Projektarbeit

Zertifikatsverifikation mittels Blockchain im Bildungswesen

An der Fachhochschule Dortmund
im Fachbereich Informatik
Studiengang Praktische Informatik
erstellte Projektarbeit
zur Erlangung des akademischen Grades
Bachelor of Science

von
Jan Lano
geb. am 21.06.1998
Matr.-Nr. 7201735

Betreuung:
Prof. Dr. Gabriele Kunau
Prof. Dr. Sebastian Bab

Dortmund, 23. Juli 2023

Inhaltsverzeichnis

1. Einleitung

1.1. Motivation

Die Digitalisierung ist eine der bedeutendsten Entwicklungen des 21. Jahrhunderts. Sie ist nichts anderes als eine enorme Transformation oder eine fortlaufende Veränderung von Gesellschaft und Wirtschaft von einer heutzutage größtenteils analogen Welt hin zu einer digitalen Welt. Die traditionellen oftmals veralteten Prozesse werden im zunehmendem Maß von neuen digitalen Prozessen ersetzt.
Im Einstellungsverfahren für Unternehmen und vor allem im Bildungswesen sind Bildungszertifikate unerlässlich. Im deutschen Bildungssystem werden Bildungszertifikate heutzutage in Papierform ausgestellt, dies bringt einige Herausforderungen mit sich. Bewerbungen, sowohl für Studiengänge als auch für Arbeitsstellen, werden heute in den meisten Unternehmen in der Regel digital eingereicht. Die Bewerber tragen ihre privaten Daten in ein digitales Bewerbungsformular ein und schicken es an die Universität oder das Unternehmen. Der Nachweis einer Qualifikation in Form eines Bildungszertifikats muss im Bewerbungsprozesses in gescannter Form mit hochgeladen werden. Die Echtheit des Bildungszertifikats wird dann nach Vorlage einer beglaubigten Kopie bestätigt.

Dieser Prozess der Verifikation ist für alle Beteiligten umständlich und ermöglicht Betrug durch Manipulation oder vollständigen Fälschungen von Dokumenten.
Nigeria ist eines der sich am schnellsten entwickelnden afrikanischen Ländern, hinzukommt, dass es sich um die größte Volkswirtschaft Afrikas handelt. Eines der größten Probleme im Bildungssektor Nigerias sind gefälschte Zertifikate. In Nigeria müssen Organisationen die Zertifikate auf Echtheit überprüfen, dies kostet Organisationen Millionenbeträge [Fra]. Im Jahr 2017 musste der Präsident Tansanias 10.000 Angestellte der Regierung aufgrund von gefälschten Bildungsnachweise entlassen [BBC].

1.2. Zielsetzung

Im Rahmen dieser Projektarbeit soll ein Konzept zur Generierung und Verifikation von Bildungszertifikaten erarbeitet werden. Die Verifikation und Generierung der Bildungszertifikate soll mithilfe einer Blockchain erfolgen.
Hierfür werden die möglichen Anforderungen von Zertifikatsaussteller, Besitzer von Zertifikaten und weiteren Stakeholdern, die mit Bildungszertifikaten Berührungspunkte haben, in Betracht bezogen.
Die Verwendbarkeit von Bildungszertifikaten bei Online-Bewerbungsprozessen spielt eine entscheidende Rolle. Das Ziel besteht darin, die Bildungszertifikate für den Online-Bewerbungsprozess nutzbar zu machen und dadurch den Bewerbungsprozess effizienter zu gestalten.

1.3. Aufbau der Arbeit

Die Arbeit gliedert sich in acht Bestandteile, wobei der erste Teil aus der Einleitung besteht. Hier wird ein kurzer Überblick über das Themengebiet gegeben, des Weiteren wird das Ziel der Arbeit definiert.
Im zweiten Abschnitt der Arbeit wird die Methodik beschrieben. Hier werden die verschiedenen Softwareprozesse vorgestellt und die zugehörigen Vorgehensmodelle.
Der dritte und vierte Teil der Arbeit bilden die Grundlagen. Darin werden die Blockchain und die rechtliche Grundlage, auf der das Projekt beruht, beschrieben.
Im fünften Teil wird der Ist-Zustand des aktuellen Systems beschrieben.
Im sechsten Abschnitt werden die Anforderungen erhoben und infolge von diesen ein Konzept entwickelt.
Im siebten Kapitel der Arbeit wird das Konzept mit den wichtigsten Eigenschaften vorgestellt.
Der achte und letzte Teil der Arbeit beinhaltet das Fazit, im Hinblick auf die zum Anfang der Arbeit definierten Zielsetzung. Des Weiteren wird ein Ausblick gegeben, bezüglich der in der Zukunft möglichen Erweiterungen.

2. Methodik in der Softwaretechnik

In diesem Kapitel werden grundlegende Konzepte des Software Engineerings, der Softwareentwicklung sowie der Softwareprozesse und Vorgehensmodelle erläutert.

2.1. Softwareentwicklung

Softwareentwicklung bezieht sich auf den Prozess der Entwicklung von Softwarelösungen für Unternehmen oder Organisationen. Sie erfolgt in der Regel durch ein Team von Softwareentwicklern, die nach bewährten Praktiken und Standards arbeiten.
Softwareentwicklung kann in die zwei Hauptgruppen individuelle- oder Standardsoftwareentwicklung unterteilt werden.
Bei der Entwicklung von Individualsoftware arbeitet ein Entwicklerteam eng mit dem Kunden zusammen, um die Anforderungen zu verstehen, die Geschäftsprozesse zu analysieren und eine maßgeschneiderte Lösung zu entwerfen. Die Software wird von Grund auf neu entwickelt oder bestehende Komponenten und Module werden entsprechend den individuellen Bedürfnissen angepasst und integriert.

Standardsoftwareentwicklung bezieht sich auf die Entwicklung von Softwareprodukten, die für eine breite Nutzerbasis konzipiert sind und in der Regel von verschiedenen Unternehmen oder Organisationen eingesetzt werden können. Es handelt sich um vorgefertigte Softwarelösungen, die auf dem Markt verfügbar sind und typischerweise eine Vielzahl von Funktionen und Features bieten, die den Anforderungen eines breiten Spektrums von Benutzern gerecht werden. Beispiele für Standardsoftware sind Betriebssysteme, Textverarbeitungsprogramme, Buchhaltungssoftware oder Content-Management-Systeme.
Bei der Verwendung von Standardsoftware ist es oft notwendig, bestimmte Einstellungen, Konfigurationen und Funktionen anzupassen, um sie optimal an die individuellen Geschäftsprozesse und Anforderungen anzupassen. Diese Anpassung von Standardsoftware an die spezifischen Anforderungen eines Unternehmens wird Customizing genannt. Je nach Umfang der erforderlichen Anpassungen kann es sein, dass bestimmte Funktionen oder Prozesse nicht durch das Customizing abgedeckt werden können. In solchen Fällen kann die Entwicklung von Individualsoftware oder die Integration zusätzlicher spezialisierter Lösungen erforderlich sein. [AMB19]

2.2. Software Engineering

Software Engineering bezieht sich auf die Anwendung von ingenieurwissenschaftlichen Prinzipien, Methoden und Werkzeugen auf den gesamten Softwareentwicklungsprozess. Es geht über die reine Programmierung hinaus und umfasst die Planung, das Design, die Implementierung, das Testen, die Wartung und die Dokumentation von Software. Das Ziel des Software Engineering ist es, hochwertige,

zuverlässige und effiziente Softwarelösungen zu entwickeln.
Der Entwicklungsprozess kann in bestimmte Phasen unterteilt werden, die parallel oder nacheinander durchgeführt werden können. Die Abfolge der Prozesse kann je nach Vorgehensmodell variieren. [PB14]

2.3. Softwareprozesse

Softwareprozesse, auch bekannt als Softwareentwicklungsprozesse, sind strukturierte Ansätze oder Modelle, die verwendet werden, um Software zu entwickeln, zu implementieren und zu warten. Sie beschreiben den Ablauf und die Schritte, die während des gesamten Softwareentwicklungslebenszyklus durchgeführt werden, um eine effiziente und qualitativ hochwertige Software zu erstellen.
Es gibt verschiedene Softwareprozessmodelle, die verschiedene Ansätze zur Organisation und Durchführung dieser Phasen bieten. Beispiele für solche Modelle sind das Wasserfallmodell, das V-Modell, das agile Manifest (mit Methoden wie Scrum oder Kanban) oder das iterative und inkrementelle Modell. [EJB16]

2.3.1. Stakeholderanalyse

Vor der Anforderungsanalyse kommt die Stakeholderanalyse bei der relevante Interessensgruppen identifiziert werden. Die Stakeholderanalyse kann parallel zur Anforderungsanalyse und zum Softwareentwurf durchgeführt werden, da sie eng miteinander verbunden sind.

Im Allgemeinen lassen sich externe und interne Stakeholder unterscheiden. Externe Stakeholder sind Personen, Gruppen oder Institutionen, die eine Rolle in einem Projekt spielen, jedoch nicht direkt in dessen unmittelbarem Umfeld agieren. Interne Stakeholder hingegen umfassen alle Beteiligten, die sich direkt im Umfeld des Projekts befinden. [PB14] Die Stakeholderanalyse besteht aus 3 Teilen:

1. Identifizierung der Stakeholder: Erstellung einer Liste von potenziellen Stakeholdern. Die Erstellung einer solchen Liste kann durch Methoden wie Brainstorming, Beobachtungen, gezielte Interviews, Umfragen usw. geschehen.

2. Analyse von Interessen: Für jeden Stakeholder werden die individuellen Interessen, Bedürfnisse, Erwartungen und Ziele ermittelt. Dabei geht es darum, herauszufinden, was für sie wichtig ist und welche Auswirkungen das Projekt auf sie haben kann.

3. Bewertung: Es wird untersucht, welchen Einfluss und welche Macht die Stakeholder auf das Projekt haben. Dabei können Faktoren wie Ressourcen, Expertise, Position, Entscheidungsbefugnis und politische Einflüsse berücksichtigt werden. Die Bewertung kann durch eine Stakeholder-Matrix erstellt vorgenommen werden.

2.3.2. Anforderungsanalyse

Die Anforderungsanalyse befasst sich mit der Erhebung, Analyse, Spezifikation und Validierung von Anforderungen an das Softwareprojekt sowie mit dem Management von Anforderungen während

des gesamten Lebenszyklus eines Softwareprodukts.
Das Hauptaugenmerk liegt darauf, ein deutliches Verständnis der Anforderungen, Erwartungen und Ziele der beteiligten Personen zu erlangen und sie in konkrete Anforderungen umzuwandeln. Diese Anforderungen dienen als Grundlage für das Design und die Entwicklung der Software.
Eine Prozessanforderung ist eine Einschränkung für die Entwicklung der Software. Prozessanforderungen können direkt vom Entwickler, ihren Kunden oder einer dritten Partei gestellt werden.
Anforderungen werden in zwei Gruppen unterteilt, funktional und nicht funktional. Funktionale Anforderungen definieren die konkreten Funktionen, Aufgaben oder Dienste, die das System bereitstellen muss, um die Anforderungen der Benutzer oder Stakeholder zu erfüllen. Die Anforderungen sollten möglichst eindeutig formuliert werden.
Nichtfunktionale Anforderungen beschreiben Eigenschaften oder Qualitätsmerkmale des Systems, die über die reinen Funktionen hinausgehen. Nichtfunktionale Anforderungen können Sicherheit, Skalierbarkeit, Wartbarkeit etc. betreffen. [PB14]
Die Anforderungsanalyse besteht aus den folgenden 4 Schritten:

1. Anforderungserfassung: In dieser Phase werden Informationen von den Stakeholdern gesammelt. Dies kann durch Interviews, Fragebögen, Brainstorming, Workshops oder durch bloße Beobachtung erfolgen. Der Fokus liegt darauf, die Bedürfnisse, Wünsche, Ziele und Einschränkungen der Stakeholder zu verstehen.

2. Anforderungsdokumentation: Die erfassten Anforderungen werden in einem formalen Dokument festgehalten. Dieses Dokument dient als Referenz für das gesamte Softwareprojekt und ermöglicht eine klare Kommunikation zwischen den Beteiligten. Es kann verschiedene Arten von Anforderungsdokumenten geben, wie beispielsweise Lastenhefte, Use-Case-Dokumentation oder User Stories.

3. Anforderungsanalyse: In dieser Phase werden die erfassten Anforderungen analysiert, um mögliche Konflikte, Widersprüche oder Unvollständigkeiten zu identifizieren. Es können Techniken wie Anforderungsprüfung, Anforderungsvalidierung und Anforderungsverfolgung eingesetzt werden, um sicherzustellen, dass die Anforderungen konsistent, klar und umsetzbar sind.

4. Anforderungsmanagement: Während des gesamten Softwareentwicklungsprozesses müssen die Anforderungen verwaltet werden. Änderungen oder Ergänzungen der Anforderungen müssen nachverfolgt, dokumentiert und gegebenenfalls mit den Stakeholdern abgestimmt werden. Das Anforderungsmanagement hilft dabei, den Überblick über den Umfang und die Prioritäten des Projekts zu behalten.

2.3.3. Softwareentwurf

Beim Softwareentwurf werden die Ergebnisse der Anforderungsanalyse verwendet, um eine architektonische Lösung zu planen und zu definieren. Der Entwurf legt fest, wie die verschiedenen Komponenten der Software zusammenarbeiten, wie sie miteinander kom-

munizieren und wie die Daten organisiert und verarbeitet werden. [PB14]
Der Softwareentwurfsprozess besteht aus den folgenden beiden Teilen:

1. High-Level Design: In dieser Phase wird das System auf hoher Ebene entworfen. Es werden die grundlegenden Komponenten, Module und Schnittstellen definiert. Das High-Level Design legt die Architektur und die Struktur der Software fest und zeigt, wie die verschiedenen Teile zusammenarbeiten.

2. Detailed Design: Hier werden die Designentscheidungen auf einer detaillierten Ebene getroffen. Es werden spezifische Algorithmen, Datenstrukturen, Datenbankdesigns, Schnittstellen und Benutzeroberflächen festgelegt. Das Detailed Design dient als Grundlage für die Implementierung der Software.

