HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Alexander Hultzsch

Implementierung einer Reputationsplattform auf Basis von Soulbound Token

Mittweida, Oktober 2022

Fakultät **Angewandte Computer- und Biowissenschaften**

BACHELORARBEIT

Implementierung einer Reputationsplattform auf Basis von Soulbound Token

Autor:
Alexander Hultzsch

Studiengang:
Angewandte Informatik

Seminargruppe:
If19wS-B

Erstprüfer:
Prof. Dr.-Ing. Andreas Ittner

Zweitprüferin:
Hira Siddiqui, M.A.

Einreichung:
Mittweida, 31.10.2022

Verteidigung/Bewertung:
Mittweida, 21.11.2022

Faculty of **Applied Computer Sciences and Biosciences**

BACHELOR THESIS

Implementing a reputation platform based on Soulbound Tokens

Author:
Alexander Hultzsch

Course of Study:
Applied Computer Science

Seminar Group:
If19wS-B

First Examiner:
Prof. Dr.-Ing. Andreas Ittner

Second Examiner:
Hira Siddiqui, M.A.

Submission:
Mittweida, 31.10.2022

Defense/Evaluation:
Mittweida, 21.11.2022

Bibliografische Beschreibung:

Hultzsch, Alexander:
Implementierung einer Reputationsplattform auf Basis von Soulbound Token. – 2022. – 40 S.
Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2022.

Referat:

Fake News und Betrugsschemata sind heutzutage ein allgegenwärtiger Bestandteil des Internets. Erfahrene Nutzer haben gelernt damit umzugehen und Richtiges von Falschem zu unterscheiden. Doch auch die erfahrensten Benutzer des Internets können von geschickten Hochstaplern und Betrügern manipuliert werden. Die Betreiber der sozialen Medien, können und wollen oftmals nicht für die Sicherheit ihrer Nutzer garantieren, weswegen ein Ansatz benötigt wird, welcher diese Betreiber ablöst. Nachdem Non-Fungible Tokens gezeigt haben, wie digitales Eigentum implementiert werden kann, zeigen sogennante Soulbound Tokens, wie digitales Vertrauen im Internet existieren kann. Diese Art von Tokens sind nicht transferierbar und für immer an ihren Besitzer gebunden, wodurch diverse, digitale Persönlichkeiten entstehen können, deren Glaubwürdigkeit von Soulbound Tokens bewiesen wird. Decentralized Reputation (DeRep) beschreibt dabei eine Reputationsplattform, auf welcher Benutzer Soulbound Tokens als Bewertung für andere Nutzer ausstellen können. Zusammen mit weiteren Funktionen, wie einem Bewertungsalgorithmus für die Profile der Nutzer, wird veranschaulicht, wie Reputation mithilfe von Soulbound Tokens generiert werden kann und welche Herausforderung dabei entstehen.

Inhaltsverzeichnis

Inhaltsverzeichnis I

Abbildungsverzeichnis II

Quelltextverzeichnis III

Abkürzungsverzeichnis IV

1 Einführung 1

2 Grundlagen 3
2.1 PGP und das Web Of Trust . . . 3
2.1.1 PGP . . . 3
2.1.2 Vertrauensbegriff und Vertrauensmodelle . . . 4
2.1.3 Funktionsweise und Prinzipien des Web of Trust . . . 5
2.1.4 Limitationen und Untergang des Web of Trust . . . 9
2.2 Reputationsplattformen . . . 10
2.3 Bewertungsmechanismen im Web 2.0 . . . 14
2.3.1 Amazon . . . 14
2.4 Bestehende Bewertungsmechanismen im Web 3.0 . . . 17
2.4.1 Soulbound Tokens . . . 18
2.4.2 Verifiable Credentials . . . 20
2.4.3 Proof of Personhood . . . 21
2.5 Probleme und Angriffsvektoren . . . 22
2.5.1 Sybil Attacks und Denunziation . . . 22
2.5.2 Identitätsverlust . . . 23
2.5.3 Privatsphäre . . . 25

3 Implementierung einer Reputationsplattform 27
3.1 Architektur . . . 28
3.2 Frontend . . . 28
3.3 Backend . . . 29
3.3.1 Smart Contract . . . 29
3.3.2 Bewertungsalgorithmus . . . 31
3.3.3 Network of Souls . . . 34

4 Schluss 38
4.1 Ausblick . . . 38

Anhang 41

A Quelltext 41

Literaturverzeichnis 44

Eidesstattliche Erklärung 48

Abbildungsverzeichnis

2.1 Hierarchichal PKI vs. Web of Trust . . . 6
2.2 Web of Trust mit Owner Trust und Key Legitimacy . . . 7
2.3 Serieller Zertifizierungspfad . . . 8
2.4 Paralleler Zertifizierungspfad . . . 9
2.5 Reputation als Teil von Online-Vertrauen . . . 11
2.6 Aufbau und Funktionsweise von verteilter Reputation . . . 13
2.7 Amazon Verkäufer Profil . . . 15
2.8 Anzahl Bewertungen eines Verkäufers auf Amazon . . . 15
2.9 Ein Beispiel für die Daten einer Bewertung . . . 16
2.10 Funktionsweise von Social Recovery . . . 24
2.11 Funktionsweise von Community Recovery . . . 24
2.12 Privatheit mithilfe von externen Verweisen. . . . 25
3.1 Kompletter Überblick über die Reputationsplattform . . . 28
3.2 Minting Page von DeRep . . . 29
3.3 Zusammensetzung der Bewertung . . . 32
3.4 Netzwerk 1: Circle of Trust . . . 34
3.5 Circle of Trust: Profil von Alice . . . 35
3.6 Rich Network of Trust . . . 36
3.7 Rich Network of Trust: Profil von Alice . . . 37

Quelltextverzeichnis

3.1 Datentyp Soul 30
3.2 Datentyp Sbt 31
A.1 mint Funktion 41
A.2 burn Funktion 41
A.3 attest Funktion 41
A.4 revoke Funktion 42
A.5 Soul Score Berechnung 42
A.6 Quantity Score Berechnung 42
A.7 Quality Score: Timestamp Berechnung 43
A.8 Quality Score: Description Berechnung 43

Abkürzungsverzeichnis

CA ..... Certification Authority

DAO ..... Decentralized Autonomous Organization

DeFi ..... Decentralized Finance

DeRep ..... Decentralized Reputation

DeSoc ..... Decentralized Society

DSGVO ..... Datenschutz-Grundverordnung

ERC ..... Ethereum Improvement Proposals

EVA ..... Eingabe-Verarbeitung-Ausgabe

GnuPG ..... GNU Privacy Guard

IPFS ..... InterPlanetary File System

KYC ..... Know Your Customer

P2P ..... Peer-to-Peer

PGP ..... Pretty Good Privacy

PKI ..... Public Key Infrastructure

PoP ..... Proof of Personhood

SBT ..... Soulbound Token

SKS ..... Synchronizing Key Server

VC ..... Verifiable Credential

VP ..... Verifiable Presentation

WoT ..... Web of Trust

1 Einführung

Das Internet hat es leicht gemacht Informationen schnell und weltweit zu teilen. In kürzester Zeit hat das Netz es geschafft sich von traditionellen Medien abzuheben und die Art und Weise wie wir Nachrichten konsumieren zu verändern. Laut dem statistischen Amt der Europäischen Union benutzten 2021 etwa 3 von 4 EU-Bürgern das Internet, um Online-Nachrichtenseiten, Zeitungen oder Nachrichtenmagazine zu lesen. [eur22] Doch auch soziale Medien stellen beliebte Alternativen dafür dar. Besonders durch die Covid19-Pandemie ist es jedoch deutlich geworden, dass Falschmeldungen ein immer größer werdendes Thema in unserer Gesellschaft spielen dürften und es immer schwieriger wird Desinformation von echten Informationen zu unterscheiden. Das Identifizieren von Falschinformation erweist sich nicht nur als eine schwer zu lösende Herausforderung, sondern stellt auch eine Gefahr für die Öffentlichkeit dar, indem einzelne Personen radikalisiert werden oder Falschinformation über die Gesundheit geteilt werden.[Fac22][Deu22] Besonders in sozialen Medien, wie Facebook und YouTube oder Messenger-Diensten, wie Whatsapp und Telegram verbreiten sich Desinformationen rasant. [Deu22] Durch reißerische Überschriften und Inhalten, welche auf die Gefühle von Menschen abzielen, können sich solche Inhalte besonders schnell verbreiten. [eik19] In sozialen Netzwerken entscheiden vor allem Algorithmen, welche Inhalte sie ihren Nutzern zeigen. Hierbei wird besonders darauf geachtet, wie oft Nutzer mit dem Inhalt interagieren oder was der Nutzer in seiner Vergangenheit gesehen hat. Die Folge ist, dass kontroverse Inhalte eher weiterempfohlen werden und Nutzer oftmals in Filterblasen landen, in denen nur personalisierte Inhalte vorzufinden sind, welche existierende Überzeugungen bestätigen.[Min+19] [Men22] Die Betreiber von diesen Netzwerken haben wenig Interesse dagegen vorzugehen, da dies zum einen einen großen Arbeitsaufwand aufstellen würde und sie zum anderen durch die erhöhte Nutzung der Plattform direkt davon profitieren. Daraus wird deutlich, dass den großen Akteuren in der heutigen Web2-dominierten Landschaft weder die Macht noch der gute Wille fehlt, daran etwas zu ändern, wodurch die Notwendigkeit einer dezentralisierten Reputation steigt. Diese Art der Reputation ist unabhängig von einer zentralen Autorität und setzt sich zusammen aus der Meinung eines verteilten Knotennetzwerks. [Suc21]

Ein besonders vielversprechender Entwicklungszweig stellt hierbei das Web3 und seine steigenden Bestrebungen für Dezentralisierung dar. Jede Transaktion die im Web3 durchgeführt wird, ist momentan finanzieller Natur, wodurch sich eine Hyperfinanzialisierung in diesem System ausgeprägt hat. Jedoch können nicht alle Formen von Transaktionen damit bewältigt werden. Für eine Vielzahl von Transaktionen im echten, als auch digitalen Leben bildet Vertrauen die Grundlage für das interagieren miteinander. Dies machen Mechanismen zur Vertrauensgewinnung in verteilten Systemen zu einem äußerst vielversprechenden Entwicklungsziel. Eine Möglichkeit, um Vertrauen zu generieren stellen Soulbound Token (SBT) dar. Die einzigartige Eigenschaft dieser Token ist es, dass sie an ein Wallet gebunden sind, also nicht weiterverschickt werden können, sobald sie einmal ausgestellt wurden. Diese Tokens können eine Vielfalt an Dingen darstellen und somit soziale Identitäten schaffen, welche den Weg des momentanen Web3 gänzlich ändern. SBT sind der Grundstein für neue Anwendungsfälle, welche sich von den bisherigen Web3 Anwendungen absetzen, indem sie nicht nur spekulativ sind und kein großes Startkapital zur Verwendung benötigen. Vielmehr kann somit eine Decentralized Society (DeSoc) aufgebaut werden, womit eine soziale Herkunft der Benutzer erschaffen wird. Diese individuellen Nutzer generieren daraufhin Reputation, welche sich von unten nach oben durchsetzt. [BOW22]

Diese Arbeit beschäftigt sich mit einem möglichen Anwendungsfall dieser neuen Technologie, und zwar dem Erstellen einer Reputationsplattform auf Basis von Soulbound Tokens. Hierbei sollen zunächst Grundlagen über den Vertrauensbegriff, Reputationssysteme und bereits existierende Technologien vermittelt werden. Sowohl die Unterschiede zwischen Web2 und Web3, als auch bestehende Schwachstellen in diesen Systemen und wie sie mithilfe von SBTs überwältigt werden können, spielen dabei große Rolle. Wobei die Soulbound Token auch selbst Limitationen besitzen, die es zu berücksichtigen gilt.

Im praktischen Teil dieser Arbeit geht es um die Implementierung der Anwendung, wobei Design Entscheidungen und Limitationen geschildert werden. Mit dieser Anwendung wird es möglich sein andere Nutzer mit SBTs zu attestieren und selbst zu erhalten. Diese Token können positive Reputation oder negative Reputation darstellen, um somit besonders vertrauenswürdige Nutzer einer Community hervorzuheben. Den Kern der Anwendung stellt eine eigene Interpretation von Soulbound Token im Form eines Smart Contracts dar, gekoppelt mit einem Bewertungsalgorithmus, der mit diesen Daten umgeht. Mithilfe eines Frontends werden alle Funktionen in Form einer Website präsentiert, welche das Nutzen dieser Funktionen von SBTs erleichtert.

Schlussendlich entsteht eine Präsentation und Demonstration für eine sehr moderne und junge Technologie, wobei Lernerfolge und Verbesserungen für weitere Arbeiten an diesem Thema aggregiert werden sollen.

2 Grundlagen

2.1 PGP und das Web Of Trust

2.1.1 PGP

Pretty Good Privacy (PGP) ist ein Verschlüsselungssystem, welches es ermöglicht, E-Mails oder andere sensible Dateien zu verschlüsseln und zu versenden. Es wurde im Jahre 1991 vom damaligen Studenten Phil Zimmermann entwickelt und ist bis heute der de facto Standard im Bereich Email-Verschlüsselung.[Jef20] Ziel von Zimmermann war es, eine Software zu entwickeln, welche sich an die verworrenen Strukturen des Internets anpasste, als auch leicht zu bedienen war für Nutzer. Trotz Problemen bezüglich Nutzerfreundlichkeit der Software, erfreute sie sich großer Beliebtheit, besonders, da die Veröffentlichung als Freeware für eine schnelle Verbreitung sorgte. [Chr01]

Ein weiterer Vorteil von PGP besteht darin, dass es ein hybrides Verschlüsselungssystem ist und somit die Vorzüge von asymmetrischen und symmetrischen Kryptosystemen kombiniert. Durch das Enkodieren des symmetrischen Schlüssels durch das asymmetrische Verfahren kann ein Sender diesen Schlüssel über einen unsicheren Kanal an seinen Empfänger schicken. Daraufhin schickt er ebenfalls die enkodierte Nachricht an den Empfänger, welcher diese nun mit dem symmetrischen Schlüssel entschlüsseln kann. Somit lässt sich die schnellere Entschlüsselungsgeschwindigkeit des symmetrischen Verfahren nutzen, ohne, dass Sender und Empfänger ihren Schlüssel vorher in einem sicheren Kanal austauschen müssen. [Ele22]

Einige Jahre nach der Erscheinung von PGP wurde das PGP Message Format entwickelt. Das daraus resultierende Standard OpenPGP definiert Methoden, wie das Signieren und Widerrufen von Schlüsseln. Als auch das allgemeine Format, dem eine PGP Nachricht folgen muss, wodurch Hersteller ihre eigenen Implementation von PGP erstellen können, wie zum Beispiel GNU Privacy Guard (GnuPG). Diese Implementierung ist auf den meisten Linux-Distributionen enthalten und stellt einen Ersatz für das ursprüngliche PGP dar. [Cal+07] Zur einfachen Übertragung und Bereitstellung der verschiedenen öffentlichen Schlüssel wurden Public Key Infrastructure (PKI)s entwickelt. Sie bevorzugen den Einsatz von sogenannten Schlüsselservern auf denen die Nutzer ihre öffentlichen Schlüssel hochladen und die Schlüssel anderer Personen finden können. OpenPGP nutzt hierfür HTTP-Keyserver, welche leicht aufzusetzen sind und durch HTTP-Schnittstellen einfach automatisiert werden können. [Chr01]

Ein Problem, dass durch den Einsatz von obengenannten Schlüsselservern entsteht, ist, dass diese Server nicht die Echtheit einer Person hinter einem Schlüssel authentifizieren können. Ein beliebiger Nutzer könnte einen öffentlichen Schlüssel generieren und daraufhin behaupten, dass dieser einer Person gehört, die er versucht nachzustellen. Aus diesem Grund haben sich verschiedene PKIs entwickelt, die dieses Problem lösen. Die am meisten verbreitete Form stellt hierbei eine hierarchisches und zentrales Modell dar, welches eine Certification Authority (CA) einsetzt, um echte Schlüssel zu zertifizieren. Eine CA kann außerdem eine Sub-CA einsetzen um Schlüssel in ihrem Namen signieren zu lassen. Der öffentlichen Schlüssel der CA ist für alle Nutzer einzusehen, sodass sie somit die Gültigkeit fremder Schlüssel überprüfen und ihnen vertrauen können. [Chr01]

2.1.2 Vertrauensbegriff und Vertrauensmodelle

Für das bessere Verständnis der folgenden Kapitel soll der Vertrauensbegriff zunächst näher gedeutet werden, da dieser je nach Kontext stark variieren kann. Im Kontext der folgenden Kapitel soll **Vertrauen** eine Beziehung zwischen zwei Parteien sein, die die Echtheit von einander bestätigen können. Echtheit bedeutet hierbei, dass ein Nutzer auch wirklich die Person ist, die er vorgibt zu sein. Daneben soll die **Gültigkeit** den Wert angeben, mit welcher Wahrscheinlichkeit ein Schlüssel valide ist. Falls die Wahrscheinlichkeit genügend hoch ist, so wird ein Schlüssel als gültig/valide betrachtet. [Vie08]

Vertrauen ist eine transitive Relation. Das bedeutet, dass wenn Alice Bob vertraut und Bob Charlie vertraut, Alice somit auch Charlie vertraut. Mit steigender Anzahl der Teilnehmer nimmt das transitive Vertrauen aber stückweise ab. Wie bereits im vorherigen Kapitel genannt, gibt es allerdings weitere Möglichkeiten, um in einer PKI Vertrauen zu generieren. Hierfür werden Vertrauensmodelle benutzt, welche beschreiben, wie man einem fremden öffentlichen Schlüssel vertrauen kann. Man unterscheidet 3 wesentliche Vertrauensmodelle:

Direct Trust - Alice vertraut Bob, da diese von ihm einen öffentlichen Schlüssel erhalten hat. Dieser wird entweder direkt übergeben oder in den meisten Fällen als Fingerprint via E-Mail übermittelt. Der Fingerprint ist hierbei eine relativ kurze, eindeutige Sequenz von Zahlen und Buchstaben, der genutzt werden kann, um einen Schlüssel zu identifizieren. Er leitet sich von dem öffentlichen Schlüssel des Besitzers und optionalen Zusatzdaten ab, welche in eine Hashfunktion eingegeben wurden. Diese Form des Vertrauens ist die zuverlässigste, da keine der beiden Parteien Interesse hat, der jeweilig anderen falsche Information zu vermitteln. Zusätzlich können Schlüssel selbst signiert werden, um eine weitere Ebene der Verifizierung anzubieten. [Vie08] [Eic01]

Der einzige Nachteil dieses Modells liegt darin, dass es nicht skaliert. Da ein paarweiser Schlüsselaustausch vorausgesetzt wird, lässt sich für n Personen die Anzahl der benötigten Austausche mit

$$n(n-1)/2$$

berechnen. Für jede neue Person, die hinzukommt, sind weiter n Austausche notwendig.[fu-04]

Hierarchical Trust - Analog zu den im vorherigen Kapitel beschriebenen CAs beruht das hierarchische Modell darauf, dass eine zentrale Instanz öffentliche Schlüssel verwaltet. Das Vertrauen basiert darauf, das ein angesehener und generell vertrauenswürdiger Nutzer nur Zertifikate bzw. Signaturen an ähnlich vertrauenswürdige Nutzer verteilt. Im oben genannten Beispiel zwischen Alice, Bob und Charlie, wäre Bob die CA für Alice, wodurch diese auch Charlie vertrauen kann. [Eic01]

Verschiedene CAs können hierbei ihr Vertrauen auf weitere Schlüssel erweitern, welche dann in ihrem Namen weitere Zertifikate ausstellen, wodurch ein Baumgraph des Vertrauens entsteht. Neben dem Internet findet dieses Modell auch in Regierungen und Unternehmen eine breite Anwendung, da diese sowieso hierarchisch aufgebaut sind. Reisepässe, Führerscheine und Kreditkarten sind Beispiele aus der echten Welt, die auf hierarchischem Vertrauen aufbauen. Der Vertrauensanker

dieser Institutionen wird hier hingegen durch Direct Trust in den öffentlichen Schlüssel der dazugehörigen CA hergestellt. Bei solchen Großakteuren wird allgemein von einer Vertrauenswürdigkeit ausgegangen, da diese sich mit bösartigen Absichten nur selbst sabotieren würden. Im Internet wird das direkte Vertrauen durch den Webbrowser und die installierte Software des Nutzers in einige Wurzelzertifikate hergestellt, von denen sich die restlichen Zertifikate ableiten. [Vie08][fu-04]

Der Nachteil des hierarchischen Vertrauensmodell liegt darin, dass Vertrauensmissbrauch große Konsequenzen mit sich zieht. Verhält sich eine CA fehl oder setzt ihr Vertrauen unachtsam in weitere Sub-CAs, so wird Fehlverhalten auf den ursprünglichen Zertifizierer reflektiert und verschlechtert das öffentliche Bild. Ebenso können böswillige Akteure, welche fälschlicherweise zertifiziert wurden, das Vertrauen der CA missbrauchen und indirekt in ihrem Namen handeln, wodurch es zu einem gänzlichen Vertrauensverlust in diesem System kommt. Da jegliche Autorität in einem einzigen Punkt konzentriert ist, stellen zentrale Instanzen außerdem ein besonders attraktives Ziel für Angreifer da. [Vie08]

Cumulative Trust - Um den soeben besprochenen Nachteil von Hierarchical Trust auszugleichen, hat sich das kumulierte Vertrauensmodell entwickelt. Wie der Name bereits vorwegnimmt, basiert dieses Modell darauf, dass ein Nutzer verschiedene Vetrauensbeweise akkumuliert. Das Prinzip dahinter geht davon aus, dass es viel schwieriger ist zwei Dokumente zu fälschen, als ein einzelnes. Ein simples Beispiel ist hierbei, das Verlangen von zwei Ausweisdokumenten eines Verkäufers, wie zum Beispiel einer Kreditkarte, als auch Personalausweis. Wenn der Käufer beide Dokumente vorweisen kann oder sogar noch mehr, kann sich der Verkäufer sehr sicher sein, dass die Person diejenige ist, die sie vorgibt zu sein.

