Zeugnisse über ein Online-Portal sind technisch machbar, organisatorisch umsetzbar und rechtlich durchführbar. Technisch erfordert dies die Anpassung und Erweiterung eines bereits exitstierenden Web-Portals, sowie die Implementierung von Schnittstellen für externe Prüfer*innen. Organisatorisch müssen Schulungen für alle Nutzergruppen durchgeführt und klare Prozesse für den Abruf und die Überprüfung der Zeugnisse definiert werden. Rechtlich ist sicherzustellen, dass der Zugang zum Portal sicher und datenschutzkonform gestaltet ist. Mit einer sorgfältigen Planung und Umsetzung können diese Anforderungen erfüllt werden, wodurch die Nutzung und Verifizierung der digitalen Zeugnisse effizient und sicher gestaltet werden kann.

6.2.5 Prozessschritt 5: Verifizierung des digitalen Zeugnisses

6.2.5.1 Technische Aspekte

Nutzung der Blockchain zur Verifizierung des Hash-Wertes des digitalen Zeugnisses

Anforderung	Der Hash-Wert des digitalen Zeugnisses muss sicher in der Blockchain gespeichert und jederzeit zur Verifizierung abrufbar sein.
Lösung	Implementierung von APIs zur Abfrage des Hash-Wertes aus der Blockchain, die die Verifizierung des Hash-Wertes ermöglichen.
Bewertung	Die Nutzung der Blockchain zur Verifizierung ist technisch machbar und bietet hohe Sicherheit und Unveränderlichkeit. Die Implementierung erfordert fundiertes Wissen über die Blockchain-Technologie. Laut der IT-Leitung der FERNFH kann diese Anforderung mit externen Experten umgesetzt werden. Diese Anforderung wird als machbar eingestuft.

Bereitstellung einer Benutzeroberfläche zur einfachen Überprüfung der Zeugnisauthentizität

Anforderung	Es muss eine benutzerfreundliche Oberfläche entwickelt werden, über die Arbeitgeber*innen und andere Institutionen die Echtheit der Zeugnisse überprüfen können.
Lösung	Entwicklung eines frei zugänglichen Web-Interfaces, welches das Hochladen eines Zeugnisses im PDF-Format ermöglicht und die Verifizierungsergebnisse anzeigt.
Bewertung	Die Entwicklung einer solchen Benutzeroberfläche ist nach Angabe der IT-Leitung der FERNFH technisch machbar. Es erfordert jedoch sorgfältige Planung und Design, um sicherzustellen, dass die Benutzeroberfläche intuitiv und leicht verständlich ist. Diese Anforderung wird als machbar eingestuft.

6.2.5.2 Organisatorische Aspekte

Einrichtung von Helpdesk- und Support-Strukturen zur Unterstützung bei der Verifizierung

Anforderung	Es muss ein Support-System eingerichtet werden, das Nutzer*innen bei der Verifizierung der Zeugnisse hilft.
Lösung	Aufbau eines Helpdesks mit geschultem Personal, das bei Fragen und Problemen zur Verfügung steht. Erstellung von FAQs und Support-Dokumentationen.
Bewertung	Die Einrichtung eines Helpdesks und die Erstellung von Support-Dokumentationen sind organisatorisch gut umsetzbar. Es erfordert jedoch Ressourcen für die Schulung des Personals und die kontinuierliche Pflege der Dokumentationen. Nach Auskunft der IT-Leitung der FERNFH ist ein Support-Team bereits vorhanden. Diese Anforderung wird als machbar eingestuft.

Dokumentation der Verifizierungsprozesse und -protokolle

Anforderung	Alle Verifizierungsprozesse müssen dokumentiert und die Protokolle gespeichert werden, um die Nachvollziehbarkeit zu gewährleisten.

Lösung	Implementierung eines Systems zur automatischen Protokollierung aller Verifizierungsvorgänge. Erstellung und Pflege von Prozessdokumentationen.
Bewertung	Die Dokumentation und Protokollierung sind laut IT-Leitung der FERNFH organisatorisch notwendig und bereits vorhanden. Es muss sichergestellt werden, dass die Systeme zur Protokollierung sicher und zuverlässig arbeiten. Diese Anforderung wird als machbar eingestuft.