2.3.4. Softwareimplementierung

In diesem Prozessschritt wird die eigentliche Implementierung der Software auf Grundlage der vorherigen erstellen Entwürfe vorgenommen. Neben der Implementierung der Software werden auch Modultests und Integrationstests durchgeführt.
Bei dem Modultest wird sichergestellt, dass die einzelnen Module oder Komponenten der Software einwandfrei funktionieren.
Nach dem Modultest folgt ein Integrationstest, hier wird sichergestellt, dass alle Module korrekt zusammengeführt worden sind. [PB14]

2.3.5. Softwarevalidierung

Der Prozess der Softwarevalidierung überprüft die erarbeitete Softwarelösung, um sicherzustellen, dass alle erarbeiteten Anforderungen erfüllt worden sind. Anschließend wird ein Testbericht mit allen identifizierten Fehlern erstellt, um einen Überblick über die Qualität der Software zu verschaffen.
Um die Software zu testen, werden eine Reihe von Testfällen entwickelt, damit alle Funktionen und Anforderungen der Software getestet werden. Testfälle beschreiben Schritte, Daten und erwartete Ergebnisse für die jeweiligen Testfälle.
Die Testfälle werden in einer vordefinierten Testumgebung entweder automatisch oder manuell ausgeführt. Das Resultat wird nach dem Test auf Fehler überprüft und in einem Fehlerbericht niedergeschrieben.
Wird ein Fehler identifiziert, wird dieser behoben und ein weiterer Testfall für den jeweiligen Fehler durchgeführt. [PB14]

2.3.6. Softwarewartung

Softwarewartung ist ein kontinuierlicher Prozess, der über die gesamte Lebensdauer der Softwareanwendung hinweg fortgesetzt wird. Es zielt darauf ab, die Software funktionsfähig, sicher, effizient und aktuell zu halten. Eine effektive Maintenance-Strategie hilft, die Lebensdauer der Software zu verlängern, Kosten zu minimieren und den Wert der Software für die Benutzer aufrechtzuerhalten. [PB14]

2.4. Vorgehensmodelle

Softwareprozessmodelle sind spezifische Vorgehensweisen oder Rahmenwerke, die den Ablauf und die Organisation des Softwareentwicklungsprozesses definieren. Sie bieten eine strukturierte Herangehensweise, um die Entwicklung von Softwareprojekten zu planen, zu steuern und zu überwachen.
Es gibt verschiedene Softwareprozessmodelle, die je nach den Anforderungen, Zielen und Besonderheiten des Projekts ausgewählt werden können. In den folgenden Modulen werden die gängigsten Modelle erklärt. [Max19]

2.4.1. Wasserfallmodell

Wie in Abbildung 2.1 zu sehen, erfolgt die Entwicklung bei einem Wasserfallmodell in sequentiellen Phasen. Jede Phase baut auf der vorherigen auf, somit erfolgt der Fortschritt in einer linearen Reihenfolge.
Die Phasen des Wasserfallmodells umfassen: Anforderungsanalyse, Softwareentwurf, Softwareimplementierung, Softwarevalidierung und Softwarewartung. Um mit einer neuen Phase zu beginnen, muss die vorherige Phase abgeschlossen sein. Sollte es in nachfolgenden Phasen zu Problemen kommen wie nicht umsetzbaren Anforderungen, können die vorherigen Schritte wiederholt werden. [EJB16]

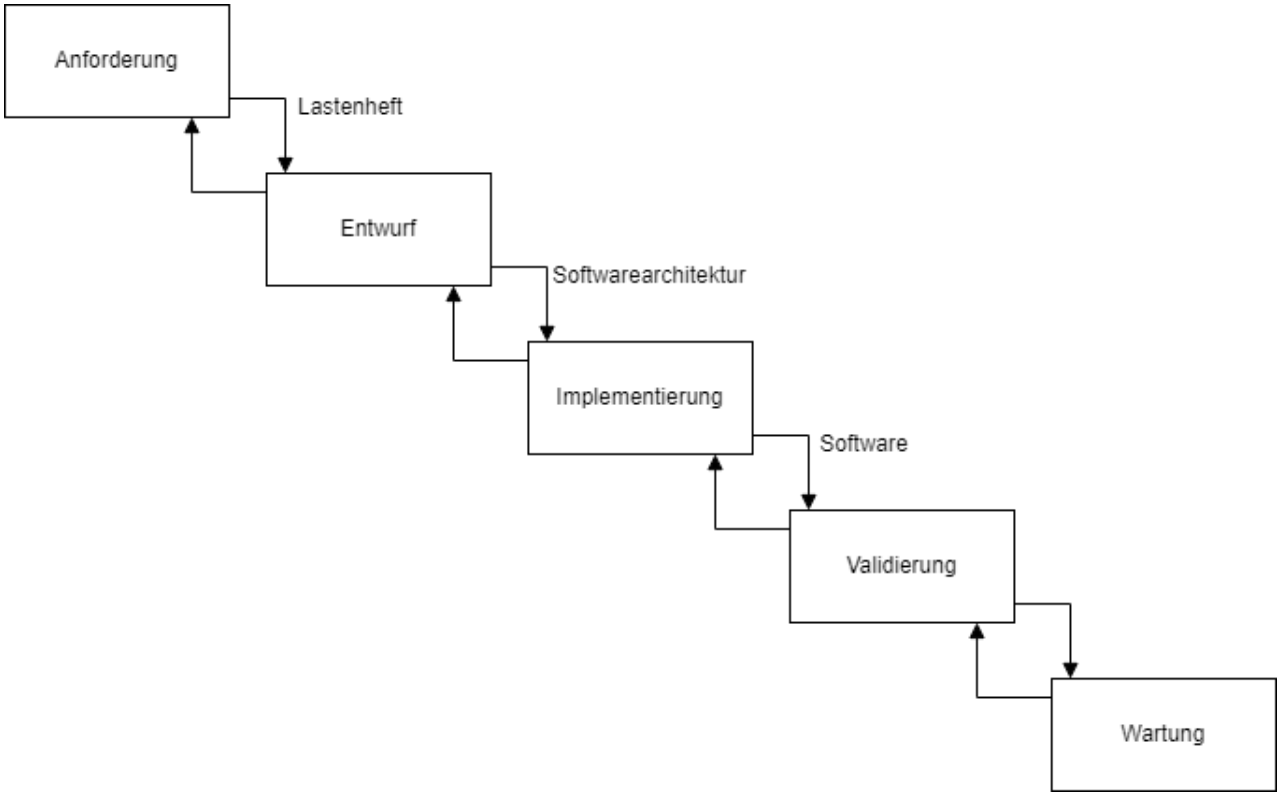

Abbildung 2.1.: Stufen des Wasserfallmodells

Vorteile

- Das Wasserfallmodell ist einfach zu verstehen und anwendbar. Es folgt einer klaren und linearen Struktur, bei der jede Phase nach der vorherigen abgeschlossen wird.
- Es werden klare Meilensteine definiert, die es ermöglichen, den Fortschritt des Projekts zu überwachen.
- Ressourcen wie Personal, Budget und Zeit können besser geplant und zugewiesen werden, da eine Phase abgeschlossen sein muss, bevor eine neue beginnen kann.

Nachteile

- Das Wasserfallmodell ist ein starres Modell, deswegen bietet es geringe Flexibilität für Änderungen der Anforderungen.
- Probleme tauchen erst in der Validierungsphase auf und bieten wenig Zeit für eine Korrektur.

2.4.2. Inkrementelle Entwicklung

Eine Schwäche des Wasserfallmodells ist die geringe Flexibilität. Bei einer inkrementellen Entwicklung wird der Entwicklungsphase in aufeinanderfolgenden Schritten aufgeteilt.
Wie in Abbildung 2.2 zu sehen ist, erfolgt die Entwicklung in zyklischer Weis, bei der die Anforderungen und der Softwareentwurf für einen Teil geplant werden. Die Implementation für die Teilmenge der fertigen Software wird anschließend getestet. Der Zyklus von Planung und Implementierung wird, solange wiederholt bis die Software entwickelt ist. [EJB16]

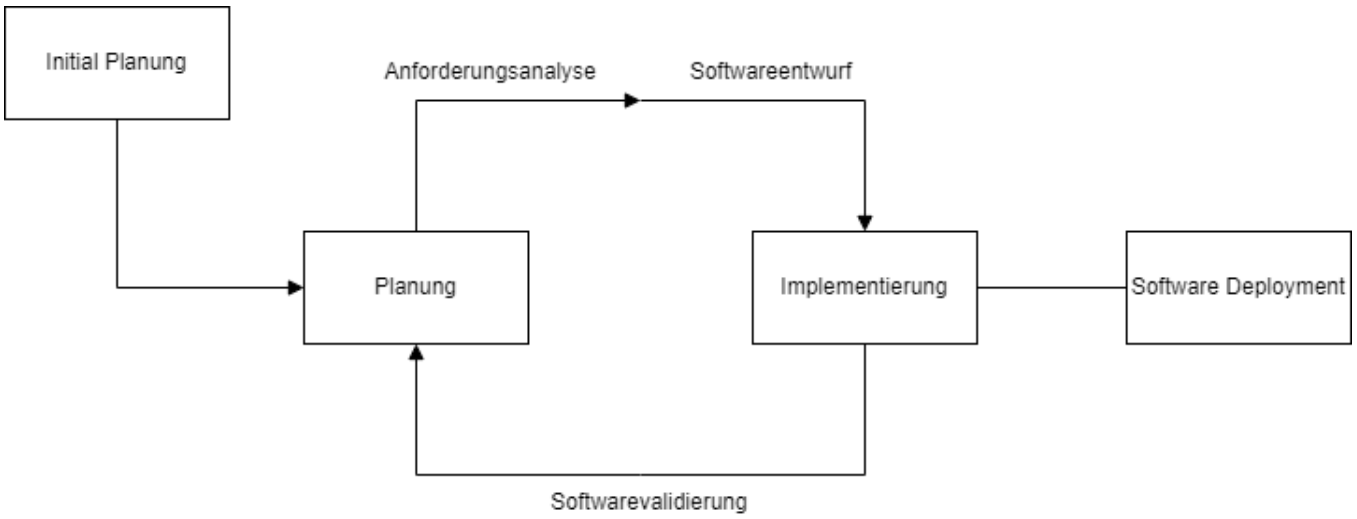

Abbildung 2.2.: Inkrementelles Vorgehensmodell

Vorteile

- Da in jeder Phase eine funktionsunfähige Software geliefert wird, kann der Kunde von dieser eher profitieren.
- Durch die Entwicklungen in kleinen Schritten können Anpassungen leicht integriert werden.
- Durch die regelmäßigen Lieferungen von kleinen Teilen der Software kann der Kunde effektiver im Projekt mitarbeiten.

Nachteile

- Die Inkremente müssen miteinander integriert werden.
- Die Architektur muss solide gestaltet werden, damit zukünftige Inkremente integriert werden können, dadurch können höhere Kosten entstehen.

2.4.3. Scrum

Scrum ist ein sehr beliebtes Framework für Softwareentwicklung, welches im Vergleich zum inkrementellen Modell gleichzeitig inkrementell und iterativ arbeitet.
In Scrum wird die Software in kurzen Abschnitten, sogenannten Sprints entwickelt. Ein Sprint dauert in der Regel ein bis vier Wochen. In jedem Sprint gibt es tägliche Meetings, den Daily Scrum. [AS13]

Ein Scrum Team besteht aus drei Rollen:

1. Product Owner: Der Product Owner ist für die Anforderung an die Software verantwortlich und arbeitet eng mit den Stakeholdern zusammen.

2. Developer Team: Das Developer Team ist für die Umsetzung der Anforderungen im Product Backlog verantwortlich.

3. Scrum Master: Der Scrum Master trägt die Verantwortung im Projekt und ist für die Moderation im Team zuständig.

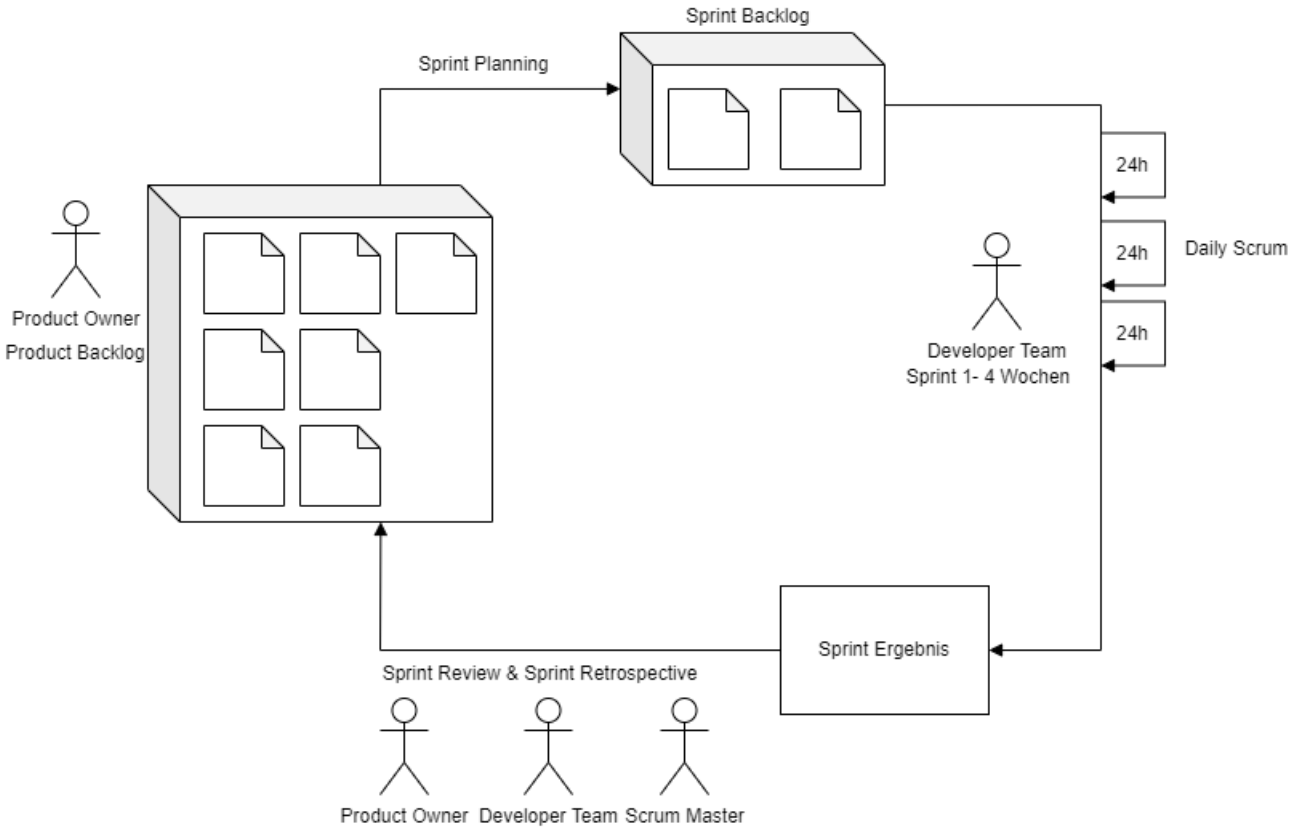

Abbildung 2.3.: Scrum-Prozessablauf

Wie in Abbildung 2.3 zu sehen ist, umfasst das Scrum Modell die folgenden fünf Schritte:

1. Product Backlog anlegen und pflegen: Der Product Backlog besteht aus den Anforderungen der Stakeholder. Anfänglich ist der Product Backlog noch sehr grob, wird mit dem Projektverlauf aber immer genauer. Anforderungen bekommen eine Priorität zugewiesen je nachdem wie wichtig diese sind.