Zu beachten ist: die Aussteller beider Dokumente entstammen unterschiedlichen, hierarchischen Systemen (Finanzdokument und Identitätsdokument) und vertrauen sich deshalb nicht gegenseitig. Doch durch das Kombinieren beider, lässt sich neues Vertrauen gewinnen. Im obigen Beispiel wurden zwei hierarchische Systeme kombiniert, allerdings lassen sich auch direkte Vertrauenssysteme kombinieren. Das bekannteste Beispiel ist hierbei das PGP Web of Trust. [Vie08]

2.1.3 Funktionsweise und Prinzipien des Web of Trust

Im Gegensatz zum klassischen, hierarchischen Aufbau eines PKI-System, benutzt PGP das dezentrale, benutzerzentrierte Web of Trust. Hierbei gibt es keine zentrale CA, welche Zertifikate verteilt, indem sie die Schlüssel anderer signiert. Stattdessen ist jeder Nutzer eine eigene CA und kann somit die Echtheit der anderen Benutzer bzw. deren Schlüssel eigenständig beglaubigen. Somit entsteht ein Netz des Vertrauens, welches keiner bestimmten Struktur zugrunde liegt und stattdessen dezentral aufgebaut ist. Die Abbildung 2.1 veranschaulicht den unterschiedlichen Aufbau zwischen den bisher bekannten hierarchischen PKIs und dem Web of Trust.

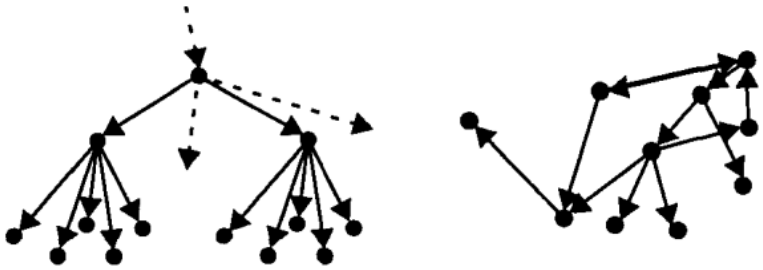

Abbildung 2.1: Hierarchichal PKI vs. Web of Trust
[Car00]

Um mit der Kommunikation im Web of Trust zu beginnen, eignen sich vor allem Kontakte, die bereits persönlich bekannt und deren Identität man bestätigen kann. Um die ersten Signaturen zu erhalten existieren auch dafür organisierte Keysigning Parties. Ein Ereignis im echten Leben, bei denen sich Nutzer zur gegenseitigen Identitätskontrolle und anschließendem Schlüsselaustausch persönlich treffen. Weitere Alternativen bieten beispielsweise Messen, auf denen einige Organisationen als Zertifizierungsstelle dienen und die Echtheit der Schlüsseln von Interessenten bestätigen. [Hei04]

Durch den Austausch untereinander, wird die Sammlung an signierten öffentlichen Schlüssel eines Nutzers immer größer. Diese Sammlung wird auch als Schlüsselbund (keyring) bezeichnet und bewahrt die öffentlichen Schlüssel der anderen Nutzer auf. Zusätzlich dazu, wird zu jedem Schlüssel der Name des Inhabers, dessen Signaturen, als auch die Werte zwei neuer, unabhängiger Vertrauensmetriken gespeichert. Neben dem Vertrauen, dass ein Schlüssel einer Person auch gültig ist, existiert zusätzlich das Vertrauen in die Prüffähigkeiten einer Person. Diese beiden Arten des Vertrauens werden jeweils als „Key Legitimacy“ und „Owner Trust“ bezeichnet.

Key Legitimacy - Bevor ein Nutzer einen öffentlichen Schlüssel einer anderen Person vertrauen und anschließend sicher benutzen kann, muss dieser sich bewusst sein, dass es sich bei diesem Schlüssel auch um die richtige Person dahinter handelt. Key Legitimacy ist der Wert für die Wahrscheinlichkeit, dass dieser Fall eintritt und ist Synonym mit der Definition für Gültigkeit aus Kapitel 2.1.2 zu gebrauchen. Zur Berechnung der Key Legitimacy L benutzt PGP die folgende Formel:

$$L = \frac{x}{X} + \frac{y}{Y}, \text{ wobei:}$$

- x: die Anzahl der marginal vertrauten Signaturen ist,
- X: die Anzahl der notwendigen marginal vertrauten Signaturen, um Gültigkeit zu erreichen,
- y: die Anzahl der vollständig vertrauten Signaturen,
- Y: die Anzahl der notwendigen vollständig vertrauten Signaturen, um Gültigkeit zu erreichen

Daraus ergeben sich 3 verschiedene, berechenbare Vertrauenslevel:

$$\frac{L{=}0}{ungültig}, \quad \frac{0{<}L{<}1}{teilweise\ gültig}, \quad \frac{L{=>}1}{gültig}$$

Die Werte X und Y können frei gewählt werden, sind aber standardmäßig auf $X = 2$ und $Y = 1$ gelegt. Ein Schlüssel benötigt also eine Signatur eines vollständig vertrauten Schlüssels oder zwei Signaturen von zwei unterschiedlichen, marginal vertrauten Schlüsseln, um als gültig betrachtet zu werden. [fu-04]

Owner Trust - Mit diesem Wert können Nutzer in unterschiedliche Stufen eingeordnet werden, welche Ihnen verschieden hohes Vertrauen bei der Signierung fremder Schlüssel zuspricht. Mit anderen Worten, gibt dieser Wert an, wie verlässlich und sorgfältig eine Person signiert. Diesen Wert kann der Benutzer selber für seine Kontakte festlegen. GnuPG sieht hierbei die folgenden Level von Owner Trust vor: [fu-04]

- Ultimate: Wird implizit vertraut. Sollte nur von Schlüsseln im eigenen Besitz verwendet werden.
- Full: Signaturen von Personen mit diesem Vertrauenslevel haben, sind immer gültig.
- Marginal: Person wird teilweise vertraut, Signaturen ordnungsgemäß zu verteilen. Meistens werden mehrere Signaturen von Marginal-Level Nutzern benötigt, um dem signierten Schlüssel zu validieren.
- Never: Signaturen, die von diesem Schlüssel ausgehen, werden unter keinen Umständen dadurch validiert.
- Unknown: Owner Trust ist unbekannt bzw. wurde noch nicht gesetzt. Von diesem Schlüssel ausgehende Signaturen werden ebenfalls nicht validiert. [gpg17]

Abbildung 2.2 stellt ein WoT und einen dazugehörigen Schlüsselbund dar. Der Schlüssel des Besitzers, hier mit *You* bezeichnet, gilt im Unterschied zu den restlichen Knoten als implizit vertrauenswürdig und ist daher als valide markiert worden:

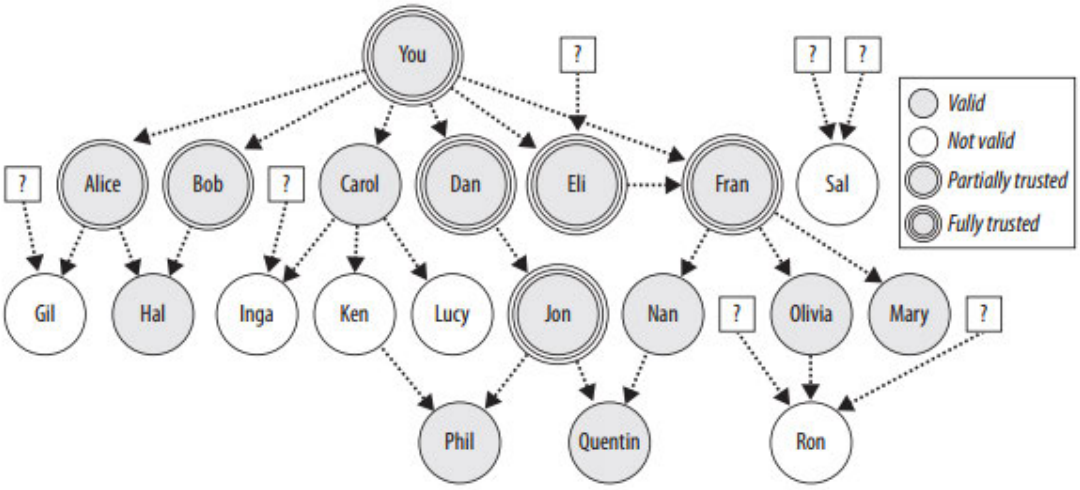

Abbildung 2.2: Web of Trust mit Owner Trust und Key Legitimacy [Vie08]

In diesem Web of Trust sind die verschiedenen Vertrauenslevel des Owner Trusts, als auch die berechneten Vertrauensgrade der Key Legitimacy zu erkennen. Der Vertrauensgrad L übernimmt hierbei die Standardwerte für $X = 2$ und $Y = 1$, sodass Signaturen, die von vollständig vertrauten Knoten ausgehen immer zur Gültigkeit führen. Durch das kumulative Vertrauensmodell des WoT können allerdings auch nur marginal vertraute Knoten andere Knoten validieren.

Alice und Bob wird beiden in der Prüffähigkeit nur teilweise vertraut, sodass sie für den Besitzer nur unter Zusammenarbeit Hal als gültig erklären können. Versucht Alice ohne Hilfe eines anderen marginal vertrauten Knoten zu validieren, so erkennt der Besitzer diesen Knoten nicht als gültig an. Ebenso haben Signaturen, die außerhalb vom Schlüsselbund kommen keine Auswirkung auf die Berechnung der Gültigkeit. Durch die Abbildung lassen sich beide Vertrauensarten auch in den Verbindungen dazwischen und den Knoten selber darstellen. Gültigkeit ist hierbei die Qualität der Knoten (Key Legitimacy), während Vertrauen eine Qualität der Kanten ist (Owner Trust).[Vie08][Mik13]

Die Abbildung visualisiert zudem, wie durch das Sammeln von Kontakten auf seinem Schlüsselbund, eine Art soziales Netzwerk entsteht. Das WoT hat also den Grundgedanken für die heute existierenden sozialen Medien wie Facebook, Instagram und Co. genutzt. Ein gutes WoT zeichnet sich dadurch aus, dass die Kontakte darin hauptsächlich auf echten sozialen Kontakten beruht. Dadurch können Communities aus Nutzern entstehen, die sich alle gegenseitig vertrauen. Diese haben einige Vorteile, wie zum Beispiel die bessere Bestimmung der Vertrauenswürdigkeit von neuen Schlüsseln. Nutzer in einer Community haben generell mehr Signaturen, wodurch sie für außenstehende vertrauenswürdiger erscheinen. Zusätzlich entstehen dadurch mehrere, redundante Verbindungen zwischen den Knoten und die Zertifizierungspfade bleiben kurz, was sich positiv auf die Gültigkeit auswirkt. Dies macht das Netzwerk außerdem robuster, da im Falle eines Schlüsselentzuges, weitere Zertifizierungspfade erhalten bleiben.[AD11] Denn umso weniger Mittelmänner zwischen einem Knoten und dessen Zielknoten liegen, desto mehr Vertrauen herrscht zwischen diesen. Das einfachste Beispiel stellen hierbei serielle Zertifzierungspfade dar. Dabei handelt es sich um Pfade, bei denen Ziel- und Startknoten nur durch einen Pfad verbunden sind:

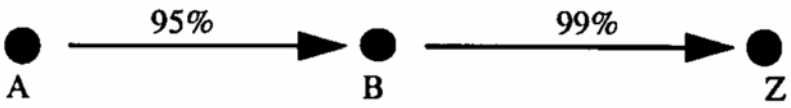

Abbildung 2.3: Serieller Zertifizierungspfad
[Car00]

Abbildung 2.3 zeigt einen solchen Pfad, mit den jeweiligen Wahrscheinlichkeiten für die Gültigkeit der folgenden Knoten. Um das Vertrauen von A in Z zu erhalten, multipliziert man lediglich alle Wahrscheinlichkeiten auf diesem Pfad. Falls angenommen wird, dass ein Knoten mit einer Wahrscheinlichkeit von 90% als valide betrachtet werden würde, so ist Knoten Z mit $0,95 * 0,99 \approx 0,94$ valide. Aus diesem Beispiel ist der Vertrauensverlust über längere Pfade ersichtlich, weswegen die maximale Anzahl an Mittelmännern in PGP generell beschränkt sein sollte. [Car00]

Die positiven Auswirkungen von redundanten Pfaden veranschaulicht Abbildung Abbildung 2.4:

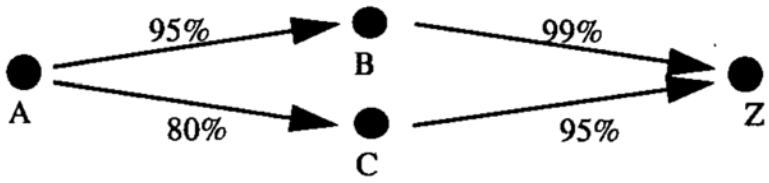

Abbildung 2.4: Paralleler Zertifizierungspfad
[Car00]

Durch die zusätzliche Verbindung über Knoten C kann die Gültigkeit für Z folgendermaßen berechnet werden: $1 - (0.99 - 0.95)(1 - 0.8 * 0.95) \approx 0.98$. Im Allgemeinen lässt sich sagen, dass durch eine erhöhte Kantenanzahl in einem WoT, der Grad des Vertrauens steigt. [Car00] Dadurch kommt es zum sogenannten Kleine-Welt-Phänomen, welches einen Graphen beschreibt, bei den die meisten Knoten nicht benachbart sind, diese aber leicht über den Nachbarn ihrer Nachbarn zu erreichen sind. Der daraus resultierende Graph ist besonders robust und immun gegen plötzlich wegfallende Knoten. [Wik22]

2.1.4 Limitationen und Untergang des Web of Trust

Das Hauptproblem des Web of Trust (WoT) liegt darin, dass es nicht in der Lage war, das Problem zu lösen, für das es entwickelt wurde: „Wie erhält man den richtigen Schlüssel einer Person, die man nicht kennt?“

Der Austausch von PGP Schlüsseln erfolgt zum größten Teil elektronisch über Schlüsselserver. Da die Schlüssel wegen ihrer schlechten Lesbarkeit und großen Länge für Menschen nur sehr schwer zu vergleichen sind, entsteht durch die Komplexität somit ein großes Sicherheitsrisiko. Fingerprints bieten zwar eine kleine Abhilfe, ersetzen aber nicht die eigentlich notwendige, manuelle Authentifizierung eines Menschen. Jedoch ist die manuelle Authentifizierung eine banale Aufgabe für den Menschen und bei geringer Aufmerksamkeit können schnell Fehler anfallen, sodass viele Nutzer diesen Schritt überspringen. Die Folgen von abwesender Authentifizierung können erfolgreiche Man-in-the-Middle Attacks sein. Dieses Problem soll mithilfe dem Einsatz von Schlüsselservern gelöst werden, jedoch besitzen diese eine Reihe von Schwächen. Ein Schlüsselserver, der von einem bösartigen Akteur betrieben wird, kann nach Eingabe eines Fingerprints einen falschen Schlüssel zurückgegeben . Dieser Fehler existierte in einer Version von GNU Privacy Guard, welche die erhaltenen Schlüssel nicht auf den richtigen Fingerprint überprüfte. Obwohl dieser Fehler nur in dieser spezifischen Ausführung von PGP existierte, hinterfragt es die Sinnhaftigkeit von Schlüsselservern und Fingerprints, wenn der direkte Austausch einer tausend langen Zeichenkette eine scheinbar sicherere Methode ist.[A F14]

Im Juni 2019 fand ein Angriff auf das Synchronizing Key Server (SKS) Netzwerk von OpenPGP statt. SKS war das am meisten verbreitete Schlüsselservernetzwerk zu der Zeit und beherbigten einen Großteil der öffentlichen Schlüssel. Die Attacke bestand aus einem Signatur-Spam gerichtet auf bekannte und populäre Mitglieder der OpenPGP Community. OpenPGP sieht keine Limitationen vor, wie viele Signaturen ein Schlüssel erhalten kann. Die Angreifer nutzten diese Schwachstelle in der Implementierung von GnuPG aus und schickten fast 150 000 Signaturen an die Zielschlüssel. Nutzer, die diese Schlüssel schließlich herunterladen wollten, würden somit die Installation von GnuPG

beschädigen und unbrauchbar machen[Rob19]. Die Folge bestand darin, dass eine neue Option `self-sign-only` in die Software eingebaut wurde, welche standardmäßig alle fremden Signaturen eines Schlüssels ignoriert. Damit lassen sich zwar alle Spam-Signaturen umgehen, jedoch auch alle validen Signaturen. Die Echtheit der Person hinter dem Schlüssel ist also so gut wie gar nicht mehr festzustellen, wodurch es zum gänzlichen Vertrauensverlust im WoT kommt.[Max19] [Sch19]

Ein weiteres Problem, das im WoT vorherrscht, ist die fehlende Privatheit bzw. unzureichender Datenschutz. Sobald ein Schlüssel erst einmal auf einem Schlüsselserver hochgeladen wurde, so kann dieser unter keinen Umständen gelöscht werden. Da sich die Schlüsselserver untereinander austauschen und immer synchronisieren, würde ein fehlender Schlüssel nach kurzer Zeit wieder ersetzt werden. Dieses Funktionalität ist beabsichtigt, da nur so sichergestellt werden kann, dass keine Zensur von Dritten vorgenommen wird. Jedoch verifizieren die Schlüsselserver auch nicht ob die Person, welche einen öffentlichen Schlüssel hochlädt auch die Person ist, die diesem Schlüssel gehört. Somit besitzt der Benutzer keine Möglichkeit zu verhindern, dass sein Schlüssel und die daran haftenden Information öffentlich gestellt werden und auch keine Möglichkeit diese zu entfernen. Mithilfe des öffentlichen Schlüsselbundes eines Benutzers, können Angreifer seinen sozialen Kreis ausspähen und sehen in welchen Communities dieser partizipiert.[pgp20]

Während es nicht möglich ist einen Schlüssel selber zu löschen, können Benutzer ein Widerrufszertifikat an ihren öffentlichen Schlüssel hängen, solange sie den dazugehörigen privaten Schlüssel noch besitzen. Diese Art von Signatur zeigt den Benutzern , die den Schlüssel herunterladen, dass dieser widerrufen wurde und nicht mehr benutzt werden sollte [pgp20]. Laut der europäischen DSGVO besitzt allerdings jede Person das Recht auf Löschung ihrer personenbezogenen Daten. Da die Betreiber der Schlüsselserver diesen Anforderungen nicht nachkommen können, wurden diese im Jahr 2021 gezwungen diese endgültig herunterzufahren, sodass das SKS Netzwerk seither nicht mehr operiert. [Imt21][Eur18] Seit dem haben sich zwar neue alternative Schlüsselserver gefunden, wie zum Beispiel *keys.openpgp.org*. Diese teilen allerdings nicht die Prinzipien des WoT, womit es heutzutage kaum noch Anwendung findet und allgemein als gescheitert betrachtet werden kann.[pgp20]

Zusammenfassend lässt sich also über das Web of Trust sagen, dass es für seine damalige Zeit eine adäquate Möglichkeit war, Vertrauen in einer PKI zu generieren. auch wenn die Konzepte des WoT immer noch als robust gelten, stößt das Design heute allerdings an seine technischen und softwareseitigen Grenzen. Während es immer noch für kleine Netze und Communities ausreichend funktioniert, wird die sowieso geringe Skalierbarkeit durch das Fehlen der Keyserver noch weiter behindert, sodass die Nutzung im großen Maßstab so gut wie ausbleibt.

