|  |  |  |
| --- | --- | --- |
|  |  | Logo_HSMW_blau_CMYK |
| **BACHELORARBEIT** |  |  |
|  |  |  |
| Herr  **Alexander Hultzsch** | * < |  |
| **Implementierung einer Reputationsplattform auf Basis von Soulbound Token** |  |  |
| Mittweida, 2022 |  |  |

|  |  |  |
| --- | --- | --- |
| Fakultät **Angewandte Computer- und Biowissenschaften** |  |  |
| **BACHELORARBEIT** |
|  |  |  |
| **Implementierung einer Reputationsplattform auf Basis von Soulbound Token** |  |  |
| Autor: **Alexander Hultzsch** |  |  |
| Studiengang: **Softwareentwicklung** |  |  |
| Seminargruppe: **If19ws-B>** |  |  |
| Erstprüfer: **Prof. Dr.-Ing. Andreas Ittner** |  |  |
| Zweitprüfer: **Hira** |  |  |
| Einreichung: **<ort>, <tag>.<monat>.<jahr>** |  |  |
| Verteidigung/Bewertung: **<ort>, <jahr>** |  |  |

|  |  |  |
| --- | --- | --- |
| Faculty of Applied Computer and Biosciences |  |  |
| **BACHELOR THESIS** |
|  |  |  |
| **Implementing a reputation platform based on Soulbound Tokens** |  |  |
| author: **Mr.**  **Alexander Hultzsch** |  |  |
| course of studies: **Software Development** |  |  |
| seminar group: **If19wS-B** |  |  |
| first examiner: **Prof. Dr.-Ing. Andreas Ittner** |  |  |
| second examiner: **<titel> <akad. grade> <vname> <name>** |  |  |
| submission: **<ort>, <tag>.<monat>.<jahr>** |  |  |
| defence/ evaluation: **<ort>, <jahr>** |  |  |

**Bibliografische Beschreibung:**

Hultzsch, Alexander:

Implementierung einer Reputationsplattform auf Basis von Soulbound Tokens – 2022 …

<name>, <vorname>:

<thema der graduierungsarbeit>. - <jahr der einreichung>. - <seitenzahl verzeichnisse>, <seitenzahl des inhalts>, <seitenzahl der anhänge> S.

Mittweida, Hochschule Mittweida, Fakultät <fakultätsbezeichner>, <art der arbeit>, <jahr>

Referat:

<kurzbeschreibung des inhaltes

Inhalt

Inhalt I

Abbildungsverzeichnis III

Tabellenverzeichnis IV

Abkürzungsverzeichnis V

1 Einführung 7

2 Grundlagen 8

2.1 Das Web of Trust als Vorgänger 8

2.1.1 Funktionsweise und Prinzipien 8

2.1.2 Limitationen 8

2.2 Blick auf bestehenden Reputationsplattformen 8

2.2.1 Bestehende Bewertungsmechanismen im Web 2.0 8

2.2.1.1 Amazon 8

2.2.1.2 LinkedIn,Kleinanzeigen? 8

2.2.1.3 Die Online Fraud Prevention Foundation und SteamRep 9

2.2.2 Bestehende Bewertungsmechanismen im Web 3.0 9

2.2.2.1 Self-Souvereign Identity 9

2.2.2.2 Verifiable Credentials 9

2.2.2.3 Proof of Personhood 9

2.3 Probleme und Angriffsvektoren 10

2.3.1 Sybil Attacks und Denunziation 10

2.3.2 Identitätsverlust 10

2.3.2 Privatsphäre 10

3 Implementierung einer Reputationsplattform 11

3.1 Methodik 11

3.1.2 Architekur 11

3.1.3 Frameworks 11

3.1.4 Smart Contract 11

3.2 Ergebnis 11

4 Schluss 12

4.1 Diskussion 12

4.2 Ausblick 12

Index 13

Literatur 15

Anlagen 17

Anlagen, Teil 1 I

Anlagen, Teil 2 III

Anlagen, Teil 3 VI

Selbstständigkeitserklärung 7

Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

Tabellenverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

Abkürzungsverzeichnis

**<abk>** <langfassung>

1 Einführung 5% 1,5

2 Grundlagen 45% 15

2.1 Das Web of Trust als Vorgänger **10**% 3

2.1.1 Funktionsweise und Prinzipien 5% 2

2.1.2 Limitationen 5% 1

2.2 Blick auf bestehenden Reputationsplattformen **15**% 8

2.2.1 Bestehende Bewertungsmechanismen im Web 2.0 5-10% 3

2.2.1.1 Amazon 2,5% 2

2.2.1.2 LinkedIn,Kleinanzeigen? 2.5% 0

2.2.1.3 Die Online Fraud Prevention Foundation und SteamRep 2,5% 1

2.2.2 Bestehende Bewertungsmechanismen im Web 3.0 **12,5**% 9

2.2.2.1 Self-Souvereign Identity 4% 1

2.2.2.2 Verifiable Credentials 4% 1

2.2.2.3 Proof of Personhood 4% 1

2.3 Probleme und Angriffsvektoren **15**% 3

2.3.1 Sybil Attacks und Denunziation 5% 1

2.3.2 Identitätsverlust 5% 1

2.3.2 Privatsphäre 5% 1

3 Implementierung einer Reputationsplattform 40% 13

3.1 Methodik **10**% 3

3.1.2 Architekur 5 2

3.1.3 Frameworks 2,5 2

3.1.4 Smart Contract 2,5 2

3.2 Ergebnis **20**% 3

4 Schluss 10 3

4.1 Diskussion 1,5

4.2 Ausblick 1,5

Index 13

1. Einführung

The spread of Fake News is on the rise…

It’s hard to find verifiable sources from trustworthy users…

SBTS may be a way to bring back trsut in web3

Web3 in particular is riddled with scams and schemes

Current problems of onlline reputation systems

(1) Low incentive for providing rating;

(2) Bias toward positive rating;

(3) Lack of effective mechanisms against unfair ratings;

(4) change of identities after reputation loss;

(5) Quality variations over time

(das ist vom Buc) Web Of Trust

Trust is a broad concept

Trust in darknet would be quite interesting

1. Grundlagen

Explain what is trust

Where does trust come from (how can we trust sbts come from trustworthy -> central authority is needed)

<jk Validity is only a score and can be used only to determine whether the name on a key is accurate. Trust is a relationship that helps us determine validity.>