2. Sprint Planning: Vor jedem Sprint trifft sich das gesamte Team, um sich auf die Anforderungen für den kommenden Sprint festzulegen. Die Anforderungen für den Sprint werden in den Sprint Backlog als Tickets geschrieben, diese werden

dann von einem Teammitglied im Sprint bearbeitet.

3. Daily Scrum: Beim Daily Scrum trifft sich das gesamte Team, bei dem jeder vom Fortschritt und den Hindernissen berichtet.

4. Sprint Review: Am Ende eines Sprints präsentiert das Team das Ergebnis den Stakeholdern. Sind die Einträge im Sprint Backlog erfüllt, werden diese aus dem Sprint Backlog entfernt und neue werden hinzugefügt.

5. Sprint Retrospective: Nach einem Sprint trifft sich das Team um die Zusammenarbeit, Abläufe und Kommunikation zu besprechen.

Vorteile

- Anforderungen des Kunden können nach dem Sprint Review schnell angepasst werden.
- Durch die täglichen Meetings können Probleme schnell identifiziert und behoben werden.
- Durch die klare Struktur von Scrum kann das Projekt effizient gesteuert werden.

Nachteile

- Die anfängliche Anpassung an Scrum kann komplex erscheinen, da alle Teammitglieder und Stakeholder auf den gleichen Stand gebraucht werden müssen.
- In größeren Projekten stellt die Koordination von mehreren Scrum Teams zusätzliche Planungsaufwand dar.

3. Blockchain

Da die Blockchain-Technologie sich noch in den Anfängen ihrer Entwicklung befindet, existiert bisher keine einheitliche Definition. In dem Bitcoin Whitepaper [?] wird der Begriff Blockchain nie definiert, jedoch wird beschrieben, dass Blöcke miteinander verkettet werden. Mark Walport definiert eine Blockchain als eine dezentrale Datenbank, in der Einträge in Blöcken gruppiert werden. Die Blöcke werden mit einer kryptographischen Signatur miteinander verbunden [Wal15]. Die Blöcke bauen aufeinander auf, sodass diese nach dem Hinzufügen nicht mehr verändert werden können.
Ein Blockchain Mechanismus kann in vier Schritten beschrieben werden:

1. In dem Datenfeld können jegliche Bewegungen von physischen und digitalen Komponenten aufgezeichnet werden.

2. Die Teilnehmer müssen sich einig sein, dass die aufgezeichneten Daten gültig sind, dies geschieht mit einem Konsensmechanismus.

3. Sobald Einigkeit unter den Teilnehmern besteht, werden die Daten in einen Block geschrieben und an die Blockchain angehängt.

4. Das System verteilt die aktuellste Kopie der Blockchain an alle Teilnehmer.

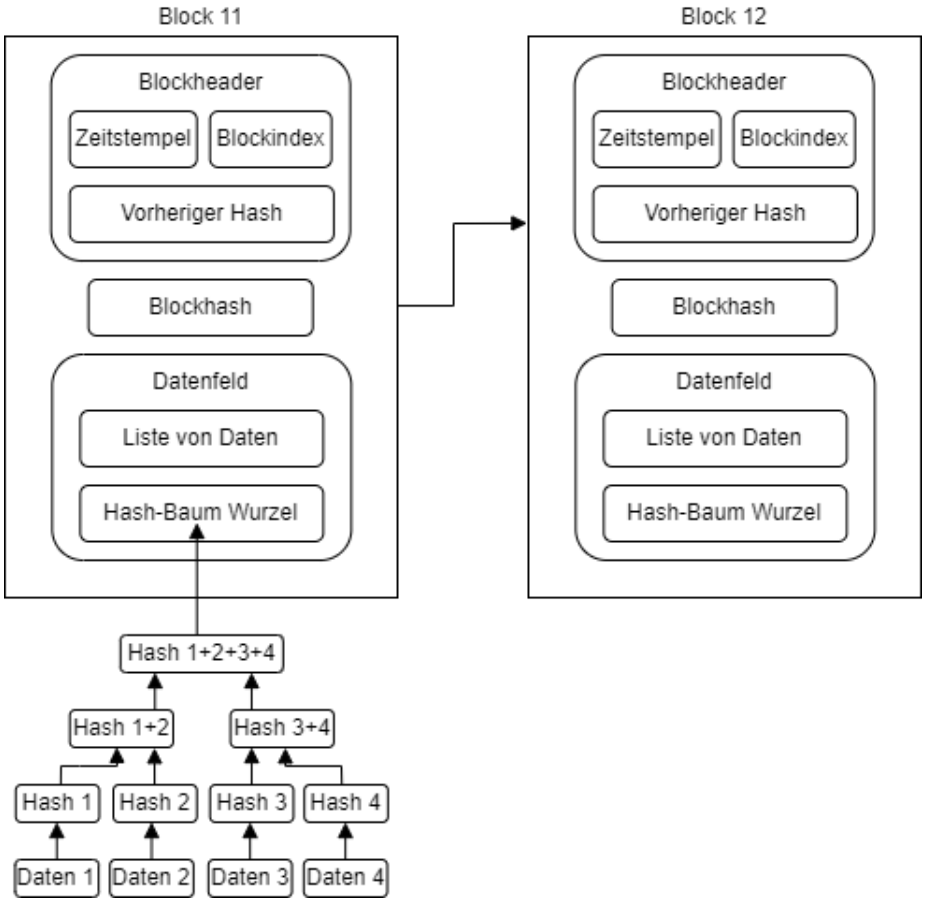

Abbildung 3.1.: Blöcke in einer Blockchain mit Hash-Baum

Wie in Abbildung 3.1 zu sehen ist besteht ein Block in einer Blockchain aus folgenden Bestandteilen:

1. Blockheader: Der Blockheader enthält Metadaten wie Blockindex, Zeitstempel und den Hashwert des vorherigen Blocks.

2. Blockhash: Der Blockhash ist ein Hashwert, der die Daten und den Blockheader repräsentiert.

3. Daten: Das Datenfeld enthält eine Liste von Daten und einen Hashwert, der diese repräsentiert. Der Hashwert der Liste wird vom Hash der Hash-Baum Wurzel angegeben. Bei einem Hash-Baum werden mehrere Hashwerte solange zusammengefasst bis nur noch einer überbleibt. Der Hash-Baum ermöglicht es, große Mengen von Transaktionsdaten in kompakter Form darzustellen und ihre Integrität effizient zu überprüfen.

3.1. Konsensmechanismen

Ein Konsensmechanismus ist ein Mechanismus, das in einer dezentralen und verteilten Netzwerkumgebung verwendet wird, um einen Konsens im System zu erreichen. In einer Blockchain entscheidet der Konsensmechanismus, wer den nächsten Block an die Blockchain hängen kann. Im Folgenden werden die am häufigsten verwendeten Konsensmechanismen erläutert. [HGF20]

3.1.1. Proof-of-Work(PoW)

Proof-of-Work ist ein Konsensmechanismus, bei dem die Teilnehmer eine komplexe mathematische Aufgabe lösen müssen. Die Teilnehmer müssen ein Nonce(Number Only Used Once) berechnen, um einen gültigen Blockhash zu berechnen, der bestimmten Kriterien erfüllen muss. Die Nonce wird in den Blockheader geschrieben. Eine Blockchain definiert die Kriterien, die beim Blockhash erfüllt sein müssen. Sobald ein Teilnehmer eine richtige Nonce gefunden hat kann er den Block an die Blockchain anhängen. Der Teilnehmer,

der die richtige Nonce gefunden hat, bekommt eine Belohnung in Form der Blockchain eigenen Währung.

3.1.2. Proof-of-Stake(PoS)

Bei Proof-of-Stake hinterlegt ein Teilnehmer, der am Konsensmechanismus teilnehmen möchte, einen Teil seiner Währung als Stake. Dieser Stake wird während des gesamten Konsensmechanismus eingefroren. Wer den nächsten Block hinzufügen kann, wird mit einem deterministischen Auswahlalgorithmus entschieden, dieser entscheidet basierend auf dem Anteil des Stakes des jeweiligen Teilnehmers. Sollte ein Teilnehmer betrügen und falsche Daten zum Block hinzufügen, wird der Stake einbehalten und der Teilnehmer von der Blockchain ausgeschlossen.

3.1.3. Proof-of-Authority(PoA)

Proof-of-Authority entscheidet basierend auf der Identität eines Teilnehmers, ob dieser einen Block an die Blockchain hängen kann. In einer PoA werden ausgewählte Teilnehmer, die auch als Validators bezeichnet werden, ermächtigt neue Blocks an die Blockchain anzuhängen. Die Validatoren werden aufgrund von Identität, Reputation und Vertrauen ausgewählt.

3.2. Blockchain-Typen

Es gibt verschiedene Arten von Blockchains, die je nach ihren Eigenschaften und Anwendungsbereichen kategorisiert werden können. Im Folgenden werden die vier gängigsten Arten erläutert. [Bas17]

3.2.1. Öffentliche Blockchains

Eine öffentliche Blockchain ist eine Art von Blockchain, die für jedermann zugänglich und transparent ist. Bei dieser Art von Blockchain kann jeder Teilnehmer eine Transaktion durchführen, neue Blöcke hinzufügen und die Integrität überprüfen.
Eine öffentliche Blockchain bietet ein hohes Maß an Dezentralisierung, da sie von einer großen Anzahl von Teilnehmern betrieben wird. Die Transaktionen in einer öffentlichen Blockchain sind für alle Teilnehmer einsehbar, was zu einer höheren Transparenz und einem gesteigerten Vertrauen in das System führt. Die Transparenz könnte eine Herausforderung für den Datenschutz darstellen. Öffentliche Blockchains stehen vor Herausforderungen hinsichtlich der Skalierbarkeit. Die Verarbeitung großer Datenmengen und die hohe Anzahl von Transaktionen können zu Leistungsengpässen führen. Ebenso ist die Weiterentwicklung der Blockchain komplex, da Entscheidungen von allen Teilnehmern getroffen werden müssen.
Die bekannteste Anwendung ist die Verwendung von öffentlichen Blockchains für Kryptowährungen wie Bitcoin [Nak08] oder Ethereum [But13]. Durch den Einsatz öffentlicher Blockchains wird eine dezentrale und transparente Abwicklung von Zahlungen ermöglicht. Durch den Einsatz von öffentlichen Blockchains können Unternehmen und Projekte Kapital durch Crowdfunding-Kampagnen auf-

bringen und digitale Token ausgeben. Dies eröffnet die Möglichkeit einer direkten Beteiligung und Interaktion mit Investoren. Eine der größten Crowdfunding Plattformen Kickstarter setzt immer mehr auf den Einsatz von Blockchain Technologie [Kic].

3.2.2. Private Blockchains

Private Blockchains sind spezielle Blockchain-Netzwerke, die von einem einzelnen Unternehmen oder einer Organisation betrieben und kontrolliert werden. Im Unterschied zu öffentlichen Blockchains, die für jedermann zugänglich sind und Transaktionen von beliebigen Teilnehmern validieren lassen, erlauben private Blockchains ausschließlich ausgewählten Teilnehmern den Zugriff und die Teilnahme am Netzwerk.
Private Blockchains gewährleisten ein erhöhtes Maß an Vertraulichkeit, da sie nur ausgewählten Teilnehmern den Zugriff erlauben. Dies ermöglicht den Teilnehmern eine umfassendere Kontrolle über ihre Daten und schützt ihre Privatsphäre. Die Betreiber haben volle Kontrolle über die Blockchain, damit ist die Weiterentwicklung viel leichter als bei einer öffentlichen Blockchain. Private Blockchains zeichnen sich durch eine bessere Skalierbarkeit aus, da sie nur ausgewählten Teilnehmern Zugriff gewähren und weniger rechenintensive Konsensmechanismen verwenden. Dadurch können sie in der Regel eine größere Anzahl von Transaktionen pro Sekunde verarbeiten, ohne dass es zu Engpässen oder Leistungsproblemen kommt. Bei privaten Blockchains müssen die Teilnehmer auf die Vertrauenswürdigkeit der beteiligten Unternehmen oder Organisationen setzen. Im Gegensatz zu öffentlichen Blockchains, bei denen alle Transaktionen für jeden Teilnehmer einsehbar sind, bieten private Blockchains

nur begrenzte Transparenz.
Unternehmen können private Blockchains einsetzen, um den gesamten Lieferkettenprozess zu verfolgen, von der Herstellung über die Logistik bis hin zur Lieferung an den Endkunden. Durch die transparente Erfassung von Transaktionen und Informationen entlang der Lieferkette können Effizienz und Rückverfolgbarkeit verbessert werden. Im Gesundheitswesen können private Blockchains genutzt werden, um Patientendaten sicher und vertraulich zu speichern und den Austausch von Informationen zwischen Krankenhäusern, Ärzten und anderen Gesundheitseinrichtungen zu ermöglichen [Bloa].

3.2.3. Hybride Blockchains

Eine hybride Blockchain ist eine Form der Blockchain-Technologie, die die Vorteile von öffentlichen und privaten Blockchains vereint, um die Anforderungen verschiedener Anwendungsfälle zu erfüllen. Im Gegensatz zu reinen öffentlichen oder privaten Blockchains bietet die hybride Variante eine flexible und anpassungsfähige Lösung für Unternehmen und Organisationen, die sowohl die Transparenz und Dezentralisierung der öffentlichen Blockchain als auch die Kontrolle und Datenschutz der privaten Blockchain benötigen.
Von der öffentlichen Blockchain übernimmt die hybride Blockchain die dezentrale Natur und Transparenz. Ähnlich wie in einer öffentlichen Blockchain können alle Teilnehmer das Netzwerk betreten und den Zustand der Blockchain einsehen. Dies fördert Vertrauen und ermöglicht eine transparente Überprüfung der Transaktionen. Die dezentrale Natur bedeutet, dass kein einzelner Punkt der Kontrolle existiert und das Netzwerk gegen Manipulationen gesichert ist.

