HAW HAMBURG

BACHELORTHESIS
Milan Nikola Eric

Eine kritische Evaluierung von Web 3.0: Konzeption und prototypische Umsetzung einer dezentralen App auf der Ethereum Blockchain

FAKULTÄT TECHNIK UND INFORMATIK
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG
Hamburg University of Applied Sciences

Milan Nikola Eric

Martikel-Nr.: [redacted]

Eine kritische Evaluierung von Web 3.0: Konzeption und prototypische Umsetzung einer dezentralen App auf der Ethereum Blockchain

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Wirtschaftsinformatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Olaf Zukunft
Zweitgutachter: Prof. Dr. Stefan Sarstedt

Eingereicht am: 30.08.2022

Milan Nikola Eric

Thema der Arbeit

Konzeption und prototypische Umsetzung einer dezentralen App zur kritischen Evaluation von Web3.

Stichworte

Web3, Blockchain, Dezentralität, Internet, Evaluation, Experimentell, Prototyp, Ethereum, The Graph, IPFS, GQM-Verfahren

Kurzzusammenfassung

Diese Bachelorarbeit hat mithilfe eines eigens erstellten Konzepts die Dezentralität, Sicherheit, Funktionalität, Effizienz und Benutzerfreundlichkeit eines Prototyps untersucht. Durch die Quantifizierung von Metriken ist zu erkennen, dass diese experimentelle Thesis kein positives Ergebnis liefert. Web3 hat klare Herausforderung in der Komplexität der Entwicklung und Anwendung von DApps. Die erfolgreichen Ergebnisse bei der Sicherheit sind auf die mangelnden Funktionalitäten des Prototyps zurückzuführen. Insgesamt ist die Sicherheit von komplexeren DApps oftmals komprimiert und ein schweres Verfahren. Dazu kommt die mangelnde Effizienz der beliebtesten Blockchain Ethereum. Diese hat oftmals mit hohen Gebühren und Scaling-Problemen zu kämpfen. Das bedeutsamste Versprechen von Web3, die Dezentralität, wurde mittelmäßig bewertet. Es gibt einige zentrale Engpässe, welche jedoch zum Teil keine großen Risiken bergen. Insgesamt lässt sich jedoch auch dieser Thesis ableiten, dass die Web3 Entwicklung komplex ist und kaum den Vorgaben der Web3 Vision entspricht. Dabei ist Web2 zu komfortabel und kann mit Effizienz, Sicherheit und Benutzerfreundlichkeit punkten. Web3 ist nicht bereit, das alte Web zu ersetzen und in Teilen auch in den Händen von Web2-Unternehmen wie Amazon.

Milan Nikola Eric

Title of Thesis

Conception and prototype Implementation of a decentralized app for a critical evaluation of Web3.

Keywords

Web3, Blockchain, Decentralization, Internet, Evaluation, experimental, prototype, Ethereum, The Graph, IPFS, GQM

Abstract

This bachelor thesis investigated a prototype's decentralization, security, functionality, efficiency, and usability using a self-developed concept. By quantifying metrics, this experimental thesis does not yield a positive result. Web3 has a clear challenge in the complexity of developing and using DApps. The positive results in security can be attributed to the lack of functionality in the prototype. Overall, the security of more complex DApps is often complicated and a difficult process. In addition, there is a lack of efficiency in the most popular blockchain Ethereum. Which often struggles with high fees and scaling issues. The most important promise of Web3, decentralization, was rated mediocre. There are some centralization approaches, but some of these do not pose significant risks. Overall, however, it can also be deduced from this theme that Web3 development is complex and hardly meets the specifications of the Web3 vision. At the same time, Web2 is too comfortable and can score with efficiency, security, and user-friendliness. Web3 is not ready to replace the old Web and is partly in the hands of Web2 companies like Amazon.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Abkürzungsverzeichnis

Web2	Web 2.0
Web3	Web 3.0
ISO	Internationale Organisation für Normung
DApp	Dezentrale Applikation
DAO	Dezentrale Autonome Organisation
PoW	Proof-of-Work
PoS	Proof-of-Stake
EVM	Ethereum Virtual Machine
EIP	Ethereum Improvement Proposal
IPFS	InterPlanetary File System
ERC	Ethereum request for comment
NFT	Non-fungible Token
HHI	Herfindahl-Hirschman inde

1 Einleitung

1.1 Einführung in das Thema

Geheimdienste kennen den Standort jeder Person, die Hochzeitspläne des Nachbarn, das Liebesleben der Tochter, die Probleme jedes Menschen. Jedoch sorgte das moderne Web dafür, dass auch Unternehmen wie Google, TikTok oder Meta (Facebook) diese Informationen besitzen (vgl. Wietlisbach 2018). Das Web ist dominiert von Plattformen, in welcher Privatsphäre nicht existiert und Zensur Alltag sein kann. Die Macht der Informationen liegt bei großen Firmen und ist die wertvollste Ressource unserer Zeit. Doch alles hat ein Ende und die nächste Generation des Webs scheint auf dem Vormarsch. Es verspricht, die Zentralität aufzulösen, die Macht an den Nutzer zurückzugeben und die Privatsphäre zu schützen sowie dem Bankensystem zu entkommen und eine neue Art der Wertschöpfung zu schaffen. Die Blockchain-Technologie soll dabei der Auslöser für den Umschwung in ein dezentrales und freies Web sein.

1.2 Ziel der Arbeit

Das Ziel dieser Arbeit ist es, das Versprechen von Web 3.0 (Web3) zu analysieren. Ist es eine Utopie oder schon dabei Web 2.0 (Web2) abzulösen? Welche Mittel benutzen Entwickler heute, was dominiert Web3, welche Tools sind fragwürdig und warum werden sie genutzt? Was sagen Kritiker und wird die Vision eingehalten? Diese und weitere Fragen gilt es zu klären, um abschließend eine finale Evaluation von Web3

abzugeben. Außerdem ist dies eine kritische experimentelle Bachelorarbeit und das Ergebnis dieser Arbeit ist vorher nicht bekannt.

1.3 Vorgehensweise

Um die vorher erwähnten Fragen zu beantworten, wird diese Bachelorarbeit mit dem GQM-Verfahren arbeiten. Dabei wird aus der Vision und Kritik von Web3 die relevantesten Grundpfeiler extrahiert und als Ziele dargestellt. Die darauffolgenden Fragen werden durch Metriken beantwortet und quantifiziert. Eine ausführliche Literaturrecherche analysiert mögliche Metriken und deren Messung.

Die verschiedenen Ziele und dessen Unterpunkte ergeben durch die Quantifizierung von Metriken Effektivitätsindikatoren, welche die Effektivität des jeweiligen Ziels in einem Spektrum von 0 bis 1 darstellt. Eigen erstellte Formeln zu Berechnung der Effektivitätsindikatoren sind Kernbestandteile des Konzepts.

Daraufhin wird das Konzept auf einen eigenen Prototyp angewandt. Dieser Prototyp spiegelt den aktuellen Entwicklungsstand für DApps wider und untersucht die beliebtesten Dienste und Protokolle. Die Ergebnisse werden zusammengefasst und erörtert. Dazu gehört die Analyse der Aussagekraft betreffender Effektivitätsindikatoren.

