Hochschule RheinMain

Hochschule RheinMain
Fachbereich DCSM
Studiengang Master of Science - Informatik

Masterthesis

zur Erlangung des akademischen Grades
Master of Science - M.Sc.1.

Entwicklung eines dezentralen Identitätsmanagementsystems basierend auf Distributed Ledger Technology (DLT)

vorgelegt von **Robert DAVIDOFF**
Matrikelnummer 1108804
Innsbrucker Straße 34
55246 Mainz-Kostheim

am ++AbgabeDatum++

Referent: Prof. Dr. Philipp SCHAIBLE
Korreferent: Prof. Dr. Unbekannt UNBEKANNT

Kompiliert am 30.07.2023 um 18:08:17 - Erstellt mit LaTeX

Formales

Erklärung gem. ABPO, Ziff. 4.1.5.4 (3)

Ich versichere, dass ich die Bachelor-Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ort, Datum Unterschrift Studierender

Hiermit erkläre ich mein Einverständnis mit den im Folgenden aufgeführten Verbreitungsformen dieser Bachelor-Arbeit:

Verbreitungsform	**ja**	**nein**
Einstellung der Arbeit in die Hochschulbibliothek mit Datenträger	X	
Einstellung der Arbeit in die Hochschulbibliothek ohne Datenträger	X	
Veröffentlichung des Titels der Arbeit im Internet	X	
Veröffentlichung der Arbeit im Internet	X	

Ort, Datum Unterschrift Studierender

Abstract

Deutsch

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

English

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Hintergrund und Motivation

Das Internet hat sich als disruptive Technologie erwiesen, die die Art und Weise, wie Menschen kommunizieren, Informationen teilen und Geschäfte abwickeln, revolutioniert hat. Im Zeitalter des Internets spielt die Identität im virtuellen Raum eine wichtige Rolle. Normalerweise erfordert die Nutzung eines Online-Dienstes eine einmalige Registrierung und im Anschluss für jede Verwendung eine Anmeldung unter Angabe der zuvor festgelegten Login-Daten. Neben den Login-Daten werden meist auch personenbezogene Daten abgefragt. Wenn eine Nutzer nun X verschiedene Online-Dienste verwendet, so werden X mal identische Daten zur Person gespeichert (Adresse, Vorname, Nachname, Geschlecht, etc). Dieses Verhalten verursacht die Entstehung von Datensilos, die mit mehreren Problemen einhergehen. Nach [CS15] summieren sich die Kosten für die Identitätsdatenspeicherung in den UK auf knapp 4 Billionen Euro und in den USA hochgerechnet auf 22 Billionen Euro.

Ein weiteres Problem ist die Benutzerfreundlichkeit für den Anwender. Dieser ist gezwungen für jeden Online-Dienst sichere Login-Daten zu selektieren. Sind diese immer identisch, so stellt dies ein Sicherheitsrisiko dar, denn wenn einmalig ein Password kompromittiert ist sind alle anderen Dienste in Gefahr. Besser wäre demnach für jeden Online-Dienst unterschiedliche Login-Daten zu verwenden, was jedoch das Merken schwer macht.

Darüber hinaus stellt die Identitätsproblematik im Internet einen potentiellen Angriffsvektor dar. Cyberkriminelle können Schwachstellen in den Authentifizierungssystemen ausnutzen, um unbefugten Zugriff auf Konten zu erlangen oder Identitätsdiebstahl zu begehen. Dies birgt Risiken für die Privatsphäre und Sicherheit der Nutzer. In den USA werden 25 Personen pro Minute Opfer von Identitätsdiebstahl, wobei sich die durchschnittlichen Kosten für einen Online-Händler pro gestohlenem Datensatz personenbezogener/sensibler Daten auf 165 USD belaufen [CS15]. Im Vorjahr 2015 betrug die Menge 105 USD.

Statistiken [Sta12] zeigen, dass 82% der Unternehmen unter gefälschten Nutzerkonten leiden. Diese Fake-User verursachen nicht nur finanzielle Schäden, sondern können auch den Ruf eines Unternehmens schädigen. Darüber hinaus werden etwa 18% der Einkaufswagen aufgrund von Problemen mit den Anmeldedaten aufgegeben. Dies führt zu Umsatzeinbußen für Unternehmen und frustriert potenzielle Kunden.

Ein weiteres Problem ist, dass ein Nutzer im Status Quo keine Macht über seine Daten besitzt. Er ist stets davon abhängig dem Anbieter zu vertrauen, dass die Daten bei Anfrage gelöscht werden, sicher gespeichert sind, nicht ungefragt weitergegeben werden, etc. Ebenso ist keinerlei Transparenz darüber gegeben, wofür die Daten im Detail verwendet oder wofür sie gebraucht werden. Alles in einem besteht keine Autonomie für den Nutzer über die Daten, die er bei einem Online-Service angeben muss.

Angesichts dieser Herausforderungen ist die Notwendigkeit einer verbesserten Identitätsverwaltung im Internet offensichtlich. Es werden Lösungen erforscht, die auf dezentralen Identitätsplattformen und Blockchain-Technologie basieren. Solche Ansätze könnten dazu beitragen, die Sicherheit, Privatsphäre und Benutzerfreundlichkeit im Internet zu verbessern, indem sie eine effizientere und sicherere Möglichkeit bieten, Identitäten zu verwalten und zu überprüfen.