Von der privaten Blockchain hingegen übernimmt die hybride Blockchain den Aspekt der Privatsphäre und der Zugriffsbeschränkungen. Bestimmte Teilnehmer erhalten spezielle Zugriffsrechte, um auf vertrauliche Informationen zuzugreifen oder bestimmte Funktionen innerhalb des Netzwerks auszuführen.
Die Flexibilität einer hybriden Blockchain ermöglicht es, sensible Daten und Transaktionen in einem privaten Bereich zu halten, der nur für ausgewählte Teilnehmer zugänglich ist. Gleichzeitig bietet der öffentliche Bereich Transparenz, Vertrauen und eine dezentrale Natur, die für viele Blockchain-Anwendungen von Vorteil sind. Im öffentlichen Bereich einer hybriden Blockchain kann die Skalierbarkeit durch den Einsatz effizienter Konsensmechanismen wie Proof-of-Stake oder Proof-of-Authority verbessert werden. Diese Mechanismen benötigen weniger Rechenleistung und ermöglichen eine schnellere Bestätigung von Transaktionen, was zu einer insgesamt besseren Leistung und Skalierbarkeit der Blockchain führt. Im privaten Teil einer hybriden Blockchain kann die Skalierbarkeit durch die Begrenzung der Teilnehmerzahl und den Einsatz effizienter Konsensmechanismen verbessert werden. Ein Nachteil, der mit einer hybriden Blockchain einhergeht, liegt in der zusätzlichen Komplexität, die sie mit sich bringt. Die Integration von öffentlichen und privaten Aspekten erfordert eine gründliche Planung, Implementierung und Verwaltung, was zu höheren Entwicklungskosten und einem erhöhten technischen Aufwand führen kann.
Durch den Einsatz hybrider Blockchains können Unternehmen Lieferketten auf transparente und sichere Weise verfolgen und verwalten. Dies geschieht, indem öffentliche Blockchains genutzt werden, um Transparenz und Vertrauen in die Lieferkette zu gewährleisten, während gleichzeitig private Blockchains verwendet werden, um sensible Unternehmensdaten und vertrauliche Informationen zu

schützen. Auf diese Weise können Unternehmen die Vorteile der Dezentralisierung und Transparenz nutzen, während sie gleichzeitig die Kontrolle über ihre internen Daten bewahren. Ein Beispiel für eine hybride Blockchain im Bereich Lieferketten ist IBM Food Trust [IBM].

3.2.4. Konsortium Blockchain

Eine Konsortium Blockchain ist eine Art von Blockchain-Netzwerk, das von einer Gruppe von Organisationen oder Unternehmen gemeinsam betrieben wird. Im Gegensatz zur öffentlichen Blockchain, die für jedermann zugänglich ist, und zur privaten Blockchain, die von einer einzigen Organisation kontrolliert wird, ermöglicht die Konsortium Blockchain eine Zusammenarbeit zwischen mehreren vertrauenswürdigen Parteien. Das Konsortium besteht aus verschiedenen Mitgliedern, die sich zusammenschließen, um gemeinsam eine Blockchain-Infrastruktur aufzubauen und zu betreiben. Jedes Mitglied des Konsortiums hat Zugriff auf das Netzwerk und kann Transaktionen verifizieren und neue Blöcke hinzufügen. Diese Transaktionen und Blöcke werden in der Regel von den Mitgliedern des Konsortiums überprüft und genehmigt, was zu einer erhöhten Vertrauenswürdigkeit des Netzwerks führt. In einer Konsortium Blockchain wird die Teilnahme in der Regel von einer zentralen Entität oder einer Gruppe von Entitäten festgelegt. Diese zentrale Entität wird als Konsortiumsmanager bezeichnet und hat die Autorität, über die Aufnahme neuer Teilnehmer zu entscheiden.
Konsortium Blockchains ermöglichen die Zusammenarbeit zwischen vertrauenswürdigen Parteien. Durch die gemeinsame Verwaltung des Netzwerks und der Validierung von Transaktionen durch die

Mitglieder entsteht ein hohes Maß an Vertrauen und Sicherheit. Im Vergleich zur öffentlichen Blockchain bieten Konsortium Blockchains ein höheres Maß an Datenschutz und Privatsphäre, da das Netzwerk von vertrauenswürdigen Parteien betrieben wird. Konsortium Blockchains sind weniger dezentralisiert, da sie von einer begrenzten Anzahl von Mitgliedern betrieben werden.
Konsortium Blockchains können verwendet werden, um die Transparenz und Effizienz in Lieferketten zu verbessern. Durch die gemeinsame Nutzung von Informationen über verschiedene Teilnehmer hinweg können Lieferkettenprozesse rationalisiert werden. Zusätzlich tragen sie zur Steigerung der Effizienz und Transparenz in Regierungsabläufen bei, einschließlich der Verwaltung von Identitäten, der Abwicklung von Steuerzahlungen und weiteren Verwaltungsaufgaben. Ein Beispiel für eine Konsortium Blockchain ist die von IBM und Maersk entwickelte Blockchain TradeLens [Tra], die Echtzeitverfolgung von Fracht und Dokumenten in der Lieferkette erlaubt.

4. Rechtliche Grundlage

Die Datenschutz-Grundverordnung (DSGVO) ist eine gesetzliche Regelung, die den Umgang mit personenbezogenen Daten in der Europäischen Union regelt. Die DSGVO gilt laut DSGVO Artikel 1 für alle Unternehmen und Organisationen, die personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig von ihrem Standort. In diesem Kapitel wird eine Auseinandersetzung mit den grundlegenden Prinzipien und Anforderungen der DSGVO bezüglich des Schutzes personenbezogener Daten stattfinden [DSG, Artikel 1].

4.1. Personenbezogene Daten

Personenbezogene Daten werden als “alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen“ definiert [DSG, Artikel 4]. Hierzu gehören Daten wie Namen, Adressen, E-Mail-Adressen, Telefonnummern und andere Informationen.

4.2. Grundsätze der Datenverarbeitung

Die DSGVO legt bestimmte Grundsätze fest, nach denen personenbezogene Daten verarbeitet werden müssen. Dazu gehören Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datensparsamkeit, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflicht [DSG, Artikel 5]. Gemäß diesem Artikel müssen Verantwortliche und Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen ergreifen, um ein angemessenes Schutzniveau für personenbezogene Daten sicherzustellen. Dazu gehört auch die Umsetzung von Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Personen Zugriff auf personenbezogene Daten haben. [DSG, Artikel 32]

4.3. Rechte der betroffenen Personen

Die DSGVO gewährt den betroffenen Personen verschiedene Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten. Diese Rechte umfassen das Recht auf Auskunft über die verarbeiteten Daten, das Recht auf Berichtigung oder Löschung von Daten, das Recht auf Einschränkung der Verarbeitung, das Recht auf Datenübertragbarkeit und das Widerspruchsrecht gegen bestimmte Arten der Verarbeitung. [DSG, Artikel 12-23]

4.4. Einwilligung und Datenschutzerklärung

Die Einwilligung der betroffenen Person ist ein wesentlicher Bestandteil der rechtmäßigen Verarbeitung personenbezogener Daten. Die DSGVO stellt strenge Anforderungen an die Einwilligung, einschließlich der Freiwilligkeit, der informierten Zustimmung und der Möglichkeit des Widerrufs. Unternehmen und Organisationen sind verpflichtet, klare und verständliche Datenschutzerklärungen bereitzustellen, in denen sie die Zwecke der Datenverarbeitung, die Rechtsgrundlage und die Rechte der betroffenen Personen erläutern. [DSG, Artikel 6,7]

4.5. Herausforderung der Blockchain-Technologie hinsichtlich der DSGVO

Die Integration der Datenschutzgrundverordnung (DSGVO) in die Blockchain-Technologie stellt spezifische Herausforderungen dar. Aufgrund der dezentralen Struktur und der Unveränderlichkeit der Blockchain ergeben sich einige Fragen hinsichtlich des Schutzes personenbezogener Daten und der Erfüllung der Grundsätze der DSGVO. Eine der grundlegenden Anforderungen der DSGVO besteht darin, personenbezogene Daten zu identifizieren und angemessene Schutzmaßnahmen zu ergreifen. In einer Blockchain können personenbezogene Daten in Form von Transaktionsdaten, digitalen Identitäten oder anderen Informationen gespeichert werden. Die Sicherheit der

in der Blockchain gespeicherten personenbezogenen Daten ist von entscheidender Bedeutung. Es müssen angemessene technische und organisatorische Maßnahmen ergriffen werden, um den Schutz und die Integrität der Daten sicherzustellen. Dies umfasst den Schutz vor unbefugtem Zugriff, Datenmanipulation und Datenverlust. Die DSGVO gewährt betroffenen Personen bestimmte Rechte, wie das Recht auf Auskunft, Berichtigung, Löschung und Datenübertragbarkeit. Bei der Nutzung einer Blockchain müssen Mechanismen implementiert werden, die es den betroffenen Personen ermöglichen, diese Rechte auszuüben und ihre Daten zu kontrollieren. In einer öffentlichen Blockchain haben Personen aus beliebigen Standorten die Möglichkeit, teilzunehmen, weshalb es herausfordernd ist, den genauen Speicherort der Daten zu ermitteln. Aufgrund dieser dezentralen Natur der Blockchain besteht die Möglichkeit, dass die Daten auch außerhalb der Grenzen der Europäischen Union gespeichert werden. [Dat]

4.6. Lösungsansätze für die DSGVO

Die Off-Chain-Speicherung bezieht sich auf die Aufbewahrung von Daten außerhalb der eigentlichen Blockchain. In der Blockchain-Technologie werden normalerweise alle Daten in der Blockchain selbst gespeichert, was bedeutet, dass alle Teilnehmer der Blockchain Zugriff auf diese Daten haben und sie überprüfen können. Die Off-Chain-Speicherung ermöglicht es jedoch, bestimmte Daten außerhalb der Blockchain zu speichern, sodass sie nicht für alle Teilnehmer sichtbar sind. In der Blockchain wird nur eine Referenz zur eigentlichen Datei gespeichert, oft in Form eines Hashwertes. Aufgrund der Einzigartigkeit dieses Werts für jede Datei lassen

sich Manipulationen an den außerhalb der Blockchain gespeicherten Daten leicht erkennen, da die Referenz ihre Gültigkeit verlieren würde. Mit der Off-Chain-Speicherung können die personenbezogenen Daten vor unbefugtem Zugriff geschützt werden. Ebenso kann das Recht auf Auskunft, Berechtigung, Löschung und Datenübertragbarkeit gewährt werden. Im Falle einer Dateilöschung wäre der Hashwert des Zertifikats immer noch in der Blockchain vorhanden, jedoch würde die Verknüpfung auf eine nicht existierende Datei verweisen.

Eine private Blockchain kann sicherstellen, dass nur befugte Teilnehmer Zugriff auf die personenbezogenen Daten haben. Statt personenbezogene Daten direkt in der Blockchain zu speichern, können sie anonymisiert oder pseudonymisiert werden, um die Identität der betroffenen Personen zu schützen. Außerdem kann sichergestellt werden, dass keine Daten außerhalb der EU in der Blockchain gespeichert werden. [Fin] [Blob]

5. Ist-Zustand-Analyse des Systems

Die Ist-Zustand-Analyse des Systems liefert einen Überblick über den aktuellen Zustand und die Funktionsweise des bestehenden Systems, um mögliche Stärken, Schwächen und Optimierungspotenziale zu identifizieren.

5.1. Ausgangssituation

In Deutschland liegt die Verantwortung für die Verifikation von Bildungszertifikaten bei den anwendenden Institutionen selbst. Dies umfasst Schulen, Hochschulen, Unternehmen und andere Institutionen. Die Verifikation erfolgt in der Regel manuell durch Prüfung der Originaldokumente, Überprüfung der Siegel und Unterschriften sowie Vergleich mit Datenbanken und Registern. In Deutschland müssen bestimmte offizielle Dokumente beglaubigt werden, um ihre Echtheit und Gültigkeit zu bestätigen. [SGV]
Abbildung 5.1 veranschaulicht den gegenwärtigen Bewerbungsprozess. Das Sequenzdiagramm zeigt die Interaktionen und den Nachrichtenaustausch zwischen den verschiedenen Objekten und ermöglicht es, den Ablauf von Aktivitäten oder Prozessen zu visualisieren.

Es zeigt die zeitliche Abfolge der Nachrichten und die Reihenfolge, in der die Objekte miteinander kommunizieren. [Fow04]
Die Beglaubigung von Dokumenten ist ein Verfahren, bei dem eine autorisierte Person oder Behörde bestätigt, dass das betreffende Dokument eine authentische Kopie des Originals ist. Die anwendende Institution muss nach Erhalt der Bewerbung, die beglaubigten Kopie in ein digitales Format übertragen, damit Teile des Bewerbungsprozesses automatisch erfolgen können.

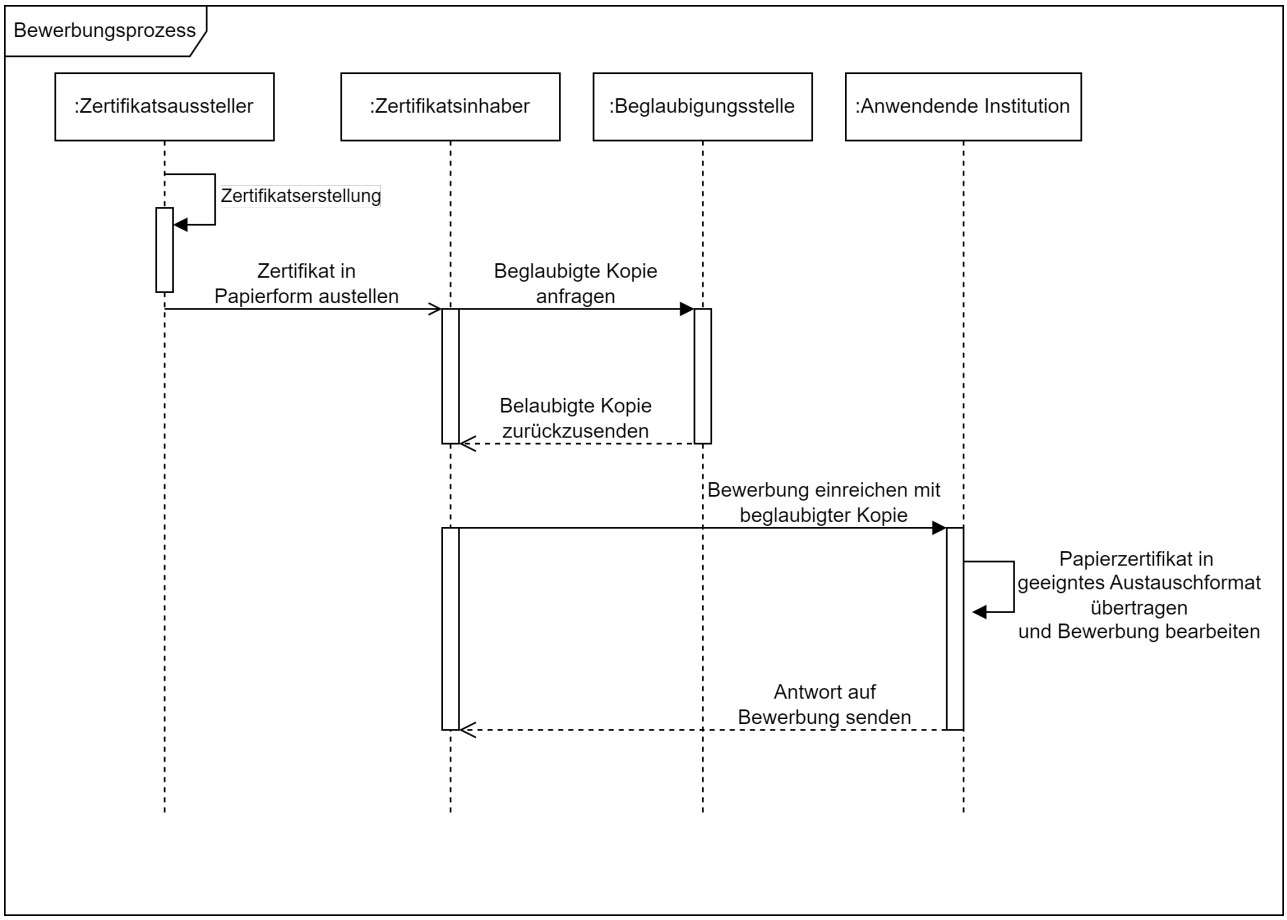

Abbildung 5.1.: Aktueller Bewerbungsprozess

5.2. Herausforderung des Verifikationsprozesses

Der Ist-Zustand der Verifikation von Bildungszertifikaten in Deutschland ist mit mehreren Herausforderungen verbunden. Dazu gehören der hohe Verwaltungsaufwand für manuelle Verifikationsprozesse, die mangelnde Standardisierung des Verfahrens zum Auslesen der Bewerbungsdaten und die begrenzte Zusammenarbeit zwischen Zertifizierungsstellen und anderen relevanten Akteuren.