2 Grundlagen

Dieses Kapitel soll grundlegendes Wissen über Web3 und deren Technologien vermitteln, die für das Verständnis des Konzepts und der prototypischen Umsetzung

dieser Bachelorarbeit fundamental sind. Es wird dabei auch auf die Versprechen und die Kritik von Web3 eingegangen.

2.1 Geschichte des Webs

Die Grundlagen für das World Wide Web (WWW) wurden hauptsächlich von Tim Berner-Lee (*1955) in den 1980er entwickelt, einem Mitarbeiter am europäischen Forschungszentrum für Teilphysik in Genf (CERN). Er programmierte unter anderem das Hypertext Transfer Protokoll (HTTP), die Hypertext Markup Language (HTML), eine Server-Software zur Dateiverwaltung (vgl. Kirpal und Vogel 2006, 143–144) und definierte 1994 unsere heutigen Web-Adressen als Uniform Ressource Locators (URL) (Berners-Lee, 1994). Die erste Implementation des WWW beinhaltete diese Kernprotokolle und charakterisierte sich durch statische Webseiten, der uneingeschränkte Zugang zu Informationen und „read-only content“ (vgl. Choudhury 2014, 8096). Die Benutzung von Hypertext „to link and access information of various kinds as a web of nodes in which the user can browse at will” (Berners-Lee und Cailliau 1990) führte zur Entstehung des Web 1.0. Dies hatte jedoch einige Begrenzungen. Es war langsam, unterstütze keine bidirektionale Kommunikation und es konnte nicht mit den Webseiten interagiert werden (vgl. Nath et al. 2014, 86).

Schon früh wurde versucht, das Web zu kommerzialisieren. Es wurde unter anderem der Zugang zum Web, Browser, Produkte und Dienstleistungen verkauft. Durch die steigende Anzahl von Web-Nutzern wurde das Geschäft mit dem Internet lukrativer (vgl. Kirpal und Vogel 2006, 144–145). Die zunehmende Konzentrierung auf den Benutzer führte zu einer Entwicklung vom „read-only“ zu einem „read-write“-Web. In dem sogenannten Web2 konnte der Benutzer Inhalte zusätzlich schreiben, modifizieren und aktualisieren (vgl. Nath et al. 2014, 86). Neue Ideen wie RSS, AJAX, REST, XML oder CSS revolutionierten Webseiten und es konnten neue Inhalte durch Anwendungen wie Blogs, Wikis oder Mashups geteilt werden (vgl. Nath et al. 2014, 87). Unternehmen fingen an, das Web als eine Plattform anzusehen, anstatt nur Produkte und Services anzubieten. Die Ära der sozialen Netzwerke begann und

Onlineplattformen wie Facebook, Linkedin, YouTube oder Flickr revolutionierte das Internet aufs Neue (vgl. Wilson et al. 2011, 2).

Heute (Stand 2022) wird das Web von einigen wenigen zentralisierten Diensten wie Google, Facebook oder Amazon dominiert. Die generelle These ist, dass Web2 ein zentralisiertes Web ist und Web 1.0 dezentral und gemeinschaftsgeführt war (vgl. Dixon 2021)

Zurzeit wird an vielen Fronten an dem sogenannten Web3 gearbeitet. Dies soll das Web zurück zur ursprünglichen Dezentralität bringen, jedoch mit den Inhalten des modernen Web2 (vgl. Marlinspike 2022).

2.2 Definition und Begriffsabgrenzung

Das Web ist ein Teil des Internets und kann beschrieben werden „as a techno-social system“ (Fuchs et al. 2010, 42), in welche Menschen mit der Technologie interagieren. Die Definitionen für die verschiedenen Generationen des Webs sind oft unterschiedlich und nicht standardisiert.

Web3 ist ein neuer Begriff und hat verschiedene Interpretationen. Es wird „cooperative Web“ (Fuchs et al. 2010, 56), „executable web“ (Choudhury 2014, 8097), “semantic web” (Dwivedi et al. 2011, 978), “decentralized web” (Wood et al. 2022) und vieles mehr genannt. Der Begriff des semantischen Webs sticht dabei öfter bei älteren Artikeln hervor. Das von Berners-Lee gegründete World Wide Web Consortium (W3C) bezeichnet das semantische Web als das „Web of linked data“ (W3C.org o .J.) und arbeitet an Technologien zur Umsetzung des neuen Webs. Daten müssen dafür so strukturiert sein, dass Sie von Maschinen und Menschen gelesen werden können. Diese strukturierten Daten erlauben es Programmen, Bedeutung zu extrahieren. Somit könnte es z. B. erkennen, ob mit „Schlange“ das Tier oder eine Reihe von Menschen gemeint ist.

Informationen sollen besser miteinander verbunden werden und Artificial Intelligence (AI) soll dafür sorgen, dass Computer schnellere und relevantere Ergebnisse liefern (vgl. Selig 2022).

Während der ursprüngliche Entwickler des Webs Berners-Lee und sein Consortium an Technologien für das semantische Web arbeiten (RDF, OWL, SKOS, SPARQL, etc.), konzentriert sich die große Mehrheit auf ein neues Thema: Kryptowährungen und Blockchain.

Anstelle von „Linked Data“, semantisches Web, AI oder machine learning, erfüllen neue Buzzwörter wie Blockchain, Dezentralität, DAOs, Tonkenization viele Definitionen von Web3. Die sogenannte „Web 3 foundation“ erwähnt das semantische Web nicht auf deren Website, sondern fokussiert sich auf Dezentralität und Blockchains (vgl. Wood et al. 2022). Es ist nun die Rede von der Eliminierung des Mittelmanns, die Revolution des Geldes und Wertschöpfung, sowie die Demokratisierung des Webs mithilfe von dezentralen Apps (DApps) (vgl. Voshmgir 2018).

Die Definition von Web3 ist daher umstritten und nicht eindeutig definierbar. Diese These beschäftigt sich jedoch nicht mit dem semantischen Web, sondern fokussiert sich auf die Blockchain-Technologie.

2.3 Grundlegende Begriffe

Im Folgenden werden grundlegende Begriffe erläutert, die für das Verständnis weiterer Konzepte und Kapitel notwendig sind.

- *Dezentralität* ist einer der am meisten erwähnten Versprechen von Web3. In klassischen zentralisierten Systemen muss jede Transaktion durch einen zentralen Server validiert werden (Beispiel: Banken). Das Web wird hauptsächlich von zentralisierten Unternehmen wie Google, Facebook, Apple oder Amazon dominiert, die Nutzerdaten zentral speichern. Bei der Dezentralität hingegen, gibt es keinen zentralen Knoten, sondern mehrere Knoten, die untereinander mehrfach miteinander verbunden sind (s. Abb. 1) (vgl. Lantz und Cawrey 2020, 3–4).

