Duale Hochschule Baden-Württemberg Mannheim

Bachelorarbeit

Entwicklung eines Showcases für Blockchain-basierte Identitätslösungen in der Telekommunikation am Beispiel von World Coin

Studiengang Wirtschaftsinformatik

Studienrichtung Data Science

Verfasser:	Christian Schmid
Matrikelnummer:	2776248
Firma:	Telefónica Germany GmbH & Co. OHG
Abteilung:	T-ASA Technology Strategy & Innovation
Kurs:	WWI21DSA
Studiengangsleiter:	Prof. Dr.-Ing. Dennis Pfisterer
Wissenschaftlicher Betreuer:	Dr. Simon Poll
Firmenbetreuer:	Karsten Erlebach, Peter Wiese
Bearbeitungszeitraum:	13.02.2024 – 03.05.2024
Eingereicht:	03.05.2024

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich die vorliegende Arbeit mit dem Titel "*Entwicklung eines Showcases für Blockchain-basierte Identitätslösungen in der Telekommunikation am Beispiel von World Coin*" selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

München, 03.05.2024
Ort, Datum

Christian Schmid

Danksagung

Mein Dank gilt Peter Wiese für die gewissenhafte Durchsicht meiner Arbeit, die maßgeblich zur Qualitätssteigerung beigetragen hat. Ebenso danke ich sowohl Peter Wiese als auch Karsten Erlebach für die Auswahl des Showcases sowie die Umsetzung des Projekts in der Innovation Experience Area. Ihre gemeinsamen Bemühungen und innovativen Ideen waren von großem Wert.

Inhaltsverzeichnis

Abbildungsverzeichnis **v**

Quelltextverzeichnis **vi**

Abkürzungsverzeichnis **vii**

Kurzfassung **viii**

1 Einleitung **1**

2 Grundlagenkapitel **3**
2.1 Blockchain . . . 3
2.1.1 Merkle-Tree . . . 5
2.1.2 Smart Contracts . . . 7
2.1.3 Layer-2-Lösungen . . . 8
2.1.4 Wallets . . . 8
2.2 Authentifizierung . . . 9
2.2.1 Zwei-Faktor-Authentifizierung . . . 9
2.2.2 Single-Sign-On . . . 9
2.2.3 Zero-Knowledge-Proof . . . 10

3 Blockchain Single-Sign-On **11**
3.1 State of the Art . . . 11
3.2 Use Case . . . 13
3.2.1 Vergleich . . . 14
3.2.2 Identifikation . . . 19
3.2.3 Schutz vor Identitätsdiebstahl . . . 21
3.3 Showcase . . . 22
3.3.1 Anforderungen . . . 22
3.3.2 Storyline . . . 23
3.3.3 Blockchain-Umsetzung . . . 26
3.3.4 Cloud-Umsetzung . . . 34
3.3.5 Key Performance Indicators . . . 38

4 Zusammenfassung **40**
4.1 Fazit . . . 41
4.2 Ausblick . . . 42

Literaturverzeichnis **43**

Abbildungsverzeichnis

2.1 Blockchain 4
2.2 Hashtree 6
2.3 Merkletree 7

3.1 Pawned 15
3.2 Anmeldung Mode-Chain 16
3.3 Nft Transaktion 17
3.4 Biometrievergleich 20
3.5 Speicherset 21
3.6 Iriscode 22
3.7 DeepLabV3-Architektur 26
3.8 Iriscode 27
3.9 Merkle Root 27
3.10 Bridge Architetktur 28
3.11 Login QR 30
3.12 Blockchain Login 31
3.13 Login per Cloud 35
3.14 OCID Sign-In 36

Quelltextverzeichnis

3.1 Konfigurationsbeispiel Schmid, 2024, Commit-ID: 008d3d4 29
3.2 Integrationsbeispiel Schmid, 2024, Commit-ID: 008d3d4 29
3.3 Vertragsinteraktion Schmid, 2024, Commit-ID: 008d3d4 31
3.4 NFT Überprüfung Schmid, 2024, Commit-ID: 008d3d4 33
3.5 Token Weitergabe Schmid, 2024, Commit-ID: 008d3d4 34
3.6 Authentifizierungsanfrage und JWT Schmid, 2024, Commit-ID: 008d3d4 . . 37

Abkürzungsverzeichnis

DHBW	Duale Hochschule Baden-Württemberg
PoW	Proof-of-Work
TXID	Transaktion-ID
DeFi	Decentralized Finance
ZK	Zero-Knowledge
ZKP	Zero-Knowledge-Proof
dApp	dezentrale Applikation
2FA	Zwei-Faktor-Authentifizierung
SSO	Single-Sign-On
JWT	JSON Web Token
KYC	Know-Your-Customer
PoH	Proof-of-Humanity
P2P	Peer-to-Peer
SSI	Self-Sovereign-Identity
NFT	Non-Fungible-Token
API	Application Programming Interface
IEA	Innovation Experience Area

Kurzfassung

Die vorliegende Bachelorarbeit beschäftigt sich mit der Entwicklung eines praxisorientierten Showcases für blockchain-basierte Identitätslösungen in der Telekommunikationsbranche, spezifisch am Beispiel von World Coin. Vor dem Hintergrund der steigenden Relevanz digitaler Identitäten in der Europäischen Union, zielt diese Arbeit darauf ab, innovative Ansätze des Identitätsmanagements unter Einsatz von Blockchain- und Cloud-Technologien zu erkunden und zu demonstrieren. Die Integration des Proof-of-Personhood-Konzepts von Worldcoin resultiert in einem neuartigen Ansatz zur Authentifizierung und zum Identitätsmanagement.

In dieser Arbeit wird ein dualer Ansatz verfolgt, bei dem sowohl Blockchain-basierte als auch Cloud-basierte Single-Sign-On Lösungen entwickelt werden. Der Showcase demonstriert, wie durch den Einsatz von Blockchain-Technologie die Integrität und Authentizität digitaler Identitäten gewährleistet und gleichzeitig die Privatsphäre der Nutzer geschützt werden kann. Die Realisierung des Projekts in der Innovation Experience Area der Telefónica Deutschland ermöglichte die Generierung praxisrelevanter Einblicke in die Implementierung und das Potential von Blockchain-Lösungen im Bereich der digitalen Identitäten.

Die Ergebnisse legen Vorteile hinsichtlich Sicherheit, Dezentralisierung, Transparenz und Fälschungssicherheit nahe, die sich aus der Blockchain-Technologie ergeben. Dies liefert Erkenntnisse für die Weiterentwicklung und eine breitere Anwendung dieser Technologie in der Telekommunikationsbranche.

1 Einleitung

Auf politischer Ebene erfährt das Thema Identitätsmanagement derzeit eine hohe Relevanz. So entwickelt die Europäische Union gegenwärtig eine eigene digitale Identitätswallet, um die Sicherheit und grenzüberschreitende Nutzbarkeit digitaler Identitäten in der EU zu fördern (Vgl. European Union, 2024).

Im Kontext dessen erlangt die sichere und effiziente Verwaltung digitaler Identitäten eine zunehmend wichtigere Bedeutung. Dies gilt insbesondere für die Telekommunikationsbranche, in der das Identitätsmanagement eine zentrale Rolle für die Bereitstellung personalisierter Dienste spielt. In diesem Zusammenhang bieten innovative Lösungen, die auf der Blockchain-Technologie basieren und den Gegenpol zu Big-Tech-Identity repräsentieren, vielversprechende Ansätze, die sich durch Sicherheit, Dezentralisierung, Transparenz und Fälschungssicherheit auszeichnen (Vgl. Dong et al., 2023).

Innovative Konzepte in der Digitalisierung sind auch wichtige Themen in der Innovation Experience Area (IEA), dem Showroom der Telefónica Deutschland im o2-Tower in München. In der IEA werden in verschiedenen Zonen neuste technologische Entwicklungen für End- und Geschäftskunden präsentiert. Insbesondere spannend ist hierbei die „Vision Zone“, in der neben den Themen Künstliche Intelligenz und Holographie auch Anwendungsgebiete für Blockchain-Technologien vorgestellt werden.

Ziel dieser Arbeit ist die Entwicklung und Demonstration eines praxistauglichen Showcase, der aufzeigt, wie Blockchain-Technologie effektiv für Blockchain-basierte Identitätsmanagement Lösungen genutzt werden kann.

Im Rahmen dieses Vorhabens erfolgt eine Integration der Blockchain in Verbindung mit Worldcoin, einer Plattform, welche darauf abzielt, Identitätsmanagement in einer dezentralen Weise für die gesamte Menschheit durch Proof of Personhood zu integrieren. Somit soll ein Beitrag zur Diskussion und Weiterentwicklung von Blockchain-Anwendungen im Bereich der digitalen Identitäten geleistet werden. Im Rahmen dessen wird erörtert, welche technischen Herausforderungen bei der Implementierung eines Blockchain-basierten Identitätsmanagementsystems bestehen und wie diese gelöst werden können.

Dafür erfolgt zunächst im anschließenden Kapitel Zwei eine allgemeine Vorstellung der Blockchain Technologie. Im Rahmen der dezentraler Architekturen wird insbesondere auf

die Funktionsweise von Transaktionen sowie die Rolle und den Aufbau von Merkle-Trees und zentrale Sicherheitsmechanismen eingegangen. Hierzu gehören unter anderem Smart Contracts und verschiedene Authentifizierungslösungen, die in Blockchain-Systemen Anwendung finden. Darüber hinaus werden die verschiedenen Authentifizierungsmöglichkeiten erörtert, um ein grundlegendes Verständnis für die in der Arbeit enthaltenen Technologien zu vermitteln.

Das dritte Kapitel befasst sich mit dem zentralen Thema dieser Arbeit, dem Blockchain Single-Sign-On (SSO). Zunächst wird der aktuelle Stand der Technik präsentiert, bevor ein detaillierter Use Case für die Implementierung eines solchen Systems in der Telekommunikationsbranche entwickelt wird. Zusätzlich wird auch ein Cloud-basiertes SSO besprochen, um alle Möglichkeiten in Kombination mit Worldcoin aufzuzeigen. Im Rahmen dessen werden technische Herausforderungen erörtert und Lösungsansätze präsentiert. Ein praktischer Showcase rundet das Kapitel ab und demonstriert die Umsetzung des SSO-Konzepts.

In der abschließenden Zusammenfassung werden die wesentlichen Erkenntnisse der Arbeit reflektiert und ein Ausblick auf zukünftige Entwicklungen und Anwendungen der Blockchain Technologie im Bereich des Identitätsmanagements gegeben.

2 Grundlagenkapitel

Um die Funktionsweise von Blockchain-SSO-Lösungen nachvollziehen zu können, ist es erforderlich, zunächst die zugrundeliegenden technischen Konzepte zu erläutern. Dies umfasst insbesondere die Blockchain-Technologie, die Funktionsweise von SSO-Systemen sowie die Rolle der Biometrie als Authentifizierungsmechanismus. Die Betrachtung der genannten Elemente dient der Entwicklung eines umfassenden Verständnisses für die Struktur und die Sicherheitsmerkmale moderner Authentifizierungslösungen.

2.1 Blockchain

Die Blockchain ist eine Technologie, die es ermöglicht, Daten in einer dezentralen und sicheren Weise zu speichern. Sie basiert auf einer Kette von Datenblöcken, die durch kryptografische Verfahren miteinander verbunden sind. Dadurch werden unzulässige Änderungen verhindert, da jede Manipulation der Daten sofort erkennbar wäre. Die Einigkeit über den Zustand der Datenkette wird durch einen Konsensmechanismus im Netzwerk erreicht, wodurch keine zentrale Kontrollinstanz benötigt wird (Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2024a). Ein Beispiel für eine Blockchain ist das Bitcoin-Netzwerk, welches als erstes seiner Art im dezentralen Peer-to-Peer-Netzwerk digitale Währungstransaktionen ermöglichte und damit den Grundstein für zahlreiche weitere kryptografische Anwendungen legte (Vgl. Nakamoto, 2008).

Die Blockchain-Technologie bietet Transparenz, Sicherheit und Unveränderlichkeit. Sie findet insbesondere Anwendung bei der Abwicklung sicherer Transaktionen. Beispiele wie Bitcoin und Ethereum demonstrieren, wie Blockchain die Grundlage für sichere und dezentralisierte Währungssysteme bildet. Des Weiteren ermöglicht die Blockchain die Entwicklung von Decentralized Finance (DeFi), einem Bereich, der traditionelle Finanzdienstleistungen wie Kredite, Börsen und Versicherungen über dezentralisierte Plattformen ohne zentrale Vermittler anbietet.

In dieser Blockchain enthält jeder Block einen kryptographischen Hash des vorherigen Blocks sowie einen Zeitstempel, wann dieser Block erstellt wurde und Transaktionsdaten wie Empfänger und Sender einer speziellen Kryptowährung. Die folgende Abbildung 2.1

zeigt den vereinfachten Transaktionsprozess sowie die Erstellung und Validierung eines Blocks im Bitcoin-Netzwerk.

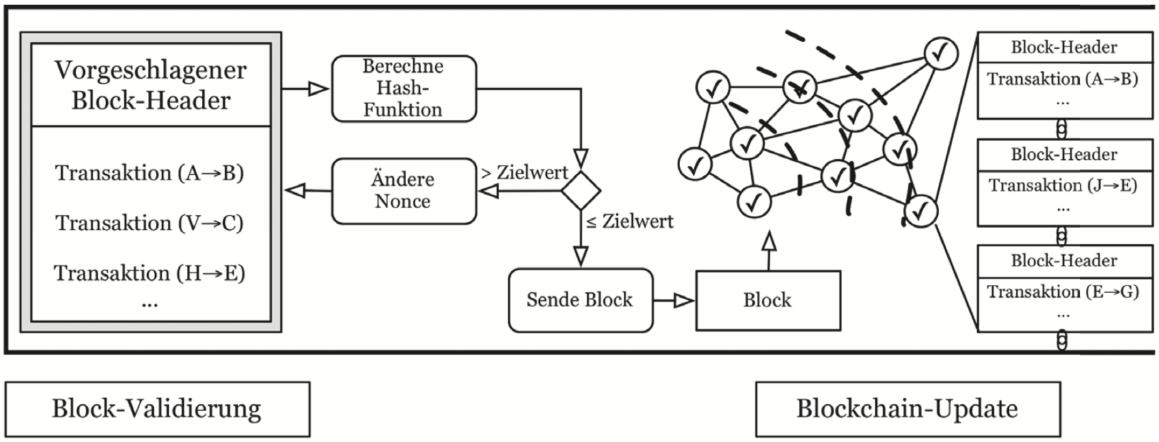


Abbildung 2.1: Der Transaktionsprozess im Bitcoin-System
Quelle: Kaucher, 2018, S. 5

Block-Header und Transaktionen: Der linke Teil der Abbildung 2.1 präsentiert den vorgeschlagenen Block-Header sowie eine Liste von Transaktionen (z.B. A →B, V →C, H →E), die in den Block aufgenommen werden sollen (Vgl. Kaucher, 2018).

Hash-Funktion und Nonce: Der mittlere Abschnitt der Grafik zeigt die Berechnung der Hash-Funktion sowie die Anpassung eines Nonce-Wertes. Hierbei wird ein Nonce (eine zufällige Nummer, die nur einmal verwendet wird) gewählt und mit den anderen Daten des Block-Headers verwendet, um einen Hash-Wert zu berechnen. Dieser Wert muss unterhalb eines bestimmten Zielwerts liegen, um als gültiger Proof-of-Work (PoW) zu gelten. Falls der Wert nicht unter dem Zielwert liegt, wird die Nonce geändert und die Hash-Funktion erneut berechnet. Dieser Prozess wird wiederholt, bis der Hash-Wert die Bedingung erfüllt. Dies stellt sicher, dass nicht jeder einen Block hinzufügen kann (Vgl. Schlatt et al., 1990).