6.2.5.3 Rechtliche Aspekte

Sicherstellung, dass die Verifizierungsprozesse transparent und nachvollziehbar sind

Anforderung	Die Verifizierungsprozesse müssen transparent und nachvollziehbar gestaltet sein, um rechtliche Anforderungen zu erfüllen.
Lösung	Dokumentation aller Schritte des Verifizierungsprozesses und Bereitstellung dieser Informationen für autorisierte Nutzer*innen. Einhaltung von gesetzlichen Anforderungen und Best Practices zur Transparenz.
Bewertung	Die Sicherstellung der Transparenz und Nachvollziehbarkeit ist notwendig und organisatorisch umsetzbar. Es erfordert die Entwicklung und Implementierung klarer Prozesse und deren konsequente Dokumentation. Aus Sicht der IT-Leitung der FERNFH ist nicht ganz klar, ob tatsächlich eine rechtliche Notwendigkeit besteht, sieht aber in der technischen Umsetzung mit Unterstützung einer rechtlichen Beratung keine Hürden. Diese Anforderung wird als machbar eingestuft.

Einbindung rechtlicher Expert*innen zur kontinuierlichen Überwachung und Anpassung der Verifizierungsprozesse

Anforderung	Rechtliche Expert*innen müssen eingebunden werden, um die Verifizierungsprozesse kontinuierlich zu überwachen und an gesetzliche Änderungen anzupassen.
Lösung	Regelmäßige Konsultation mit Datenschutzbeauftragten und rechtlichen Berater*innen. Durchführung regelmäßiger Audits und Überprüfungen der Verifizierungsprozesse.

Bewertung	Die Einbindung rechtlicher Expert*innen ist notwendig, um die rechtliche Konformität zu gewährleisten. Es erfordert kontinuierliche Zusammenarbeit und regelmäßige Überprüfungen. An der FERNFH ist bereits die Funktion als Datenschutzbeauftragte*r eingerichtet. Audits werden alle vier Jahre durchgeführt. Die Anforderung gilt als machbar.

6.2.5.4 Zusammenfassung der Machbarkeitsanalyse für den 5. Prozessschritt

Die Verifizierung der digitalen Zeugnisse über die Blockchain ist technisch machbar, organisatorisch umsetzbar und rechtlich durchführbar. Technisch erfordert dies die Implementierung und Entwicklung einer benutzerfreundlichen Verifizierungsoberfläche. Organisatorisch können vorhandene Helpdesk- und Support-Strukturen verwendet, sowie Verifizierungsprozesse dokumentiert und protokolliert werden. Rechtlich ist sicherzustellen, dass die Verifizierungsprozesse transparent und nachvollziehbar sind und kontinuierlich überwacht werden. Mit einer sorgfältigen Planung und Umsetzung können diese Anforderungen erfüllt werden, wodurch die Echtheit und Integrität der digitalen Zeugnisse zuverlässig überprüft werden können.

7. Fazit

In Kapitel 6.2 wurde die Machbarkeit der Einführung von Blockchain-Technologie an der FERNFH, für die Ausstellung von Blockchain basierten Zeugnissen, untersucht. Dabei wurden technische, organisatorische und rechtliche Aspekte umfassend analysiert. Die Ergebnisse zeigen, dass alle Anforderungen als machbar eingestuft werden können.

7.1 Zusammenfassung der Ergebnisse

7.1.1 Technische Machbarkeit

Technisch bietet die Blockchain-Technologie erhebliche Vorteile in Bezug auf Sicherheit, Transparenz und Unveränderlichkeit digitaler Zeugnisse. Die dezentrale Natur der Blockchain reduziert das Risiko von „Single-Points-of-Failure“ und erhöht die System Resilienz gegenüber Angriffen. Die Implementierung kryptographischer Techniken zur Sicherstellung der Authentizität und Integrität der Zeugnisse ist problemlos möglich. Herausforderungen wie die Anforderungen an die Netzwerkinfrastruktur, die Skalierbarkeit von Transaktionen und die Integration in bestehende IT-Systeme sind durch sorgfältige Planung und geeignete Maßnahmen lösbar. Die Implementierung der Blockchain erfordert fundierte technische Kenntnisse und eine sorgfältige Auswahl der Plattform. Es ist technisch machbar, wenn die erforderlichen Ressourcen und das Fachwissen vorhanden sind.

7.1.2 Organisatorische Machbarkeit

Organisatorisch erfordert die erfolgreiche Implementierung der Blockchain-Technologie umfassende Maßnahmen. Die Einführung muss durch Schulungsprogramme unterstützt werden, die alle Beteiligten mit den Grundlagen der Blockchain-Technologie, spezifischen Anwendungsfällen und Best Practices vertraut machen. Fortlaufende Schulungen und Workshops sind notwendig, um sicherzustellen, dass die Kenntnisse aktuell bleiben und die IT-Mitarbeiter*innen über die erforderlichen Kompetenzen verfügen. Diese Maßnahmen werden dazu beitragen, die Akzeptanz der neuen Technologie zu fördern und eine reibungslose Einführung zu gewährleisten. Die FERNFH hat bereits die notwendigen Voraussetzungen geschaffen, um diese organisatorischen Herausforderungen zu bewältigen.