2.2 Reputationsplattformen

Wenn Menschen im echten Leben miteinander interagieren, baut sich mit der Zeit eine Historie an Interaktionen auf, die man miteinander unternommen hat. Beide Parteien haben eine Vorstellung von den Fähigkeiten und Veranlagungen des jeweilig Anderen. Die Angst vor Vergeltung bzw. das Prinzip der Gegenseitigkeit erschafft hierbei den Anreiz für gutes Verhalten. Die Erwartung, dass Menschen die Vergangenheit des anderen in zukünftigen Interaktionen berücksichtigen, schränkt das Verhalten in der Gegenwart ein. Dieses Verhalten wird auch als “Schatten der Zukunft” bezeichnet. [PK00]

Die Abwesenheit eines solchen Schattens und dessen Folgen sind vor allem in digitalen Landschaften aufzufinden, in welchen das Aufbauen von Vertrauen zwischen fremden Personen weitaus schwerer ist. Interaktionen finden größtenteils nur in der Gegenwart statt. Das Fehlen einer Vergangenheit bzw. Aussicht auf zukünftige Interaktionen beseitigen den Anreiz für gutes Verhalten. Demgegenüber fehlen durch Pseudonymisierung auch jegliche Konsequenzen für schlechtes Verhalten, da Nutzer immer neue Identitäten anlegen und durch ihre alten, behafteten Identitäten austauschen können. [PK00]

Reputationsplattformen versuchen diesen Schatten der Zukunft zu etablieren. Sie nehmen den Platz zwischen zwei sich unbekannten Parteien in einer Umgebung ein, in welcher die eine oder beide Parteien ungenügend Informationen übereinander besitzen. Denn nur somit lassen sich Transaktionen zwischen fremden Personen bzw. ein sicherer Informationsaustausch gewährleisten und Urteile über die Vertrauenswürdigkeit eines Nutzers fällen. Das Vertrauen wird hierbei von anderen Nutzern direkt verteilt. Die Art und Weise wie Nutzer ihr Feedback gegenüber äußern können, implementiert jede Plattform unterschiedlich. Die Plattform sammelt das Feedback und stellt die Gesamtheit davon daraufhin adäquat als Reputation dar.[NSS09]

Die Reputation oder Ruf einer Person oder Gruppe, gibt Auskunft darüber wie diese von der Allgemeinheit wahrgenommen wird. Sie leitet sich von einem gegebenen sozialen Netzwerk ab, welches diesem zugrunde liegt und ist für alle Mitglieder des Netzes öffentlich einsichtig. In anderen Worten ist Reputation das kollektive Maß an Vertrauenswürdigkeit, die einer Person oder Gruppierung von anderen zugesprochen wird. Diese Metrik ist wichtig, denn sie gibt Außenstehenden eine Möglichkeit Fremden zu vertrauen. Jedoch ist wichtig zu unterscheiden, dass Personen mit einer schlechten Reputation nicht zwangsläufig nicht vertraut werden kann. Wenn eine Person einer anderen trotz ihres schlechten Rufes vertraut, so ist davon auszugehen, dass die Person privates Wissen über die andere besitzt. Die Meinung der Allgemeinheit spielt eine untergeordnete Rolle für eine Person, die privates Wissen über eine andere besitzt. Dadurch ist Reputation am Besten für Interaktionen geeignet, bei denen persönlicher Kontakt nicht stattgefunden hat, wie der Großteil von Handlungen im Online-Raum. [ARC07]

Reputation stellt hierbei nur eine Form dar, mit welcher Vertrauen digital geäußert werden kann. Typisch für Reputationsplattformen ist, dass ein großer Wert des Vertrauens mithilfe von quantitativen Daten generiert wird. Ein Beispiel wäre die Menge von positiven und negativen Attestierungen, welche die Benutzer sich gegenseitig vergeben. Die Differenz beider Werte kann benutzt werden, um die Reputation zu berechnen, welche ein Benutzer dann erhält. Abbildung 2.5 veranschaulicht dieses und weitere Elemente, mit welchen Vertrauen generiert werden kann.

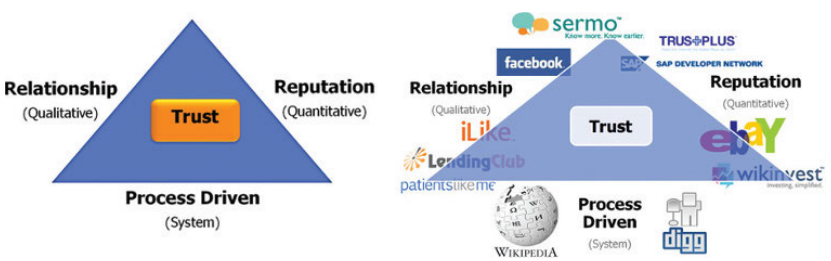

Abbildung 2.5: Reputation als Teil von Online-Vertrauen [Gol09]

Neben quantitativen Modellen, wie zum Beispiel das Rezensionssystem von Ebay und Amazon, existieren auch Modelle welche auf qualitativen Daten, wie Beziehungen zwischen Menschen achten, zum Beispiel Facebook. Ein ausgeschmücktes Profil mit vielen Freundschaften vermittelt einen vertrauenswürdigeren Blick als ein leeres und potentielles Fake-Profil. Zusätzlich gibt es Plattformen, welche Nutzer basierend auf ihren generierten Inhalten bewerten, wie Wikipedia. Hierbei können sich Nutzer einen Namen machen, indem ihre Änderungen und Beiträge an Artikeln beständig positiv aufgenommen werden von anderen Nutzern.

Ein System muss hierbei 3 Hauptfunktionen erfüllen, damit es funktioniert:

- Validieren, ob eine Person die ist, die sie behauptet zu sein.
- Überprüfen, ob eine Person in der Lage ist eine bestimmte Aufgabe auszuführen.
- Überprüfen, ob eine Person das gewünschte Ergebnis beständig liefern kann.

Damit diese Funktionen ausführt werden können, findet eine Datenverarbeitung nach dem EVA-Prinzip statt. [NSS09]

Eingabe - Eine Plattform kann Daten über die Reputation eines Nutzers auf zwei verschiedene Arten sammeln, explizit oder implizit. Explizite Informationssammlung bezieht sich auf Daten, welche direkt von einem Nutzer in das System hinzugefügt werden. Das kann mithilfe von Abstimmungen oder Bewertungen geschehen, was es einfach macht diese Art von Information zu gruppieren und zu summieren. Dadurch lässt sich eine reiche Vergangenheit über verschiedene Nutzer generieren, welche notwendig ist, um Vertrauen zu gewinnen. Die implizite Informationssammlung wird hingegen nicht direkt vom Nutzer beeinflusst und beschreibt Daten, die ohne das Wissen des Nutzers gewonnen werden. Beispiel für diese Art von Daten sind Netzwerkverhaltensdaten oder wie lange ein Nutzer auf einer Website verweilt. Für das Weitergehen dieser Arbeit wird diese Art der Eingabe allerdings eine untergeordnete Rolle darstellen. [NSS09]

Ausgabe - Eine gängige Art, um Reputation auszudrücken ist in Form einer Wertung als Punktzahl, Skala oder als Kommentar. Diese wird meist mit der Person oder Gegenstand angezeigt, welche zu bewerten ist, wodurch andere Nutzer einen direkten Einblick in die historische Qualität erhalten und sich eine Meinung bilden können. Multimediale Eindrücke, wie Bilder und Videos können auch Teil der Ausgabe sein, wodurch die Tiefe einer Bewertung steigt.

Verarbeitung - Die Informationen, welche in ein Reputationssystem fließen können entweder zentral oder dezentral verarbeitet werden. In der ersteren Variante existiert eine zentrale Autorität, welche Kontrolle über die Eingaben der Nutzer hat. Sie sammelt die Eingabeinformationen und stellt daraufhin eine Wertung für das Produkt, den Service oder den Teilnehmern aus. Diese Wertung ist eine Zusammenfassung aller Bewertungen der Nutzer, die dazu eine Bewertung abgegeben haben. [NSS09]

Bewertungen werden meistens in Form von e-voting bzw. e-rating abgegeben, also expliziten Eingabevarianten, deren Statistiken außerdem Zugang zu impliziten Informationen gewährt.

E-rating erlaubt es Nutzern Bewertungen zu verfassen, womit die Qualität einer Transaktion eingestuft werden kann. Rezensionen auf Amazon sind beispielsweise eine Form des e-ratings. Eine wichtige Eigenschaft ist die dadurch entstehende Historie, womit Nutzer gegenseitig ihr vergangenes

Verhalten überprüfen können. [NSS09] Ebay erlaubt es seinen Nutzern ihre Bewertung als positiv (+1), negativ(-1) oder auch als neutral(0) zu kennzeichnen und summiert diese gegeneinander auf, um somit eine Wertung für den Nutzer zu generieren.

E-voting stellt, im Gegensatz zum e-rating, eine Möglichkeit mit Limitationen in der Eingabe dar. Anstelle von aufwendig geschriebenen Texten, Rezensionen et cetera, werden einfachen Abstimmungen wie zum Beispiel Reddit's Upvotes und Downvotes genutzt. Durch den geringeren Zeitaufwand, der benötigt wird, um eine Bewertung abzugeben, wird somit eine erhöhte Partizipation erreicht. Der Nachteil bei dieser Eingabevariante ist, dass die Qualität der erhaltenen Information deutlich geringer ist, weswegen die Verbindung mit impliziten generierten Informationen wichtig ist, um eine aussagekräftige Schlussfolgerung zu ziehen. [NSS09]

Dezentrale Reputationssysteme zeichnen sich durch eine abwesende Zentralbehörde aus, welche Informationen sammelt und auswertet. Stattdessen existiert ein Netzwerk aus dezentralisierten Knoten, welche die Erfahrungen und Meinungen voneinander selber abspeichern. Daraufhin wird ein lokaler Reputationswert berechnet, welcher auf Anfrage an andere Knoten verteilt wird. Wenn ein Knoten mit einem anderen interagieren bzw. prüfen möchte, so muss dieser so viele Bewertungen wie möglich von anderen Knoten einholen, die einen direkten Kontakt mit dem Zielknoten hatten. [ARC07]

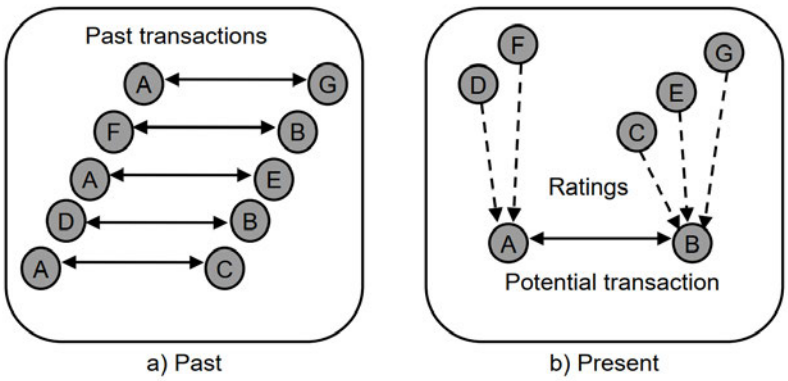

Abbildung 2.6: Aufbau und Funktionsweise von verteilter Reputation [ARC07]

Abbildung 2.6 visualisiert die Funktionsweise, wie Knoten an Reputation in einem solchen System gelangen. Abbildung a) zeigt hierbei die vergangenen Transaktionen zwischen den verschiedenen Usern. Abbildung b) zeigt hingegen, wie die vergangenen Transaktionen aus a) genutzt werden, um Vertrauen zwischen zwei unbekannten Knoten zu berechnen. In diesem Fall möchten Knoten A und B eine Verbindung zueinander aufbauen. Beide Partner suchen dabei zunächst nach anderen Knoten, die in der Vergangenheit mit dem jeweiligen Zielknoten interagiert haben. A entdeckt, dass Knoten D und F bereits in der Vergangenheit mit B interagiert haben, sodass A Die Rating von D und F für B betrachtet. Dieses Prinzip funktioniert analog zu für den Knoten B. Am Ende können beide Knoten A und B einen Schatten der Zukunft über den jeweilig anderen werfen, indem sie das Wissen von Vielen nutzen, um daraufhin zu entscheiden, ob sie miteinander interagieren möchten.

Verteilte Reputationssysteme besitzen zwei Kernaspekte:

- Ein verteiltes Kommunikationsprotokoll, womit Knoten Bewertungen voneinander vergleichen.
- Eine Berechnungsmethode für Reputation, womit die Informationen von verschiedenen gesammelt werden können, um eine Bewertung für einen Zielknoten zu berechnen. [ARC07]

Die Verarbeitung der Wertungen ist davon abhängig, ob die objektiven Aktivitäten eines Peers gemessen werden oder ob subjektive Bewertungen anderer Peers eingebunden werden. Ersteres ist hierbei ähnlich wie das Auswerten von impliziten Informationsströmen wie Statistiken und daher einfach realisierbar. Die subjektiven Bewertungen von anderen Peers zu verwenden ist allerdings weitaus schwieriger als das Äquivalent von zentralen Systemen wie e-rating und e-voting. [NSS09]

Peer-to-Peer (P2P) Netzwerke sind ein gutes Beispiel für ein Ökosystem, in welchem dezentrale Reputationssysteme angewandt werden können. Da in einem P2P Netzwerk alle Knoten sowohl die Rolle eines Clients, als auch Servers übernehmen, spielen die Teilnehmer eine aktive Rolle in allen Schritten der Vertrauensgewinnung. Der Ablauf eines solches Systems lässt sich in zwei Phasen einteilen, die Suchphase und Download-Phase. Der erste Teil besteht darin, die gewünschten Knoten im Netzwerk zu lokalisieren, welche die nötigen Information für eine Reputationsbewertung besitzen. Dieser Part kann auch von einer zentralisierten Instanz übernommen werden. Im zweiten Teil, der Download-Phase, geht es darum die lokalisierten Information auf den eigenen Knoten zu übertragen, woraufhin sie verwendet werden können. [ARC07]

2.3 Bewertungsmechanismen im Web 2.0

Während das Web 1.0 vorwiegend als ein einseitiges Übertragungsmedium angesehen werden kann, fördert der Aufstieg von Web 2.0 und die dadurch verbundenen ansteigenden Nutzerzahlen aktiv den Diskurs der Benutzer untereinander. Informationen werden aus Dialogen und nicht mehr aus Monologen gewonnen.[Gol09] Einige Hauptprinzipien des Web 2.0 inkludieren:

- Individuelle Nutzergenerierte Inhalte
- Die kollektive Intelligenz der Benutzer wahrzunehmen
- Eine Architektur der Partizipation [NSS09]

Diese Prinzipen haben zusammen einen starken Eindruck hinterlassen und heutige Reputationsplattformen maßgeblich geformt. Sie zeichnen sich durch große Partizipation der Nutzer aus, wodurch riesige Datenmengen entstehen. Die Verarbeitung solcher Datenmengen geben wertvolle Einsichten in das Verhalten der Nutzer, sodass Online-Handel sich besser auf die Konsumenten einstellen kann. Amazons Online Review System ist ein Paradebeispiel für ein Web 2.0 Reputationssystem und gleichzeitig Teil einer der erfolgreichsten E-Commerce Plattformen. Diese soll im folgenden Abschnitt genauer untersucht werden.

2.3.1 Amazon

Das Bewertungssystem von Amazon stellt einen zentralen Bestandteil der Plattform dar. Es ist für Kunden die einzige Möglichkeit Informationen über die Qualität eines Produkts oder Verkäufers auf der Seite zu erhalten. Bewertungen sind das Hauptmotiv für Kaufentscheidungen der Kunden und schützt diese vor schlechten Produkten. Dadurch haben sowohl der Kunde, als auch Amazon selber daran Interesse, dass Bewertungen aussagekräftig und authentisch sind.[AJ19]

Kunden können Produkten auf Amazon mithilfe einer 5-Sterne Skala bewerten, wobei 1 Stern die schlechteste und 5 Sterne die beste Bewertung ist. Anschließend müssen Benutzer eine textliche Evaluation ihrer Erfahrung hinterlassen und ihre Entscheidung begründen. Die gepostete Bewertung kann nachfolgend noch von anderen Benutzern bewertet werden, wobei diese als “hilfreich” und “nicht hilfreich” eingestuft werden kann. Die Bewertungen aller Nutzer werden aggregiert und die durchschnittliche Anzahl an vergebenen Sternen angezeigt. [AJ19]

Im Jahr 2015 wurde die Berechnung des Durchschnitts verändert und bezieht nun einige Bewertungen mehr ein als andere. Während vorher alle Bewertungen als gleichwertig angesehen wurden und nur die Anzahl der vergebenen Sterne berücksichtigt wurde, wurden nun weitere Faktoren für die Berechnung betrachtet. Unter anderem spielt das Alter einer Bewertung eine Rolle, als auch die Länge und Detailreichhaltigkeit der Beschreibung.[Fee19a] Als weitere Vertrauensmetrik können Nutzer sich ihren Kaufstatus verifizieren lassen, wodurch ihre Bewertung eher berücksichtigt wird und anderen Nutzern Authentizität sichert. Bewertungen ohne solcher Verifizierung werden nicht in die Berechnung einbezogen, solange ein Nutzer nicht weitere Details wie Text, Bild oder Video hinzufügt. Mithilfe von maschinellem Lernen, können nach eigenen Angaben somit Bewertungen hoher Qualität und Authentizität von weniger authentischen separiert werden. [Ama22]

Neben Produkten können auch Verkäufer direkt bewertet werden, solange der Kunde vorher ein Produkt von diesem gekauft hat. Auf dessen Profil wird eine aggregierte Wertung aus den letzten 12 Monaten angezeigt, sowie die Anzahl aller positiven, negativen, als auch neutralen Bewertungen in verschiedenen Zeiträumen. Abbildung 2.7 und Abbildung 2.8 zeigen ein Beispiel für ein Verkäuferprofil und dessen Bewertungen. Diese wurden in ein einmonatigen, dreimonatigen und jährlichen Zeitraum unterteilt, wobei Abbildung 2.7 veranschaulicht, dass nur Bewertungen der letzten 12 Monate in die Gesamtwertung fließen. Die anderen Zeiträume erlauben den Benutzern einen Einblick in die Historie und Entwicklung des Verkäufers zu erlangen, wodurch ein Schatten der Zukunft geworfen wird. [AJ19]

Abbildung 2.7: Amazon Verkäufer Profil
[Ama22]

	30 Tage	90 Tage	12 Monate	Laufzeit
Positiv	66%	69%	87%	81%
Neutral	3%	3%	5%	4%
Negativ	31%	28%	7%	15%
Anzahl	32	78	395	1.017

Abbildung 2.8: Anzahl Bewertungen eines Verkäufers auf Amazon
[Ama22]

In einem 2018 veröffentlichten Datensatz von Amazon werden alle Daten von ca. 223 Millionen Bewertungen und deren Metadaten zusammengefasst. Ein Beispiel für den Aufbau einer Bewertung von Amazon lässt sich in Abbildung 2.9 sehen. Hierbei werden folgende Daten gesammelt:

- reviewerID - ID des Bewerters
- asin - Id des Produkts
- reviewerName - Name des Bewerters
- vote - Anzahl der Nutzer, die die Bewertung als hilfreich markiert haben.
- style - Ein Dictionary Datentyp für jeweilige Metadaten
- reviewText - Text des Reviews
- overall - Anzahl der vergebenen Sterne
- summary - Zusammenfassung der Bewertung
- unixReviewTime - Zeitpunkt der Bewertung in unix Zeit
- reviewTime - Zeitpunkt der Bewertung
- image - Bilder des bewerteten Produkts [JJJ19]