Block-Validierung: Im Falle der Identifizierung eines gültigen Hash-Wertes ($Hash \leq Zielwert$) erfolgt die Übermittlung des Blocks an das Netzwerk (rechter Abschnitt der Abbildung 2.1), um in die Blockchain aufgenommen zu werden. Die übrigen Knoten des Netzwerks führen eine Block-Validierung durch, um die Einhaltung der Netzwerk-Regeln zu gewährleisten. Dies beinhaltet die Überprüfung der Transaktionen und des PoW. Nach erfolgreicher Validierung wird der Block zur Blockchain hinzugefügt, wobei jeder nachfolgende Block auf dem vorherigen aufbaut und somit die Kette bildet (Vgl. Kaucher, 2018).

Der Name „Blockchain“ leitet sich aus dieser Eigenschaft ab. Jeder zusätzliche Block verstärkt hierbei, die Sicherheit der vorhergehenden Blöcke (Vgl. Kaucher, 2018).

Transparenz und Sicherheit: Jeder Block enthält den Hashwert des Vorgängerblocks. Sollte sich der Hashwert ändert, ändert sich auch der Hashwert des folgenden Blocks. Auch bei kleinen Modifikationen an den Daten ergibt sich ein komplett anderen Hash Wert und alle nachfolgenden Hashes sind ungültig. (Vgl. Panuntun et al., 2023).

Der PoW-Mechanismus gewährleistet zudem die Sicherheit des Netzwerks, da er beim Hinzufügen neuer Blöcke eine wesentliche Rolle spielt. Miner, die Teilnehmer im Bitcoin-Netzwerk sind, verwenden spezielle Hardware, um komplexe mathematische Rätsel zu lösen. Diese Aufgabe ist notwendig, um neue Blöcke zur Kette hinzuzufügen und erfordert erhebliche Rechenleistung. Eine nachträgliche Änderung würde bedeuten, dass der PoW für den manipulierten Block und alle folgenden Blöcke neu berechnet werden muss. Bei einer umfangreichen und gut vernetzten Blockchain ist dies aufgrund des immensen Rechenaufwands nahezu unmöglich (Vgl. Nakamoto, 2008).

2.1.1 Merkle-Tree

Ein Merkle-Tree, auch unter dem Begriff Hash-tree bekannt, stellt eine spezielle Art von Datenstruktur dar, welche in der Informatik, insbesondere in der Blockchain-Technologie verwendet wird. Diese Datenstruktur dient der Verwaltung und Überprüfbarkeit einer großen Datenmenge. Die Struktur eines Merkle-Tree besteht aus einer Vielzahl unterschiedlicher Knoten, welche jeweilige Daten oder deren Hash-Werte enthalten. Die Daten, welche sich an den untersten Knotenpunkten des Baumes, auch als Blätter bezeichnet, befinden, sind Hashes von Transaktionsdaten. Diese Blätter stellen die grundlegendsten Elemente des Baumes dar (Vgl. Borde, 2022). Ein Beispiel eines solchen Hash-Tree ist in untenstehender Abbildung 2.2 zu sehen.

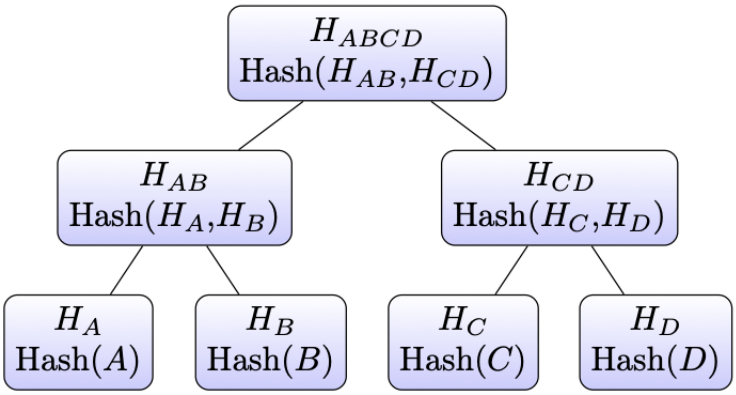


Abbildung 2.2: Einfacher Hash-Tree bei dem H_{abcd} die Merkle-Root darstellt
Quelle: Borde, 2022, S. 3

Ein Merkle-Tree besteht aus zwei grundlegenden Elementen: den Blattknoten und den intermediären Knoten. Ein Blattknoten ist ein Knoten, der jede einzelne Transaktion innerhalb eines Blocks verarbeitet. Dazu wird zunächst eine kryptografische Hash-Funktion auf die Transaktion angewendet, um einen einzigartigen Hash-Wert zu erzeugen. Dieser wird als Transaktion-ID (TXID) bezeichnet und dient als eindeutiger Identifikator der Transaktion in der Blockchain (Vgl. Borde, 2022).

Als Intermediäre Knoten werden diejenigen bezeichnet, welche sich zwischen den Blattknoten und den Wurzelknoten (Merkle Root) des Merkle-Tree befinden. Sie dienen der Verarbeitung der TXIDs. Im Anschluss werden die TXIDs paarweise zusammengefasst und die resultierenden Zeichenketten erneut gehasht. Der Prozess wird rekursiv wiederholt, wobei auf jeder höheren Ebene des Baumes die Hashes der darunter liegenden Ebene zusammengefasst und gehasht werden, bis nur noch ein Hash übrig bleibt. Der Wurzelknoten stellt die oberste Ebene des Merkle-Tree dar und besteht aus einem einzelnen Knoten. Der Wurzelknoten enthält den Hash, der aus der Kombination aller darunter liegenden Hashes resultiert. Er repräsentiert eine kompakte Zusammenfassung aller Transaktionen des Blocks (Vgl. Borde, 2022).

Ein Beispiel für die Verwendung in der Blockchain ist in der nachfolgenden Abbildung 2.3 dargestellt. Die Abbildung präsentiert einen Ausschnitt des Merkle-Trees, der spezifisch für die Transaktion Tx3 erstellt wurde. Der dargestellte Abschnitt des Merkle-Trees veranschaulicht die Verifikation einer einzelnen Transaktion, ohne dass der gesamte Baum hierfür erforderlich wäre.

Zur Verifikation der Transaktion Tx3 würde ein Netzwerkteilnehmer zunächst den Hash von Tx3 (Hash3) berechnen und ihn dann mit Hash2 kombinieren, um Hash23 zu bilden. Im Anschluss würde er Hash23 mit dem entsprechenden Hash auf der gleichen Ebene (Hash01) kombinieren, um zu überprüfen, ob der resultierende Hash mit dem im Block Header gespeicherten Merkle Root übereinstimmt.

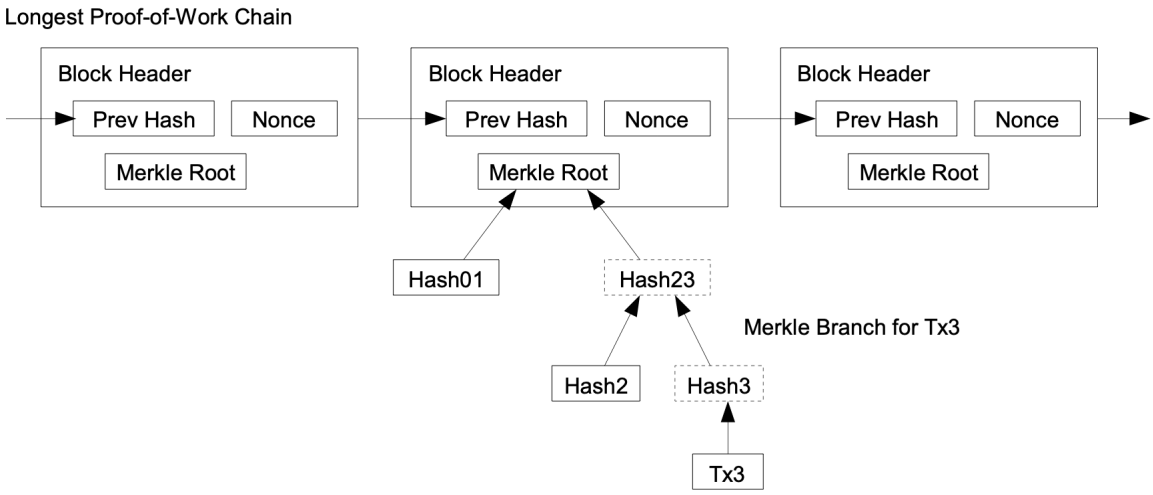


Abbildung 2.3: Vereinfachte darstellung einer Zahlungsüberprüfung aus dem Bitcoin Whitepaper
Quelle: Nakamoto, 2008, S. 5

2.1.2 Smart Contracts

Bei Smart Contracts handelt es sich um ausführbaren Code, welcher auf Blockchain-Knoten läuft und dazu dient, Verträge oder DeFi-Interaktionen oder Transaktionen digital zu erleichtern, zu verifizieren oder durchzusetzen. Sie werden in die Blockchain implementiert und automatisch ausgeführt, wenn vordefinierte Bedingungen erfüllt sind. Dadurch ermöglichen sie die Verifizierung, Ausführung und Durchsetzung von Transaktionen und Vereinbarungen, ohne dass eine zentrale Autorität, ein Rechtssystem oder externe Durchsetzungsmechanismen erforderlich sind (Vgl. Hu et al., 2018).

Smart Contracts werden bereits in einer Vielzahl von Anwendungsbereichen wie dem Internet of Things (IOT), Smart Property oder der Verwaltung von Musikrechten und Digitalem Handel eingesetzt (Vgl. Abdelhamid und Hassan, 2019).

2.1.3 Layer-2-Lösungen

Layer-2-Lösungen sind sekundäre Protokolle, die auf einer bestehenden Blockchain aufbauen und darauf abzielen, Transaktionen außerhalb der Hauptkette abzuwickeln. Dies reduziert die Last auf der Hauptkette und ermöglicht höhere Transaktionsgeschwindigkeiten. Beispiele für Layer 2 Lösungen sind:

State Channels: Bei State Channels werden Transaktionen zwischen Knoten außerhalb der Kette durchgeführt und nur die Eröffnungs- und Schließungstransaktionen auf der Hauptkette aufgezeichnet. Dies ermöglicht schnelle und kostengünstige Transaktionen zwischen den beteiligten Parteien (Vgl. Sguanci et al., 2021).

Sidechains: Sidechains sind eigenständige Blockchains, die parallel zur Hauptkette laufen und mit dieser verbunden sind. Sie können schneller sein, da weniger Knoten beteiligt sind, was aber oft zu einer geringeren Dezentralität führt (Vgl. Sguanci et al., 2021).

Rollups: Rollups führen Transaktionen außerhalb der Kette aus, melden aber den Status dieser Transaktionen kontinuierlich und in komprimierter Form an die Hauptkette zurück. Zwei Formen sind Zero-Knowledge (ZK) Rollups, die die Gültigkeit von Transaktionen durch Zero-Knowledge-Proof (ZKP) nachweisen, und Optimistic Rollups, die auf einem interaktiven Beweissystem basieren (Vgl. Sguanci et al., 2021). Diese Lösungen gehen das Problem der Skalierbarkeit direkt an, indem sie die Anzahl der Transaktionen, die in der Hauptkette verarbeitet werden müssen, reduzieren.

2.1.4 Wallets

Kryptowallets sind digitale Geldbörsen, die zum Speichern, Senden und Empfangen von Kryptowährungen wie Bitcoin und Ethereum verwendet werden. Es lassen sich zwei Haupttypen von Kryptowallets unterscheiden: Custodial und Non-Custodial Wallets.

Custodial Wallets werden von einem Dritten verwaltet. Die privaten Schlüssel, die für den Zugriff auf die Kryptowährungen notwendig sind, werden von dieser dritten Partei gehalten (Vgl. Gomzin, 2022).

Bei Non-Custodial Wallets befinden sich die privaten Schlüssel ausschließlich im Besitz des Nutzers (Vgl. Gomzin, 2022). Auf dieser Grundlage kann dem Nutzer ein höheres Maß an Unabhängigkeit gewährt werden, da er die vollständige Kontrolle über die betreffenden Vermögenswerte hat.

2.2 Authentifizierung

Die Authentifizierung bezeichnet den Prozess der Überprüfung der Identität einer Person oder eines Systems. Sie spielt eine entscheidende Rolle in der Sicherheit von Informationssystemen, da sie sicherstellt, dass Zugang und Ressourcen nur autorisierten Nutzern gewährt werden. Im Folgenden werden die in der vorliegenden Arbeit verwendeten Grundlagen der Authentifizierungsmethoden dargelegt.

2.2.1 Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung (2FA) stellt einen Sicherheitsmechanismus dar, der die Identität einer Person oder einer anderen Entität bestätigt, indem zwei verschiedene Authentifizierungsfaktoren verwendet werden. Diese Faktoren umfassen in der Regel Dinge die der Nutzer weiß, wie etwa ein Passwort, sowie Gegenstände, welche der Nutzer physisch besitzt, beispielsweise ein Smartphone oder einen Sicherheitstoken (Vgl. Reese et al., 2019). Der primäre Zweck der 2FA besteht in der Erhöhung der Sicherheitsebene, indem eine zusätzliche Barriere gegen unbefugten Zugriff implementiert wird. Dies erfordert, dass ein potenzieller Angreifer beide Faktoren kompromittiert, um Zugang zu erhalten.

2.2.2 Single-Sign-On

Single-Sign-On (SSO) bezeichnet ein Authentifizierungssystem, welches es Benutzern ermöglicht, sich einmalig anzumelden und dadurch Zugang zu mehreren unabhängigen Softwareanwendungen oder Diensten zu erlangen (Vgl. Radha und Reddy, 2012). Das Prinzip von SSO basiert auf einer zentralen Authentifizierungsinstanz, welche die Identität des Benutzers einmalig prüft und diese Bestätigung dann an andere verbundene Systeme und Dienste weitergibt, die ebenfalls SSO fähig sind. Der Ablauf der Authentifizierung gestaltet sich typischerweise wie folgt:

- Der Benutzer gibt seine Anmeldeinformationen (beispielsweise Benutzername und Passwort) in die SSO-Lösung ein.
- Nach erfolgreicher Authentifizierung erstellt die SSO-Lösung ein Authentifizierungstoken. Dieses Token enthält Informationen, die die Identität des Benutzers bestätigen.

- Sobald der Benutzer auf eine andere Anwendung oder einen Dienst zugreift, wird das Token automatisch an diese Anwendung gesendet.
- Token-Validierung: Die angeforderte Anwendung validiert das Token mit Hilfe der zentralen SSO-Lösung. Stimmt das Token überein, wird dem Benutzer Zugriff gewährt, ohne dass er sich erneut anmelden muss (Vgl. Sakimura et al., 2014).

Die Implementierung von SSO kann auf Basis verschiedener Protokolle und Standards erfolgen. Ein Beispiel hierfür ist OpenID Connect, welches auf dem OAuth 2.0-Protokoll aufbaut und es Clients ermöglicht, die Identität eines Endbenutzers zu verifizieren und grundlegende Profilinformationen über ihn zu erhalten (Vgl. Sakimura et al., 2014).

2.2.3 Zero-Knowledge-Proof

Zero-Knowledge-Proofs ZKPs sind kryptografische Protokolle, die es ermöglichen, die Gültigkeit einer Information zu bestätigen, ohne dabei weiteren Informationen über den Inhalt dieser Information preiszugeben. Laut Goldreich, Micali und Wigderson, werden solche Beweise durch den Einsatz mathematischer Algorithmen erstellt, die die Fähigkeit besitzen, die Korrektheit einer Aussage zu überprüfen, ohne dass spezifische Details dieser Aussage enthüllt werden müssen (Vgl. Goldreich et al., 1991).