SBTs can be used in markets alongside nfts to gain trust of sellers of nfts

* 1. Das Web of Trust als Vorgänger

### Funktionsweise und Prinzipien

### Limitationen

* 1. Blick auf bestehenden Reputationsplattformen
* Reputation System: for markets to collect feedback from participants and decide whom to trust, also encourages trustworthy behaviors
* For trust in stranger „establish shadow oft he future“ i.e. track historic data (Blockchain gud for this?
* Ebays Feedback forum is well studied, showing commercial succes for better reputation
* Web 2.0 vs Web 1.0 -> folksonomy, empowerment of ordinary user who posts himself (social media)
* **Reputation Systems and Reputation**
* Reputation is funky basically, ist very dynamic. A publisher gets reputation based on different aspects (gender, quality)
* In Web, its important to get credit of product/orga
* 3 Major Properties for a system to function:
* (i) authenticating the subject is who  
  they claim to be,
* (ii) determining the subject is capable of performing some specific  
  service
* (iii) determining if the subject can consistently deliver the desired result
* **Input**
* 2 types: Implizit and explicit:
* Explicit: info entered by uiser i.e. votes or rating. Can be summarized to generate history(ebay)
* Implicit; Derived without user knowing -> network behavioral data (Facebook, LinkedIn)
* **Processin**
* Either **centralized** or distributed network
* Central authority collects members information about product/service and summarize into score (e-rating,-evoting) use explicit and implciit info
* E: rating lets users enter evaluation for quality of transaction of buyer/seller (Ebay/Amazon) and get past behaviour publicly. Ebay has +1/-1 which is works for everyone around the globe! Yay!
* E-voting, also ballot box communication uses limited cummonication ways. It’s cheap in time to particiapte, so you gett many-to one voices (Youtube, Digg/(Reddit?). But little knowledge is captured, easy to manipulate. Access Statistics (views, comments) often released in conjuction to imply popularity.
* Very useful in cnjunction i.e 1mil views 50/50 votes vs 500k views and 90/10 votes ?:)
* **Decentralized** lack central authority instead, hosted on nodes who take locally generated reputation and spread to generate global rating score
* Scores depend on objective node activity (like views form earlier) or subjective node opinions
* **Using peer subjective ratings to generate reputation scores in a P2P  
  network, however, is more complicated and requires considerable academic work in developing algorithms than e-rating and e-voting in centralized reputation systems**
* We have 2 direction probabilistic estimations and social networks:
* Proba uses estimation techniques like maximum likelihood estimation and Bayesian estimation + some global feedboch to score a peer.
* Social network approach aggeragates the globally available feedback to asses reputation
* **Output**
* Usually just a score, a scale or comments along with the objects
* While accompanying objetcs with their score is great for historic quality, that shit is scattered all over the website and har dto aggregate categorize and ocmpare
* Rep infor could be analyzed and used internally , but there are strategies to use this inofmration to reach customers on ecommerce or online communities
* **Problems with Pre 2.0 RepSys**
* Shit often fails, cuz it misrepresents performance of communit o rare artifially inflated/deflated, maybe even maliciously???
* Creating an Incentive for feedback is a real feedback, who ensures honesty? Malfoys can collarborate or collude
* You can’t track history, since everyone can just create a new identity and erase it. A Lack of history makes predicitons impossible. Participants with a history are concerned with it because it takes time to build
* Reputation accumulated cannot be shared on another site i.e lack of portability.
* Different communites user different measures to compare reputation making travelling between them difficult
* Users are reluctant to carry over their scores because of privacy
* Miscalculation like score pure positive vs same score but mixed, it also doesnt say a lout about the participant (could be good in plants but shit in nuclear physics). Also doesnt count in time and context of score.
* Social network is pretty good, only using explicit is not good

### 2.2.1 Bestehende Bewertungsmechanismen im Web 2.0

#### Amazon

* Amazon is succesful ecommerce can it address the weakness of pre 2.0 reputation? And what new weaknesses appear
* Multimedia feedback -> text video images, richer information to avoid misinterpretation in the score
* Very useful for non physical products, image made by the camera itself allow to testify and let users make their own judgement (sbt link to image?)
* Folksonomy(social taggin) (Verschlagwortung) Amazon bietet bei jedem produkt reihe von Schlagwörtern an
* Ilustrated in a tag list, the tags that members use to describe a product to indicate product specific tag reputation
* More customers who tag a particular product indicates more interestr
* It used tob e product centered, now it embraces reviwers reputation.
* A profile is displayed to each review
* Reviews ranked on quality (most imnportant), currentnes, number of reviews of reviwer
* Quality depends on how man marked it as „being helpful“
* Reviewers als get badges „top 10 reviwer“ as top top ranked, „real name“ real identity by credit card (those are good ideas for sbts)
* „community forum 04 badge“ recognizes reviwer as participant of 2004 community forum at amazon headuqarter
* Badges that are not review oriented (liek last 2) are also helpful, to establish credibility to reviewer
* Badges are acts to earn reputation and be recognized at amazon which in turn is incentive at participation
* System measures reputaion of every user, ist is important incentivce in web 2
* Amazon provides various opprtunites to participate (dauntin like writin review, less daunting like taggin a product )
* Amazon records evry tag, every reviewmdiscussion, image, list etc.
* Uses implicit measure to see how often review has been read
* Reputation is a sum of all contributions,
* Discussion forums allow users to comment on each others review to voice smth

Als größter online retailer geht amazon rigoros gegen gekaufte reviews vor und verbietet diese, allerdings sind viele dennoch gekauft wodurch die meisten reviews fragwürdig sind. Real life example: <https://www.reddit.com/r/de/comments/vruxmk/wie_nett_ein_amazon_verkäufer_hat_mich_darauf/>