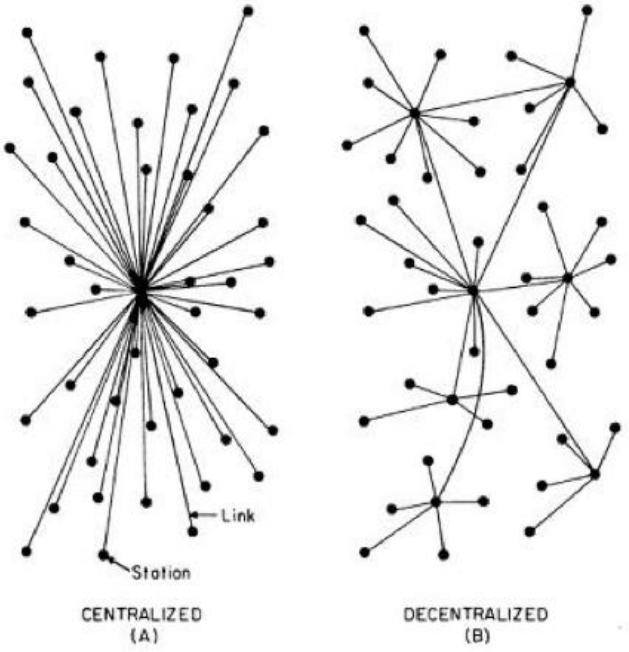

Abbildung 1: Centralized vs. Decentralized (vgl. Lantz und Cawrey 2020, 4)

- Ein *Peer-to-Peer-System* ist ein Computernetzwerk, das es Peers ermöglicht, Netzwerkressourcen, Rechenleistung und Datenspeicherung gemeinsam zu nutzen, ohne auf eine zentrale Autorität angewiesen zu sein. Diese verbundenen Peers handeln gleichzeitig als Server und Client (vgl. Fill und Meier 2020, 293).
- *Turing-Vollständigkeit* ist eine Maschine, die mit ausreichend Zeit, Speicher und den nötigen Anweisungen jedes noch so komplexe Rechenproblem lösen kann. Python, C++ oder auch die Blockchain Ethereum sind Turing-vollständig. Dies ist besonders bei Ethereum relevant, um die Smart Contracts zu verstehen (vgl. Antonopoulos und Wood 2019, 8)

2.4 Blockchain-Technologie

2.4.1 Grundlegende Technologien

Um die Blockchain-Technologie zu verstehen, müssen vorerst ein paar essenzielle Konzepte aus der Kryptografie und Informatik dargelegt werden.

- *Hash-Funktionen* bilden mithilfe von Funktionen Informationen auf eine vorher bestimmte Größe ab. Dabei soll möglichst keine Kollision auftreten und zwei verschiedene Eingabemengen ergeben unterschiedliche Zielwerte. Eine starke Kollisionsresistenz ist entscheidend für Blockchains. Wäre dies nicht der Fall, ist die Blockchain nicht manipulationssicher, unveränderbar und es wäre nicht nachweisbar, wer zu welchem Zeitpunkt z.B. welche Bitcoin-Menge besessen hat. Bitcoin verwendet den SHA-256-Hash-Algorithmus, ein Standard für viele Blockchains (vgl. Fill und Meier 2020, 5–8).

- *Hash-Bäume* sind Baumstrukturen aus der Graphentheorie, die aus aufeinanderfolgenden Hashwerten bestehen. Sie erlauben eine effiziente und sichere Verifikation von großen Datensätzen (vgl. Bashir 2017, 173).

- *Digitale Signaturen* sind ein fundamentales Konzept für die Blockchain-Technologie. Jeder Benutzer besitzt einen privaten und öffentlichen Schlüssel. Der Hashwert einer Transaktion wird mit dem privaten Schlüssel verschlüsselt. Diese digital unterschriebene Transaktion wird vom Empfänger verifiziert. Es wird mithilfe des öffentlichen Schlüssels des Senders der verschlüsselte Hashwert enthüllt. Stimmt dieser mit dem Hashwert der erneuten Anwendung des Hash-Algorithmus auf die Transaktion überein, ist die Signatur korrekt und die Transaktion ist abgeschlossen (vgl. Zheng et al. 2018, 356). Siehe Abbildung 2 für eine visuelle Erläuterung.

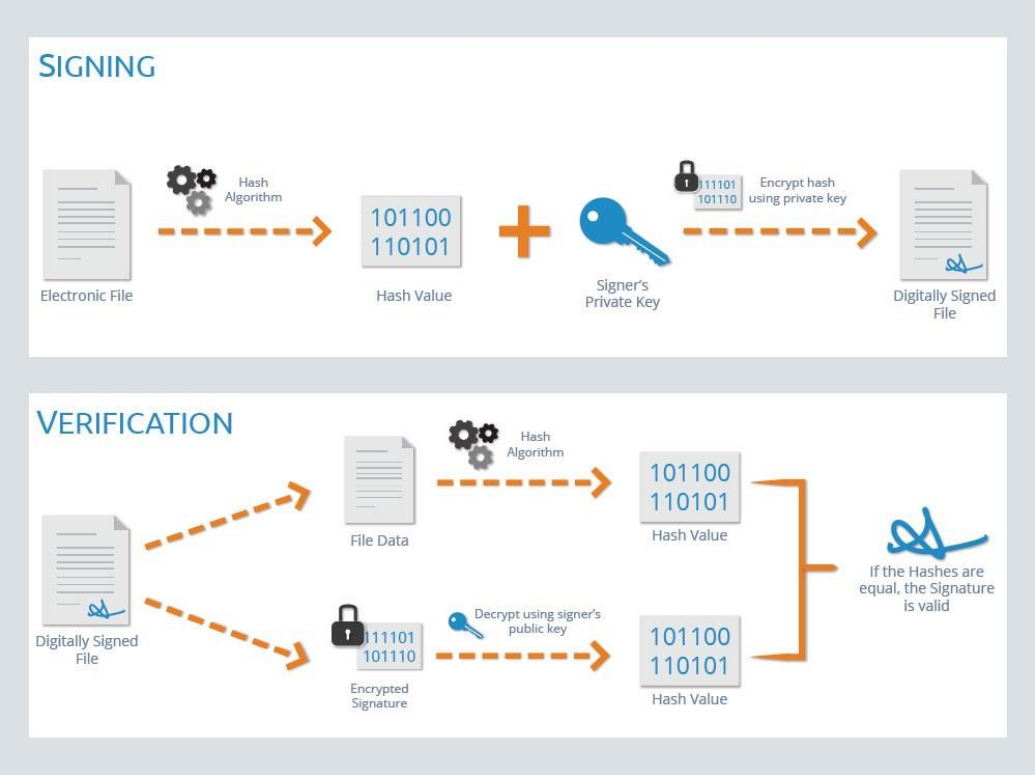

Abbildung 2: Digital Signaturen und Public Key als Identities (vgl. Zhao 2018)

2.4.2 Definition und Begriffsabgrenzung

Die Blockchain-Technologie ist eine noch recht neue Technologie (Stand 2022) und zahlreiche Unternehmen haben sich während des ersten richtigen Hypes 2016/17 damit beschäftigt. Damals, so wie heute, gab es noch keine einheitliche Definition der Blockchain-Technologie oder Industriestandards (vgl. Meinel und Gayvoronskaya 2020, 5).

Die Internationale Organisation für Normung (ISO) hat jedoch unter der Arbeit des ISO TC 307 angefangen, Standards zu veröffentlichen. Zurzeit (Stand Mai 2022) wird an 10 ISO Standards gearbeitet und 7 wurden veröffentlicht (ISO/TC 307 2020). Erst im Jahre 2020 wurde eine erste Version für die Standards der Terminologie in der Blockchain-Technologie veröffentlicht (ISO/TC 307 2020, ISO 22739:2020). Auf Basis dieser Terminologie lässt sich eine erste Definition bilden.