1.2 Zielsetzung der Arbeit

Als Ziel soll ein Konzept erarbeitet werden, dass dem Nutzer erlaubt Herrscher seiner Daten zu sein. Er soll eigenständig in der Lage seine Informationen hinzuzufügen, zu teilen, zu modifizieren und Berechtigungen zu erteilen/entfernen. Verwirklicht werden soll dieses Konzept mittels der DTL (Distributed Ledger Technology). Prototypisch soll eine Anwendung implementiert werden, die es erlaubt einem Nutzer seine Daten zu pflegen und Anfragen zu genehmigen/abzulehnen. Dabei sind unter anderem die Anforderungen: Sicherheit (Security), Kontrollierbarkeit, Übertragbarkeit und Skalierbarkeit.

Ein möglicher Anwendungsfall ist, dass ein Nutzer ein Profil anlegt mit Informationen, die er potentiell freigeben möchte (Bankinformation, Adresse, etc.). Diese werden so gespeichert, dass es - abgesehen für den Nutzer - unmöglich ist diese zu lesen. Nun kann eine Organisation oder Person (beispielsweise der Arbeitgeber um das Gehalt zu überweisen) Information anfragen. Diese Anfrage liegt dem Nutzer vor, welche er akzeptieren oder ablehnen kann. Passiert ersteres, so erhält der Anfragende die Informationen. Anderenfalls werden alle Informationen vorenthalten.

1.3 Forschungsfragen

Folgende Forschungsfragen werden in dieser Arbeit beantwortet:

- Ist es möglich Daten privat aber öffentlich zu speichern?
- Wie werden die Daten gespeichert? (Hash, Verschlüsselt, etc.)
- Welcher Mehrwert wird generiert für den User und die Online-Dienste?
- Kann das Problem der Fake-user hiermit gelöst werden?
- Welche Service-Level-Agreements könnten angegeben werden?
- Was passiert im Falle einer Kompromittierung? Recovery-Optionen?
- Wie sollen Informationen wieder ungültig gemacht werden? (Revokation)
  - Wieviel kostet der Betrieb?
  - Wie teuer sind solche Dienste in der Regel für den User/Online-Dienst?
- Wie kann sichergestellt werden, dass die Identität wirklich der Person zuzuordnen ist?
- Wie soll das Problem gelöst werden, dass man evtl. verschiedene Identitäten auf verschiedenen Plattformen verwenden möchte (Reddit-Account-Identität vs Online-Banking-Account)
- Blockchain-Forschungsfragen:
  - Welcher Consensus-Algorithmus ist am passensten für das entwickelte Identitätsmanagementsystem?
  - Soll eine private oder eine öffentliche Blockchain verwendet werden?
  - Wie und wo werden die privaten Schlüssel speichern?
  - Sollen 'permissioned' oder 'permissionless' Blockchains verwendet werden?
  - Sind Authentifikations-Graphen valide Lösungsansätze?
  - Können die Dokumente als NFT's gespeichert werden?
  - Welche Rolle spielen Zero-Knowledge-Proofs für die Entwicklung eines Identitätsmanagementsystems?

1.4 Aufbau der Arbeit

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen

Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 2

Grundlagen

2.1 Historie von Identitätsmanagementsystemen und deren Status Quo

Die Historie von Identitätsmanagementsystemen ist geprägt von verschiedenen Ansätzen, darunter die zentralisierte Identität (centralized Identity), die föderierte Identität (federated Identity), die nutzerzentrierte Identität (user-centric Identity) und die selbstbestimmte Identität (self-sovereign Identity). Die angegeben Identitätssysteme schließen sich nicht gegenseitig aus und vor allem die dezentrale Identität wird in modernen dezentralen Identitätsmanagementsystemen in Kombination mit seinen Vorgängern implementiert.

Zentralisierte Identitätssysteme waren lange Zeit vorherrschend, bei denen Identitätsinformationen in zentralen Datenbanken gespeichert wurden. Organisationen und Behörden kontrollierten den Zugriff auf diese Daten und verwalteten die Identitäten der Benutzer. Dabei authentifiziert sich ein Nutzer mit einer Nutzeridentifikation und einem Password. Dieser Ansatz führte jedoch zu Fragmentierung, Ineffizienz und möglichen Sicherheitsrisiken, wenn Nutzer nicht unterschiedliche Login-Daten für jeden Online-Dienst verwenden.

Mit der Einführung der föderierten Identitätssysteme wurde versucht, diese Probleme zu lösen. Hierbei können Benutzer über einen Identitätsanbieter, wie beispielsweise ein soziales Netzwerk oder ein Unternehmenskonto, auf verschiedene Dienste zugreifen. Der Identitätsanbieter fungiert als Vermittler und ermöglicht den nahtlosen Zugriff, ohne dass Benutzer separate Anmeldeinformationen für jeden Dienst bereitstellen müssen. Das Konzept hinter der föderierten Identität lautet *Single-Sign-On (SSO)*. Dabei gibt der Nutzer pro Sitzung seine Login-Daten einem *Identitätsanbieter* (Google, Facebook, etc), welcher im Gegenzug ein signiertes Token ausstellt, welches für kommende Logins verwendet wird. Die dabei verwendeten Technologien sind beispielsweise *SAML* [Loc+05] oder *OpenID Connect* [Id1e].

Die nutzerzentrierte Identität rückt den Benutzer in den Mittelpunkt des Identitätsmanagements. Bei diesem Ansatz behalten Benutzer die Kontrolle über ihre Identitätsdaten und können sie in einer sicheren Umgebung speichern. Sie können ihre Daten selektiv freigeben und verwalten, was zu mehr Privatsphäre und Kontrolle führt. Eine Implementierung hierfür ist BrowserID[Id1c]. Durchgesetzt hat sich diese Technologie jedoch nicht, da es an Akzeptanz und Integration durch Webseiten mangelte.