ZKPs sind besonders nützlich in sensiblen Bereichen, wie Blockchain-Technologien. Hier helfen sie, die Details von Transaktionen geheim zu halten und gleichzeitig sicherzustellen, dass diese Transaktionen gültig sind. Sie funktionieren durch den Austausch speziell erstellter mathematischer Beweise, die so gestaltet sind, dass sie keine verwertbaren Daten über die eigentlichen Informationen preisgeben (Vgl. Chainlink Foundation, 2023).

ZKPs lassen sich in zwei Formen unterteilen: interaktive und nicht-interaktive. Bei interaktiven Proofs muss der Beweisende seine Beweisführung für jeden Prüfer einzeln vorführen. Nicht-interaktive Proofs hingegen erlauben es dem Beweisenden, einen einmaligen Beweis zu erstellen, den dann jeder Prüfer eigenständig überprüfen kann (Vgl. Yang und Li, 2020).

3 Blockchain Single-Sign-On

Die vorliegende Arbeit beschäftigt sich mit der Zielsetzung, einen Anwendungsfall für Blockchain basiertes Single-Sign-On (SSO) im Identitätsmanagement der Telekommunikationsbranche zu entwickeln. Zu diesem Zweck erfolgt in diesem Kapitel zunächst eine detaillierte Vorstellung des aktuellen Stands der Technik sowie der führenden Anbieter sowohl im Bereich Web-2 als auch Web-3. Der vorliegende Überblick bildet die Grundlage für die Untersuchung und Implementierung von Blockchain-Technologien in bestehende und zukünftige SSO-Systeme.

3.1 State of the Art

Im Bereich der SSO-Lösungen, welche als zentrale Komponenten zur Vereinfachung des Zugriffs auf verschiedene Online-Dienste und Anwendungen dient, lassen sich signifikante Unterschiede zwischen Web-2 und Web-3 Technologien feststellen.

Web-2 SSO-Lösungen basieren hauptsächlich auf zentralisierten, traditionellen Authentifizierungsmethoden wie Passwörtern, oft ergänzt durch 2FA. Sie sind in der Regel proprietär und intransparent. Diese Systeme, überwiegend entwickelt und kontrolliert von großen Technologieunternehmen wie Google, Microsoft, GitHub und Amazon Web Services, nutzen zwar robuste Application Programming Interface (API)s zur Integration, die internen Mechanismen und Datenverarbeitungspraktiken bleiben jedoch verborgen. Die Intransparenz dieser Systeme kann zu Kritikpunkten hinsichtlich des Datenschutzes und weiterer Sicherheitsbedenken führen.

Fortgeschrittene, tokenbasierte Authentifizierung mittels Security Assertion Markup Language (SAML) (Vgl. Google, 2023) und JSON Web Token (JWT) gewährleistet zwar sichere Prozesse, allerdings bleibt auch hier die fehlende Transparenz ein relevanter Punkt.

Darüber hinaus bieten spezialisierte SSO-Dienstleister wie Okta, OneLogin und Auth0 umfangreiche SSO-Lösungen an. Diese Dienstleister unterstützen Unternehmen bei der Implementierung und Verwaltung von SSO-Funktionen, um eine reibungslose Integration in die vorhandene IT-Infrastruktur zu ermöglichen.

Im Gegensatz zu den Web-3 SSO-Ansätzen basieren Blockchain-Technologien auf dezentralisierten Authentifizierungsverfahren. Diese sind durch ihre Natur, offen und transparent, da sich jede Transaktion oder Interaktion nachverfolgen lässt. Zusätzlich ermöglichen Wallets und kryptografische Schlüssel den Nutzern eine größere Kontrolle über ihre Daten. Ein fortschrittlicher State-of-the-Art im Web-3-Segment beinhaltet den Einsatz von ZKPs zur Steigerung von Datenschutz und Sicherheit. Diese ermöglichen die Verifikation, ohne Informationen preiszugeben, wodurch die Sicherheit auch über nicht vertrauenswürdige Netzwerke hinweg gewährleistet werden kann (Vgl. Journal und Journal, 2020).

In diesem Kontext ist zkSync eine führende Layer-2-Lösung, die ZKPs nutzt, um die Transaktionsgeschwindigkeit und Skalierbarkeit auf der Ethereum-Blockchain zu verbessern, ohne dabei Kompromisse bei der Sicherheit einzugehen (Vgl. Matter Labs, 2023).

Auch im Web-3-Bereich gibt es verschiedene Anbieter und Verfahren. Eine dieser Methoden ist die Authentifizierungslösung „Sign in with Ethereum", eine Open-Source Anwendung, die eine sichere und anonyme Anmeldung über Wallets ermöglicht. Für die Implementierung dieser Lösung ist jedoch eine individuelle Programmierung erforderlich, wobei der offene Quellcode eine hohe Anpassbarkeit an spezifische Anforderungen ermöglicht. Die Integration dieser Lösung in den Open-Source-Anbieter NextAuth.js ermöglicht die Einbindung in moderne Tech-Stacks wie Next.js.

Des Weiteren bieten auch Web-2-Anbieter wie Auth0 eine Integrationsmöglichkeit von Web-3-Diensten, beispielsweise die Möglichkeit, sich mit Ethereum anzumelden. Diese Integration erfordert weniger Programmieraufwand und ermöglicht Nutzern eine sichere Anmeldung mit geringerem Aufwand. Die Authentifizierung erfolgt durch das Signieren einer Nachricht in der eigenen Wallet, welche eine Nonce (ein einmaliger, zufälliger Wert) enthält. Im Anschluss wird die Nonce an die verifizierende Seite zurückgesendet, um zu bestätigen, dass die Wallet-Adresse dem jeweiligen Nutzer gehört.

Ein weiterer führender Anbieter für Authentifizierung im Web-3-Bereich ist ConnectKit. Hierbei handelt es sich um eine Bibliothek für React, die entwickelt wurde, um das Verbinden einer Wallet mit dezentrale Applikation (dApp) zu vereinfachen. Sie enthält Komponenten, die mit den meisten Wallet-Verbindungsmethoden und Blockchain-Netzwerken kompatibel sind (Vgl. Open Interfaces Ltd, 2024). Dies ermöglicht eine Verbindung zwischen Webseiten und verschiedenen Non-Custodial Wallets, wie Metamask und Ledger. ConnectKit ermöglicht nicht nur die Authentifizierung, sondern auch das Durchführen von Transaktionen. ConnectKit und ähnliche Dienste wie RainbowKit und WalletConnect er-

freuen sich bei der Entwicklung von Web-3-Seiten großer Beliebtheit, da sie in moderne Technologie-Stacks umfassend integriert sind (Vgl. Open Interfaces Ltd, 2024).

Im Gegensatz zu den Web-2-Diensten können die Authentizität und die Integrität einer Wallet im Web-3 mithilfe von sogenannten Know-Your-Customer (KYC)-Verfahren überprüft werden. Diese Überprüfung erfolgt durch verschiedene Proof-of-Humanity (PoH)-Anbieter wie beispielsweise Gitcoin. Dabei wird ein „Passport“ erstellt, der die Authentizität der Nutzer bestätigt. Zusätzlich müssen Nutzer mehrere „On-Chain“ (auf der Blockchain) Aktivitäten nachweisen, um zu bestätigen, dass es sich bei ihnen um echte Personen handelt und nicht um Sybil-Angriffe (Attacke auf Peer-to-Peer (P2P)-Netzwerke, durch die Erstellung falscher Identitäten). Die genannten Methoden tragen zu einer erhöhten Sicherheit und Authentizität im Web-3-Umfeld bei.

Anders als bei den aktuellen Web3-Protokollen, die in der Regel Passwörter oder Wallet-Anmeldungen (sog. „Wallet Sign-Ins“) zur Authentifizierung von Nutzern verwenden, bietet Worldcoin eine innovative Methode der Identifizierung: die Authentifizierung mittels biometrischer Daten, konkret durch einen Iris-Scan. Dabei wird die Iris des Nutzers gescannt und ein einzigartiger, kryptografischer Hash-Wert erzeugt. Dieser Hash-Wert wird mit dem Web-3-Wallet des Nutzers verknüpft und auf der Blockchain gesichert. Die Speicherung auf der Blockchain gewährleistet, dass die Daten nicht verändert oder manipuliert werden können, dank der inhärenten Sicherheits und Unveränderlichkeitsmerkmale der Blockchain-Technologie.

Worldcoin verwendet einen fortschrittlichen ZKP Mechanismus, um sowohl die Privatsphäre und Anonymität der Nutzer zu gewährleisten als auch ihre Echtheit als einzigartige Individuen zu verifizieren. In der Anwendung von Worldcoin bedeutet dies, dass eine Person ihre Identität verifizieren kann, ohne sensible Daten offenlegen zu müssen.

3.2 Use Case

Als Use Case soll ein Blockchain-SSO mit Hilfe von Worldcoin für ein Blockchain-basiertes Identitätsmanagement implementiert werden. Zunächst erfolgt ein Vergleich der Vor- und Nachteile verschiedener Integrationsmöglichkeiten. Besonderes Augenmerk liegt dabei auf der Identifizierung von Einzigartigkeiten, um die Authentizität der Nutzer sicherzustellen. Zusätzlich werden Maßnahmen zum Schutz vor Identitätsdiebstahl erörtert.

3.2.1 Vergleich

Web-2 Im Rahmen des Identitätsmanagements im Web-2 werden Datenbanken eingesetzt, die Identitäten verwalten. Dazu gehören Ausweisdokumente, E-Mails, Namen und andere personenbezogene Informationen. Der Zugriff auf diese Daten erfolgt in der Regel über die E-Mail-Adresse des Nutzers zusammen mit einem Passwort. Bei korrekter Eingabe ermöglicht das Passwort den Zugang zum jeweiligen Benutzerprofil. Die Sicherheit dieser Zugangsdaten hängt stark von der Komplexität des gewählten Passworts ab. Ein einfaches Passwort kann bei einem Hackerangriff leicht erraten werden, während ein komplexes Passwort deutlich mehr Schutz bietet.

Das zentralistische Design von Web-2-SSO, bei dem Nutzerdaten auf einem zentralen Ort im Netz gespeichert werden, birgt das Risiko, dass bei Datenlecks Nutzerdaten wie E-Mails und Passwörter durch Cyberangriffe im großen Stil gestohlen werden. Die Angreifer nutzen diese Informationen, um Zugang zu den Accounts der Betroffenen auf verschiedenen Plattformen zu erhalten. Das Risiko wird erheblich gesteigert, wenn ein Anwender dieselbe Passwortkombination auf mehreren Diensten verwendet. Dies zeigt eine Studie zum Passwortwiederverwendungsverhalten. Demnach sind etwa 35% der Benutzerkonten aufgrund von Passwortwiederverwendungen anfällig für Cyberangriffe (Vgl. Poornachandran et al., 2016).

Um Maßnahmen gegen solche Vorfälle zu ergreifen und den Nutzern Hinweise auf mögliche Datenverluste zu geben, gibt es Online-Plattformen wie „Have I Been Pwned“. Diese Plattformen informieren die Benutzer über Datenpannen und vergleichen die von ihnen eingegebenen E-Mail-Adressen mit kompromittierten Datenbankeinträgen. Dadurch können Anwender betroffene Passwörter aktualisieren oder deren Sicherheit erhöhen. Ein Beispiel, wie ein komprimierter Account auf „Have I Been Pwned“ angezeigt wird, ist in der nachfolgenden Abbildung 3.1 zu finden.

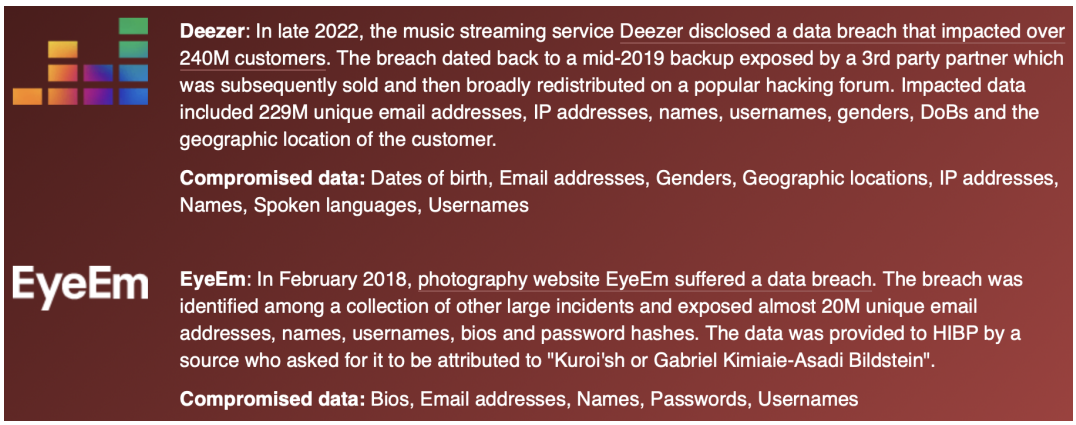


Abbildung 3.1: Die Grafik zeigt komprimierte Accounts bei Deezer und EyeEm
Quelle: Superlative Enterprises Pty Ltd, 2024, S. 1

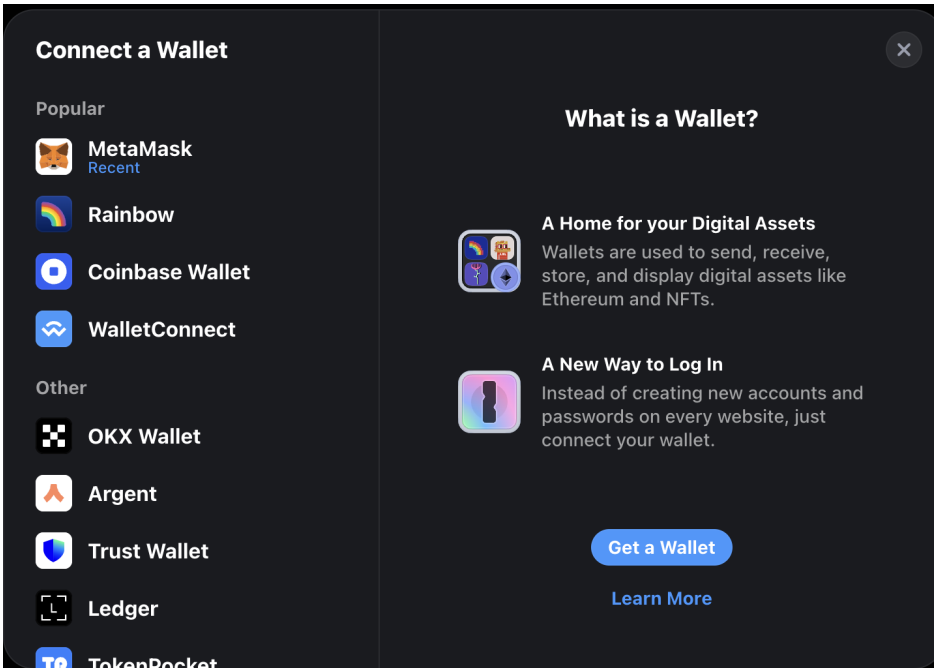
Ein alternativer Ansatz zur Steigerung der Sicherheit bei SSOs besteht darin, die Verifizierung durch 2FA, einzubeziehen oder Passkeys zu implementieren. Allerdings ist dies meist nur auf aktuellen Geräten umsetzbar (Vgl. Apple Inc., 2024). Bei der Anwendung von 2FA ist es erforderlich, dass der Nutzer seine Telefonnummer, E-Mail oder einen Code aus einer Authentifikator-App angibt, um den Zugriff zu verifizieren.