Wie der Name andeutet, ist die Blockchain eine Kette von „Blöcken“ (s. Abb. 3). Sie ist technisch gesehen eine dezentrale Datenbank, die auf allen Rechnern des Netzwerks separat gespeichert wird. Die Blöcke enthalten je nach Anwendungsfall Daten. Bei Kryptowährungen, wie Bitcoin, werden Transaktionen gespeichert. Fortschrittlicheren Kryptowährungen, wie Ethereum, können zudem Code speichern und ausführen. Die Blöcke enthalten außerdem weitere Metadaten und werden mithilfe kryptografischer Verfahren verkettet (vgl. Yaga et al. 2018, iv–v)

Bis zu diesem Zeitpunkt wäre eine Datenbank, die sich von allen Teilnehmern andauernd repliziert, eine mögliche Alternative. Die eigentliche Innovation ist der Einsatz eines Konsensmechanismus für die Unterbindung von Manipulationsversuchen. Alle Mitglieder des Netzwerkes bilden einen Konsens für neu erstellte Blöcke (s. Kapitel 2.4.5).

Oftmals wird Blockchain mit dem Begriff „Distributed Ledger“ (DL) gleichgesetzt, jedoch verwendet nicht jede DL eine Verkettung von Blöcken (vgl. van de Velde et al. 2016, 5). Die Blockchain ist eine Sonderform der Distributed Ledger Technolgy (DLT). Ein DL ist übersetzt ein „verteiltes Kontenbuch“ und hat im Vergleich zum „Centralised Ledger“ (CL) keine zentrale Institution. Es ist ein dezentrales Netzwerk, das von allen Teilnehmern bearbeitet und eingesehen werden kann (vgl. Yaga et al. 2018, 1).

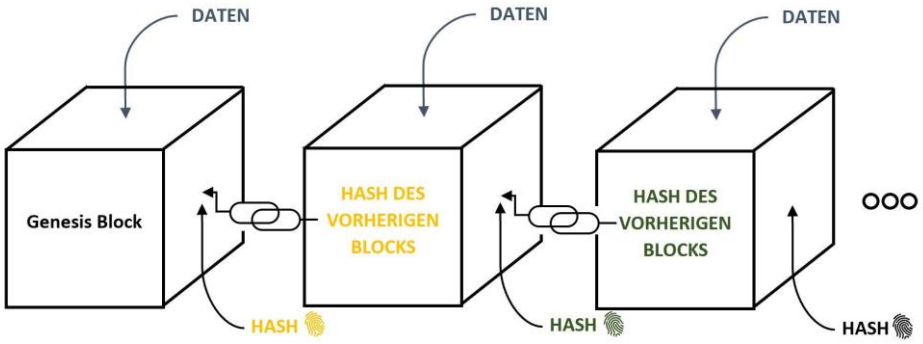

Abbildung 3: Visualisierung einer Blockchain (vgl. Döring 2019)

Blockchains werden auch als „Zustandsmaschinen“ beschrieben. Dies bedeutet, dass sie einen bestimmten Programmzustand und zukünftige Zustände beibehält, die auf dieser Maschine erlaubt sind. Diese Zustandsmaschinen werden mit einem Genesis-

Zustand instanziiert und haben Regeln (Konsensus), die definieren, wie dieser Zustand übergehen kann (vgl. Kasireddy 2022).

Es gibt verschiedene Typen von Blockchains, die sich in einigen Punkten unterscheiden. Der bekannteste Typ ist die öffentliche Blockchain. Sie ist, wie der Name suggeriert, offen und für jeden zugänglich. Ethereum und Bitcoin sind öffentliche Blockchains (vgl. Bashir 2017, 64)

2.4.3 Aufbau einer öffentlichen Blockchain

Eine öffentliche Blockchain hat in ihrer Architektur bestimmte Kerncharakteristiken (s. Abb. 4).

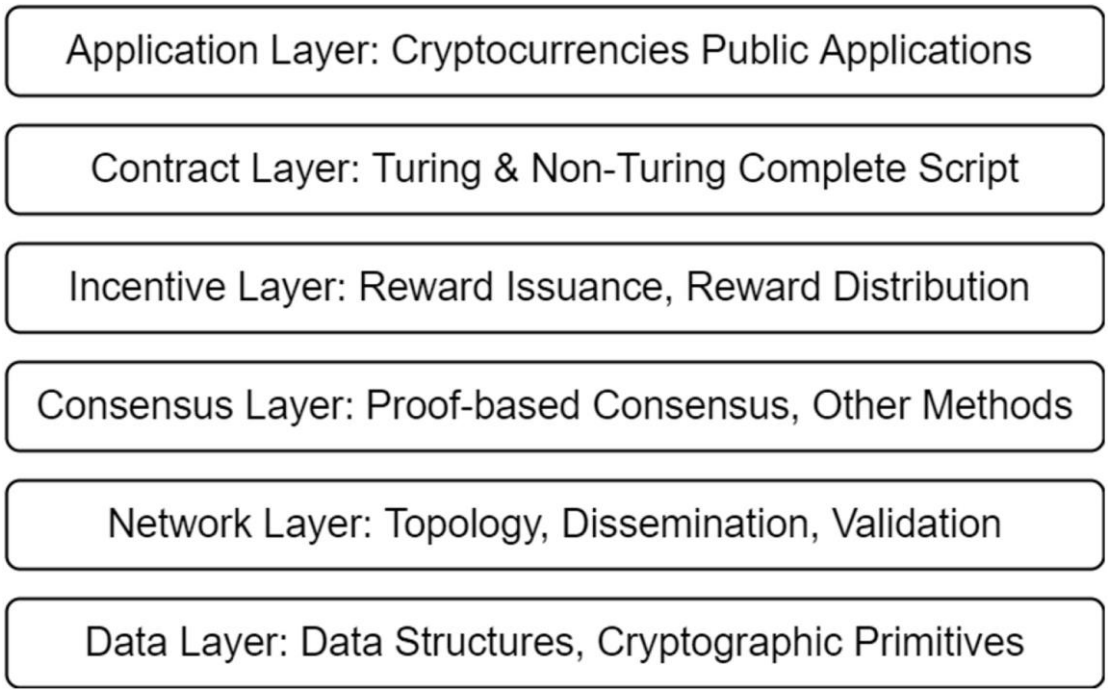

Abbildung 4: geschichtete Ansicht der Architektur einer öffentlichen Blockchain (vgl. Sai et al. 2021, 5)

Es beginnt mit der Speicherung der Daten in Datenstrukturen (Data Layer), welche durch die Netzwerkschicht an weitere Peers gesendet werden können (Network Layer). Nachdem ein Zustand geändert wurde, müssen die Teilnehmer des Netzwerkes mehrheitlich mithilfe eines Konsensmechanismus zustimmen

(Consensus Layer). Gutartiges Handeln wird durch Incentives, der Ausschüttung des jeweiligen Tokens der Blockchain, geschützt (Incentive Layer). Diese Operationen werden durch die Ausführung von Rechenskripten durchgeführt (Contract Layer). Die Basisoperationen können mithilfe von DApps erweitert werden (Application Layer) (vgl. Sai et al. 2021, 4–5).