5.3. Technologischer Lösungsansatz

Die Verwendung von digitalen Signaturen und Blockchain-Technologie bietet Potenzial, um die Echtheit von Zeugnissen zu gewährleisten und die Integrität der Daten zu schützen. Die Einführung eines zentralen Registers für Bildungsnachweise und die Nutzung von Datenbanken zur automatisierten Verifikation könnten ebenfalls die Effizienz steigern und die Überprüfungsprozesse vereinfachen.

6. Anforderungserhebung

Die erfolgreiche Umsetzung eines Projekts erfordert ein tiefes Verständnis der Bedürfnisse und Anforderungen der beteiligten Stakeholder. Bei der Entwicklung eines Systems zur Verwaltung von Bildungszertifikaten mithilfe von Blockchain-Technologie ist es von entscheidender Bedeutung, eine umfassende Stakeholder- und Anforderungserhebung durchzuführen. Dieser Prozess ermöglicht es uns, die unterschiedlichen Interessengruppen zu identifizieren, ihre Erwartungen zu verstehen und ihre Anforderungen an das System zu erfassen. [Max19] Die Stakeholder- und Anforderungserhebung bildet die Grundlage für die weitere Konzepterstellung und Entwicklung des Blockchain-gestützten Bildungszertifikatssystems.

6.1. Vorgehensmodell

Das Wasserfallmodell bietet eine strukturierte Herangehensweise zur Entwicklung eines detaillierten Konzepts. Durch eine gründliche Anforderungsanalyse und eine systematische Vorgehensweise kann ein solides Konzept erstellt werden, das als Grundlage für die weitere Umsetzung dient. Durch eine gründliche Analyse und Planung zu Beginn des Projekts können die Anforderungen klar definiert und dokumentiert werden, was eine gute Grundlage für die weitere

Projektarbeit schafft. Das Wasserfallmodell ermöglicht eine sequenzielle Abwicklung des Projekts, bei der jede Phase nacheinander abgeschlossen wird. Da das Projekt in Eigenregie durchgeführt wird, besteht kein Bedarf für gleichzeitige Aufgabenbearbeitung oder eine hohe Flexibilität in der Umsetzung. Die sequenzielle Abwicklung des Wasserfallmodells passt gut zu einem Einzelprojekt, da es eine klare Struktur und klare Meilensteine bietet, die das Projektziel verfolgen.[Max19]

6.2. Stakeholderanalyse

Die Stakeholder wurden durch eine Bestandsaufnahme des derzeitigen Systems ermittelt. Bei dieser Betrachtung ergeben sich hauptsächlich drei zentrale Interessengruppen.
Im folgenden Abschnitt werden die jeweiligen Interessengruppen vorgestellt und ihre individuellen Aufgaben, Bedürfnisse und Interaktionen werden kurz erläutert.

6.2.1. Zertifikatsaussteller

Der Zertifikatsaussteller spielt eine Schlüsselrolle bei der Ausstellung und Verwaltung von Zertifikaten, die in verschiedenen Branchen und Kontexten eingesetzt werden. Zertifikatsaussteller sind Institution wie Schulen, Universitäten, Industrie- und Handwerkskammern oder Unternehmen, die Bildungszertifikate ausstellen.

- Aufgabe im System
  - Es werden Zertifikate erstellt und an Zertifikatsinhaber wie Schüler ausgehändigt.
- Grundbedürfnis
  - Unkomplizierte Erzeugung von Zertifikaten.
  - Abwärtskompatibilität zu dem vorherigen System.
- Interaktion
  - Verwendet einen Dienst, der die Erstellung und Absicherung von Zertifikaten ermöglicht.

6.2.2. Zertifikatsinhaber

Zertifikatsinhaber sind Personen, die Bildungszertifikate von einem Zertifikatsaussteller erhalten, darunter Schüler, Studierende und andere Individuen. Diese Zertifikate bestätigen den Abschluss bestimmter Bildungsprogramme oder den Erwerb bestimmter Qualifikationen.

- Aufgabe im System
  - Empfängt ein Zertifikat von einem Zertifikatsaussteller, um es im Rahmen eines Bewerbungsprozesses an eine anwendende Organisation weiterzureichen.

- Grundbedürfnis
  - Elektronische Weiterleitung von Zertifikaten an anwendende Institutionen ohne den Gang zu Behörden zur Beglaubigung.
- Interaktion
  - Empfängt Zertifikate und leitet diese eigenständig elektronisch weiter.

6.2.3. Anwendende Institution

Anwendende Organisationen sind Institutionen oder Unternehmen, bei denen die Zertifikatsinhaber ihre Zertifikate vorlegen müssen. Diese Organisationen können eine Vielzahl von Bereichen abdecken, wie beispielsweise Arbeitgeber, Behörden, öffentliche oder private Institutionen, Verbände oder andere Einrichtungen, die einen Nachweis über bestimmte Fähigkeiten, Kenntnisse oder Qualifikationen verlangen.

- Aufgabe im System
  - Empfängt elektronische Zertifikate von Zertifikatsinhabern, führt eine Echtheitsprüfung durch und startet daraufhin den Bewerbungsprozess.

- Grundbedürfnis
  - Die Zertifikate werden digital erfasst, daraufhin findet eine automatisierte Prüfung statt und schließlich erfolgt die Weiterverarbeitung der Daten.
- Interaktion
  - Verwendet ein Service, der die Echtheitsprüfung von Zertifikaten übernimmt.

6.3. Anforderungsermittlung

Ein Interview wurde als Methode zur Anforderungserhebung gewählt, da es eine direkte und persönliche Interaktion mit den Stakeholdern ermöglicht. Es bietet die Möglichkeit, detaillierte Informationen über ihre Bedürfnisse, Erwartungen und Anforderungen zu erhalten. Während eines Interviews können potenzielle Unklarheiten oder Missverständnisse bezüglich der Anforderungen sofort geklärt werden. Der Interviewer kann gezielte Fragen stellen, um eine tiefere Einsicht in die Bedürfnisse des Stakeholders zu erhalten und sicherzustellen, dass alle Informationen verstanden werden. [Lin20] [Fau19]

6.3.1. Interview

Im Rahmen der Anforderungsermittlung wurden gezielte Interviews mit verschiedenen Stakeholdern aus unterschiedlichen Bereichen durchgeführt. Die Interviews richteten sich an Ingenieursfirmen, Studierende, Schüler und Schulen, um eine breite Palette von Perspekti-

ven und Bedürfnissen abzudecken. Jede Gruppe hatte spezifische Anforderungen und Anwendungsfälle, die in die Konzeption des Blockchain-Systems für Bildungszertifikate einfließen sollten.
Die Interviews mit Studierenden und Schülern zielten darauf ab, ihre Perspektiven und Erwartungen hinsichtlich der Verwendung von Blockchain für Bildungszertifikate zu erfassen. Es wurden Fragen zu Benutzerfreundlichkeit und Zugänglichkeit gestellt, um sicherzustellen, dass das System ihren Bedürfnissen und Ansprüchen gerecht wird.
Die Interviews mit Ingenieursfirmen zielten darauf ab, ihre Bedürfnisse in Bezug auf die Überprüfung und Validierung von Zertifikaten zu erfassen. Es wurde nach ihren Anforderungen an die Authentizität und Verifizierbarkeit von Zertifikaten gefragt, um sicherzustellen, dass das System ihren Anforderungen entspricht und ihre Prozesse unterstützt.
Schulen wurden ebenfalls in die Interviews einbezogen, um ihre Anforderungen an die Verwaltung und Ausstellung von Zertifikaten zu verstehen. Es wurden Fragen zur Integration des Systems in ihre bestehenden Verwaltungsprozesse, zur Skalierbarkeit und zur Schulung der Administratoren gestellt, um sicherzustellen, dass das System effizient in ihre Abläufe integriert werden kann.
Bei der Durchführung der Interviews werden alle wichtigen Informationen und Aussagen stichpunktartig mitgeschrieben. Dies ermöglicht eine effiziente Erfassung der Kernpunkte und verhindert, dass wertvolle Informationen verloren gehen.

6.3.2. Interviewanalyse

Während der Interviews werden alle relevanten Informationen und Aussagen erfasst und anschließend in die entsprechenden Kategorien eingeordnet. In diesem Fall werden die Interviews in die Kategorien Benutzerfreundlichkeit, Effizienz und Sonstige einsortiert. Die Kategorie Benutzerfreundlichkeit umfasst alle Aussagen, die sich auf die Bedienbarkeit, intuitive Nutzung und Benutzererfahrung beziehen. Hier geht es darum, wie einfach und angenehm das System für die Anwender ist und ob es ihre Anforderungen und Erwartungen erfüllt. Die Kategorie Effizienz bezieht sich auf Aussagen, die die Leistungsfähigkeit und Geschwindigkeit des Systems betreffen. In der Kategorie Sonstige werden Aussagen eingeordnet, die nicht direkt den Bereichen Benutzerfreundlichkeit oder Effizienz zugeordnet werden können, aber dennoch relevant sind. Dies können beispielsweise Aussagen zu Sicherheitsaspekten, Erweiterbarkeit des Systems oder spezifischen Anforderungen sein, die nicht in die anderen Kategorien passen. [EJB16]

6.4. Anforderungsdokumentation

User Stories werden häufig für die Anforderungsdokumentation in der Softwareentwicklung eingesetzt. Sie bieten eine effektive Methode, um die Bedürfnisse der Benutzer zu verstehen und in konkrete Anforderungen umzuwandeln.
User Stories zeichnen sich durch ihre hohe Verständlichkeit und ihre benutzerfreundliche Kommunikation aus. Sie sind in einer klaren und einfachen Sprache verfasst, wodurch die Kommunikation zwischen Teammitgliedern, Stakeholdern und dem Entwicklungsteam

erleichtert wird. Jeder kann schnell den Inhalt und die Bedeutung einer User Story erfassen, was zu einer effektiven Zusammenarbeit und einer klaren Kommunikation beiträgt. Durch die Verwendung von verständlichen User Stories wird eine reibungslose und effiziente Zusammenarbeit im Projekt gewährleistet.
Die Flexibilität und Anpassungsfähigkeit von User Stories ist ein wesentliches Merkmal. Sie werden bewusst absichtlich vage formuliert, um Raum für Interpretation und Kreativität zu lassen. Dadurch wird dem Entwicklungsteam ermöglicht, verschiedene Lösungsansätze zu erkunden und flexibel auf sich ändernde Anforderungen zu reagieren. [Rob12]

6.4.1. User Stories

Im weiteren Verlauf werden die Anforderungen in Form von User Stories präsentiert.

- Als Zertifikatsinhaber, möchte ich direkten Zugriff auf mein beglaubigtes Zertifikat haben, damit ich es während eines Bewerbungsprozesses verwenden kann. Ich erwarte, dass ich elektronisch oder physisch auf mein beglaubigtes Zertifikat zugreifen kann, um es bei Bedarf an potenzielle Arbeitgeber oder Bildungseinrichtungen weiterzugeben.

- Als Zertifikatsinhaber, möchte ich sicherstellen, dass meine digitalen Zertifikate nur bei mir selbst und denjenigen vorliegen, denen ich das Zertifikat gesendet habe. Ich möchte verhindern, dass unbefugte Personen Zugriff auf meine Zertifikate haben und diese missbräuchlich verwenden können.

- Als Zertifikatsinhaber, möchte ich die Möglichkeit haben, Papierdokumente parallel zu den digitalen Zertifikaten ausstellen und verwenden zu können, da es bestimmte Szenarien gibt, in denen Papierdokumente im rechtlichen Kontext oder traditionellen Kontext benötigt werden.

- Als anwendende Institution, möchte ich, dass die Daten des Zertifikats wie die Informationen zur Schule/Hochschule, zum Inhaber und zu den Noten elektronisch auslesbar sind. Durch die elektronische Lesbarkeit der Zertifikatsdaten können verschiedene automatisierte Prozesse unterstützt werden, wie beispielsweise die Überprüfung der Echtheit der Zertifikate oder die automatische Verarbeitung der Noten für statistische Auswertungen.

- Als anwendende Institution, des Systems möchte ich sicherstellen, dass nur registrierte Institutionen Zertifikate absichern können. Dadurch wird die Integrität und Vertrauenswürdigkeit der eingetragenen Zertifikate gewährleistet.

- Als Zertifikatsaussteller, möchte ich, dass mein Zertifikat vielfältig sein kann und verschiedene Arten von Zertifikaten wie Abitur, Diplom, Leistungsnachweis über Kurs im Studium oder Weiterbildungsnachweis enthalten kann.

7. Konzeptentwicklung

Ein entscheidender Schritt bei der Durchführung eines Projekts ist die Konzepterstellung. In diesem Kapitel werden die Grundlagen und die Planung für die Umsetzung des Projekts festgelegt. Die Konzepterstellung bildet das Gerüst, auf dem das gesamte Projekt aufbaut und legt den Kurs für den erfolgreichen Abschluss fest und basiert auf den bereit ermittelten Anforderungen. Besonderes Augenmerk wird dabei auf die Erfüllung der datenschutzrechtlichen Anforderungen gemäß der Datenschutz-Grundverordnung (DSGVO) gelegt, um die Privatsphäre und die Rechte der Nutzer zu wahren.

7.1. Funktionalitäten

Um den Bedürfnissen der Zertifikatsinhaber gerecht zu werden und ihnen eine effiziente Nutzung der Blockchain-basierten Bildungszertifikate zu ermöglichen, spielen die Funktionalitäten des Systems eine entscheidende Rolle. Im nächsten Abschnitt werden die wesentlichen Funktionalitäten detailliert beschrieben, um einen umfassenden Einblick in deren Umfang und Nutzen zu geben.