7.1.3 Rechtliche Machbarkeit

Rechtlich steht der Einführung der Blockchain-Technologie nichts im Wege, sofern die geltenden Vorschriften beachtet werden. Die Einhaltung der Datenschutzbestimmungen der DSGVO wird durch Maßnahmen wie Anonymisierung und Pseudonymisierung personenbezogener Daten, sowie die Sicherstellung des Rechts auf Löschung gewährleistet. Die rechtlichen Rahmenbedingungen müssen mithilfe von

Datenschutzbeauftragten oder rechtlichen Berater*innen gründlich geprüft und interne Richtlinien gegebenenfalls angepasst werden, um die rechtskonforme Nutzung der Blockchain-Technologie zu ermöglichen. Die rechtliche Prüfung hat gezeigt, dass die FERNFH in der Lage ist, diese Anforderungen zu erfüllen und somit die Blockchain-Technologie rechtskonform zu nutzen.

7.2 Beantwortung der Forschungsfrage

Die unter Kapitel 1.3.2 beschriebene Hypothese konnte bestätigt werden:

Die Ausstellung von Blockchain basierten Zeugnissen an der Ferdinand Porsche FERNFH ist in Bezug auf technische, organisatorische und rechtliche Aspekte machbar.

7.3 Ausblick

Diese Arbeit hat gezeigt, dass die Einführung der Blockchain-Technologie zur Verwaltung und Verifizierung digitaler Zeugnisse an der FERNFH sowohl technisch, organisatorisch als auch rechtlich machbar ist. Die umfangreiche Analyse der technischen Infrastruktur, der erforderlichen organisatorischen Maßnahmen und der rechtlichen Rahmenbedingungen hat ergeben, dass die FERNFH gut positioniert ist, um diese innovative Technologie zu implementieren und ihre zahlreichen Vorteile zu nutzen.

Weltweit gibt es bereits einige erfolgreiche Blockchain-Projekte an verschiedenen Hochschulen. Diese Projekte haben gezeigt, dass die Technologie nicht nur theoretisch, sondern auch praktisch umsetzbar ist. Hochschulen wie das Massachusetts Institute of Technology (MIT) und die Open University in Großbritannien haben Blockchain-Technologien zur Verwaltung von Zertifikaten und Zeugnissen eingeführt und damit positive Erfahrungen gemacht. Diese Beispiele dienen als wertvolle Referenz und Motivation für die FERNFH, ähnliche Initiativen zu ergreifen.

In dieser Arbeit wurden einige wichtige Aspekte nicht ausführlich behandelt, wie zum Beispiel die wirtschaftliche Machbarkeit der Einführung der Blockchain-Technologie. Wirtschaftliche Überlegungen, wie die Kosten für die Implementierung und den laufenden Betrieb der Technologie sowie mögliche Einsparungen und Effizienzsteigerungen, sind entscheidend für eine umfassende Bewertung. Zukünftige Untersuchungen sollten diese wirtschaftlichen Aspekte detailliert analysieren, um ein möglichst vollständiges Bild der Machbarkeit und Sinnhaftigkeit zu erhalten.

Die Sinnhaftigkeit der Blockchain-Technologie für den geprüften Anwendungsfall an der FERNFH kann diskutiert werden. Eine höhere Sinnhaftigkeit ergibt sich jedoch, wenn beispielsweise mehrere Hochschulen ein gemeinsames Blockchain-Netzwerk nutzen. Ein solches Netzwerk würde die Interoperabilität und den Datenaustausch zwischen verschiedenen Institutionen erleichtern und die Vorteile der Technologie weiter verstärken. Durch die Zusammenarbeit mehrerer Hochschulen könnte ein

standardisiertes und weit verbreitetes System zur Verifizierung von Bildungsnachweisen entstehen, das die Akzeptanz und Nutzung der Blockchain-Technologie im Bildungssektor erheblich fördern würde.

Zusammenfassend lässt sich sagen, dass die Einführung der Blockchain-Technologie zur Verwaltung digitaler Zeugnisse an der FERNFH technisch, organisatorisch und rechtlich machbar ist. Die positiven Erfahrungen anderer Hochschulen weltweit und die umfassende Analyse der Machbarkeit in dieser Arbeit legen nahe, dass die FERNFH gut positioniert ist, um diese innovative Technologie zu implementieren. Zukünftige Untersuchungen sollten die wirtschaftlichen Aspekte weiter beleuchten und die Möglichkeiten der Zusammenarbeit mit anderen Hochschulen erkunden, um die volle Sinnhaftigkeit und das Potenzial der Blockchain-Technologie im Bildungssektor auszuschöpfen.