2.4.4 Charakteristiken und Einschränkungen einer Blockchain

Zusammenfassend gibt es folgende Hauptcharakteristiken:

- *Dezentralität*. Transaktionen können via Peer-to-peer ohne eine zentrale Autorität ausgeführt werden. Es reduziert dadurch Serverkosten und umgeht „perfomance bottlenecks at the central server“ (Zheng et al. 2018, 357)

- *Persistenz.* Es ist fast unmöglich die Daten zu manipulieren, da jeder neue Block und dessen Transaktionen von den anderen Knoten validiert werden müssen (vgl. Zheng et al. 2018, 357)

- *Anonymität.* Jede Blockchain hat einen gewissen Grad der Anonymität, da keine persönlichen Daten für die Generierung einer Adresse nötig sind. Es gibt keine zentrale Entität, die private Daten speichert und nutzt (vgl. Zheng et al. 2018, 357).

- *Transparenz.* Jede validierte Transaktion hat einen Zeitstempel und Referenzen auf ältere Transaktionen. Jeder kann vergangene Transaktionen verfolgen (vgl. Zheng et al. 2018, 357)

Die Blockchain-Technologie hat jedoch auch einige Limitationen, an denen zurzeit gearbeitet wird. Unter anderem Skalierbarkeit, Anpassungsfähigkeit, Komplexität, Regulierungen und Kinderkrankheiten einer noch unausgereiften Technologie (vgl. Bashir 2017, 86). Diese Probleme und Herausforderungen finden sich auch in dem auf Blockchain-basierten Web3.

2.4.5 Konsensusmechanismen

„Consensus is a process of agreement between distrusting nodes on a final state of data" (Bashir 2017, 48). Bei einer Standard-Client-Server Architektur ist es unkompliziert sich zu einigen. Wenn mehrere Knoten einen Konsens finden müssen, gibt es Konsensmechanismen bzw. Algorithmen, die bestimmen, wie sich geeinigt wird.

Die beiden berühmtesten Konsensmechanismen sind Proof of Work (PoW) und Proof of Stake (PoS). PoW wurde bekannt durch Satoshi Nakamato, dem Ersteller von Bitcoin. Diese Art von Konsensmechanismus sorgt dafür, dass Blockchain-Teilnehmer Belohnungen bekommen (den Token der Blockchain, z. B. Bitcoin), wenn sie eine Transaktion durch das Lösen von kryptografischen Puzzles validieren und neue Blöcke erzeugen. Im Netzwerk müssen sogenannte Miner konkurrieren, um Blöcke an der Blockchain anzuhängen. Jeder Miner hat eine Erfolgswahrscheinlichkeit, die proportional zum verwendeten Rechenaufwand ist (vgl. Nakamoto 2008, 3).

Es gibt jedoch starke Kritik an diesem Verfahren. PoW ist vom Design her ausgesprochen rechenaufwendig und es entsteht dadurch ein Hardware-Wettrüsten. Das Mining von Bitcoin verursacht ~125 Terrawattstunden Strom pro Jahr. Das entspricht 0,59 % des Stromverbrauchs der Welt (vgl. Bocksch 2022). Eine Blockchain, die PoW benutzt, kann außerdem mit genug Rechenpower (51 %) angegriffen werden (vgl. Yaga et al. 2018, 25).

PoS ist eine von vielen Alternativen zu PoW. Blockchain-Teilnehmer sind sogenannte „Validators", die eine bestimmte Menge des Tokens der jeweiligen Blockchain mithilfe von Smart Contracts sperren. Im Gegenzug bekommen die Teilnehmer eine Chance, neue Transaktionen zu validieren und damit eine Belohnung zu bekommen. Diese Methode wird „staking" genannt. Der Validator wird bestraft, falls falsche Daten validiert werden und kann einige oder alle gesperrte Token verlieren. Je mehr ein Nutzer sperrt, desto höher ist die Chance für die Erstellung des nächsten Blocks auserwählt zu werden (vgl. Antonopoulos und Wood 2019, 577). PoS eliminiert die stromintensiven Rechnungen und ist damit klimafreundlicher. Es gibt dabei die Kritik,

dass die Vermögenden sich hier leichter Macht erkaufen und das Netzwerk mit 51 % Anteil dominieren könnten. Dies ist in den meisten Fällen jedoch äußerst kostspielig und kann durch Varianten von PoS z. T. verhindert werden (vgl. Yaga et al. 2018, 22–23).

2.4.6 Ethereum

Ethereum ist eine dezentrale, open-source Blockchain, die im Jahre 2013 vom Programmierer Vitalik Buterin konzipiert wurde. Die Idee war es, die Mängel von Bitcoin zu beheben. Diese neue Art von Blockchain machte es möglich, Programmiercode in Form von sogenannten „Smart Contracts“ auf einer Blockchain zu speichern. Diese werden ausgelöst, sobald die angegebenen Konditionen eintreffen. Dies ermöglicht es unter anderem, dass zwei Parteien ohne Vertrauen eine Vereinbarung treffen können, ohne jeglichen Mittelmann oder Zeitverlust (vgl. Frankenfield 2016).

Angetrieben wird dies durch die Ethereum Virtual Machine (EVM). Es ist eine Art dezentraler globaler Computer, der Millionen von ausführbaren Objekten beinhaltet. EVM ist „quasi“-Turing-Vollständing; „quasi“, weil die Ausführung des Prozesses davon abhängt, ob genug Ether für die Gebühren da sind (vgl. Antonopoulos und Wood 2019, 543).

Ethereum verwendet PoW als Konsensmechanismus, arbeitet jedoch daraufhin, auf PoS zu wechseln. Das Netzwerk leidet nämlich unter dem Vorwurf der Energieverschwendung und einer schlechten Skalierbarkeit. Eine Ethereum TransaktionEthereum-Transaktion verbraucht so viel Energie, wie der Verbrauch eines durchschnittlichen US-Haushaltes in einer Woche. Diese Probleme sollen laut dem Gründer Vitalik Buterin mit Ethereum 2.0 und das Wechseln auf PoS behoben sein (vgl. Bybit Learn 2022).

Buterin ist eine Schlüsselfigur in der heutigen (Stand 2022) Web3 Entwicklung und entwickelte Ethereum unter anderem auch, um die Erstellung von dezentralen Applikationen (DApp) zu vereinheitlichen. Ethereum 1.0 ähnelt dem Prinzip des Apple App-Stores, ein Anbieter für unendlich viele Applikationen, die den gleichen

Basisregeln folgen. Regeln, die im Netzwerk von Ethereum fest codiert sind. Ein Entwickler kann darauf aufbauend seine eigenen Regeln in einer DApp aufstellen. Jedoch gibt es keine zentrale Autorität wie beim Apple Store und die Macht geht zurück an die Gesellschaft (vgl. cointelegraph 2021).