Zur Bestimmung der Authentizität einer Bewertung, wird vor allem auf die Werte *true* und die Nutzer Abstimmungen vote geachtet, als auch auf die Länge von *reviewText*. Für die durchschnittliche Bewertung wird zusätzlich auf die Werte der *overall* Sterne-Bewertung geachtet, sowie den Zeitpunkt der Rezension *reviewTime*. Bewertungen die nicht als authentisch oder sogar als gefälscht identifiziert werden können, gehen mit geringerer bzw. gar keiner Wertung in die Berechnung ein. [Fee19a]


```
{
"image": ["https://images-na.ssl-images-
amazon.com/images/I/71eG75FTJJL._SY88.jpg"],
"overall": 5.0,
"vote": "2",
"verified": True,
"reviewTime": "01 1, 2018",
"reviewerID": "AUI6WTTT0QZYS",
"asin": "5120053084",
"style": {
        "Size:": "Large",
        "Color:": "Charcoal"
        },
"reviewerName": "Abbey",
"reviewText": "I now have 4 of the 5 available colors of this
shirt... ",
"summary": "Comfy, flattering, discreet--highly recommended!",
"unixReviewTime": 1514764800
}
```


Abbildung 2.9: Ein Beispiel für die Daten einer Bewertung

Dennoch kann Amazon nicht alle Bewertungen von gefälschten und echten unterscheiden. Tatsächlich stellen sogenannte fake Reviews eine riesiges Problem dar, welches seid Jahren versucht wird zu bekämpfen. Laut Fakespot, einem Plugin, das es erlaubt Bewertungen auf Echtheit und Vertrauenswürdigkeit zu prüfen, sind 42% aller Rezensionen auf Amazon gefälscht. Neben Fakespot gibt es auch Websites wie Reviewmeta, welche sich auf Amazon konzentriert und potentiell gefälschte Bewertungen herausfiltern kann. allerdings fehlen diesen Anwendungen die proprietären Daten Amazons, wie zum Beispiel aus Abbildung 2.9 und die dazugehörigen Metadaten, wodurch die Effektivität der angewandten Algorithmen laut Amazon unbekannt bleibt. Jedoch untergräbt die bloße Existenz externer Programme schon die Vertrauenswürdigkeit des Reputationssystems. [Lee20]

Zum Erstellen von Fake Reviews werden immer wieder neue Wege gefunden, um Schwachstellen im System auszunutzen. Zum Beispiel kaufen einige unseriöse Händler ihre Produkte mit einem neuen Account selber und lassen das Produkt an zufällige Haushalte schicken, um anschließend Rezensionen mit dem verifizierten Kaufstatus zu schreiben.[Car17] Das traditionelle Einkaufen von Bewertungen stellt eine zusätzliche Bedrohung für die Authentizität der Plattform dar. Bestechungen des Kunden mit Gutscheinen und Geldgeschenken sind weiterhin eine weit eingesetzte Praxis, obwohl es gegen die Richtlinien von Amazon geht und die Firma stark dagegen vorgeht. [Der21][The22] So werden immer wieder Firmen von Amazon verklagt, welche es sich zum Geschäft gemacht haben gefälschte Bewertungen zu verkaufen. [Bis22] Doch das Problem reicht auch bis in das Firmeninnere, in welchem festgestellt wurde, dass Mitarbeiter Bestechungsgelder angenommen haben, um negatives Feedback zu löschen. [Fee19b]

Doch auch abseits der Authentizität, stellt die Transparenz der Darstellung einer Bewertung durch die 5-Sterne Skala einen Schwachpunkt dar. Während sie sehr simpel und schnell zu lesen ist, gibt die Skala kaum einen Ausblick über die tatsächliche Qualität eines Produkts. In der Kategorie “Bücher” sind 90% der Bewertungen im 3-5 Sterne Bereich. Wenn man davon ausgeht, dass 3 Sterne für ein durchschnittliches Produkt steht, man also die gesamte Skala benutzt, entsteht ein falsches Bild, da dies nicht der Fall ist. Der tatsächliche Durchschnitt einer Buchbewertung liegt bei 4.3 Sterne, sodass ein Buch mit einer Bewertung von 4 Sternen bereits als unterdurchschnittlich angesehen werden muss.[Car17] Es ist also nicht nur der Ursprung der Bewertungen selber irreführend, sondern auch die Darstellung.

Zusammenfassend sollten Bewertungen auf Amazon nicht vollständig vertraut werden, ohne sich vorher eine Reihe aus scheinbar echten Nutzern herauszusuchen, welche echte Bewertungen geschrieben haben. Zusätzlich können Tools wie Reviewmeta oder Fakespot benutzt werden, um einige Fälschungen herauszufiltern und das System transparenter zu machen. Neue Nutzer, welche allerdings kein Vorwissen über das Reputationssystem besitzen und was es dabei zu beachten gilt, leiden sehr wahrscheinlich unter den genannten Nachteilen und werden getäuscht.

2.4 Bestehende Bewertungsmechanismen im Web 3.0

Das heutige Internet ist dominiert von Technologieunternehmen, welche einen Großteil der Infrastruktur und Dienstleistungen des Internet betreiben, um im Gegenzug Geld an persönlichen Daten zu verdienen. Durch diese Monopolisierung können einige wenige Akteure entscheiden, welche Inhalte ein Großteil der Nutzer sieht und diese nach Belieben zensieren. Web3 bezeichnet hierbei Anwendungen, welche auf der Ethereum-Blockchain existieren. Diese Anwendungen können von jedem Menschen weltweit benutzt werden, solange sie eine Internetverbindung haben. Es existiert keine Instanz, welche es verbieten kann einen Service zu benutzen und Zahlungen durchzuführen.

Beide Ansätze haben Vorteile und Nachteile. Zentrale Anwendungen haben meist eine bessere Leistung und sind einfacher zu implementieren, leiden jedoch unter Zensur und sind anfälliger für Angriffe. Das ganze System kann abgerissen werden, sollten böswillige Akteueren die zentrale Authorität erfolgreich angreifen (Single Point of Failure). Dezentrale Anwendungen leiden zwar unter Performance Einbußen und einer komplexeren Implementation, sind allerdings auch weitaus robuster und inklusiver.[eth22]

Neben Dezentralisierung und Berechtigunsfreiheit ist eine weitere Eigenschaft vom Web3, dass es kein Vertrauen braucht, um zu funktionieren. Statt sich auf vertrauenswürdige Dritte zu verlassen, werden wirtschaftliche Anreize genutzt, um Nutzer zum positiven Handeln zu bringen. Dieser Ansatz hat zur Folge, dass das Web3 im momentanen Zustand unter einer Hyperfinanzialisierung leidet, in welchem alle Vermögenswerte finanzieller Natur sind und gehandelt werden können. Obwohl Blockchain Technologien inhärent kein Vertrauen benötigen, um zu funktionieren, kann das Einbinden von Vertrauen neue Anwendungsfälle eröffnen und bereits existierende bereichern.[BOW22]

2.4.1 Soulbound Tokens

Im März 2022 wurde ein Forschungsbericht namens “Decentralized Society: Finding Web3’s Soul” von Vitalik Buterin, E. Glen Weyl und Puja Ohlhaver veröffentlicht, in welchem die Autoren von einer neuen Möglichkeit berichten, um soziale Beziehungen basierend auf Vertrauen im heutigen Web3 zu erschaffen. Die dort dargestellte Vision bietet eine Reihe von neuen Anwendungsfällen, welche näher erläutert werden sollen.[BOW22]

Soulbound Tokens sind öffentlich einsehbare, nicht transferierbare, aber widerrufbare Tokens. Diese Eigenschaften wurden gewählt, da diese besonders leicht zu implementieren sind mit den gegebenen technologischen Grundlagen der Blockchain. Allerdings ist die Privatheit von Tokens ein wichtiges Thema und könnte daher in der Zukunft auch eine Eigenschaft von ihnen sein. Als Souls (dt. Seelen) werden Accounts oder Wallets bezeichnet, die diese Tokens halten. SBTs können eine Reihe von Dingen darstellen, wie zum Beispiel Bescheinigungen, Affiliationen oder anderweitige Zugehörigkeiten. [BOW22]

Seelen können sich SBTs selber ausstellen (wie bei einem Lebenslauf) oder andere Seelen damit attestieren. Sie können verschiedene Entitäten darstellen, wie zum Beispiel Unternehmen, Stiftungen oder Einzelpersonen. Zu beachten ist hierbei, dass eine Seele nicht unbedingt zu einer Person gehören muss. Da es keine Bedingung ist, zu überprüfen, ob jede Person genau eine Seele besitzt, ist davon auszugehen, dass sie mehrere Pseudonyme anlegen wird. Die Identität ließe sich beispielsweise mit besonderen SBTs ausdrücken, welche eine echte Identität bestätigen. Eine weitere Herangehensweise besteht darin, die Möglichkeit von mehreren Seelen so zu nutzen, dass eine Person verbesserte Privatheit erhält. So lassen sich die eigenen Interessen in verschiedene Seelen einteilen, welche in verschiedenen Gemeinschaften oder DAOs partizipieren, wie zum Beispiel eine für Hobbys, eine für Bildung et cetera.[BOW22]

Durch das entstehende Ökosystem aus Seelen und SBTs wird der Aufbau von sozialen Beziehungen zwischen Individuen verstärkt. Durch die geschaffene soziale Identität eröffnen sich im Web3 Bereich neue Anwendungsfälle, wie zum Beispiel das Erschaffen von unterbesicherten Kreditmärkten mithilfe von Reputation, das Messen von Dezentralisierung oder auch das Verhindern von Kooperation bei Abstimmungen. Dieses Netzwerk wird von den Autoren als Decentralized Society (DeSoc) bezeichnet und beschreibt ein stochastisches, soziales und pluralistisches Ökosystem. Es ist von unten nach oben aufgebaut und nicht von oben nach unten wie im Web2, bei denen jegliches Vertrauen auf zentrale Instanzen zurückzuführen ist. Während die Blockchain es erlaubt, den Zeitpunkt der Erstellung eines Objektes zurückzuverfolgen, können SBTs dabei helfen, ihre soziale Provenienz zurückzuverfolgen. Damit lassen sich Seelen und die Dinge, an denen sie beteiligt waren, in einen

sozialen Kontext einordnen, wodurch Einzigartigkeit entsteht. Für Kunstwerke bedeutet dies zum Beispiel, dass Fälschungen sehr einfach erkannt werden können, da ihnen der soziale Kontext fehlen würde, in welchem sie entstanden sind.[BOW22]

sozialer Kontext erlaubt es Herausforderungen im momentanen Web3 Ökosystem zu überwinden. Momentan ist es in diesem nicht möglich eine unbesicherte Kreditvergabe durchzuführen, da alle Vermögenswerte transferierbar und verkäuflich sind. Traditionelle Finanzmärkte nutzen dafür zentralisierte Bewertungen über Kreditwürdigkeit eines Individuum. Kreditnehmer, die nicht genügend Beweise für ihre Kreditwürdigkeit aufbringen können, wie ärmere Menschen oder Minderheiten, werden in diesem System benachteiligt. SBTs erlauben es ein zensurresistententes Sozialkreditsystem zu erschaffen, in welchem relevante Informationen, wie zum Beispiel Abschlüsse und Arbeitshistorie als SBT dargestellt werden können. Darlehen könnten ebenfalls vom Darlehensgeber als SBT an den Kreditnehmer attestiert werden. Diese behält die Seele solange, bis ihre Schulden abgebaut sind, an welchem Punkt der Token zurückgezogen wird und mit einem ersetzt wird, welcher als Zahlungsnachweis dient. [BOW22]

Zusätzlich haben SBTs das Potential ein wichtiges Werkzeug für das Messen von Pluralismus innerhalb eines Netzwerkes zu sein. Besonders DAOs sind gefährdet von Sybil-Attacken oder ähnlichen Angriffen, bei welchen faire Abstimmungen manipuliert werden können. Mithilfe eines sozialem Kontext können wahrscheinliche Sybil-Nutzer oder Bots von echten, SBT-reichen Seelen unterschieden werden. Ebenfalls können somit Korrelationen zwischen Seelen erkannt werden, welche gleich abstimmen. Diesen Seelen wird automatisch ein geringeres Stimmrecht zugewiesen, da es sich um (zufällig) koordinierte Gruppierungen handeln können, die eine Abstimmung aus Versehen oder absichtlich in eine bestimmte Richtung bewegen. Das momentane Web3-Ökosystem ist anfällig für diese Formen der Zentralisierung, wodurch es schwierig ist die wahrhaftige Dezentralisierung in einem Netzwerk zu bestimmen. Soziale Abhängigkeiten, schwache Zugehörigkeiten, und starke Solidaritäten sind gute Metriken, um die Dezentralisierung in DAOs, Netzwerken oder Protokollen zu messen. Es ist davon auszugehen, dass das Ergebnis einer Abstimmung für welches eine große Anzahl von unterschiedlichen, nicht korrelierten Seelen stimmen, besser für die Allgemeinheit ist, als eins für welches eine große Anzahl von korrelierten Seelen stimmen, die die selben Interessen verfolgen. Mit anderen Worten: Ein Votum, welches zwar weniger, aber dafür unterschiedlichere und unabhängigere Seelen vereinigt ist wahrscheinlich förderlicher für eine Gemeinschaft, da sie die Zustimmung von vielen einzigartigen Persönlichkeiten sammelt und sollte daher mehr gewichtet werden. Bei vielen ähnlichen und korrelierenden Seelen ist davon auszugehen, dass das Ergebnis einer Abstimmung nur die Interessen dieser einen bestimmten Gruppierung vertritt und daher alle außerhalb der Gruppe benachteiligt. Ein reiches Ökosystem von Seelen und SBTs wäre also ein bedeutender Schritt in Richtung echter Dezentralisierung, welches Diversität und Pluralismus fördert.[BOW22]

Die hier beschriebene Vision der Autoren stellt natürlich auch einige Herausforderungen dar, welche vorher gelöst werden müssen. Das Offenlegen der Beziehungen zwischen Seelen zueinander könnte zu Spannungen führen, bei welchen Seelen ausgeschlossen werden, wenn sie nicht die selben SBTs besitzen wie andere. Diese Form der Diskriminierung wäre mit dem oben beschriebenen Szenario in der Lage automatisiert zu werden. Digitale Infrastruktur wird nicht inhärent demokratisch mithilfe von SBTs, vielmehr stellt es das Werkzeug dar, wodurch vorhandene Strukturen demokratisiert werden können. Obwohl DeSoc Muster besitzt, die in ein dystopisches Szenario enden könnten, befindet sich der momentane Stand des Web2 und Web3 auf einem Pfad der unausweichlich dystopisch zu

betrachten ist. In beiden Systemen ist der meiste Reichtum in einer kleinen Nutzerbasis konzentriert, welcher dadurch den meisten Einfluss ausüben kann. Während diese Eigenschaften im Web2 schon weitgreifende Folgen hat (Monopolisierung von großen Tech-Firmen), ist der momentane Stand von DeFi im Web3 ähnlich. Obwohl explizite Formen der Zentralisierung umgangen werden können, existiert kein Mechanismus, um implizite Zentralisierung in Form von Absprache und Marktmacht zu verhindern. Mithilfe von sozialer Identität ist es möglich, diese Strukturen aufzubrechen und die Interessen von verschiedenen Menschen über einem breiten Netzwerk zu vertreten, wodurch SBTs ein wichtiger Schritt in Richtung eines weniger autoritären Internets zu sein.[BOW22]

2.4.2 Verifiable Credentials

In der analogen Welt werden Dokumente, Zeugnisse und Ausweise gebraucht, um die Identität einer Person oder deren Fähigkeiten zu beglaubigen. Mithilfe von Verifiable Credentials ist es möglich, diese Beglaubigungsschreiben in die digitale Welt zu übertragen und zu nutzen. Hierbei beschreiben Verifiable Credentials einen W3C Standard, der erklärt, wie man diese digitalen Beglaubigungen kryptographisch sichert, Privatsphäre respektierend und automatisch verifizierbar macht. Die Credentials können hierbei alle Arten von Daten und Dokumenten repräsentieren, unabhängig davon ob es eine Äquivalent in der physischen Welt dazu gibt. Nicht nur ist es möglich, dass dadurch neue Bescheinigungen entstehen, diese sind auch mithilfe von digitalen Signaturen sicherer und dadurch auch vertrauenswürdiger. [SLC22]

Jedes Verifiable Credential (VC) wird von einem Issuer erstellt. Issuer können hierbei Einzelpersonen, Organisationen oder andere Einrichtungen sein, welche die Informationen auf dem VC bestätigen können, wie zum Beispiel eine Universität für ein Abschlusszeugnis. Die Person, welcher das VC zusteht bzw. besitzt wird auch als Holder bezeichnet und wahrt dieses in ihrer Wallet auf. Daraufhin kann der Holder die im VC hinterlegten Informationen beweisen und einem Verifier vorlegen. Der Verifier hat nun die Möglichkeit, den ihm vorgelegten Informationen zu vertrauen oder nicht. Hierbei muss die Entität betrachtet werden, welche die Bescheinigung ausgestellt hat, da nicht alle Issuer gleich vertrauenswürdig sind für den Verifier. [ver21] Diese Situation kann verglichen werden mit Reisepässen aus verschiedenen Ländern. Jedes Land hat unterschiedliche Vorschriften, was die Herkunft von Einreisenden angeht.

Um die Sicherheit zu gewährleisten, überprüfen Verifier die digitale Signatur mit welcher das VC unterschrieben wurde. Somit kann gewährleistet werden, dass die Bescheinigungen von einem echten Issuer kommt und sich nicht um eine Fälschung handelt. Mithilfe eines vertrauenswürdigen Datenregisters, wie zum Beispiel einer Blockchain, lassen sich die öffentlichen Schlüssel eines jeden Issuers finden und jegliche dessen Signaturen validieren. [Mic20]

Der Prozess des Vorzeigens eines VC von einem Holder gegenüber einem Verifier wird auch als Verifiable Presentation (VP) bezeichnet. VPs stellen Informationen von einem oder mehreren VCs dar und sind so verpackt, das die Aussteller der Daten immer noch verifizierbar sind. Somit kann der Nutzer sich eine Reihe von VPs aufbauen, welche alle einen Teil seiner Persönlichkeit widerspiegeln, wie zum Beispiel für Gesundheit, Beruf usw., um damit seine Privatheit zu schützen. [SLC22]

VCs bilden eine exzellente Ergänzung zu den Datenschutzbedenken von SBTs, da die Informationen, welche auf SBTs stehen, inhärent öffentlich sind. Solange die Tokens keine zusätzlichen Funktionen erhalten, womit die Zugänglichkeit zu sensiblen Inhalten gesenkt wird, ist es unangemessen, sensible Daten auf SBTs zu lagern. Diese Lücke könnten VCs füllen und das SBT-Ökosystem somit bereichern. Jedoch ist das Prinzip nach welchem VCs Privatsphäre handhaben inkompatibel mit der Vision von DeSoc. Die selektive Offenlegung von Information ist nicht vereinbar mit den in Kapitel 2.4.1 veranschaulichten Anwendungsfällen. Wenn Seelen nicht ihre gehaltenen SBTs mit anderen Seelen teilen wollen, so ist es unmöglich eine Decentralized Society aufzubauen, da somit das Vertrauen entfernt wird und das System anfälliger für Angriffe wird. Das Verlangen nach einseitiger Privatheit, welches durch VC geschaffen wird, erschwert das Aufbauen von Relationen und demnach auch Vertrauen zwischen zwei Personen, da der Schatten der Zukunft somit verschleiert werden kann. [BOW22]

2.4.3 Proof of Personhood

Proof of Personhood (PoP) beschreibt ein Konsens Protokoll, bei dem jeder Teilnehmer in einem Netzwerk das selbe Stimmrecht und Belohnungen erhält. Proof of Personhood unterscheidet sich zu anderen Konsensmechanismen dadurch, dass es hierbei egal ist, wie stark ein Teilnehmer in einer Aktivität oder Ressource investiert ist. Proof of Stake und Proof of Work zeichnen sich dadurch aus, dass Teilnehmer Belohnungen korrelierend mit ihrem Investment erhalten. Bitcoin und viele seiner Forks benutzen Proof of Work, um ihr Netzwerk zu sichern. Dieser Ansatz benötigt nicht nur eine hohe Menge an Energie, sondern auch spezielle Mining Hardware, wodurch das Netzwerk in den Händen einiger weniger, privilegierten Nutzern liegt, welche sich diese Kosten leisten können. Proof of Stake wird ebenfalls zur Netzwerksicherung und Konsens benutzt, verwendet allerdings viel weniger Energie, indem das Mining mithilfe bereits existierender Wertgüter vollzogen wird. Dieser Konsensmechanismus leidet allerdings unter dem selben Nachteil wie Proof of Work und zwar, dass reiche Nutzer einen klaren Vorteil haben und mehr Tokens schneller erzeugen können. [Bor+17]

Proof of Personhood versucht diesen Prozess zu demokratisieren und führt ein System ein, bei dem jeder Teilnehmer die gleiche Anzahl von Belohnung für die Partizipation erhält. Die gängigste Methode, um die Identität einer Person zu überprüfen und zu gewährleisten, dass jeder nur einmal teilnimmt, stellt KYC dar. Know Your Customer (KYC) benötigt das Vorlegen von Dokumenten, welche die Identität eines Menschen nachweisen. Weitere Methoden inkludieren das Einsetzen von Biometrie oder gleichzeitig stattfindenden, globalen Key Signing Parties wie im WoT. Dadurch lässt sich ebenfalls eine moderate Sybil Resistenz aufbauen, also Schutz gegen einen Angriff, bei welchem ein Angreifer mit einer Reihe von falschen Identitäten versucht einen Vorteil zu erlangen. Dieser Angriff wird in Kapitel 2.5.1 näher erklärt. Mit PoP Protokollen können somit also eine Reihe von individuellen Identitäten aufgebaut werden. [Hum22] [BOW22]

Der Unterschied zu SBTs liegt darin, dass diese individuellen Identitäten sich auf Einzigartigkeit beschränken. SBTs versuchen hingegen soziale Identitäten zu erschaffen, wodurch PoP für Anwendungen beschränkt ist, in welchen alle Menschen als gleich behandelt werden. Die Anwendungsfälle mit denen sich SBTs beschäftigen, benötigen allerdings mehr als nur Einzigartigkeit. Relationen und Solidaritäten sind das, was Menschen voneinander differenziert und womit Entscheidungen getroffen werden, welche Vertrauen voraussetzen. Zusätzlich sind Proof of Personhood Ansätze wahrschein-

lich für die meiste Zeit nicht Sybil resistent, da es immer Menschen geben wird, welche sich noch nicht für ein PoP Service registriert haben. Diese Menschen könnten von böswillige Akteure rekrutiert oder bestochen werden, um ihre Identität an sie abzugeben.