Lots of fake reviews on amazon, its a business to buy fake reviews ->

<https://reviewmeta.com>

bekämpft symtpom aber nicht ursache

#### LinkedIn,Kleinanzeigen?

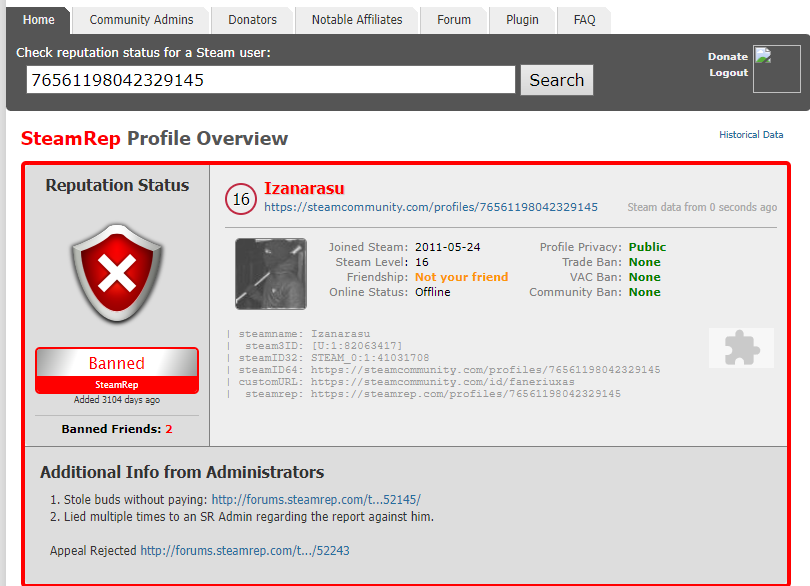
Weitere Beispiele anbringern? Benötigt weitere recherche, um zu sehen was die meisten gemeinsam haben und ob es einige ausreißer gibt, die es wert ist noch zu nennen.

https://www.reddit.com/r/de/comments/vruxmk/wie\_nett\_ein\_amazon\_verkäufer\_hat\_mich\_darauf/

#### Die Online Fraud Prevention Foundation und SteamRep

Online trading Communites have been fighting Fraud for a long time now, here is their implementation of a trust system…

Positive merkmale feststellen und Vision der Plattform vergrößern auf Soziale Medien, News Outlets usw.



Beispiel für einen untrustworthy User. Immediately apparaent

### Bestehende Bewertungsmechanismen im Web 3.0

Könnte man auch alles in einen Punkt zusammenfassen je nach Inhaltsdichte.

#### 2.2.2.1 Self-Souvereign Identity

Der zweite Baustein aus dem \acrshort{SSI}s bestehen sind sog. \acrfull{DID}s.

Während \acrshort{VC}s die Dokumente belegen, die ein Nutzer vorlegen kann, wird die Identiät des Nutzers selber dadurch nicht direct bestätigt. Ein DID ist ein Identifier für eine Identität, ähnlich wie eine URL für eine Website. Mit dem Unterschied dass keine zentrale Authorität gebraucht wird und… https://gataca.io/blog/self-sovereign-identity-ssi-101-decentralized-identifiers-dids-verifiable-credentials-vcs

#### 2.2.2.2 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 beschreibt wie man diese digitalen Beglaubigungen kryptographisch sichert, Privatssphäre 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 können dadurch neue Bescheinigungen entstehen, diese sind auch mithilfe von digitalen Signaturen sicherer und dadurch auch vertrauenswürdiger. https://www.w3.org/TR/vc-data-model/#dfn-verifiable-presentations

Jedes \acrshort{VC} wird von einem Issuer erstellt. Issuer können hierbei Einzelpersonen, Organisationen oder andere Einrichtungen sein, welche die Informationen auf dem \acrshort{VC} bestätigen können, wie z.B. Eine Universität für ein Abschlusszeugnis. Die Person, welcher das \acrshort{VC} zusteht bzw. besitzt wird auch als Holder bezeichnet und wahrt dieses in ihrer Wallet auf. Nun kann der Holder die im \acrshort{VC} hinterlegten Informationen beweisen und einem Verifier vorlegen. Der Verifier hat nun die Möglichkeit, den ihm vorgelegten Information zu vertrauen oder nicht. Hierbei muss die Entität betrachtet warden, welche die Bescheinigung ausgestellt hat, da nicht alle Issuer gleich vertrauenswürdig sind für den Verfiier. https://verifiablecredential.io/learn 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 \acrshort{VC} unterschrieben wurde. Somit kann gewährleistet warden, dass die Bescheinigungen von einem echten Issuer kommt und sich nicht um eine Fälschung handelt. Mithilfe der Blockchain lassen sich die öffentlichen Schlüssel eines jeden Issuers finden und jegliche dessen Signaturen validieren.

