Digital identitymanagement for decentralized service platforms

Masterarbeit

Berisha Ilirjana

Matrikelnummer: S15530850

Referent: Dr. C. Hitz
Co-Referent: Dr. M. Gellrich

School of Management and Law
Zurich University of Applied Sciences

Diese Arbeit wurde eingereicht zur Erlangung des Titels
Master of Science (MSc) ZHAW in Wirtschaftsinformatik

Mai 2023

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Diplomarbeit die Sprachform des generischen Maskulinums angewendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschliessliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

Management Summary

In der heutigen digitalen Welt gewinnt das Thema Identitätsmanagement zunehmend an Bedeutung, da traditionell zentralisierte Ansätze häufig Sicherheits- und Datenschutzprobleme aufweisen. Daher besteht die Notwendigkeit, alternative Lösungen zu erforschen und zu entwickeln, die den Nutzern eine sichere und selbstbestimmte Verwaltung ihrer Identität ermöglichen. Die Ausgangslage ist geprägt von der steigenden Verbreitung von Blockchain-Technologie und dem aufkommenden Konzept der Self-Sovereign Identity (SSI). Eine public permissionless Blockchain bietet ein dezentrales und transparentes Umfeld, das neue Möglichkeiten für das Identitätsmanagement eröffnet. Dennoch existieren noch keine etablierten Modelle oder Standards für ein solches dezentrales Identitätsmanagement in einer public permissionless Blockchain. Das Ziel dieser Forschung ist die Identifizierung und Analyse der Anforderungen an ein solches Modell. Dabei wurden die identifizierten Anforderungen für die ersten Schritte zur Entwicklung eines Identitätsmanagement-Modells verwendet.

Um die Anforderungen zu identifizieren, wird ein iterativer Ansatz verwendet, der das Design Science Research Framework mit dem Design Theorizing Framework kombiniert. Bei der Recherche relevanter Literatur wurden aufgrund der technologischen Entwicklungen im untersuchten Bereich hauptsächlich Publikationen aus den letzten drei Jahren berücksichtigt.

Die Ergebnisse dieser Arbeit liefern einen umfassenden Leitfaden für die Entwicklung eines dezentralen Identitätsmanagement-Modells, das den identifizierten Anforderungen an Dezentralisierung, Standardisierung, Interoperabilität, Privatsphäre und Kontrolle, Implementierung, Sicherheit, Compliance, Nutzerakzeptanz sowie Stellvertretung und Vererbung gerecht wird. Es wurde eine theoretische Evaluierung des entwickelten Modells anhand der identifizierten Anforderungen durchgeführt sowie eine praktische Evaluierung anhand von zwei realen Anwendungsfällen. In der Evaluation wird festgestellt, dass das entwickelte Modell zwar den meisten aber nicht allen Anforderungen gerecht wird. Die Anforderungen Interoperabilität und Implementierungen konnten bei der theoretischen Evaluation nicht beurteilt werden, da diese aus technischer Sicht noch erforscht werden

müssen. Des Weiteren bestehen noch Optimierungsbedarf bei der Regelung der Vererbung einer digitalen Identität sowie bei der Unterscheidung der Identitäten einer real oder digital existierenden Persönlichkeit.

Durch die Kombination von theoretischer Fundierung und praktischer Anwendbarkeit trägt diese Arbeit zur Lösung des Problems des Identitätsmanagements mittels Blockchain-Technologie und SSI bei und fördert die Entwicklung sicherer, dezentraler und benutzerfreundlicher Identitätslösungen. Es ist wichtig anzumerken, dass das entwickelte Modell zwar vielversprechende Ergebnisse liefert, jedoch weitere Forschung und Entwicklung notwendig sind, um den vollen Umfang der Herausforderungen im Bereich des Identitätsmanagement auf dezentralisierten Plattformen zu bewältigen. Die in dieser Masterarbeit erzielten Erkenntnisse stellen eine solide Grundlage für zukünftige Forschungsarbeiten dar und tragen zu einem tieferen Verständnis bei, wie das Identitätsmanagement auf dezentralisierten Plattformen effektiv angegangen werden kann.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzungen

bzw.	beziehungsweise
CCPA	California Consumer Privacy Act
d.h.	das heisst
dApps	decentralized Application
DID	Decentralized Identifiers
DIDcomm	Decentralized Identifier Communication
DLT	Distributed-Ledger-Technology
DPA	Data Processing Agreement
DSGVO	Datenschutz-Grundverordnung
eIDAS	rechtliche Grundlage für elektronische Identitfizierung und Vertrauensdienst in der Europäischen Union
ePA	elektronischer Personalausweis
ID	Identität
IdM	Identitätsmanagement-Modell
IdP	Identity Provider
IdT	Identitätsträger
IoT	Internet of Things
KI	Künstliche Intelligenz
LGPD	General Personal Data Protection LAW

NFT	Non-Fungible Token
PK	private key
SP	Service-Provider
SSI	Self-Sovereign Identity
VC	Verifiable Credentials
vgl.	vergleiche
VP	Verifiable Presentation
z. B.	zum Beispiel
ZGB	Zivilgesetzbuch
ZKP	Zero Knowledge Proof

1 Einleitung

Dieses Kapitels bietet dem Leser einen umfassenden Überblick über den Aufbau und Inhalt dieser Masterarbeit. Sie umfasst die Ausgangslage, die Relevanz der Arbeit, die Zielsetzung und Forschungsfrage, die inhaltliche Abgrenzung sowie den Aufbau der gesamten Arbeit.

1.1 Ausgangslage

Im digitalen Zeitalter sind Identitäten ein wertvolles Gut, insbesondere für die digitale Transformation und den Schutz vor Cyberkriminalität (Rohrer, 2022). Im Gegensatz zur analogen Identität, die in der Regel durch äussere Merkmale definiert wird, ist die digitale Identität vielfältiger und umfasst eine Teilmenge von Attributen einer Person (Rohrer, 2022). Individuen nutzen verschiedene digitale Identitäten für unterschiedliche Zwecke und Dienste wie zum Beispiel für den Zugriff auf Sozialmediakanäle, Onlineshops oder das Ausfüllen der Steuererklärung (Rohrer, 2022). Wenn eine Person in der analogen Welt ihre Identität nachweisen muss, wird die Vorlage eines amtlich ausgestellten Ausweises, zum Beispiel eines Reisepasses oder Personalausweises genutzt (Rohrer, 2022). Amtlich ausgestellte Dokumente können durch alleiniges Vorweisen Zugang zu Dienstleistungen und anderen Serviceleistungen ermöglichen, ohne dabei einen elektronischen Fingerabdruck zu hinterlassen (Rohrer, 2022).

In der digitalen Welt hingegen erfordert der Nachweis ihrer Identität verschiedene Methoden, die häufig die Weitergabe persönlicher Daten und die Dienstleistungen von Identitätsanbietern erfordern (Rohrer, 2022). Diese Anbieter speichern und verwalten unsere Daten und senden bei jeder Identifikationsanfrage Kopien unseres Ausweises an die von uns genutzten Webdienste (Rohrer, 2022). Diese aus Nutzersicht komfortable Lösung wirft Bedenken hinsichtlich des Datenschutzes auf, da sie nicht nur ihre Identität angeben, sondern auch Kopien ihres Ausweises bei einem privaten Unternehmen hinterlegen (Rohrer, 2022). Die steigende Verbreitung digitaler Lösungen erhöht die Wichtigkeit von Mechanismen zur Etablierung von Vertrauen in digitale Identitäten und deren Verwahrung (LEI,

2020). Der Umgang mit digitalen Identitäten stellt ein anspruchsvolle Thematik dar, das nicht nur technische sondern auch organisatorische und rechtliche Fragen aufwirft (Anke & Richter, 2023, S. 278-279).

Eine Umstellung von zentralisierten zu dezentralen Identitäten ist notwendig, um den Fokus auf den Menschen zu legen und sich von geschlossenen, beziehungsweise zentral verwalteten Identitätssystemen, zu lösen (Wrobel, 2022). Deshalb gibt es einen wachsenden Bedarf an dezentralen Identitätsmanagement-Modellen, die auf der Blockchain-Technologie basieren (Wrobel, 2022). Die Blockchain-Technologie kann Identitätsdaten sicher und vertrauenswürdig verwalten, indem sie ein System nutzt, das dezentral, transparent und unveränderlich ist (Wrobel, 2022). Ein Paradigmenwechsel zu dezentralen Identitäten würde es Einzelpersonen ermöglichen, ihre eigene Identität zu besitzen und zu kontrollieren, was zu einem verbesserten Datenschutz führt und die Abhängigkeit von zentralisierten Organisationen verringert (Rohrer, 2022). Obwohl die Vorteile einer selbstverwalteten Identität und des Schutzes der Privatsphäre bekannt sind, bestehen ungelöste Fragen hinsichtlich der Datenverwaltung und -aufbewahrung, sowie der Vertrauensbildung im generellen (Rohrer, 2022).

1.2 Relevanz der Arbeit

Das World Wide Web (WWW) hat in den letzten Jahrzehnten eine grundlegende Veränderung der Informationsaustauschmöglichkeiten bewirkt (Voshmgir, 2020). Mit dem Aufstieg des Web2 wurden Interaktionen und der Handel über das Internet massentauglich (Voshmgir, 2020). Online-Plattformen ermöglichten der Gesellschaft die weltweite Kommunikation, den Kauf von Waren und Dienstleistungen sowie den Austausch von Wissen (Voshmgir, 2020). Dennoch stehen sie auch weiterhin vor grundlegenden Herausforderungen, insbesondere im Bereich des Identitätsmanagements (Voshmgir, 2020). Bisher wurden vor allem analoge Nachweise wie Ausweise, Zertifikate und andere physische Dokumente verwendet, um die Identität gegenüber anderen Parteien nachzuweisen (Urban, 2022). Allerdings stossen diese herkömmlichen Methoden in der digitalen Welt auf zahlreiche Schwierigkeiten und Risiken (Urban, 2022). Denn die Übertragung analoger Identitätsnachweise in die digitale Welt erweist sich als komplexer Prozess (Urban, 2022). Eine einfache Digitalisierung der physischen Dokumente, beispielsweise durch Fotos oder Scans, genügt oft nicht den Anforderungen (Urban, 2022). Dies erfordert eine aufwändige Überprüfung der Nachweise auf der Empfängerseite, um ihre Echtheit und Gültigkeit zu bestätigen (Urban, 2022). Darüber hinaus birgt die rein digitale Erfassung von Nachweisen erhebliche Sicherheitsrisiken, da Sicherheitsmerkmale der Originaldokumente bei

der Fotografie oder dem Scannen verloren gehen oder nicht richtig funktionieren können (Urban, 2022). In der heutigen digitalen Welt werden die Menschen gezwungen, sich bei verschiedenen Plattformen und Diensten anzumelden, persönliche Daten preiszugeben und Vertrauen in zentrale Autoritäten zu setzen, die ihre Identitäten verwalten (Voshmgir, 2020). Häufig haben die Menschen jedoch nur wenig Kontrolle darüber, wie ihre Daten verwendet und geschützt werden (Voshmgir, 2020). Diese Situation ruft nach innovativen Lösungen, um das Identitätsmanagement zu revolutionieren und die damit verbundenen Herausforderungen zu bewältigen (Voshmgir, 2020). Hier setzt das Aufkommen des Web3 und der Blockchain-Technologie an (Voshmgir, 2020).

Die Blockchain, als treibende Kraft hinter dem Web3, eröffnet neue Möglichkeiten, das Identitätsmanagement zu verbessern (Voshmgir, 2020). Statt die Daten an zentrale Behörden oder Plattformen weiterzugeben, können die Identitätsinformationen sicher und transparent auf der Blockchain gespeichert werden (Voshmgir, 2020). Dadurch kann die volle Kontrolle über die eigenen Daten behalten und selektiv entschieden werden, mit wem welche Informationen geteilt werden möchten (Voshmgir, 2020). Die dezentrale Natur der Blockchain ermöglicht es den Nutzern, die Kontrolle über ihre Identitätsdaten zu behalten und gleichzeitig das Vertrauen in die Authentizität und Integrität der Informationen zu gewährleisten (Ebeling, 2020). Darüber hinaus bietet die Blockchain eine erhöhte Widerstandsfähigkeit gegenüber Manipulationen oder Datenverlusten, da die Informationen auf mehreren Knoten im Netzwerk gespeichert werden (Ebeling, 2020). Dies stellt sicher, dass digitale Identitäten zuverlässig und sicher genutzt werden können, ohne dass ein zentraler Vermittler erforderlich ist (Ebeling, 2020). Obwohl Blockchain-Systeme viele Stärken aufweisen, gibt es einen entscheidenden Aspekt, der ihre Anfälligkeit offenbart: *ihre Offenheit* (Ebeling, 2020). Aufgrund der transparenten Natur der Blockchain müssen zusätzliche Massnahmen ergriffen werden, um sensible Informationen innerhalb des Netzwerks sicher von einem Punkt zum anderen zu übertragen (Ebeling, 2020). Während die in der Blockchain gespeicherten Daten vor Manipulation geschützt sind, können sie von allen Teilnehmern eingesehen werden (Ebeling, 2020). Besonders der Umgang mit Identitäten, insbesondere wenn sie personenbezogene Daten preisgeben, stellt eine kritische Anforderung dar (Ebeling, 2020). Darüber hinaus ist der Begriff „Identität“ auch auf Objekte anwendbar, wie im Internet der Dinge (IoT), wo jede eingebundene Einheit eindeutig identifizierbar sein muss (Ebeling, 2020). Falls Identifikationsdaten in die falschen Hände geraten, können unerwünschte Folgen wie der Verlust von Betriebsgeheimnissen auftreten (Ebeling, 2020). Die Einführung eines effektiven dezentralen Identitätsmanagements ist notwendig, um eine Grundlage für eine sichere und effizientere digitale Identitätsverwaltung zu schaffen (Urban, 2022).

1.3 Zielsetzung und Forschungsfrage

Das Ziel dieser Forschung ist das Identifizieren der Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain. Die identifizierten Anforderungen werden für die Entwicklung eines Identitätsmanagement-Modells genutzt. In dieser Forschung wird ein Identitätsmanagement-Modell entwickelt, das als Ansatz für weitere Forschungsarbeiten genutzt werden kann. Für die Entwicklung dieses Modells soll in dieser Masterarbeit die nachfolgende Forschungsfrage beantwortet werden:

Was sind die Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain?

1.4 Inhaltliche Abgrenzung

Die vorliegende Masterarbeit fokussiert sich auf die Identifizierung der Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain. Die Anforderungen werden hauptsächlich aus der Sicht des Nutzers definiert. Diese Forschung konzentriert sich nicht auf die technischen Aspekte oder die Implementierung des Modells, sondern vielmehr auf die Anforderungen an ein solches Modell und dessen Berücksichtigung beim Entwickeln eines dezentralen Identitätsmanagement-Modell. Aus diesem Grund werden technische Grundlagen und Begriffsdefinitionen möglichst verständlich erklärt. Obwohl dezentralisiertes Identitätsmanagement ein globales Thema ist, befasst sich diese Arbeit bei rechtlichen Aspekten nur mit dem Schweizer Recht.

1.5 Aufbau der Arbeit

Die vorliegende Masterarbeit ist in sieben Kapitel unterteilt. Im ersten Kapitel wird der Hintergrund und die Motivation der Arbeit dargelegt. Dabei wird auf die Relevanz des Themas und den aktuellen Stand der Forschung eingegangen. In diesem Kapitel wird auch das Forschungsziel definiert. Das zweite Kapitel befasst sich mit den Grundlagen und Begriffsdefinitionen. Hier werden die wichtigsten theoretischen Konzepte und Terminologien eingeführt und erläutert, um ein gemeinsames Verständnis der Begrifflichkeiten zu schaffen. Im dritten Kapitel wird das methodische Vorgehen beschrieben. Hier wird dargelegt, welche Forschungsmethoden angewendet werden, um die Forschungsfrage zu beantworten. Das vierte Kapitel befasst sich mit den Anforderungen und Einflussfaktoren des untersuchten Identitätsmanagement-Modells. Hier wird untersucht, welche Faktoren einen

Einfluss auf das Identitätsmanagement-Modell haben und welche Anforderungen an eine erfolgreiche Entwicklung eines Identitätsmanagement-Modell gestellt werden. Das entwickelte Modell wird im fünften Kapitel vorgestellt und erläutert. Dabei wird aufgezeigt, wie das Konzept auf die Anforderungen und Einflussfaktoren abgestimmt wurde und welche Erfolgsfaktoren berücksichtigt wurden. Im sechsten Kapitel, der Evaluation, wird das entwickelte Konzept auf seine Wirksamkeit überprüft. Dabei werden die Ergebnisse der Umsetzung des Modells dargestellt und erläutert. Im letzten Kapitel wird das Fazit dieser Forschung aufgeführt.

Ein Teil der Arbeit behandelt technische Aspekte, die für den Leser ohne entsprechenden Hintergrund schwer verständlich sein können. Aus diesem Grund werden für das Verständnis komplexere Konzepte anhand von Beispielen erklärt.

2 Grundlagen und Begriffsdefinitionen

Dieses Kapitel gibt einen grundlegenden Überblick über die wichtigsten Begriffe und Konzepte im Zusammenhang mit dem Identitätsmanagement in dezentralisierten Plattformen. Die relevanten Grundlagen und Begriffsdefinitionen dienen als Vorbereitung auf die nachfolgenden Kapitel, in denen auf die konkreten Herausforderungen und Lösungsansätzen für das Identitätsmanagement in dezentralisierten Plattformen eingegangen wird.

2.1 Identitätsmanagement

In diesem Kapitel wird die digitale Identität erklärt sowie die verschiedenen Identitätsträger aufgeführt und beschrieben. Konkret wird erläutert, wie die Identitäten verwaltet und welche Modelle dazu verwendet werden.

2.1.1 Digitale Identität und Identitätsträger

Eine digitale Identität umfasst sämtliche Informationen, die online über eine Person, eine Organisation oder ein elektronisches Gerät existieren (D. L. AG, 2023). Zu den Bestandteilen einer digitalen Identität gehören unter anderem Benutzername und Passwörter, Suchverlauf oder Kaufabwicklungen (D. L. AG, 2023). Digitale Identitäten sind ein wesentliches Instrument, um Benutzer im digitalen Raum zu identifizieren und authentifizieren (Ehrlich et al., 2021). Sie ermöglichen es, Benutzern den Zugang zu digitalen Diensten zu gewähren und sicherzustellen, dass nur autorisierte Personen auf vertrauliche Informationen zugreifen können (Ehrlich et al., 2021). Eine Identität (ID) wird durch eine Menge von Attributen beschrieben und mithilfe von Identifikatoren unterschieden (Anke & Richter, 2023, S. 264). Eine Identität bezeichnet eine spezifische Kombination von Eigenschaften und Rollen, die einem Objekt zugeordnet werden und durch einen eindeutigen Bezeichner identifiziert werden können (Tsolkas & Schmidt, 2017, S.24). Rollen und Eigenschaften unterscheiden sich darin, dass Rollen aktiv ausgeführt werden, während Eigenschaften passive Merkmale beziehungsweise Attribute darstellen (Tsolkas & Schmidt,

2017, S. 24) (siehe Abbild 2.1).

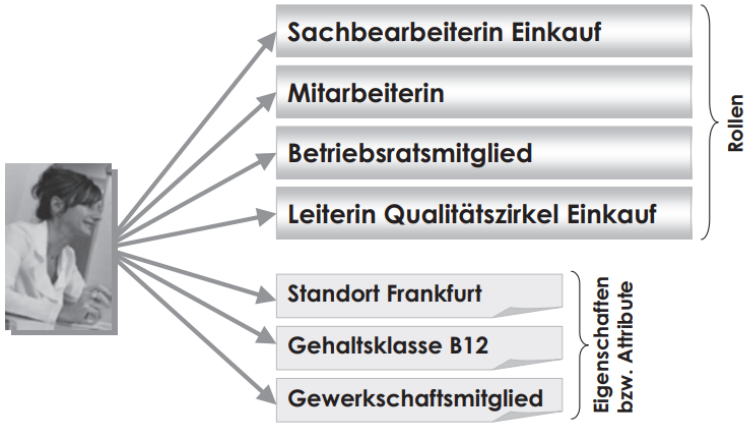

Abbildung 2.1 Identitätsbildende Rollen und Eigenschaften (Tsolkas & Schmidt, 2017, S. 25)

Die gelebte Identität eines Mitarbeiters im Unternehmen wird durch die Übernahme von Rollen und die Ausprägung von Eigenschaften gebildet (Tsolkas & Schmidt, 2017, S. 24). Die Eigenschaften und Rollen bestimmen nicht nur den Informationsaustausch zwischen den einzelnen Identitäten, sondern auch wie eine Identität handelt und mit anderen Identitäten interagiert (Tsolkas & Schmidt, 2017, S. 24). Um die Sicherheit zu gewährleisten, werden digitale Identitäten durch Credentials (dt. Berechtigungsnachweise) an die zugehörige Entität gebunden (Anke & Richter, 2023, S. 264). Credentials enthalten Informationen zur Identität, Berechtigungen und Qualifikationen sowie eigene Attribute wie das Ausgabedatum oder die Gültigkeitsdauer (Anke & Richter, 2023, S. 264). Die Anwendung von Credentials werden im Abschnitt 2.4.2 genauer erläutert. In Abbildung 2.2 ist der Aufbau einer digitalen Identität dargestellt.

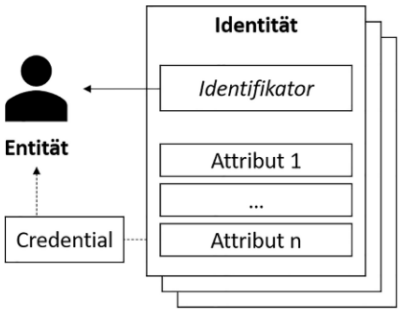

Abbildung 2.2 Der Aufbau einer digitalen Identität (Anke & Richter, 2023, S. 264)

Eine Identität kann sowohl eine einzelne Person als auch eine Gruppe bestehend aus mehreren Personen beziehungsweise Identitäten sein (Tsolkas & Schmidt, 2017, S. 24). Wenn mehrere Identitäten über die gleichen Eigenschaften verfügen, können sie zu Gruppen zusammengefasst werden (Tsolkas & Schmidt, 2017, S. 24). Eine Gruppe kann über eine eigene Identität verfügen (Tsolkas & Schmidt, 2017, S. 30). Personen können zudem mehrere kontextuelle und logische Identitäten haben, indem sie verschiedene Rollen übernehmen (Tsolkas & Schmidt, 2017, S. 24). Zum Beispiel kann ein Mitarbeiter in einem Unternehmen mehrere Identitäten haben, indem dieser unterschiedliche Rollen und Eigenschaften annimmt (Tsolkas & Schmidt, 2017, S. 24) (siehe Abbild 2.3).

Abbildung 2.3 Personelle, gelebte und kontextuelle Identität (Tsolkas & Schmidt, 2017, S. 25)

Identitätsträger (IdT) können nebst natürlichen Personen auch IT-Systeme, IT-Applikationen, Rollen und Funktionen, Gegenstände, Internet of Things (IoT)-Geräte sowie juristische Personen und Organisationseinheiten sein (Tsolkas und Schmidt, 2017, S. 27-30; Oracle, 2023). In der Tabelle 2.1 sind die einzelnen Identitätsträger mit einer kurzen Beschreibung aufgeführt.

Tabelle 2.1 Identitätsträger (Tsolkas & Schmidt, 2017, S. 27-30)

Natürliche Personen	IT-System	IT-Applikation	Rollen und Funktionen im Unternehmen
Einer Person wird eine Berechtigung bzw. eine Identität zugeordnet	Server, Client oder virtuelle Systeme, die über eigene Berechtigungen verfügen	Software-Anwendungen oder Tools Identitätsverwaltung läuft auf Systemebene oder Applikationsebene	Berechtigungen und Identitäten werden den Rollen zugeordnet Funktions-Accounts oder gemeinsame Accounts (logische Identität «Admin» mit den Berechtigungen der Rolle Administration)

Gegenstände	IoT-Geräte	Juristische Personen und Organisationseinheiten
Gegenstände agieren nicht eigenständig und sind nicht von sich aus aktiv. Fahrzeuge verfügen über verschiedene Berechtigungen. Ein PKW mit Anhänger hat nicht die gleichen Berechtigungen wie ein PWK ohne Anhänger (Tempolimit auf der Autobahnstrecke etc.)	Internetfähige Geräte, die mit Sensoren, Software und weiteren Technologien ausgestattet sind. IoT-Geräte vernetzen sich über das Internet mit anderen Geräten und Systemen, um Daten auszutauschen.	Gruppen, Abteilungen oder einzelne Bereiche eines Unternehmens können über Berechtigungen verfügen und als eine einzige Identität behandelt werden

Nebst den verschiedenen IdT, lassen sich auch die digitalen Identitäten aufgrund ihrer Eigenschaften unterschiedlich kategorisieren (Ehrlich et al., 2021, S. 252-254; Anke und Richter, 2023, S. 266-270):

- *Isolierte Identitäten* beziehen sich auf eine Identität, die von einem einzigen Dienst oder einer einzigen Organisation bereitgestellt wird und auf diese beschränkt ist. Das bedeutet, dass diese Identität nicht in der Lage ist, mit anderen Diensten oder Organisationen zu interagieren oder Informationen auszutauschen (Ehrlich et al., 2021, S. 252-254; Anke und Richter, 2023, S. 266-270).

- *Föderierte Identitäten* hingegen beziehen sich auf eine Identität, die von mehreren Diensten oder Organisationen gemeinsam genutzt wird. Dies ermöglicht es Benutzern, dieselbe Identität für verschiedene Dienste zu verwenden, ohne sich für jeden Dienst separat anmelden oder registrieren zu müssen (Ehrlich et al., 2021, S. 252-254).

- *Elektronischer Personalausweis (ePA) und andere staatliche Identitäten* sind Identitätsdokumente, die von Regierungsbehörden ausgestellt werden und die Identität einer Person verifizieren. Sie werden normalerweise für behördliche Zwecke wie zum Beispiel bei der Beantragung von Reisepässen oder bei der Durchführung von Bankgeschäften verwendet (Ehrlich et al., 2021, S. 252-254).

- *Self-Sovereign Identity (SSI)* (dt. selbstbestimmte Identität) ist ein Ansatz für digitale Identitäten, bei dem Benutzer die Kontrolle über ihre Identität haben und diese selbst verwalten können, ohne dass eine zentrale Autorität oder eine dritte Partei erforderlich ist (Anke & Richter, 2023, S. 266-270). Dabei werden Blockchain-Technologien und kryptographische Verfahren eingesetzt, um die Sicherheit und Vertraulichkeit der Identitätsdaten zu gewährleisten (Ehrlich et al., 2021, S. 253-255). SSI ermöglicht es Benutzern, ihre Identität über verschiedene Dienste und Organisationen hinweg zu nutzen und zu verwalten, ohne dass sie sich auf eine zentrale Stelle oder eine dritte Partei verlassen müssen (Ehrlich et al., 2021, S. 253-255). Der SSI-Ansatz wird im Abschnitt 2.4 genauer erläutert.