Die selbstbestimmte Identität oder Self-Sovereign Identity (SSI) stellt den neuesten Ansatz dar. Bei SSI behalten Benutzer die vollständige Kontrolle über ihre Identitätsdaten, indem sie kryptografische Schlüssel verwenden. Die Identitätsdaten werden dezentralisiert und auf der Blockchain oder anderen verteilten Systemen gespeichert. Benutzer können selektiv Informationen freigeben und verifizieren, wodurch ihre Privatsphäre und Sicherheit gestärkt werden.

2.2 Self-Sovereign-Identity

2.2.1 Das Konzept hinter SSI

Das Konzept der Self-Sovereign Identity [TR17] basiert auf den folgenden Prinzipien:

1. Benutzerkontrolle: Der Benutzer hat die ultimative Kontrolle über seine Identität und die damit verbundenen Daten. Der Benutzer kann bestimmen, welche Informationen er teilen möchte, mit wem und zu welchen Bedingungen.

2. Dezentralisierung: Die Identitätsdaten sind nicht an eine zentrale Institution oder Datenbank gebunden. Stattdessen werden sie dezentral auf verschiedenen Plattformen, Geräten oder Blockchains gespeichert. Der Benutzer hat die Möglichkeit, seine Identitätsdaten an einem sicheren Ort seiner Wahl zu speichern.

3. Interoperabilität: SSI strebt nach Interoperabilität zwischen verschiedenen Identitätsplattformen und -systemen. Das bedeutet, dass Identitätsdaten zwischen verschiedenen Diensten und Organisationen ausgetauscht und verifiziert werden können, ohne dass eine zentrale Instanz benötigt wird.

4. Vertrauensmodelle: SSI nutzt kryptografische Technologien, wie digitale Signaturen und Blockchain, um die Integrität und Vertrauenswürdigkeit von Identitätsdaten zu gewährleisten. Es ermöglicht auch das Prinzip der Verifizierung von Ansprüchen, bei dem die Authentizität bestimmter Daten von anderen Parteien bestätigt werden kann.

5. Datenschutz und Privatsphäre: SSI legt großen Wert auf Datenschutz und Privatsphäre. Der Benutzer hat die Kontrolle darüber, welche Informationen freigegeben werden und welche nicht. Es ermöglicht auch selektive Offenlegung, bei der

nur die notwendigen Informationen für einen bestimmten Zweck oder Kontext offengelegt werden.

Das Ziel von Self-Sovereign Identity ist es, die Verwaltung von Identitätsdaten für Benutzer transparenter, sicherer und benutzerzentrierter zu gestalten. Es bietet die Möglichkeit, Identitätsinformationen nahtlos zwischen verschiedenen Diensten und Organisationen zu nutzen, während die Kontrolle über die eigenen Daten in den Händen des Benutzers bleibt.

2.2.2 Identität

Im Kontext der Self-Sovereign Identity (SSI) gibt es verschiedene Konzepte, die verschiedene Aspekte der Identität und Kontrolle berücksichtigen. Zwei solcher Konzepte sind die *Weak/Nym Identity* und die *Partial/Strong Identity*.

Die Weak/Nym Identity bezieht sich auf eine Identität, die nur begrenzte Informationen über den Benutzer enthält. Bei dieser Identität wird bewusst darauf verzichtet, persönliche Informationen oder Details preiszugeben, die zur Identifizierung des Benutzers verwendet werden könnten. Stattdessen wird ein Pseudonym oder ein Alias verwendet, um die Privatsphäre des Benutzers zu schützen. Die Weak/Nym Identity ermöglicht es dem Benutzer, Transaktionen durchzuführen und Dienste zu nutzen, ohne seine wahre Identität preiszugeben.

Im Gegensatz dazu bezieht sich die Partial/Strong Identity auf eine Identität, die umfassendere Informationen über den Benutzer enthält. Diese Identität kann persönliche Daten wie Name, Adresse, Geburtsdatum und andere relevante Informationen enthalten. Die Partial/Strong Identity ermöglicht eine genauere Identifizierung und Authentifizierung des Benutzers, was in einigen Situationen erforderlich sein kann, beispielsweise bei behördlichen Anforderungen oder bei Zugang zu sensiblen Diensten. Die Partial/Strong Identity erfordert eine sorgfältige Verwaltung der Identitätsdaten, um sicherzustellen, dass sie sicher und geschützt bleiben.

Beide Identitätskonzepte haben ihre eigenen Vor- und Nachteile in Bezug auf Datenschutz, Sicherheit und Benutzerkontrolle. Die Entscheidung für eine bestimmte Identität hängt von den individuellen Anforderungen, dem Kontext und den Präferenzen des Benutzers ab. SSI strebt jedoch nach Flexibilität und Wahlfreiheit für Benutzer, um die Identität zu wählen, die ihren Bedürfnissen am besten entspricht und gleichzeitig die Sicherheit und den Schutz ihrer Daten gewährleistet.

In den folgenden Kapiteln wird in der Konzeption und Implementierung ein Minimum an Daten preisgegeben, also eine schwache Identität. Jedoch werden auch Anwendungsfälle berücksichtigt, wo Informationen zur Identität benötigt werden

2.2.3 Technische Grundlagen

Um das Konzept der Self-Sovereign Identity (SSI) aus technologischer Sicht zu verstehen und anzuwenden, sind folgende Kernkonzepte erforderlich [Id1d] [Ish20]:

1. Trust-Registries: Diese dienen als gemeinsame und vertrauenswürdige Aufzeichnung bestimmter Informationen. Mit anderen Worten fungieren sie als 'Vertrauensebene' und 'einzige Quelle der Wahrheit'. Eine mögliche Realisierung einer Trust-Registry ist ein dezentraler Speicher (Distributed Ledger), der alle Aktivitäten in Transaktionen speichert.