Passkeys vereinfachen die Identifikation im Rahmen der 2FA, indem sie die Notwendigkeit herkömmlicher Passwörter umgehen. Die Authentifizierung erfolgt stattdessen durch Auflegen des Fingers auf einen Fingerabdruckscanner oder durch die Verwendung von Gesichtserkennung via Kamera. Ein Nachteil dieses Systems ist jedoch, dass es ein relativ aktuelles Gerät voraussetzt. Ältere Modelle sind oft nicht mit den erforderlichen Technologien ausgestattet, um diese Methoden der Identifizierung zu unterstützen. So schreibt Apple auf ihrer Support Seite „[...]Zum Verwenden von Passkeys ist iOS 16, iPadOS 16, macOS 13 oder tvOS 16 (oder neuer) erforderlich.[...]“ (Apple Inc., 2024, S. 1).

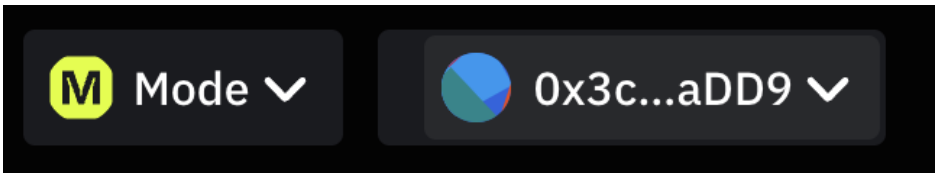
Web-3 Beim übergang von Web-2 auf Web-3 im Bereich des Identitätsmanagements ist die Art und Weise, wie Benutzeridentitäten verwaltet und geschützt werden grundsetzlich verschieden. Der Kern dieses Wandels ist weg von zentralen Datenbanken und Firmen hin zu dezentral gespeicherten Daten mithilfe von P2P Funktionalität der Blockchain.

So werden Zugriffsrechte „On-Chain“ gespeichert und ermöglichen den Nutzern zusätzlich die volle Kontrolle über ihre persönlichen Daten zu behalten und selbst zu entscheiden, welche Informationen sie mit Dritten teilen möchten.

Um Zugriff auf seine Daten zu bekommen gibt es verschiedenste Integrationsmöglichkeiten. Eine dieser ist die Verwendung von Self-Sovereign-Identity (SSI) bei dieser jeder Nutzer eine oder mehrere SSI besitzt. Diese Identitäten sind nicht an eine zentrale Autorität gebunden und ermöglichen eine selbstbestimmte Identitätsverwaltung. So kann man sich zum Beispiel mit der jeweiligen Wallet seiner Wahl auf Webseiten via ConnectKit anmelden. Hierbei wird der Public Key der Wallet, welcher „On-Chain“ gespeichert ist, als Identifier verwendet und dem Nutzer der Zutritt gewährt (Vgl. Mühle et al., 2018). Ein Beispiel einer solchen Anmeldung ist in folgender Abbildunge 3.2 zu sehen.



Wallet Anmeldefenster



Wallet erfolgreich verbunden

Abbildung 3.2: Beispiel einer Anmeldung per Wallet Connect auf der Website von Mode über die Mode-Chain
Quelle: Mode, 2024, S. 1

Ein weiterer Ansatz zur Integration ist die tokenbasierte Zugangskontrolle. Das Wallet, dass Zugang zu bestimmten Diensten benötigt, verfügt in diesem Fall über ein einzigartiges Non-Fungible-Token (NFT). Das NFT wird auf der spezifischen Blockchain, an die

jeweilige Wallet Adresse gesendet und steht ausschließlich dem betreffenden Nutzer zur Verfügung. Der entscheidende Aspekt hierbei ist der festgelegte „Identifier“ des NFTs, der seine Einzigartigkeit garantiert und sicherstellt, dass es kein zweites Mal existiert. Wenn ein Nutzer nun Zugriff auf einen Dienst beantragt, führt der Anbieter eine API-Abfrage durch, um zu überprüfen, ob eine Transaktion auf der Blockchain vorhanden ist, welche aufzeigt das das NFT, an die jeweilige Nutzer Wallet geschickt worden ist. Wenn dies bestätigt wird, erhält der Nutzer Zugang.

Es gibt verschiedene Methoden, um einen solchen NFT zu erlangen. Eine Möglichkeit ist der „Airdrop“(meist unaufgeforderte, in der Regel kostenlose Verteilung eines Tokens oder einer Kryptowährung), bei dem der Herausgeber NFTs an bestimmte Wallets verteilt, um ausgewählten Nutzern Zugang zu gewähren. Eine andere Variante ist das Prägen (Minten) des NFTs direkt auf der Plattform des Anbieters, vorausgesetzt, man hat sich zuvor erfolgreich angemeldet. In der nachstehenden Abbildung 3.3 ist ein illustrierendes Beispiel für eine Transaktion dieser Art auf der Blockchain zu sehen.

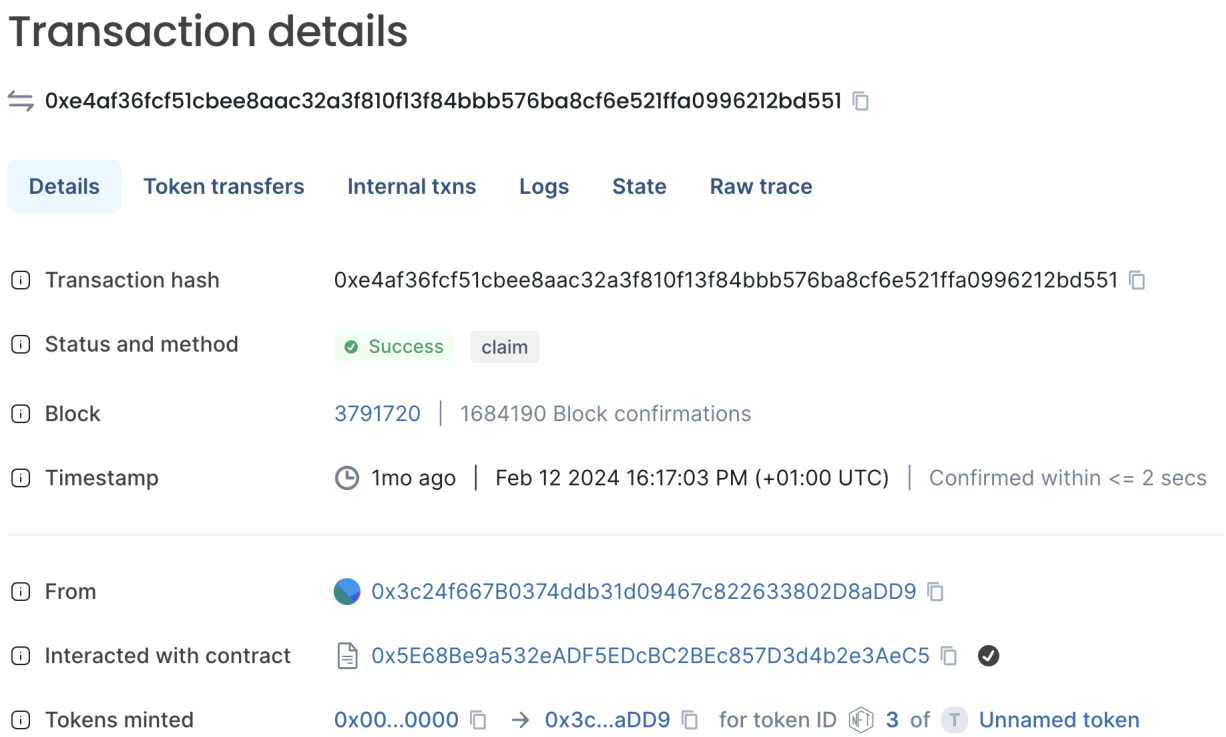


Abbildung 3.3: Die Abbildung zeigt die Transaktion eines NFT von einer Contract Adresse zu einem User
Quelle: Blockscout.com, 2024, S. 1

Eine Methode, die mehr Sicherheit bietet, ist das Hinzufügen einer Wallet zur „White-

list“(einer Liste auf der nur befugte Adressen stehen) bei einem Smart Contract. Smart Contracts sind ausführbare Programme, die auf der Blockchain laufen. Diese Strategie garantiert, dass ausschließlich die auf der „Whitelist“ eingetragene Wallet-Adresse und folglich der Nutzer, der sie kontrolliert Zugang erhält. Jedoch ist diese Vorgehensweise global betrachtet eher nachteilig, da sie den Zugriff auf eine begrenzte Anzahl von Wallet-Adressen begrenzen würde.

Aber auch in der Web-3-Welt gibt es Schwachstellen. Angreifer haben die Möglichkeit, bestimmte „kontaminierte“ Token an willkürliche Wallet-Adressen zu versenden. Diese Token imitieren durch ihre Bewegungen innerhalb der Blockchain scheinbar legitime Vermögenswerte und bergen somit ein Risiko. Wenn ein Anwender versucht, den Token auf einer dezentralisierten Tauschbörse (Dex) gegen andere Vermögenswerte einzutauschen, könnte der Angreifer durch den dem Token innewohnenden Smart Contract Zugriff auf alle Vermögenswerte in der betroffenen Wallet erlangen. Die potenziellen Auswirkungen eines solchen Übergriffs hängen vom Wert der digitalen Währungen ab, die sich im Wallet des Benutzers befinden, und könnten weitreichende Konsequenzen haben.

Im Gegensatz zu Web-2-Technologien, bei denen Passwörter und Schlüssel oft zentral von Firmen gespeichert werden, liegt beim Web-3 der Fokus auf der dezentralen Speicherung. Nutzer sind hierbei für die sichere Aufbewahrung ihrer privaten Schlüssel selbst verantwortlich. Diese Schlüssel gewähren uneingeschränkten Zugriff auf die entsprechenden digitalen Wallets und sollten daher niemals preisgegeben werden.

Ein besonders hohes Risiko besteht darin, dass Hacker sich als technischer Support ausgeben und die Herausgabe der Schlüssel fordern. Einmal in den falschen Händen, kann der Verlust des privaten Schlüssels durch einen persönlichen Hacker-Angriff nicht rückgängig gemacht werden, im Gegensatz zu traditionellen Banktransfers, bei denen fehlerhafte Überweisungen oft storniert werden können, ist der Verlust der Kontrolle über digitale Werte durch Diebstahl oder Betrug irreversibel, sodass die Werte vollständig auf den Angreifer übergehen.

Im folgenden Kapitel wird erläutert, wie Konten im Web-2 und Web-3 mittels biometrischer Daten auf globaler Ebene effektiv geschützt werden können.

3.2.2 Identifikation

Die Überprüfung der Einzigartigkeit von Personen ist entscheidend für zahlreiche Anwendungen wie Sicherheitssysteme, Wahlverfahren und Finanztransaktionen, bei denen Identitätsbetrug oder Doppelregistrierungen schwerwiegende Folgen haben können. Traditionelle Verifizierungsmethoden wie Online-Accounts, offizielle ID-Kontrollen, soziale Netzwerkanalysen und „Web of Trust“ stoßen bei der weltweiten Gewährleistung der Einzigartigkeit von Personen an ihre Grenzen, da Daten und Aktivitäten manipulierbar sind. Diese Methoden weisen Schwachstellen auf, die ihre Effektivität in Frage stellen. Einige dieser Schwachstellen sind im folgenden gelistet:

1. Bei Online-Konten ist es möglich, dass eine Person auf verschiedenen Plattformen mehrere Konten besitzt. Diese Konten sind nicht an eine bestimmte Person gebunden und können daher leicht auf andere übertragen werden. CAPTCHAs, die üblicherweise verwendet werden, um Bots zu verhindern, sind hier nicht immer wirksam, da sie von Menschen leicht überwunden werden können (Vgl. Worldcoin, 2024b).

2. KYCs sind auf globaler Ebene nicht inklusiv. Mehr als 50% der Weltbevölkerung haben keinen Ausweis, der digital überprüft werden kann. Außerdem ist es schwierig, eine KYC-Überprüfung so zu gestalten, dass die Privatsphäre gewahrt bleibt. Bei der Nutzung von KYC-Anbietern müssen sensible Daten an diese weitergegeben werden (Vgl. Worldcoin, 2024b).

3. Soziale Graphenanalysen ist nicht geeignet, da sie stark von der Fähigkeit abhängt, authentische zwischenmenschliche Beziehungen digital nachzuweisen. Es ist schwierig, weltweit einzigartige Identitäten effektiv zu verifizieren, da der Aufbau echter, vielfältiger sozialer Beziehungen zeitintensiv ist und in manchen Kontexten schwer nachweisbar sein kann. Die Einbeziehung von Institutionen wie Arbeitgebern oder Universitäten kann zu Komplexität führen. Es besteht die Gefahr, dass KI-Technologien gefälschte Profile erstellen können, die anscheinend authentische soziale Bindungen aufweisen. Dies würde die Grundannahme der Einzigartigkeit eines menschlichen Nutzers gefährden (Vgl. Worldcoin, 2024b).

4. Im Kontext von Web-3 wird das Konzept des „Web of Trust“ als Methode zur dezentralisierten Identitätsverifizierung durch Ausweisdokumente und Gesichtsscans angewendet. Allerdings ist diese Methode anfällig für Täuschungen durch Deepfakes, da hier keine Person die scans Überprüft sondern diese per Software verifiziert werden (Vgl. Worldcoin, 2024b).

Um sicherzustellen, dass es sich um die richtige Person handelt, setzt man im Web-2 sowie im Web-3 deshalb auf Biometrie. Worldcoin nutzt hierbei den Orb, um mittels Iris-Scanning die Einzigartigkeit einer Person zu bestätigen und somit den Nachweis der Menschlichkeit (Proof of Personhood) zu erbringen. Der Prozess beinhaltet eine Deduplizierung, um sicherzustellen, dass jeder Nutzer sich nur einmal verifizieren kann (Vgl. Worldcoin, 2024b).

Im Gegensatz zu Methoden wie Face ID oder Fingerabdruckscannern ermöglicht der Iris-Scan eine globale Implementierung. Dies wird in der nachfolgenden Abbildung 3.4 durch Vergleiche mit anderen Methoden verdeutlicht.

Biometric Modalities

	Fingerprint	Face	DNA	Iris
Privacy	Possible	Possible	Hard	Possible
Accuracy for global scale	Not enough	Not enough	Sufficient	Sufficient
Scalability	High	High	Low	High
Modification	Easy	Medium	Hard	Hard
Liveness detection	Hard	Good	Hard	Good

Abbildung 3.4: Die Abbildung vergleicht verschiedene Biometriemethoden mit dem Worldcoin Iris-Scan
Quelle: Worldcoin, 2024b, S. 1, Fig. 6

Der Iris-Scan ermöglicht einen Vergleich von 1:N gegen Milliarden von Datensätzen, wobei N die Gesamtzahl der zuvor verifizierten Nutzer ist. Während traditionelle Techniken wie Face-ID auf 1:1-Vergleiche mit lokal gespeicherten Daten beschränkt sind. Die folgende Abbildung 3.5 veranschaulicht dies genauer und zeigt den Vergleich von Face-ID und einem Iris-Scan.