Zumal juristische oder natürliche Personen Identitätsträger von mehreren Identitäten sein können, gehört die entsprechende Verwaltung der Identitäten zu einer zentralen Aufgabe des Identitätsmanagements (Petrlic et al., 2023, S. 69-71).

2.1.2 Verwaltung der Identitäten

Das Identitätsmanagement (IdM) verwaltet die verschiedenen Identitäten von Personen oder Entitäten innerhalb eines Systems oder einer Organisation (Petrlic et al., 2023, S. 69). Im IdM werden Identitätsinformationen erstellt, überprüft, gespeichert, verwaltet und verwendet. Mit diesen Funktionen kann der Zugriff auf die Ressourcen innerhalb des Systems oder der Organisation reguliert und geschützt werden (Petrlic et al., 2023, S. 69; Kunze, 2003, S. 42-44). Es ist die Aufgabe des IdM sicherzustellen, dass ausschliesslich die im Kontext relevanten Informationen ausgetauscht werden (Tsolkas & Schmidt, 2017, S. 37). Im Mittelpunkt des IdM stehen die Benutzer und ihre Bedürfnisse. Mithilfe des Identitätsmanagements kann der Benutzer entscheiden, welche Personen in welchen Situationen auf bestimmte Daten Zugriff erhalten (Petrlic et al., 2023, S. 69; Kunze, 2003, S. 42-44). Im digitalen Raum ist das Vertrauen besonders wichtig, da die Benutzer in der Regel keinen physischen Kontakt miteinander haben und somit die üblichen Indikatoren von Vertrauen wie Mimik, Gestik und Körpersprache fehlen. Digitale Identitäten können nur dann Vertrauen schaffen, wenn die damit verbundenen Daten sicher und geschützt sind (Ehrlich et al., 2021). Die Aufgabe eines IdM besteht deshalb nicht nur aus der Identitätsverwaltung, sondern auch aus dem Identitätsschutz vor Identitätsdiebstählen oder Datenschutzverletzungen (Ehrlich et al., 2021). Eine wichtige Rolle spielt dabei die Authentifizierungsart innerhalb der ausgewählten Identitäten, wie zum Beispiel die Verwendung von Passwörtern, biometrischen Daten sowie Zwei-Faktor-Authentifizierung (Petrlic et al., 2023, S. 69; Kunze, 2003, S. 42-44; Ehrlich et al., 2021).

2.2 Identitätsmanagement-Modelle

Für das IdM können zentrale oder dezentrale Modelle verwendet werden. Die Unterschiede der Modelle beziehen sich hauptsächlich auf den Speicherort, den Schutz der Privatsphäre, den Gültigkeitsbereich, sowie die Datenkontrolle der Benutzer (Anke & Richter, 2023, S. 266-267). Für die folgend beschriebenen IdM-Modelle dienen die isolierten, föderierten und selbstbestimmten Identitäten als Basis (siehe Abbild 2.4)

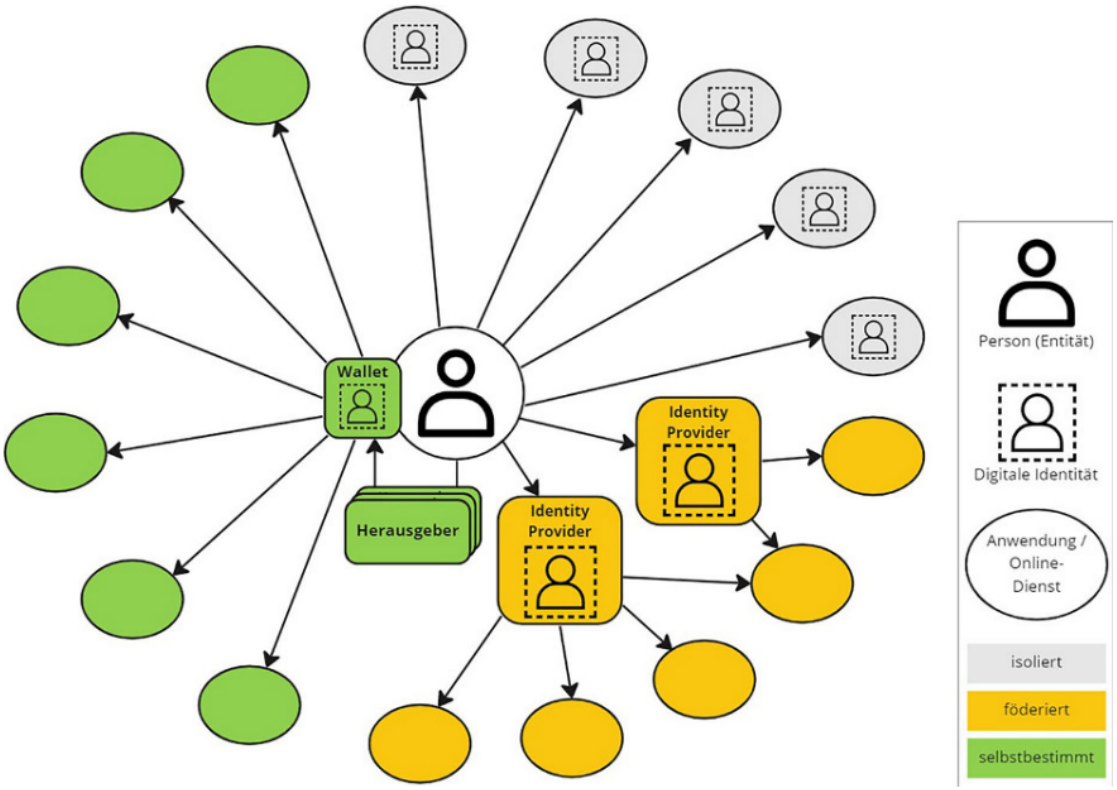

Abbildung 2.4 Identitätsmanagement-Modelle (Anke & Richter, 2023, S.267)

2.2.1 Zentrales Identitätsmanagement-Modell für isolierte Identitäten

Beim isolierten IdM registriert sich der Benutzer (User) bei einem Dienstanbieter (Service Provider) und erstellt so eine digitale Identität. Dabei wird auf dem Server des Dienstanbieters (Identity Provider) die erstellte Identität gespeichert. In der Regel wird für die Registrierung eine Emailadresse benötigt und ein Passwort definiert (Anke & Richter, 2023, S. 266-267). Die Identität kann mit weiteren Informationen wie Name, Adresse oder Telefonnummer ergänzt werden. Nach der erfolgreichen Registrierung ist es den Benutzern möglich den Dienst zu nutzen (Anke & Richter, 2023, S. 266-267). Je nach Sicherheitsrichtlinien des Dienstanbieters muss zusätzlich auf einem Authentifizierungsgerät (Smartphone, Kartenleser oder ähnliches) die Anmeldung von einem Benutzer bestätigt werden, bevor der Dienst freigeschaltet wird (Anke & Richter, 2023, S. 266-267).

Ein Nutzerkonto im isolierten IdM-Modell ist nur für den jeweiligen Dienst gültig, was dazu führt, dass Nutzer viele verschiedene digitale Identitäten verwalten müssen. Dies ist zeitaufwendig und kann problematisch sein, da die Nutzerdaten auf zahlreichen Internet-

servern gespeichert sind und es oft unbekannt ist, wie gut die Daten vom Dienstanbieter geschützt werden (Anke & Richter, 2023, S. 266-267). Die folgende Abbildung 2.5 zeigt den Ablauf eines IdM-Modells für isolierte Identitäten, welches nachfolgend anhand eines Beispieles erläutert wird.

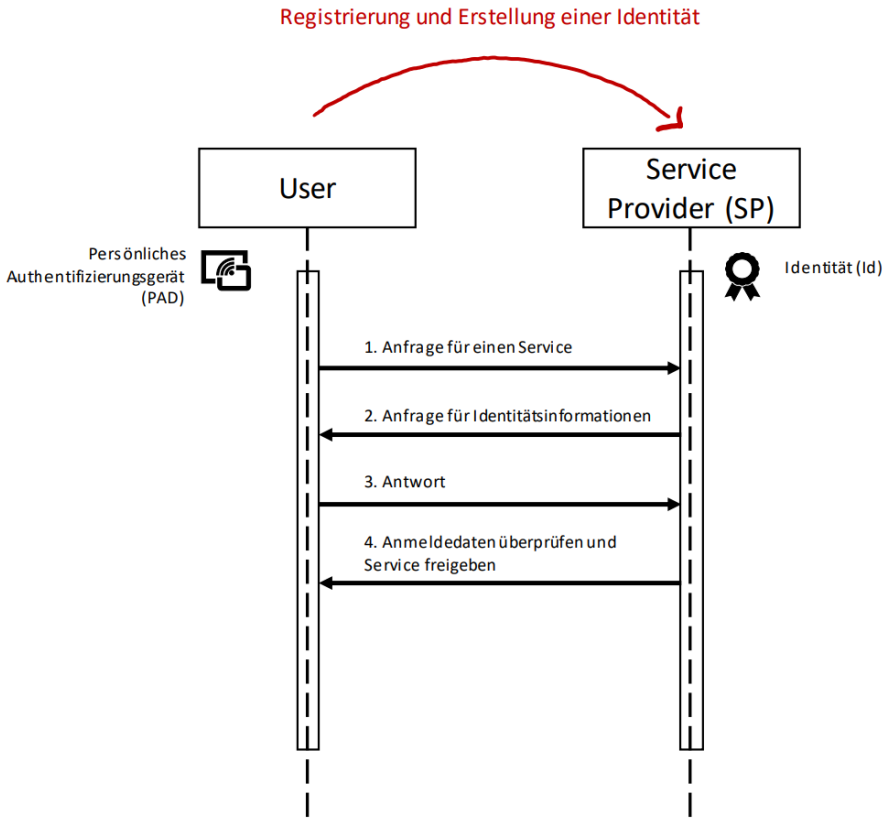

Abbildung 2.5 Prozess eines IdM-Modell für isolierte Identitäten

Alice registriert sich für die Nutzung des E-Bankings bei ihrer Bank (SP) und erstellt somit eine Identität (ID).

1. Alice möchte sich mit ihrem E-Bankingkonto anmelden und besucht die entsprechende Webseite ihrer Bank.
2. Der SP verlangt über die Webseite die Identitätsinformationen (Login-Daten) von Alice.
3. Alice gibt ihre Login-Daten ein.
4. Die Login-Daten werden vom SP überprüft und aus Sicherheitsgründen generiert der SP für die Authentifizierung eine Bestätigungsanfrage auf Alice's Smartphone. Diese Authentifizierungsanfrage muss von Alice auf ihrem Smartphone bestätigt werden, damit der Login-Prozess erfolgreich abgeschlossen wird.

Je mehr Dienste eine natürliche oder juristische Person nutzt, umso mehr isolierte Identitäten müssen sicher verwaltet werden. Um die Verwaltung benutzerfreundlicher zu gestalten setzen viele Benutzer auf ein zentrales Identitätsmanagement.

2.2.2 Zentrales Identitätsmanagement Modell für föderierte Identitäten

Eine bedienungsfreundlichere Lösung bietet das föderierte Identitätsmanagement, bei dem ein dedizierter Identity Provider (IdP) die Registrierung, Identifikation und Authentifizierung der Nutzer übernimmt. Dienste, die diesen IdP verwenden, werden als Relying Party bezeichnet. Wenn mehrere Dienste denselben IdP nutzen, bilden sie eine sogenannte Föderation (Anke & Richter, 2023, S. 267-268). Unternehmen nutzen diesen Ansatz beispielsweise als Single-Sign-On (SSO), um den Mitarbeitern nach einer einmaligen Authentifizierung den Zugang zu unterschiedlichen internen Anwendungen zu ermöglichen. Grosse Technologiekonzerne wie Google, Microsoft oder Apple, unterstützen den sogenannten Social-Login-Mechanismus (Anke & Richter, 2023, S. 267-268). Dieser Mechanismus ermöglich es Internetnutzern mit demselben Login auf mehrere Internetdienste zugreifen zu können (Anke & Richter, 2023, S. 267-268). Konkret bedeutet dies, dass unabhängige Internetdienste den Social-Login-Mechanismus und somit vorhandene Identitäten nutzen können, um ihren Nutzern den Anmeldeprozess zu vereinfachen (Anke & Richter, 2023, S. 267-268). Dadurch werden Einstiegshürden reduziert und es wird Nutzern ermöglicht, sich schnell und einfach bei verschiedenen Diensten anzumelden (Anke & Richter, 2023, S. 267-268).

Authentifizieren sich Nutzer mittels einer föderierten Identität, werden sie zum Identity Provider (IdP) weitergeleitet. Dadurch sammelt sich beim IdP ein umfangreiches digitales Profil des Nutzerverhaltens, was beispielsweise für Werbezwecke genutzt werden kann (Anke & Richter, 2023, S. 267-268). Ausserdem hängen Nutzer und Online-Anbieter stark vom IdP ab, der die Nutzungsbedingungen vorgibt und im schlimmsten Fall Teilnehmer ausschließen kann. Diese Abhängigkeit kann dazu führen, dass Nutzerdaten in die Hände von Dritten geraten, wenn der IdP beispielsweise kompromittiert wird. Daher sollten Nutzer bei der Entscheidung, ob sie eine föderierte Identität verwenden möchten, sorgfältig abwägen und sich über die Sicherheitsmassnahmen des jeweiligen IdPs informieren (Anke & Richter, 2023, S. 267-268).

Folgende Abbildung 2.6 zeigt den Prozess eines zentralen IdM-Modells für föderierte Identitäten. In der Praxis könnte so ein Prozess wie folgt ablaufen:

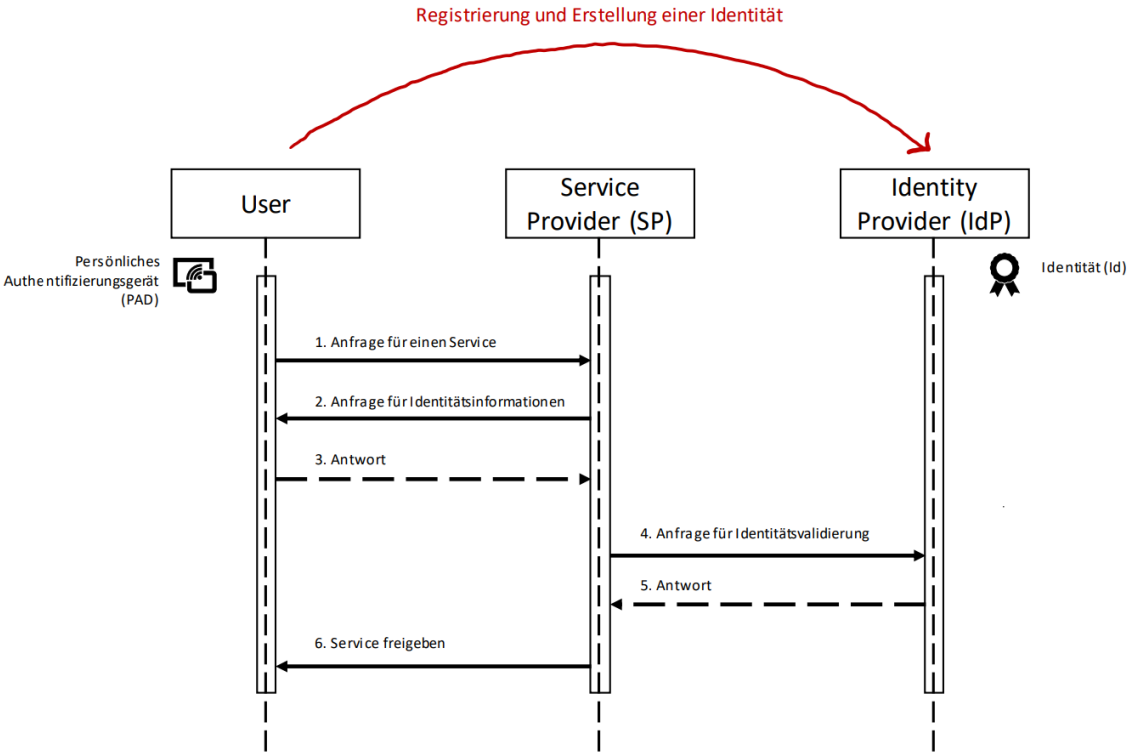

Abbildung 2.6 Prozess eines IdM-Modell für föderierte Identitäten

Alice hat sich vor langer Zeit auf Facebook (IdP) registriert, damit sie den Kontakt zu ihren alten Schulfreunden nicht verliert. Nebst Facebook nutzt Alice weitere Dienste, wie z.B. ein App eines öffentliches Nachrichtendienst.

1. Alice möchte sich beim Nachrichtendienst registrieren, um die vollen Funktionen wie z.B. die Suchfunktion weiterhin verwenden zu können. Sie klickt daher beim SP auf «Registrieren und Suche starten».

2. Der SP sendet eine Anfrage für die Identitätsinformationen

3. Auf der Seite des Nachrichtendiensts erscheint die Meldung nach der E-Mailadresse oder die Möglichkeit sich mit einem Login eines anderen Diensts, wie z.B. Facebook, anzumelden.

4. Alice möchte nicht noch mehr Logins verwalten und entscheidet sich mit ihrem Facebook-Account anzumelden. Sie gibt ihre Facebook-Login-Daten ein.

5. Die eingegeben Login-Daten werden vom SP an Facebook weitergeleitet und überprüft.

6. Der IdP Facebook bestätigt die Login-Daten und sendet die Bestätigung an den SP Nachrichtendienst.

7. Der SP Nachrichtendienst akzeptiert das Login. Die Suchfunktion und weitere Funktionen werden freigeschaltet. Alice findet es praktisch, dass das so schnell und unkompliziert funktioniert. Gleichzeitig hat sie bedenken zum Thema Datenschutz. Sie fragt sich, welche weiteren Daten sonst noch von ihr geteilt werden und ob sie über ihre Datenteilung nicht selbst bestimmen kann.

2.2.3 Einführung in dezentrales Identitätsmanagement-Modell für selbstbestimmte Identitäten

Das Konzept der selbstbestimmte Identität arbeitet anders als die zentralen IdM-Modelle. Es baut auf direkte Verbindungen zwischen Interaktionspartnern auf, die mittels asymmetrischer Kryptografie (siehe Abschnitt 2.3.3) und der Nutzung von privaten und öffentlichen Schlüsseln ermöglicht werden (Anke & Richter, 2023, S. 267-270). Die Kommunikation zwischen den Partnern erfolgt über direkte Peer-to-Peer-Verbindungen. Es wird kein zentraler Identitätsprovider (IdP) benötigt, dafür eine verteilte Systemarchitektur (Anke & Richter, 2023, S. 267-270).

Der Aufbau und die Funktion eines dezentralen IdM-Modells wird aufgrund der Komplexität erst nach den Begriffsdefinitionen und Grundlagen im Abschnitt 2.4 genauer erläutert.

2.3 Verteilte Systemarchitektur

Verteilte Systemarchitektur, besser bekannt unter der Bezeichnung „Distributed Ledger Technologie“ (DLT) ist ein Konzept, das auf einer dezentralen Systemarchitektur basiert (Urban & Urban, 2020, S. 15-17) und es ermöglicht Datentransaktionen sicher und transparent in einem Netzwerk zu verwalten (Egloff & Turnes, 2019, S. 23-24). Im Gegensatz zu zentralen Systemen, die alle Kommunikationswege zentralisiert, oder dezentralen Systemen, die Teilbereiche des Netzwerks bündelt, gibt es bei DLT keine zentrale Instanz, welche die Kontrolle über die Daten hat (Urban und Urban, 2020, S. 15-17; Egloff und Turnes, 2019, S. 21-29). Stattdessen wird die Kontrolle durch das Teilnehmernetzwerk ausgeübt (Egloff & Turnes, 2019, S. 21-29). DLT basiert auf einem verteilten Datenbankmodell, das dem Teilnehmernetzwerk ermöglicht, gemeinsam auf die Daten zuzugreifen und diese zu aktualisieren (Egloff & Turnes, 2019, S. 21-29). Dabei ist jeder Node (Netzwerkknoten) direkt in das Netzwerk integriert und kann direkt mit allen anderen Nodes interagieren (Urban und Urban, 2020, S. 15-17; Urban und Urban, 2020, S. 16). Ein DLT-Netzwerk besteht also aus mehreren Nodes, die als Servernetzwerk betrachtet werden können (Urban & Urban, 2020, S. 15-17). Diese Architektur bietet Schutz vor Ausfällen und Cyberangriffen, da der Ausfall einzelner Nodes das Netzwerk nicht beeinträchtigt (Urban & Urban, 2020, S. 15-17). Zudem müsste ein Angreifer, um eine erfolgreiche Datenmanipulation durchzuführen, mehr als 50 Prozent der Nodes zur gleichen Zeit in gleicher Weise kontrollieren (Urban & Urban, 2020, S. 15-17). Die Nodes haben die Aufgabe, die im Netzwerk durchgeführten Transaktionen zu validieren und zu speichern (Urban & Urban, 2020, S. 15-17). Jeder teilnehmende Node besitzt eine eigene lokale Kopie des gesamten Ledgers, auch als Shared Ledger bezeichnet (Urban & Urban, 2020, S. 15-17). Somit wird eine umfassende Aufzeichnung aller jemals im Netzwerk durchgeführten Transaktionen gewährleistet (Urban & Urban, 2020, S. 15-17). DLT hat zahlreiche Anwendungsmöglichkeiten, wie zum Beispiel die Verwaltung von Kryptowährungen, die Umsetzung von Smart Contracts oder die Verwaltung von digitalen Identitäten. Dabei bietet DLT viele Vorteile wie Transparenz, Sicherheit und Dezentralisierung, die in verschiedenen Anwendungsbereichen genutzt werden können (Egloff & Turnes, 2019, S. 21-29).

Im Abbild 2.7 sind die verschiedenen Systemarchitekturen aufgeführt. Wichtig zu beachten ist, dass ein verteiltes System immer dezentral organisiert ist, wobei ein dezentrales System nicht zwingend verteilt ist (Egloff & Turnes, 2019, S. 29). Zu den am weitesten verbreiteten DLT-Systemarchitekturen gehört die Blockchain-Technologie (Egloff & Turnes, 2019, S. 31).

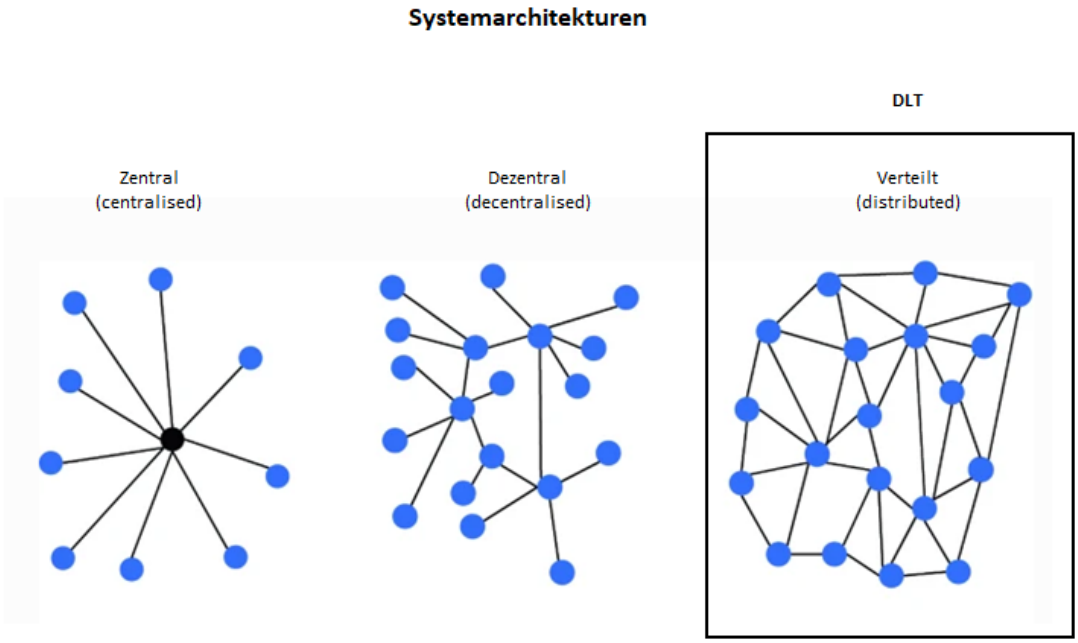

Abbildung 2.7 Systemarchitekturen (Egloff & Turnes, 2019, S. 29)

2.3.1 Blockchain

Die Blockchain ist eine verteilte Datenbank, die Datenblöcke miteinander verkettet. Jeder Block enthält eine Liste von Transaktionen, die von verschiedenen Benutzern oder Geräten im Netzwerk ausgeführt wurden. In einer neuen Transaktion wird die vorherige Transaktionshistorie im neuen Block integriert. So entsteht eine Kette von Datenblöcken, also eine Blockchain (Reinwald, 2022, S. 15-16). Die Abbildung 2.8 zeigt eine vereinfachte Form einer Blockchain.

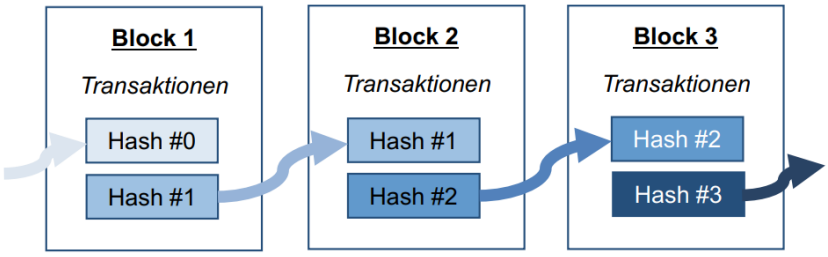

Abbildung 2.8 Veranschaulichung einer Blockchain (Reinwald, 2022, S. 16)

Ein Block in einer Blockchain besteht aus mehreren wichtigen Bestandteilen, die alle eine spezifische Funktion erfüllen (Egloff & Turnes, 2019, S. 46-47). Der erste Bestandteil ist der *Header* des Blocks, der grundlegende Informationen über den Block enthält (Egloff

& Turnes, 2019, S. 46). Dazu gehören die Blocknummer, der Zeitstempel der Erstellung (Datum und Uhrzeit mit Zeitzone), die automatisch vom System generiert wird, eine Referenz des vorherigen Blocks (dessen Hashwert) und ein Nonce-Wert (Number Used Once) für den Proof-of-Work-Algorithmus (Egloff & Turnes, 2019, S. 46).

Ein weiterer wichtiger Bestandteil ist der Transaktionsdatensatz, der alle Transaktionen enthält, die in diesem Block verarbeitet werden (Egloff & Turnes, 2019, S. 46-47). Jede Transaktion besteht aus einer Absenderadresse, einer Empfängeradresse, einem Betrag und weiteren relevanten Informationen (Egloff & Turnes, 2019, S. 46-47). Diese Transaktionsdaten werden in der Regel in Form eines Merkle Trees organisiert, um die Integrität und Effizienz der Datenverarbeitung zu gewährleisten. Damit der Header mit der Transaktion verbunden wird, wird durch die Verwendung eines weiteren Hash-Werts ein Verweis oder eine Referenz zur Transaktion hergestellt (Egloff & Turnes, 2019, S. 46-47). Die beiden Blöcke werden mit dieser Referenz untrennbar miteinander verknüpft (Egloff & Turnes, 2019, S. 47) (siehe Abbild 2.9). Die Anzahl der maximal möglichen Transaktionen innerhalb eines Blocks, variiert je nach Blockchain-Protokoll und der festgelegten Blockgrösse (Egloff & Turnes, 2019, S. 46-47). So ist beispielsweise das Bitcoin-Protokoll auf einen Speicherplatz von maximal 1 Megabyte (MB) pro Block beschränkt. Diese Einschränkung entspricht ca. 2000 Transaktionen (Egloff & Turnes, 2019, S. 46).