<https://didproject.azurewebsites.net/docs/verifiable-credentials.html>

Der Prozess des Vorzeigens eines \acrshort{VC} von einem Holder gegenüber einem Verifier wird auch als Verifiable Presentation bezeichnet. \acrshort{VP}s stellen Informationen von einem oder mehreren \acrshort{VC}s dar und sind so verpackt, das die Aussteller der Daten immer noch verifizierbar sind. Mit ihnen ist es möglich nur die nötigen Informationen für eine gegebene Situation preiszugeben. Somit kann der Nutzer sich eine Reihe von \acshort{VP}s aufbauen, welche alle einen Teil seiner Persönlichkeit wiederspiegeln, wie z.B. ein Gesundheits Persona, Berufs Persona etc. und damit seine Privatheit schützen.

https://www.w3.org/TR/vc-data-model/#presentations

#### 2.2.2.3 Proof of Personhood

* 1. Probleme und Angriffsvektoren

### Sybil Attacks und Denunziation

SBT Spam

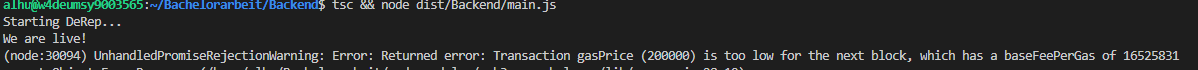
### 2.3.2 Identitätsverlust

Verkauf von Souls, Verlust -> Community recovery

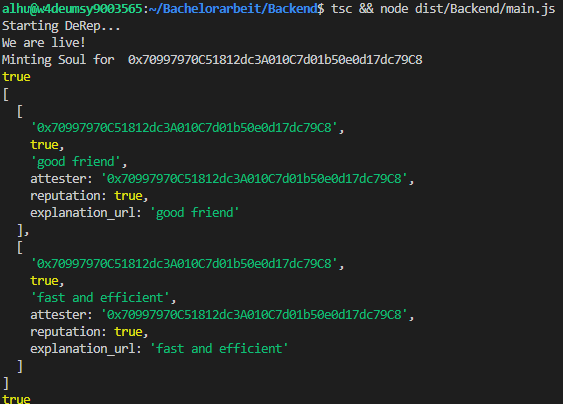
### 2.3.2 Privatsphäre

Public vs private sbts

1. Implementierung einer Reputationsplattform

****

****

****

Implementierung via Typescript

**3.1 Methodik**

### 3.1.2 Architekur

### 3.1.3 Frameworks

### 3.1.4 Smart Contract

**3.2 Ergebnis**

Präsentation von Key Methoden

Further researches in this area are clearly needed and likely very productive

1. Schluss

**4.1 Diskussion**

**4.2 Ausblick**

Index

Webservice

Kernelemente 2

Literatur

|  |  |
| --- | --- |
| [namenskürzeljahr] | <name>, <vorname>: <titel des buches|artikels|…>,  <erscheinungsort>, <verlag>, <jahr>  oder <url>, verfügbar am <datum, uhrzeit> |
|  |  |
|  |  |
|  |  |
|  |  |

Anlagen

Teil 1 …………………………………………………………………………………… A-I

Teil 2 …………………………………………………………………………………… A-III

Teil 3 …………………………………………………………………………………… A-V

Anlagen, Teil 1

<inhalt anlage teil1>

Anlagen, Teil 2

<inhalt anlage teil2>

Anlagen, Teil 3

<inhalt anlage teil3>

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

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

<ort>, den <tag>.<monat>.<jahr>

<unterschrift>

<vorname> <name>