2. Kryptografische Schlüssel: Diese übertragen die Kontrolle über digitale Identitäten und ermöglichen grundlegende Funktionen wie Verschlüsselung und Authentifizierung. Hierbei handelt es sich um klassische private/öffentliche Schlüsselpaare, die im Falle von der Bitcoin-Blockchain 48 Byte / 256 Bit lang sind [Id1b] und dem Verschlüsseln/Entschlüsseln/Signieren von Daten dienen.

3. Dezentrale Identifikatoren (DIDs): DIDs sind globale und einzigartige Identifikatoren, die keine zentrale Register zur Speicherung benötigen. Sie unterscheiden sich zu UUIDs in dem Sinne, dass DIDs auf sog. DID-Documents zurückzuführen sind und mit kryptographischen Mechanismen Eigentumsverhältnisse zeigen. DID's sind aufgebaut wie folgt:
   "did:"⟨Methodenname⟩":"⟨methodenspefizische-ID⟩
   Beispiel:"did:btcr:abcd-1234-wxyz:789"
   Dabei zeigt ein DID immer auf ein DID-Dokument, welches im JSON-Format Metadaten wie öffentliche Schlüssel oder Authentifizierungsmethoden beinhaltet.

   Aussehen tut ein DID-Document wie folgt:

```
1  {
2          "id": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9JPhl_xLDI9Nfk38
               w5w",
3          "@context": [
4          "https://www.w3.org/ns/did/v1",
5          {
6                  "@base": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ9
                       JPhl_xLDI9Nfk38w5w"
7          }
8          ],
9          "service": [
10         {
11                 "id": "#linkedin",
12                 "type": "linkedin",
13                 "serviceEndpoint": "linkedin.com/in/henry-tsai-6b8
                       84014"
14         },
15         {
16                 "id": "#github",
17                 "type": "github",
18                 "serviceEndpoint": "github.com/thehenrytsai"
19         }
20         ],
21         "verificationMethod": [
```

```
        {
                "id": "#someKeyId",
                "controller": "did:ion:EiClkZMDxPKqC9c-umQfTkR8vvZ
                    9JPhl_xLDI9Nfk38w5w",
                "type": "EcdsaSecp256k1VerificationKey2019",
                "publicKeyJwk": {
                        "kty": "EC",
                        "crv": "secp256k1",
                        "x": "WfY7Px6AgH6x-_dgAoRbg8weYRJA36ON-
                            gQiFnETrqw",
                        "y": "IzFx3BUGztK0cyDStiunXbrZYYTtKbOUzx16
                            SUK0sAY"
                }
        }
        ],
        "authentication": [
        "#someKeyId"
        ]
}
```

Es ist zu erkennen, dass dieses DID-Document festlegt für welche Services dieses Dokument die Authentifikation definiert (in diesem Falle LinkedIn und Github). Unter 'verificationMethod' wird der Typ ËcdsaSecp256k1VerificationKey2019ängegeben, was einer Public-Key-Authentifikation entspricht, welche Elliptic-Curve-Kryptographie verwendet.

4. Verifizierbare Nachweise (VCs): VCs sind digitale Identitätsdokumente, die von jedem auf ihre Gültigkeit, Integrität, Authentizität und Herkunft hin überprüft werden können. Sie beinhalten sog. *Claims*, also Informationen/Behauptungen über die Entität (beispielsweise den Namen, Geburtsdatum, etc.). Wichtig ist, dass VCs aus Datenschutz- und Compliance-Gründen niemals auf einer Blockchain gespeichert werden. Ein VC kann wie folgt aussehen:

```
{
        "@context": [],
        "id": "e9ea3429-b32f-44ad-b481-b9929370bb90",
        "type": [ "VerifiableCredential", "ExampleCredential" ],
        "issuer": { "id": "did:btcr:2d28bb79-87a9-4224-8c63-d28b29
            716b67" },
        "issuanceDate": "2022-01-01T00:00:00Z",
        "credentialSubject": {
                "id": "did:example:7564cb9c-165c-4857-a887-bfc2460
                    af867",
                "birth_date": "1970-01-01"
        },
        "expirationDate": "2023-01-01T00:00:00Z",
        "proof": {<SignatureOfIssuer>}
}
```

Es ist zu erkennen, dass in dem VC unter anderem Claims ('credentialSubject' genannt) enthalten sind (in diesem Falle das Geburtsdatum), der Issuer des VC, ein Auslaufdatum und ein 'Proof', also eine digitale Signatur des Issuer's, um die Integrität des VC's zu überprüfen.

5. Wallets: Wallets speichern unsere Schlüssel und VCs und ermöglichen die Verwaltung und Nutzung unserer digitalen Identitäten und Daten über benutzerfreund-

liche Anwendungen.

Diese Kernkonzepte bilden die Grundlage der SSI-Technologie. Sie ermöglichen es Einzelpersonen, die Kontrolle über ihre digitalen Identitäten zu haben, verifizierbare Nachweise sicher zu teilen und vertrauenswürdige Interaktionen mit anderen durchzuführen.

Das grobe Zusammenspiel der Komponenten sieht dabei wie folgt aus:

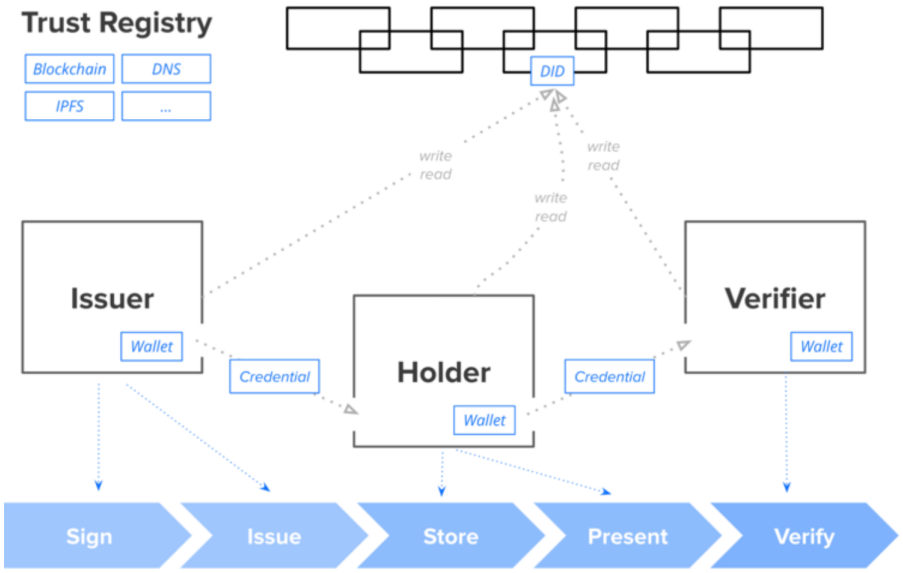

Abbildung 2.1: Zusammenspiel von Issuer, Holder und Verifier

Es ist zu erkennen, dass sowohl Issuer, Holder und Verifier Eigentümer von einem Wallet sind. Der Issuer (Beispielsweise eine Bank) stellt VC's aus, die der Holder (Beispielsweise eine Privatperson) in seinem Wallet speichert. Muss sich dieser nun ausweisen, so reicht er dem Verifier (Beispielsweise der Arbeitgeber) eine VC-Representation ein. Diese VC-Representation (oder auch Verifiable Presentation *VP* genannt) beinhaltet in der Regel ein VC, kann jedoch in komplexeren Szenarien mehrere VC's enthalten. Zudem ist der jeder (insbesondere der Verifier) in der Lage die Authentizität des VP zu überprüfen.

Issuer, Holder und Verifier können jeweils alle drei Rollen annehmen, besitzen eine DID und sind DID-Subjects. Folgende Zusammenhänge existieren zwischen dem DID-Subject, DID, DID-URL, DID-Controller, DID-Document und der Verifiable Data Registry:

Die DID-URL beinhaltet die DID und erweitert die Syntax um die URI-Komponenten wie Pfade oder Anfrage-Parameter. Sowohl DID's als auch DID-Documents werden auf einem Verifiable Data Registry persistiert. Diese werden beispielsweise als Datenbanken oder dezentrale Dateisysteme realisiert. In diesem Kontext sind jedoch distributed Ledger die Speicher der Wahl. Das DID-Dokument wird durch die DID-URL (de-

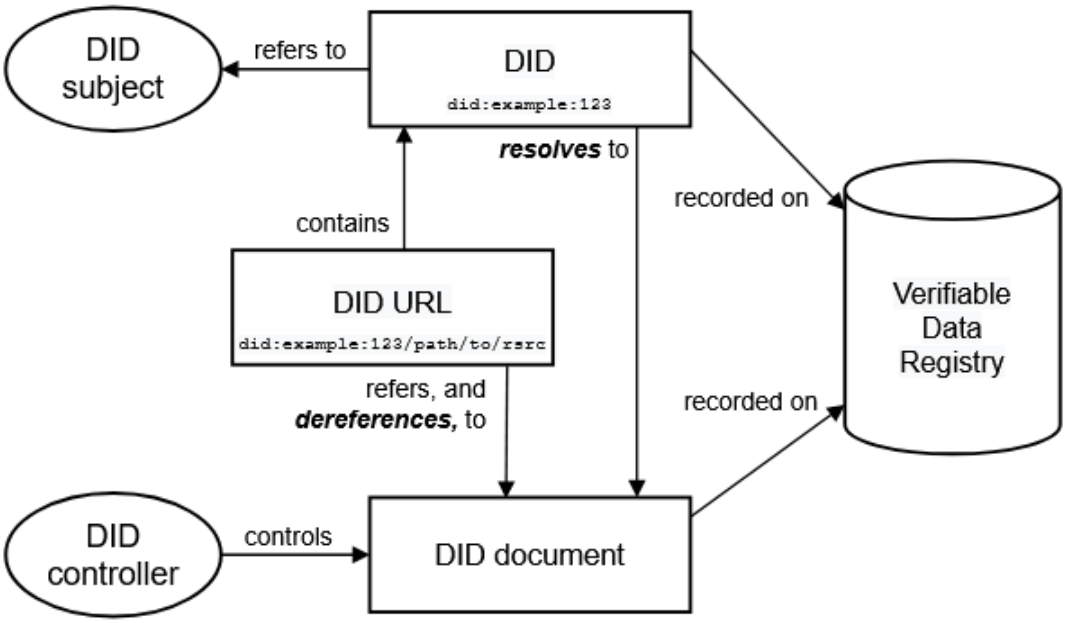

Abbildung 2.2: Zusammenspiel von Issuer, Holder und Verifier [Id1a]

)referenziert und durch die DID auf sich verwiesen. Der DID-Controller ist die Entität, die das DID-Document modifizieren kann. In der Regel ist diese Entität das DID-Subject der DID, es kann jedoch auch ein ein oder mehrere andere DID-Subjecte sein.