2.5 Probleme und Angriffsvektoren

Jedes Reputationssystem wird ab einer bestimmten Größe ein attraktives Angriffsziel für Angreifer. Es ist also wichtig, sich vorab Angriffsszenarien vorzustellen und wie man diese am Besten verhindert. Der folgende Abschnitt wird einige gewöhnliche Angriffsszenarien nennen und erklären, wie SBTs helfen können, um dagegen vorzugehen. Denn auch SBTs besitzen Limitationen, welche vorher geklärt werden müssen. Sollten diese Technologie in der Zukunft einen signifikanten Teil unsere digitalen Identität ausmachen, so ist davon auszugehen, dass es Seelen geben wird, welche sich einen unfairen Vorteil gegenüber anderen verschaffen wollen. Ähnlich wie bei Amazon könnten neue Geschäftszweige entstehen, die es sich zur Aufgabe gemacht haben gefälschte SBTs zu verkaufen. Mit einem groß genügendem Netzwerk könnten somit auch gefälschte Seelen und SBTs authentisch wirken, wodurch die Pfeiler des Vertrauens in einer DeSoc zerbrechen. Lösungen wie das Fördern von Whistleblowern, Bestrafen von kollusiven Gruppen oder Aufbauen von Relationen im echten Leben könnten wertvolle Herangehensweisen sein, um dieses Problem zu lösen. Dadurch entwickelt sich ein komplexer Zweig, welcher definitiv eine Rolle in zukünftigen Forschungsarbeiten spielen wird.[BOW22]

2.5.1 Sybil Attacks und Denunziation

Eine Sybil Attacke beschreibt einen Angriff, bei der ein böswilliger Akteur versucht die Kontrolle über eine Netzwerk zu erlangen, indem er mehrere Accounts bzw. Knoten erstellt. Mit genügend falschen Identitäten können somit Abstimmungen in DAOs manipuliert werden, um das Stimmrecht des Angreifers zu verstärken. In Abstimmungssystemen, welche für jede Abstimmung ein Token benötigt, können Angreifer einfach 51% der Tokens sammeln, um eine Mehrheit durchzusetzen und die restlichen 49% ignorieren. Das Anlegen von neuen Wallets ist mit keinen Kosten verbunden, sodass eine einzelne Person sich unendlich viele Identitäten anlegen kann. Diese Eigenschaft ist beabsichtigt, da sie einen wichtigen Teil der zensurresistenten Natur der Blockchain ausmacht. [CF05] [BOW22]

Besonders die Effektivität von Reputationssystemen leidet allerdings, sobald Nutzern die Möglichkeit gegeben wird mit einer neuen Identität von vorn zu beginnen. Seelen mit einer schlechten Reputation müssten hierbei ihren bisherigen Fortschritt aufgeben, um eine neue Identität aufzubauen, wodurch böswillige Akteure immer eine Möglichkeit haben zurückzukommen. Aus diesem Grund sollte neuen Nutzern grundsätzlich nicht vertraut werden, solange sie sich noch keinen Namen gemacht haben. Ansätze mithilfe von PoP können hierbei Verwendung finden, um Teilnehmern ein einmaliges Pseudonym zu verteilen.[ARC07]

Sybil Attacken können sich in einer Reihe von verschiedenen Formen manifestieren. Eine offensichtliche Methode stellt hierbei das Akkreditieren von positiven Bewertungen für sich selbst dar. Dabei kann ein böswilliger Akteur eine Reihe von verschiedenen Identitäten anlegen und diese benutzen, um sich selbst in einem besseren Licht dazustellen. Umgekehrt kann dieser Mechanismus benutzt

werden, um Rivalen mit Bewertungen zu spammen. Hierbei ist es egal, ob es sich um positive oder negative Bewertungen handelt, da beide das Angriffsziel in einem unseriösen Licht hinterlassen. Eine Reihe von negativen Bewertungen senken die Reputation des Ziels, während offensichtliche, positive Falschbewertungen Maßnahmen zur Betrugsverhinderung auslösen können. Bei dieser Form der Denunziation ist es besonders schwer den Angreifer zu ermitteln.

Mithilfe von SBTs können solche Angriffe sehr stark eingeschränkt werden, um Sybil Resistenz aufzubauen. Seelen ohne einzigartigen SBTs können leicht von authentischen Seelen mit einer reichen SBT-Diversität unterschieden werden. Somit können Seelen als Sybil identifiziert werden und ihnen jegliches Abstimmungsrecht entzogen werden. Alternativ kann man auch einzigartigen Seelen ein höheres Stimmrecht zuteilen, sodass aktive Nutzer, welche sich eine Reputation bereits aufgebaut haben belohnt werden und weniger dazu geneigt sind sich neue Identitäten zu schaffen. Im Falle von Denunziation können die Seelen, von welchen die Bewertungen ausgehen kontextualisiert und daraufhin entschieden werden, ob es sich um ehrliche Äußerungen oder einen Angriff in Form Denunziation handelt.[BOW22]

2.5.2 Identitätsverlust

Ein wichtiges Szenario, welches es zu betrachten gilt, ist der Verlust einer Seele bzw. wie dieser zu Verhindern ist. Da Seelen in einer richtigen DeSoc eine Reihe von wichtigen Daten halten werden, könnte der Verlust enorme Konsequenzen für den Besitzer haben. Da die zugrunde liegenden Wallets auf einer PKI basieren, können diese mit einem privaten Schlüssel wiederhergestellt werden, den nur der Besitzer kennt. Die meisten Wallets geben den Nutzern stattdessen die Möglichkeit eine mnemonische Passphrase bestehend aus einer einzigartigen Kombination von Wörtern zu verwenden. Diese Wortgruppen sind leichter zu merken bzw. aufzubewahren und können ein Wallet wiederherstellen, sollte es verlorengehen. Jedoch ist der Besitzer selber dafür verantwortlich auf diese aufzupassen.

Eine Alternative stellen sogenannte *social recovery* Wallets dar. Hierbei benutzt der Besitzer eines solchen Wallets einen einzelnen Signatur Schlüssel, um Transaktionen zu legitimieren. Zusätzlich muss er mindestens 3 weitere “Guardians” anlegen, was andere Wallets, Indivduen oder Institutionen sein können. Diese Guardians haben in der Mehrheit das Recht einen neuen Signatur Schlüssel für den Besitzer anzulegen, sollte er seinen verlieren.[But21]

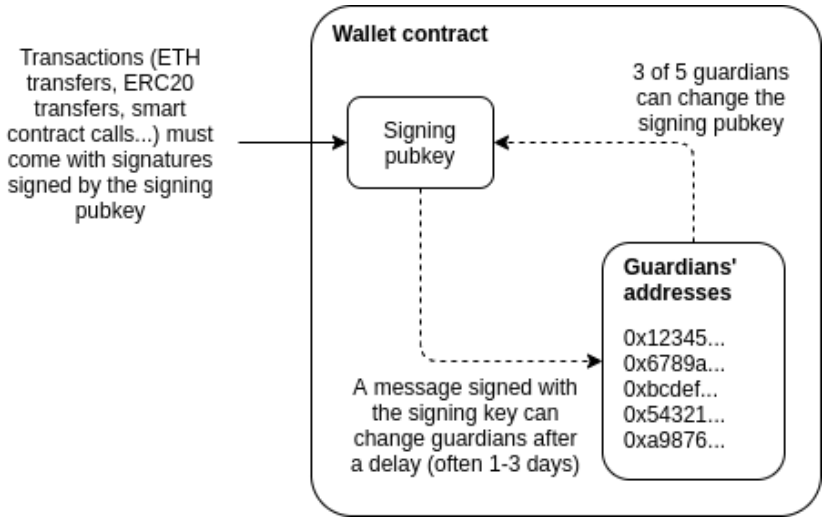

Abbildung 2.10: Funktionsweise von Social Recovery
[But21]

Ein Nachteil von diesem Verfahren ist, dass der Besitzer vertrauenswürdige Guardians auswählen muss, die seine Schlüssel beschützen. Falsch ausgewählte Guardians könnten kooperieren und somit den ursprünglichen Besitzer bestehlen. Zusätzlich muss beachtet werden, dass Beziehungen im echten Leben sich verschlechtern können oder Menschen sterben, wodurch dieser Mechanismus eine menge Aufmerksamkeit vom Besitzer benötigt. [BOW22]

Eine Verbesserung wäre es, die Wiedererlangung eines Schlüssels mit den Communities zu verknüpfen, in welcher eine Seele partizipiert. Da SBTs die Zugehörigkeit zu einer bestimmten Gruppe darstellen können, ist es möglich Mitglieder dieser Community als Guardians zu wählen. Die Communities können hierbei zufällig gewählt werden, sowie die Mitglieder, die sich dazu bereit erklären. Der Vorteil ist, dass die Guardians in diesem Fall automatisch aktualisiert werden, ja nachdem in welchen Gemeinschaften man partizipiert.

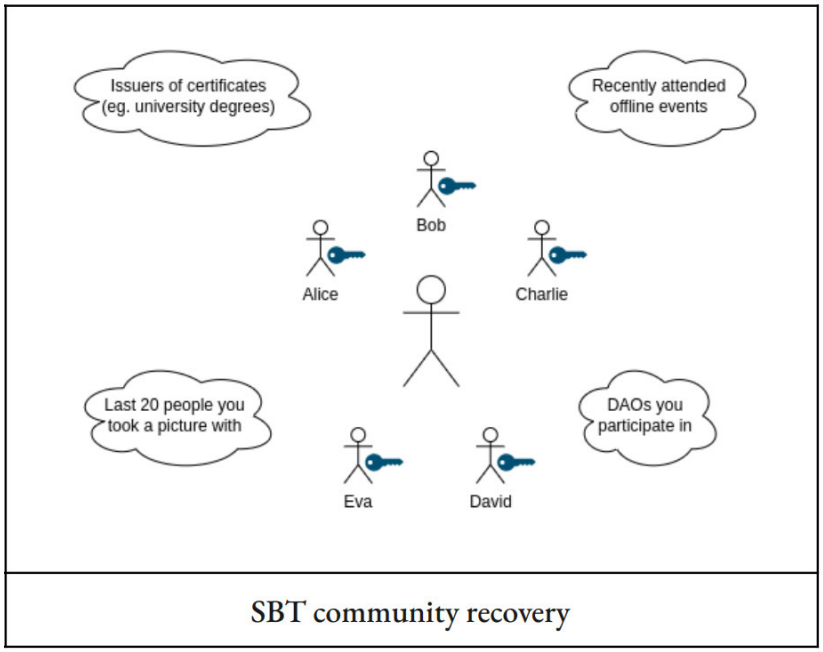

Abbildung 2.11: Funktionsweise von Community Recovery
[BOW22]

Indem Sicherheit in Sozialität eingebaut wird, kann somit auch der Diebstahl oder das Verkaufen von Seelen verhindert werden. Der ursprüngliche Besitzer kann sein Wallet im Falle eines Verlust oder Betruges wiederherstellen und das Verkaufen wird erschwert, da er die sozialen Abhängigkeiten nicht verkaufen kann.

2.5.3 Privatsphäre

Die bisherige Vision von DeSoc hat Privatsphäre, als ein untergeordnetes Thema behandelt. Dies liegt daran, dass das Thema sehr schwer zu implementieren ist. Da alle Blockchain basierten Systeme inhärent öffentlich sind, sind Beziehungen zwischen zwei Nutzern nicht nur für sich, sondern auch für die restlicher Welt einsichtig. SBTs würden damit nicht in Frage kommen, um sensible Daten geschweige denn irgendwelche identifizierenden Daten zu speichern, da das Potential für Überwachung und sozialer Kontrolle zu groß wäre. Diese Eigenschaft ist allerdings beabsichtigt, da sie einige Vorteile mit sich bringt. Private SBTs können Beziehungen und Korrelationen zwischen Seelen verheimlichen, sodass die Intentionen von Nutzern nicht mehr eindeutig sind. Zusätzlich lässt sich somit negative Reputation sehr schlecht umsetzen, wenn jeder Nutzer entscheiden kann, welche Token er öffentlich einsehbar macht. Es gilt also Lösungen zu finden, welche Öffentlichkeit und Privatheit verbindet.[BOW22]

Eine simple Lösung wäre es, die auf SBTs zu findenden Information außerhalb der Blockchain zu lagern und stattdessen einen Hash zu hinterlegen, welcher auf diese verweist. Eine solche Implementierung ist in Abbildung 2.12 ersichtlich.

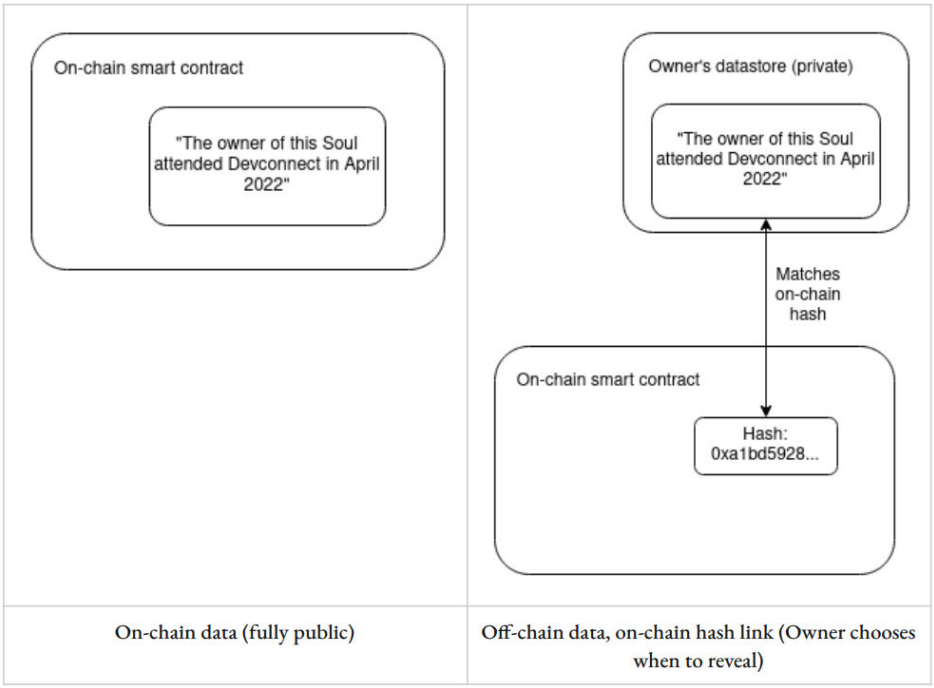

Abbildung 2.12: Privatheit mithilfe von externen Verweisen.
[BOW22]

Falls ein Benutzer ein SBT benutzen will, um sich zu verifizieren, so kann er seine persönlichen Informationen einem Smart Contract vorlegen. Dieser hasht daraufhin die Eingabe und vergleicht, ob das Ergebnis identisch mit dem Hash auf der Blockchain ist. Wenn dies der Fall, so wird der Benutzer erfolgreich als Halter des Tokens identifiziert. Der Benutzer kann hierbei selber wählen, wo er die Informationen speichern will. Einige Möglichkeiten inkludieren dabei das Verwenden eines vertrauten Cloud Service oder das Nutzen vom IPFS. [BOW22] Das InterPlanetary File System (IPFS) ist ein dezentrale aufgebautes Dateisystem, welches Teilnehmern ermöglicht Dateien über ein weltweites P2P-Netzwerk zu speichern und freizugeben. Jede Datei in diesem Netzwerk besitzt eine einzigartige Inhaltskennung, welche genutzt wird um die Datei wiederzufinden. Eine solche Kennung kann benutzt werden, um externe Inhalte zu verlinken. [Clo22]

Auf diese Art und Weise können Berechtigungen aufgeteilt werden. Smart Contracts haben immer noch das Recht Daten auf SBTs zu schreiben, doch der Besitzer des Tokens hat nun das Recht zu entscheiden, ob er die dahinterliegenden Informationen offenlegt oder nicht. Dies hätte auch positive Auswirkungen auf die Skalierbarkeit, da somit große Datenmengen zu einem Hash zusammengefasst werden können, um somit Gas Kosten zu sparen. [BOW22]

Eine weitere Technologie, welche beim Thema Privatsphäre eine große Rolle spielen wird, sind sog. Zero-Knowledge Proofs (dt. Null-Wissen-Beweis). Sie bezeichnen ein kryptographisches Verifizierungsprotokoll, womit ein Prüfer A einem Verifizierer B beweisen kann, dass A im Besitz eines Geheimnis ist, ohne zu verraten was dieses Geheimnis ist. B kann diese Behauptung daraufhin verifizieren und entscheiden ob er A vertraut. Somit können sich eine Reihe von mit Datenschutz verbundenen Problemen lösen, da somit ausgedrückt werden kann, dass man im Besitz von Wissen oder eines Dokumentes ist, ohne weitere Informationen darüber preiszugeben.

Zero-Knowledge Proofs können auch über SBTs berechnet werden, um somit gewisse Charakteristiken und Eigenschaften einer Seele zu beweisen. Ein SBT, welches beispielsweise Informationen eines Personalausweises besitzt kann verwendet werden, um die Herkunft eines Nutzers zu bestätigen, ohne die Identität preiszugeben. Somit lässt sich Privatheit von sensiblen Daten mit der inhärenten Öffentlichkeit der Blockchain vereinbaren. Indem man beweisen kann, dass man ein gewisses SBT besitzt, können somit der Großteil der Funktionalitäten einer DeSoc ausgeführt und soziale Provenienz beibehalten werden. [eth02]

3 Implementierung einer Reputationsplattform

Im Zuge dieser Arbeit wird eine Reputationsplattform mithilfe von Soulbound Tokens implementiert, welche es gilt im folgenden Kapitel genauer zu untersuchen. Mithilfe der Plattform wird veranschaulicht, wie ein möglicher Anwendungsfall von SBTs aussehen könnte. Der Name der Applikation lautet Decentralized Reputation (DeRep) und sie dient dazu die Grundfunktionen von SBTs einzubauen, sowie diese in eine anwenderfreundliche Website zu verpacken. Mithilfe der Plattform ist es möglich SBTs an andere Nutzer der Plattform zu attestieren. Nachdem ein Benutzer eine Seele mithilfe seiner Wallet Adresse erstellt hat, welche als dezentrale Identität dient, kann er beginnen SBTs an andere Nutzer zu verteilen beziehungsweise zu erhalten. Die Tokens können hierbei als simple Bewertungen angesehen werden und entweder positiv oder negativ sein, sodass es möglich ist eine Reihe von SBTs zu sammeln und somit Vertrauen aufzubauen. Zusätzlich soll auch der Umgang mit den auf SBTs vorzufindenden Informationen demonstriert werden, indem ein simpler Bewertungsalgorithmus diese ausliest und eine Wertung für die Nutzer berechnet. Das eingesetzte Vertrauensmodell wird hierbei ein Quantitatives sein, welches der Algorithmus für die Endbewertung berücksichtigen wird und somit die Anzahl von Attestierungen als Hauptmetrik nutzt. Somit können Benutzer gesammelte SBTs auf ihrem Profil ausstellen und eine Wertung von DeRep zu diesen SBTs erhalten.