7.1.1. Ausstellung von Zertifikaten

Eine essenzielle Funktion des Systems besteht darin, Bildungszertifikate an die entsprechenden Zertifikatsinhaber auszustellen. Dieser Prozess beinhaltet die Generierung eines eindeutigen Zertifikats, das alle relevanten Informationen wie den Namen des Inhabers, das abgeschlossene Programm und das Ausstellungsdatum enthält. Das Zertifikat kann sowohl in digitaler Form erstellt als auch auf Papier gedruckt werden, um den individuellen Präferenzen der Zertifikatsinhaber gerecht zu werden.

7.1.2. Verifikation von Zertifikaten

Die Möglichkeit, die Echtheit von Bildungszertifikaten zu verifizieren, spielt eine entscheidende Rolle für Arbeitgeber, Bildungseinrichtungen und andere relevante Parteien. Die Funktion zur Überprüfung von Zertifikaten ermöglicht es Dritten, die Authentizität eines Zertifikats zu überprüfen, indem sie auf die Informationen in der Blockchain zugreifen. Dies trägt zur Stärkung des Vertrauens bei und erleichtert die nahtlose Integration der Zertifikate in den Bewerbungs- und Einstellungsprozess. Durch die Überprüfung der Zertifikate können Arbeitgeber die Richtigkeit der Bildungsleistungen eines Bewerbers bestätigen.

7.1.3. Übertragung von Zertifikaten

Die Übertragung von Zertifikaten ermöglicht es den Zertifikatsinhabern, ihre erworbenen Qualifikationen an Organisationen weiterzugeben. Ein solcher Nachweis kann insbesondere von Bedeutung sein, wenn eine Person den Arbeitsplatz wechselt oder an einer Weiterbildung teilnimmt. Die Funktion ermöglicht eine sichere und transparente Übertragung der Zertifikate, wobei die Integrität und Gültigkeit des Zertifikats erhalten bleiben.

7.2. Systemarchitektur

Die Systemarchitektur bildet das grundlegende Gerüst und die technische Blaupause jedes Softwareprojekts. Sie legt die Struktur, Komponenten und Interaktionen des Systems fest, um die festgelegten Anforderungen effizient und zuverlässig zu erfüllen. Im Verlauf dieses Kapitels werden die einzelnen Komponenten der Architektur erläutert und ihre Zusammenarbeit beschrieben.

7.2.1. Kontrollinstanz

Die Kontrollinstanz spielt eine wichtige Rolle in der Architektur des Systems zur Zertifikatserstellung und -verwaltung. Die Kontrollinstanz wird vom Bildungsministerium oder einer ähnlichen autorisierten Stelle repräsentiert.
Zertifikatsaussteller, die anerkannte Bildungseinrichtungen oder Organisationen sind, können sich bei der Kontrollinstanz um Aufnahme bewerben. Die Kontrollinstanz prüft die eingereichten Anträge

und bewertet die Qualifikationen, Erfahrungen und sonstigen relevanten Kriterien der Bewerber. Die Kontrollinstanz betreibt eine Datenbank, die die IP-Adressen der Zertifikatsaussteller enthält.

7.2.2. Blockchain

Die Blockchain stellt einen wesentlichen Bestandteil unserer Architektur dar. Es handelt sich um eine Konsortium Blockchain, die von den Zertifikatsausstellern betrieben wird. Zertifikatsaussteller sind Institution wie Schulen, Universitäten, Industrie- und Handwerkskammern oder Unternehmen. Der Konsortiumsmanager, in diesem Fall die Kontrollinstanz, übernimmt die Rolle der übergeordneten Autorität und ist für den Betrieb und die Aufrechterhaltung der Blockchain verantwortlich. Die Konsortium Blockchain ermöglicht es, dass mehrere vertrauenswürdige Institutionen oder Organisationen gemeinsam die Blockchain betreiben und verwalten.
In der Blockchain werden Referenzen auf die Bildungszertifikate gespeichert. Die Referenzen in der Blockchain beziehen sich auf verschlüsselte PDF Dateien auf dem Server des Zertifikatsausstellers. Dies stellt sicher, dass keine personenbezogenen Daten direkt in der Blockchain gespeichert werden und somit die DSGVO eingehalten wird. Die Referenz, die in die Blockchain geschrieben wird, kombiniert den Namen des Zertifikatsausstellers und den Hashwert des Zertifikats. Diese Kombination stellt sicher, dass die Verbindung zwischen dem Aussteller und dem Zertifikat eindeutig und unveränderlich ist. Jedes Zertifikat kann somit durch seine eindeutige Referenz in der Blockchain identifiziert und überprüft werden. Wenn die Referenz ausschließlich aus dem Hashwert des Zertifikats bestehen würde, bliebe sie selbst nach der Löschung oder Änderung

des Zertifikats weiterhin als gültig bestehen, da die Blockchain Unveränderlichkeit ist. Die IP-Adresse des Zertifikatsausstellers kann sich mit der Zeit ändern, deswegen wird der Name des Zertifikatsausstellers in der Referenz verwendet.
Im Rahmen einer Konsortium Blockchain können die Teilnehmer gemeinsam die Regeln und Richtlinien für den Zugriff und das Schreibrecht festlegen. Um die Integrität und Sicherheit der Blockchain zu gewährleisten, wird der Konsensmechanismus Proof of Authority verwendet. Dieser Mechanismus ermöglicht es, dass nur autorisierte Teilnehmer mit Schreibzugriff auf die Blockchain ausgestattet sind. Der Konsortiumsmanager, der als vertrauenswürdige Instanz agiert, autorisiert die Teilnehmer und überwacht die Einhaltung der Konsensregeln. Dadurch wird sichergestellt, dass nur berechtigte Entitäten die Fähigkeit haben, neue Transaktionen in die Blockchain einzufügen. Die Zertifikatsaussteller, in der Regel Bildungseinrichtungen oder Organisationen, die für die Ausstellung von Zertifikaten verantwortlich sind, haben Schreibrechte auf die Blockchain.
Die Speicherung der Hashwerte der Zertifikate in der Blockchain verhindert die Fälschung von Zertifikaten. Durch die unveränderliche und nachvollziehbare Aufzeichnung aller Transaktionen in der Blockchain werden Manipulationen und Betrug effektiv verhindert. Der Proof-of-Authority Konsensmechanismus ermöglicht eine hohe Skalierbarkeit der Blockchain, da er auf einem ausgewählten Satz von vertrauenswürdigen Knoten basiert. Dadurch können Transaktionen schnell und effizient verarbeitet werden, was für den Einsatz in großen Bildungssystemen von Vorteil ist.

7.2.3. Framework zur Zertifikatserstellung

Das Framework zur Zertifikatserstellung wird von der Kontrollinstanz zur Verfügung gestellt wird und ist nahtlos in bestehende Programme zu integrieren. Es ermöglicht die Ausstellung von Zertifikaten sowohl in Papierform als auch in digitaler Form im PDF-Format.
Das PDF Format ist ein weit verbreitetes und etabliertes Austauschformat, das von den meisten Betriebssystemen und Anwendungen unterstützt wird. Es gewährleistet die Konsistenz und Integrität des Zertifikatslayouts, unabhängig von der Plattform, auf der es angezeigt wird. PDF bietet Sicherheitsfunktionen wie Passwortschutz und Verschlüsselung, die die Vertraulichkeit und Integrität der Zertifikate gewährleisten können. Durch den Einsatz von Sicherheitsfunktionen wie Passwortschutz und Verschlüsselung können die Vertraulichkeit und Integrität der Zertifikate gewährleistet werden. Diese Sicherheitsmechanismen dienen dazu, sicherzustellen, dass die Zertifikate vor unbefugtem Zugriff geschützt sind und ihre Informationen vertraulich bleiben. [PDFb]
Um die Zertifikate für eine maschinelle Verarbeitung zugänglich zu machen, werden die relevanten Daten für den Zertifikatsinhalt in der PDF-Datei als ELMO Format [ELM] eingebettet. Dadurch wird eine strukturierte und standardisierte Darstellung der Zertifikatsdaten ermöglicht, die von automatisierten Systemen leicht gelesen und interpretiert werden kann. ELMO ist ein Datenformat für Austausch von Bildungsinformationen, welches auf den beiden Normen EuroLMAI [EN1a] und MLO [EN1b] basieren. Mit ELMO können Informationen wie Schulungen, Noten, Auslandsaufenthalte usw. in das PDF eingebettet werden.
Der Zertifikatsaussteller ist für die sichere Speicherung der Zertifika-

te verantwortlich. Dies erfolgt in einem dedizierten Speichersystem, das den Zugriff und die Verwaltung der Zertifikate gewährleistet. Der Name der PDF-Datei auf dem Server des Zertifikatsausstellers ist der Hashwert des jeweiligen Zertifikats.
Der Hashwert des Zertifikates wird mit einer mitgelieferten standardisierten Hashfunktion ermittelt. Der Name des Zertifikatsausstellers wird in den Metadaten der PDF-Datei gespeichert.
Nur Organisationen, die vom Konsortiumsmanager die Schreibrechte auf die Blockchain erhalten haben, können die Referenz auf die Zertifikate in die Blockchain schreiben. Dies gewährleistet die Vertraulichkeit und Zugriffssteuerung der Zertifikatsdaten und ermöglicht gleichzeitig eine transparente und nachvollziehbare Überprüfung der Zertifikate.

7.2.4. Webseite zur Verifikation

Die Webseite zur Verifikation von Zertifikaten dient dazu, die Echtheit von Zertifikaten zu überprüfen und einen sicheren Verifikationsprozess zu gewährleisten. Die Webseite wird von der Kontrollinstanz betrieben. Auf diese Weise wird gewährleistet, dass die Verifikation auf einer vertrauenswürdigen Plattform erfolgt und der Prozess von einer autorisierten Instanz überwacht wird.
Abbildung 7.1 veranschaulicht den Verifikationsprozess mit der Blockchain. Ein Flussdiagramm ermöglicht es, komplexe Prozesse in einfachere Schritte zu unterteilen. Dadurch wird der Prozessablauf verständlicher und leichter nachvollziehbar. [Fow04] Der Verifikationsprozess beginnt mit dem Hochladen des Zertifikats in Form eines PDFs. Der Name des Zertifikatsausstellers wird aus den Metadaten des Zertifikats ausgelesen. Anschließend wird mithilfe einer stan-

dardisierten Hashfunktion der Hashwert des Zertifikats berechnet. Im nächsten Schritt wird die Referenz, bestehend aus dem Namen des Zertifikatsausstellers und dem Hashwert des Zertifikats, mit der Blockchain abgeglichen. Sollte die Referenz in der Blockchain vorhanden sein, wird die IP-Adresse des Zertifikatsausstellers herausgesucht. Hierfür existiert eine Datenbank, die von der Kontrollinstanz betrieben wird, die die zugehörigen IP-Adressen für jeden Zertifikatsaussteller enthält. Der Name des Zertifikatsausstellers wird in eine IP-Adresse übersetzt, um die Anfrage an den richtigen Server zu senden. Anschließend wird überprüft, ob das Zertifikat auf dem Server des Zertifikatsausstellers vorhanden ist. Falls das Zertifikat gefunden wird, wird eine Bestätigung an den Benutzer gesendet, die die Echtheit des Zertifikats bestätigt.

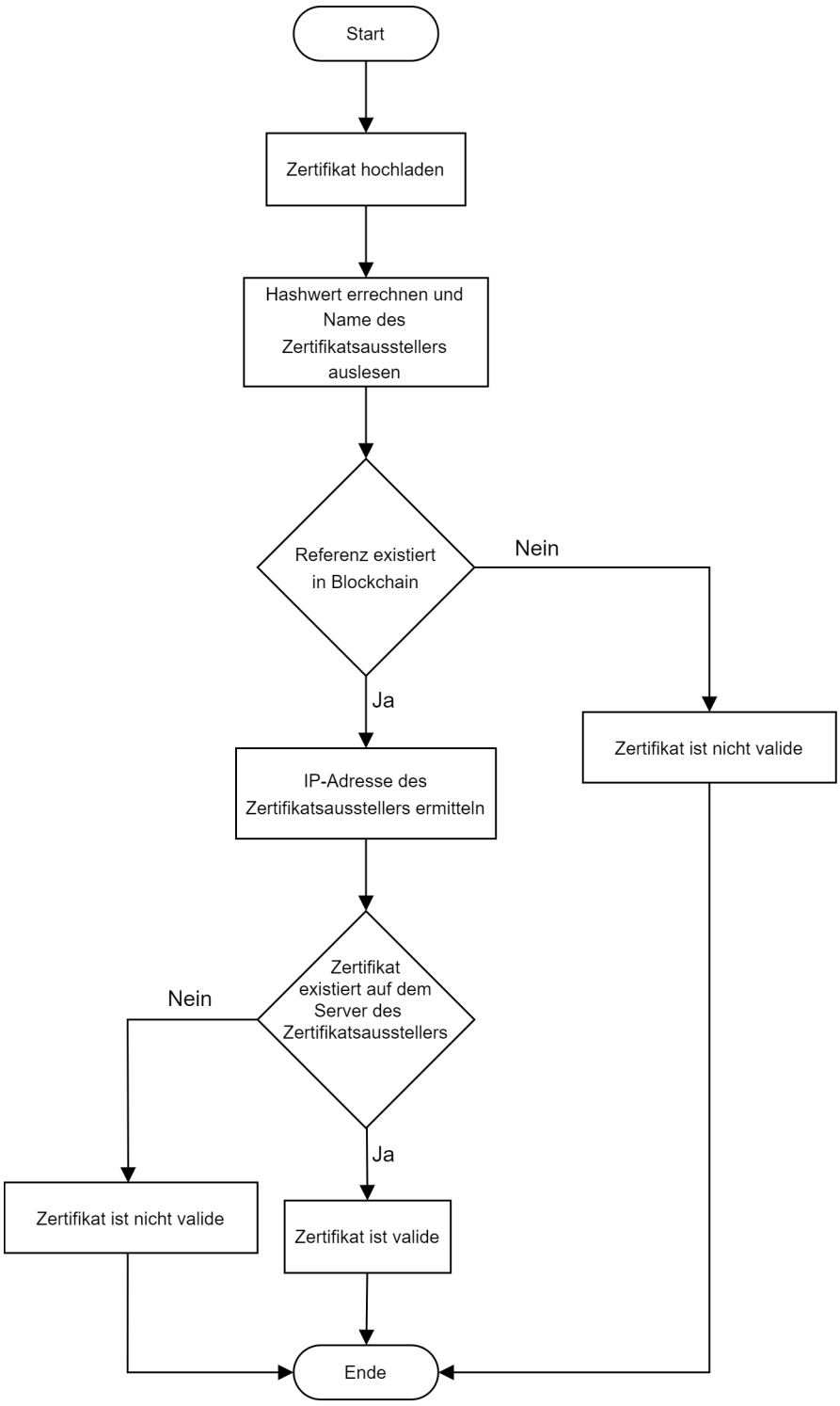

Abbildung 7.1.: Ablauf des Verifikationsprozesses

7.3. Datenmanagement

Das Kapitel Datenmanagement bildet einen wichtigen Bestandteil der Gesamtarchitektur und zielt darauf ab, effektive Mechanismen für die Dateispeicherung und Löschung von Daten zu etablieren. Diese Aspekte sind entscheidend, um die Integrität, Verfügbarkeit und Sicherheit der Informationen zu gewährleisten.