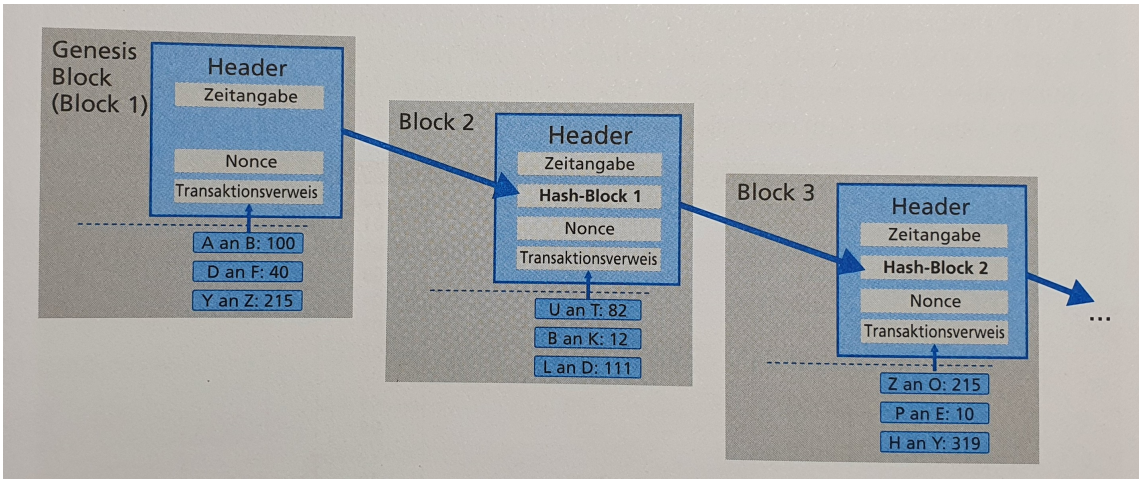

Abbildung 2.9 Verkettung von Blöcken (Egloff & Turnes, 2019, S. 47)

Für die Verschlüsselung und Sicherung der Daten, wird in der Blockchain die sogenannte kryptografische Hash-Funktion verwendet (Lewrick & Giorgio, 2018, S. 55-58). Bei der Hash-Funktion handelt es sich um eine mathematische Funktion, die die Fähigkeit besitzt, aus einem beliebigen Eingabewert einen Ausgabewert zu definieren (Bogensperger, 2021). Dabei wird eine beliebig lange Eingabe (Input) in eine feste Länge von Ziffern (Output) umgewandelt (Lewrick & Giorgio, 2018, S. 55-58). Der Output wird als Hash

bezeichnet (Lewrick & Giorgio, 2018, S. 55-58). Der Hash-Algorithmus besteht aus einer One Way (Einweg-)Funktion und funktioniert nur in eine Richtung (Lewrick & Giorgio, 2018, S. 55-58). Das bedeutet, dass der Algorithmus aus einem Input immer ein Output erzeugt (Lewrick & Giorgio, 2018, S. 55-58). Es ist fast unmöglich, aufgrund vom Output auf den ursprüngliche Input zurückzuschliessen (Lewrick & Giorgio, 2018, S. 55-58). Mit dem Hash-Verfahren wird in der Blockchain die Datenintegrität überprüft (Lewrick & Giorgio, 2018, S. 55-58). Dabei wird der Hash-Wert einer Datei berechnet und aufbewahrt (Lewrick & Giorgio, 2018, S. 55-58). Bei einer Veränderung der Daten wäre der Hash-Wert nicht mehr identisch, was darauf hindeutet, dass die Datei manipuliert wurde (Lewrick & Giorgio, 2018, S. 55-58). Mit dem Hash-Wert kann die Unverfälschtheit einer Datentransaktion garantiert werden, denn sobald ein Buchstabe oder Zeichen in der Transaktion verändert wird, verändert sich auch deren Hash-Wert (Reinwald, 2022, S. 15; Adam et al., 2020, S. 30). Abbild 2.10 zeigt Sätze, die in einem Hash-Wert umgewandelt werden. Der zweite Satz veranschaulicht, dass lediglich die Auswechslung eines Satzzeiches genügt, um den Hash-Wert zu verändern.

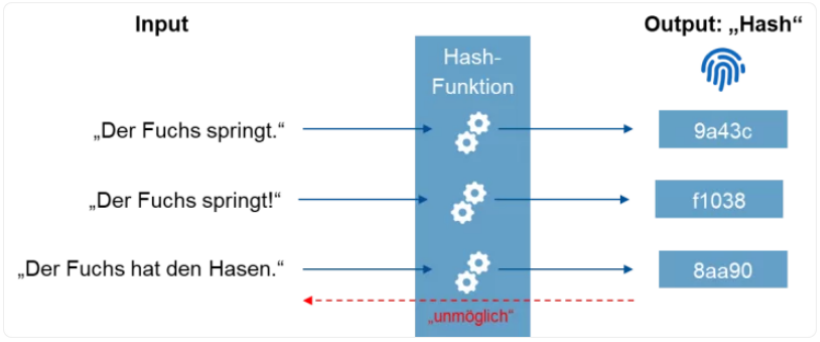

Abbildung 2.10 Anwendung einer kryptographischen Hashfunktion auf unterschiedlichen Eingabetexten (Bogensperger, 2021)

Die Überprüfbarkeit von Transaktionen beruht auf dem Prinzip der dezentralen Konsensbildung (Egloff & Turnes, 2019, S. 51-52). In einem dezentralen System wird beispielsweise beim Bargeldbezug vom Bancomaten die Transaktion direkt auf dem Bankkonto abgebucht (Egloff & Turnes, 2019, S. 51-52). Die Transaktion ist meist innert kürzester Zeit ersichtlich (Egloff & Turnes, 2019, S. 51-52). Die beiden beteiligten Parteien (Kunde und Bank) können die Transaktion überprüfen und haben somit einen Konsens über den aktuellen Kontostand (Egloff & Turnes, 2019, S. 51). Bei einem dezentralen System müssen bei einer Transaktion alle Teilnehmende des Netzwerks, alle Nodes, informiert werden (Egloff & Turnes, 2019, S. 51-52). Hier besteht die Gefahr, dass bei einer Verzögerung doppelte Ausgaben (Double Spending) entstehen (Egloff & Turnes, 2019, S. 51-

52). Beispielsweise könnte ein Kunde bei einem Kontostand von CHF 200.- den gesamten Betrag beziehen (Egloff & Turnes, 2019, S. 51-52). Wenn die Synchronisierung bei einem dezentralen Netzwerk nicht funktioniert, könnte es vorkommen, dass der Bancomat nebenan von der Transaktion nicht Bescheid weiss und es dem Kunden ermöglicht, weitere CHF 200.- zu beziehen, obwohl sein Kontostand bereits CHF 0.- beträgt (Egloff & Turnes, 2019, S. 51-52). Aus diesem Grund werden in einem dezentralen Netzwerk die Transaktionen durch einen Konsensmechanismus synchronisiert (Egloff & Turnes, 2019, S. 51-52). In diesem Mechanismus werden alle zu verarbeitenden Transaktionen überprüft, bevor sie alle Nodes im System über die neuen Transaktionen informiert (Egloff & Turnes, 2019, S. 51-52). So wird sichergestellt, dass nur gültige Blöcke zur Blockchain hinzugefügt werden und die Mehrheit der Netzwerkteilnehmer den Konsens über die Reihenfolge der Blöcke und die enthaltenen Transaktionen erreicht (Egloff & Turnes, 2019, S. 51-52). Die Grundidee der Blockchain kann durch fünf wesentliche Eigenschaften charakterisiert werden (Urban & Urban, 2020, S. 20):

- *Unveränderbarkeit:* Die Transaktion bleibt dauerhaft unveränderlich gespeichert, nach dem sie in die Blockchain hinzugefügt wurde (Urban & Urban, 2020, S. 20).
- *Nicht-Abstreitbarkeit:* Aufgrund der kryptografischen Signatur und Nachverfolgbarkeit aller vergangenen Transaktionen ist eine rechtsverbindliche Überprüfung der gespeicherten Daten möglich (Urban & Urban, 2020, S. 20).
- *Integrität:* Aufgrund der kryptografischen Signatur und Nachverfolgbarkeit aller vergangenen Transaktionen ist eine rechtsverbindliche Überprüfung der gespeicherten Daten möglich (Urban & Urban, 2020, S. 20).
- *Transparenz:* Alle Teilnehmer des Netzwerks haben öffentlichen Zugriff auf die Blockchain und die darin enthaltenen Daten, wodurch vollständige Transparenz gewährleistet wird (Urban & Urban, 2020, S. 20).
- *Gleichberechtigung:* Es bestehen dieselben Zugriffs- und Schreibrechte innerhalb der Blockchain für alle Nodes (Teilnehmer) im Netzwerk (Urban & Urban, 2020, S. 20).

Nachfolgend wird die Funktionsweise der Blockchain-Technologie in einem vereinfachten Prozess gemäss Abbild 2.11 erläutert.

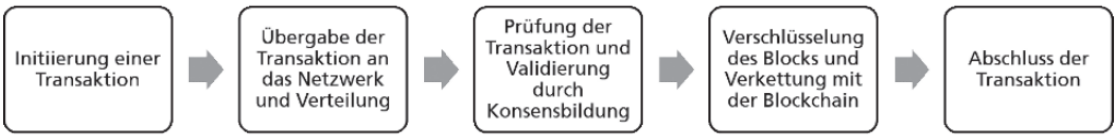

Abbildung 2.11 Funktionsweise einer Blockchain (Neugebauer, 2018, S. 313)

1. Der Sender erstellt eine Transaktion, die digital signiert wird (Neugebauer, 2018, S. 313). Eine Transaktion kann beispielsweise die Registrierung eines Dokuments, das Überbringen einer Nachricht oder die Überweisung einer Kryptowährung sein (Neugebauer, 2018, S. 313). Für die Codierung der Transaktion wird das Hash-Verfahren angewendet (Neugebauer, 2018, S. 313). Durch das Hash-Verfahren wird jede Transaktion mit einem digitalen Fingerabdruck zur späteren Validierung und Manipulationssicherheit der Transaktion versehen (Reinwald, 2022, S. 15). Bei einer Veränderung der Daten im Block gilt der Hash-Wert als ungültig (Reinwald, 2022, S. 15). Dadurch kann die Unverfälschtheit des Blockes garantiert werden (Reinwald, 2022, S. 15).

2. Die erstellte Transaktion wird an das zugrundeliegende Blockchain-Netzwerk gesendet und an die beteiligten Validierungs-Knoten verteilt.

3. Die Transaktion wird durch die Nodes des Netzwerkes auf ihre Gültigkeit überprüft (Neugebauer, 2018, S. 313). Die Validierung erfolgt durch den Konsensmechanismus, der über verschiedene Verfahren gebildet werden kann (Neugebauer, 2018, S. 313). Nicht jedes Blockchain-System nutzt denselben Konsensmechanismus. Die verbreitesten Konsensmechanismen sind „Proof of Work“ und „Proof of Stake“ Verfahren (Reinwald, 2022, S. 17). Nach der Konsensfindung wird die Transaktion validiert (Neugebauer, 2018, S. 313).

4. Die validierte Transaktion wird in einem Block gespeichert. Der verschlüsselte Block wird mit den bereits bestehenden Blöcken durch eine Verkettung miteinander verbunden. Es entsteht eine Kette aus Blöcken (die Blockchain) (Neugebauer, 2018, S. 313; Reinwald, 2022, S. 15).

5. Die Transaktion ist abgeschlossen (Neugebauer, 2018, S. 313).

Bei neuen Transaktionen beginnt der Prozess von vorne und die neu erstellten Blöcke werden in der bestehenden Verkettung aufgenommen. Damit die Datensätze beziehungsweise die Datenblöcke jeder Zeit verfügbar sind, werden sie in allen Nodes des DLT-Netzwerkes kopiert (Neugebauer, 2018, S. 313).

2.3.2 Kategorien der Blockchain-Netzwerke

Eine Blockchain kann zwischen öffentlich und privat unterschieden werden (Egloff & Turnes, 2019, S. 38-39). Diese Unterscheidung bezieht sich auf die Nutzerauthentifizierung («wer hat Zugriff») (Egloff & Turnes, 2019, S. 38-39).

In einer public (dt. öffentlich) Blockchain sind alle Transaktionen transparent und für alle ersichtlich (Egloff & Turnes, 2019, S. 38-39). Für die Teilnahme an der Public Blockchain wird keine Erlaubnis benötigt, lediglich ein Computer und eine Internetverbindung (Egloff & Turnes, 2019, S. 38-39). Der uneingeschränkte Zugriff erschwert die Überwachung und Identifizierung der Identität der Teilnehmenden (Egloff & Turnes, 2019, S. 38-39). Das Bitcoin und Ethereum Protokoll stellen eines der bekanntesten Beispiele einer Public Blockchain dar (Egloff & Turnes, 2019, S. 38-39).

In einer private (dt. privat) Blockchain hingegen ist der Zutritt im Netzwerk eingeschränkt (Egloff & Turnes, 2019, S. 38-39). Nur Teilnehmende mit entsprechenden Zugriffsrechten können sich an einer Private Blockchain beteiligen und sind somit dem Netzwerk bekannt (Egloff & Turnes, 2019, S. 38-39). Die Transaktionen einer Private Blockchain sind in der Regel vertraulich und nur für die beteiligen Parteien der jeweiligen Transaktion einsehbar (Egloff & Turnes, 2019, S. 38-39). Hyperledger Fabric stellt eines der bekanntesten Beispiele einer Private Blockchain dar (Egloff & Turnes, 2019, S. 38-39).

Nebst der Unterscheidung zwischen öffentlich und privat, kann zwischen permissionless (dt. erlaubnislos) und permissioned (dt. erlaubt) differenziert werden (Egloff & Turnes, 2019, S. 38-39). Diese Differenzierung bezieht sich auf die Nutzerautorisierung («Wer darf was tun?») (Egloff & Turnes, 2019, S. 38-39). In der Regel handelt es sich bei einer Public Blockchain, um eine permissionless Blockchain (keine Teilnahme-Erlaubnis notwendig) und bei der privaten Blockchain, um eine permissioned Blockchain (Teilnahme nur mit Erlaubnis) (Egloff & Turnes, 2019, S. 38-39). Die Blockchains können in unterschiedlichen Varianten auftreten (Egloff & Turnes, 2019, S. 38-39). Zum Beispiel kann eine Blockchain auch public und permissioned sein (Egloff & Turnes, 2019, S. 38-39). Alle könnten teilnehmen (public), jedoch mit unterschiedlicher Rechten (permissioned) (Egloff & Turnes, 2019, S. 38-39).

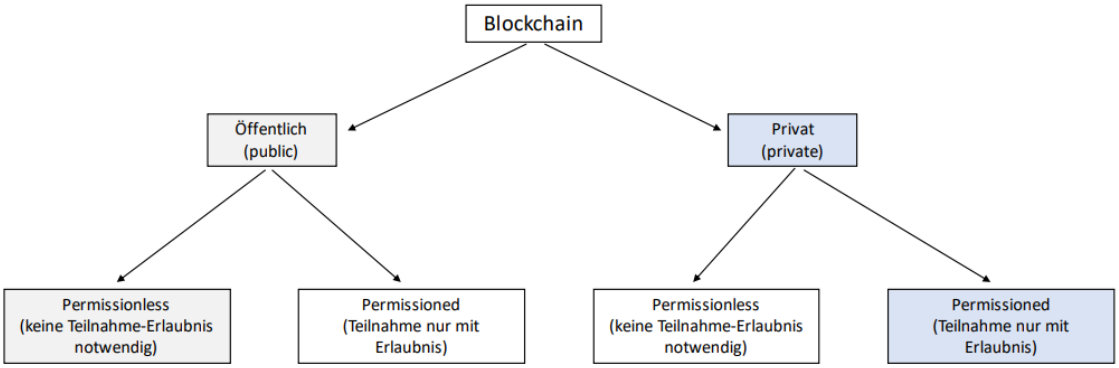

Abbildung 2.12 Kategorien der Blockchain-Netzwerke (Egloff & Turnes, 2019, S. 38-39)

2.3.3 Kryptografie

Bei der Kryptografie handelt sich um ein Wort aus dem Griechischen mit der Bedeutung «geheimes Schreiben» (Egloff & Turnes, 2019, S. 40). Die Kryptografie wird zur Verschlüsselung von Texten, Daten oder Informationen verwendet und spielt eine zentrale Rolle bei der Absicherung von Daten in der Blockchain (Egloff & Turnes, 2019, S. 40-44). Die Anwendung von Kryptografie ermöglicht es, Transaktionen sicher und vertraulich durchzuführen (Egloff & Turnes, 2019, S. 40-44). Die verschlüsselten Nachrichten können nur durch die berechtigten Personen mit dem korrekten Schlüssel wieder entschlüsselt und gelesen werden (Egloff & Turnes, 2019, S. 40-44). Es gibt zwei verschiedene Verschlüsselungsverfahren, die symmetrische und asymmetrische Verschlüsselung (Egloff & Turnes, 2019, S. 40-44).

Bei der symmetrischen Verschlüsselung wird derselbe Schlüssel (engl. key) für die Verschlüsselung und Entschlüsselung von Daten verwendet (Egloff & Turnes, 2019, S. 40-42). Das bedeutet, dass der Sender und der Empfänger gleichen geheimen Schlüssel kennen müssen, um die Nachricht zu lesen (Egloff & Turnes, 2019, S. 40-42). Die Verwendung dieser Methode könnte riskant sein, wenn die Informationen über unsichere Netzwerke übertragen werden, da der Schlüssel gestohlen oder abgefangen werden kann (Egloff & Turnes, 2019, S. 40-44). Abbild 2.13 stellt eine symmetrische Verschlüsselung dar.

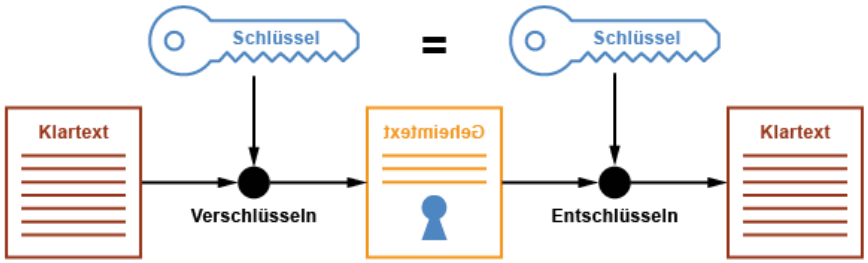

Abbildung 2.13 Symmetrische Verschlüsselung (Schnabel, 2022)

Die asymmetrische Verschlüsselung hingegen verwendet zwei verschiedene Schlüssel für die Verschlüsselung und Entschlüsselung von Daten: einen öffentlichen Schlüssel (engl. pubilc key) und einen privaten Schlüssel (engl. private key) (Egloff & Turnes, 2019, S. 42-44). Beide Schlüssel bilden zusammen ein Schlüsselpaar. Der public key wird vom private key mithilfe eines Algorithmus erstellt (Egloff & Turnes, 2019, S. 42-44). Der Algorithmus besteht aus einer Einbahnfunktion (One Way), weshalb es nicht möglich ist den private key anhand des public keys zu identifizieren. (Egloff & Turnes, 2019, S. 42-44) Die einzige Möglichkeit wäre es, jegliche mögliche Zahlenkombinationen mit dem Algorithmus zu testen, bis zufallsmässig die korrekte Zufallszahl herausgefunden würde (Egloff & Turnes, 2019, S. 42-44). Aufgrund der grossen Anzahl Zeichen oder Zahlen eines private keys ist es mit dem heutigen Stand der Technik fast unmöglich, den private key zu identifizieren (Egloff & Turnes, 2019, S. 42-44).

Der public key wird für die Verschlüsselung der Nachricht verwendet und kann von jedem empfangen werden. Der private key wird für die Entschlüsselung der Nachricht benötigt und wird nur dem Empfänger bekannt gegeben (Egloff & Turnes, 2019, S. 40-44). Durch diese Eigenschaft wird die asymmetrische Verschlüsselung als eine sichere Methode der Datenübertragung definiert, da der private key nur vom Empfänger verwendet werden kann und somit schwerer zu entwenden oder abzufangen ist (Egloff & Turnes, 2019, S. 40-44). Aus diesem Grund wird die asymmetrische Kryptografie bei Transaktionen auf der Blockchain angewendet (Egloff & Turnes, 2019, S. 40-44). Im nachfolgendem Abbild 2.14 ist die asymmetrische Verschlüsselung dargestellt.

Abbildung 2.14 Asymmetrische Verschlüsselung (Schnabel, 2022)

Beim Verschlüsseln und Entschlüsseln der Nachricht, wird die Nachricht zusätzlich signiert (Egloff & Turnes, 2019, S. 40-44). Bei einem Verlust des private keys verliert der Eigentümer die Kontrolle der verbundenen Daten, Vermögenswerte oder Informationen, die beispielsweise in einem digitalen Wallet gespeichert sind (Egloff & Turnes, 2019, S. 40-44).

2.3.4 Digitale Wallets

Ein Wallet ist eine Software, die als Schnittstelle zwischen dem Benutzer und der Blockchain fungiert und es Benutzern ermöglicht, ihre digitalen Vermögenswerte wie Kryptowährungen, Non-Fungible-Token oder andere elektronische Dateien sicher zu verwalten und Transaktionen durchzuführen (Egloff und Turnes, 2019, S. 44; Bitpanda, 2023). Ein Wallet speichert die Währungen nicht direkt, sondern die dazugehörigen private und public keys. Diese gestatten den Nutzern den Zugriff auf ihre Wallet-Adressen, mit und dementsprechend auf ihre Vermögenswerte (Bitpanda, 2023). Ein Wallet stellt keine physische Geldbörse dar. Sie bietet unterschiedliche Sicherheitsstufen, je nach den Anforderungen des Benutzers (Bitpanda, 2023). Die Wallets können mehrere private keys enthalten und es können mehrere Wallets erstellt werden, um eine maximale Sicherheit bei der Aufbewahrung von digitalen Vermögenswerten zu gewährleisten (Bitpanda, 2023).

Auf das Wallet kann nur mit dem private key zugegriffen werden. Wenn der Speicherort (public address) und der dazugehörige Schlüssel (private key) jemandem bekannt ist, kann diese Person auf das Wallet zugreifen (Bitpanda, 2023). Es ist deshalb wichtig, dass der private key an einem sicheren Ort aufbewahrt wird und vor unbefugtem Zugriff geschützt wird (Egloff & Turnes, 2019, S. 87-89). Medienberichten zu folge gab es viele Fälle von Hacker-Angriffen auf Blockchain-Netzwerke, wobei digitale Vermögenswerte entwendet werden konnten (Egloff & Turnes, 2019, S. 89). Dies ist jedoch irreführend, da Angriffe in der Regel nicht auf die Blockchain, sondern auf die Wallets durchgeführt werden. (Egloff & Turnes, 2019, S. 89) Der Angreifer (Hacker) konnte mit dem Besitz des private key alle

damit verbundenen digitalen Vermögenswerte entwenden, indem er diese an seine eigene Adresse sendete (Egloff & Turnes, 2019, S. 89).

Aufgrund der spezifischen technischen Architektur einer Wallet werden viele Gestaltungsmöglichkeiten geboten (Bastian et al., 2023, S. 387). Die verschiedenen Lösungen unterscheiden sich hauptsächlich durch den Ort an dem die Credentials gespeichert werden, den sicheren Mechanismus zur Schlüsselverwaltung und die Nutzerauthentifizierung (Bastian et al., 2023, S. 387). Einige Beispiele für die verschiedenen Wallet-Arten sind: das Software Wallet, das Hardware Wallet und das Paper Wallet beziehungsweise das physische Wallet (Bitpanda, 2023). Des Weiteren gibt es eine Auswahl von native, mobile Wallet-App-Lösungen (auch Edge- oder Non-Custodial Wallets genannt), die keine zusätzlichen Backend-Dienste benötigen, bis hin zu vollständig cloudbasierten Wallet-Diensten (auch Managed oder Custodial Wallets genannt), die nicht an ein Nutzergerät gebunden sind (Bastian et al., 2023, S. 387). Zusätzlich existieren hybride Architekturen in denen Nutzergeräte als auch Backend-Dienste genutzt werden. Die technische Ausgestaltung hat dabei einen wesentlichen Einfluss auf das Sicherheitskonzept sowie Eigenschaften wie Backup and Recovery, Sperrmechanismen, Offline-Unterstützung und Privatsphäre (Bastian et al., 2023, S. 387). Nachfolgend werden einige Wallet-Arten genauer erläutert:

- Das *Software Wallet* wird auf einem Gerät (Smartphone oder Computer) heruntergeladen und bieten eine einfache Bedienung, die den Benutzern ermöglicht, schnell und einfach Transaktionen durchzuführen (Egloff & Turnes, 2019, S. 89-91) (Bitpanda, 2023). Bei dieser Anwendung werden die private keys auf der lokalen Festplatte des Gerätes gespeichert (Hellwig et al., 2021, S. 48). Aufgrund ihrer Verbindung zum Internet werden Software Wallets grundsätzlich als unsicher eingestuft, da sie anfällig für Hacker, Malware oder Viren sind, die sich beim Gerät des Nutzers Zugang verschaffen könnten (Hellwig et al., 2021, S. 48). Ein Hacker könnte jedes Passwort, das auf einem Bildschirm erscheint, sehen und aufzeichnen oder sogar mit Hilfe von Spyware stehlen (Hellwig et al., 2021, S. 48).