Die Plattform selber passt sich an die momentanen Strukturen des Web2 Raumes an und kann in diesen eingegliedert werden. Die effektivste Methode, um die Plattform zu nutzen, wäre es demnach das Profil des jeweiligen Nutzers mit den bereits bestehenden sozialen Netzwerken oder ähnlichem von ihm zu verbinden. Dadurch können Profile direkt mit einer bestehenden Identität verbunden werden, wodurch bereits mehr Glaubwürdigkeit vermittelt wird, welche mithilfe dem Sammeln von Attestierungen weiter verbessert werden kann. Während dies keine Funktionen direkt einschränkt, ist es wichtig zu erwähnen, dass eine solche Verknüpfung eines Wallets mit Vorsicht zu genießen ist, da somit alle Informationen preisgegeben werden, die mit dem Wallet in Verbindung stehen, wie zum Beispiel die Transaktionshistorie. Daher ist es zu empfehlen, ein eigens dafür kreiertes Wallet zu benutzen, sodass nur die sowieso öffentlichen Informationen der SBTs einzusehen ist.

An diesem Punkt wird angemerkt, dass das Programm dezentrale, als auch zentrale Aspekte vereint. Der Bewertungsalgorithmus selber ist nicht Teil des dezentralen Smart Contracts und daher Sache des jeweiligen Anbieters der Plattform (in diesem Fall DeRep). Die zugrunde liegende Technologie in Form von SBTs ist allerdings für jedermann zugänglich und kann von jedem verwendet werden. DeRep stellt also lediglich eine mögliche Interpretation dieser Daten dar und zeigt wie eine solche Plattform die Daten verarbeiten könnte, um daraus Vertrauen zu gewinnen. Dieser Ansatz steht im Gegensatz zu den in Kapitel 2.2 beschriebenen Kernaspekten eines dezentralen Reputationssystems, da die Bewertung kein eingebauter Teil des Kommunikationsprotokolls ist.

Für die Zukunft von SBTs wäre es allerdings von Vorteil, wenn es eingebaute, dezentrale Mechanismen gibt, um die in Kapitel 2.4.1 beschriebenen Funktionen zu implementieren. Dieser Schritt ist allerdings ohne einem uniformen Standard für Soulbound Token noch nicht zu realisieren.

3.1 Architektur

Die Anwendung lässt sich in zwei Teile gliedern. Zum Einen in das Backend, welches sich um alle Blockchain-basierten Aufgaben kümmert und das Frontend, welches als Schnittstelle für den Benutzer agiert. Die zugrunde liegende Ethereum Blockchain wird mit einem selbst verfassten Smart Contract angesteuert, welcher zuständig dafür ist alle Funktionalitäten bereitzustellen, welche man mit dem Umgang von SBTs braucht. Mithilfe des Smart Contracts können Benutzer ihre Seelen anlegen und sich daraufhin gegenseitig attestieren. Das dadurch entstehende Netzwerk wird als “Network of Souls” bezeichnet und beinhaltet alle Seelen, die miteinander interagieren. Das Verschicken von SBTs ist an diesem Punkt vollständig möglich. Darauf aufbauend befindet sich die Reputationsplattform DeRep, welche das Suchen nach Knoten, als auch das Attestieren erleichtert. Der Bewertungsalgorithmus ist ein Teil von DeRep, sodass dieser sich ebenfalls auf dieser Ebene befindet. Auf Abbildung Abbildung 3.1 kann die soeben besprochene Struktur nochmals betrachtet werden.

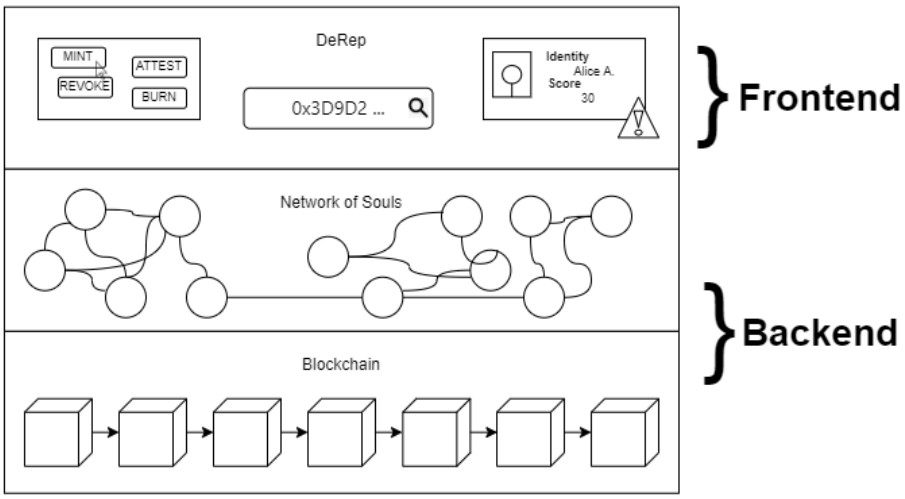

Abbildung 3.1: Kompletter Überblick über die Reputationsplattform

3.2 Frontend

Das Frontend der Applikation wird über eine Website gehostet, welche die zugrunde liegenden Funktionen des Backends zugänglich macht. Dafür ist eine Metamask Verbindung notwendig, welche die Anbindung zu einem ausgewählten Wallet des Nutzers ermöglicht. Ein Metamask Prompt erscheint beim erstmaligen Laden der Seite sofort, insofern noch keine Verbindung hergestellt ist. Die momentan verbundene Adresse wird zu jedem Zeitpunkt in der Navigationsbar dargestellt und kann zu jeder Zeit getrennt werden. Das Ändern einer Wallet Adresse ist ebenfalls zu jedem Zeitpunkt möglich, wobei die Darstellung automatisch aktualisiert wird.

Den ersten Schritt, den neue Nutzer befolgen müssen, ist das Anlegen einer Seele für eine Wallet Adresse auf der Minting Page. Diese Seite lässt sich über die Navigationsbar aufrufen. Hier können neue Nutzer die Identität für ihre Seele angeben, welche aus einem Namen und einem Link zu einer externen Bezugsquelle besteht. Ein Twitter Nutzer könnte hierbei sein Twitter Profil angeben und

beide Profile somit koppeln. Nach dem Anlegen bzw. falls der Nutzer bereits zuvor eine Seele erstellt hat, zeigt die Minting Page hinterlegte Informationen zu dieser Seele an. Nutzer, welche erfolgreich eine Seele gemintet haben, können sich nun gegenseitig SBTs attestieren.

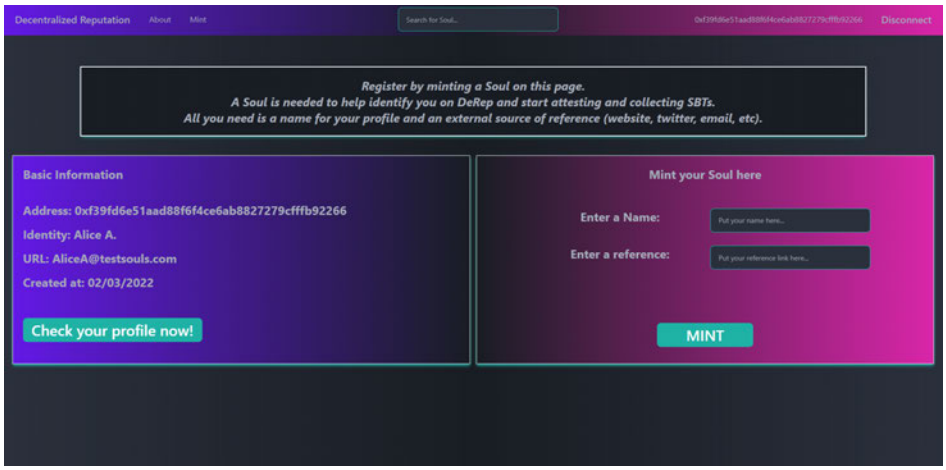

Abbildung 3.2: Minting Page von DeRep

Mithilfe einer Suchleiste, welche zentral in der Navigationsbar aufzufinden ist, können andere Profile von Wallets gesucht werden. Falls die gesuchte Adresse eine Seele besitzt, wird die dazugehörige Profilseite angezeigt. Hier sind grundlegenden Informationen über die gesuchte Seele zu finden, eine Liste der besessenen Tokens, als auch eine Wertung, welche angibt wie vertrauenswürdig das Profil erscheint. Die attestierten SBTs sind dabei nach dem Alter sortiert und farblich gekennzeichnet. Positive Token sind mit einem grünen Hintergrund dargestellt und negative mit einem roten Hintergrund. Zusätzlich sind alle sonstigen Informationen, die noch auf den SBTs liegen, auch hier aufzufinden. Die Bewertung wird mithilfe einer Zahl zwischen 0 und 100 angegeben und mit einem zusätzlichen Symbol dargestellt. Vertrauenswürdige Profile erhalten ein grünes Abzeichen als Symbol, mittelmäßige ein gelbes und nicht vertrauenswürdige ein rotes. Das Aussehen des Profils für eine Seele wird im Abschnitt 3.3.3 gezeigt.

Zusätzlich existiert noch eine About-Page, auf welcher Grundbegriffe und das Prinzip von DeRep mithilfe von Zitaten dieser Arbeit erklärt werden.

3.3 Backend

3.3.1 Smart Contract

Da es noch keinen gemeinsamen ERC-Standard für SBTs gibt, wird für die Anwendung ein selbst verfasster Solidity Smart Contract für die Ethereum Blockchain verwendet. Der Smart Contract basiert allerdings auf einer bereits existierenden Interpretation von James Bachini [Bac22] und erweitert diesen um einige weitere Grundfunktionen oder passt ihn an einigen Stellen an. Die übernommenen Teile inkludieren hierbei den Aufbau und die dazugehörigen Funktionen zum Erstellen, Anpassen und Löschen einer Seele. Konkret wurde das *Soul*-struct, als auch die *mint*-Funktion komplett übernommen, während alle anderen Inhalte um Funktionalitäten mit SBTs ergänzt beziehungsweise neu

verfasst wurden. Im Folgenden Kapitel sollen die wichtigsten Funktionen des SBT Smart Contracts, als auch die grundlegenden Datentypen erklärt werden. Hierbei ist wichtig zu erwähnen, dass der Aufbau der Datentypen und Funktionen keineswegs final sind und sich nach den spezifischen Anwendungsfällen richten können. Der hier verwendete Aufbau wurde für diesen Zweck simpel und allgemein gehalten.

Um zu beginnen Tokens auszustellen, benötigt jeder Nutzer zuerst eine Seele, welche dabei helfen soll diese zu identifizieren und einer eindeutigen Persönlichkeit zu zuordnen. Das Anlegen einer Seele für eine Wallet Adresse kann also als eine Art Registrierung für die Plattform angesehen werden. Der Aufbau einer Seele im Smart Contract lässt sich in Quelltext 3.1 sehen. Die Strings *identity* und *url* sind die einzigen Daten, die vom User angelegt werden. Die Identität bezeichnet hierbei Informationen, die einen Benutzer eindeutig identifizieren sollen, wie zum Beispiel ein voller Name. Zusätzlich kann eine URL angegeben werden, welche auf zusätzliche Informationen verweist, wie eine persönliche Website, E-Mail Adresse et cetera. Der Wert *score* gibt die Wertung der Seele im Bezug auf Vertrauenswürdigkeit an, welcher mit dem Bewertungsalgorithmus berechnet wird. Der Startwert ist hierbei immer 0. Die *timestamp* wird automatisch beim Minten im Smart Contract gesetzt und gibt den Zeitpunkt der Erstellung an. Um später allerdings selber ein Netzwerk aus unterschiedlichen Test Seelen anzulegen, ist es notwendig, dass man alle Werte selbst anlegen kann, sodass *timestamp* und *score* vorerst nicht im Smart Contract generiert werden. Zum Vermeiden von unnötigen Gaskosten ist das Aktualisieren der *score* Variable nicht im Smart Contract enthalten, sondern vorerst nur auf der Reputationsplattform vorzufinden.

```
struct Soul {
    string identity;
    // add issuer specific fields below
    string url;
    uint256 score;
    uint256 timestamp;
```

Quelltext 3.1: Datentyp Soul

Die *mint*-Funktion aus Quelltext A.1 im Anhang legt eine neue Seele auf der Blockchain an und weist diese dem Wallet zu, das die Funktion aufgerufen hat. Dabei darf ein Wallet nur eine Seele besitzen. Die *burn*-Funktion aus Quelltext A.2 erlaubt es Nutzern ihre angelegte Seele wieder zu löschen. Hierbei wird das öffentliche *sbt* Array des Smart Contract nach Soulbound Tokens gesucht, die der Nutzer vergeben hat, um diese zu löschen. Daraufhin wird die Seele gelöscht und das dazugehörige Mapping, welches verfolgt wie viele SBTs eine Seele besitzt. Dabei ist wichtig anzumerken, dass das Löschen der Daten aufgrund der Arbeitsweise einer Blockchain nicht möglich ist, sondern die Daten nur von allen zukünftigen Blöcken ausgeschlossen werden. Dadurch ist ein „echtes“ Entfernen der Daten nicht möglich, sobald sie einmal aufgenommen wurden.

Der Aufbau eines Soulbound Tokens lässt sich in Quelltext 3.2 erkennen. Jeder Token besitzt eine einzigartige ID, womit man ihn identifizieren kann. Auf jedem Token lässt sich die Adresse *attester* finden, welche ihn ausgestellt hat. Der Aussteller hat hierbei die Möglichkeit die Reputation des Tokens festzulegen und ihm eine Beschreibung hinzuzufügen. Ein Token wird sich positiv auf die Reputation der Zielperson auswirken, wenn das *reputation* flag auf *true* gesetzt wurde. Die Bezeichnung im Smart Contract für die Beschreibung ist *explanation_url*, dies hat den Grund, dass der Nutzer statt einer ausführlichen Rezension, einen Link zu dieser übergibt und somit die entstehenden Gaskosten reduzieren kann. Alternativ kann auch ein Hash übergeben werden, welche auf externe Information

verweist, um somit die Privatsphäre zu schützen. Ähnlich wie beim Datentyp *Soul* gibt es auch die Eigenschaft *timestamp*, welche angibt, wann der Token ausgestellt wurde. Schlussendlich gibt das flag *active* an, ob der Token vom Aussteller zurückgezogen wurde oder noch aktiv ist.

```
struct Sbt {
    uint tokenId;
    address attester;
    bool reputation;
    string explanation_url;
    bool active;
    uint256 timestamp;
}
```

Quelltext 3.2: Datentyp Sbt

Um schließlich einen Token auszustellen, wird die *attest*-Funktion verwendet. Bedingungen dafür sind, das sowohl der Aussteller, sowie die Zielperson eine Seele besitzen. Der Benutzer vergibt hierbei die Art der Reputation (positiv/negativ), als auch eine Beschreibung. Im Smart Contract werden *tokenId*, timestamp und *active* flag automatisch hinzugefügt. Das SBT wird daraufhin in das öffentliche sbt Array beigefügt und der Zielperson gutgeschrieben. Jede Seele besitzt einen eigenen Zähler, welcher die Anzahl der besessenen Tokens verfolgt und je nach Funktion inkrementiert bzw. dekrementiert wird. Der Smart Contract besitzt zudem eine öffentliche variable *tokenId*, welche nach jedem Aufrufen der *attest*-Funktion ebenfalls inkrementiert. Nutzer haben auch die Möglichkeit ihre ausgestellten Tokens zu widerrufen, falls das Vertrauen zur Zielperson gebrochen wird und die Bewertung nicht mehr zeitgemäß ist. Dies geschieht durch die *revoke*-Funktion und der Bereitstellung der tokenId des vergebenen SBT. Hierbei wird die *active* flag auf false gesetzt, wodurch die Revokation des Tokens ausgedrückt wird. Durch das Widerrufen wird die Anzahl der besessenen SBTs einer Zielperson außerdem um 1 verringert. Den Quelltext zur *revoke*- und *attest*-Funktion lässt sich ebenfalls im Anhang unter Quelltext A.3 und Quelltext A.4 finden.

Der Smart Contract wird mithilfe von Hardhat kompiliert, getestet und auf einer der Blockchain eines lokalen Knotens eingesetzt.

3.3.2 Bewertungsalgorithmus

Zusätzlich zu den Grundfunktionen, zeigt die Plattform automatisch zu jedem Profil einer Seele auch eine Vertrauensbewertung an, welchen Nutzern helfen soll zu entscheiden, ob sie einer Person vertrauen. Die Ausgabe wird von einer Zahl zwischen 0 und 100 dargestellt. Hierbei gibt es 3 verschiedene Vertrauenslevel, die erreicht werden können. Werte über 60 werden allgemein als “trusted” wahrgenommen und von der Plattform als solche dargestellt. Werte unter 20 Punkten werden hingegen als “untrusted” wahrgenommen und setzen somit einen vorsichtigen Umgang mit ihnen voraus. Die meisten Nutzer, die zu dieser Kategorie gehören sind neue Nutzer, welche noch keine weiteren Interaktionen mit der Plattform durchgeführt haben. Alle Wertungen zwischen diesen beiden Grenzen werden mit “caution” zusammengefasst und bezeichnen Seelen, dessen Vertrauenswürdigkeit nicht genau vorhergesagt werden kann und daher von einer genaueren Betrachtung des Nutzers selber unterliegen sollten. Die im folgenden Abschnitt gezeigten Formeln, werden später im Abschnitt 3.3.3 für Beispielberechnungen verwendet.

Der eingesetzte Bewertungsalgorithmus besteht aus einer Reihe von Sub-Algorithmen, welche die verschiedenen Anteile berechnen, die in die finale Wertung fließen. Faktoren, die diese Wertung beeinflussen sind unter anderem, das Alter der Seele, die Anzahl der besessenen SBTs, als auch qualitative Faktoren der SBTs. In Abbildung 3.3 lässt sich der Einfluss der einzelnen Faktoren auf die Gesamtbewertung erkennen.

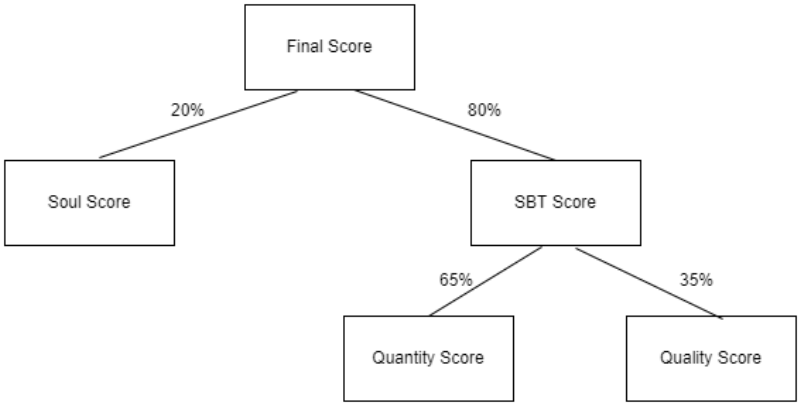

Abbildung 3.3: Zusammensetzung der Bewertung

Durch die Prozentzahlen der Pfade lässt sich schließen, dass die Anzahl der SBTs (Quantity Score) mit 52% Einfluss in die Wertung der wichtigste Faktor ist, gefolgt vom Quality Score (28%) und dem Soul Score (20%). Grund dafür ist, dass es sich bei DeRep um eine quantitative Reputationsplattform handelt. Das meiste Vertrauen kann nur mithilfe von anderen Personen erzeugt werden, die eine jeweilig andere attestieren. Mit jeder weitere Vertrauensausstellung sinkt die Wahrscheinlichkeit, dass es sich bei einer Person, um einen bösartigen Akteur handelt. Dennoch sind weitere Faktoren nötig, die das Außenbild einer Person bereichern und unabhängig davon verifizieren. Den Quelltext für die im folgenden Abschnitt beschriebenen Berechnungen sind im Anhang zu finden.

Der **Soul Score** beschreibt die Qualität und Vertrauenswertung der Seele an sich. In der momentanen Implementationen sind die einzig messbaren Werte einer Seele der Zeitstempel ihrer Erstellung. Andere Werte wie die der *identity*-String können nicht automatisch auf ihr Wahrheitsmaß überprüft werden, sodass diese vorerst arbiträr bleiben. Das bedeutet, dass 20% der finalen Punktzahl vom Alter der Seele abhängig sind, da davon auszugehen ist, dass junge Seelen weniger vertrauenswürdig sind als bereits länger bestehende. Die Punktzahl steigt linear zum Alter einer Seele bis zu einem Maximum von 100, welches nach einem Jahr erreicht wird. Somit werden Benutzer für kontinuierliche Nutzen einer Seele belohnt und sind entmutigt neue Seelen anzulegen, da diese ein beachtliches Zeit Investment fordern würden, um den alten Score wiederherzustellen. Die Formel zur Berechnung der Wertung sieht wie folgt aus:

$$SoulScore = \frac{unixtimestamp_{today} - unixtimestamp_{soul}}{1000 * 3600 * 24 * 365}$$

Der Soul Score beschreibt somit den Quotient aus der Differenz zwischen dem heutigen Datum und dem Erstellungsdatum einer Seele in Millisekunden und der Anzahl von Millisekunden in einem Jahr.