Die FERNFH steht vor der spannenden Möglichkeit, eine Vorreiterrolle bei der Einführung der Blockchain-Technologie im Bildungsbereich zu übernehmen und damit die Zukunft der digitalen Bildungsnachweise maßgeblich zu gestalten.

Literaturverzeichnis

Antonopoulos, A. M. (2018). *Bitcoin & Blockchain - Grundlagen und Programmierung: Die Blockchain verstehen, Anwendungen entwickeln.* (P. Klicman, Übers.) Sebastopol, USA: O'Reilly.

A-Trust. (2024). Abgerufen am 29. Mai 2024 von A-Trust: https://www.a-trust.at/de/

Bartek, M., & Goudz, A. (2019). *Blockchain-Technologie in der Energiewirtschaft* (1 Ausg.). Springer Vieweg Berlin, Heidelberg. doi:10.1007/978-3-662-60568-4

Berghoff, C., Gebhardt, U., Lochter, M., & Maßberg, S. (März 2019). *Bundesamt für Sicherheit in der Informationstechnik.* (B. f. (BSI), Hrsg.) Abgerufen am 18. Jänner 2024 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3

Bild.de. (06. 12 2017). Abgerufen am 03. 12 2021 von https://www.bild.de/news/ausland/bitcoin/81-millionen-euro-weg-brite-schmeisst-festplatte-auf-den-muell-54098636.bild.html

Bitpanda. (08. Jänner 2024). *Bitpanda*. Abgerufen am 08. Jänner 2024 von Bitpanda: https://www.bitpanda.com/academy/de/lektionen/was-ist-eine-bitcoin-node/

Bogensperger, A., Zeiselmair, A., Hinterstocker, M., Dossow, P., Hilpert, J., Wimmer, M., . . . Völter, F. (2021). *Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft?* Bayreuth: Bayreuther Arbeitspapiere zur Wirtschaftsinformatik, No. 68, Universität Bayreuth, Lehrstuhl für Wirtschaftsinformatik. doi:https://doi.org/10.15495/EPub_UBT_00005707

Bundesnetzagentur. (Juli 2021). *Bundesnetzagentur.* (G. T. Bundesnetzagentur für Elektrizität, Hrsg.) Abgerufen am 18. Februar 2024 von https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjEl9fk7emEAxU7VPEDHUu7Bzw4ChAWegQIFhAB&url=https%3A%2F%2Fwww.bundesnetzagentur.de%2FDE%2FFachthemen%2FDigitalisierung%2FTechnologien%2FBlockchain%2FLinks_Dokumente%2F

Burgwinkel, D. (2016). *Blockchain Advisory.* (D. Burgwinkel, Hrsg.) Berlin/Boston: De Gruyter Mouton. doi:978-3-11-048731-2

Chibber, J. (21. Juni 2021). *Dr. Datenschutz*. Abgerufen am 23. Februar 2024 von https://www.dr-datenschutz.de/digitales-schulzeugnis-datenschutz-mit-blockchain/

Drescher, D. (2017). *Blockchain Grundlagen* (1. Ausg.). (G. Lenz, Übers.) Frechen: mitp Verlags GmbH & Co. KG.

Espich, J. (27. März 2019). Potenziale der Blockchain-Technologie für die Finanzindustrie in Deutschland. Landshut, Deutschland.

Ferdinand Porsche FERNFH. (2023a). *Ferdinand Porsche FERNFH.* (Ferdinand Porsche FERNFH, Hrsg.) Abgerufen am 20. März 2024 von https://www.fernfh.ac.at/fileadmin/user_upload/FernFH/Presse/Basispressetexte/Geschichte_der_Ferdinand_Porsche_FERNFH.pdf

Ferdinand Porsche FERNFH. (2023b). *Ferdinand Porsche FERNFH.* (Ferdinand Porsche FERNFH, Hrsg.) Abgerufen am 20. März 2024 von https://www.fernfh.ac.at/fileadmin/user_upload/FernFH/Presse/Basispressetexte/11-2023_-_Daten_und_Fakten_FERNFH.pdf

Fill, H.-G., & Meier, A. (2019). *Blockchain kompakt - Grundlagen, Anwendungsoptionen und kritische Bewertung* (1 Ausg.). Springer Vieweg Wiesbaden. doi:10.1007/978

Fill, H.-G., & Meier, A. (2020). *Blockchain - Grundlagen, Anwendungsszenarien und Nutzungspotenziale.* Deutschland: Springer Fachmedien Wiesbaden GmbH. doi:10.1007/978-3-658-28006-2