- Das *Hardware Wallet* ist ein physisches Gerät, das die private keys des Benutzers offline speichert. Das kryptographisch gesicherte Gerät besitzt meistens einen USB-Anschluss und kann damit an einem Computer angeschlossen werden (Egloff und Turnes, 2019, S. 92; Bitpanda, 2023). Bei der ersten Initialisierung einer Hardware Wallet, wird der Nutzer aufgefordert eine Reihe von Wörtern (in der Regel sind es 12 oder 24 Wörter) zu notieren (Moreland, 2022). Diese Wörter dienen für die Wiederherstellung einer Hardware Wallet, d.h. falls eine vorhanden Hardware Wal-

let zurückgesetzt werden muss oder für die Initialisierung einer neuen Hardware-Wallet (Hellwig et al., 2021, S. 47). Die Sequenz der 12 oder 24 Wörter werden als Wiederherstellungsphrase (Moreland, 2022) oder Wiederherstellungs-Seed genannt (Hellwig et al., 2021, S. 47). Innerhalb der Hardware Wallets wird jeder private Schlüssel mithilfe eines Pseudozufallszahlengenerators (PRNG) von einer Zufallszahl abgeleitet, die durch einen „Seed“ initialisiert wurde (Hellwig et al., 2021, S. 47). Dieser Seed entspricht der Anfangszufallszahl oder der „nullten“ Zufallszahl in einer PRNG-generierten Sequenz und wird isoliert gespeichert (Hellwig et al., 2021, S. 47). Die Hardware Wallet gewährleistet Sicherheit, indem eine Sammlung privater Schlüssel ausschliesslich auf der Hardware gespeichert wird und somit „Software-isoliert“ ist, sodass kein private key jemals die Wallet verlässt (Hellwig et al., 2021, S. 47; Bitpanda, 2023). Der Besitzer hält die private keys direkt und muss sich keine Sorgen machen, dass sie gestohlen werden (Hellwig et al., 2021, S. 47). Selbst wenn ein Angreifer in einen Computer eindringt, kann er die Tokens (siehe Abschnitt 2.3.5) des Benutzers ohne den korrekten Seed nicht übertragen (Hellwig et al., 2021, S. 47).

- Bei einem *Paper Wallet* wird ein Ausdruck mit der public address und dem dazugehörigem private key generiert, der auf einem Stück Papier gedruckt werden kann (Egloff & Turnes, 2019, S. 92). Der Ausdruck muss sicher aufbewahrt werden (Bitpanda, 2023). Bei einem Verlust kann der private key nicht wiederhergestellt werden (Bitpanda, 2023).

- Bei einem *mobilen Wallet* wird das Smartphone als Speicherort und für die Nutzerauthentifizierung, welches nur lokal gegenüber dem Gerät stattfindet, genutzte (Bastian et al., 2023, S. 387). Alle Credentials und keys werden auf dem eigenen Smartphone gespeichert (Bastian et al., 2023, S. 387).

Im nachfolgendem Abbild 2.15 ist die Wallet-Funktion grafisch dargestellt.

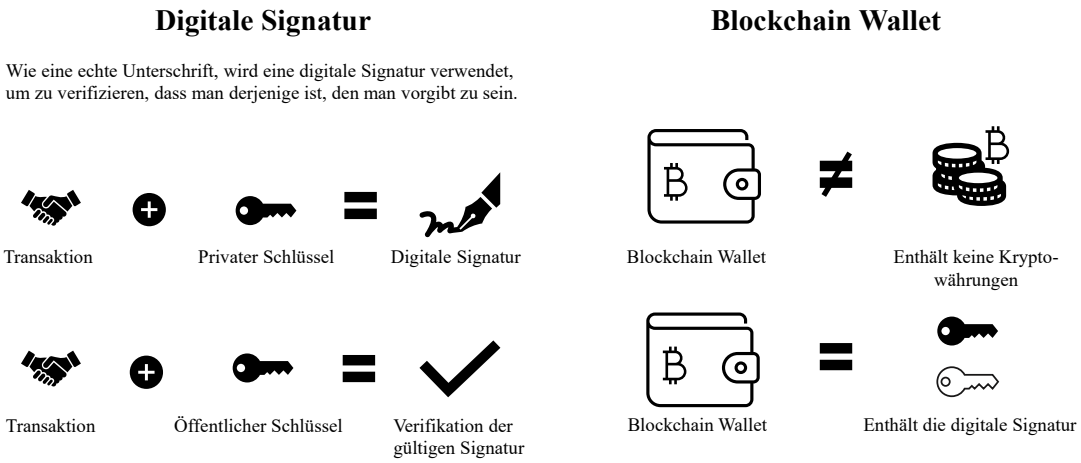

Abbildung 2.15 Wallet-Funktion (Voshmgir, 2020)

2.3.5 Digitale Tokens

Tokens sind digitale Einheiten, die auf der Blockchain-Plattform erstellt und verwendet werden können. Diese Einheiten können als Repräsentation von Vermögenswerten, Dienstleistungen oder Nutzungsrechten in einem Netzwerk betrachtet werden (Lesavre et al., 2021, S. 5-8). Tokens können fungible als auch nonfungible sein (Lesavre et al., 2021, S. 5-8).

Fungible Tokens haben identische Eigenschaften und sind daher austauschbar (Lesavre et al., 2021, S. 5-8). Das bedeutet, dass jedes Token in einer bestimmten Menge gleichwertig ist und keinen einzigartigen Wert besitzt (Lesavre et al., 2021, S. 5-8). Beispiele für fungible Tokens sind Kryptowährungen wie Bitcoin und Ether (Lesavre et al., 2021, S. 5-8). Ein Bitcoin ist ein Bitcoin und jeder andere Bitcoin ist genauso wertvoll wie der andere (Lesavre et al., 2021, S. 5-8; Egloff und Turnes, 2019, S. 84-86). Fungible Tokens werden nicht nur für Kryptowährungen verwendet, sondern können für verschiedenste Anwendungsfälle genutzt werden (Lesavre et al., 2021, S. 6). Unternehmen können Fungible Tokens als Teil ihrer Reward-Programme einsetzen, um Kunden für ihre Treue zu belohnen (Lesavre et al., 2021, S. 46-49). Die Kunden können die Tokens dann gegen Produkte oder Dienstleistungen austauschen (Lesavre et al., 2021, S. 46-49).

Nonfungible Tokens (NFT) hingegen sind einzigartig und können nicht durch andere Tokens ersetzt werden (Lesavre et al., 2021, S. 5-8). NFTs haben individuelle Merkmale oder Eigenschaften, die sie von anderen unterscheiden (Lesavre et al., 2021, S. 5-8). NFTs können beispielsweise als digitale Sammlerstücke dienen (Lesavre et al., 2021, S. 5-8). Beispiele hierfür sind CryptoKitties, die auf der Ethereum-Blockchain zu finden sind (Lesavre et al., 2021, S. 5-8). Jedes CryptoKitty ist einzigartig und hat individuelle Eigenschaften wie Farbe, Muster und Augenform (Lesavre et al., 2021, S. 5-8). NFTs können auch digitale Kunstwerke repräsentieren (Lesavre et al., 2021, S. 51-53). Künstler können ihre Werke als NFTs ausgeben und sie dann an Sammler verkaufen (Lesavre et al., 2021, S. 51-53). Dadurch können sie den Wert ihrer Werke besser kontrollieren und verwalten (Lesavre et al., 2021, S. 51-53). Ausserdem können NFTs als Identitätsnachweise eingesetzt werden (Lesavre et al., 2021, S. 51-53). Eine Person kann einen Token besitzen, der als digitaler Ausweis fungiert (Lesavre et al., 2021, S. 52-53). Dieser Ausweis kann dann für verschiedene Zwecke, wie für den Zugang zu Online-Diensten oder für digitale Abstimmungen verwendet werden (Lesavre et al., 2021, S. 52-53).

Wie bereits im Abschnitt 2.3.1 erwähnt, ist die Unveränderbarkeit der bestätigten Transaktion einer der grundlegenden Prinzipien der Blockchain-Technologie. Folgerichtig können getätigte Transaktionen auf der Blockchain nicht mehr storniert, verändert oder rückgängig gemacht werden (Exodus, 2023). Bei Tokens können hingegen Berechtigungen, die für Zugriffe erteilt worden sind, widerrufen werden (Opensea, 2023). Die erteilten Berechtigungen beziehungsweise Genehmigungen, ermöglichen es dezentralisierten Applikationen (siehe Abschnitt 2.3.7) eine bestimmte Aktion mit den Tokens des Nutzers durchzuführen (Opensea, 2023). Die erteilten Berechtigungen können auf einen bestimmten Zeitraum begrenzt werden, so dass sie nach Ablauf des Zeitraums automatisch widerrufen werden können (Opensea, 2023).

2.3.6 Smart Contracts

Smart Contracts (dt. intelligente Verträge) sind digitale Verträge, die auf Computerprotokollen basieren und automatisch abgewickelt werden (Meitinger, 2017, S. 371-372). Ein Smart Contract besteht aus einer selbst ausführenden Code-Datei, die auf einer Blockchain ausgeführt wird und in verschiedenen Programmiersprachen (Meitinger, 2017, S. 371-372), wie Solidity oder Serpent, geschrieben werden kann (Hellwig et al., 2021, S. 81). Für die Implementierung von nicht-trivalen Computerprogrammen ist die Funktionalität von Solidity oder Serpent notwendig, mit denen fast jedes Rechenproblem gelöst und Schleifen- und Verzweigungsanweisungen durchgeführt werden können (Hellwig et al., 2021, S. 81). Smart Contracts setzen eine DLT-Technologie voraus, auf der sich als zweite

Ebene ein Protokoll mit Plattformfunktion, wie zum Beispiel das Bitcoin oder Ethereum-Protokoll, befindet (Egloff & Turnes, 2019, S. 17). Smart Contracts agieren vollständig automatisch und bieten einen vielzähligen Anwendungsbereich wie beispielsweise in Geschäftsfeldern der Logistik und in der Immobilien- oder Finanzbranche (Steidl, 2022). Bei IoT-Geräten können Smart Contracts für die Kommunikation beziehungsweise für den Datenaustausch inkl. eigenständiger Interaktionen zwischen den vernetzten Geräten eingesetzt werden (Wilkens & Falk, 2019, S. 19).

Im Protokoll eines Smart Contracts werden die Bedingungen einer Vereinbarung zwischen den Parteien als Input und Outputs definiert (Neugebauer, 2018, S. 317; Egloff und Turnes, 2019, S. 141). Smart Contracts sind in der Lage, die Einhaltung der Vertragsbedingungen selbstständig zu überprüfen und entsprechend zu handeln (Hellwig et al., 2021, S. 81). Durch eine Benutzerinteraktion oder ein externes Event, in Form einer Transaktion auf der zugrundeliegenden Blockchain, kann der Smart Contract aktiviert werden. Nach der Aktivierung werden die definierten Bedingungen überprüft (Neugebauer, 2018, S. 317). Werden diese erfüllt, wird das Protokoll beziehungsweise der Vertrag automatisch durchgeführt, und zwar ohne die Notwendigkeit einer Zwischeninstanz wie beispielsweise einem Anwalt (BalthasarLegalAG, 2022). Für Smart Contracts wird keine menschliche Überwachung benötigt (BalthasarLegalAG, 2022). Zur Veranschaulichung dient Abbild 2.16.

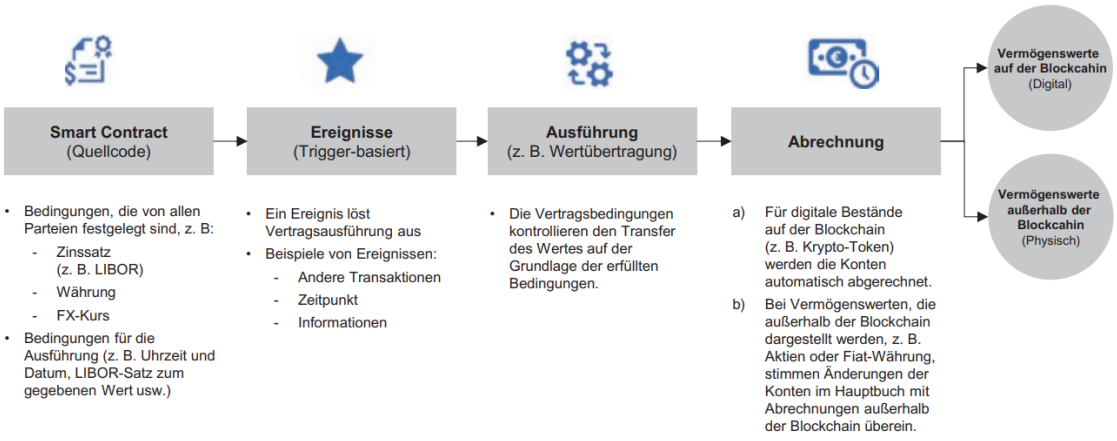

Abbildung 2.16 Ablaufdiagramm eines Smart Contracts (Hellwig et al., 2021, S. 82)

Die Ethereum-Plattform ist bisher die am weitesten entwickelte Smart Contract-Plattform und bietet eine Turing-vollständige Smart Contract-Funktionalität. Das bedeutet, dass mit der Programmiersprache Solidity jedes Rechenproblem gelöst werden kann (Hellwig et al., 2021, S. 81). Somit wird die Implementierung jeder beliebigen Logik möglich (Hellwig et al., 2021, S. 81). Mehrere Technologieunternehmen haben bereits Pilotprojekte mit der Ethereum-Infrastruktur durchgeführt, einschliesslich IBM und Microsoft (Hellwig et al.,

2021, S. 81).

Im nächsten Abbild 2.17 ist ein simples Codebeispiel für einen Smart Contract aufgeführt. Dieser Codeausschnitt in der Programmiersprache „Solidity“ stellt das Glücksspiel ’Münzwurf’ in einer WENN-DANN-Logik („if...then...else“) dar (Wilkens & Falk, 2019, S. 9). Der Smart Contract generiert eine Zufallszahl, wenn ein Spieler eine entsprechende Transaktion an den Smart Contract sendet (Wilkens & Falk, 2019, S. 9). Falls die Zufallszahl durch zwei teilbar ist, verdoppelt der Smart Contract den Wetteinsatz des Spielers (Wilkens & Falk, 2019, S. 9). Wenn die Zufallszahl nicht durch zwei teilbar ist, bleibt der Einsatz beim Smart Contract (Wilkens & Falk, 2019, S. 9).

```
pragma solidity ^0.4.18;
contract muenzwurf;
function();
var einsatz = msg.value;
if (block.timestamp % 2 == 0);
msg.sender.send(2 * einsatz);
else;
return;
```

Abbildung 2.17 Solidity-Codebeispiel „Münzwurf“ (Hellwig et al., 2021, S. 82)

Nachfolgend wird ein Beispiel für die Nutzung von Smart Contracts aufgeführt, die in der realen Welt Anwendung finden könnte, um autonome und dezentrale Entscheidungen zu treffen und Transaktionen durchzuführen. Dieses Beispiel wurde bereits von Samsung und IBM getestet (Wilkens & Falk, 2019, S. 19):

Eine Waschmaschine, die eigenständig Waschmittel nachbestellen und bezahlen kann. Die Waschmaschine überprüft eigenständig ihren Garantiestatus und bestellt bei Bedarf einen Handwerker. Darüber hinaus kann die Maschine den lokal erzeugten Strom von Photovoltaikanlagen nutzen, der von Gemeindemitgliedern bereitgestellt wird, und im Gegenzug eine bestimmte Anzahl von Waschgängen anbieten (Wilkens & Falk, 2019, S. 19).

Smart Contracts bilden die Grundlage für dezentrale Applikationen (Egloff & Turnes, 2019, S. 140), die im nächsten Abschnitt genauer erläutert werden.

2.3.7 Dezentrale Applikationen (DApps)

Dezentrale Applikationen (engl. Decentralised Applications, abgekürzt DApps) sind auf Smart Contracts basierende Applikationen, die über eine benutzerfreundliche Oberfläche verfügen und somit eine einfache Interaktion für die Nutzer erlauben (Egloff & Turnes, 2019, S. 155). Die Benutzerinteraktion mit einer DApp erfolgt über eine Benutzeroberfläche, die über das Internet zugänglich ist (Egloff & Turnes, 2019, S. 155). Eine DApp besteht aus mindestens einem Smart Contract sowie möglicherweise weiteren Front- und Backend-Programmcodes (Egloff & Turnes, 2019, S. 155-156). Im Abbild 2.18 ist der Aufbau einer DApp ersichtlich.

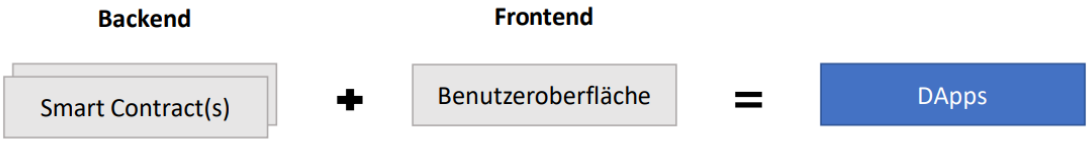

Abbildung 2.18 Aufbau DApps (Egloff & Turnes, 2019, S. 155)

Das Frontend kann auch auf einem zentralen Server betrieben werden (Egloff & Turnes, 2019, S. 155-156). So wäre die Benutzeroberfläche zwar auf einem zentralen Server gespeichert, das Backend (die Grundlogik der DApp) hingegen in den dezentral gehaltenen Smart Contracts, die mit dem zugrundeliegenden Blockchain-Netzwerk interagieren (Egloff & Turnes, 2019, S. 155-156). Eine digitale Anwendung (App) muss folgende Anforderungen erfüllen, um als DApp bezeichnet zu werden (Hellwig et al., 2021, S. 93):

- Die gesamten Daten werden kryptografisch gesichert in einer Blockchain gespeichert (Hellwig et al., 2021, S. 93).
- Bei der Applikation handelt es sich um eine Open-Source-Software, die vorzugsweise von einer offenen Community entwickelt wird (Hellwig et al., 2021, S. 93).
- Entscheidungen werden idealerweise durch die Blockchain selbst getroffen, indem sie im Konsens der Community verarbeitet werden (durch den zugrundeliegenden Konsensmechanismus) (Hellwig et al., 2021, S. 93).
- Der Zugang und die Belohnungen werden durch bereits vorhandene oder neu erstellte Token reguliert (Hellwig et al., 2021, S. 93).

2.4 Dezentrales Identitätsmanagement-Modell für selbstbestimmte Identitäten

Das Ziel einer dezentralen IdM-Lösung ist die Benutzer zu anonymisieren und gleichzeitig mit allen Funktionen auszustatten, ohne dabei einen Vertrauensverlust zu erleiden (Kulabukhova, 2019). Der Benutzer soll über die Datenhoheit verfügen und selbst entscheiden können, wem er Zugang zu seinen Daten gewähren möchte, ohne dabei an Sicherheit zu verlieren (Kulabukhova, 2019). In diesem Abschnitt wird die derzeit existierende Technologie im Bereich der selbstbestimmte Identität (engl. Self Sovereign Identity (SSI)) genauer erläutert. Eine relevante Rolle spielt dabei das Prinzip des Null-Wissens-Beweis (engl. Zero-Knowledge Proof (ZKP)) (Kulabukhova, 2019).

Wie bereits im Abschnitt 2.2.3 erwähnt, ist SSI ein Ansatz, bei dem Individuen die Kontrolle über ihre eigenen Identitätsdaten haben, anstatt dass diese von einer zentralen Behörde oder einer zentralen Datenbank verwaltet werden (Kulabukhova, 2019; Ehrlich et al., 2021). Demzufolge kann SSI dazu beitragen Vertrauen im digitalen Raum aufzubauen (Ehrlich et al., 2021). Denn SSI ermöglicht es den Benutzern, ihre Identität sicher und privat zu verwalten und zu teilen, was dazu beiträgt, das Vertrauen in digitalen Identitäten und damit in den digitalen Raum insgesamt zu stärken (Ehrlich et al., 2021).

2.4.1 Hauptkomponente der SSI

Die SSI umfasst drei Hauptkomponenten und wird als «Dreieck des Vertrauens» bezeichnet (Ehrlich et al., 2021, S. 254):

1. **Herausgeber (Issuer):**
   Der Issuer ist eine Stelle, die eine digitale Identität ausstellt und damit die Identität einer Person oder Organisation bestätigt (Ehrlich et al., 2021, S. 250-251). Er ist damit eine Art Vertrauensanker im SSI-Ökosystem (Ehrlich et al., 2021, S. 250-251). Der Issuer kann beispielsweise eine Regierungsbehörde, eine Bildungseinrichtung oder ein Arbeitgeber sein (Ehrlich et al., 2021, S. 250-251). Um eine digitale Identität auszustellen, muss der Issuer die Identität der Person überprüfen und die entsprechenden Informationen sammeln (Ehrlich et al., 2021, S. 250-251). Dazu können verschiedene Methoden, wie die Vorlage eines Personalausweises oder eine persönliche Identitätsüberprüfung, verwendet werden (Ehrlich et al., 2021, S. 250-251). Sobald die Identität bestätigt wurde, kann der Issuer eine digitale Identität ausstellen und sie mit einem kryptografischen Schlüsselpaar signieren, um ihre Echtheit zu

garantieren (Ehrlich et al., 2021, S. 250-251). Die digitale Identität kann dann vom sogenannten Holder verwendet werden, um sich bei verschiedenen Diensten und Anwendungen zu authentifizieren, ohne dass er seine Daten an Dritte weitergeben muss (Ehrlich et al., 2021, S. 250-251).

2. **Inhaber (Holder):**
   Der Holder ist eine Person oder eine Organisation, die eine digitale Identität besitzt und kontrolliert (Ehrlich et al., 2021, S. 250-251). Die digitale Identität wird von einem Issuer ausgestellt und vom Holder aufbewahrt (Ehrlich et al., 2021, S. 250-251). Für die Aufbewahrung kann der Holder ein Wallet-App nutzen (Ehrlich et al., 2021, S. 250-251). Der Holder ist damit der Besitzer und Verwalter seiner eigenen Identitätsdaten und hat die volle Kontrolle darüber, wie und wann diese Daten freigegeben werden (Ehrlich et al., 2021, S. 250-251). Der Holder verwendet seine digitale Identität, um sich bei verschiedenen Diensten und Anwendungen zu authentifizieren, ohne seine persönlichen Daten an Dritte weiterzugeben (Ehrlich et al., 2021, S. 250-251). Die Identität wird dabei vom Holder selbst verwaltet, gespeichert und genutzt, was ihm ein hohes Mass an Autonomie und Kontrolle über seine Identität gibt (Ehrlich et al., 2021, S. 250-251).

3. **Akzeptanzstelle (Verifier):**
   Der Verifier ist eine Person oder Organisation, die die Identität eines Holders prüfen möchte, bevor sie ihm Zugang zu einem bestimmten Dienst oder einer bestimmten Anwendung gewährt (Ehrlich et al., 2021, S. 250-251). Der Verifier kann eine Regierungsbehörde, ein Unternehmen oder eine andere Organisation sein, die einen Identitätsnachweis von einem Holder benötigt, bevor sie diesem einen bestimmten Service oder eine bestimmte Leistung anbieten kann (Ehrlich et al., 2021, S. 250-251). Der Verifier interagiert mit dem Holder, um die Echtheit der digitalen Identität des Holders zu überprüfen. Der Holder gibt dabei nur diejenigen Informationen bekannt, die für den jeweiligen Verifier notwendig sind, ohne seine gesamte Identität offenzulegen (Ehrlich et al., 2021, S. 250-251). Die Identitätsdaten werden von dem Holder mit Hilfe von kryptographischen Methoden signiert und können so vom Verifier überprüft werden (Ehrlich et al., 2021, S. 250-251).

Im SSI-Ökosystem ist die Interaktion zwischen Verifier und Holder aufgrund der dezentralen Architektur einfach und sicher (Ehrlich et al., 2021, S. 250-251). Der Verifier fordert die Identitätsdaten vom Holder an, der daraufhin entscheidet, welche Informationen er freigeben möchte (Ehrlich et al., 2021, S. 250-251). Sobald der Verifier die Identitätsdaten erhalten hat, kann er deren Echtheit mit Hilfe von

kryptographischen Verfahren prüfen (Ehrlich et al., 2021, S. 250-251).

Nebst den drei Hauptkomponenten gibt es eine weitere Komponente, die zu beachten ist: **das Subjekt** (Ehrlich et al., 2021, S. 250). Als Subjekt wird die Entität bezeichnet, auf die sich die Identifikationsmerkmale beziehen (Ehrlich et al., 2021, S. 250). Dabei kann es sich um ein Objekt handeln, das sich im Besitz des Holders befindet oder um eine Person, für die der Holder verantwortlich ist oder eine Vollmacht hat (Ehrlich et al., 2021, S. 250). Das Subjekt stimmt in den meisten Fällen mit dem Holder überein (Ehrlich et al., 2021, S. 250).

2.4.2 Elemente der SSI

Zur Umsetzung eines SSI-Systems werden drei Grundelemente benötigt, für die bereits Standardisierungsaktivitäten laufen, die sich mit der Entwicklung und Implementierung dieser drei Elemente befassen (Ehrlich et al., 2021, S. 256).

Tabelle 2.2 Grundelemente der SSI (Ehrlich et al., 2021, S. 256)

Bestandteile eines SSI-Systems	Standardisierungen
(1) Dezentrale Identifikatoren für verschiedene Entitäten	Decentralized Identifiers
(2) Kryptografisch abgesicherte Datenformate zur Beschreibung der Identitätsmerkmale	Verifiable Credentials
(3) Ein Protokoll für die Peer-to-Peer Kommunikation zwischen den beteiligten Parteien	DIDcomm

Die drei Standardisierungen der Elemente werden nachfolgend genauer erläutert.

Decentralized Identifiers

Decentralized Identifiers (DID) sind eine Art digitale Identitäten, die einzigartig, dezentralisiert und kryptografisch sicher sind (Ehrlich et al., 2021, S. 256). Sie werden verwendet, um einen eindeutigen Identitätsnachweis für eine Person oder eine Organisation zu erstellen, der unabhängig von einem zentralen Autoritätssystem ist (Ehrlich et al., 2021, S. 256). Technisch gesehen besteht eine DID aus zwei Hauptkomponenten: der DID-URL und dem DID-Dokument (Ehrlich et al., 2021, S. 256-257).

Die DID-URL ist die eindeutige Identifikation für eine DID und besteht aus der Zeichenfolge 'did:' gefolgt von einem bestimmten DID-Method-Name, der für die gewählte Methode zur Erstellung der DID steht (Ehrlich et al., 2021, S. 256-257). Zum Beispiel könnte der DID-Method-Name 'sov' für eine DID auf der Hyperledger Indy-Blockchain verwendet werden (Ehrlich et al., 2021, S. 256-257). Die DID-URL enthält auch die eindeutige ID für die DID, die normalerweise aus einer zufällig generierten Zeichenfolge besteht (Ehrlich et al., 2021, S. 256-257).

Das DID-Dokument enthält alle Informationen, die für die DID erforderlich sind, einschliesslich der öffentlichen Schlüssel, die zur Verifizierung der DID verwendet werden (Ehrlich et al., 2021, S. 256-257). Ein typisches DID-Dokument könnte folgende Felder enthalten (Ehrlich et al., 2021, S. 256-257):

- Kontext: Gibt das Kontextformat für das Dokument an, z.B. JSON-LD
- ID: Die eindeutige ID für die DID
- Public Key: Der öffentliche Schlüssel, der zur Verifizierung der DID verwendet wird
- Authentication: Ein Feld, das die Möglichkeiten für die Authentifizierung der DID angibt
- Service: Ein Feld, das zusätzliche Informationen über den Service oder die Organisation enthält, die die DID erstellt hat

Das DID-Dokument wird auf einer dezentralen Plattform wie einer Blockchain oder einem dezentralen Register gespeichert (Ehrlich et al., 2021, S. 256-257). Jede Änderung am DID-Dokument wird durch eine Transaktion auf der Plattform verifiziert und muss von den beteiligten Parteien genehmigt werden (Ehrlich et al., 2021, S. 256-257). Wenn eine Person eine DID erstellt, erzeugt sie einen public und einen private key (Ehrlich et al., 2021, S. 256-257). Der public key wird in das DID-Dokument eingefügt und der private key wird von der Person selbst aufbewahrt (Ehrlich et al., 2021, S. 256-257). Wenn ein Serviceprovider eine Anfrage an die DID sendet, um die Identität der Person zu überprüfen, kann der Serviceprovider den public key verwenden, um das DID-Dokument zu überprüfen und sicherzustellen, dass es von der Person selbst erstellt wurde (Ehrlich et al., 2021, S. 256-257). Dadurch wird das Vertrauen in die Identität der Person gestärkt, ohne dass eine zentrale Autorität erforderlich ist (Ehrlich et al., 2021, S. 256-257). Im Abbild 2.19 ist die Beziehung zwischen DID, DID-Dokument, DLT und der Entität ersichtlich.