Der **SBT Score** ist für 80% der Punktzahl verantwortlich und setzt sich aus zwei Bestandteilen zusammen. Der Quantity Score beschreibt die Anzahl der gehaltenen SBTs, während der Quality Score die durchschnittliche Qualität der Tokens anhand von Beschreibung und Alter beschreibt .

Der **Quantity Score** benötigt 2 Parameter, um generiert zu werden. Diese bestehen aus der reinen Anzahl von besessenen SBTs C und der Anzahl von einzigartigen Beglaubigern E. Die Einzigartikeit wird im 2. Teil der Berechnung genutzt um den Einzigartigkeitsfaktor U zu berechnen. Vorerst wird eine Punktzahl basierend auf der Quantiät mithilfe von $Score_{Quantity} = C/SBTCOUNTCAP$ berechnet. *SBTCOUNTCAP* bezeichnet hierbei die nötige Anzahl von Tokens die gebraucht werden, um die maximale Punktzahl zu erhalten. In der derzeitigen Implementation ist dieser Wert auf 10 gesetzt, sodass ein Nutzer nur die volle Punktzahl erhält, wenn er 10 oder mehr Tokens hält. Um zu verhindern, dass die Tokens von ein und derselben Person erhalten werden können, wird der Einzigartigkeitsfaktor U eingeführt. Dieser stellt den Quotient von der Anzahl der besessenen SBTs und der Anzahl der einzigartigen Beglaubigern dar; $UniquenessFactor\ U := C/E$. Ist der Einzigartigkeitsfaktor größer oder gleich 0,8, so entstehen keine Abzüge für den originalen Quantity Score. Alle Werte darunter führen zu einem Abzug der Punktzahl mit dem Einzigartigkeitsfaktor bis zu einem maximalen Straffaktor von 0,2. Dadurch werden besonders die Nutzer belohnt, welche nicht nur eine hohe Anzahl von Attestierungen besitzen, sondern auch eine hohe Diversität von Beglaubigern vorzeigen können. Es ist davon auszugehen, dass solche Nutzer vertrauenswürdiger sind als andere, da mehr unterschiedliche Menschen ihnen das Vertrauen zusprechen müssen. Andererseits können mehrfache Attestierungen von der selben Adresse nicht immer ausgeschlossen werden, zum Beispiel bei einer Universität, die ihre Abschlüsse zusätzlich als SBT ausgibt. Um Abzüge bei solchen Fällen zu vermeiden reicht es aus, wenn 80% der Attestierungen einzigartig sind.

Der **Quality Score** besteht aus zwei unterschiedlichen Metriken, die unabhängig voneinander berechnet werden. 55% des Quality Scores gehen auf das Alter der SBTs eines Nutzers zurück, denn umso jünger ein SBT ist, desto mehr Wert hat der Token. Hierbei wird jedem einzigartigen Beglaubiger genau ein SBT zugeordnet. Falls ein Benutzer von derselben Person mehrfach attestiert wurde, so wird lediglich der neueste Token für die Berechnung benutzt. Dies gleicht die Strafe aus, die angewandt wird, wenn eine Seele zu viele Tokens von dem selben Beglaubiger erhält, indem veraltete Tokens die Punktzahl nicht beeinträchtigen und durch die neuen ersetzt werden. Die Berechnung des Alters erfolgt analog zum Soul Score mit dem Unterschied, dass hierbei ein Durchschnitt von allen validen SBTs gebildet und daraufhin zurückgegeben wird.

Die andere Hälfte (45%) des **Quality Scores** wird mithilfe der Beschreibung eines jeden SBT berechnet. Da das maschinelle Auswerten der Qualität von Text Bewertungen keine triviale Aufgabe ist, beschränkt sich dieser Algorithmus darauf lediglich die Länge und Anzahl der Wörter zu untersuchen. Bei allen Beschreibungen mit einer Zeichenlänge von mehr als 100, als auch einer Wortlänge von mehr als 20, ist davon auszugehen, dass es sich um eine seriöse Beschreibung handelt. Alle Werte die darunter liegen, werden mithilfe folgender Formel berechnet:

$$DescriptionScore := \Sigma_i^{Numberof SBTs} = 0.5 * (\frac{DesriptionLength_i}{100}) + 0.5 * (\frac{WordCount_i}{20})$$

Hierbei ist es wichtig zu erwähnen, dass die Berechnung noch auf viele Arten und Weisen verbessert werden kann, indem zum Beispiel ein Spam-Filter eingebaut wird oder nach weiteren Zeichen gesucht wird, die einen qualitativen Text voraussetzen, wie Satzzeichen, Absätze usw. Ebenfalls

kann solch eine Art der Berechnung nicht angewandt werden, wenn man davon ausgeht, dass die hinterlassenen Informationen lediglich ein Hash oder einen externen Verweis, wie eine URL darstellen. Wie in vorherigen Kapiteln beschrieben, stellt das eine Möglichkeit dar, um Privatheit herzustellen, in welchem Fall Beschreibungen nicht immer ausgelesen werden können. Da Metrik allerdings einen untergeordneten Wert für die Bewertung spielt, soll dieser naive Ansatz für den konkreten Anwendungsfall genügen und für Demonstrationszwecke reichen.

3.3.3 Network of Souls

Zusätzlich zur Reputationsplatform wurde eine Reihe von Skripten entwickelt, womit es möglich ist ein Testnetzwerk aus Seelen zu generieren, welche sich gegenseitig SBTs beglaubigen. Somit soll ein echtes Netzwerk mit verschiedenen Parteien simuliert werden, welche die Funktionsweise der Reputationsplattform zeigen. Darüber hinaus sollen auch Beispielwertungen berechnet werden, womit demonstriert werden kann, welche Wertung verschiedene Nutzer erhalten.

Im ersten Beispiel wird eine Art “Circle of Trust” gebildet, in welchem die 3 Parteien Alice, Bob und Charlie sich gegenseitig attestieren. Diese Art von Netzwerk kann beispielsweise bei neuen Nutzern entstehen, welche erst damit begonnen haben sich mit SBTs zu beschäftigen.

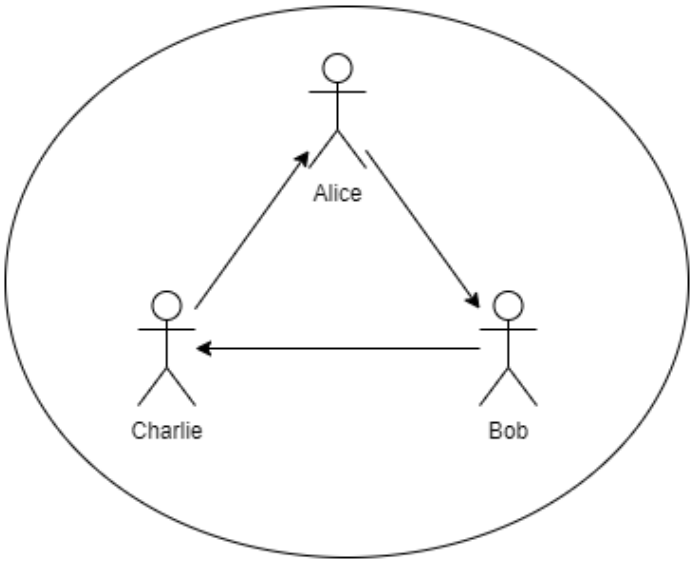

Abbildung 3.4: Netzwerk 1: Circle of Trust

Hierbei besitzt jede Seele insgesamt ein SBT. Die Bewertung lässt sich mithilfe der folgenden Formel berechnen:

$$Score = 0.8(Score_{SBT}) + 0.2(Score_{Soul})$$

$$Score_{SBT} = 0.65(Score_{Quantity}) + 0.35(Score_{Quality})$$

$$Score_{quantity} = 1/10 = 0.1$$

Der Einzigartigkeitsfaktor kann in diesem Fall vernachlässigt werden, da die Anzahl von SBTs $C = 1$ und Anzahl von einzigartigen Beglaubigern $E = 1$, also $1/1 = 1$ ist.

Es wird davon ausgegangen, dass das SBT kurz vorher erstellt wurde und die Länge der Beschreibung ebenfalls adäquat ist, also:

$$Score_{Quality} \approx 1$$

$$Score_{SBT} = 0.65(0.1) + 0.35(1) \approx 0.42$$

Für den Zeitpunkt der Erstellung der Seele, wird der 02.03.2022 gewählt, welcher nach Unix Zeit 1 646 206 905 000 ist. Für das heutige Datum wird der 17.10.2022 eingesetzt, welcher nach Unix Zeit 1 666 036 602 500 ist. Somit entsteht der Soul Score:

$$Score_{Soul} = \frac{1666036602500 - 1646206905000}{1000 * 3600 * 24 * 365} \approx 0.629$$

Dadurch ergibt sich für den finalen Score:

$$Score = 0.8(0.415) + 0.2(0.628) \approx 0.46$$

Auf der Reputationsplattform selber wird die Wertung folgendermaßen repräsentiert:

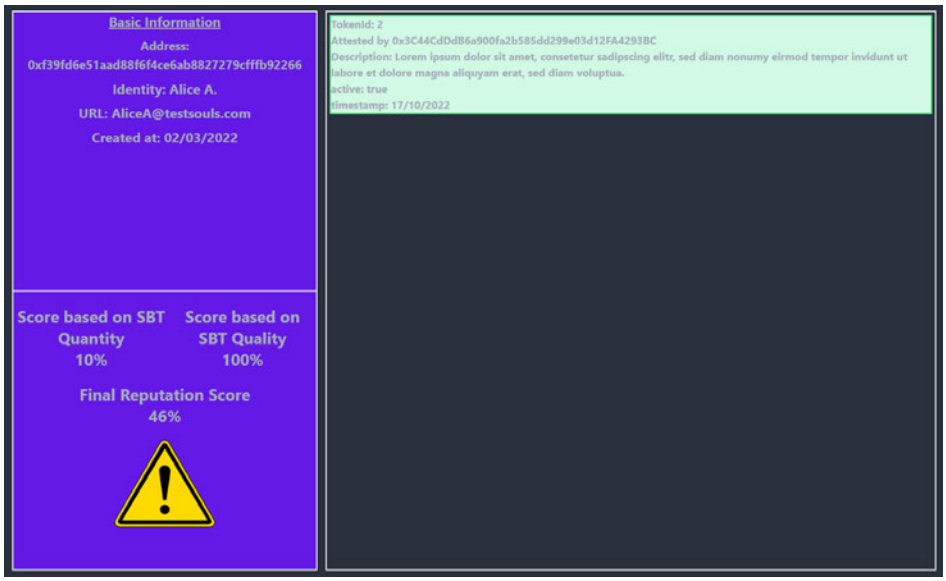

Abbildung 3.5: Circle of Trust: Profil von Alice

Hieraus lässt sich erkennen, dass solange alle anderen Kriterien wie Alter und Qualitätsmerkmale von SBTs gegeben sind, beinahe 50% der Punkte erreicht werden können. Die hier fehlenden Punkte kommen hauptsächlich davon, dass Alice unzureichend viele SBTs besitzt und die maximale Wertung für das Alter der Seele noch nicht ausgereizt ist.

Das nächste Netzwerk soll das Nutzerprofil eines aktiven Nutzers simulieren und verschiedene Attestierungen von sowohl Einzelpersonen, als auch Institutionen beinhalten. Die Institutionen bestehen in diesem Fall aus einer Universität, einem Arbeitgeber und einer Konferenz für Entwickler. Zusätzlich erhält Alice auch von einer Reihe von Einzelpersonen Attestierungen, welche Freunde, Familie oder auch Kollegen darstellen können. Die folgende Grafik visualisiert, dieses Verhältnis.

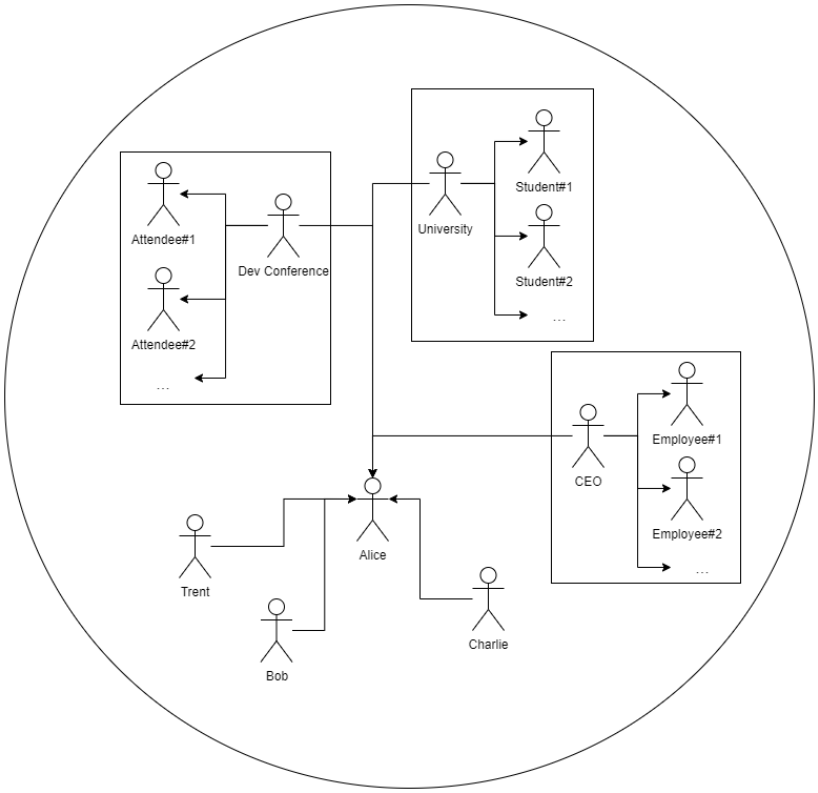

Abbildung 3.6: Rich Network of Trust

Für die Berechnung wird angenommen, dass die Qualitätsmerkmale so gut wie vollständig eingehalten wurden (0.95) und das Erstellungsdatum der Seele ebenfalls der 02.03.2022 ist. Dadurch lässt sich die Berechnung wie folgt anpassen:

Alice besitzt in diesem Fall 6 einzigartige SBTs.

$$Score_{SBT} = 0.65(0.6) + 0.35(0.95) \approx 0.72$$

$$Score = 0.8(0.72) + 0.2(0.628) \approx 0.7$$

Die zusätzlich erhaltenen SBTs rufen einen starken Anstieg der Wertung hervor. Durch die verschiedenen Attestierungen von verschiedenen vertrauenswürdigen Institutionen, erweckt das Profil von Alice außerdem einen vertrauensvollen Eindruck für das menschliche Auge.

Abbildung 3.7: Rich Network of Trust: Profil von Alice

Trotz eines guten Aussehens auf den ersten Blick ist es dennoch immer wichtig die Aussteller solcher Tokens selber auf Vertrauenswürdigkeit zu überprüfen. Die Aussteller eines jeden SBT sind immer in diesem verlinkt, sodass man sehr leicht zu deren Profil gelangen und diese unabhängig prüfen kann. Somit kann ausgeschlossen werden, dass offensichtliche Hochstapler ein fremdes Profil künstlich vertrauenswürdig aussehen lassen. Die Adressen von zentralen Vertrauensankern wie Universitäten sollten ihre Adresse öffentlich einsehbar haben, sodass diese schnell mit Profilen verglichen kann, welche sich als diese ausgeben.

4 Schluss

Das Web of Trust hat bereits früh demonstriert, welches Potenzial hinter dezentralisiertem Vertrauen steckt. Allerdings konnte es nicht mit dem schnellen Wachstum des Internets mithalten, was zu dessen Obsoleszenz führte. Stattdessen haben zentrale Autoritäten die Frage übernommen, wie man Vertrauen im Internet abbilden kann und dabei maßgeblich das heutige Internet geformt. Durch hohe Skalierung und hohen Komfort für Benutzer konnten zentrale Instanzen somit zu mächtigen Akteuren im Internet werden. Doch dadurch sind auch Nachteile entstanden, wie beispielsweise Möglichkeiten zur Zensur. Gerade das hohe Aufkommen von Fake News hat dazu geführt, dass zentrale Vertrauensanker vor einem gänzlichen Vertrauensverlust stehen und zunehmend verwundbarer gegenüber einem zensurfreien und dezentralen Web3 werden. Während das Web3 sich momentan hauptsächlich in finanziellen Räumen bewegt, entwickelt sich dadurch eine neuer Zweig in Richtung dezentralisiertem Vertrauen. Die Einführung von Soulbound Tokens können bestehende Bewertungsmechanismen verbessern und somit der Grundstein für neue Reputationsplattformen sein. DeRep stellt einen Startpunkt, für den Beginn von dezentralisierter Reputation und Vertrauen dar. Doch auch unabhängig von Reputationsplattformen haben SBTs ein gewaltiges Potential, durch das Erschaffen einer DeSoc. Das Schaffen von sozialen Identitäten und Relationen eröffnet eine Reihe von neuen Anwendungsfällen, welche auf Vertrauen anstatt Kapital basieren. In Kapitel 3 wurde gezeigt, dass die technologischen Voraussetzungen für eine DeSoc in Form von SBTs nicht sehr fern sind. Ein wichtiger nächster Schritt für die Voranbringung dieser Technologie ist die Vereinheitlichung der Tokens mithilfe eines ERC-Standards, um sie massentauglich zu machen und die Anwendungsfälle einer DeSoc freizuschalten. Nichtsdestotrotz zeigt DeRep, dass auch ohne einen solchen Standard, das Konzept von SBTs bereits anwendbar ist und als solches funktioniert. Auf der anderen Seite zeigt DeRep auch, dass viele Detailfragen noch geklärt und einige Konzepte weiterführend getestet werden müssen.

4.1 Ausblick

Eine wichtige Frage ist, wie man reale Identitäten ihren Web3 Identitäten zuordnen kann. In der momentanen Ausführung von DeRep wird die wirkliche Identität eines Nutzers nicht bestätigt oder abgefragt. Dies ist allerdings auch nicht unbedingt notwendig, wenn davon ausgegangen wird, dass Benutzer der Plattform ihr DeRep-Profil mit anderen Medien verknüpfen und man über deren Verlinkung zum Profil des Nutzers gelangt. Für das bloße Aufbauen von Reputation und Sammeln von SBTs reicht diese Herangehensweise. Komplexere Anwendungsfälle könnten allerdings voraussehen, dass nur Nutzer mit einer bestätigten Identität mit diesem interagieren dürfen, wie zum Beispiel Kreditmärkte. In einem solchen Fall könnten personalisierte SBTs verwendet werden, welche die Identität einer Seele explizit bestätigen. Die Aussteller eines solchen SBTs könnten Regierungen oder Ähnliches sein. Somit können auch zentrale Vertrauensanker in die dezentralen Strukturen eingebunden werden.

Ein Nachteil der momentanen Lösung mit dem Verlinken des DeRep-Profils mit existierenden Social Media Accounts ist, dass somit weitere Daten an Unternehmen wie Meta und Co. gegeben werden. Das Verknüpfen einer Wallet Adresse erlaubt es Datenkraken weitere Informationen wie die Transaktionshistorie von Individuen einzusehen. Aus diesem Grund sollten Benutzer der Plattform die

Vorteile der Pseudonymisierung nutzen und verschiedene Wallets für verschiedene Zwecke verwenden. Zum Beispiel ein Wallet für das Sammeln von öffentlich einsehbaren SBTs und ein Wallet für Transaktionen und Käufe. Die Privatheit im Bereich von SBTs wird weiterhin einer der vielversprechendsten Forschungszweige auf diesem Gebiet sein. Technologien wie Zero-Knowledge Proofs und dezentrale Soziale Medien, wie zum Beispiel Lens Protocol könnten dabei eine große Rolle spielen.

Obwohl es Funktionen zum Löschen einer Seele im Smart Contract gibt, sind diese momentan nicht in der Reputationsplattform verbaut worden, da die Nützlichkeit einer solchen Funktion aufgrund der Natur einer Blockchain stark eingeschränkt ist. So kann zwar verhindert werden, dass gespeicherte Informationen in zukünftigen Blöcken nicht mehr zu finden sein werden, jedoch sind die Daten immer noch im Nachhinein auf den alten Blöcken der Blockchain wiederzufinden.