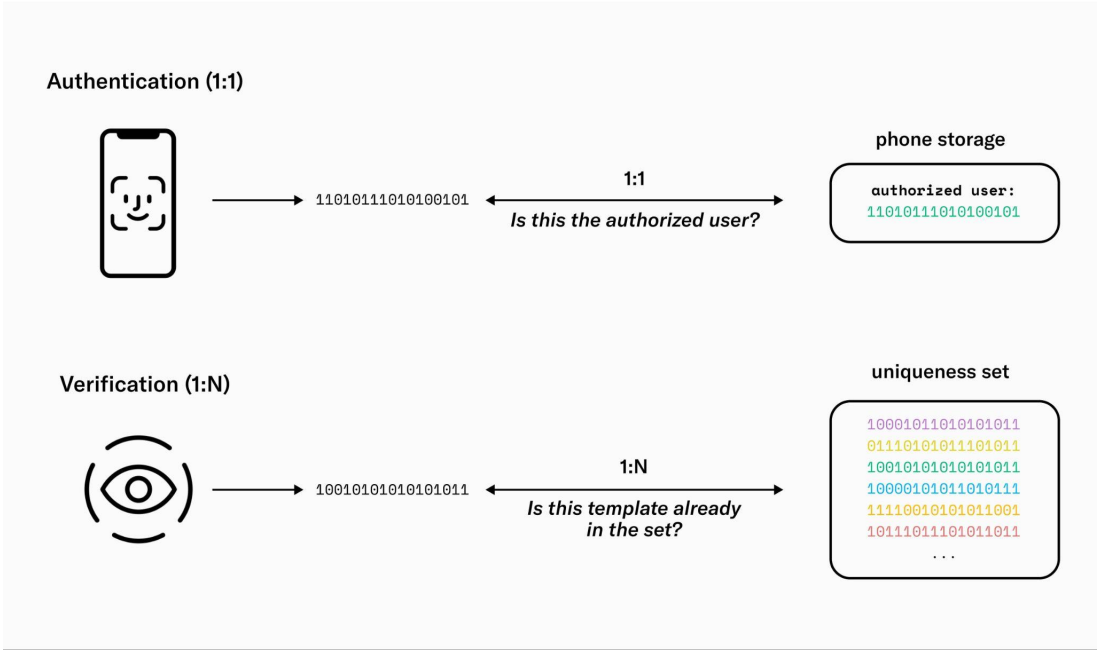


Abbildung 3.5: Die Abbildung vergleicht 1:1 mit 1:N auf globaler Ebene
Quelle: Worldcoin, 2024b, S. 1, Fig. 5

Diese Technologie zeichnet sich durch niedrige Falschübereinstimmungsraten aus, die eine Genauigkeit von mehr als eins zu 40 Milliarden erreicht, was einer Rate von $2,5 \times 10^{-14}$ (Vgl. Worldcoin, 2024b) entspricht, und bietet somit Sicherheit für globale Anwendungen. Aus diesem Grund basiert die biometrische Authentifizierung des Use Cases auf dieser Methode und ermöglicht einen Blockchain-basierten SSO für dezentrale Identitäten.

3.2.3 Schutz vor Identitätsdiebstahl

Angesichts der zunehmenden Verfügbarkeit von Künstlicher Intelligenz, die das Fälschen von Fotos oder Videos ermöglicht und sogar Deepfakes mit nur wenigen Fotos erstellen kann, gewinnt der Schutz vor Identitätsdiebstahl immer mehr an Bedeutung. Doch nicht nur KI-Technologie stellt eine Gefahr dar, auch Cyberangriffe auf Datenbanken, die wichtige Dokumente wie Ausweise oder persönliche Daten speichern, sind häufige Ziele für Cyberkriminelle. Durch solche Hacks erbeutete Daten können für illegale Aktivitäten missbraucht werden, wie beispielsweise das Bestellen von Waren unter der Identität einer betroffenen Person oder das Durchführen anderer identifikationspflichtiger Transaktionen im Internet.

Durch den Orb von Worldcoin, der den Iris-Scan durchführt, ist es nicht möglich, die Identität zu stehlen. Der Iris-Scan wird in einen Iris-Code umgewandelt, der in der nachfolgenden Abbilung 3.8 zu sehen ist. Dieser Code wird dann mit dem Public Key des Nutzers verbunden und als Transaktion auf die Blockchain geschrieben. Somit ist dieser Iris-Code nur dieser einzigen Wallet und somit dem Nutzer zugeordnet. Bei einem Hack braucht der Angreifer zusätzlich zugriff auf das Wallet mit dem Private Key des Nutzers um sich zu Authentifizieren.

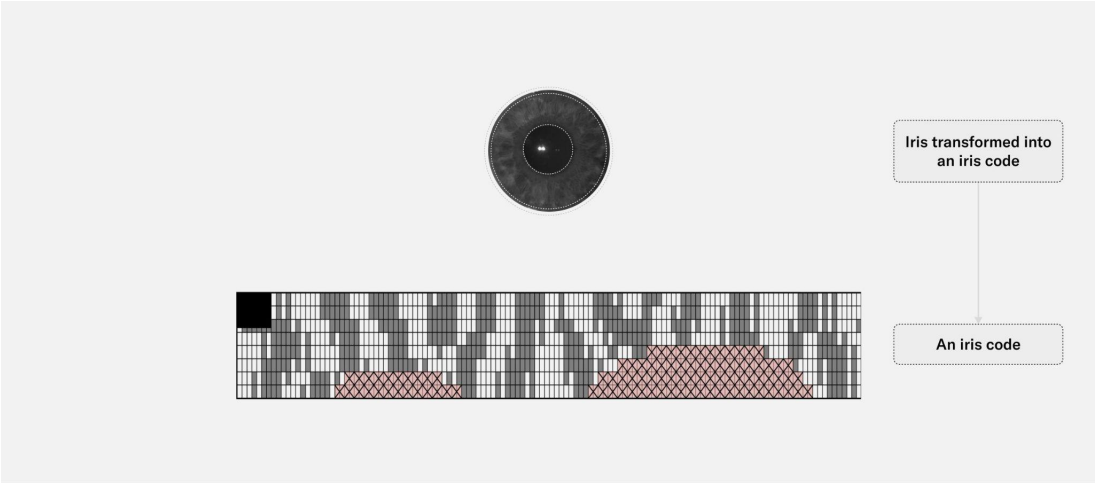


Abbildung 3.6: Die Abbildung zeigt die Umwandlung des Iris-Scan in den Iris-Code
Quelle: Worldcoin, 2024b, S. 1, Fig. 3.37

3.3 Showcase

In der Telefónica IEA soll ein Blockchain-basiertes Identitätsmanagement integriert werden. „Die Innovation Experience Area ist ein Inkubator für Innovationen, der Entscheidungsträgern und Partnern zeigt, was Technologie in verschiedenen Industrien bewirken kann“ (Telefónica Germany GmbH & Co. OHG, 2024, S. 1). Im Folgenden wird eine theoretische Umsetzung dieser Integration erarbeitet. Auf dieser theoretischen Grundlage soll anschließend eine mögliche praktische Umsetzung für die IEA entstehen.

3.3.1 Anforderungen

Die Anforderungen an ein Blockchain-SSO-System lassen sich in mehrere Etappen gliedern und können in drei Hauptkategorien unterteilt werden:

Anforderungen an den Use-Case

- Erste Etappe: Die Nutzer sollen sich nach erfolgreicher Anmeldung über ihr Wallet, das Worldcoin integriert, automatisch auf anderen Seiten anmelden können. Dies ermöglicht eine schnellere Authentifizierung und ein verbessertes Zeitmanagement.
- In der zweiten Etappe erfolgt die Verifizierung neuer Nutzer auf Blockchain-Ebene mittels des Orb von Worldcoin. Dieser scannt die Iris des Nutzers und verbindet den Iris-Code mit dem Nutzer-Wallet. Jeder Nutzer erhält hierbei eine eindeutige Wallet-Adresse.

Anforderungen an die Hardware

- In der Dritte Etappe wird ein Bildschirm oder Monitor vor Ort benötigt, auf dem die Anmeldeseite sichtbar ist.
- Vierte Etappe: Zusätzlich sind eine Maus und eine Tastatur erforderlich, um Eingaben tätigen zu können.

Anforderungen an die Software

- Fünfte Etappe: Für die Authentifizierung im Chrome-Browser ist die MetaMask Erweiterung notwendig, welche als Non-Custodial Wallet dient.

3.3.2 Storyline

Um zu verstehen, warum ein Blockchain SSO wichtig ist und welche neuen Möglichkeiten sich durch ein solches Projekt ergeben, wird das Projekt mit einer Storyline versehen. Hierfür gibt es mehrere Möglichkeiten, einige davon werden im Folgenden aufgezeigt, um die Wichtigkeit dieser Technologie zu untermauern.

1. Dienstleistungen: Wenn ein Unternehmen mehrere Anwendungen verwendet, die eine oder mehrere Anmeldungen erfordern, kann eine mögliche Integration Abhilfe schaffen. Auf diese Weise hat man mit einer Anmeldung Zugriff auf alle Anwendungen. Des Weiteren lässt sich der Zugriff auf bestimmte Services besser durch Smart Contracts beschränken. Nur eine im Contract hinterlegte Wallet-Adresse kann sich auf einem beliebigen Service anmelden. Sollte eine nicht vertrauenswürdige Wallet dies versuchen, würde eine Fehlermeldung an diese Wallet zurückgeschickt werden und der jeweilige User würde keinen Zugriff erhalten.

2. Authentifizierung: Blockchain SSO könnte nicht nur bei Anwendungen, sondern auch für andere Zwecke wie die Authentifizierung jeglicher Art verwendet werden. Eine Möglichkeit wäre der Zutritt zu Bürogebäuden oder beschränkten Abteilungen. So wäre sichergestellt, dass nur der autorisierte Nutzer Zugang erhält und dadurch die Sicherheit erhöht wird. Ein Nutzer würde einen QR-Code scannen und die Anmeldung mit seiner Wallet signieren, um Zugriff zu erhalten.

3. Digitale Identität: Blockchain SSO könnte nicht nur für Authentifizierungsdienste oder Anmeldungen verwendet werden. Durch den Iris-Scan und den zugehörigen Code wird die Identität des Nutzers auf der Blockchain gespeichert und kann in Zukunft beispielsweise für die Authentifizierung bei staatlichen Behörden, Autovermietungen, Universitäten oder Online-Zahlungsdiensten genutzt werden. Dadurch könnte der KYC-Prozess und dessen Schwachstellen, welcher im Kapitel 3.2.2 'Identifikation' behandelt wurde, abgelöst werden.

4. Verträge: Ein weiterer Anwendungsfall ist die Möglichkeit, Verträge online über die Blockchain abzuschließen. Durch den Iris-Scan wird sichergestellt, dass es sich um eine Person handelt. In Zukunft wäre es möglich, Verträge wie zum Beispiel einen neuen o2-Mobilfunkvertrag über eine mögliche Schnittstelle abzuschließen. Hierbei wäre die Identität des Käufers gewahrt, da kein Ausweisdokument vorgezeigt werden muss. Der Datenschutz wird durch den ZKP-Mechanismus gewährleistet, wodurch der Nutzer sicher eingeloggt wird und auf der Blockchain agieren kann. Dabei behält er die volle Kontrolle über seine Daten.

Auswahl der Storyline für die IEA

Problemstellung:

Im Kontext der IEA, einem Ort für die Präsentation und Interaktion mit neuester Technologie, besteht das Bedürfnis nach einem sicheren und effizienten Zugangssystem. Zusätzlich ist es wichtig, ein Umfeld zu schaffen, das potenzielle Sicherheitsverletzungen, wie Diebstahl oder unbefugten Zugriff, abschreckt. In diesem Kontext wird sich der Authentifizierungspunkt angeschaut.

Lösung:

Die Implementierung eines Blockchain-basierten SSO erfolgt über QR-Codes, welche die Besucher mit der Worldcoin-App scannen müssen. Das System nutzt Blockchain Technologie in kombienation mit dem Iris-Scan, um eine sichere, unveränderliche und verifizierbare Identitätsbestätigung durch biometrische Daten zu gewährleisten.

Funktionsweise der Lösung:

1. Die Registrierung erfolgt folgendermaßen: Die Teilnehmer registrieren sich einmalig in der Worldcoin App, indem sie ihre biometrischen Daten per Iris-Scan hinterlegen. Diese Daten werden zur Erstellung einer digitalen Identität verwendet, die in der Blockchain verifiziert und gespeichert wird.
2. Der Zugang zur IEA erfolgt mittels eines QR-Codes, welcher bei Ankunft durch den Besucher gescannt wird. Die Worldcoin-App führt daraufhin einen biometrischen Check durch und sendet eine Zugriffsanfrage an die Blockchain. Der Zugriff wird nur gewährt, wenn die Identität bestätigt wird und der Nutzer für den spezifischen Bereich autorisiert ist.
3. Die Blockchain dient hierbei der Abschreckung von Diebstahl und unbefugtem Zugriff, da jeder Zugangsversuch aufgezeichnet wird, wobei Zeitstempel, Wallet und WorldID des Nutzers erfasst werden. Die Transparenz und Nachverfolgbarkeit schrecken potenzielle Diebe ab, da ihre Identität im Falle eines Diebstahls oder eines anderen Sicherheitsvorfalls sofort bekannt wäre. Unbefugte Zugriffsversuche werden automatisch erkannt und protokolliert.

Präsentation in der IEA:

1. Im Rahmen einer interaktiven Demonstration wird gezeigt, wie Besucher durch das Scannen von QR-Codes sicher und schnell Zugang erhalten. Zudem wird aufgezeigt, wie im Falle eines unbefugten Zugriffs die Tür verschlossen bleibt.
2. Desweiteren wird in einer detaillierten Präsentation die technische Umsetzung erläutert. Anschließend sind die Vorteile der Blockchain-Technologie für Sicherheit und Datenschutz sowie die speziellen Sicherheitsfeatures, welche Diebstahl und unbefugten Zugriff abschrecken, darzustellen.

Diese Anwendungsmöglichkeiten sind nur ein kleiner Teil dessen, was möglich ist. Im Folgenden soll nun eine mögliche Integration ausgearbeitet werden.

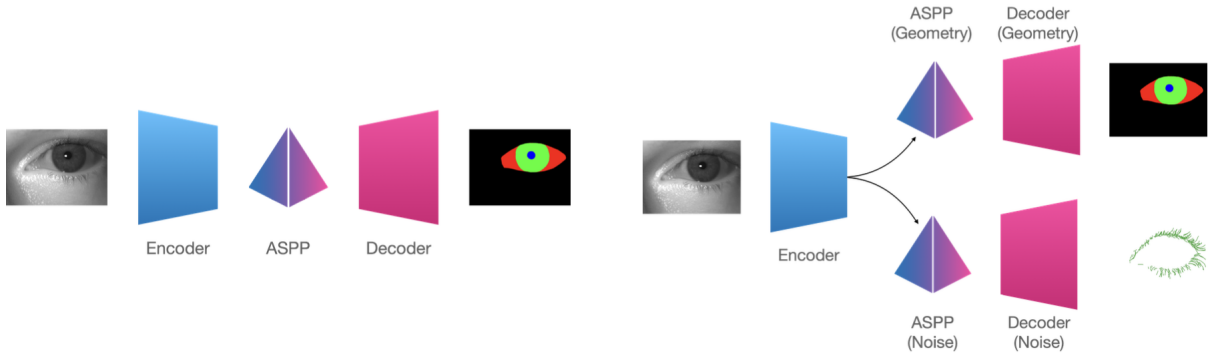
Die Worldcoin App in Kombination mit der MetaMask Browser Extension wird für die Integration verwendet. Bei einer möglichen Umsetzung gibt es zwei Varianten: eine Ausarbeitung mit Blockchain und eine ohne Blockchain. Letztere Variante unterstützt die in der

Arbeit voran gegangenen Sicherheiten wie den Iris-Scan nicht. Die nichtblockchainbasierte Variante baut auf einer Cloud-Lösung mit der Worldcoin API auf. Dennoch werden beide Varianten als mögliche Integration ausgearbeitet, um alle Möglichkeiten aufzuzeigen.

3.3.3 Blockchain-Umsetzung

Um einen Nutzer in die mögliche Umsetzung des SSO zu integrieren und den Service zugänglich zu machen, wird der Iris-Code des Nutzers benötigt, da auf der Blockchain nur Orb-verifizierte Nutzer Transaktionen oder Nachrichten signieren und sich somit einloggen können. Hierfür wird der Orb benötigt, welcher die Iris des Nutzers scannt. Bei diesem Vorgang werden beide Augen eingescannt und mithilfe von Deep-Learning-Algorithmen segmentiert und zu einem Iris-Code umgewandelt.