Abbildung 2.19 Beziehung zwischen DID, DID-Dokument (mit JSON-LD Repräsentation), DLT und Entität (Ehrlich et al., 2021, S. 256)

Verifiable Credentials (VC)

Verifiable Credentials (VC) sind digitale Zertifikate, die eine bestimmte Aussage über eine Person oder Organisation enthalten, z.B. dass sie ein bestimmtes Alter haben, eine bestimmte Ausbildung oder Berufserfahrung haben, oder dass sie Mitglied einer bestimmten Organisation sind (Ehrlich et al., 2021, S. 254). Diese Zertifikate können von einer vertrauenswürdigen Stelle ausgestellt werden und enthalten auch kryptografische Beweise, die es anderen Parteien ermöglichen, ihre Gültigkeit zu überprüfen, ohne die Identität der Person oder Organisation offenlegen zu müssen (Ehrlich et al., 2021, S. 254). Ein VC besteht aus drei Hauptkomponenten: der Aussage, Metadaten und dem Beweis (Ehrlich et al., 2021, S. 254). Die Aussage beschreibt die behauptete Information bezüglich des Subjektes, z.B. dass eine Person ein bestimmtes Alter hat oder dass sie einen bestimmten Abschluss hat (Ehrlich et al., 2021, S. 254). Die Metadaten beschreiben das Zertifikat selbst, einschliesslich seinem Issuer und seines Ablaufdatums (Ehrlich et al., 2021, S. 254). Aus Sicherheitsgründen sind diese Daten signiert (Ehrlich et al., 2021, S. 254). Mit der Unterstützung von DID kann der Issuer und das Subjekt des VC referenziert werden und ermöglicht somit die Rollen eindeutig zu identifizieren (Ehrlich et al., 2021, S. 254). Der Beweis besteht aus einem digital signierten Zertifikat und gewährleistet, dass die Behauptung tatsächlich vom Issuer des VC ausgestellt wurde (Ehrlich et al., 2021, S. 254). Um ein VC zu erstellen, kann eine Person eine Anfrage an eine vertrauenswürdige Stelle senden, welches die Aussage bestätigt (Ehrlich et al., 2021, S. 254-259). Die vertrauenswürdige Stelle muss die Aussage überprüfen und ein digitales Zertifikat ausstellen können (Ehrlich et al., 2021, S. 254-259). Das digitale Zertifikat wird dann in das VC eingefügt und das VC wird an die Person zurückgegeben (Ehrlich et al., 2021, S. 254-259).

Um die Behauptungen innerhalb des VC in Interaktionen geltend zu machen, muss der Verifier sie mit geeigneten Mitteln überprüfen (Ehrlich et al., 2021, S. 254-259). Für die Überprüfung wird vom Verifier Vertrauen zum Issuer vorausgesetzt (Ehrlich et al., 2021, S. 254-259). Der Verifier bekommt vom Holder keine direkte Kopie des VC, sondern eine spezielle Datenstruktur namens „Verifiable Presentation“, die ausgewählten Daten aus verschiedenen VC enthält (Ehrlich et al., 2021, S. 254-259). In der Verifiable Presentation (VP) werden zusätzliche Metadaten wie Nutzungsbedingungen aufgeführt, sowie ein weiterer Beweis beigefügt, der die Integrität der Datenstruktur absichert (Ehrlich et al., 2021, S. 254-259).

Im Abbild 2.20 ist ein Beispiel von einem VC ersichtlich. Im Anhang A sind die Grundkomponenten und Inhalte von einem VC und VP detaillierter dargestellt. Für den Beweis werden mathematische Methoden wie Zero-Knowledge-Proof angewendet, die es ermöglichen, dass eine Person ihre Aussagen beweist, ohne die eigentlichen Daten offenlegen zu müssen (Ehrlich et al., 2021, S. 254-259). Dadurch kann die Privatsphäre der Person geschützt werden, während gleichzeitig die Gültigkeit der Aussage bestätigt wird (Ehrlich et al., 2021, S. 254-259). Das Prinzip des Zero-Knowledge Proofs wird im Abschnitt 2.4.3 genauer erläutert. Das Vorweisen von Präsentationen, die durch Zero-Knowledge-Proofs abgesichert sind und in Verbindung mit DID stehen, erfüllt die Prinzipien von SSI konsequent und ermöglicht den sicheren Nachweis von Behauptungen, während gleichzeitig die Kontrolle über kontextspezifische Identifikatoren beim Subjekt verbleibt (Ehrlich et al., 2021, S. 258-259).

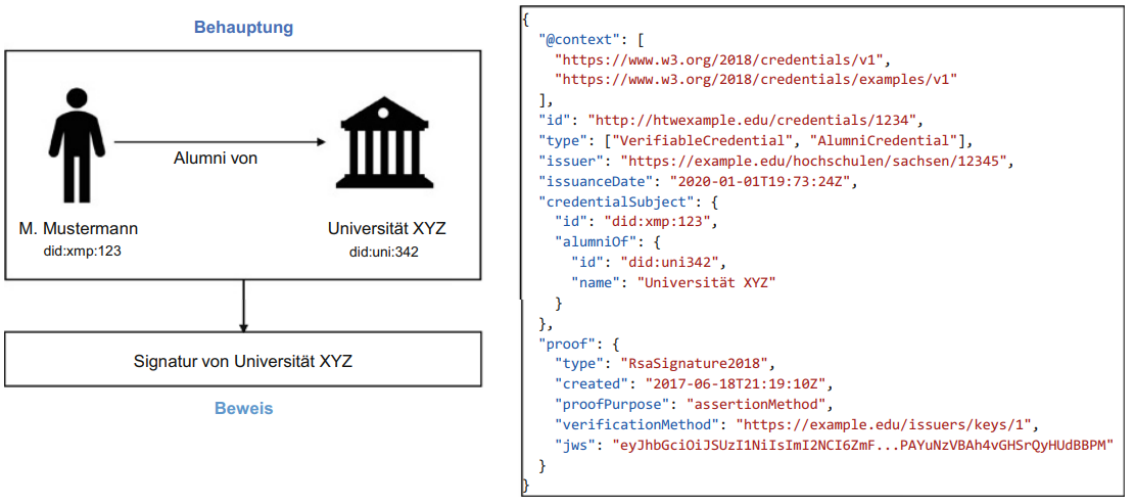

Abbildung 2.20 Anwendungsbeispiel Verifiable Credential inkl. JSON-LD Repräsentation (Ehrlich et al., 2021, S. 258)

Im nächsten Abbild 2.21 wird in einem Drei-Akteuren-Modell der Prozess der Ausstellung eines VC und der Ausgabe einer VP vereinfacht dargestellt (Schardong & Custódio, 2022, S. 6-7).

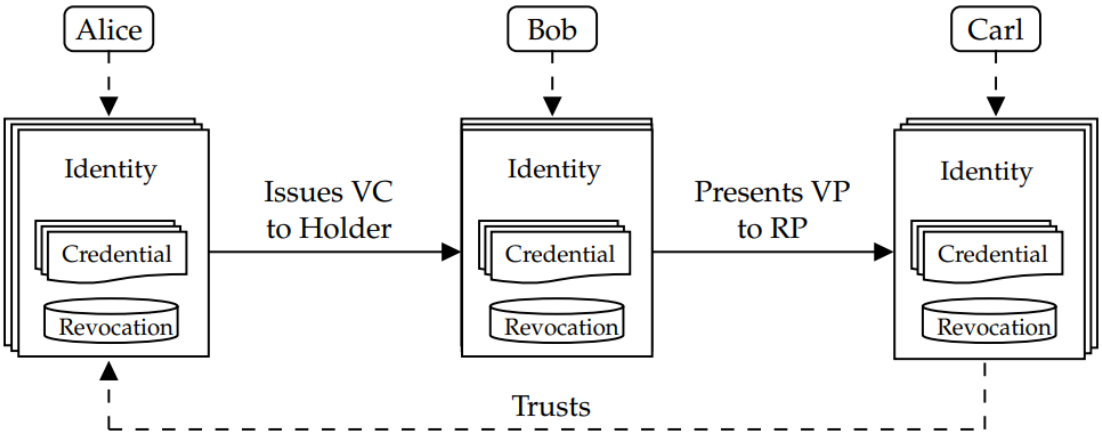

Abbildung 2.21 VC und VP Prozess im Drei-Akteuren-Modell (Schardong & Custódio, 2022, S. 6-7)

Drei Personen Alice, Bob und Carl besitzen ihre elektronischen Identitäten, die jeweils auf bestimmte Situationen zugeschnitten sind. Die Identitäten beinhalten eine Verknüpfung zu den Datenbanken, die ausgestellte und empfangene Berechtigungsnachweise sowie ein Widerrufsregister für abgelaufene oder widerrufene Berechtigungsnachweise enthalten (Schardong & Custódio, 2022, S. 6-7). Alice möchte belegen, dass Bob ein seriöser Verkäufer von hochwertigen Weinen ist und stellt seiner elektronischen Identität einen Berechtigungsnachweis (VC) aus. Bob möchte Carl beweisen, dass er einen guten Ruf hat und schickt ihm als Beweis eine erstellte VP basierend auf dem VC von Alice. Alice ist eine weltweit anerkannte Winzerin, weshalb Carl der Ausstellerin des VCs (Alice), vertraut. Aufgrund des VP und des Vertrauens an Alice nimmt Carl Verhandlungen mit Bob auf (Schardong & Custódio, 2022, S. 6-7).

DIDcomm

DIDcomm (ausgeschrieben 'Decentralized Identifier Communication') ist ein sicheres Kommunikationsprotokoll, das für den Austausch von verschlüsselten Nachrichten zwischen DIDs verwendet wird (Ehrlich et al., 2021, S. 259). DIDcomm stellt sicher, dass die Kommunikation zwischen den Parteien sicher und vertraulich bleibt, indem es eine Ende-zu-Ende-Verschlüsselung und einen eindeutigen Schlüsselaustausch zwischen den Parteien ermöglicht (Ehrlich et al., 2021, S. 259). Dazu verwendet DIDcomm eine verschlüsselte und signierte JSON-Struktur namens 'DIDcomm Message' (Ehrlich et al., 2021, S. 256-260). Jede DIDcomm Message enthält eine Nachrichten-ID, eine Liste von Empfänger-

und Absender-DIDs sowie den Inhalt der Nachricht, der entweder eine verschlüsselte VC oder eine verschlüsselte Textnachricht sein kann (Ehrlich et al., 2021, S. 256-260). Die Verschlüsselung der Nachrichten wird durch die Verwendung der öffentlichen Schlüssel der Empfänger-DIDs und der Verwendung der privaten Schlüssel der Absender-DIDs erreicht (Ehrlich et al., 2021, S. 256-260). Jeder Empfänger kann seine eigene Nachricht entschlüsseln, indem er den privaten Schlüssel seiner eigenen DID verwendet (Ehrlich et al., 2021, S. 256-260). Dadurch können nur die Empfänger, die im Besitz des privaten Schlüssels ihrer eigenen DID sind, die Nachricht entschlüsseln (Ehrlich et al., 2021, S. 256-260). Um sicherzustellen, dass die Nachrichten nicht gefälscht oder manipuliert werden, wird jeder DIDcomm Message eine digitale Signatur hinzugefügt, die mit dem privaten Schlüssel der Absender-DID erzeugt wird (Ehrlich et al., 2021, S. 256-260). Die Empfänger können dann die Signatur mit dem öffentlichen Schlüssel der Absender-DID überprüfen, um sicherzustellen, dass die Nachricht tatsächlich von der angegebenen Absender-DID stammt und nicht manipuliert wurde (Ehrlich et al., 2021, S. 256-260). DIDcomm wird auch durch ein spezielles Protokoll namens 'DIDcomm Protocol' unterstützt, das den Nachrichtenaustausch zwischen verschiedenen SSI-Systemen erleichtert (Ehrlich et al., 2021, S. 256-260). Das DIDcomm Protocol legt Regeln und Standards fest, wie Nachrichten ausgetauscht werden und wie die verschiedenen Parteien in einem SSI-Ökosystem miteinander kommunizieren können (Ehrlich et al., 2021, S. 256-260).

Vertrauenswürdiges Datenregister

Dezentrale Datenregister werden häufig eingesetzt, um DIDs und VCs zu registrieren, aktualisieren oder zu widerrufen oder um die Verifizierungsverfahren und Schemata zu beschreiben (Ehrlich et al., 2021, S. 259). Zusätzlich werden Beschreibungen von VC-Attributen und Gültigkeitsdefinitionen aufgeführt (Ehrlich et al., 2021, S. 259). Der Verifier benötigt einen Vertrauensanker zur Überprüfung, wenn VC von Dritten herausgegeben werden und verifiziert werden müssen und nutzt deshalb ein vertrauenswürdiges Datenregister (Ehrlich et al., 2021, S. 259). Um VC in das vertrauenswürdige Datenregister zu speichern, muss der Benutzer eine Transaktion an die Blockchain senden. Diese Transaktion enthält die relevanten Informationen des VC sowie die digitale Signatur des Herausgebers (Ehrlich et al., 2021, S. 256-259). Die Transaktion wird dann von den Knotenpunkten im Blockchain-Netzwerk validiert und in der dezentralen Datenbank gespeichert (Ehrlich et al., 2021, S. 256-259). Um einen VC abzurufen, muss der Benutzer den Hash-Wert des VC in der Blockchain nachschlagen (Ehrlich et al., 2021, S. 256-259). Der Hash-Wert dient als eindeutige Kennung des VC und ermöglicht es den Benutzern, den Ursprung und die Authentizität des VC zu überprüfen (Ehrlich et al., 2021, S. 256-259).

Im nachfolgendem Abbild 2.22 ist die SSI-Architektur mit allen Komponenten und Elementen aufgeführt.

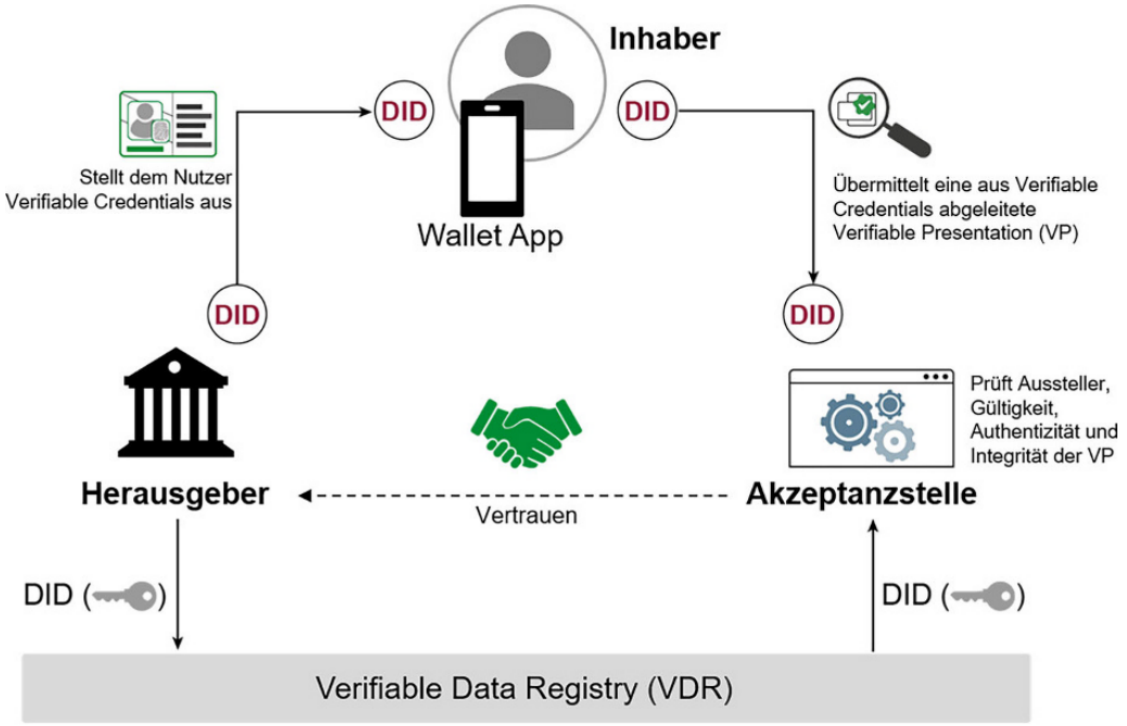

Abbildung 2.22 Architektur von Self-Sovereign Identity (Anke & Richter, 2023, S. 269)

2.4.3 Zero Knowledge Proof

Zero Knowledge Proof (ZKP) ist ein kryptographisches Protokoll, das auf mathematischen Gleichungen basiert (Babel & Sedlmeir, 2023) und wird zur Gewährleistung von Privatsphäre und Sicherheit der Benutzer eingesetzt (Kulabukhova, 2019). ZKP erlaubt dem Benutzer, Informationen auszutauschen, ohne dabei konkrete Informationen offenzulegen (Kulabukhova, 2019; Babel und Sedlmeir, 2023). Der Beweisende erstellt eine digitale Signatur für die Aussage, die er beweisen möchte, und teilt diese digitale Signatur mit dem Verifizierenden (Ethereum, 2023). Der Verifizierende kann nun überprüfen, ob die digitale Signatur korrekt ist, ohne tatsächliche Informationen über den Beweis zu kennen (Ethereum, 2023). Beispielsweise könnte ein Benutzer beweisen, dass er über 18 Jahre alt ist, ohne sein genaues Geburtsdatum bekanntzugeben (Kulabukhova, 2019; Ethereum, 2023). Dadurch wird die Datensparsamkeit erhöht und die persönlichen Daten des Benutzers bleiben geschützt (Babel & Sedlmeir, 2023). ZKP bieten ein hohes Mass an Datenschutz und Sicherheit (Kulabukhova, 2019). In der SSI können ZKP verwendet werden, um die Identität einer Person zu bestätigen, ohne persönliche Informationen zu übermit-

teln (Kulabukhova, 2019). ZKP bieten auch in anderen Bereichen, wie bei Online-Banking Plattformen oder bei der Authentifizierung von IoT-Geräten Anwendung (Kulabukhova, 2019). Es gibt verschiedene Arten von ZKP-Protokollen, darunter interaktive und nicht-interaktive Protokolle (Yang und Wang, 2023, S. 517; Ethereum, 2023). Interaktive Protokolle erfordern eine Interaktion zwischen den Beweisenden und den Verifizierenden, um den Beweis zu generieren und zu überprüfen (Yang und Wang, 2023, S. 517; Ethereum, 2023). Nicht-interaktive Protokolle hingegen erlauben die Erstellung und Überprüfung von Beweisen ohne eine direkte Interaktion zwischen den beiden Parteien (Yang und Wang, 2023, S. 517; Ethereum, 2023).

2.4.4 Modell

Nachfolgend werden die Modelle des zentralen IdM-Modell (siehe Abbild 2.5 vom Abschnitt 2.2.1 und Abbild 2.6 vom Abschnitt 2.2.2) auf das dezentrale SSI-IdM Modell abgeleitet und anhand eines Beispiels erläutert. Die drei vorherigen Entitäten aus dem zentralen IdM-Modell ändern sich im dezentralen IdM-Modell wie folgt:

- Der User wird zum **Holder (Inhaber)**
- Der Identity Provider (IdP) wird zum **Verifier (zur Prüfstelle)**
- Der **Service Provider (SP)** bleibt weiterhin bestehen
- Zusätzlich wird eine weitere Entität, nämlich der **Issuer (Aussteller)**, benötigt

Wird das zentrale IdM-Modell mit den entsprechenden Entitäten angepasst, resultiert daraus das nachfolgende Abbild 2.23. Der Prozess würde wie folgt ablaufen:

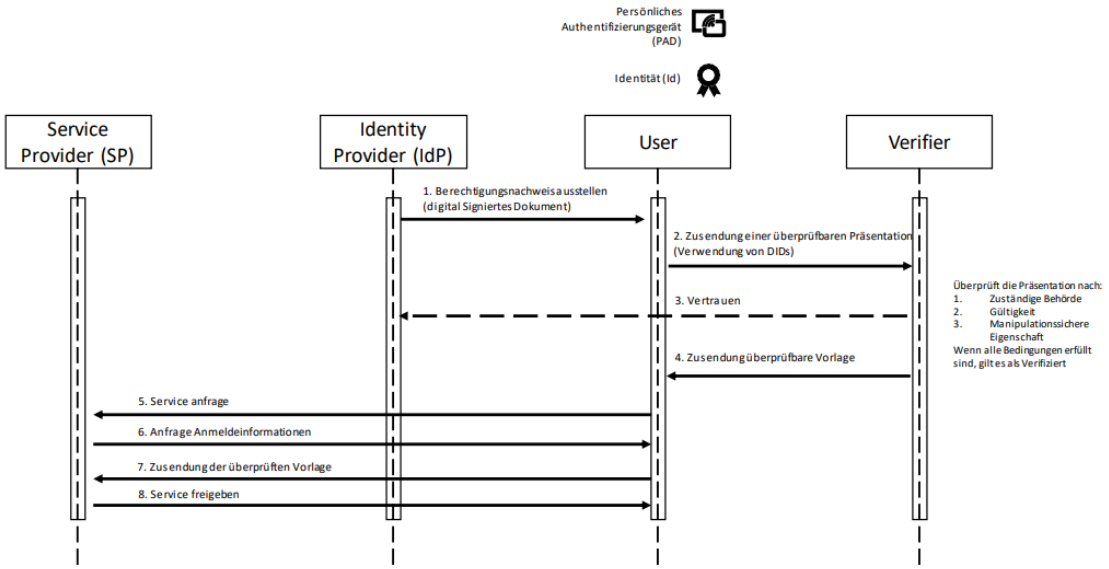

Abbildung 2.23 Vereinfachung eines dezentrales IdM-Modell mit SSI

1. Eine Universität (Issuer) stellt der Absolventin Alice (Holder) das Diplom (VC) für ihren Masterabschluss aus.

2. Alice (Holder) bewahrt das Diplom in einem sicheren und verschliessbaren Aktenkoffer (Wallet). Für die internationale Anerkennung des Diploms wird eine Kopie sowie weitere benötigte Dokumente (VP) der Behörde (Verifier) für die Überprüfung und Akzeptanz geschickt.

3. Die Behörde (Verifier) überprüft die Kopie des Diploms und die weiteren Dokumente (VP) auf ihre Echtheit und Gültigkeit. Die Behörde (Verifier) vertraut dabei der Universität (Issuer), dass das Diplom gerechtfertigt ausgestellt wurde.

4. Nach der erfolgreichen Überprüfung sendet die Behörde (Verifier) eine Bestätigung (VC) an Alice (Holder).

5. Alice (Holder) bewirbt sich bei einem Unternehmen für eine ausgeschriebene Stelle.

6. Für die ausgeschriebene Stelle wird ein Hochschulabsolvent gesucht. Das Unternehmen (Service Provider) fordert von Alice (Holder) eine Bescheinigung (VC) eines Hochschulabschlusses.

7. Alice (Holder) schickt dem Unternehmen (Service Provider) die Bestätigung (VC), die sie von der Behörde erhalten hat.

8. Das Unternehmen (Service Provider) stellt daraufhin Alice (Holder) ein.

Jedoch gibt es auch beim SSI-Ansatz wichtige Aspekte zu beachten, die bei der Umsetzung Herausforderungen darstellen könnten.

2.4.5 Herausforderungen

Nachfolgenden werden die wesentlichsten Hürden aufgeführt und erläutert. Dabei werden die Erkenntnisse aus der Literaturrecherche im Kapitel 4 abstrahiert und in Anforderungen an ein dezentrales IdM-Modell transformiert.

1. Organisation:
   Die Einführung von SSI markiert nicht nur eine neue Technologie, sondern auch einen fundamentalen Wandel im Paradigma der Datenverwaltung (Ehrlich et al., 2021, S. 264). Dies hat zur Folge, dass Diskussionen über fehlende technische Standards oder regulatorische Hürden wie die DSGVO und eIDAS bei der Planung neuer Produkte und Geschäftsmodelle entstehen (Ehrlich et al., 2021, S. 264). Die bisherigen Ansätze, die auf föderierten und isolierten Identitäten basierten, sind nicht mehr ausreichend und erfordern eine Überprüfung und Anpassung an die neuen Prinzipien von SSI (Ehrlich et al., 2021, S. 264). Dies kann zu Herausforderungen und Unsicherheiten führen, da Organisationen ihre Herangehensweise an Identitätsmanagement und Datenverwaltung überdenken und anpassen müssen, um den Anforderungen und Potenzialen von SSI gerecht zu werden (Ehrlich et al., 2021, S. 264). Es ist notwendig, innovative Geschäftskonzepte, Prozesse und Kooperationen zu entwickeln, um das volle Potenzial von SSI zu nutzen und gleichzeitig die Einhaltung von regulatorischen Vorgaben sicherzustellen (Ehrlich et al., 2021, S. 264). Im Vergleich zur Umsetzung einer dezentralen Verwaltung könnte der Aufwand jedoch abschreckend sein, da alle beteiligten Parteien individuell prüfen müssen, wo und wie eine Dezentralisierung sinnvoll ist (Ehrlich et al., 2021, S. 264). Dezentralisierung ist jedoch wichtig, um die Kontrolle über Identitätsinformationen den Benutzern zu überlassen und nicht auf zentralisierte Institutionen zu vertrauen (Ehrlich et al., 2021, S. 251). Es muss den Benutzern möglich sein, über ihre eigene Identität und Identitätsinformationen zu verfügen, sie selbst zu verwalten und zu kontrollieren (Ehrlich et al., 2021, S. 251; Draht, 2019). Der Benutzer muss Zugang zu seinen eigenen Daten haben (van Dijk et al., 2021, S. 8). Die Verwendung der Identität darf nur mit Zustimmung des Benutzers erfolgen (van Dijk et al., 2021, S. 8). Dabei sollen nicht mehr Daten offengelegt werden als das der Nutzer möchte (van Dijk et al., 2021, S. 8). Langfristig wird eine Standardisierung für das Datenmanagement und für Wallets benötigt (Soltani et al., 2021, S. 8), um eine Übertragbarkeit von

Daten zwischen verschiedenen Wallet-Arten bieten können (van Dijk et al., 2021, S. 39-40). Dadurch könnten Endnutzer ihre Daten einfach und sicher von einem Wallet zum Anderen übertragen, ohne dass ein Kontinuitätsproblem entsteht, wenn ein Wallet-Anbieter seine Dienste einstellt (van Dijk et al., 2021, S. 39-40). Das Wallet soll die Fähigkeit haben, unkompliziert zwischen den von vielen verschiedenen Organisationen zur Verfügung gestellten Zugangsdaten navigieren zu können, wobei jede Organisation zum Wallet eine oder mehrere aktive Verbindungen hat (van Dijk et al., 2021, S. 39-40). Ausserdem müssen Identitäten langlebig und flexibel sein, um Änderungen im Laufe des Lebens, wie zum Beispiel Namens- oder Adressänderungen, des Identitätsinhabers zu ermöglichen (Soltani et al., 2021, S. 7). Es sollte den Identitätsinhabern möglich sein, Identitätsdaten zu erhalten, ändern oder entfernen zu können (Soltani et al., 2021, S. 7). Identitätsdaten müssen transportabel sein, um deren Langlebigkeit zu gewährleisten (Soltani et al., 2021, S. 7). Es ist notwendig, dass diese Daten nicht an ein einziges Unternehmen gebunden sind, um Missbrauch zu vermeiden (Soltani et al., 2021, S. 7).