2.3 Politik, Recht und Ethik in Bezug auf SSI

2.3.1 Politik

Aus politischer Sicht spielt SSI eine wichtige Rolle, da das Potential besteht das Monopol des Staates in Bezug auf die Ausstellung, Aufrechterhaltung und Entzug von Ausweisdokumenten zu verlieren. Durch die Einführung von digitalen Entitäten - mit denen man sich auch in der analogen Welt ausweisen könnte - können staatliche Institutionen nicht mehr uneingeschränkt über den genannten Prozess verfügen. Betroffen sein können unter anderem die Digitalisierung der Grenzkontrollen oder das Migrationsmanagement, indem Pässe, Visa und ähnliche Dokumente als VC zur Verfügung gestellt werden.
Eine weitere Auswirkung ist, dass durch SSI das aktuelle Monopol im Identitätsmanagement von Unternehmen wie Meta (Facebook) und Google durch föderierte Identitätsmanagementsysteme abgelöst wird. Dadurch haben letztere Unternehmen nicht mehr die Kontrolle über die Daten ihrer Nutzer, was auch monetäre Auswirkungen hat. Die zuvor für Marketingzwecke verwendeten Daten stehen demnach nicht mehr zu Verfügung für personalisierte Werbung und Ähnlichem.
Insgesamt hat SSI das Potenzial, das bestehende Identitätsmanagement-System zu re-

volutionieren und die Kontrolle über digitale Identitäten in die Hände der Nutzer zu legen. Dies wirkt sich auf verschiedene Bereiche aus, darunter die Politik, das Monopol des Staates, die Digitalisierung von Grenzkontrollen und die Monetarisierung von Daten.

2.3.2 Recht

Die Einführung von SSI wirft auch rechtliche Fragen und Aspekte auf. Eine zentrale Frage betrifft die rechtliche Anerkennung von digitalen Identitäten und die damit verbundenen Rechte und Pflichten. Da SSI die traditionelle Vorstellung von staatlich ausgestellten Ausweisdokumenten und Identitätsnachweisen herausfordert, müssen rechtliche Rahmenbedingungen geschaffen werden, um die Verwendung und den Schutz digitaler Identitäten zu regeln. Dies könnte die Festlegung von Standards für digitale Identitäten, Datenschutzbestimmungen, Haftungsfragen und den Zugriff auf und die Verwaltung von persönlichen Daten umfassen. Zudem muss auch geklärt werden, wie SSI in bestehende Rechtssysteme und -strukturen integriert werden kann, beispielsweise in Bezug auf Verträge, Gerichtsverfahren oder behördliche Angelegenheiten. Die rechtlichen Aspekte von SSI sind daher von großer Bedeutung, um die rechtliche Sicherheit, den Schutz der Privatsphäre und die Gewährleistung der Rechte und Pflichten aller beteiligten Parteien zu gewährleisten.
Weitere zu beachtende Aspekte sind die juristische Verantwortlichkeit oder Datenschutz. Vor allem Ersteres spielt eine Rolle, wenn es sich um die Verwendung von Identitätsinformationen, Identitätsdiebstahl oder Fälschungsversuchen handelt. Zweiteres ist relevant in Bezug auf die rechtlichen Anforderungen die mit Datenverwaltung einhergehen.

2.3.3 Ethik

Auch auf ethnischer Sicht zeigt sich die Relevanz von SSI. Gerade das Konzept der Dezentralisierung und die Tatsache, dass keine Instanz mehr Macht über die Identitäten hat als andere wirft ethnische Fragestellungen auf. In [Ish20] beschreibt Ishmaev das Paradoxon, dass einerseits SSI zuletzt genannte Eigenschaften fordert, jedoch andererseits verschiedene Levels an 'Vertrauen' an Entitäten in der analogen Welt existieren. So sind beispielsweise Dokumente, die von einer staatlichen Autorität zugewiesen werden bedeutender als das Sportabzeichen für Grundschüler. Dieser Zustand wird in dem SSI-Konzept jedoch nicht berücksichtigt und zeigt den Kompromiss, den SSI-Identitätsmanagementsysteme implementieren müssen.
Ein weiterer problematischer Aspekt, ist die von Ishmaev genannte Tatsache, dass die Macht über die Freigabe der Daten zwar bei dem Nutzer liegt, die Macht über die Nutzung eines Dienstes liegt jedoch weiterhin bei dem Anbieter. So kann ein Großkonzern für die Nutzung eines Dienstes eine unmoralische Menge an Informationen fordern.

Dadurch wird klar, dass weiterhin eine problematische Machtrelation existiert.

Ein weiterer Punkt ist die Diskrepanz zwischen SSI im sozialen und im technischen Kontext. SSI-Systeme unterscheiden nicht zwischen den handelnden Entitäten, ob es sich um Privatpersonen, Institutionen oder - im Rahmen von Internet-of-Things - Hardware handelt. Gerade dadurch weißt die Interpretation von ’Vertrauen’ in sozialen oder cybersecurity Bereich Unterschiede auf. Es gibt eine Vielzahl an Definitionen für "Vertrauen", wobei diese meist in Abhängigkeit zu dem Kontext stehen, in dem sie verwendet werden. Eine allgemeine Definition wurde von McKnight und Chervany (1996) festgelegt: Vertrauen ist der Grad zu welchem eine Partei einwilligt abhängig zu etwas oder jemanden in einer Situation zu sein mit einem Gefühl von Sicherheit. Hierbei werden explizit und implizit folgende drei Bestandteile von Vertrauen dargestellt [Jø+05]:

- Abhängigkeiten zwischen Parteien
- Zuverlässigkeit einer Partei
- Risiko, dass eine Partei nicht wie erwartet agiert

Alle diese drei Charakteristika unterscheiden sich, je nachdem ob es sich um IoT-Geräte, Software oder Menschen handelt.