2.4.6.1 Ethereum-Governance

Es gibt viele verschiedene Parteien in der Ethereum-Community, die ein Mitspracherecht im Governance-Prozess haben (vgl. ethereum.org 2022, Governance):

- *Protokollentwickler* („Core Developer“): Entwickler, welche Ethereum-Implementierungen pflegen (z. B. go-ethereum Repository).
- *Miner/Validator:* Personen, die Knoten des Netzwerkes betreiben und neue Blöcke zur Ethereum-Blockchain hinzufügen.
- *EIP-Autoren*: Personen, die an Veränderung des Ethereum-Protokolls arbeiten und Verbesserungen vorschlagen.
- *Anwendungs-/Tool-Entwickler*: Entwickler, die Anwendungen auf der Ethereum-Blockchain erstellen oder Tools wie Wallets.
- Anwendungsbenutzer: Personen, die mit den jeweiligen Anwendungen interagieren.
- *Ether-Halter:* Personen, die Ether besitzen.

2016 gründeten die Nutzer des Ethereum-Netzwerkes eine Dezentrale Autonome Organisation (DAO). Eine DAO macht es möglich, demokratisch Veränderungen am Netzwerk zu bestimmen. So eine Organisation ist mithilfe von Smart Contracts codiert. Dies erschien eine neue und revolutionierende Entwicklung zu sein, wurde jedoch schnell ausgenutzt. Ein Sicherheits-Exploit machte es möglich, dass ein Hacker über 3.6M Ether stahl. Daraufhin hatte das Ethereum-Netzwerk einen sogenannten „harten fork“ (Kettenspaltung), ein Softwareupdate, das sich vom alten komprimierten Netzwerk löste und ein neues erstellte. Das alte Netzwerk ist heute als Ethereum Classic bekannt, mit dem Token ETC (vgl. Antonopoulos und Wood 2019, 339). Es kam außerdem zum Vorschein, dass die Wahlbeteiligung äußerst niedrig ist, die

meisten Nutzer davon nichts wussten und nur Ether-Halter ein Abstimmungsrecht hatten. Infolgedessen hat die Community beschlossen, nicht mehr diesen Weg der Einmischung zu gehen (vgl. ethereum.org 2022, Governance).

Die Weiterentwicklung des Ethereum-Protokolls findet heute über sogenannte Ethereum-Verbesserungsvorschläge (EIP) statt. EIPs sind Standards für neue Funktionen und Prozesse, wie der EIP-20 Vorschlag für die Standardisierung zur Erstellung von Tokens (mehr zum Thema Tokens in Kapitel 2.6.3). Als OpenSource-Projekt, kann jeder einen EIP Vorschlag machen (vgl. ethereum.org 2022, Governance).

Dieser Vorschlag wird größenteils informell in Foren diskutiert, bis es zu einem offiziellen „All Core Devs-Call“ kommt und der Vorschlag diskutiert wird. „All Core Devs“ ist ein digitales Treffen aller relevanten Protokollentwickler, Core-Ethereum Forscher und Client-Entwickler, sowie Gastauftritte von Experten in einem bestimmten relevanten Bereich. Dieses Meeting bestimmt den CFI („Consider for Inclusion“) Status eines EIP. Hat ein EIP die Interessenvertreter überzeugt, gibt es wiederholte Anpassungen für die Sicherheit und Funktionalität des EIP, bis alle einen Kompromiss getroffen haben. Daraufhin wird es auf einem Test-Netzwerk getestet und anschließend auf das Mainnet (Hauptnetzwerk) gespielt (vgl. ethereum GitHub 2022, network-upgrades).

2.4.7 Smart Contracts

Ein Smart Contract ist ein digitales Protokoll, das die Bedingungen eines Vertrages ausführt. Sie müssen deterministisch sein, denn sie werden von den Knoten der Blockchain ausgeführt, sobald alle Teilnehmer das gleiche Ergebnis haben. Es sorgt für Transparenz und Vertrauen zwischen unbekannten Geschäftspartnern (vgl. Yaga et al. 2018, 32–33).

Codiert werden Smart Contracts in verschiedenen alten und neuen Programmiersprachen. Solidity ist dabei der klare Spitzenreiter und wird hauptsächlich für die Ethereum-Blockchain verwendet. Siehe

für ein Beispiel mit Erläuterung. Es ähnelt JavaScript und hat verschiedene Funktionen wie Vererbung, Bibliotheken und Datentypen. JavaScript oder C# können ebenfalls für verschiedene Blockchains verwendet werden. Für Ethereum wird jedoch Solidity empfohlen, um die Korrektheit und Vollständigkeit zu garantieren (vgl. Wayner 2019). Der Prototyp dieser Arbeit wird das Ethereum-Netzwerk und die Solidity-Programmiersprache nutzen.

Jede Transaktion hat Gebühren, das sogenanntes „Gas“. Während die EVM eine Transaktion ausführt, wird das Gas nach bestimmten Regeln schrittweise aufgebraucht. Wenn das Gas eines Nutzers ab irgendeinem Punkt erschöpft ist, wird die Ausführung beendet und alle Zustände auf den alten Stand zurückgerollt. Der Preis entsteht aus Angebot und Nachfrage. Miners können Transaktionen ablehnen und konzentrieren sich auf die hohen Angebote. Nutzer zahlen somit dafür, ein Teil des nächsten validierten Blocks zu sein (vgl. ethereum GitHub 2022, docs.solidity.org). Dies kann in Zeiten von hoher Netzwerklast zu exorbitanten Gebühren führen. Am 01. Mai 2022 gab es eine groß erwartete Auktion von digitalen Immobilien (mehr zum Thema NFTs im Kapitel 2.6.3), was dazu führte, dass Gebühren im Wert von $181M verschwendet wurden. Ein anonymer Käufer musste für einen digitalen Gegenstand im Wert von $5,800 Gebühren im Wert von $45,000 zahlen. Es stellte sich außerdem heraus, dass die für die Auktion verwendeten Smart Contracts nicht optimiert waren. Die Transaktionen waren von Natur aus, zusätzlich zu dem Ansturm auf das Netzwerk, ineffizient und teuer (vgl. Nover 2022).

2.5 Web3

Das vorangegangene Kapitel ist ein oberflächlicher Einblick in die Blockchain-Technologie und spezifischer Ethereum. Ein tiefgründigerer Blick ist für das

Verständnis dieser Thesis ist nicht notwendig. Detailreicheres Wissen über die Technologie gibt es in den verwendeten Hauptquellen (vgl. Bashir 2017; Lantz und Cawrey 2020; Fill und Meier 2020; Meinel und Gayvoronskaya 2020; Yaga et al. 2018; Zheng et al. 2018).

In diesem Kapitel geht es um das Web3, ihr Aufbau, deren Versprechen und Kritik.

2.5.1 Web3 Architektur

Eine einheitliche Definition über den Aufbau von Web3 ist noch nicht vorhanden. Es lässt sich jedoch ein grobes Bild verfassen. Web3 existiert zurzeit neben Web2 und bietet eine Alternative zu den klassischen Web2-Webseiten. Diese Alternative sind DApps. Web3 ist die Menge aller DApps und dessen Tools. Fundamental ändert sich nichts am Internet, nur die Art, wie es genutzt wird.

Es müssen jedoch neue technologische Lösungen entwickelt werden, um alle Schichten vom Web2 zu dezentralisieren. Das Fundament bilden die Peer-to-Peer-Protokolle und plattformneutrale Berechnungsbeschreibungssprachen (z.B. EVM von Ethereum). Es müssen jedoch ebenfalls Scaling-Lösungen geschaffen werden, dezentrale Datenspeicherungen und Entwickler-Tools. Diese Tools müssen Daten außerhalb der Blockchain erfassen, sichere und dezentrale Kommunikation ermöglichen, sowie Testumgebungen und DApp-Entwicklung bereitstellen (vgl. Web3 Foundation o. J.).