7.3.1. Datenspeicherung

Die Speicherarchitektur spielt eine entscheidende Rolle im Datenmanagement für das Bildungszertifikatssystem. Angesichts der Anforderungen, dass die Zertifikate nicht direkt in der Blockchain, sondern Off-Chain von jedem Zertifikatsaussteller gespeichert werden sollen, ist es wichtig, eine geeignete Speicherart zu wählen, die sowohl die aktuellen Anforderungen als auch die Langzeitspeicherung berücksichtigt. In Deutschland gibt es keine einheitliche Regelung für die Aufbewahrungszeiten von Zeugnissen. Die Aufbewahrungsfristen können je nach Bundesland und Bildungseinrichtung unterschiedlich sein. In Nordrhein-Westfalen beträgt die Aufbewahrungsfrist für Abschlusszeugnisse von Schülerinnen und Schülern 50 Jahre. [SGV]
Im Rahmen der Speicherarchitektur und insbesondere der Langzeitspeicherung wird besonderes Augenmerk auf die Wahl des geeigneten Speichermediums gelegt. Ein vielversprechendes Speichermedium, das für seine Langlebigkeit und Haltbarkeit bekannt ist, ist die M-DISC. Ein Hauptvorteil von optischen Speichermedien liegt in ihrer physikalischen Natur. Die Daten werden durch Laserlicht in die Disc eingebrannt und sind dadurch gegenüber äußeren

Einflüssen wie magnetischen Feldern oder elektrostatischer Entladung unempfindlich. Ein zusätzlicher positiver Aspekt der M-DISC liegt in ihrer potenziellen langen Haltbarkeit. Herstellerangaben zufolge kann die M-DISC eine Lebensdauer von bis zu 1.000 Jahren haben.[MDI]
Das PDF/A-Format wurde als spezielle Variante des PDF-Formats entwickelt und ist darauf ausgerichtet, elektronische Dokumente langfristig zu archivieren. Es wurde geschaffen, um sicherzustellen, dass die gespeicherten Daten auch über einen langen Zeitraum hinweg lesbar und zugänglich bleiben. [PDFa]

7.3.2. Löschung von Daten

Wie in Kapitel 4 beschrieben haben betroffenen Personen Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten, dazu gehört das Recht auf Löschung von Daten. [DSG, Artikel 12-23]
Die Zertifikatslöschung im Rahmen der Zertifikatsverwaltung erfolgt auf einfache und effiziente Art und Weise, indem die entsprechende Datei auf dem Server des Zertifikatsausstellers entfernt wird. Durch das Entfernen der Datei wird sichergestellt, dass die Referenz zu diesem Zertifikat nicht mehr funktioniert. Bei dem Verifikationsprozess des Zertifikats kann die Datei nicht mehr abgerufen werden, somit wird das Zertifikat als nicht valide.

8. Evaluationsanalyse

Die Evaluation und der Vergleich mit anderen Konzepten sind entscheidende Schritte im Softwareengineering, um die Qualität und Effektivität des entwickelten Konzepts zu bewerten. Diese Phase ermöglicht es, das Konzept kritisch zu prüfen und Schwachstellen zu identifizieren. Im Wasserfallmodell erfolgt die Konzeptevaluation in der Entwurfsphase. [PB14]

8.1. Evaluationsmethode

Evaluationsmethoden spielen eine wichtige Rolle bei der Bewertung von Konzepten, um ihre Stärken, Schwächen und Potenziale zu identifizieren. Eine häufig verwendete Methode zur Evaluation ist die Vergleichsanalyse, bei der das zu evaluierende System mit einem anderen System oder einem etablierten Referenzstandard verglichen wird. Durch den Vergleich mit anderen ähnlichen Systemen, Produkten oder Lösungen können Benchmarks erstellt werden. Dies ermöglicht es, die Leistung und den Fortschritt des zu evaluierenden Systems im Vergleich zu anderen zu beurteilen. Eine Vergleichsanalyse hilft dabei, die Stärken und Schwächen des zu evaluierenden Systems im Vergleich zu anderen herauszuarbeiten. Dadurch können gezielte Verbesserungsmaßnahmen ergriffen

werden, um die Leistung und Effektivität des Systems zu optimieren.

8.2. Bewertungskriterien

Für die Vergleichsanalyse werden Bewertungskriterien festgelegt, auf die sich besonders konzentriert wird. Skalierbarkeit ist ein wichtiges Kriterium, da es die Anpassungsfähigkeit einer Lösung an wachsende Anforderungen und steigende Benutzerzahlen betrifft. Eine skalierbare Lösung ist in der Lage, ihre Leistungsfähigkeit beizubehalten und auf steigende Lasten oder größere Datenmengen zu reagieren, ohne dass dies zu Leistungseinbußen führt. Effizienz ist ein zentrales Bewertungskriterium, da sie die Leistungsfähigkeit einer Lösung in Bezug auf Zeit- und Ressourcennutzung widerspiegelt. Eine effiziente Lösung ist in der Lage, Aufgaben und Prozesse schnell und mit minimaler Ressourcennutzung auszuführen. Durch die Konzentration auf die Funktionalität können die Lösungen hinsichtlich ihrer Erfüllung der gestellten Anforderungen bewertet werden.

8.3. Datenerhebung

Bei der Datenerhebung im Rahmen der Evaluationsanalyse wird das System EMREX [EMR] genauer betrachtet und seine Architektur vorgestellt. Die Architektur eines Systems gibt einen Einblick in seine grundlegende Struktur und Funktionsweise. EMREX ist ein europäisches Netzwerk und System zur elektronischen Übertragung von Studienleistungen und -ergebnissen zwischen Hochschulen

und Bildungseinrichtungen. Durch den Vergleich des zu evaluierenden Systems mit EMREX können wertvolle Erkenntnisse gewonnen werden. EMREX wird in den Niederlanden als Verfahren für den elektronischen Austausch für Daten von Studierenden verwendet. Bisher wurden nur in den Niederlanden 10 Millionen Zertifikate im Netzwerk gespeichert. [Neta] Im Folgenden werden die Hauptkomponenten der EMREX-Architektur erläutert:

- EMC: Der EMREX Client bietet den Benutzern eine Schnittstelle, über die sie auf ihre eigenen Bildungsdaten zugreifen, sie verwalten und mit anderen Institutionen teilen können. Dies umfasst Funktionen wie das Hochladen und Teilen von Transkripten, Zeugnissen oder anderen relevanten Dokumenten, das Suchen nach passenden Studienprogrammen oder Austauschmöglichkeiten, die Verwaltung von Anfragen und die Kommunikation mit anderen Institutionen.

- EMP: Der EMREX Contact Point ist der Zugangspunkt, den der EMC nutzt, um Ergebnisse von der Bildungsinstitution abzurufen. Innerhalb eines Netzwerks können mehrere EMPs existieren, wobei ein EMP entweder eine einzelne oder mehrere Bildungsinstitutionen repräsentieren kann. Die gängigste Lösung besteht darin, dass ein EMP alle Institutionen eines Landes repräsentiert. Die genaue Ausgestaltung eines EMPs kann von Land zu Land variieren.

- EWP Registry: EMREX Registry dient als zentrale Datenbank, in der Informationen über die teilnehmenden Hochschulen, ihre Studiengänge, Kurse und andere relevante Daten gespeichert werden. Sie bildet die Grundlage für den Austausch von Bildungsdaten und die Anerkennung von Studienleistungen. Der EMC verwendet das EWP Registry, um den zuständigen EMP zu finden.

Für alle Zertifikate im EMREX-System wird das ELMO-Format verwendet. ELMO ist ein standardisiertes Datenformat, das speziell für den Austausch von Bildungsdaten entwickelt wurde. [ELM]
Der Ablauf der Zertifikatsabfrage in einem EMREX-System, wie in Abbildung 8.1 veranschaulicht, startet mit dem Einloggen auf dem EMC (EMREX-Client). Sobald der Benutzer angemeldet ist, wird eine Anfrage an das EWP Registry gesendet, um den zugehörigen EMP (EMREX Contact Point) zu ermitteln. Die EMP dient als Vermittler zwischen dem EMC und den beteiligten Bildungsinstitutionen. Der EMP sendet Anfragen an alle relevanten Bildungsinstitutionen, um die entsprechenden Zertifikate für den jeweiligen Benutzer abzurufen. Der EMC erhält die validierten Zertifikate vom EMP und stellt sie dem Benutzer zur Verfügung. Anschließend kann der Nutzer auf die Zertifikate zugreifen, deren Gültigkeit überprüfen und sie bei verschiedenen Gelegenheiten nutzen, beispielsweise bei der Bewerbung um einen Studienplatz oder für die Anerkennung von Studienleistungen. [Netb]
Eine gesamte Implementierung von Zertifikaten für eine Bewerbung bei einer Universität oder einem Unternehmen existiert noch nicht. In Norwegen existiert ein Pilotprojekt für die Implementierung von EMREX in das Bewerbungsportal. [Nor]

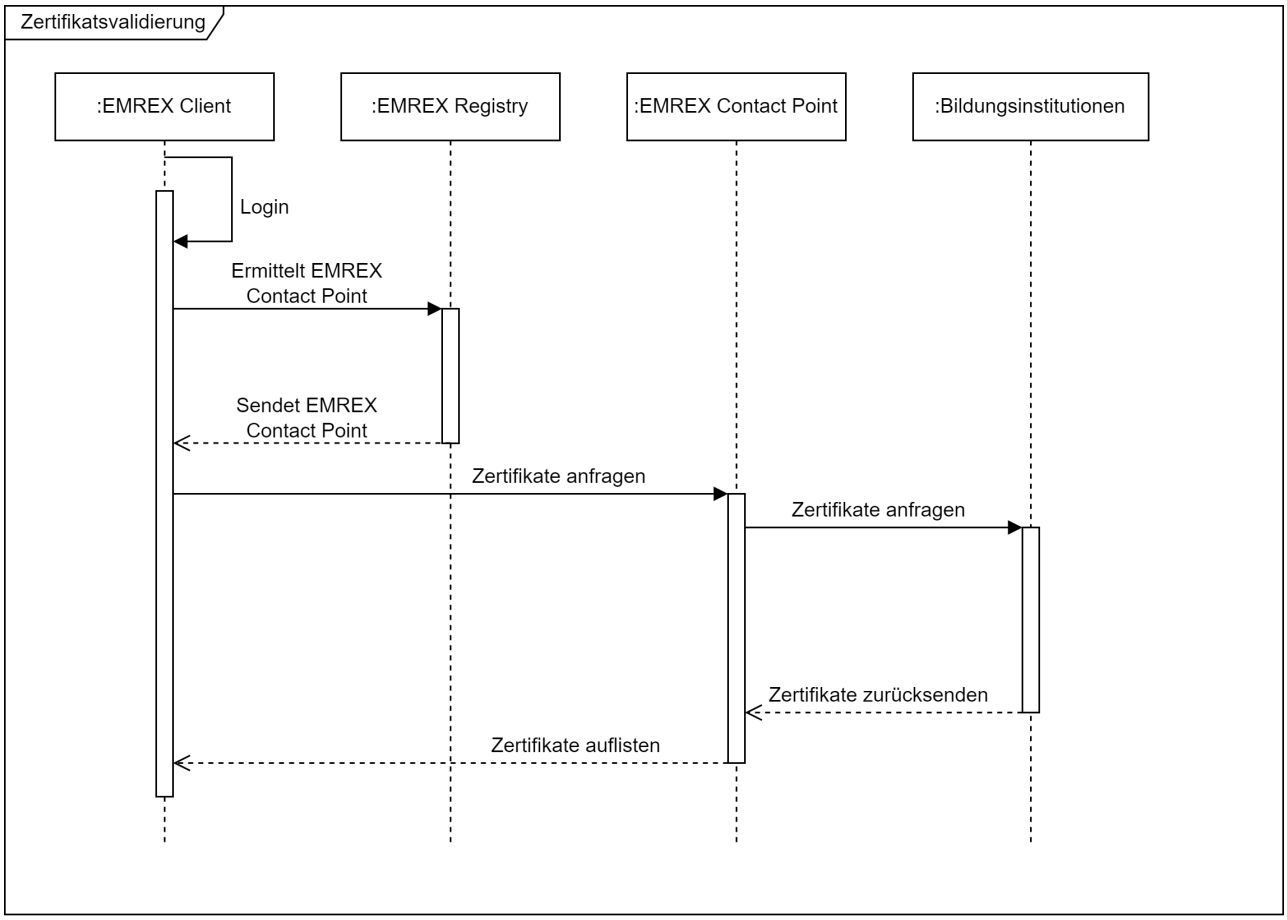

Abbildung 8.1.: Zertifikatsabfrage in EMREX

8.4. Vergleichsanalyse

Die Vergleichsanalyse zwischen dem erarbeiteten Konzept und dem EMREX-System ermöglicht eine Bewertung der Unterschiede und Gemeinsamkeiten zwischen den beiden Ansätzen.

- Effizienz:
  - Im erarbeiteten System erfolgt die Verifikation der einzelnen Zertifikate durch zwei Abfragen. Zunächst wird das Zertifikat auf der Blockchain überprüft, um sicherzustellen, dass es nicht manipuliert worden ist. Anschließend wird eine weitere Abfrage auf dem Server des Zertifikatsausstellers durchgeführt, um die Echtheit und Gültigkeit des Zertifikats zu bestätigen.
  - Im Vergleich dazu zeichnet sich das EMREX System durch eine effiziente Arbeitsweise aus. Die Bildungszertifikate werden vom EMP (EMREX Contact Point) von allen relevanten Bildungsinstitutionen zusammengetragen. Das Zusammentragen aller Zertifikaten des Benutzers erfolgt simultan.
- Skalierbarkeit:
  - Im erarbeiteten System muss sowohl die Blockchain als auch die Datenbank des Zertifikatsausstellers müssen entsprechend skaliert werden, um den steigenden Anforderungen und dem wachsenden Benutzerstamm gerecht zu werden. In einer Konsortium-Blockchain ist die Anzahl der Teilnehmer beschränkt, wodurch eine reibungslose

und schnelle Verarbeitung der Transaktionen gewährleistet wird. Aufgrund dieser Begrenzung der Teilnehmeranzahl behält eine Konsortium-Blockchain auch bei zunehmender Nutzerzahl und steigendem Transaktionsvolumen eine hohe Leistungsfähigkeit und Stabilität bei. Die Datenbank des Zertifikatsausstellers kann durch vertikales oder horizontales Skalieren erweitert werden.