Kapitel 3

Distributed Ledger Technology

3.1 Merkmale und Vorteile von DLT

Distributed Ledger ist - wie der Titel bereits beschreibt - eine , für diese Arbeit, bedeutende Technologie. Dabei sind folgende Merkmale und Vorteile der DTL relevant [KAN+23]:

- DLT ermöglicht das Betreiben einer hochverfügbaren Datenbank (eines 'Ledgers'), da nicht eine zentrale Instanz für die Verfügbarkeit verantwortlich ist, sondern die Gesamtheit der Knoten in dem Netzwerk.
- Ebenso ermöglicht die Dezentralität des DLT eine verteilte Speicherung und Verarbeitung.
- Manipulationsresistenz wird durch kryptographische Verfahren innerhalb der Blockchain sichergestellt. Im Fall der Blockchain sind sind sind diese in der Regel asymmetrische Verfahren, was bedeutet, dass private/öffentliche Schlüssel zum Ent- oder Verschlüsseln der Daten verwendet werden, wobei 'Integer Factorization', "Discrete Logarithm' oder 'Elliptic Curves' verwendet werden können [Bas17]
- Zensurresistenz kann gewährleistet, indem beispielsweise alle Knoten die gleichen Berechtigungen haben und somit keine machthabende Instanz existiert. Alle Teilnehmer im Netzwerk werden als Knoten (Nodes) bezeichnet und besitzen jeweils eine lokale Kopie des Ledgers. Änderungen werden nun auf der Kopie ausgeführt und im Anschluss in dem Netzwerk synchronisiert. Das Netzwerk gilt als üntrustworthy"(nicht vertrauenswürdig), wenn willkürliche einzelne Knoten sog. 'Byzantine-Failures' [LSP82] [Sun19] erzeugen können. Dies bedeutet, dass versucht wird beliebig falsches Verhalten im System zu erzeugen (unauthentische Daten, Zusammensturz des Systems, etc). Der Resistenzgrad des Netzwerks gegenüber diesen Angriffen wird als 'Byzantine-Toleranz' bezeichnet und wird in der Regel durch Abstimmungen im Netzwerk (Beispielsweise Konsensus-

Algorithmen) verhindert. Beispiele im Blockchain-Kontext sind 'Proof-of-Work' oder "Proof-of-Stake' [Min+17] Algorithmen.

- Möglichkeit zur 'Demokratisierung' von Daten: Durch DLT kann ermöglicht werden, dass Individuen und/oder Organisationen kooperativ Kontrolle über Daten ausüben

3.2 Anwendung von DLT im Bereich der digitalen Identität

Die oben genannten Eigenschaften sind für das Betreiben eines Identitätsmanagementsystems optimal, da diese hochverfügbar sein sollten, mit möglichst kurzen oder nicht existierenden Downtimes. Auch ist eine verteilte Speicherung und Verarbeitung eine effiziente Möglichkeit große Menge an Anfragen zu bearbeiten oder eine Vielzahl an Identitätsdaten zu speichern. Zusätzlich ist Manipulationsresistenz von großer Bedeutung, da die Identitätsdaten stets authentisch sein müssen, um beispielsweise Dokumentenfälschung oder Identitätsdiebstahl zu vermeiden. Ebenso können finanzielle Transaktionen hiermit abgewickelt werden, was in der analogen Welt oft im Zusammenhang mit der Dokumentenausstellung stattfinden. Ein Beispiel hierfür sind die Gebühren beim Beantragen eines Reisepasses oder die Strafgebühr für das zu späte Neubeantragen eines Abgelaufenen Ausweises. Die Möglichkeit sog. 'smart contracts' - also eigene Programme - zu schreiben ist eine Eigenschaft, die nicht in allen DLT's gegeben ist. Dennoch wird diese Eigenschaft an dieser Stelle erwähnt, da einige Blockchains wie Ethereum Letzteres unterstützen und somit einem Software-Entwickler die Chance geben fehlende Software im Identitätsmanagementsystems zu implementieren.

Diese Merkmale von DLT machen es zu einer idealen Technologie für die Umsetzung von Self-Sovereign-Identity. Sie ermöglicht eine sichere, vertrauenswürdige und selbstbestimmte Verwaltung von Identitätsinformationen, wodurch Benutzer die Kontrolle über ihre Identität zurückerlangen und die Notwendigkeit von zentralen, vertrauenswürdigen Dritten verringert wird.

Kapitel 4

Anforderungsanalyse

Folgende Anforderungen gelten für das Identitätsmanagementsystem und entsprechen den von der OECD festgelegten Eigenschaften [Id2b] [Id2a].

4.1 Funktionale Anforderungen

- Widerruf: Informationen müssen widerruflich sein
- Auswahl: Es muss dem Nutzer gegeben sein zwischen den Identitätsplattformen zu wählen
- Überprüfbarkeit: Es muss dem Nutzer möglich sein die Daten über sich zu überprüfen. Dazu gehört: Welche Daten stehen zur Verfügung und warum, Wer hat Zugriff auf diese Daten und wann wurden die Daten in das System eingetragen.
- Selektive-Veröffentlichung: Dem Nutzer muss es möglich sein nur einzelne Claims zu veröffentlichen

4.2 Nicht-Funktionale Anforderungen

- Vertraulichkeit: Eigenschaften einer Identität müssen vor unautorisierten Offenlegung geschützt werden
- Integrität: Informationen dürften nur autorisiert modifiziert werden
- Unverknüpfbarkeit: Es darf einem Angreifer nicht möglich sein zwei Transaktionen zu verknüpfen und somit unerlaubte Informationen zu erlangen
- Non-Replay: Operationen dürfen nicht erneut ausführbar sein
- Nichtabstreitbarkeit: Das Senden von Daten durch den Nutzer kann im Nachhinein nicht abgesprochen werden

- Diebstahlschutz: Die Daten dürften nicht von Unbefugten lesbar sein

4.3 Technische Anforderungen

Als technische Anforderung wird lediglich festgelegt, dass eine DLT verwendet werden soll, was in dieser Arbeit durch die Blockchain realisiert wird. Davon abgesehen werden Komponenten und Schnittstellen verwendet, die die oben genannten (Nicht-) funktionalen Anforderungen erfüllen. Auch gilt sich in dem Design und Implementierung an möglichst viele Standards zu halten:

- W3C Standard für Verifiable Credentials: https://www.w3.org/TR/vc-data-model/
- DIF Presentation Exchange: https://identity.foundation/presentation-exchange/
- ...