2. Technische Umsetzung:
   Die Umsetzung von SSI bringt technische Herausforderungen mit sich, wie zum Beispiel die Notwendigkeit einer sicheren und zuverlässigen Speicherung von Identitätsinformationen und Schlüsseln sowie die Integration von SSI-Systemen in bestehende IT-Infrastrukturen (Ehrlich et al., 2021, S. 265). Darüber hinaus gibt es Herausforderungen bei der Entwicklung von sicheren und benutzerfreundlichen SSI-Apps und -Diensten (Ehrlich et al., 2021, S. 265). Eine zentrale Hürde ist die unzureichende Netzinfrastruktur im Bereich Internet und Mobilfunk, insbesondere in Europa, wo die Netzabdeckung nicht flächendeckend ist (Ehrlich et al., 2021, S. 265). Unternehmen ermöglichen oft ihren Mitarbeitern die Einbindung von privaten Geräten in das WLAN-Netz, während beispielsweise Fahrer von Logistikunternehmen auf Mobilfunk angewiesen sind (Ehrlich et al., 2021, S. 265). Obwohl ein Gastzugang in ein WLAN-Netz aus technischer Sicht möglich ist, verbieten viele Unternehmen aus Sicherheitsgründen externe Mobilgeräte oder die Freigabeprozesse sind im Vergleich zum Nutzen zu aufwändig (Ehrlich et al., 2021, S. 265). Die Datenverfügbarkeit stellt eine weitere technische Hürde dar, da Organisationen daran gewöhnt sind, uneingeschränkt auf Informationen zuzugreifen (Ehrlich et al., 2021, S. 265). Durch die dezentrale Aufbewahrung mit Erlaubniseinforderung werden diese gewohnten Arbeitsprozesse eingeschränkt (Ehrlich et al., 2021, S. 265). Vor allem wenn sich der Service Provider in einer anderen Zeitzone als der Dateninhaber befindet, könnte es ein Problem darstellen (Ehrlich et al., 2021, S. 265). In solchen Fällen können Identity Hubs oder entsprechend konfigurierte Agents helfen, Freiga-

ben basierend auf festgelegten Regeln automatisch zu erteilen und Abhilfe zu schaffen (Ehrlich et al., 2021, S. 265).

3. Sicherheit:
   Ein weiterer Aspekt betrifft die Sicherheitsanforderungen von Wallets, um Angriffen vorzubeugen und unbefugten Zugriff zu verhindern (Ehrlich et al., 2021, S. 265). Gleichzeitig müssen Wallets dem Nutzer eine komfortable Möglichkeit bieten, auf verschiedene Blockchain-Netzwerke zuzugreifen und Credentials sowie Präsentationen flexibel zu verwalten (Ehrlich et al., 2021, S. 265). Ab diesem Zeitpunkt tragen die Nutzer die Eigenverantwortung ihrer Daten (Ehrlich et al., 2021, S. 265). Für das Tragen dieser Eigenverantwortung sollten die Nutzer technisch als auch pädagogisch sensibilisiert sein (Ehrlich et al., 2021, S. 265). Bei aktuellen Wallets werden oft nur Akzeptieren-Abbruch-Funktionen eingeführt, die dem Nutzer jedoch nicht das Gefühl von Kontrolle vermittelt, sondern eher mit den Lizenzbestimmungen von Software oder Cookie-Informationen vergleichbar sind (Ehrlich et al., 2021, S. 265). Ein weiteres Problem stellt die Kompromittierung des Wallets dar (Kubach et al., 2020, S. 43). Ein Hacker könnte den private Key eines Nutzers kopieren und die dazugehörigen Anmeldeinformationen verwenden (Kubach et al., 2020, S. 43). Der Nutzer würde davon nichts mitbekommen, da der privat Key nicht fehlt sondern nur kopiert wurde (Kubach et al., 2020, S. 43). Die Identitätsinformationen müssen vor technischen Ausfällen, Störungen oder Cyber-Angriffen geschützt werden (Draht, 2019).

4. Compliance:
   Angesichts der steigenden Digitalisierung ergeben sich in der Nachlassplanung neue Herausforderungen, insbesondere für Besitzer von Kryptowährungen (Wysshaar, 2021). In der Schweiz wird der Nachlass mit dem schweizerischen Erbrecht im Zivilgesetzbuch (ZGB) Art. 457 bis 640 geregelt und verfolgt das Ziel, die Übertragung des Vermögens einer verstorbenen Person auf die Erben zu regeln (T. I. (AG, 2021). Im Erbrecht wird auch die Regelung bezüglich eines Testaments oder einem Erbvertrag festgehalten (T. I. (AG, 2021). Wenn eine Person stirbt, werden alle Rechte und Pflichten der verstorbenen Person auf die Erben übertragen. Das Erbe umfasst sowohl Vermögenswerte als auch Schulden, einschliesslich eventuell vorhandener Konten bei Banken in der Schweiz (T. I. (AG, 2021). Die Bestimmung der Erben und die Aufteilung des Erbes erfolgt nicht nach schweizerischem Recht, sondern richtet sich nach der Gesetzgebung am letzten Wohnsitz der verstorbenen

Person, ohne zusätzliche Regelungen (T. I. (AG, 2021). Schweizer Banken verlangen zu ihrem eigenen Schutz, vor der Auszahlung der Vermögenswerte an den Erben, eine schriftliche Zustimmung aller Erben (T. I. (AG, 2021). Das bedeutet, das von den Erben eine einvernehmliche Einigung über die Aufteilung des Vermögens stattfinden muss (T. I. (AG, 2021). Das Vermögen bleibt bei einer Uneinigkeit unberührt auf dem Schweizer Bankkonto der verstorbenen Personen (T. I. (AG, 2021). Hinterlegte Daueraufträge bei der Bank können nach dem Tod nur von den Erben unterbrochen oder gelöscht werden. Bis dahin werden die Aufträge weiterhin ausgeführt (T. I. (AG, 2021). Hingegen werden hinterlegte Vollmachten von Dritten in der Regel nach dem Tod automatisch ungültig (T. I. (AG, 2021).

Im Gegensatz zum herkömmlichen Vermögen besteht in Bezug zu Kryptowährungen eine Unsicherheit der Rechtslage (Wysshaar, 2021). Es wird darüber diskutiert, ob es sich bei Kryptowährungen um eine «Sache» im Sinne des Zivilgesetzbuches oder um Vermögenswerte handelt (Wysshaar, 2021). Aufgrund der fehlenden regulierenden Gesetzgebung für Kryptowährungen wird allgemein in der Lehre davon ausgegangen, dass eine weite Auslegung von Art. 560 ZGB vorliegt. Das bedeutet, dass Kryptowährungen als Teil des Nachlasses gelten und automatisch auf die Erben übergehen (Wysshaar, 2021). Eine abweichende Auffassung würde zur Folge haben, dass Kryptowährungen und somit auch das Vermögen im Todesfall unwiederbringlich verloren gehen könnten (Wysshaar, 2021). Es wird deshalb empfohlen eine Nachlassplanung durchzuführen (Wysshaar, 2021). Hierfür ist die Wahl zwischen einem Custodial Wallet und einem Non-Custodial Wallet entscheidend (Wysshaar, 2021). Bei einem Custodial Wallet wird das Vermögen von einem Dritten wie beispielsweise einer Krypto-Bank verwaltet, was bedeutet, dass nur dieser Zugang zum Wallet und somit zu den Kryptowährungen hat (Wysshaar, 2021). Dieses Verhältnis entspricht einem Auftrag, wodurch die Erben gemäss Erbrecht ein Recht über Auskunft und Informationen erhalten (Wysshaar, 2021). Hingen müssen die Erben bei einem Non-Custodial Wallet über den Zugriff auf die Kryptowährungen informiert werden (Wysshaar, 2021). Fehlt ihnen die Information, können sie nach dem Tod nicht auf das Wallet zugreifen und die vorhandenen Kryptowährungen würden verloren gehen (Wysshaar, 2021).

In der digitalen Identitätslandschaft und beim Schutz personenbezogener Daten haben mehrere Gesetze wie die Datenschutz-Grundverordnung (DSGVO) in der EU, das Datenverarbeitungsabkommen (DPA) im Vereinigten Königreich, das California Consumer Privacy Act (CCPA) und das brasilianische allgemeine Datenschutzgesetz (LGPD) zu einer Veränderung geführt (Warrington, 2022). Die neue Gesetz-

gebung stellt die Rechte des Einzelnen in den Vordergrund, indem sie das Recht einführt (Warrington, 2022):

- die Kontrolle über ihre Identität und personenbezogene Daten auszuüben (Warrington, 2022)
- ausdrücklich der Erhebung, Speicherung und Nutzung ihrer personenbezogenen Daten für einen bestimmten Zweck und eine bestimmte Dauer zuzustimmen (Warrington, 2022)
- vergessen zu werden, indem ihre personenbezogenen Daten aus den Datenbanken entfernt werden (Warrington, 2022)
- die Übertragbarkeit ihrer Daten auf Anfrage an eine autorisierte Person oder einen Dritten in einem geeigneten Format zu erhalten (Warrington, 2022)
- Informationen darüber zu erhalten, wie ihre Daten gesammelt werden, wie lange sie gespeichert werden und zu welchem Zweck sie verwendet werden (Warrington, 2022)

5. Nutzerakzeptanz:
   Die Akzeptanz von SSI-Systemen durch die Benutzer kann eine Herausforderung darstellen, insbesondere wenn es um die Komplexität und den Aufwand geht, die mit der Verwaltung und Überprüfung von Identitätsinformationen verbunden sind (Schardong & Custódio, 2022, S. 33-34). In einem SSI-System sind die Benutzer verantwortlich ihre Schlüssel an einem sicheren Ort zu bewahren und Identitäten sowie VC zu sichern. Zusätzlich sind die Benutzer für Erstellung und Einreichung von VC oder VP zuständig (Schardong & Custódio, 2022, S. 33-34). Eine benutzerfreundliche und verständliche Lösung könnte es den Benutzern erleichtern, ihre Identitätsinformationen zu verwalten und zu teilen, ohne eine Beschränkung der Sicherheit zu erlangen (Ehrlich et al., 2021, S. 251; van Dijk et al., 2021, S. 9). Die Systeme müssen dabei für den Nutzer transparent sein (van Dijk et al., 2021; Ehrlich et al., 2021, S. 251). Ausserdem sollte die Lösung eine einfache Nutzung für alle berechtigten Nutzer gewährleisten und komplexe Registrierungsprozesse vermeiden (Ehrlich et al., 2021, S. 251). Die eindeutige Identifikation der Nutzer muss gewährleistet werden können, um rechtssichere Transaktionen durchführen zu können (Ehrlich et al., 2021, S. 251). Es soll eine effiziente und kostengünstige Implementierung des IdM-Modells ermöglichen, um eine breitere Akzeptanz des Modells zu erreichen (Ehrlich et al., 2021, S. 251). Es könnte eine Herausforderung sein, die Benutzer davon zu überzeugen, dass sie die Verantwortung für ihre digitalen Identitäten übernehmen und sich an neue Technologien und Verfahren anpassen sollten (Schardong & Custódio, 2022, S. 33-34). Eine detaillierte Aufklärung über die Vorteile von SSI kann

die Akzeptanz eines SSI-Systems erhöhen (Ehrlich et al., 2021, S. 265-266). Deswegen müssen vorher die Schnittstellen von SSI-Systemen und der Umgang von Menschen mit einem SSI-System erforscht werden (Schardong & Custódio, 2022, S. 33-34). Interaktionen zwischen Nutzern und Anwendungen, vor allem zwischen Individuen, sind entscheidend (Schardong & Custódio, 2022, S. 33-34). Ohne eine solche Forschung ist es unwahrscheinlich, dass Nutzer bereit sind, ihre aktuellen föderierten oder benutzerzentrierten Identitäten aufzugebend (Schardong & Custódio, 2022, S. 33-34). In der Usability-Forschung von SSI wurde die Nachahmung physischer Geldbörsen, um den Nutzern vertraute Alltagsszenarien zu bieten, zu einem gängigen Trend (Schardong & Custódio, 2022, S. 33-34).

6. Bindungsproblem:
   Bei Projekten die sich mit SSI, NFT und digitalen Identitäten beschäftigen, stellt das Bindungsproblem eine zentrale Herausforderung dar (Millenaar, 2022). Die Herausforderung liegt darin herauszufinden, wie die Verbindung von einem NFT oder einem Objekt mit dem dazugehörigen Vermögenswert sichergestellt werden kann (Millenaar, 2022). Dasselbe Problem besteht schon seit der Existenz des Internets bei den Menschen (Millenaar, 2022). Für ihre digitale Identität müssen Menschen einen Nachweis liefern, dass sie über das Eigentum verfügen (Millenaar, 2022). Bisher basierten die meisten Lösungen auf Wissen (etwas, das die Person weiss) wie zum Beispiel ein Passwort (Millenaar, 2022). Mittlerweile basiert es auf dem Besitz (etwas, das die Person besitzt) wie zum Beispiel einen privaten Schlüssel oder eine Karte für den Zugang (Millenaar, 2022). Bei Berücksichtigung von Datenschutzgesetzen wie beispielsweise DSGV, muss vor der Bereitstellung eines Dienstes überprüft werden, wie viele Informationen benötigt werden, um ausreichend Vertrauen zur Identität aufbauen zu können (Millenaar, 2022). In Europa existieren bereits Vorschriften (eIDAS-Vorschriften) mit einer definierten Skala der Zuverlässigkeit (Levels of Assurance Scale) die verschiedene Sicherheitsniveaus für die Identifizierung ermöglichen (Millenaar, 2022). Im Anhang B ist der Level of Assurance Scale ersichtlich. Die jeweiligen Stufen (niedrig, substanziell oder hoch) der Skala definieren die Menge an Daten, die offengelegt werden müssen (Millenaar, 2022). Bei einem hohen Sicherheitsniveau müssen mehr Daten offengelegt werden, was zu einer Erhöhung des Vertrauens in die Identifizierung bringt (Millenaar, 2022). Durch diese Flexibilität können Diensteanbieter ihre Sicherheitsanforderungen an die spezifischen Bedürfnisse ihrer Anwendungen anzupassen und gleichzeitig die Gewährleistung der Datenintegrität und des Datenschutzes zuliefern (Millenaar, 2022). Für Menschen und Organisationen stellt das Bindungsproblem auf der Block-

chain mit SSI ein tieferes Problem dar. Mit dem SSI-Ökosystem können eine Vielzahl von Identifikationsnachweisen von niedrigem bis hohem Sicherheitsniveau von verschiedenen Ausstellern bereitgestellt und Tools zur Minimierung des Datenaustauschs verwenden werden (Millenaar, 2022). Ausserdem verfügen sie über einen privaten Schlüssel, die für die Verifizierung genutzt werden, kann. Bei einem IoT-Gerät ist es dasselbe (Millenaar, 2022). Die digitale Identität, die an ein IoT-Gerät gebunden ist, kann vom Gerät selbst verwaltet werden (Millenaar, 2022). Dafür wird die Kontrolle des privaten Schlüssels dem Gerät übergeben, das für die Authentifizierung benötigt wird (Millenaar, 2022). Digitale oder physische Vermögenswerte können ohne elektronische Schaltung keine Authentifizierung oder Beweise liefern (Millenaar, 2022). Ein NFT kann nicht nachweisen, dass es an einen Vermögenswert gebunden ist, und ein Vermögenswert kann nicht beweisen, dass er an das NFT gebunden ist (Millenaar, 2022). Für die Bindung des Vermögenswerts an eine Identität, gibt es aktuell keine technische oder rechtlich definierte Lösung (Millenaar, 2022). Eine weitere Herausforderung stellt die voranschreitende Entwicklung von Künstlicher Intelligenz (KI) dar, die sogar bei namhaften Experten, wie zum Beispiel Apple-Mitgründer Steve Wozniak, zu einer Besorgniserregung führt (Wagner, 2023). Denn durch die KI könnte ein Kontrollverlust entstehen (Wagner, 2023). Zum Beispiel hat im März 2023 ein Nutzer via Twitter mitgeteilt, dass ChatGPT - ein Chatbot von OpenAI, das auf einem Maschinenlernmodell basiert (Müller, 2023) – selbständig für ihn eine Marketing-Firma gegründet hat (Jahn, 2023). Des Weiteren wird seit Anfangs April 2023 beim Sender M Le Média aus Lausanne (Schweiz) die Wetterprognose von einem weiblichen Avatar namens «Jade» und nicht von einer realen Person übermittelt (Spörri, 2023). Erst nach der Veröffentlichung wurde den Zuschauern bewusst, dass es sich bei der Frau um einen Avatar handelte (Spörri, 2023). Ein Avatar ist eine Darstellung eines Benutzers innerhalb der 3D- und sozialen Umgebung des Metaverse (metamandrill, 2022). Der Avatar kann beliebig aussehen und verschiedene Unternehmen haben unterschiedliche Implementierungen von Avatar-Systemen, von einfachen bis hin zu fotorealistischen Avataren (metamandrill, 2022). Diese Avatare können als automatische Assistenten auf Internetseiten arbeiten oder als virtuelle Prominente in verschiedenen Medien (Beil & Rauscher, 2018, S. 350). Mittels KI und die Nutzung von Avatars könnten echt wirkende Videos erstellt werden, die für das Beweisen von unrealistischen Thesen verwendet werden, die an keine Identität gebunden sind (Wagner, 2023).

3 | Methodisches Vorgehen

Die vorliegende Forschung orientiert sich am Framework von Hevner (2007), das Methoden der gestaltungs- und verhaltensorientierten Forschung vereint (vgl. Abbild 3.1). Die Grundlage des Modells bildet der iterative Ansatz, mit dem ein IT-Artefakt erstellt, überprüft und verbessert wird. Diese Methodik besteht aus drei zyklischen Phasen: dem Relevance Cycle, dem Rigor Cycle und dem Design Cycle (Hevner, 2007).

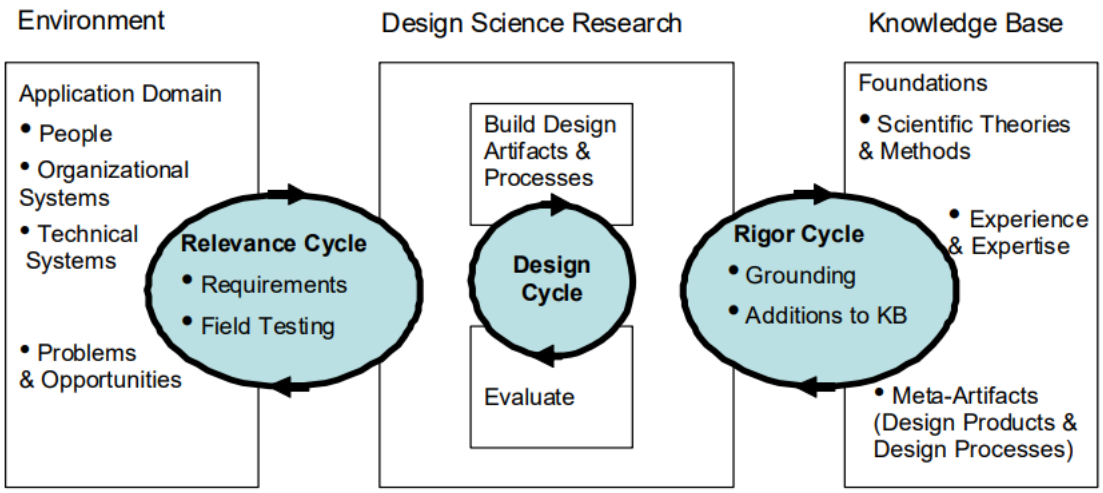

Abbildung 3.1 Design Science Cycle (Hevner, 2007, S. 2)

Im *Relevance Cycle* wird ein Verständnis für die Problemdomäne und die Bedürfnisse der Stakeholder entwickelt. In dieser Phase werden relevante Literatur, vorhandene Systeme und Stakeholderanforderungen anhand einer Literaturrecherche untersucht (Hevner, 2007, S. 2-3). Für die Recherche relevanter Literatur im Rahmen des theoretischen Teils dieser Arbeit (Kapitel 2) wurde die Methode von Booth's Standards for Reporting Literature Searches (STARLITE) Booth (2006) angewendet. Für eine qualitativ hochwertige Literaturrecherche tragen gemäss STARLITE acht Aspekte bei (Booth, 2006, S. 424). Die acht Aspekte sind im Anhang C dokumentiert. Für die Literatursuche werden die verfügbaren Medien der Zürcher Fachhochschule für Angewandte Wissenschaften verwendet. Bei der Recherche wurde der Hauptfokus auf die Aktualität der Literatur gelegt. Aufgrund

der technologischen Entwicklungen im untersuchten Bereich wurden hauptsächlich Publikationen aus den letzten drei Jahren berücksichtigt. Dies ermöglichte es, die neuesten Erkenntnisse und Fortschritte auf dem Gebiet der Technologie und ihrer Anwendungen in die Forschung einfliessen zu lassen. Durch diese Herangehensweise wurde sichergestellt, dass die Ergebnisse und Schlussfolgerungen auf einer soliden Grundlage aktueller Forschungsergebnisse basieren.

Im *Rigor Cycle* werden Design Science Artefakte entwickelt und rigoros evaluiert. Die Design Science Artefakte können aus neuen oder überarbeiteten Konstrukten, Modellen, Methoden oder Instanzen bestehen. In dieser Phase wird das Artefakt auf seine Nützlichkeit, Qualität und Wirksamkeit hin untersucht, um sicherzustellen, dass es die Anforderungen der Stakeholder erfüllt (Hevner, 2007, S. 3-4).

Im *Design Cycle* wird das Design Science Artefakt in einer realen Umgebung implementiert und evaluiert. In dieser Phase wird das Artefakt anhand eines realen Anwendungsfalles getestet. Die Ergebnisse dieser Tests werden genutzt, um das Design Artefakt zu verbessern und zu optimieren (Hevner, 2007, S. 4-5).

Das *Design Theorizing Framework* von Lee et al. (2011) wird verwendet, um das Problem für die Lösungssuche zu abstrahieren. In dieser Methodik werden die im Abbild 3.2 ersichtlichen vier zentrale Schritte beschrieben: Abstraction, Solution search, De-Abstraction und Registration (Lee et al., 2011, S. 7-9).

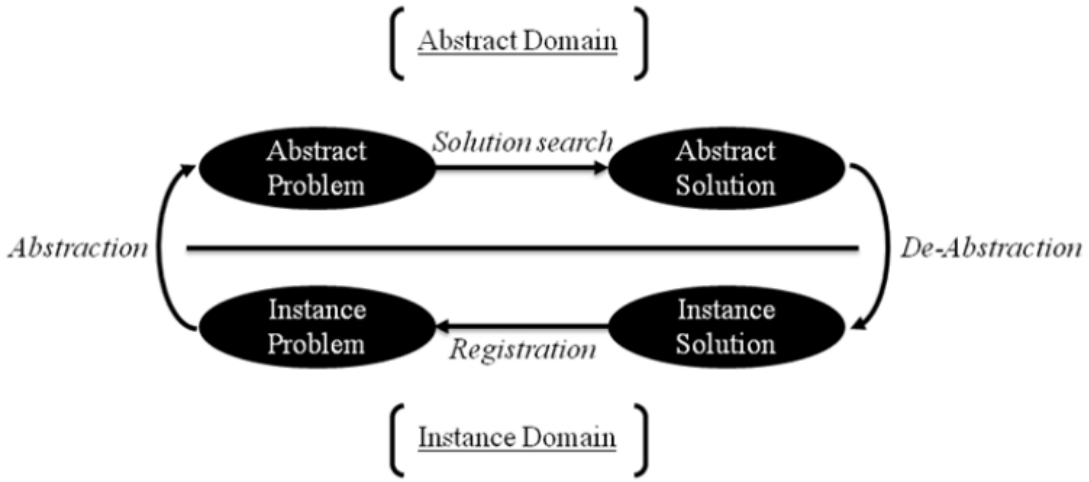

Abbildung 3.2 Design Science Cycle (Lee et al., 2011, S. 6)

- *Abstraction:* Im ersten Schritt der Abstraktion wird das zu untersuchende Problem in eine abstrakte Form gebracht. Dieser Prozess zielt darauf ab, das Problem auf das Wesentliche zu reduzieren, indem es von seiner konkreten, spezifischen Form abstrahiert wird.
- *Solution search:* In diesem Schritt werden abstrakte Lösungen für das abstrakte Problem gesucht. Es werden verschiedene abstrakte Lösungen generiert, die in einem späteren Schritt auf ihre Anwendbarkeit geprüft werden.
- *De-Abstraction:*Im dritten Schritt der De-Abstraktion werden die abstrakten Lösungen in eine konkrete Form gebracht, indem sie auf das konkrete Problem angewendet werden. Dabei werden die Lösungen an die spezifischen Gegebenheiten des Problems angepasst und konkretisiert.
- *Registration:* Der letzte Schritt besteht in der Registrierung der Lösung. Hier wird die gefundene Lösung dokumentiert und für die weitere Verwendung festgehalten.

Diese Schritte bilden eine iterative Methodik, die es erlaubt, immer wieder zwischen den abstrakten und konkreten Ebenen zu wechseln, um ein besseres Verständnis für das Problem und dessen Lösung zu erlangen.

Die beiden Ansätze lassen sich gut kombinieren, um eine umfassende und fundierte Forschung durchzuführen. Während das Design Science Research von Hevner den Prozess der Entwicklung von Design-Artefakten und deren Evaluierung unterstützt, hilft das Design Theorizing Framework von Lee et al. dabei, die theoretischen Grundlagen zu entwickeln, die den Design-Artefakten zugrunde liegen. Durch die Kombination dieser beiden Ansätze wird eine umfassende, praxisnahe und wissenschaftlich fundierte Forschung ermöglicht, die zur Lösung des Problems des Identitätsmanagements mittels Blockchain-Technologie und SSI beitragen kann.