Fundamental haben die meisten Blockchain-Netzwerke ähnliche Ziele. Sie wollen mithilfe von Blockchain-Technologien ein dezentrales Web erschaffen. Mit demokratischen Organisationen und einer Token-Ökonomie. Außerdem soll Web3 mehr nutzerorientiert sein und eine „zero-server architecture“ anstreben (vgl. Bambacht und Pouwelse 2022, 1).

2.5.2 Aufbau einer Web3 Anwendung

Web3-Applikationen (DApps) sind im Wesentlichen komplexer als Web2-Anwendungen. Eine Zusammenfassung der meisten Web2-Anwendungen (s. Abb. 5) lässt sich in drei Teile aufteilen: Datenspeicher, Back-End Code und Front-End Code.

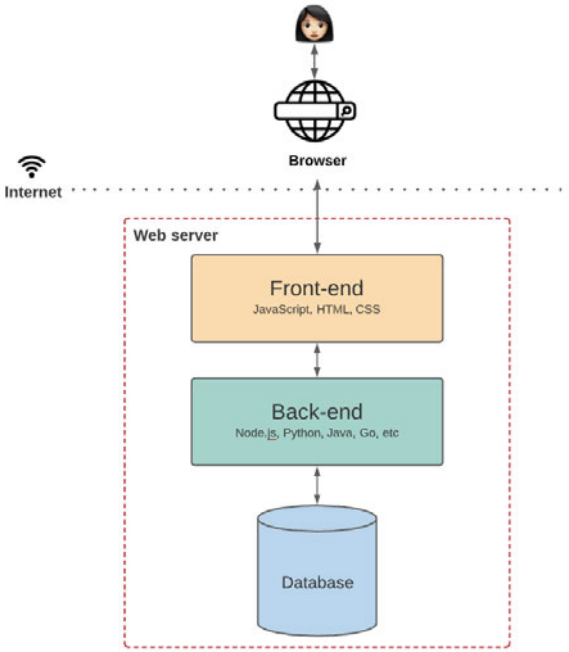

Abbildung 5: Eine Standard Web2-Anwendung (Kasireddy 2022)

Der Code einer Web2-Anwendung ist auf zentralen Servern gespeichert und erreicht den Nutzer über das Internet. Es wird mit dem Front-End interagiert, das mit dem Back-End kommuniziert, welches wiederum mit der Datenbank verknüpft ist (vgl. Kasireddy 2022).

Web3-Anwendungen nutzen jedoch Blockchains und haben keine zentrale Datenbank (s. Abb. 6). Die Architektur einer typischen Ethereum Anwendung könnte so aussehen:

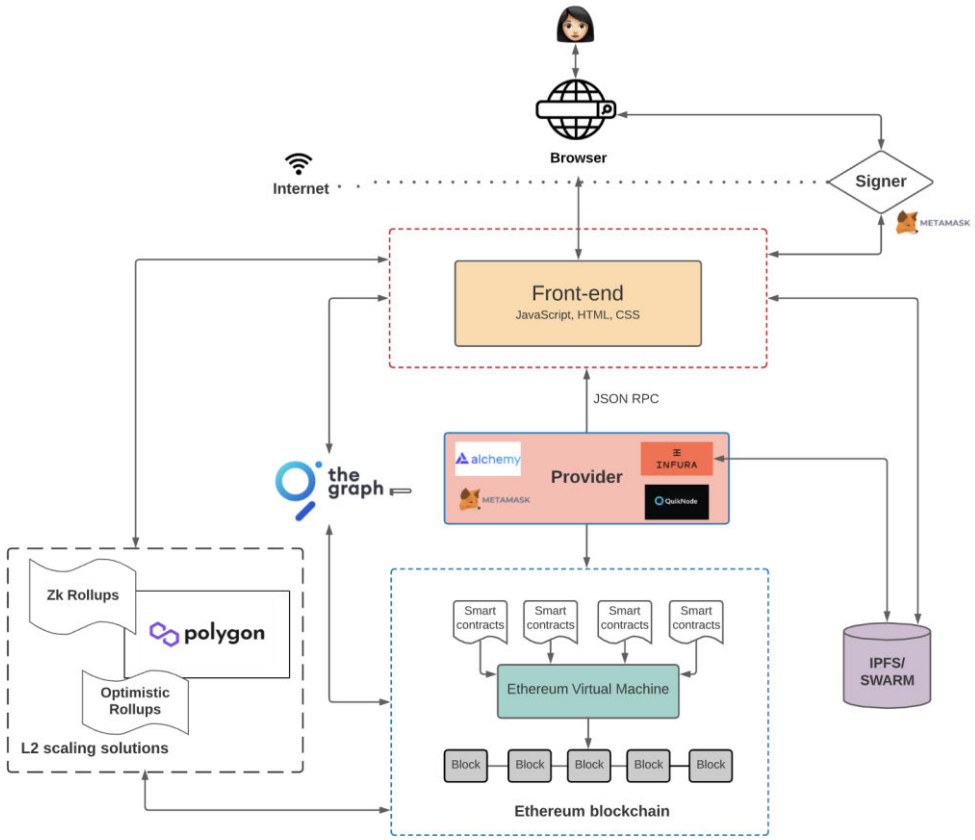

Abbildung 6: Architektur einer möglichen Ethereum DApp (vgl. Kasireddy 2022)

Das Back-End ist in diesem Fall durch die Ethereum Blockchain ersetzt worden. Das Front-End ist unverändert und wird weiterhin mit HTML, CSS und JavaScript programmiert und designt.

Um mit Daten auf der Blockchain zu interagieren, muss mit einem der Knoten interagiert werden. Dies liegt daran, dass jeder Knoten eine Anforderung für eine auf der EVM auszuführende Transaktion senden kann. Ein Miner wird dann die Transaktion ausführen und die resultierende Zustandsänderung an den Rest des Netzwerks weitergeben.

Dafür gibt es zwei Wege:

1. Einen eigenen Knoten aufstellen, auf welcher die Ethereum-Blockchain läuft
2. Die Knoten von Providern benutzen (Alchemy, Infura, etc.)

Einen eigenen Knoten aufzusetzen kann Tage dauern und benötigt die Synchronisation von vielen Daten. Es steigen außerdem die Kosten der Datenspeicherung, je größer die DApp wird. Es werden weitere Knoten benötigt und der Einsatz von DevOps Ingenieuren wird vorteilhaft, um die Infrastruktur am Laufen zu halten. Daher verwenden viele Entwickler Provider, um die Infrastruktur zu verwalten. Jedoch entsteht dadurch „a centralized chokepoint“ (Kasireddy 2022).

Sobald die Blockchain angebunden ist, kann der Zustand gelesen werden. Um jedoch auf den Zustand zu schreiben, muss eine Transaktion mit dem eigenen privaten Schlüssel signiert werden. Nur dann kann eine Transaktion auf die Blockchain akzeptiert werden. Dafür wird hauptsächlich „MetaMask“ verwendet, eine Browsererweiterung, die den privaten Schlüssel eines Nutzers speichert und das Signieren von Transaktionen im Browser ermöglicht (vgl. Kasireddy 2022).