Kapitel 5

System-Design

5.1 Architektur des dezentralen Identitätsmanagementsystems Anforderungen

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

5.2 Komponenten und deren Funktionalitäten

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

5.3 Interaktion zwischen den Komponenten

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

5.4 Integration von DLT in das Systemdesign

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 6

Implementierung

6.1 Auswahl geeigneter DLT

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

6.2 Ausführung von Performance-Tests

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

6.3 Implementierung

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

6.4 Sicherheitsmechanismen

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 7

Evaluation

7.1 Festlegen der Evaluations Metriken

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

7.2 Durchführen der Tests

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

7.3 Sicherheitsevaluierung

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

7.4 Analyse der Ergebnisse

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 8

Diskussion

8.1 Zusammenfassen der Ergebnisse

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

8.2 Vergleich mit vorhandenen Ansätzen

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

8.3 Potenziale und Herausforderungen des dezentralen Identitätsmanagementsystem

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

8.4 Ausblick auf zukünftige Forschungsrichtungen

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Kapitel 9

Fazit

9.1 Zusammenfassung der Arbeit

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

9.2 Erfüllung der Zielsetzung

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

9.3 Beitrag zur Forschung im Bereich „Dezentrale Identitätsmanagement

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.

Literatur

[Bas17] Imran Bashir. *Mastering Blockchain*. 1. März 2017.

[CS15] CTRL-SHIFT. “Economics of Identity”. In: (2015).

[Id1a] “Decentralized Identifiers (DIDs) v1.0”. In: (30. Juni 2023). URL: https://www.w3.org/TR/did-core/.

[Id1b] *Die Chain Key Technologie: Schlüssel des Internet Computers*. URL: https://internet-computer.de/wissen/chain-key-technologie-kryptographie/.

[Id1c] *Introducing BrowserID – easier and safer authentication on the web*. 21. Juli 2011. URL: https://hacks.mozilla.org/2011/07/introducing-browserid-easier-and-safer-authentication-on-the-web/.

[Id1d] *Introduction to Self-Sovereign Identity (SSI)*. 26. Juni 2023. URL: https://walt.id/white-paper/self-sovereign-identity-ssi.

[Id1e] *OpenID*. 17. Juni 2023. URL: https://openid.net/.

[Id2a] “Digital Identity Management”. In: (1. Jan. 2011). URL: https://www.oecd.org/sti/ieconomy/49338380.pdf.

[Id2b] *Identity Management System Requirements*. URL: https://ebrary.net/24577/computer_science/identity_management_system_requirements#gads_btm.

[Ish20] Georgy Ishmaev. “Sovereignty, privacy, and ethics in blockchain-based identity management systems”. In: *Ethics and Information Technology* (30. Nov. 2020).

[Jø+05] Audun Jøsang u. a. “Trust Requirements in Identity Management”. In: (1. Jan. 2005).

[KAN+23] NICLAS KANNENGIEßER u. a. “Trade-offs between Distributed Ledger Technology Characteristics”. In: (1. Mai 2023). URL: https://www.w3.org/TR/did-core/.

[Loc+05] Hal Lockhart u. a. “Security Assertion Markup Language (SAML) V2.0 Technical Overview”. In: (2005).

[LSP82] Leslie Lamport, Robert Shostak und Marshall Pease. “The byzantine generals problem”. In: *ACM Trans. Program.Lang. Syst. 4, 3* (1982).

[Min+17] Du Mingxiao u. a. “A Review on Consensus Algorithm of Blockchain”. In: (5. Okt. 2017).

[Sta12] Statista. “Why Do Shoppers Drop Out of an Online Purchase”. In: (2012).

[Sun19] Ali Sunyaev. “Distributed ledger technology. In Internet Computing: Principles of Distributed Systems and Emerg- ing Internet-based Technologies”. In: (2019).

[TR17] Andrew Tobin und Drummond Reed. “The Inevitable Rise of Self-Sovereign Identity”. In: (2017), S. 1–23.

Kapitel 10

Codebeispiele

```
14          public class Factorial
15          {
16                  public static void main(String[] args)
17                  {   final int NUM_FACTS = 100;
18                          for(int i = 0; i < NUM_FACTS; i++)
19                          System.out.println( i + "! is " + factorial(i))
                                ;
20                  }
21
22                  public static int factorial(int n)
23                  {   int result = 1;
24                          for(int i = 2; i <= n; i++)
25                          result *= i;
26                          return result;
27                  }
28          }
```

And you can reference line 24 in the code!

Kapitel 11

Evaluierungsergebnisse

Dies hier ist ein Blindtext zum Testen von Textausgaben. Wer diesen Text liest, ist selbst schuld. Der Text gibt lediglich den Grauwert der Schrift an. Ist das wirklich so? Ist es gleichgültig, ob ich schreibe: „Dies ist ein Blindtext“ oder „Huardest gefburn“? Kjift – mitnichten! Ein Blindtext bietet mir wichtige Informationen. An ihm messe ich die Lesbarkeit einer Schrift, ihre Anmutung, wie harmonisch die Figuren zueinander stehen und prüfe, wie breit oder schmal sie läuft. Ein Blindtext sollte möglichst viele verschiedene Buchstaben enthalten und in der Originalsprache gesetzt sein. Er muss keinen Sinn ergeben, sollte aber lesbar sein. Fremdsprachige Texte wie „Lorem ipsum“ dienen nicht dem eigentlichen Zweck, da sie eine falsche Anmutung vermitteln.