Zur Optimierung der Erkennung von Augenmerkmalen in der Iriserkennung wird eine angepasste Version der sogenannten DeepLabV3-Technologie verwendet. Diese Technik beinhaltet einen zentralen Baustein (Encoder), der Daten an zwei spezielle Auswerter (Decoder) weiterleitet. Der erste Auswerter konzentriert sich auf die Erkennung der Form und Struktur des Auges, also auf Teile wie den Augapfel, die Iris und die Pupille. Der zweite Auswerter ist für die Entfernung von Störungen im Bild zuständig, beispielsweise Wimpern (Vgl. Lazarski et al., 2006). Diese Architektur ermöglicht eine präzisere Segmentierung, indem sie Augenstrukturen von visuellem Rauschen unterscheidet und somit die Qualität der Bildanalyse verbessert. Die zugehörige Abbildung 3.7 veranschaulicht den angepassten Prozess.



(a) DeepLabV3 architecture. (b) Two-headed architecture.

Abbildung 3.7: Die Grafik zeigt den Vergleich von der DeepLabV3-Architektur gegen über der Modifizierten variante welche bei dem Orb zum Einsatz kommt
Quelle: Lazarski et al., 2006, S. 3.

Nach der Segmentierung der Iris Bilder wird aus diesen Merkmalen ein Iris Code erstellt. Dieser ist in nachfolgender Abbildung 3.8 Veranschaulicht.

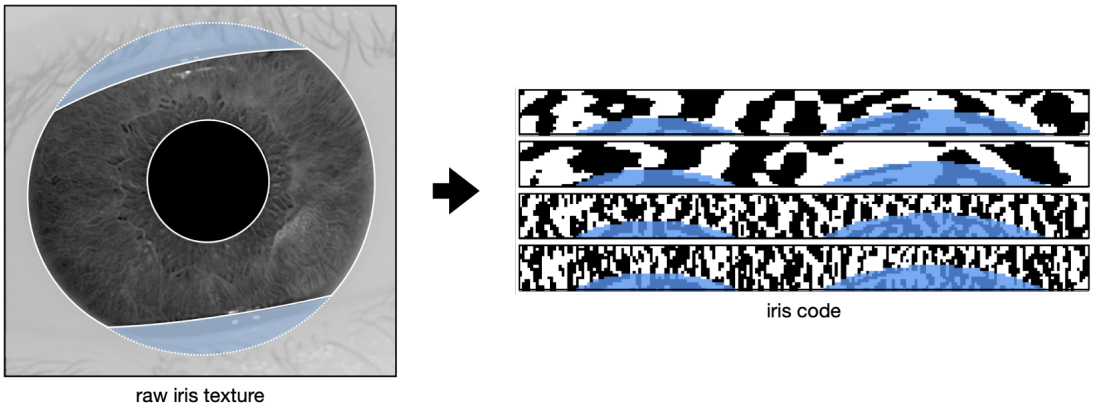


Abbildung 3.8: Die Grafik zeigt die Umwandlung der Iris Textur in den Iris Code
Quelle: Worldcoin, 2024b, S. 1, Fig. 24

Wenn der Scanvorgang ein positives Ergebnis liefert und der Iris-Scan als einzigartig identifiziert wird, wird der öffentliche Schlüssel des Wordcoin-Kontos in den Merkle-Tree integriert. Dabei wird der neu hinzugefügte Eintrag mit den bereits vorhandenen Einträgen abgeglichen. Wenn seine Einzigartigkeit festgestellt wird, wird die ID zusammen mit dem aktualisierten Merkle-Tree in die Blockchain eingetragen. Ein Beispiel hierfür findet sich in der Abbildung 3.9. Sie zeigt, wie Änderungen im World ID Router und im Identity Manager-Vertrag auf der Ethereum-Blockchain vermerkt werden.

```
> *** TreeChanged (index_topic_1 uint256 preRoot, index_topic_2 uint8 kind, index_topic_3 uint256 postRoot)
[topic0] 0x25f6d5cc356ee0b49cf708c13c68197947f5740a878a298765e4b18e4afdaf04
[topic1] 0x166e761330a724e1fafa5677d7054d5811c1fe84321328b9a8d4aa7a139eb27e
[topic2] 0x0000000000000000000000000000000000000000000000000000000000000000
[topic3] 0x177b45847e276ffe9ba62ec81c6dc6bc7ccd1c3b94b16addd6a6e0bf52fb0a70
```

Abbildung 3.9: Die Grafik zeigt Transaktionen des Identity Manager Contracts die neue Einträge zu den Identitäten hinzufügt
Quelle: Etherscan.io, 2024, S. 1

Nach erfolgreicher Veränderung des Merkle Trees wird der Proof of Personhood automatisch im jeweiligen Account der WorldCoin App gespeichert und kann nun zur Authentifizierung verwendet werden.

Für die Implementierung des Use-Cases wird der Smart Contract von Worldcoin auf der Optimism-Chain eingesetzt, da die Transaktionsgebühren auf der Ethereum-Blockchain

hoch sind und je nach Auslastung des Netzes im niedrigen zweistelligen oder hohen dreistelligen Bereich liegen. Die Optimism-Chain bietet geringere Netzwerkgebühren und eine schnellere Identitätsverifizierung als die Ethereum-Blockchain. Die Abbildung 3.10 zeigt die alternative Architektur zur Realisierung auf der alternativen Blockchain.

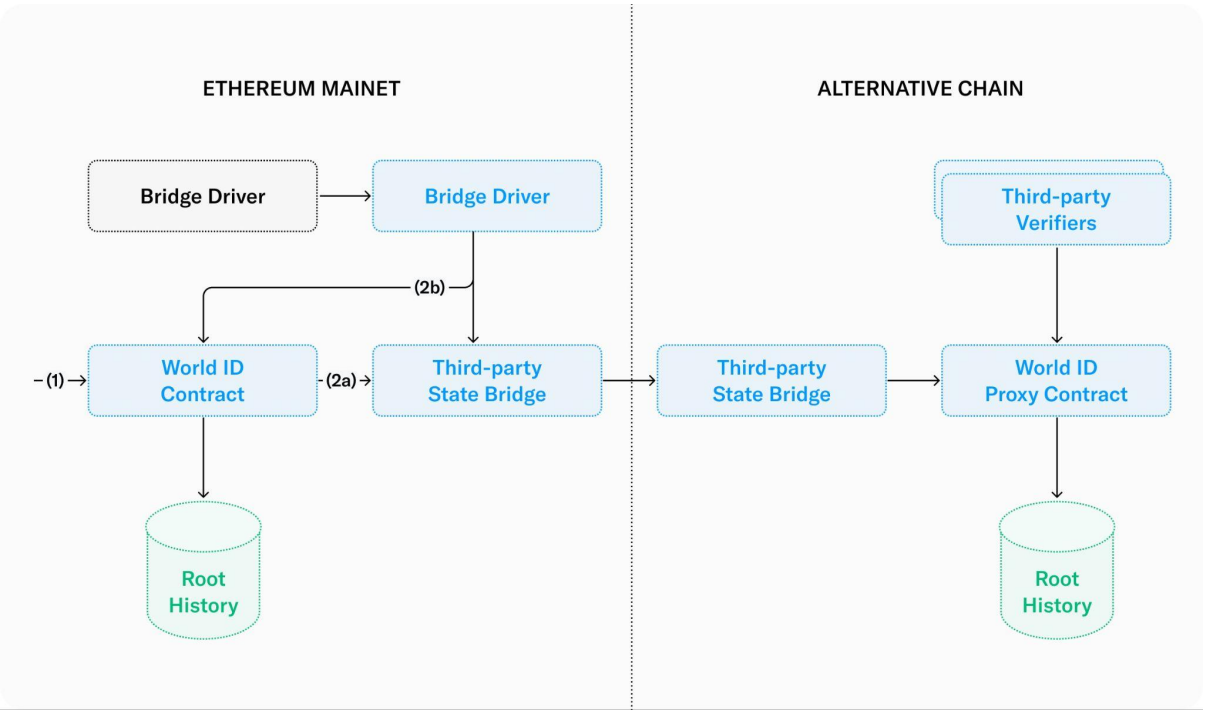


Abbildung 3.10: Die Grafik zeigt die Alternative verwendung von Chains außer Etherium
Quelle: Worldcoin, 2024b, S. 1, Fig. 33

Nach erfolgreicher Verifizierung mit dem Orb benötigt der Nutzer die MetaMask-Erweiterung aus dem Chrome Web Store oder auf mobilen Endgeräten aus dem App/Play Store. Die Verifizierung ist auch mit anderen Non-Custodial Wallets möglich. Non-Custodial Wallets sind digitale Geldbörsen, bei denen der Nutzer die vollständige Kontrolle über seine privaten Schlüssel behält, im Gegensatz zu Custodial Wallets, bei denen die Schlüssel von einer dritten Partei verwahrt werden. Wir beschränken uns jedoch auf MetaMask, da dies die am weitesten verbreitete Non-Custodial Wallet ist. Der Benutzer muss ein neues Wallet erstellen, um sein Benutzer-Wallet mit seinem Worldcoin-Konto zu verknüpfen. Während des Erstellungsprozesses werden dem Nutzer 12 nummerierte Wörter angezeigt, die den geheimen Recovery-Phrase darstellen.

Diese Phrase spiegelt das Passwort in der Web-2-Welt wider. Mit diesen Wörtern kann der Nutzer jederzeit von jedem Endgerät auf der Welt aus auf seinen Account zugreifen. Da-

her ist besondere Vorsicht geboten, wenn man diese Wörter aufbewahrt. Denn mit diesen Wörtern in der richtigen Reihenfolge kann jeder Zugriff auf diese Wallet-Adresse erhalten.

Sobald der Nutzer diese aufgeschrieben und bestätigt hat, erhält er eine Adresse auf der Blockchain, die seinen Account widerspiegelt. Diese wird dann verwendet, um die Identität zu verifizieren.

Der Nutzer hat nun die Möglichkeit, sich über MetaMask und die Worldcoin-App zu verifizieren. Um dies zu ermöglichen, muss eine Website erstellt werden, die eine Integration für Web-3-Wallets unterstützt. Für die Umsetzung des Use Cases wird Next.js verwendet, da es für die meisten Integrationen unterstützt wird.

Als Schnittstelle wird der Dienst von ConnectKit verwendet, einer React-Komponentenbibliothek, die verschiedene Wallets mit dApps oder Metaverse-Umgebungen verbindet.

Zunächst wird eine Konfiguration erstellt, die die verwendeten Chains enthält. In unserem Fall handelt es sich um Optimism und die Remote Procedure Call (RPC)-Schnittstelle, die standardmäßig von Worldcoin auf Infura oder Alchemy fällt. Im folgenden Code ist diese Konfiguration zu sehen.

```
const client = createClient(
        getDefaultClient({
                appName: APP_NAME,
                infuraId: process.env.INFURA_ID,
        })
)
```

Quelltext 3.1: Konfigurationsbeispiel Schmid, 2024, Commit-ID: 008d3d4

Nun muss diese Konfiguration noch an die App übergeben werden, um ConnectKit zu verwenden. Dies geschieht im folgenden Code.

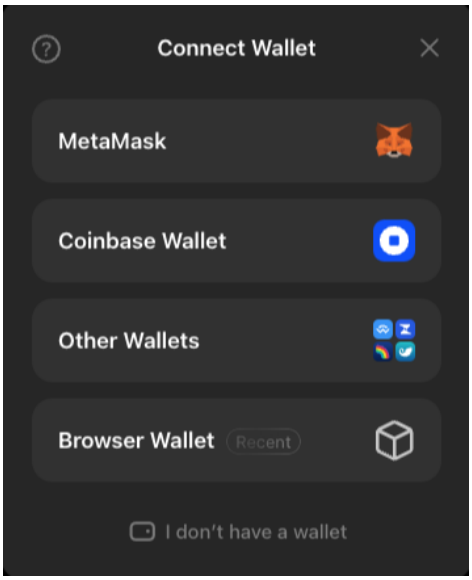
```
export default function App({ Component, pageProps }: AppProps) {
        return (
                <WagmiConfig client={client}>
                        <ConnectKitProvider>
                                <Component {...pageProps} />
                        </ConnectKitProvider>
                </WagmiConfig>
        )
```

```
}
```

Quelltext 3.2: Integrationsbeispiel Schmid, 2024, Commit-ID: 008d3d4

Nach erfolgreicher Integration kann man nun im Code mit der Blockchain interagieren. Um den Blockchain SSO zu ermöglichen, wird eine Authentifizierung benötigt. Diese erfolgt einerseits mit Worldcoin und andererseits mit MetaMask über eine digitale Signatur. Zunächst wird der Benutzer gebeten, sein Wallet zu verbinden.

Nach erfolgreicher Verbindung muss der von der Website generierte QR-Code mit der Worldcoin-App gescannt werden, um zu verifizieren, dass es sich um eine reale Person und nicht um einen Computer handelt. Hierfür muss der Benutzer einen Iris-Scan durchgeführt haben. Ein Beispiel für den Login ist in folgender Abbildung 3.11 dargestellt.



Anmeldefenster um sich mit dem MetaMask Wallet zu verbinden

Website genarierten QR code für die Worldcoin App verifizierung

Abbildung 3.11: Beispiel einer Anmeldung aus der Nutzer sicht für den Blockchain SSO auf der Projektwebsite
Quelle: Schmid, 2024, Commit-ID: 008d3d4

Nun muss die Authentifizierung auf der Blockchain durchgeführt werden. Im folgenden Abschnitt wird ein praxisnahes Beispiel für die Implementierung einer Authentifizierungsmethode in einer webbasierten Anwendung unter Verwendung der Blockchain-Technologie präsentiert. In der nachfolgenden Abbildung 3.12 wird ein vereinfachter Login-Prozess veranschaulicht.

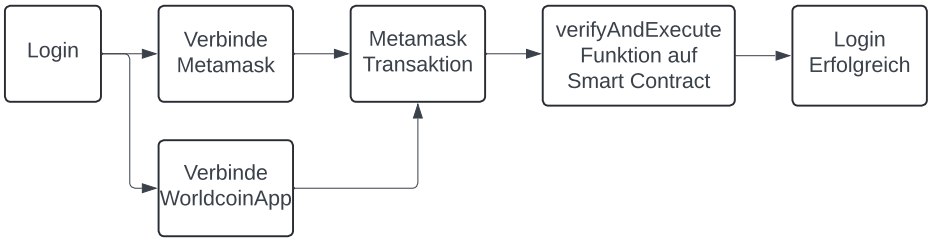


Abbildung 3.12: Schritte für einen Blockchain Login
Quelle: Eigene Darstellung

Nachdem der Nutzer sein MetaMask Wallet und die Worldcoin App, verbunden hat und Orb verifiziert ist, wird nun eine Transaktion an den Optimism Smart Contract gesendet. Dabei wird die „verifyAndExecute“ Funktion des Contracts aufgerufen, um zu überprüfen, ob der Nutzer existiert. Falls der Aufruf an den Contract erfolgreich ist, wird der Nutzer eingeloggt und somit authentifiziert.