4 Anforderungen an das IdM-Modell

Im vorliegenden Kapitel werden die im Abschnitt 2.4.5 identifizierten Herausforderungen abstrahiert und in einem ersten *Design Cycle* zusammengeführt, mit dem Ziel die Anforderungen an das zu entwickelnde IdM-Modell zu definieren. Die Anforderungen werden stichwortartig aufgeführt. Dabei wird nur die im Abschnitt 2.4.5 verwendete Literatur genutzt. Um eine bessere Übersicht und Vergleichbarkeit der Anforderungen zu gewährleisten, werden diese in der nachfolgenden Tabelle 4.1 zusammengefasst. Die daraus resultierenden Anforderungen an einem dezentralen IdM-Modell werden als Leitfaden für die Entwicklung einer solchen Lösung im Kapitel 5 genutzt.

Tabelle 4.1 Anforderungen an einem dezentralem Identitätsmanagement-Modell

Herausforderungen	**Anforderungen**
Organisatorisch	Dezentralisierung • Keine zentralisierten Institutionen • Eigenverantwortung der Identitätsinformationen Standardisierung • Datenmanagement und Wallet Interoperabilität • Kompatibel mit verschiedenen Systemen und Diensten • Einfache Übertragung Privatsphäre und Kontrolle • Zugang zu eigenen Daten • Verwendung der Daten nur mit Zustimmung • Sammlung und Übertragung von Identitätsinformationen auf ein Minimum begrenzen
Technische Umsetzung	Implementierung • Interoperabilität • Sicherstellung des Zugriffs • Datenverfügbarkeit
Sicherheit	Sicherheit • Sichere Speicherung und Übertragung • Schutz vor technischen Ausfällen und Cyber-Angriffen
Compliance	Datenschutz • Gewährleistung des Datenschutzes Vererbung und Stellvertretung • Vollmachtsregelung • Möglichkeit für Vererbung des private key
Nutzerakzeptanz	Benutzerfreundlichkeit • Einfache und verständliche Nutzung • Transparenz • Aufklärung über die Verantwortung
Bindungsproblem	Inhaber und Verantwortung digitaler Identitäten • Verbindung von Vermögen und Identität • Verantwortung von KI und Avatare

5 | Modellentwicklung

In diesem Kapitel wird ein Konzept für ein dezentrales IdM-Modell für eine public permissionless Blockchain entwickelt. Hierbei werden die im Vorfeld im Kapitel 4 ermittelten Anforderungen berücksichtigt. Ziel ist es, ein Modell zu gestalten, das eine sichere und transparente Verwaltung von Identitätsdaten ermöglicht und zugleich die Kontrolle über persönliche Informationen den Nutzenden überlässt.

5.1 Gestaltung des Identitätsmanagement-Modell

Das Modell (siehe Abbild 5.1) besteht aus verschiedenen miteinander interagierenden Elementen. Im Zentrum des Modells steht das Subjekt, das immer eine reale Person darstellt. Das Subjekt erstellt auf der Blockchain eine Identität nach dem SSI-Prinzip, die es befähigt, ein oder mehrere Objekte zu besitzen. Ein Objekt kann zum Beispiel ein Unternehmen oder eine Organisation sein, die eine eigene Identität in Form einer Objekt-ID erhält. Diese Identität ist jedoch nur dann gültig, wenn sie einem Subjekt zugeordnet ist. Dadurch wird sichergestellt, dass hinter jeder Identität eine reale Person steht, welche die Verantwortung für diese Identität übernimmt. Das Objekt kann wiederum Besitzer von weiteren Identitäten sein, wie zum Beispiel von einem Avatar oder einem IoT-Gerät. Diese Identitäten werden als Subobjekt-ID bezeichnet. Ein Subobjekt kann ebenfalls Besitzer eines Objekts sein. Voraussetzung hierfür ist jedoch, dass die Identität des Subobjekts mindestens einem Objekt oder direkt einem Subjekt zugewiesen ist. Zusätzlich können Subjekte auch mit Objekten verbunden sein, ohne jedoch die Verantwortung für das betreffende Objekt zu tragen. In diesem Fall sind dem Subjekt bestimmte Rollen und Regeln zugewiesen, die es ihm ermöglichen, das Objekt für bestimmte Zwecke zu nutzen.

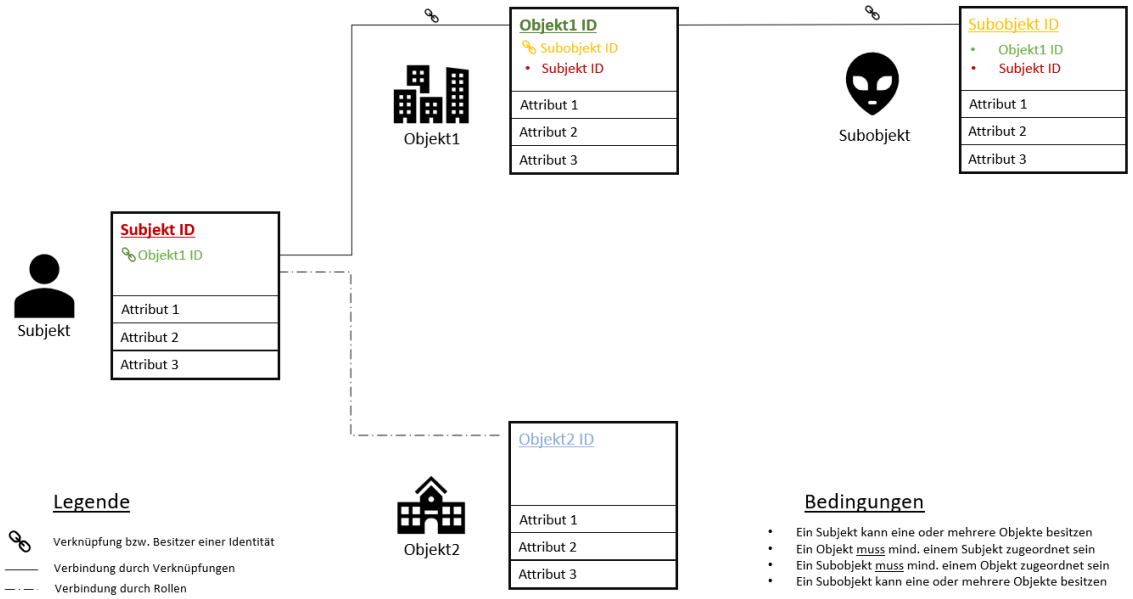

Abbildung 5.1 Dezentrales IdM-Modell für die Blockchain

Die digitalen Identitätsträger und deren ID-Zuordnung sind in der nachstehenden Tabelle 5.1 aufgeführt.

Tabelle 5.1 ID-Zuordnung an Identitätsträger

Identitätsträger	**ID-Zuordnung**
Natürliche Personen	Subjekt
IT-System	Objekt
IT-Applikation	Objekt
Rollen und Funktionen im Unternehmen	Objekt
Gegenstände	Subobjekt
IoT-Geräte	Subobjekt
Juristische Personen und Organisationseinheiten	Objekt
Avatare	Subobjekt

Zusammenfassend gelten für das Modell folgende Bedingungen:

- Ein Subjekt kann eine oder mehrere Objekte besitzen
- Ein Objekt **muss** mindestens einem Subjekt zugeordnet sein
- Ein Subobjekt **muss** mindestens einem Objekt zugeordnet sein
- Ein Subobjekt kann eine oder mehrere Objekte besitzen

Nebst der Struktur des Modells gehört auch die Verwendung eines Wallets zu einem wichtigen Bestandteil der Identitätsverwaltung. Die gewählte Struktur wird im Account-Modell im nächsten Abschnitt genauer erläutert.

5.2 Account-Modell

Für dieses Modell wurde ein Hybrid Wallet-System entwickelt, das die Vorteile einer Hardware Wallet und eines Mobile Wallets kombiniert. Das Ziel ist, eine hohe Sicherheit zu gewährleisten und gleichzeitig eine benutzerfreundliche Anwendung zu bieten. Das Hybrid-Wallet-System besteht aus einer Hardware Wallet, die für die Aufbewahrung des Schlüssels zuständig ist, und einem Mobile Wallet, das für die Identitätsverwaltung verwendet wird. Durch die Verwendung einer Hardware Wallet kann der Schlüssel sicher von einem Mobilgerät getrennt aufbewahrt werden. Das Mobile Wallet bietet hingegen eine benutzerfreundliche Oberfläche zur Verwaltung der Identitäten. Die Wallets sind nur kombiniert verwendbar und das Mobile Wallet muss eine DApp sein. Für Transaktionen werden Offline-Signierung angewendet. Bei der Offline-Signierung wird die Signierung von Transaktionen, die den private key erfordern, auf dem Hardware Wallet selbst durchgeführt, ohne dass der private key das Hardware Wallet verlässt. Dabei werden folgende Schritte durchgeführt:

1. Transaktionsvorbereitung: Das Wallet App auf dem mobilen Gerät bereitet die Transaktion vor, indem es alle relevanten Transaktionsdetails wie Empfängeradresse, Betrag und Transaktionsgebühr sammelt. Diese Informationen werden dann in ein signierbares Format gebracht.
2. Signierungsauftrag: Das Wallet App sendet den Signierungsauftrag an das Hardware Wallet. Dabei wird die Transaktion nicht signiert, sondern nur eine Anfrage zur Signierung an das Hardware Wallet gesendet.

3. Signierung auf dem Hardware Wallet: Das Hardware Wallet empfängt den Signierungsauftrag und prüft die Transaktionsdetails. Wenn alles korrekt ist und der Nutzer die Transaktion bestätigt, signiert das Hardware Wallet die Transaktion offline mit dem private key, der sicher auf dem Gerät gespeichert ist.

4. Übermittlung der signierten Transaktion: Nachdem die Transaktion offline signiert wurde, sendet das Hardware Wallet die signierte Transaktion zurück an das Wallet App.

5. Übertragung der signierten Transaktion an das Netzwerk: Das Wallet App übernimmt die Aufgabe, die signierte Transaktion an das Blockchain-Netzwerk zu übertragen. Die signierte Transaktion enthält alle notwendigen Informationen und Signaturen, um von den Knoten im Netzwerk verifiziert und bestätigt zu werden.

Durch die Offline-Signierung bleibt der private key des Hardware Wallets geschützt und wird niemals an das Wallet App oder andere potenziell unsichere Umgebungen übertragen. Das Wallet App fungiert lediglich als Vermittler zwischen dem Nutzer, der die Transaktion initiieren möchte, und dem Hardware Wallet, das die Transaktion sicher signiert. Dies bietet ein hohes Mass an Sicherheit und Schutz vor möglichen Angriffen auf den private key. Das Wallet App wurde so einfach wie möglich konzipiert, um eine intuitive Bedienung zu gewährleisten. Im Hauptmenü des Wallet-Apps erhalten Benutzende eine Übersicht zu ihren Identitäten, sowie eine Übersicht über die VC, VP und Objekte die sie besitzen (siehe Abbild 5.2). Die Menüauswahl ist im Abbild 5.3 ersichtlich.

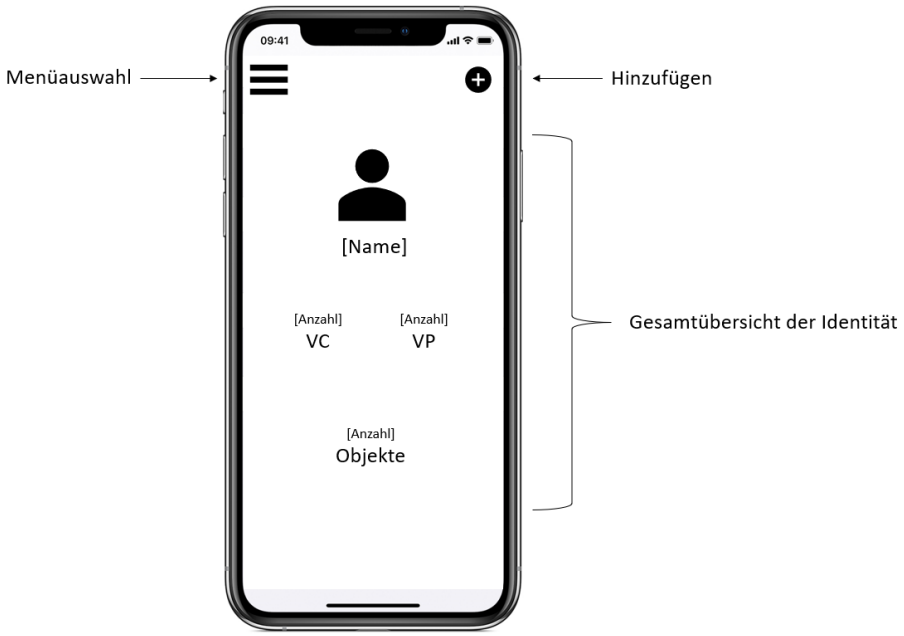

Abbildung 5.2 Übersicht einer Wallet-App

Abbildung 5.3 Einstellungen einer Wallet App

Im Abbild 5.4 ist der Prozess für den Erhalt eines VC dargestellt. Sobald der Benutzer eine neue VC erhält, erscheint eine Anfrage, ob das VC jetzt oder später angesehen werden soll. Nach der Einsicht hat er die Möglichkeit die Anfrage zu akzeptieren oder abzulehnen. Bevor er sich entscheidet, kann er die Details der VC einsehen. Mit dem Wallet App lassen sich verschiedene Bedürfnisse vereinfacht darstellen. So kann der User über das Feld „hinzufügen“ zum Beispiel eine neue VP erstellen, in dem er die einzelnen Informationen selbständig auswählt, die er benötigt.

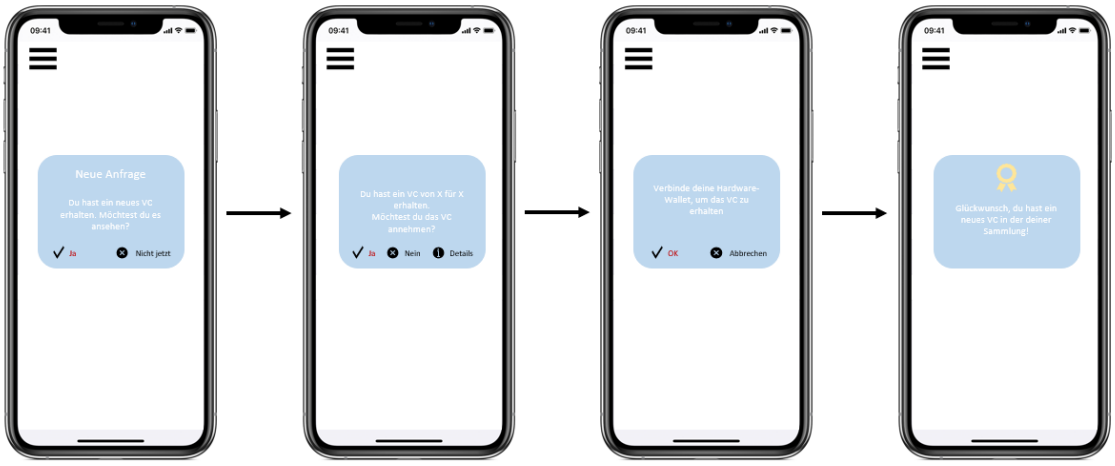

Abbildung 5.4 Der Prozess einer Wallet-App für den Erhalt von VC

Gemäss dem entwickelten IdM-Modell werden im Falle des Todes einer Person bestimmte Massnahmen ergriffen, um den Zugang zu den digitalen Vermögenswerten und Identitäten zu ermöglichen und gleichzeitig die Sicherheit zu gewährleisten. Der folgende Ablauf beschreibt den Prozess der Aktivierung der Todesmeldung und die Freigabe des Wallets an die rechtmässigen Erben:

1. Hinterlegung von drei Personen: Jedes Subjekt hat die Möglichkeit, drei Personen zu hinterlegen, die im Falle seines Todes zum Einsatz kommen sollen. Diese Personen werden mit ihrem Vor- und Nachnamen sowie ihrer E-Mail-Adresse im Wallet App hinterlegt.

2. Übernahme der Hardware Wallet: Im Falle des Todes wird die Hardware Wallet des Verstorbenen den Erben übergeben. Die Hardware Wallet enthält die private keys und ist durch eine sichere Verschlüsselung geschützt.

3. Aktivierung der Todesmeldung: Die Erben können die Todesmeldung aktivieren, indem sie eine vorher festgelegte Tastenkombination verwenden, die im Testament des Verstorbenen aufgeführt ist. Durch die Eingabe dieser Tastenkombination wird die Todesmeldung auf der Wallet App ausgelöst.

4. Benachrichtigung der hinterlegten Personen: Sobald die Todesmeldung aktiviert ist, erhalten alle drei hinterlegten Personen eine E-Mail-Benachrichtigung. In der E-Mail werden sie über den Tod des Subjekts informiert und aufgefordert, auf die E-Mail zu antworten, um ihre Zustimmung zur Freischaltung des Wallets zu bestätigen.

5. Offline-Signierung der Zustimmung: Nachdem die hinterlegten Personen ihre Zustimmung per E-Mail gegeben haben, werden die Zustimmungsnachrichten in das Wallet App übertragen. An diesem Punkt wird die Offline-Signierung angewendet. Das Wallet App erstellt eine Transaktion, die die Zustimmungsnachrichten enthält, und sendet den Signierungsauftrag an das Hardware Wallet.

6. Signierung auf dem Hardware Wallet: Das Hardware Wallet empfängt den Signierungsauftrag und signiert die Transaktion offline mit dem private key, der sicher auf dem Gerät gespeichert ist. Die signierte Transaktion wird dann an das Wallet App zurückgesendet.

7. Bestätigung der Freischaltung: Sobald das Wallet App die signierte Transaktion erhalten hat, kann es die Freischaltung des Wallets bestätigen. Es wird eine Meldung auf dem Wallet App angezeigt, die besagt, dass das Wallet innerhalb von 48 Stunden freigeschaltet wird.

8. Freischaltung des Wallets: Falls keine Abbrüche innerhalb der vorgegebenen Frist von 48 Stunden erfolgen, wird das Wallet freigeschaltet. Die rechtmäßigen Erben erhalten Zugriff auf die digitalen Vermögenswerte und können diese verwalten.

Dieser Ablauf stellt sicher, dass im Todesfall einer Person ein geordneter Prozess für die Übertragung der digitalen Vermögenswerte stattfindet. Durch die Inkludierung der hinterlegten Personen und die Bestätigung ihrer Zustimmung wird sichergestellt, dass die Freischaltung des Wallets nur durch die Zustimmung erfolgt. Dies gewährleistet sowohl den Schutz der Identität als auch die Verhinderung unbefugter Zugriffe auf die digitalen Vermögenswerte.

6 | Resultate

Im vorliegenden Kapitel werden die Resultate aus der Evaluation des IdM-Models präsentiert, sowie die Forschungsfrage „*Was sind die Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain?*“ beantwortet. Weiter werden die zur Weiterentwicklung und Umsetzung des IdM-Modells als relevanten erachteten Erkenntnisse aus Theorie und Empirie veranschaulicht.

6.1 Evaluation des Modells

In diesem Abschnitt wird das in Kapitel 5 vorgestellte IdM-Modell zur Verwaltung von digitalen Identitäten evaluiert. Um die Anwendungsmöglichkeiten des entwickelten IdM-Modells zu überprüfen, wird dieses im nächsten Abschnitt 6.1.1 auf theoretischer Ebene anhand der formulierten Anforderungen aus dem Kapitel 4 analysiert. Anschliessend wird im Abschnitt 6.1.2 das IdM-Modell auf praktischer Ebene anhand von zwei realen Anwendungsfällen getestet. Die Resultate liefern Einblicke in die Schwächen und Potenziale des Modells sowie in mögliche Herausforderungen. Die Evaluation soll als Grundlage für weitere Entwicklungen und Anpassungen dienen können.

6.1.1 Theoretische Evaluierung anhand der Anforderungen

Im Rahmen der theoretischen Evaluierung wird die Anforderungstabelle um eine zusätzliche Spalte „Beurteilung des Modells“ erweitert, um die Beurteilung des Modells detailliert darzustellen. Diese Bewertung erfolgt in der nächsten Tabelle 6.1 durch farbliche Markierungen, wobei erfüllte Anforderungen in grün, nicht beurteilbare Anforderungen in gelb und nicht erfüllte Anforderungen in rot gekennzeichnet werden. Durch diese visuelle Darstellung wird eine übersichtliche Einschätzung des Modells in Bezug auf die gestellten Anforderungen ermöglicht.

Tabelle 6.1 Theoretische Beurteilung des Modells

Anforderungen	**Beurteilung des Modells**
Dezentralisierung • Keine zentralisierten Institutionen • Eigenverantwortung der Identitätsinformationen	Dezentralisierung: Erfüllt Da das Modell auf der Blockchain basiert, ist die Dezentralisierung gegeben
Standardisierung • Datenmanagement und Wallet	Standardisierung: Erfüllt Das Modell bietet eine Möglichkeit zur Standardisierung an
Interoperabilität • Kompatibel mit verschiedenen Systemen und Diensten • Einfache Übertragung	Interoperabilität: Nicht beurteilbar Die Interoperabilität muss technisch gelöst werden
Privatsphäre und Kontrolle • Zugang zu eigenen Daten • Verwendung der Daten nur mit Zustimmung • Sammlung und Übertragung von Identitätsinformationen auf ein Minimum begrenzen	Privatsphäre und Kontrolle: Erfüllt Die Privatsphäre und Kontrolle der Daten sind gegeben. Der Nutzer verfügt über die eigenen Daten und kann selbst entscheiden, mit wem sie geteilt wird. Ohne Zustimmung werden keine Daten geteilt
Implementierung • Integration in bestehenden IT-Systemen • Sicherstellung des Zugriffs • Datenverfügbarkeit	Implementierung: Nicht beurteilbar Nicht beurteilbar, muss technisch gelöst werden
Sicherheit • Sichere Speicherung und Übertragung • Schutz vor techn. Ausfällen und Cyber-Angriffen	Sicherheit: Erfüllt Blockchain bietet aufgrund ihrer Dezentralität und verteilen Architektur eine hohe Sicherheit vor Ausfällen und Anonymität
Datenschutz • Gewährleistung des Datenschutzes	Datenschutz: Erfüllt Da das Modell auf der Blockchain basiert, ist die Einhaltung des Datenschutzes gegeben
Vererbung und Stellvertretung • Vollmachtregelung • Möglichkeit für Vererbung des private key	Vererbung und Stellvertretung: Erfüllt Vererbung und Stellvertretung sind mit der Hinterlegung im App und der Hybrid -Lösung möglich
Benutzerfreundlichkeit • Einfach und verständliche Nutzung • Transparenz • Aufklärung über die Verantwortung	Benutzerfreundlichkeit: Erfüllt Das Wallet App bietet eine übersichtliche und benutzerfreundliche Übersicht. Der Nutzer wird über die geteilten Identitäten informiert und kann selbst darüber bestimmen.
Inhaber und Verantwortung digitaler Identitäten • Verbindung von Vermögen und Identität • Verantwortung von KI und Avatare	Inhaber und Verantwortung digitaler Identitäten: erfüllt Identitäten von Gegenständen können mit einem Chip verbunden werden. Die Verantwortung von KI und Avatare könnten getragen werden, da diese als Subobjekte definiert sind und nicht ohne ein Subjekt agieren können.

Die Tabelle zeigt, dass viele der gestellten Anforderungen erfüllt werden. Das Modell bietet eine solide Basis für die Entwicklung und Implementierung eines effektiven und vertrauenswürdigen Systems zur Verwaltung digitaler Identitäten. Die noch bestehenden Herausforderungen in Bezug auf Implementierung und Interoperabilität müssen durch weitere technische Entwicklungen und Anpassungen angegangen werden, um das volle Potenzial des Modells auszuschöpfen.

6.1.2 Praktische Evaluierung anhand von Anwendungsfällen

Die praktische Evaluierung der Modell-Funktionalität wird mit Hilfe von zwei Anwendungsfällen in diesem Abschnitt durchgeführt. Bei der Definition und Wahl der Anwendungsfälle wird darauf geachtet, dass eine möglichst umfassende Bewertung des Modells ermöglicht wird. Für beide Anwendungsfälle wird jeweils ein Szenario inklusive dessen Anforderungen an das Modell genutzt. Dabei sollen verschiedene Fälle aufgezeigt werden, um eine möglichst umfassende Bewertung des IdM-Modells zu ermöglichen. Zu den beiden Anwendungsfällen wird je ein Szenario aufgeführt mit dessen Anforderungen an das Modell.

Im ersten Anwendungsfall wird die Vererbungsfunktion des Modells überprüft. Hierbei soll getestet werden, ob das Modell in der Lage ist, Erben von vertrauenswürdigen Identitäten und VPs zu definieren und diese im Todesfall des ursprünglichen Besitzers weiterzugeben. In der nächsten Tabelle 6.2 ist die Beurteilung des ersten Anwendungsfall ersichtlich.

Tabelle 6.2 Praktische Beurteilung des Modells: 1. Anwendungsfall

Szenario 1	
Angenommen, eine Person namens Anna ist eine aktive Nutzerin einer dezentralen Plattform, die auf Blockchain-Technologie basiert. Anna hat digitale Vermögenswerte, persönliche Daten und Zugriffsrechte auf verschiedene Dienste innerhalb der Plattform. Um sicherzustellen, dass ihre Identität und ihre digitalen Vermögenswerte nach ihrem Tod richtig verwaltet werden, wird das entwickelte IdM-Modell eingesetzt.	
Anforderungen an das Szenario	**Beurteilung des Modells**
1. Nach dem Tod von Anna soll das Modell automatisch benachrichtigt werden und den Tod verifizieren.	Nicht erfüllt Das Modell wird nicht automatisch benachrichtigt. Der Tod von Anna wird erst mitgeteilt, wenn die Erben von Anna ihren Hardware-Wallet erhalten und mit einer Tastenkombination die Todesmeldung aktivieren.
2. Das Modell überprüft, ob Anna eine Regelung für die Vererbung ihrer digitalen Vermögenswerte und Daten festgelegt hat.	Erfüllt Mit dem Account-Modell wird überprüft, ob eine Regelung hinterlegt ist.
3. Wenn eine Regelung vorhanden ist, werden die entsprechenden Vermögenswerte an die benannten Erben übertragen.	Erfüllt Mit der Regelung der Vererbung bietet das Modell die Möglichkeit, die Zugriffe respektive den private key an den Erben zu übertrage.
4. Falls keine spezifische Regelung vorhanden ist, kann das Modell auf vordefinierte Standards zurückgreifen, wie beispielsweise die Übertragung an die nächsten Angehörigen oder eine andere Vertrauensperson.	Nicht erfüllt Das Modell ist so konzeptioniert, dass das schweizerische Erbrecht gilt. Jedoch lässt sich dies nicht umsetzen, wenn keine Personen für die E-Mail-Benachrichtigung hinterlegt werden oder wenn diese nicht auf das Mail antworten (es könnte sein, dass die hinterlegten Personen vorher sterben). Hierfür wurde keine Regelung definiert
5. Das Modell sorgt für die Löschung oder Anonymisierung der persönlichen Daten von Anna, falls gewünscht oder gesetzlich erforderlich.	Teilweise erfüllt Die Blockchain bietet Anonymität an. Jedoch können auf der Blockchain aufgrund ihrer Eigenschaft «Unveränderlichkeit» keine erfolgreich durchgeführten Transaktionen gelöscht werden.
6. Die dezentrale Plattform und andere relevante Dienste werden über den Tod von Anna informiert und ihre Zugriffsrechte werden entsprechend angepasst oder deaktiviert.	Teilweise erfüllt Die Blockchain bietet die notwendige Transparenz an. Alle Netzwerk-Teilnehmer werden bei einer Aktivierung der Todesmeldung informiert. Für eine automatische Anpassung oder Deaktivierung der Zugriffsrechte ist jedoch keine Regelung hinterlegt.