  - Im EMREX System liegt der Fokus der Skalierbarkeit in erster Linie auf der Datenbank der Bildungsinstitutionen. Durch die Kombination von vertikaler und horizontaler Skalierung können Bildungsinstitutionen die Leistung und Kapazität ihrer Datenbanksysteme verbessern und somit effizienter auf das Wachstum der Studentendaten und Anfragen reagieren. Dies ermöglicht eine reibungslose Abwicklung des Datenmanagements und eine bessere Bewältigung steigender Belastungen. Im EMREX-System ist es im Gegensatz zum erarbeiteten System lediglich erforderlich, eine zentrale Datenbank zu skalieren, anstatt zwei separate Datenbanken.

- Funktionalität:

  - Das erarbeitete System konzentriert sich gezielt darauf, die Zertifikatsverifikation in Bewerbungsprozessen zu verbessern. Es wurde entwickelt, um die Anforderungen und Bedürfnisse der Stakeholder in Bezug auf die Verifikation von Zertifikaten zu erfüllen. Das System bietet effektivere Mechanismen zur Überprüfung der Echtheit und Gültigkeit von Zertifikaten, was zu einem effizienteren und vertrauenswürdigen Bewerbungsprozess führt.

– Das EMREX-System wurde hauptsächlich entwickelt, um die Kooperation und den Datenaustausch zwischen verschiedenen Bildungseinrichtungen zu erleichtern und zu verbessern. Sein Hauptziel ist es, den Transfer von Bildungsinformationen, wie akademischen Leistungen und Zertifikaten, nahtloser und effizienter zu gestalten. Trotzdem erfüllt es nicht alle Anforderungen, vor allem, wenn es um den Bewerbungsprozess für Unternehmen geht. Jedoch erfüllt das EMREX-System nicht alle Anforderungen, insbesondere in Bezug auf den Bewerbungsprozess für Unternehmen. In diesem spezifischen Kontext zeigt das EMREX-System gewisse Einschränkungen und deckt nicht alle Bedürfnisse und Erwartungen von Unternehmen und Arbeitgebern im Rahmen der Zertifikatsverifikation ab.

8.5. Ergebnisse

Das erarbeitete Konzept erfüllt alle festgelegten Anforderungen im Vergleich zum IMREX-System. Es bietet eine zuverlässige und sichere Plattform für den Austausch von Bildungsdaten, die den Bedürfnissen der Zertifikatsaussteller und der Zertifikatsträger entspricht. Das IMREX-System zeigt eine deutlich höhere Effizienz in Bezug auf die Abfrage von Zertifikaten. Im Vergleich dazu kann im erarbeiteten Konzept nur ein Zertifikat gleichzeitig abgefragt werden, was zu geringfügigen Einschränkungen in Bezug auf die Effizienz führt. Das IMREX-System zeigt ebenfalls eine bessere Skalierbarkeit in Bezug auf die Validierung der Zertifikate, da nur eine Datenbank betrieben werden muss. Im erarbeiteten Konzept hingegen müssen zwei separate Datenbanken für die Validierung der Zertifikate verwaltet werden.

9. Fazit

Das erarbeitete Konzept hat sich als effektives Instrument zur Verbesserung des Datenaustauschs im Bildungsbereich erwiesen. Es erfüllt die definierten Anforderungen und bietet eine zuverlässige Plattform für den Austausch von Bildungsdaten. Allerdings ist zu beachten, dass das Konzept auf Länder zugeschnitten ist, in denen die Datenschutz-Grundverordnung (DSGVO) gilt. In Ländern wie Nigeria, die nicht unter die DSGVO fallen, wäre das Konzept ohne weitere Anpassungen nicht direkt anwendbar. Die Evaluationsanalyse hat gezeigt, dass das IMREX-System im Vergleich zum erarbeiteten Konzept effizienter und besser skalierbar ist. Es bietet eine höhere Leistungsfähigkeit bei der Abfrage von Zertifikaten und erfordert nur geringfügige Anpassungen, um den Anforderungen gerecht zu werden. Dies weist darauf hin, dass das IMREX-System bereits eine solide Basis für den Bildungsdatenaustausch bietet und nur noch entsprechend angepasst werden muss. In Bezug auf die verwendete Blockchain-Technologie hat sich herausgestellt, dass sie im erarbeiteten Konzept eher ein Hindernis darstellt. Eine herkömmliche Speicherlösung kann die gleichen Anforderungen erfüllen, ohne die Komplexität und zusätzliche Ressourcen einer Blockchain. Daher könnte die Entfernung der Blockchain und der Einsatz eines regulären Speichersystems eine sinnvolle Verbesserung sein.

Literaturverzeichnis

[AMB19] Anett Mehler-Bicher, Nicolai Kuntze Sibylle Kunz Bernhard Ostheimer Lothar Steiger Hans-Peter W. Frank Mehler M. Frank Mehler: *Wirtschaftsinformatik Klipp und Klar.* Springer Fachmedien Wiesbaden;Springer Gabler, 2019. – ISBN 3658264934, 978–3658264932

[AS13] Andrew Stellman, Jennifer G.: *Learning Agile: Understanding Scrum, XP, Lean, and Kanban.* 1. O'Reilly Media, 2013. – ISBN 1449331920, 978–1449331924

[Bas17] Bashir, Imran: *Mastering Blockchain.* 2017. – ISBN 1787125440,978–1787125445

[BBC] *Tanzania's President Magufuli sacks 10,000 over fake certificates.* `https://www.bbc.com/news/world-africa-39745362`, Abruf: 04.04.2023

[Bloa] *Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.* `https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf`, Abruf: 07.06.2023

[Blob] *Blockchain und Datenschutz.* https://www.bitkom.org/sites/default/files/file/import/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf, Abruf: 08.06.2023

[But13] Buterin, Vitalik: *Ethereum White Paper: A Next Generation Smart Contract / Decentralized Application Platform.* https://github.com/ethereum/wiki/wiki/White-Paper. Version: 2013, Abruf: 07.06.2023

[Dat] *White Paper Datenschutz in der Blockchain.* https://publica-rest.fraunhofer.de/server/api/core/bitstreams/a0954b60-9304-4f68-ac6f-560886860150/content, Abruf: 08.06.2023

[DSG] *DSGVO Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR).* https://dsgvo-gesetz.de/, Abruf: 20.04.2023

[EJB16] Eric J. Braude, Michael E. B.: *Software Engineering: Modern Approaches.* 2. Waveland Press, Inc., 2016. – ISBN 1478632305, 978–1478632306

[ELM] *ELMO XML Format.* https://github.com/emrex-eu/elmo-schemas, Abruf: 05.07.2023

[EMR] *EMREX.* https://emrex.eu/, Abruf: 09.07.2023

[EN1a] *DIN EN 15981 Europäisches Modell für Lernermobilität - Angaben über die Leistung (EuroLMAI).* https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:136531652, Abruf: 04.07.2023

[EN1b] *DIN EN 15982 Metadaten für Lernangebote (MLO).* https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:139945569, Abruf: 04.07.2023

[Fau19] Faulbaum, Frank: *Methodische Grundlagen der Umfrageforschung.* 1. Aufl. Springer Fachmedien Wiesbaden; Springer VS, 2019. – ISBN 3531178776;978–3531178776

[Fin] Finanzen, Bundesministerium der: *Blockchain-Strategie der Bundesregierung.* https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=1, Abruf: 08.06.2023

[Fow04] Fowler, Martin: *UML distilled: a brief guide to the standard object modeling language.* 3rd ed. Addison-Wesley Professional, 2003;2004. – ISBN 9780321193681, 978–0321193681

[Fra] *Tackling the Rise of Fake Qualifications in Nigeria.* https://thisisafrica.me/politics-and-society/tackling-rise-fake-qualifications-nigeria/, Abruf: 04.04.2023

[HGF20] Hans-Georg Fill, Andreas M.: *Blockchain kompakt: Grundlagen, Anwendungsoptionen und kritische*

Bewertung. 1. Aufl. 2020. Springer Fachmedien Wiesbaden;Springer Vieweg, 2020 (IT kompakt). – ISBN 3658274603, 978–3658274603

[IBM] *IBM Food Trust*. https://www.ibm.com/de-de/products/supply-chain-intelligence-suite/food-trust, Abruf: 08.06.2023

[Kic] *Let's Build What's Next for Crowdfunding Creative Projects*. https://www.kickstarter.com/articles/lets-build-whats-next-for-crowdfunding-creative-projects, Abruf: 07.06.2023

[Lin20] Lindner, Dominic: *Forschungsdesigns der Wirtschaftsinformatik: Empfehlungen für die Bachelor- und Masterarbeit*. 1. Aufl. Springer Fachmedien Wiesbaden;Springer Gabler, 2020. – ISBN 3658311398,978–3658311391

[Max19] Maxim, Roger S. Pressman; Bruce R.: *Software Engineering: A Practitioner's Approach*. 9. McGraw-Hill Education, 2019. – ISBN 1260548007, 978–1260548006

[MDI] *M-DISC*. https://www.mdisc.com/, Abruf: 29.06.2023

[Nak08] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://bitcoin.org/bitcoin.pdf. Version: 2008, Abruf: 20.04.2023

[Neta] *EMREX Netherlands*. https://emrex.eu/the-netherlands/, Abruf: 09.07.2023

[Netb] *EMREX Network Architecture*. https://emrex.eu/wp-content/uploads/2020/01/Technical-Guide-to-EMREX.pdf, Abruf: 09.07.2023

[Nor] *Norwegen Automatisierung der Zulassung.* https://emrex.eu/2023/01/31/emrex-newsletter-january-2023/, Abruf: 09.07.2023

[PB14] Pierre Bourque, Richard E. F.: *Guide to the Software Engineering Body of Knowledge (SWEBOK(r)): Version 3.0.* IEEE Computer Society Press, 2014. – ISBN 0769551661, 978–0769551661

[PDFa] *ISO 19005-1:2005 Document management — Electronic document file format for long-term preservation — Part 1: Use of PDF 1.4 (PDF/A-1).* https://www.iso.org/standard/38920.html, Abruf: 29.06.2023

[PDFb] *PDF association.* https://pdfa.org/resources/, Abruf: 29.06.2023

[Rob12] Robertson, Suzanne Robertson; J.: *Mastering the Requirements Process: Getting Requirements Right.* 3rd Edition. Addison-Wesley Professional, 2012. – ISBN 0321815742,9780321815743

[Sch14] Schibi, Ori: *Managing stakeholder expectations for project success : a knowledge integration framework and value focused approach.* J Ross Publishing, 2014. – ISBN 1604270861, 978–1604270860

[SGV] *Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I).* https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=2&gld_nr=2&ugl_nr=223&bes_id=10526&aufgehoben=N&menu=&sg=0, Abruf: 29.06.2023

[Tra] *TradeLens*. https://www.tradelens.com/, Abruf: 20.06.2023

[Wal15] WALPORT, Mark: *Distributed Ledger Technology: beyond block chain*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Version: 2015, Abruf: 20.04.2023

A. Anhang

A.1. Interview mit Ingenieursfirmen

- Frage 1: Wie gestalten Sie derzeit den Bewerbungsprozess in Bezug auf die Verifizierung von Zertifikaten und Qualifikationen der Bewerber?
  - Prüfung anhand von digitalen Scans verarbeiten
  - Verifizierung anhand von beglaubigten Kopie
  - Verifizierung erfolgt durch Kontaktierung der ausstellenden Institutionen (OSCP)
- Frage 2: Welche Herausforderungen und Schwierigkeiten sehen Sie in Bezug auf den Bewerbungsprozess im Zusammenhang mit Zertifikaten?
  - Keine automatische Weiterverarbeitung der PDFs
  - Auswertung erfolgt manuell von einer Person
  - Weiterverarbeitung von Hochschulzertifikaten/Schulabschlüssen erfolgt manuell

- Frage 3: Inwiefern hat der Bewerbungsprozess mit Zertifikaten Auswirkungen auf die Geschwindigkeit und Genauigkeit Ihrer Auswahlverfahren?
  - Manuelle Überprüfung der Zertifikate kann zeitaufwendig sein und den Prozess verzögern
  - Der Bewerbungsprozess kann leicht verzögert werden
- Frage 4: Wie könnten Verbesserungen im Bewerbungsprozess mit Zertifikaten Ihre Arbeitsabläufe, die Effizienz und die Qualität der Bewerberauswahl beeinflussen?
  - Automatisierte Verifizierung von Zertifikaten würde Arbeitsabläufe vereinfachen
  - Reduzierung des Zeitaufwands für die manuelle Weiterverarbeitung von Zertifikaten im Bewerbungsprozess
  - Die Effizienz der Bewerberqualifikationen wird durch schnelle und zuverlässige Überprüfung verbessert

A.2. Interview mit Studierenden und Schülern

- Frage 1: Welche Herausforderungen oder Schwierigkeiten treten bei der Nutzung des aktuellen Systems auf?
  - Aufbewahrung ist nur in Papierform, vorhanden und nicht digital
  - Eigenes Einscannen der Zeugnisse
  - Lange Wartezeiten beim Amt für die Beglaubigung
  - Beglaubigungsprozess ist träge und dauert lange
- Frage 2: Wie empfinden Sie die Zugänglichkeit des Systems, insbesondere in Bezug auf die Verfügbarkeit von Bildungszertifikaten und die Möglichkeit, diese an potenzielle Arbeitgeber oder Bildungseinrichtungen zu übermitteln?
  - Zeugnisse sind nur in Papier zugänglich
  - Eigenes Einscannen ist notwendig
  - Originalzeugnisse müssen an einem Ort aufbewahrt werden
- Frage 3: Was würden Sie sich von einem verbesserten System wünschen, um die Benutzerfreundlichkeit, Zugänglichkeit und Sicherheit beim Verwalten und Übermitteln von Bildungszertifikaten zu verbessern?
  - Zeugnisse auch in digitaler Form
  - Beglaubigungsprozess effizienter gestalten

  - Zeugnis als PDF ausstellen
  - Zertifikate sollen sicher gespeichert werden

A.3. Interview mit Schule

- Frage 1: Wie erfolgt derzeit die Verwaltung und Ausstellung von Zertifikaten an Ihrer Schule?
  - Zeugnisse werden in Papierform ausgegeben
  - Abschlusszeugnisse werden für 50 Jahre archiviert
  - Zeugnisse werden digital archiviert
- Frage 2: Welche Herausforderungen oder Schwierigkeiten treten bei der Verwaltung und Ausstellung von Zertifikaten auf?
  - Zeugnisse können nur in Papierform ausgegeben werden und nicht in Digitalform
  - Ersatzzeugnisses kann nur in digitaler Form ausgestellt werden, bei Umzügen kann das zu Problemen führen