Der vorliegende Code zeigt die technische Implementierung und ist ein Ausschnitt der fertigen Anwendung. Eine Erklärung der einzelnen Bausteine erfolgt im Anschluss an das Code-Beispiel.

```
1  const { config } = usePrepareContractWrite({
2          address: process.env.NEXT_PUBLIC_CONTRACT_ADDR as `0x${string}`,
3          abi: ContractAbi,
4          enabled: proof != null && address != null,
5          functionName: 'verifyAndExecute',
6          args: [
7                  address!,
8                  proof?.merkle_root ? decode<BigNumber>('uint256',
9                  proof?.merkle_root ?? '') : BigNumber.from(0),
10                 proof?.nullifier_hash ? decode<BigNumber>('uint256',
11                 proof?.nullifier_hash ?? '') : BigNumber.from(0),
12                 proof?.proof
13                 ? decode<[BigNumber, BigNumber, BigNumber, BigNumber,
14                 BigNumber, BigNumber, BigNumber, BigNumber]>(
15                 'uint256[8]',
16                 proof?.proof ?? ''
17                 )
```

```
                    : [
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                            BigNumber.from(0),
                    ],
          ],
})
```

Quelltext 3.3: Vertragsinteraktion Schmid, 2024, Commit-ID: 008d3d4

Die Komponente besteht aus der Zustandsvariable 'proof', welche das Ergebnis der Authentifizierung speichert. Die Authentifizierung erfolgt durch die IDKitWidget-Komponente von World-ID. Diese bietet eine Schnittstelle für Benutzer, um ihre Identität zu verifizieren, ohne persönliche Daten preiszugeben. Nach erfolgreicher Verifizierung ermöglicht der Code das Ausführen einer Smart Contract-Funktion (verifyAndExecute). Diese Funktion führt spezifische Logik für die jeweilige Anwendung aus und wird durch die Hooks „usePrepareContractWrite“ und „useContractWrite“ ermöglicht. Diese Hooks erlauben es, die für den Aufruf des Smart Contracts notwendigen Parameter vorzubereiten und die Transaktion auszuführen.

Die notwendigen Parameter für die „verifyAndExecute“ Funktion sind hierbei:

1. Benutzeradresse (address): Die Ethereum-Adresse des Benutzers, die aus der Wallet-Autorisierung stammt.
2. Merkle Root (proof?.merkle_root): Wenn vorhanden, wird der Wert der Merkle Root aus dem Authentifizierungsbeweis dekodiert zu einem BigNumber-Format. Andernfalls wird der Wert auf 0 gesetzt. Dies ermöglicht die Überprüfung, dass der Beweis Teil eines bekannten Datensatzes ist.
3. Nullifier Hash (proof?.nullifier_hash): Ein weiterer Teil des Authentifizierungsbeweises, der sicherstellt, dass jeder Beweis eindeutig ist und nicht wiederverwendet werden kann, ebenfalls dekodiert zu einem BigNumber-Format.

4. Beweis (proof?.proof): Ein komplexeres Datenfeld, das aus mehreren BigNumber-Werten besteht, welche zusammen den kryptographischen Beweis für die Authentifizierung darstellen.

Nach erfolgreicher Authentifizierung können Benutzer auf andere Dienste zugreifen, die das Blockchain-basierte SSO-System unterstützen, ohne sich erneut anmelden zu müssen. Die SSO-Funktionalität wird durch ein NFT oder persistente Tokens realisiert, die zwischen den Diensten geteilt werden.

Nach erfolgreicher Authentifizierung über den Smart Contract wird eine weitere Funktion im Contract aufgerufen, welche einen NFT an die Adresse sendet, die den Aufruf gemacht hat. Der NFT enthält den Authentifizierungsnachweis und die Adresse der autorisierten Person. Außerdem ist der NFT nicht transferierbar, sodass er nicht zwischen Konten hin und her bewegt werden kann. Dies stellt sicher, dass nur der autorisierte Nutzer Zugang bekommt. Dieser NFT dient als dauerhafter Nachweis der Identität und Berechtigung, um Zugang zu verschiedenen Diensten zu erhalten, ohne den Authentifizierungsprozess jedes Mal erneut durchlaufen zu müssen.

Im Anschluss muss auf den Seiten, die den SSO per NFT unterstützen möchten, noch eine Validierung des Zugriffs integriert werden. Der Nutzer verbindet sein MetaMask-Wallet auf der jeweiligen Seite und eine Funktion prüft dann, ob der verbundene Account dieses NFT hält. Sollte das der Fall sein, bekommt er Zugriff auf seine Account-Seite. Eine mögliche Abfrage ist im folgenden Code gegeben.

```
1  async function verifyAccess(userAddress) {
2      const contract = new ethers.Contract(
3          process.env.CONTRACT_ADDRESS,
4          [
5          function balanceOf(address owner)
6          public view returns (uint256)
7          ],
8          provider
9      );
10
11     const balance = await contract.balanceOf(userAddress);
12     return balance > 0;
13 }
```

Quelltext 3.4: NFT Überprüfung Schmid, 2024, Commit-ID: 008d3d4

Eine weitere Möglichkeit besteht darin, nach erfolgreicher Authentifizierung durch den Smart Contract ein JWT für den Benutzer zu generieren. Dieser Prozess kann über eine Authentifizierungsschnittstelle auf dem Server erfolgen. Das generierte Token wird an den Client zurückgesendet und dort im localStorage oder in einem Cookie gespeichert. Bei jedem Request an einen Dienst, der das SSO-System unterstützt, wird das Token im Authorization-Header mitgesendet. Dies geschieht, wie im folgenden Codebeispiel dargestellt:

```
fetch('api/protected-route', {
    headers: {
        'Authorization': `Bearer ${localStorage.getItem('authToken')}`
    }
});
```

Quelltext 3.5: Token Weitergabe Schmid, 2024, Commit-ID: 008d3d4

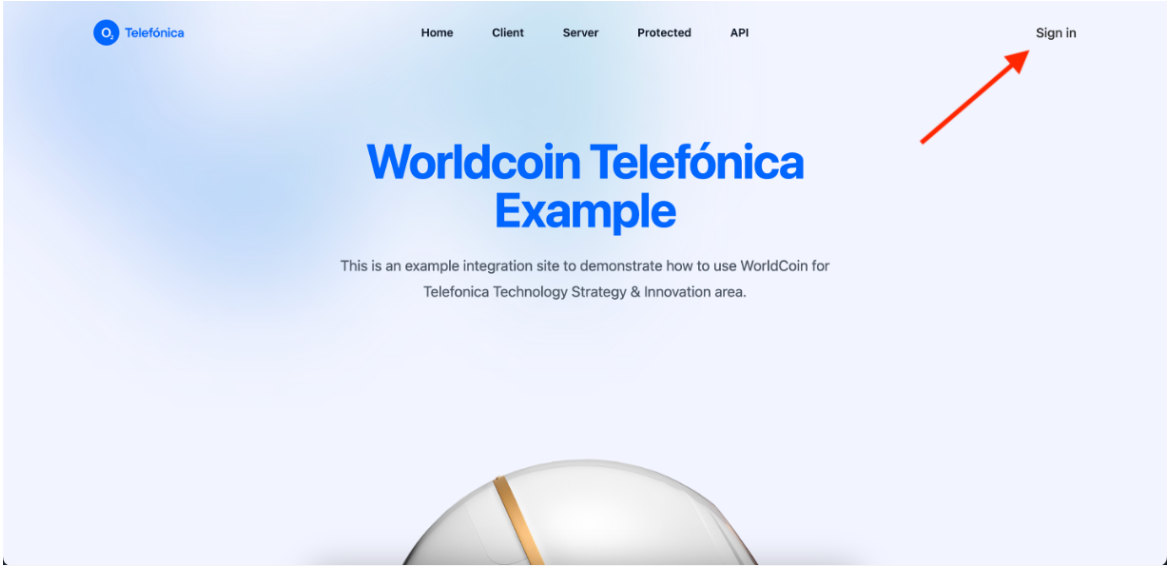
Anschließend muss jeder Dienst, der Teil des SSO-Systems ist, in der Lage sein, das JWT zu validieren. Dies beinhaltet die Überprüfung der Signatur und des Ablaufdatums des Tokens. Nachdem nun die mögliche Umsetzung des SSO per Blockchain Untersucht wurde soll nun auch auf eine Mögliche Umsetzung ohne Blockchain Technologie eingegangen werden, um Transparenz für alle Möglichkeiten zu schaffen.

3.3.4 Cloud-Umsetzung

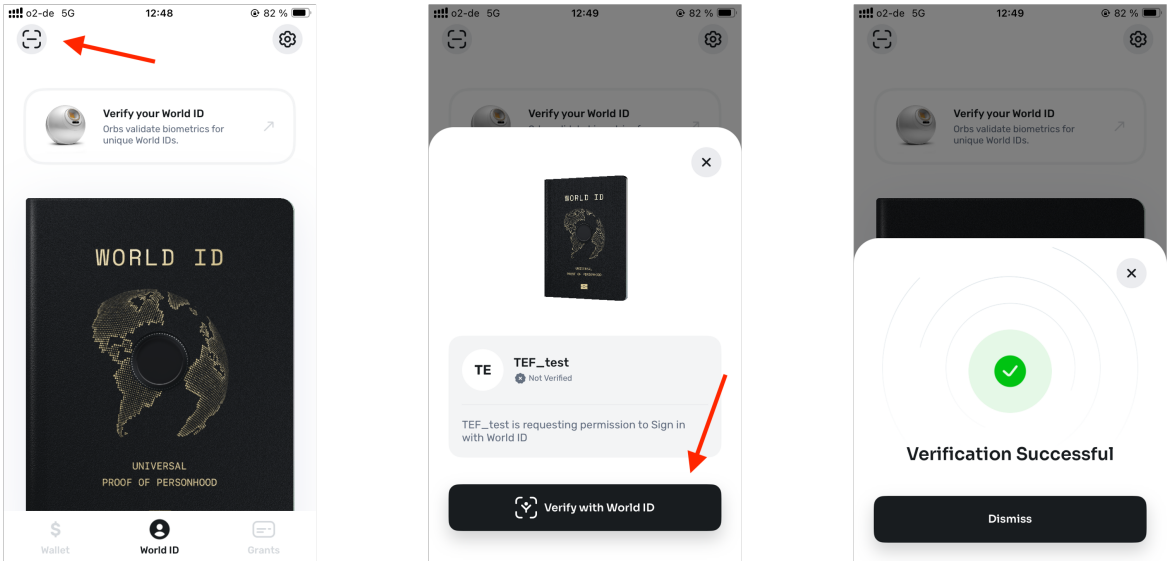
Bei dieser Umsetzung wird World-ID mit NextAuth.js genutzt, einer Bibliothek für Next.js-Anwendungen, um den Nutzer zu authentifizieren. NextAuth.js ermöglicht die Einrichtung der Authentifizierung in Next.js-Projekten. Dabei können Anmeldungen mit E-Mail, Passwort und Drittanbieter-Identitätsanbietern wie Google, Facebook, Twitter und anderen durchgeführt werden. Es unterstützt die Verwaltung von JWT-Token und die Handhabung von Sitzungen.

Um sich zu authentifizieren, muss der Nutzer die World-Id-App besitzen, auf der er ein Konto hat. Anschließend hat er die Wahl zwischen einem Iris-Scan oder einer späteren Durchführung. In diesem Fall kann der Nutzer auf einen Iris-Scan verzichten, da nun die Cloud-Variante und nicht die Blockchain-Variante aufgezeigt werden soll. Nach Abschluss des Registrierungsprozesses kann der Nutzer mithilfe der App einen QR-Code scannen,

der auf der jeweiligen Website angezeigt wird, um sich einzuloggen. In folgender Abbildung 3.13 sind die Schritte des Nutzerverhaltens dargestellt: Zunächst klickt der Nutzer auf „Sign in“, anschließend auf das Scan-Icon in der App, um den QR-Code zu scannen welcher nach dem Betätigen des Login-Buttons auf der Website erscheint, und verifiziert sich anschließend.



a) Cloud-Lösung programmierte Website mit integriertem Login-Button. Eigener Screenshot aus der programmierte Website



b) Worldcoin App aus sicht des Nutzers. Eigener Screenshot aus der Wordlcoin App

Abbildung 3.13: Beispiel einer Anmeldung aus der Nutzersicht für den Login auf der Projektwebsite
Quelle: a) Schmid, 2024, Commit-ID: 008d3d4

Zur Authentifizierung wird OpenID Connect (OIDC) genutzt. OIDC ist ein offenes Authentifizierungsprotokoll, das auf OAuth 2.0 basiert, mehr dazu im Grundlagenkapitel unter Single-Sign-On. Die folgende Abbildung 3.14 zeigt den Authentifizierungsablauf einer möglichen App-Integration.

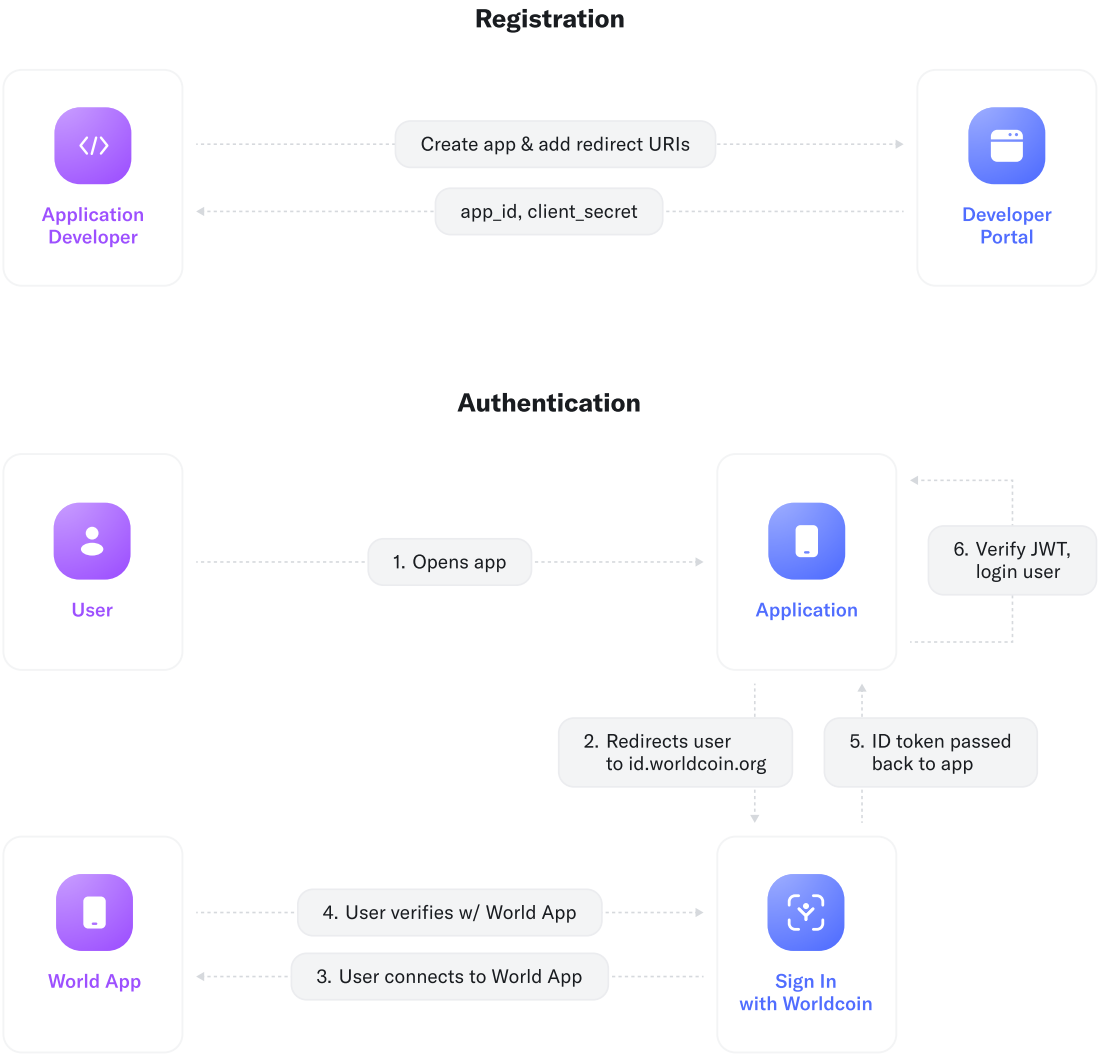


Abbildung 3.14: Die Abbildung zeigt den OCID Authentifizierungsablauf
Quelle: Worldcoin, 2024a, S. 1

Um Single Sign On umzusetzen, muss zunächst im Worldcoin Developer Portal eine App angelegt werden, die für den SSO genutzt werden soll. Anschließend werden die App-ID und das Client-Secret erstellt und in eine .env-Datei auf der jeweiligen NextAuth.js-Seite eingefügt, um sich zu identifizieren und eine Verbindung mit der angelegten App herzustellen. Außerdem muss im Developer-Portal eine Weiterleitungs-URL eingetragen

werden, um eingehende Authentifizierungsanfragen zu bearbeiten.