Grech, A., Balaji, V., & Miao, F. (2022). *UNESCO.* doi:https://doi.org/10.56059/11599/4131

Haqshanas, R. (08. September 2023). *Techopedia*. Abgerufen am 13. Jänner 2024 von Techopedia: https://www.techopedia.com/de/die-rolle-von-layer-2-loesungen-bei-der-skalierung-von-blockchains

Hosp, J. (2018). *Blockchain 2.0 – einfach erklärt – mehr als nur Bitcoin.*

Hyperledger Foundation (Hrsg.). (17. 12 2015). *Hyperledger Fabric*. Abgerufen am 27. Mai 2024 von Hyperledger Fabric: https://wiki.hyperledger.org/display/fabric/Ecosystem

Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the Future of Digital Learning Credential Assessment and Management. *Journal of Teacher Education for Sustainability, 20*(1), 145-156. doi:10.2478/jtes-2018-0009

Kirstein, F., Lämmel, P., & Altenbernd, A. (2021). *Mythos Blockchain: Zwischen Hoffnung und Realität* (1. Ausg.). Berlin: Kompetenzzentrum Öffentliche IT - Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS.

Laaff, M. (17. Februar 2022). *Zeit Online*. Abgerufen am 12. November 2023 von Zeit Online: https://www.zeit.de

Laaff, M. (17. Februar 2022). *Zeit Online*. (Z. Online, Herausgeber) Abgerufen am 02. Jänner 2024 von https://www.zeit.de/digital/2022-02/digitale-zeugnisse-schule-blockchain-digitalisierung

Laurence, T. &. (2017). *Blockchain für Dummies* (Bd. 1. Aufl.). Wiley-VCH.

Metzger, J. (19. Februar 2018). *Gabler Wirtschaftslexikon*. Abgerufen am 28. Dezember 2023 von Gabler Wirtschaftslexikon: https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410/version-277444

Mitschele, A. (19. Februar 2018). *Gabler Wirschafslexikon*. Abgerufen am 23. November 2023 von Gabler Wirschafslexikon: https://wirtschaftslexikon.gabler.de/definition/blockchain-54161/version-277215

Moiseev, A. (31. Oktober 2018). *Kaspersky Daily*. Abgerufen am 14. Jänner 2024 von Kaspersky Daily: https://www.kaspersky.de/blog/blockchain-and-privacy/18026/

Müller, N. (24. Jänner 2024). *Chip.de*. Abgerufen am 16. März 2024 von https://www.chip.de/news/Sind-Sie-betroffen-Die-5-heftigsten-Hackerangriffe-in-Deutschland-2023_185110063.html

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Abgerufen am 19. 11 2021 von bitcoin.org: http://bitcoin.org/bitcoin.pdf

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

Pramer, P. (04. November 2021). *Der Standard*. Abgerufen am 13. Jänner 2024 von Der Standard: https://www.derstandard.at/story/2000130809343/bitcoin-frisst-so-viel-strom-wie-manche-staaten-muss-das

Schacht, S., & Lanquillon, C. (2019). *Blockchain und maschinelles Lernen.* (C. Lanquillon, Hrsg.) Deutschland: Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2019. doi:https://doi.org/10.1007/978-3-662-60408-3

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution* (4. Ausg.). (P. Pyka, Übers.) Plassen Verlag. doi:978-3-86470-388-1

Thylmann, M. (2021). *Bundesdruckerei*. Abgerufen am 29. Februar 2024 von https://www.bundesdruckerei.de/de/newsroom/pressemitteilungen/digitales-zeugnis-einfach-und-sicher

Thylmann, M. (10. Februar 2022). *Bundesdruckerei*, Update vom 12.09.2022. (Bundesdruckerei, Herausgeber) Abgerufen am 28. Dezember 2023 von https://www.bundesdruckerei.de/de/newsroom/pressemitteilungen/statement-digitale-schulzeugnisse#

Wittenberg, S. (2020). *Blockchain für Unternehmen: Anwendungsfälle und Geschäftsmodelle für die Praxis.* Stuttgart, Deutschland: Schäffer-Poeschel Verlag.

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

CA ..... *Certificate Authority*
DLT ..... *Distributed Ledger Technologie*
DSFA ..... *Datenschutz-Folgenabschätzung*
DSGVO ..... Datenschutz Grundverordnung
IDS ..... *Intrusion Detection Systems*
OZG ..... *Onlinezugangsgesetz*
PoS ..... *Proof-of-Stake*
PoW ..... *Proof-of-Work*