Im zweiten Use Case wird die Subjekt-ID-Verknüpfung mit einem Avatar getestet. Hierbei soll untersucht werden, ob das Modell in der Lage ist, die Subjekt-ID-Verknüpfung mit einem Avatar in einer eindeutigen und leicht verständlichen Weise darzustellen. In der nächsten Tabelle 6.3 ist die Beurteilung des zweiten Anwendungsfalls ersichtlich.

Tabelle 6.3 Praktische Beurteilung des Modells: 2. Anwendungsfall

Szenario 2	
Angenommen, wir haben eine dezentrale Plattform, auf der natürliche Personen ihre Subjekt-IDs erstellen und Avatare als Subobjekt-IDs erstellen können. Die Plattform ermöglicht die Interaktion zwischen den Subjekt-IDs der Personen und den Subobjekt-IDs der Avatare.	
Anforderungen an das Szenario	**Beurteilung des Modells**
1. Erstellung von Subjekt-IDs: Das Modell ermöglicht natürlichen Personen die Erstellung ihrer eigenen Subjekt-IDs auf der Blockchain.	Erfüllt Natürliche Personen können eine Identität auf der Blockchain erstellen.
2. Erstellung von Subobjekt-IDs (Avataren): Das Modell ermöglicht die Erstellung von Subobjekt-IDs in Form von Avataren auf der Blockchain.	Erfüllt Das Modell ermöglicht die Erstellung von Identitäten, auch für Avatare.
3. Verknüpfung von Subjekt-IDs und Subobjekt-IDs: Das Modell gewährleistet, dass eine transparente und unveränderliche Verknüpfung zwischen den Subjekt-IDs der Personen und den Subobjekt-IDs der Avatare auf der Blockchain hergestellt wird. Dadurch wird sichergestellt, dass nur verifizierte und berechtigte Avatare mit den entsprechenden Subjekt-IDs interagieren können.	Teilweise erfüllt Das Modell gewährleistet eine transparente Verknüpfung zwischen einem Subjekt-ID und einem Subobjekt-ID. Eine Interaktion von einem Subobjekt-ID ist nur zulässig, wenn eine Verknüpfung zu einem Subjekt-ID vorhanden ist. Diese Unterscheidung ist nur möglich, wenn eine Subobjekt-ID von einem Subjekt oder Objekt erstellt wird. Jedoch könnte es sein, dass ein Avatar separat eine digitale Identität als Subjekt erstellt.
4. Nachvollziehbarkeit der Verknüpfung: Das Modell ermöglicht es allen Benutzern, die Verknüpfung zwischen Subjekt-IDs und Subobjekt-IDs auf der Blockchain nachzuvollziehen. Jederzeit kann überprüft werden, welche Avatare mit welchen Subjekt-IDs verbunden sind, und es werden keinerlei unautorisierte Änderungen an den Verknüpfungen zugelassen.	Erfüllt Aufgrund der Eigenschaft «Transparenz» der Blockchain, können die Verknüpfungen jederzeit nachvollzogen werden. Die Verknüpfungen können nur vom jeweiligen Besitzer der Identität verändert werden.
5. Konsistente Darstellung auf der Plattform: Das Modell stellt sicher, dass die Subjekt-ID-Verknüpfung mit Avataren in einer klaren und einheitlichen Weise auf der Plattform dargestellt wird. Dies kann beispielsweise durch visuelle Symbole oder Tags erfolgen, die den Nutzern ermöglichen, die Identitäten der Avatare und deren Verbindung zu den Subjekt-IDs leicht zu erkennen.	Nicht beurteilbar Diese Anforderung müsste bei der technischen Umsetzung berücksichtigt werden.

Nach der Evaluation von den beiden Anwendungsfällen lässt sich feststellen, dass das entwickelte IdM-Modell einige Anforderungen zwar vollständig erfüllt, während andere nicht erfüllt werden und eine weitere Anforderung nicht beurteilbar ist. Es wird deutlich, dass weiterhin Optimierungsbedarf besteht, um das IdM-Modell in allen Bereichen den gestellten Anforderungen gerecht zu werden. Die erzielten Ergebnisse bieten jedoch wertvolle Einblicke und bilden eine Grundlage für zukünftige Weiterentwicklungen und Verbesserungen des Identitätsmanagementsystems.

6.2 Beantwortung der Forschungsfrage

In diesem Kapitel wird die Forschungsfrage *Was sind die Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain?* beantwortet.

Die Anforderungen an ein dezentrales Identitätsmanagement-Modell in einer public permissionless Blockchain umfassen die Gewährleistung von Dezentralisierung, Eigenverantwortung der Identitätsinformationen, Standardisierung, Interoperabilität, Privatsphäre und Kontrolle, Implementierung, Sicherheit, Datenschutz, Benutzerfreundlichkeit sowie die Verbindung von analogen und digitalen Gegenständen zu einer Identität.

7 | Fazit

Die vorliegende Masterarbeit verdeutlicht die Notwendigkeit eines IdM-Modell für dezentrale Plattformen, die die Verwaltung und Nutzung der digitalen Identitäten regelt und den Bedürfnisse der Nutzenden gerecht wird. In einer zunehmend vernetzten und digitalisierten Welt ist eine zuverlässige und vertrauenswürdige Verwaltung von Identitäten von entscheidender Bedeutung. Diese Masterarbeit liefert einen wichtigen Beitrag zur Erforschung der Anforderungen an ein dezentrales IdM-Modell und für die Entwicklung eines entsprechenden Modells. Allerdings ist anzumerken, dass das IdM-Modell seine Grenzen hat und nicht alle Aspekte der Anforderungen vollständig abdeckt. Während einige Anforderungen nicht getestet werden konnten, wurden andere teilweise oder gar nicht erfüllt. Insbesondere in Bezug auf die technische Umsetzung, besteht weiterer Forschungsbedarf. Eine mögliche Richtung für zukünftige Arbeiten besteht darin, das IdM-Modell umfangreicher zu testen. Durch umfangreichere Testläufe können potenzielle Schwachstellen und Verbesserungsmöglichkeiten erkannt werden. Dabei ist es wichtig, dass die Tests nicht nur auf technischer Ebene stattfinden sollen, sondern auch unter Einbeziehung der Benutzerperspektiven. Das Feedback und die Bewertungen von Benutzern und Experten können wertvolle Einblicke liefern und zur Weiterentwicklung des IdM-Modells beitragen. Ausserdem sollte erforscht werden, ob allenfalls gewisse Gesetze, wie zum Beispiel die DSGVO, revidiert und sich dem Modell und den neuen technologischen Möglichkeiten anpassen müssen. Des Weiteren ist es notwendig, das IdM-Modell hinsichtlich Interessenskonflikten zwischen den Akteuren kritisch zu hinterfragen.

Literaturverzeichnis

Erstellt mit BibLaTeX (v3.16) im german APA (v9.14) Stil.

Adam, K., et al. (2020). Blockchain-Technologie für Unternehmensprozesse. *Sinnvolle Anwendungen der neuen Technologie in Unternehmen. Berlin*, (Siehe S. 20)

AG, D. L. (2023). *Decentralized Identity Management vs. Centralized Identity Management*. Zugriff 13. März 2023 unter https://www.dock.io/post/decentralized-identity#:~:text=Decentralized%20identity%20management%20is%20a,a%20central%20organization%20or%20company (Siehe S. 6)

AG, T. I. ((2021). *ERBE EINES SCHWEIZERISCHEN BANKKONTOS*. Zugriff 23. April 2023 unter https://www.geissmannlegal.ch/publikationen/digitale-nachlassplanung-was-passiert-mit-meinen-kryptowaehrungen-nach-dem-tod/ (Siehe Seiten 47, 48)

Anke, J., & Richter, D. (2023). Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik*, 1–22 (Siehe Seiten 2, 6, 7, 10–14, 16, 42)

Babel, M., & Sedlmeir, J. (2023). Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs. *arXiv preprint arXiv:2301.00823*, (Siehe S. 42)

BalthasarLegalAG. (2022). *Smart Contracts im Spannungsverhältnis zum Datenschutz*. Zugriff 18. Dezember 2022 unter https://balthasar-legal.ch/smart-contracts-im-spannungsverhaeltnis-mit-dem-datenschutz/ (Siehe S. 31)

Bastian, P., Kraus, M., & Fischer, J. (2023). Konzepte für sichere wallets in dezentralen Identitätsökosystemen. *HMD Praxis der Wirtschaftsinformatik*, *60*(2), 381–404 (Siehe Seiten 27, 28)

Beil, B., & Rauscher, A. (2018). Avatar. *Game Studies*, 201–217 (Siehe S. 51)

Bitpanda. (2023). *Was ist eine Wallet und wo bekomme ich eine?* Zugriff 13. März 2023 unter https://www.bitpanda.com/academy/de/lektionen/was-ist-eine-wallet-und-wo-bekomme-ich-eine/ (Siehe Seiten 26–28)

Bogensperger, A. (2021). *Beitragsreihe Blockchain Deep Dives: Hashing und Merkle Trees für datenschutzgerechte Dokumentation*. Zugriff 18. Dezember 2022 unter https://www.ffe.de/veroeffentlichungen/beitragsreihe-blockchain-deep-dives-hashing/ (Siehe Seiten 19, 20)

Booth, A. (2006). "Brimful of STARLITE": toward standards for reporting literature searches. *Journal of the Medical Library Association*, *94*(4), 421 (Siehe S. 52)

Draht, M. (2019). *Bedarf an Identitätsmanagement für die Welt von morgen*. Zugriff 17. März 2023 unter https://www.btc-echo.de/news/deloitte-studie-bedarf-an-identitaetsmanagement-fuer-die-welt-von-morgen-81871/ (Siehe Seiten 45, 47)

Ebeling, A. (2020). *Dezentrales Identitätsmanagement mittels Blockchain und ZKP*. Zugriff 22. Mai 2023 unter https://www.it-administrator.de/article-332850 (Siehe S. 3)

Egloff, P., & Turnes, E. (2019). *Blockchain für die Praxis*. SKV Zürich. (Siehe Seiten 17–21, 23–29, 31–33)

Ehrlich, T., Richter, D., Meisel, M., & Anke, J. (2021). Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. *HMD Prax. Wirtsch. 58*(2), 247–270 (Siehe Seiten 6, 10, 11, 34–41, 45–47, 49, 50)

Ethereum. (2023). *ZERO-KNOWLEDGE PROOFS*. Zugriff 15. März 2023 unter https://ethereum.org/en/zero-knowledge-proofs/ (Siehe Seiten 42, 43)

Exodus. (2023). *Can you cancel or reverse a transaction?* Zugriff 13. März 2023 unter https://www.exodus.com/support/article/1732-cancel-or-reverse-transaction#:~:text=They%20can't%20be%20canceled,of%20the%20way%20blockchains%20work (Siehe S. 30)

Hellwig, D., Karlic, G., & Huchzermeier, A. (2021). *Kryptowährungen*. In *Entwickeln Sie Ihre eigene Blockchain: Ein praktischer Leitfaden zur Distributed-Ledger-Technologie* (S. 31–56). Springer. (Siehe Seiten 27, 28, 30–33)

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, *19*(2), 4 (Siehe Seiten 52, 53)

Jahn, T. (2023). *Was die KI von OpenAI alles kann*. Zugriff 22. April 2023 unter https://www.handelsblatt.com/technik/it-internet/chatgpt-was-die-ki-von-openai-alles-kann-/28941524.html (Siehe S. 51)

Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and Decentralized identity as the future of identity management? *Open Identity Summit 2020*, (Siehe S. 47)

Kulabukhova, N. (2019). Zero-knowledge proof in self-sovereign identity. *CEUR Workshop Proceedings*, *2507*, 381–385 (Siehe Seiten 34, 42, 43)

Kunze, C. P. (2003). Digitale Identität und Identitäts-Management. *Hamburg, Universität Hamburg, Fachbereich Informatik*, (Siehe S. 11)

Lee, J. S., Pries-Heje, J., & Baskerville, R. (2011). Theorizing in design science research. *Service-Oriented Perspectives in Design Science Research: 6th International Conference, DESRIST 2011, Milwaukee, WI, USA, May 5-6, 2011. Proceedings 6*, 1–16 (Siehe S. 53)

LEI, S. (2020). *Die Bedeutung des Vertrauens in die Identität im digitalen Zeitalter*. Zugriff 29. April 2023 unter https://schweiz-lei.ch/die-bedeutung-des-vertrauens-in-die-identitat-im-digitalen-zeitalter/ (Siehe S. 1)

Lesavre, L., Varin, P., & Yaga, D. (2021). *Blockchain networks: Token design and management overview* (Techn. Ber.). National Institute of Standards und Technology. (Siehe Seiten 29, 30)

Lewrick, M., & Giorgio, C. (2018). *Live aus dem Krypto-Valley*. Vahlen. (Siehe Seiten 19, 20)

Meitinger, T. H. (2017). Smart contracts. *Informatik-Spektrum*, *40*(4), 371–375 (Siehe S. 30)

metamandrill. (2022). *Metaversum-Avatar-Leitfaden; Verkörpere dich in der Metaverse*. Zugriff 22. April 2023 unter https://metamandrill.com/de/metaverse-avatar/#the-future-for-metaverse-avatars (Siehe S. 51)

Millenaar, J. (2022). *The Binding Problem for SSI and NFTs*. Zugriff 15. März 2023 unter https://blog.iota.org/the-binding-problem-for-ssi-and-nfts/ (Siehe Seiten 50, 51, 78)

Moreland, K. (2022). *Wichtige Tipps für Hardware-Wallets*. Zugriff 7. Mai 2023 unter https://www.ledger.com/de/academy/wichtige-tipps-fuer-hardware-wallets (Siehe Seiten 27, 28)

Müller, F. (2023). *ChatGPT gründet erfolgreiche Online-Firma im Wert von 25'000 Dollar*. Zugriff 22. April 2023 unter https://www.nau.ch/news/wirtschaft/chatgpt-grundet-erfolgreiche-online-firma-im-wert-von-25000-dollar-66451059 (Siehe S. 51)

Neugebauer, R. (2018). *Digitalisierung*. Springer. (Siehe Seiten 22, 23, 31)

Opensea. (2023). *How can I revoke token approvals and permissions on Ethereum?* Zugriff 13. März 2023 unter https://support.opensea.io/hc/en-us/articles/4416083190291-How-can-I-revoke-token-approvals-and-permissions-on-Ethereum- (Siehe S. 30)

Oracle. (2023). *Was ist das IoT?* Zugriff 13. März 2023 unter https://www.oracle.com/ch-de/internet-of-things/what-is-iot/ (Siehe S. 8)

Petrlic, R., Sorge, C., & Ziebarth, W. (2023). *Einführung in den Technischen Datenschutz*. In *Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie* (S. 9–27). Springer. (Siehe Seiten 10, 11)

Reinwald, R. (2022). *Currency Token*. In *Die steuerliche Behandlung von Krypto-Assets* (S. 27–27). Springer. (Siehe Seiten 18, 20, 22)

Rohrer, M. (2022). *Self Sovereign Identity – Identitäten im digitalen Zeitalter*. Zugriff 29. April 2023 unter https://www.ipg-group.com/details/blog_self_sovereign_identity (Siehe Seiten 1, 2)

Schardong, F., & Custódio, R. (2022). Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. *Sensors*, *22*(15), 5641 (Siehe Seiten 40, 49, 50)

Schnabel, P. (2022). *Verschlüsselung / Chiffrierung*. Zugriff 18. Dezember 2022 unter https://www.elektronik-kompendium.de/sites/net/1907041.htm (Siehe Seiten 25, 26)

Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, *2021*, 1–26 (Siehe Seiten 45, 46)

Spörri, J. (2023). *Diese Westschweizer Moderatorin ist kein Mensch – doch niemand hat es bemerkt*. Zugriff 23. April 2023 unter https://www.aargauerzeitung.ch/

schweiz/kuenstliche-intelligenz-diese-westschweizer-moderatorin-ist-kein-mensch-doch-niemand-hat-es-bemerkt-ld.2445502?reduced=true (Siehe S. 51)

Steidl, V. (2022). *Smart Contracts: Definition, Beispiele und Coins*. Zugriff 18. Dezember 2022 unter https://bitcoin-2go.de/smart-contracts/ (Siehe S. 31)

Tsolkas, A., & Schmidt, K. (2017). *Rollen und Berechtigungskonzepte: Identity-und Access-Management im Unternehmen*. Springer-Verlag. (Siehe Seiten 6–9, 11)

Urban, N. T. (2022). *Self-Sovereign Identity*. Zugriff 22. Mai 2023 unter https://www.it-daily.net/spezial/web3/self-sovereign-identity (Siehe Seiten 2, 3)

Urban, N. T., & Urban, N. T. (2020). Blockchain als verteilte Netzwerktechnologie. *Blockchain for Business: Erfolgreiche Anwendungen und Mehrwerte für Netzwerkteilnehmer identifizieren*, 11–29 (Siehe Seiten 17, 21)

van Dijk, N., Kerver, B., Kodden, H., & Uitdehaag, M. (2021). *Technical exploration Ledger-based Self Sovereign Identity*. Zugriff 7. Mai 2023 unter https://www.surf.nl/files/2021-05/technical-exploration-surf-ledger-based-self-sovereign-identity.pdf (Siehe Seiten 45, 46, 49)

Voshmgir, S. (2020). *Token economy: How the Web3 reinvents the internet* (Bd. 2). Token Kitchen. (Siehe Seiten 2, 3, 29)

W3C. (2022). *Verifiable Credentials Data Model v1.1*. Zugriff 27. Mai 2023 unter https://www.w3.org/TR/vc-data-model/ (Siehe Seiten 76, 77)

Wagner, L. (2023). *Wie gefährlich kann KI für die Welt werden?* Zugriff 22. April 2023 unter https://www.zdf.de/nachrichten/digitales/gefahren-kuenstliche-intelligenz-entwicklung-stopp-gpt-100.html#:~:text=Es%20gibt%20auch%20Bedenken%20hinsichtlich,oder%20feindlichen%20Nationen%20missbraucht%20werden (Siehe S. 51)

Warrington, S. (2022). *The changing landscape of digital identity*. Zugriff 17. März 2023 unter https://www.tcs.com/what-we-do/industries/communications-media-information-services/white-paper/digital-identity-consent-management-solution (Siehe Seiten 48, 49)

Wilkens, R., & Falk, R. (2019). Smart contracts. *Aufl., Wiesbaden*, (Siehe Seiten 31, 32)

Wrobel, L. (2022). *Decentralized Identity – Secure Digital Identity Management?* Zugriff 29. April 2023 unter https://ccecosystems.news/en/decentralized-identity-secure-digital-identity-management/ (Siehe S. 2)

Wysshaar, K. (2021). *DIGITALE NACHLASSPLANUNG – WAS PASSIERT MIT MEINEN KRYPTOWÄHRUNGEN NACH DEM TOD?* Zugriff 23. April 2023 unter https://www.geissmannlegal.ch/publikationen/digitale-nachlassplanung-was-passiert-mit-meinen-kryptowaehrungen-nach-dem-tod/ (Siehe Seiten 47, 48)

Yang, K., & Wang, X. (2023). Non-interactive zero-knowledge proofs to multiple verifiers. *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part III*, 517–546 (Siehe S. 43)

A | VC und VP Grundkomponenten

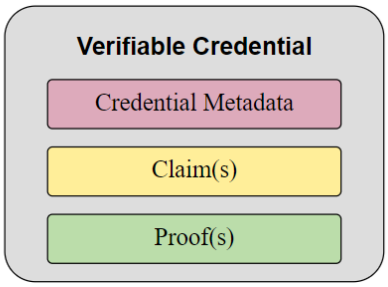

Abbildung A.1 Grundkomponenten eines VC (W3C, 2022)

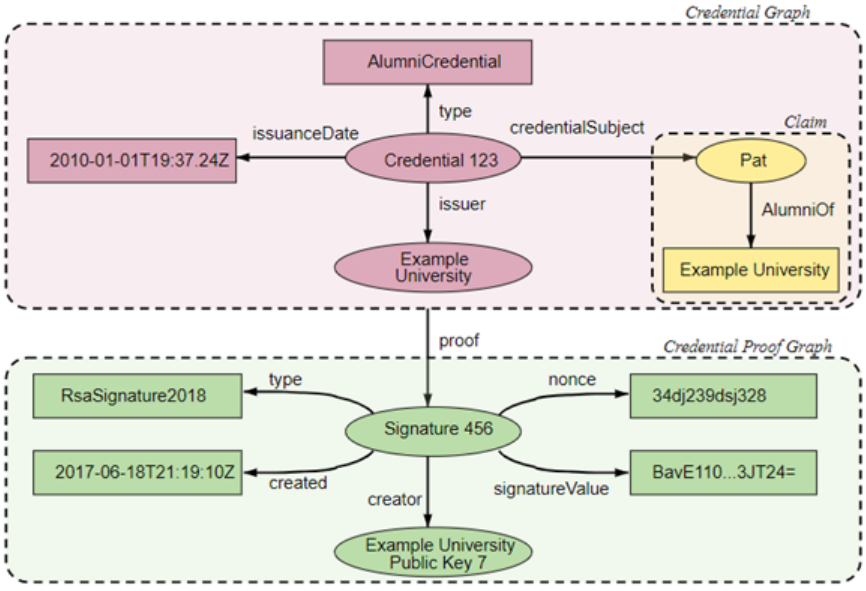

Abbildung A.2 Informationsdiagramme eines VC, die einem einfachen überprüfbaren Berechtigungsnachweis zugeordnet sind (W3C, 2022)

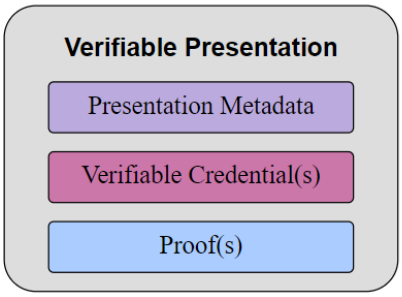

Abbildung A.3 Grundkomponenten einer VP (W3C, 2022)

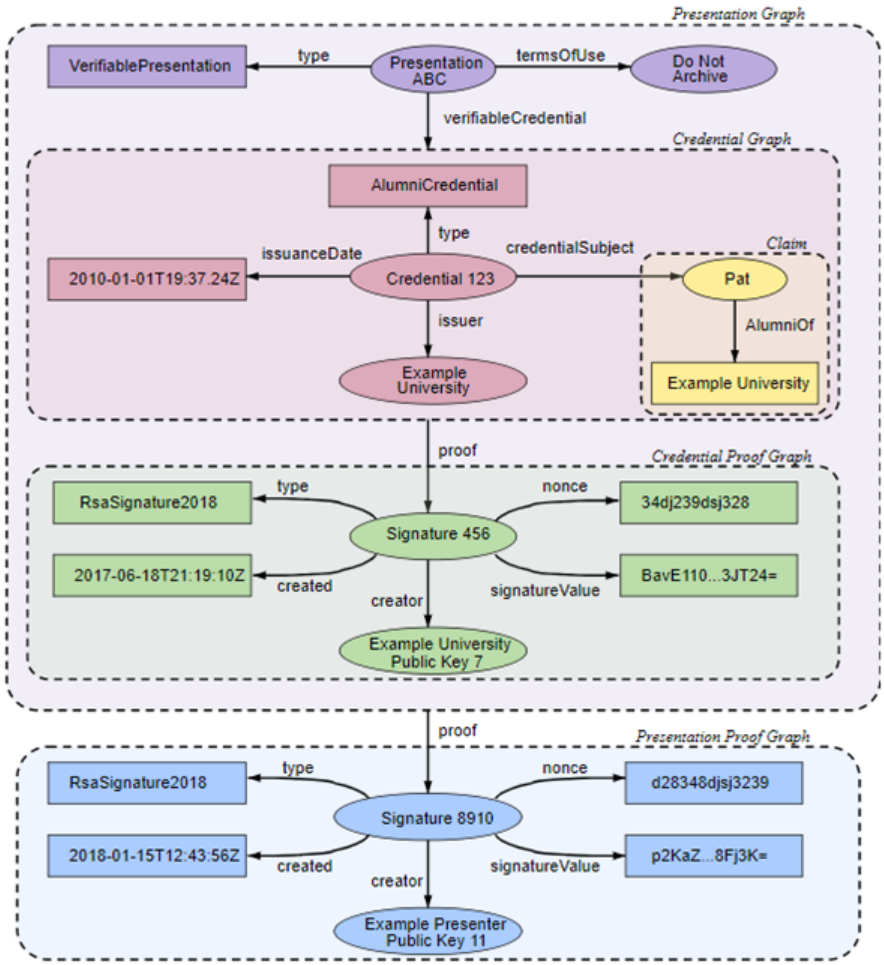

Abbildung A.4 Informationsdiagramme einer VP, die einem einfachen überprüfbaren Berechtigungsnachweis zugeordnet sind (W3C, 2022)

B | eIDAS Skala der Zuverlässigkeit

Abbildung B.1 eIDAS Levels of Assurance Scale (Millenaar, 2022)

C | Aspekte der Literaturrecherche

Tabelle C.1 Aspekte der Literaturrecherche gemäss STARLITE

Aspekte der Literaturrecherche	**Vorgehen**
S – Sampling strategy	Eine umfassende Suche nach allen relevanten Studien zur Schliessung der Forschungslücke.
T – Type of studies	Meta-Analysen und systematische Literaturüberblicke.
A – Approaches	Mittels einer Stichwortsuche wurde nach relevanter Literatur gesucht. Anschliessend wurden weitere Literaturen anhand des Schneeballprinzips analysiert.
R – Range of years	Für die Stichwortsuche wurden hauptsächlich aktuelle Quellen der letzten drei Jahre berücksichtigt, da sich die Technologie schnell weiterentwickelt und ältere Quellen möglicherweise veraltet sind. Für das Schneeballprinzip wurde keine zeitliche Eingrenzung definiert.
L – Limits	Die Literaturrecherche wurde auf deutsch- und englischsprachigen Artikeln beschränkt.
I – Inclusions and exclusions	Die Literaturrecherche umfasste nebst Studien über das Identity Management auch umfassende Studien zur Blockchain-Technologie und deren Funktionalität
T – Terms used	Identity Management, SSI, blockchain, token, NFTs, Wallet, digitale Identität, IAM, Rollen und Berechtigungen, Identitätsmanagement, DLT, Smart Contracts, Web 3.0, Identität in der digitalen Welt, Interessenskonflikte im Web 3.0, Funktion Blockchain, Web 2.0 vs Web 3.0, Arten von Blockchain, Wallet Arten, SSI umsetzen, Identity Management Modelle, verschiedene Arten von Token, dApps, Funktionalität Smart Contracts usw.
E – Eletronic sources	IEEE Xplore, Google Scholar, ZHAW swisscovery etc.