Eine zusätzliche Implementierung könnte daraus bestehen, dass SBTs selbst bewertet beziehungsweise ihnen verschiedene Wertungen zugesprochen werden können. Somit können SBTs von vertrauenswürdigen und weniger vertrauenswürdigen Ausstellern unterschieden werden. Die aktuelle Implementation des Bewertungsalgorithmus behandelt alle SBTs gleichwertig, was für das bloße Ausstellen von Bewertungen zureichend ist. Allerdings sollten SBTs von Institutionen mit einer umfangreichen Historie, wie Unternehmen oder Universitäten eine höhere Stellung besitzen, als von Nutzern, welche soeben erst ein Wallet erstellt haben. Zukünftige Algorithmen, um Wertungen von Nutzern zu berechnen, sollten die Herkunft von SBTs in Betrachtung ziehen, um somit ein besseres Bild über einen Nutzer zu erhalten. Somit lassen sich außerdem Fake-Profile einfacher von echten Profilen unterscheiden, da es für falsche Profile schwerer ist, SBTs aus vertrauenswürdigen Quellen zu erhalten.

Ein weiterer interessanter Zweig ist die automatische Vergabe von SBTs. Anstatt Nutzern manuell ein SBT zu- beziehungsweise abzusprechen, können Smart Contracts eingesetzt werden, um Seelen, welche eine bestimmte Errungenschaft erzielt haben, automatisch einen Token zuzusprechen. Ein einfaches Beispiel wäre die Vergabe von Alters-SBTs auf DeRep. Anstatt den Score über das Alter einer Seele zu berechnen, könnte man aktiven Nutzern automatisch ein SBT nach 1, 5 oder auch 10 Jahren der Aktivität zusprechen. Aussteller wäre hierbei die Reputationsplattform selber, sodass der Token direkt von einer vertrauenswürdigen Quelle stammt. Benutzer könnten diese SBTs von verschiedenen Plattformen sammeln, um somit die Aktivität, als auch die Gebundenheit in verschiedenen Communities zu belegen. Eine solche Funktionsweise stellt auch die Existenz des Soul-structs im Smart Contract infrage. Momentan müssen Nutzer zuerst mit ihrer Wallet Adresse eine Seele minten, um daraufhin SBTs zu erhalten bzw. auszuteilen. Zusammen mit den oben besprochenen Identitäts-SBTs können Alters-SBTs diesen Datentyp vollständig ablösen, da es momentan nur dazu da ist, um eine Adresse mit einer selbst gewählten Identität zu verknüpfen, als auch ein Erstelldatum zu speichern. Die Speicherung des Scores auf einer Seele selber hat sich als unbrauchbar herausgestellt, da bei jedem Aktualisieren der Wertung Gaskosten anfallen. Somit könnte die Funktionalität des Soul-Datentyps in Zukunft obsolet gemacht werden und stattdessen inhärent auf alle Wallets angewandt werden.

Mit all diesen Erweiterungen kann die Reputationsplattform in Zukunft zu einem starken Werkzeug für die Schaffung von Vertrauen im Web sein, um Falschinformationen und Betrugsschemata vorzubeugen. Doch auch ohne diese Verbesserungen ist DeRep bereits ein lehrreicher Beitrag für den Beginn von dezentraler Reputation im Internet, der womöglich zu einem standardisierten Design für Soulbound Tokens beitragen kann.

Anhang A: Quelltext

```
function mint(address _soul, Soul memory _soulData) external {
    require(keccak256(bytes(souls[_soul].identity)) == zeroHash, "Soul
        already exists");
    souls[_soul] = _soulData;
    emit Mint(_soul);
}
```

Quelltext A.1: mint Funktion

```
function burn(address _soul) external {
    require(msg.sender == _soul, "Only Soul Owner have rights to delete
        their data");

   // delete users sbts
    for (uint i=0; i<sbts.length; i++) {
        if (SbtToSoul[i] == _soul) {

        delete sbts[i];
        delete SbtToSoul[i];
        }
    }

    delete souls[_soul];
    delete soulSbtCount[_soul];
    emit Burn(_soul);
```

Quelltext A.2: burn Funktion

```
function attest(address _targetSoul, bool _reputation, string memory _
    explanation_url) external {
    //Target soul has to exist
    require(keccak256(bytes(souls[_targetSoul].identity)) != zeroHash, "
        Cannot send SBT to Soul that has not been minted");
    require(keccak256(bytes(souls[msg.sender].identity)) != zeroHash, "
        Attester has to have a Soul themselves");
    sbts.push(Sbt(tokenId, msg.sender, _reputation, _explanation_url,
        true, block.timestamp));
    SbtToSoul[tokenId] = _targetSoul;
    soulSbtCount[_targetSoul]++;
    tokenId++;
    emit Attest(_targetSoul);
}
```

Quelltext A.3: attest Funktion

```
function revoke(uint _tokenId) public{
    require(_tokenId <= tokenId, "Entered TokenId does not exist");
    require(sbts[_tokenId].active == true ,"SBT has already been revoked
        ");
    require(sbts[_tokenId].attester == msg.sender, "Only attester may
        revoke Token");
    soulSbtCount[SbtToSoul[_tokenId]]--;
    sbts[_tokenId].active = false;

    emit Revoke(_tokenId);
}
```

Quelltext A.4: revoke Funktion

```
function calculateSoulTimestampScore(timestamp: number): number {
    const today = Date.now();
    const difference = ((today - timestamp ) / ( 1000 * 3600 * 24 * 365))
        ;

    return difference > 1 ?
        1 :
        difference;
}
```

Quelltext A.5: Soul Score Berechnung

```
const SBTCOUNTCAP = 10;
function calculateSbtQuantityScore(sbts: Sbt[]): number {
    let score = 0;

    const sbtCount = sbts.length;
    score = sbtCount > SBTCOUNTCAP ?
        1 :
        sbtCount / SBTCOUNTCAP;

    /*
    * Calculate Uniqueness Factor
    */
    const sbtSouls = sbts.map((sbt) => sbt.attester);
    const uniqueSoulCount = new Set(sbtSouls).size;

    const uniquenessFactor = uniqueSoulCount / sbtSouls.length;
    if (uniquenessFactor < 0.8) {
        score = score * (uniquenessFactor + 0.2);
    }

    return score;
}
```

Quelltext A.6: Quantity Score Berechnung

```
function calculateSbtQualityScore(sbts: Sbt[]): number {
    score = 0;
    let timestampScore = 0;

    // get element with highest timestamp for each unique attester
    const newestSbts = sbts.reduce((accumulator, sbt) => {
    if (!accumulator[sbt.attester] || accumulator[sbt.attester].timestamp
        < sbt.timestamp) {
    accumulator[sbt.attester] = sbt;
    }
    return accumulator;
    }, {} as Sbt[]);

    // calculate average timestamp of sbts
    const today = Date.now();
    for (const sbt of Object.values(newestSbts)) {
    //*1000 because in the smart contract unix timestamp is in seconds
    const difference = ((today - sbt.timestamp * 1000) / ( 1000 * 3600 *
       24 * 365)) ;
    timestampScore += difference;
    }
    timestampScore = 1 - timestampScore / sbts.length;
```

Quelltext A.7: Quality Score: Timestamp Berechnung

```
    // check the length of the description of sbts a soul has, the longer
        the sbt the more value
    // accumulate score of all sbts and then use average  as score for
       the description parameter
    let descritpionScore = 0;
    for (const sbt of sbts) {
    let sbtDescriptionScore: number;

    const sbtDescription = sbt.explanation_url;
    const descriptionLength = sbtDescription.length;
    const wordcount = sbtDescription.split(' ').length;

    if ( descriptionLength > 100 && wordcount > 20) {
    sbtDescriptionScore = 1; // 100% score for sbts with a description of
        100 characters and 20 words or more
    } else {
    sbtDescriptionScore = descriptionLength / 100 * 0.5 + wordcount / 20
       * 0.5;
    }
    descritpionScore += sbtDescriptionScore;
    }

    descritpionScore = descritpionScore / sbts.length;

    //  calculate final quality score
    score = 0.45 * descritpionScore + 0.55 * timestampScore;
    return score;
```

Quelltext A.8: Quality Score: Description Berechnung

Literaturverzeichnis

[eur22] eurostat. „Consumption of online news rises in popularity“. In: *Eurostat* (24.08.2022). URL: https://ec.europa.eu/eurostat/de/web/products-eurostat-news/-/ddn-20220824-1.

[Fac22] Faculty of Business and Economics. *Fake News in the Age of COVID-19*. 2.10.2022. URL: https://fbe.unimelb.edu.au/newsroom/fake-news-in-the-age-of-covid-19.

[Deu22] Deutschlandfunk.de. *Desinformation in den sozialen Medien - Gefahr vor allem durch Messenger-Dienste*. 2.10.2022. URL: https://www.deutschlandfunk.de/desinformation-in-den-sozialen-medien-gefahr-vor-allem-100.html.

[eik19] eikito_kw_2019. „Wie sich Fake News verbreiten“. In: *Klickwinkel* (9.08.2019). URL: https://klickwinkel.de/tutorials/wie-sich-fake-news-verbreiten/.

[Min+19] Yong Min u. a. „Endogenetic structure of filter bubble in social networks“. In: *Royal Society open science* 6.11 (2019), S. 190868. ISSN: 2054-5703. DOI: 10.1098/rsos.190868.

[Men22] Filippo Menczer. *Facebook's algorithms fueled massive foreign propaganda campaigns during the 2020 election – here's how algorithms can manipulate you*. 13.09.2022. URL: https://theconversation.com/facebooks-algorithms-fueled-massive-foreign-propaganda-campaigns-during-the-2020-election-heres-how-algorithms-can-manipulate-you-168229.

[Suc21] Peter Suciu. „Spotting Misinformation On Social Media Is Increasingly Challenging“. In: *Forbes* (2.08.2021). URL: https://www.forbes.com/sites/petersuciu/2021/08/02/spotting-misinformation-on-social-media-is-increasingly-challenging/?sh=65de24432771.

[BOW22] Vitalik Buterin, Puja Ohlhaver und E. Glen Weyl. „Decentralized Society: Finding Web3's Soul“. In: (2022).

[Jef20] Jeff Petters. *What is PGP Encryption and How Does It Work?* 2020. URL: https://www.varonis.com/blog/pgp-encryption.

[Chr01] Christian Kirsch. *S/MIME vs. OpenPGP: Eine Entscheidungshilfe*. 2001. URL: http://2014.kes.info/archiv/online/01-01-60-SMIMEvsOpenPGP.htm.

[Ele22] Elektronik-Kompendium.de, Hrsg. *Hybride Verschlüsselungsverfahren*. 11.08.2022. URL: https://www.elektronik-kompendium.de/sites/net/1910141.htm.

[Cal+07] J. Callas u. a. *OpenPGP Message Format*. 2007. DOI: 10.17487/RFC4880. URL: https://www.rfc-editor.org/rfc/rfc4880#section-1.

[Vie08] John Viega. *Beautiful security*. Theory in practice. Farnham: O'Reilly, 2008. ISBN: 0596527489.

[Eic01] Thomas Eicker. *Vertrauensmodell | Definition | Ein kleines! Lexikon des Internet*. 2001. URL: http://kleines-lexikon.de/w/v/vertrauensmodell.shtml.

[fu-04] fu-berlin. „Vorlesung Rechnersicherheit“. In: (2004). URL: https://www.mi.fu-berlin.de/inf/groups/ag-idm/teaching/Rechnersicherheit/RS9.pdf.

[Car00] G. Caronni. „Walking the Web of trust“. In: *Proceedings IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2000)*. Hrsg. von Matthew L. Nelson, Michael J. Shaw und Troy J. Strader. IEEE Comput. Soc, 2000, S. 153–158. ISBN: 0-7695-0798-0. DOI: 10.1109/ENABL.2000.883720.

[Hei04] Heise Medien. „Krypto-Kampagne“. In: *heise online* (26.03.2004). URL: https://www.heise.de/security/dienste/Krypto-Kampagne-2111.html.

[gpg17] gpgTools. *What is Ownertrust? Trust-levels explained / FAQ / Knowledge Base - GPGTools Support*. 2017. URL: https://gpgtools.tenderapp.com/kb/faq/what-is-ownertrust-trust-levels-explained.

[Mik13] Mike Perry. *Why the Web of Trust Sucks*. 2013. URL: https://cryptome.org/2013/09/web-trust-sucks.htm.

[AD11] Vijay Atluri und Claudia Diaz. *Computer Security – ESORICS 2011*. Bd. 6879. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011. ISBN: 978-3-642-23821-5. DOI: 10.1007/978-3-642-23822-2.

[Wik22] Wikipedia, Hrsg. *Small-world network*. 2022. URL: https://en.wikipedia.org/w/index.php?title=Small-world_network&oldid=1104203505.

[A F14] A Few Thoughts on Cryptographic Engineering. *What's the matter with PGP?* 2014. URL: https://blog.cryptographyengineering.com/2014/08/13/whats-matter-with-pgp/.

[Rob19] Robert J. Hansen. *SKS Keyserver Network Under Attack*. 2019. URL: https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f.

[Max19] Maximilian Weber. *PGP - The Web of Trust is Dead | inversegravity.net*. 2019. URL: https://inversegravity.net/2019/web-of-trust-dead/.

[Sch19] Jürgen Schmidt. „PGP: Der langsame Tod des Web of Trust“. In: *heise online* (10.07.2019). URL: https://www.heise.de/hintergrund/PGP-Der-langsame-Tod-des-Web-of-Trust-4467052.html.

[pgp20] pgp. *MIT PGP Key Server – Frequently Asked Questions*. 8.10.2020. URL: http://pgp.mit.edu/faq.html.

[Imt21] Imtermet Archive: The WaybackMachine. *SKS Keyservers*. 2021. URL: https://web.archive.org/web/20220119094712/https://www.sks-keyservers.net/.

[Eur18] Europäische Union. *Art. 17 DSGVO – Recht auf Löschung (Recht auf Vergessenwerden)*. 2018. URL: https://dsgvo-gesetz.de/art-17-dsgvo/.

[PK00] Paul Resnick und Ko Kuwabara Richard Zeckhauser Eric Friedman. *Reputation Systems*. 2000. URL: https://cacm.acm.org/magazines/2000/12/7494-reputation-systems/fulltext.

[NSS09] Matthew L. Nelson, Michael Shaw und Troy J. Strader. *Value creation in e-business management: 15th Americas conference on information systems, AMCIS 2009, SIGeBIZ track, San Francisco, CA, USA, August 6-9, 2009 selected papers*. Bd. 36. Lecture notes in business information processing. Berlin und New York: Springer, 2009. ISBN: 9783642031311.

[ARC07] Jøsang Audun, Ismail Roslan und Boyd Colin. *A Survey of Trust and Reputation Systems for Online Service Provision*. 2007. DOI: 10.24071/llt.v24i2.2962.s346.

[Gol09] Jennifer Golbeck. „Trust and Online Reputation Systems“. In: (2009).

[AJ19] Mohammad Alsmirat und Yaser Jararweh, Hrsg. *A Brief Analysis of Amazon Online Reviews: Granada, Spain, October 22-25, 2019*. Piscataway, NJ: IEEE, 2019. ISBN: 9781728129464. DOI: 10.1109/SNAMS47927.2019. URL: https://ieeexplore.ieee.org/servlet/opac?punumber=8926314.

[Fee19a] FeedbackWhiz. *How Are Amazon Product Ratings Calculated? - FeedbackWhiz*. 2019. URL: https://www.feedbackwhiz.com/blog/how-does-amazon-calculate-product-ratings/.

[Ama22] Amazon. *Understanding Customer Reviews and Ratings - Amazon-Kundenservice*. 2022. URL: https://www.amazon.com/-/de/gp/help/customer/display.html/ref=cm_cr_dp_d_omni_lm_btn?nodeId=G8UYX7LALQC8V9KA.

[JJJ19] Jianmo Ni, Jiacheng Li und Julian McAuley. *Justifying recommendations using distantly-labeled reviews and fined-grained aspects: Empirical Methods in Natural Language Processing (EMNLP), 2019*. 2019. URL: https://nijianmo.github.io/amazon/index.html.

[Lee20] Isabelle Lee. „Amazon Fake Reviews Reach Holiday Season Levels During Pandemic“. In: *Bloomberg* (19.10.2020). URL: https://www.bloomberg.com/news/articles/2020-10-19/amazon-fake-reviews-reach-holiday-season-levels-during-pandemic.

[Car17] Samuel Carter. „Amazon's rating system is broken and it might be your fault“. In: *LinkedIn* (7.06.2017). URL: https://www.linkedin.com/pulse/amazons-rating-system-broken-might-your-fault-samuel-carter.

[Der21] DerSpiegel. „Angebliche Fake-Bewertungen: Amazon wirft offenbar mehrere bekannte Händler raus“. In: *DER SPIEGEL* (12.05.2021). URL: https://www.spiegel.de/netzwelt/web/aukey-betroffen-amazon-wirft-offenbar-mehrere-bekannte-haendler-raus-a-1a00b423-b671-41ee-8476-35af7021310f-amp.

[The22] TheSpiritOfFunk. *r/de - Wie nett. Ein Amazon Verkäufer hat mich darauf hingewiesen doch noch eine Review zu schreiben*. 7.2022. URL: https://www.reddit.com/r/de/comments/vruxmk/wie_nett_ein_amazon_verk%C3%A4ufer_hat_mich_darauf/.

[Bis22] Todd Bishop. „Amazon sues six alleged fake review sites — we chatted with one that didn't believe suit was real“. In: *GeekWire* (12.08.2022). URL: https://www.geekwire.com/2022/amazon-sues-six-alleged-fake-review-sites-we-chatted-with-one-who-didnt-believe-the-suit-was-real/.

[Fee19b] FeedbackWhiz. *Amazon Fake Reviews - Should You Trust All Reviews? - FeedbackWhiz*. 2019. URL: https://www.feedbackwhiz.com/blog/amazon-fake-reviews-should-you-trust-all-reviews/.

[eth22] ethereum.org. *Web2 vs Web3 | ethereum.org*. 2.10.2022. URL: https://ethereum.org/en/developers/docs/web2-vs-web3/#top.

[SLC22] Manu Sporny, Dave Longley und David Chadwick. *Verifiable Credentials Data Model v1.1*. 2022. URL: https://www.w3.org/TR/vc-data-model/#presentations.

[ver21] verifiablecredentials.iol. *An Introduction to Verifiable Credentials*. 22.07.2021. URL: https://verifiablecredential.io/learn.

[Mic20] Microsoft. *What are Verifiable Credentials? | Decentralized Identity Developer Docs*. 21.11.2020. URL: https://didproject.azurewebsites.net/docs/verifiable-credentials.html.

[Bor+17] Maria Borge u. a. „Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies“. In: *2nd IEEE European Symposium on Security and Privacy workshops*. Piscataway, NJ: IEEE, 2017, S. 23–26. ISBN: 978-1-5386-2244-5. DOI: 10.1109/EuroSPW.2017.46. URL: https://berkeley-defi.github.io/assets/material/Proof%20of%20Person.pdf.

[Hum22] Humanode.io. „Proof of Personhood Approaches“. In: (2022). URL: https://blog.humanode.io/proof-of-personhood-approaches/.

[CF05] Alice Cheng und Eric Friedman. „Sybilproof reputation mechanisms“. In: *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. Hrsg. von Kevin Fall. ACM Conferences. New York, NY: ACM, 2005, S. 128. ISBN: 1595930264. DOI: 10.1145/1080192.1080202. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1010.1001&rep=rep1&type=pdf.

[But21] Vitalik Buterin. *Why we need wide adoption of social recovery wallets*. 2021. URL: https://vitalik.ca/general/2021/01/11/recovery.html.

[Clo22] Cloudflare. *Interplanetary File System (IPFS) · Cloudflare Web3 docs*. 2022. URL: https://developers.cloudflare.com/web3/ipfs-gateway/concepts/ipfs/.

[eth02] ethereum.org. *Zero-knowledge proofs | ethereum.org*. 2002. URL: https://ethereum.org/en/zero-knowledge-proofs/.

[Bac22] James Bachini. *GitHub - jamesbachini/Solidity-SBT-Soul-Bound-Token: An experiment in creating a soul bound token (SBT)*. 2022. URL: https://github.com/jamesbachini/Solidity-SBT-Soul-Bound-Token.

Eidesstattliche Erklärung

Hiermit versichere ich – Alexander Hultzsch – an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe.

Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Mittweida, 21. November 2022 | Alexander Hultzsch

Ort, Datum | Alexander Hultzsch