Diese Anfragen werden dann an id.worldcoin.org gesendet. Der Nutzer muss in seiner App die Authentifizierung bestätigen. Bei erfolgreicher Bestätigung wird ein ID-Token an die Applikation zurückgesendet. Dieser Token sagt dem Server der Applikation, dass der Nutzer berechtigt ist, Zugriff zu erhalten. Um diesen Vorgang nicht immer wiederholen zu müssen, wird gleichzeitig ein JWT-Token nach erfolgreicher Anmeldung erstellt. Dieser Token enthält den ID-Token, weitere Benutzerdaten sowie das Ablaufdatum, um den Benutzer einfacher einzuloggen.

Nachdem der JWT und die Session bestätigt wurden, kann man in der Applikation einfach über den Session-Status abfragen, welche Seiten und Funktionen nur nach dem Login sichtbar oder möglich sein sollen. Anschließend können die Nutzer an die jeweiligen authentifizierten Seiten weitergeleitet werden. Ein Beispiel für die Authentifizierungsanfrage, die von der Serverseite der Applikation stammt und das zugehörige Admin-JWT verwendet, ist im folgenden Code sichtbar.

```
1  {
2    id: "worldcoin",
3    name: "Worldcoin",
4    type: "oauth",
5    wellKnown: "https://id.worldcoin.org/.well-known/openid-configuration",
6    authorization: { params: { scope: "openid" } },
7    clientId: process.env.WLD_CLIENT_ID,
8    clientSecret: process.env.WLD_CLIENT_SECRET,
9    idToken: true,
10   profile(profile) {
11         return {
12         id: profile.sub,
13         name: profile.sub,
14         credentialType: profile
15         ["https://id.worldcoin.org/beta"]
16         .credential_type,
17         }
18     },
19 },
20 callbacks: {
21  async jwt({ token }) {
```

```
22    token.userRole = "admin"
23    return token
24   },
25  },
```

Quelltext 3.6: Authentifizierungsanfrage und JWT Schmid, 2024, Commit-ID: 008d3d4

Mit dieser Umsetzung kann nun in den Applikationen, die den SSO unterstützen sollen, das vorhandene JWT und somit die Session geprüft werden. Dadurch können einmalige Anmeldungen ermöglicht werden.

3.3.5 Key Performance Indicators

Um die beiden möglichen Umsetzungsvarianten bewerten zu können, werden im Folgenden sieben passende Key Performance Indikatoren (KPI) erläutert. Anhand dieser Indikatoren kann nach erfolgreichen Tests in Produktiv- oder Testumgebungen ein wirksamer Vergleich erzielt werden. Da die beiden in der Arbeit beschriebenen Umsetzungen bereits als Code verfügbar sind, jedoch noch nicht in Umgebungen getestet wurden, dienen diese KPIs lediglich als Anhaltspunkt für weitere Schritte nach erfolgreicher Implementierung und werden hier nur theoretisch aufgeführt.

- **Authentifizierungszeit:** Die Zeit, die benötigt wird, um einen Benutzer erfolgreich zu authentifizieren und ihm Zugriff zu gewähren.
  Ziel: Minimierung der Authentifizierungszeit, um eine schnelle Benutzererfahrung zu gewährleisten.
- **Fehlerrate bei der Authentifizierung:** Prozentsatz der fehlgeschlagenen Authentifizierungsversuche im Verhältnis zu den gesamten Authentifizierungsversuchen.
  Ziel: Reduzierung der Fehlerrate, um die Zuverlässigkeit des SSO-Systems zu erhöhen.
- **Anzahl der unterstützten Dienste:** Die Anzahl der verschiedenen Dienste oder Anwendungen, die das SSO-System integrieren und unterstützen.
  Ziel: Erweiterung der Kompatibilität mit verschiedenen Diensten, um die Vielseitigkeit des SSO-Systems zu erhöhen.
- **Skalierbarkeit des Systems:** Fähigkeit des Systems, mit einer zunehmenden Anzahl von Benutzern oder Anfragen effizient umzugehen.

Ziel: Gewährleistung einer robusten Skalierbarkeit, um Spitzenlasten und Wachstum zu bewältigen.

- **Sicherheitsverletzungen:** Anzahl der erkannten Sicherheitsvorfälle, die das SSO-System betreffen.
  Ziel: Minimierung der Sicherheitsvorfälle, um die Sicherheit der Benutzerdaten und des Zugriffs zu gewährleisten.
- **Durchschnittliche Uptime:** Prozentsatz der Zeit, in der das SSO-System ohne Ausfälle verfügbar ist.
  Ziel: Maximierung der Systemverfügbarkeit, um eine kontinuierliche Zugänglichkeit zu gewährleisten.
- **Integration und Deployment-Zeit:** Die benötigte Zeit, um das SSO-System in bestehende Systeme zu integrieren oder neue Dienste hinzuzufügen.
  Ziel: Effizienz bei der Integration und beim Deployment, um schnelle Anpassungen und Erweiterungen zu ermöglichen.

4 Zusammenfassung

Im Rahmen dieser Arbeit wurde die Entwicklung und Demonstration eines Blockchain-basierten SSO-Systems für Identitätslösungen im Bereich der Telekommunikation am Beispiel von Worldcoin erforscht. Ziel war es, zu untersuchen, wie Blockchain-Technologie effektiv in die Praxis umgesetzt werden kann, um die Sicherheit des Identitätsmanagements zu verbessern.

Im ersten Teil der Arbeit erfolgt eine Erläuterung grundlegender Konzepte der Blockchain-Technologie. Dies umfasst die Architektur von Blockchain, die Funktion von Smart Contracts sowie die Bedeutung von Merkle-Trees. Zudem werden verschiedene Authentifizierungsmethoden, einschließlich 2FA und SSO-Systeme, behandelt.

Der Hauptteil der Arbeit fokussiert sich auf die Entwicklung eines Blockchain-basierten SSO-Systems. Zu diesem Zweck wurde ein detaillierter Use Case für die Telekommunikationsbranche entwickelt und implementiert. Es konnte gezeigt werden, dass durch die Integration von Blockchain-Technologie und den Einsatz von biometrischen Verfahren wie dem Iris-Scan die Sicherheit signifikant erhöht werden kann. Die Verwendung von ZKP gewährleistet zudem den Datenschutz der Nutzer, da keine sensiblen personenbezogenen Daten gespeichert werden müssen.

Des Weiteren wurde die Entwicklung eines Cloud-basierten SSO-Systems in Kombination mit Worldcoin entwickelt, um eine einfachere Integration in bestehende Tech-Stacks zu ermöglichen und eine praktikable Alternative für Umgebungen darzustellen, in denen eine schnelle und einfache Implementierung gefordert ist.

Zusätzlich werden verschiedene Anwendungsszenarien erörtert, die in der IEA ausgestellt werden könnten. Im Rahmen der Untersuchung wurde die Authentifizierung für den Zutritt zu Bürogebäuden oder beschränkten Abteilungen als potenzielles Anwendungsszenario identifiziert.

4.1 Fazit

Die vorliegende Arbeit hatte zum Ziel, einen praxistauglichen Showcase zu entwickeln und zu demonstrieren, der veranschaulicht, wie Blockchain-Technologie effektiv für Identitätsmanagementlösungen genutzt werden kann. Da die bisherige Forschung theoretischer Natur ist und die praktischen Tests noch ausstehen, fokussiert das Fazit auf die erwarteten Vorteile und Herausforderungen der vorgestellten Technologien.

Erhöhte Sicherheit: Es wird prognostiziert, dass die Integration von Blockchain Technologie mit Iris-Scans eine signifikant höhere Sicherheitsebene gewährleisten wird. Diese Kombination soll den unbefugten Zugriff effektiv reduzieren, indem sie eine verlässliche und schwer zu fälschende Methode der Nutzerauthentifizierung nutzt.

Verbesserter Datenschutz: Die Anwendung von ZKPs innerhalb der Blockchain Implementierung zielt darauf ab, die Speicherung sensibler persönlicher Informationen zu vermeiden. Dadurch kann der Datenschutz erheblich verbessert und die Privatsphäre der Nutzer geschützt werden.

Komplexität und Nutzerverantwortung: Die zu erwartende Lösung wird voraussichtlich eine höhere Komplexität für die Nutzer mit sich bringen, da diese ihre privaten Schlüssel sicher verwalten müssen. Dies könnte höhere Anforderungen an das technische Verständnis der Nutzer stellen.

Regulatorische Bedenken: Ein kritischer Punkt, ist die vorübergehende Einschränkung der Aktivitäten von Worldcoin in Spanien durch die spanische Datenschutzbehörde (AEPD) (Vgl. Roush, 2024). Dies unterstreicht die Bedeutung von Datenschutzfragen und die Herausforderungen, die mit der Unmöglichkeit verbunden sind, einmal erteilte Zustimmungen zur Datennutzung zu widerrufen (Vgl. Roush, 2024). Ähnliche Herausforderungen könnten bei staatlich geplanten Projekten wie den Central Bank Digital Currencies (CBDC) auftreten und weisen auf die Notwendigkeit hin, die Balance zwischen technologischer Entwicklung und den Implikationen für Privatsphäre und individuelle Freiheiten zu bewerten (Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2024b).

4.2 Ausblick

Während die in dieser Arbeit präsentierten Lösungen theoretisch erhebliche Vorteile bieten, steht die Bestätigung dieser Vorteile durch praktische Tests noch aus. Zukünftige Forschungsarbeiten sollten sich daher auf die praktische Implementierung dieser Technologien konzentrieren und deren Optimierung vorantreiben. Zudem ist es von entscheidender Bedeutung, die öffentliche Wahrnehmung und Akzeptanz biometrischer Verfahren zu verbessern und potenzielle psychologische Barrieren, im Zusammenhang mit dem Iris-Scan abzubauen.

Literaturverzeichnis

Abdelhamid, M., & Hassan, G. (2019). Blockchain and smart contracts. *ACM International Conference Proceeding Series*, 91–95. https://doi.org/10.1145/3328833.3328857

Apple Inc. (2024). Verwenden von Passkeys zum Anmelden bei Apps und Websites auf dem iPhone - Apple Support (DE). https://support.apple.com/de-de/guide/iphone/iphf538ea8d0/ios

Blockscout.com. (2024). Mode transaction NFT Transfer. https://explorer.mode.network/tx/0xe4af36fcf51cbee8aac32a3f810f13f84bbb576ba8cf6e521ffa0996212bd551

Borde, H. S. D. O. (2022). An Overview of Trees in Blockchain Technology: Merkle Trees and Merkle Patricia Tries. https://www.researchgate.net/publication/358740207

Bundesamt für Sicherheit in der Informationstechnik. (2024a). BSI - Blockchain & Kryptowährung. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2024b, Februar). BSI - Presse - BSI veröffentlicht TR zu Digitalem Zentralbankgeld (CBDC). https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/Digitales_Zentralbankgeld_240208.html

Chainlink Foundation. (2023, November). Zero-Knowledge Proof (ZKP) — Explained | Chainlink. https://chain.link/education/zero-knowledge-proof-zkp

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. *PeerJ Computer Science*, *9*, e1705. https://doi.org/10.7717/PEERJ-CS.1705/TABLE-3

Etherscan.io. (2024). Worldcoin: World ID Identity Manager 2 | Etherscan. https://etherscan.io/address/0xf7134CE138832c1456F2a91D64621eE90c2bddEa#events

European Union. (2024, April). EU Digital Identity Wallet Pilot implementation | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation

Goldreich, O., Micali, S., & Wigderson, A. (1991). Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, *38*, 690–728. https://doi.org/10.1145/116825.116852

Gomzin, S. (2022). How to Choose the Wallet. *Crypto Basics*, 165–182. https://doi.org/10.1007/978-1-4842-8321-9_8

Google. (2023). Einmalanmeldung (SSO) | Cloud Architecture Center | Google Cloud. https://cloud.google.com/architecture/identity/single-sign-on?hl=de

Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2018). Blockchain-based Smart Contracts - Applications and Challenges. https://arxiv.org/abs/1810.04699v2

Journal, S., & Journal, U. (2020). International Journal of Innovative Technology and Exploring Engineering (IJITEE). https://doi.org/10.35940/ijitee.I6917.079920

Kaucher, A. (2018). Blockchain: Funktionsweise und Applikationsmöglichkeiten. https://www.h-brs.de/sites/default/files/2018-01-14_seminar_alexander_kaucher_final.pdf

Lazarski, W., Zieba, M., Jeanneau, T., Zillig, T., & Brendel, C. (2006). Two-headed eye-segmentation approach for biometric identification. https://arxiv.org/pdf/2209.15471

Matter Labs. (2023). zkSync | Scaling the Ethos and technology of Ethereum. https://zksync.io/

Mode. (2024). Mode App - The Modular DeFi L2 - Airdrop. https://bridge.mode.network/

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, *30*, 80–86. https://doi.org/10.1016/J.COSREV.2018.10.002

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

Open Interfaces Ltd. (2024). ConnectKit Introduction | Family Docs. https://docs.family.co/connectkit

Panuntun, L. H., Susanti, B. H., & Rosdiana, S. (2023). Performance Test of Hash Functions in Proof of Work Schemes in Blockchain. *Proceedings - 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, ICoCICs 2023*, 47–52. https://doi.org/10.1109/ICOCICS58778.2023.10277647

Poornachandran, P., Nithun, M., Pal, S., Ashok, A., & Ajayan, A. (2016). Password reuse behavior: How massive online data breaches impacts personal data in web. *Advances in Intelligent Systems and Computing*, *413*, 199–210. https://doi.org/10.1007/978-981-10-0419-3_24

Radha, V., & Reddy, D. H. (2012). A Survey on Single Sign-On Techniques. *Procedia Technology*, *4*, 134–139. https://doi.org/10.1016/J.PROTCY.2012.05.019

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A Usability Study of Five Two-Factor Authentication Methods. https://www.usenix.org/conference/soups2019/presentation/reese

Roush, T. (2024, März). Spanien vebietet Worldcoin - Forbes. https://www.forbes.at/artikel/spanien-vebietet-worldcoin.html#

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014, Februar). Final: OpenID Connect Core 1.0. https://openid.net/specs/openid-connect-core-1_0-final.html

Schlatt, V., Schweizer, A., Urbach, N., & Fridgen, G. (1990). Blockchain: Grundlagen, Anwendungen und Potenziale. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf

Schmid, C. (2024). Bachelor Project, Zugriff nur mit Berechtigung, Commit-ID: 008d3d4. https://github.com/chris017/Bachelor-Project-Web3

Sguanci, C., Spatafora, R., & Vergani, A. M. (2021). Layer 2 Blockchain Scaling: a Survey. https://arxiv.org/abs/2107.10881v1

Superlative Enterprises Pty Ltd. (2024). Have I Been Pwned: Check if your email has been compromised in a data breach. https://haveibeenpwned.com/

Telefónica Germany GmbH & Co. OHG. (2024). Innovation Experience Area | Telefónica Deutschland. https://www.telefonica.de/netze/innovation-experience-area.html#

Worldcoin. (2024a). OCID Architecture. https://docs.worldcoin.org/further-reading/oidc

Worldcoin. (2024b). Proof of Personhood (PoP) | Worldcoin Whitepaper. https://whitepaper.worldcoin.org/#proof-of-personhood-(pop)

Yang, X., & Li, W. (2020). A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security*, *99*, 102050. https://doi.org/10.1016/J.COSE.2020.102050