Die Speicherung der Daten auf der Blockchain kann schnell teuer werden. Der Nutzer bezahlt jedes Mal Gas, um neue Daten auf der Blockchain zu speichern. Um diese Unannehmlichkeit zu verhindern, kommt ein verteiltes Datenverteilungsprotokoll zum Einsatz (z.B. IPFS oder Swarm).

In Web2 sind Daten auf zentralen Servern gespeichert und im Falle eines Ausfalls nicht mehr erreichbar. Durch das „Location based addressing“ Prinzip wird dem Computer mitgeteilt, wo eine Datei zu finden ist (IP-Adresse oder Domainname im Internet). Dies soll sich in Web3 mithilfe von z. B. InterPlanetary File System (IPFS) zum „Content based addressing“ ändern (vgl. Benet 2014, 6). Dabei werden Dateien anhand ihres Inhalts gesucht.

IPFS speichert Daten auf einem Peer-to-Peer-Netzwerk. Provider wie Infura bieten ebenfalls einen IPFS Knoten an. Es wird außerdem mithilfe der Kryptowährung „Filecoin“ ein Anreiz geschaffen, dass Knoten überall in der Welt Daten speichern und herausgeben. Genaueres zu dem Thema Anreize und Token-Ökonomie gibt es im Kapitel 2.6.3.

Um die Daten der Smart Contracts zu lesen und auszuwerten, gibt es zurzeit zwei Möglichkeiten:

1. *Smart Contract Events*

   Es gibt Bibliotheken bei Web3.js (Ethereum JavaScript API), die es ermöglichen, auf Smart Contract Ereignisse zu hören und daraufhin eine bestimmte Aktion auszuführen. Diese Methode hat jedoch Limitationen und im Falle von vergessenen Ereignissen kann ein Smart Contract nicht bearbeitet werden (vgl. Kasireddy 2022).

2. *The Graph*

   The Graph ist ein dezentralisiertes Protokoll zum Indizieren und Abfragen von Daten aus Blockchains. So wie Google das Web indiziert, indiziert The Graph Blockchain-Daten von Netzwerken wie Ethereum und Filecoin. Diese Daten werden in offenen APIs gruppiert, die als Subgraphen bezeichnet werden und von jedem abgefragt werden können (vgl. Tal et al. 2018, 2).

Die Skalierung von Blockchain-Netzwerken ist zurzeit beschränkt. Das Ethereum-Netzwerk selbst hat keine Möglichkeiten zu skalieren. Dafür sind sogenannte „L2 scaling solutions“ vorhanden. Beim Ethereum-Netzwerk wird dieses Prinzip „Sidechains“ genannt. Hier können separate Blockchains parallel zum Mainnet von Ethereum laufen und unabhängig agieren. Die Sidechains basieren auf der EVM und sind Teil von Ethereum (vgl. ethereum.org 2021, Sidechains).

Um hohe Gebühren und volle Blöcke zu vermeiden, kann zum Beispiel Polygon eingesetzt werden. Polygon hat Sidechains, die Transaktionen ausführen können. Sie dient als zweitrangige Blockchain, die mit der Haupt-Blockchain verbunden ist. Von Zeit zu Zeit sendet die Sidechain eine Aggregation ihrer letzten Blöcke zurück an die Haupt-Blockchain (vgl. Kasireddy 2022).

Am Ende entsteht eine DApp mit allen gewünschten Funktionen (s. Abb. 6). Das Zusammenführen all dieser Elemente ist komplexer als bei Web2 Anwendungen und Entwickler-Frameworks sind ein bedeutender Bestandteil heutiger Web3 Entwickler.

2.6 Versprechen und Kritik an Web3

2.6.1 Von einer Datenmonarchie zur Datendemokratie

Web3 verspricht Dezentralität und die Macht an den Nutzer zurückzugeben. Das Ziel ist die komplette Dezentralität der Plattformen, Server und Inhalte. Das Internet ist heute auf der Logik von eigenständigen Computern gebaut, in welcher Daten zentral gespeichert und verarbeitet werden. Jedes Mal, wenn ein Service in Web2 genutzt wird, werden Datenpakete an den zentralen Server gesendet und der Nutzer verliert das Eigentum über seine Daten. Dies ist unter anderem eine Verletzung der Datenprivatsphäre und führt zu Problemen im Back-End von z. B. E-Commerce Operationen oder entlang der Lieferkette. Da das Datenmanagement dieser Back-End-Prozesse umständlich, teuer und ineffizient ist (vgl. Voshmgir 2018).

Blockchain verspricht eine transparente Lösung mit Einhaltung der Privatsphäre durch Kryptografie. Es hat außerdem das Prinzip einer Anreizökonomie ins Leben gerufen, die Akteure wirtschaftlich dafür belohnt, sich korrekt zu verhalten. Denn das Blockchain-Netzwerk nimmt an, dass jeder potenziell korrupt ist. Um die Netzwerksicherheit zu gewährleisten, wird der Token des Netzwerks verwertet, um die Akteure zu bezahlen (vgl. Voshmgir 2018).

Andere Experten sehen zentralisierte Plattformen jedoch als ein Teil einer „matured Web3.0 era“ (Zhuotao et al. 2021, 3). Sie kompensieren Funktionalitäten, die schwierig oder unmöglich auf der Blockchain auszuführen sind. Diese zentralen Plattformen sollten jedoch folgende Charakteristiken haben, um Teil von Web3 sein zu können: „(i) (…) verifiable proof to certify the correctness of the state (…), and (ii) all published state should have the concept of finality (..)“ (Zhuotao et al. 2021, 3).

2.6.2 Governance

Die Gesellschaft ist heutzutage in traditionellen top-down Organisationen aufgeteilt. Es gibt eine legale Entität, die irgendwo registriert ist. Das gibt den Menschen die Möglichkeit, diese Organisation im Falle eines ungeklärten Problems zu verklagen.

Die Beziehung zu diesen Organisationen ist definiert durch Verträge. Dies geschieht, da es grundsätzlich kein Vertrauen zwischen den beiden Entitäten gibt. Im Falle einer Verletzung dieses Vertrages gibt es den Akteuren die Möglichkeit dies vor einem Gericht zu bringen. Gleiches gilt für Beziehungen zwischen Organisationen und Ländern (vgl. Voshmgir 2018).

Die Blockchain-Technologie verspricht diese traditionellen top-down Organisationen mithilfe von DAOs zu verbessern.

2.6.2.1 Dezentrale Autonome Organisation (DAO)

In der akademischen Literatur gibt es mehrere Anläufe zur spezifischen Definition von DAOs. Da diese Bachelorarbeit keinen großen Fokus auf DAOs legt, gibt es eine ausführliche Charakterisierung in Anhang 1.1: Dezentrale Autonome Organisation (DAO). Buterin beschreibt DAOs im Ethereum Whitepaper als eine “virtual entity that has a certain set of members or shareholders which [...] have the right to spend the entity's funds and modify its code” (Buterin 2014).

2.6.3 Token-Ökonomie

Es gibt grundlegend zwei Arten von Tokens, „Fungible“ und „Non-Fungible“ Tokens. Eine neue Art von „Semi-Fungible“ kann den Status von fungible zu non-fungible ändern (s. Abb. 7)

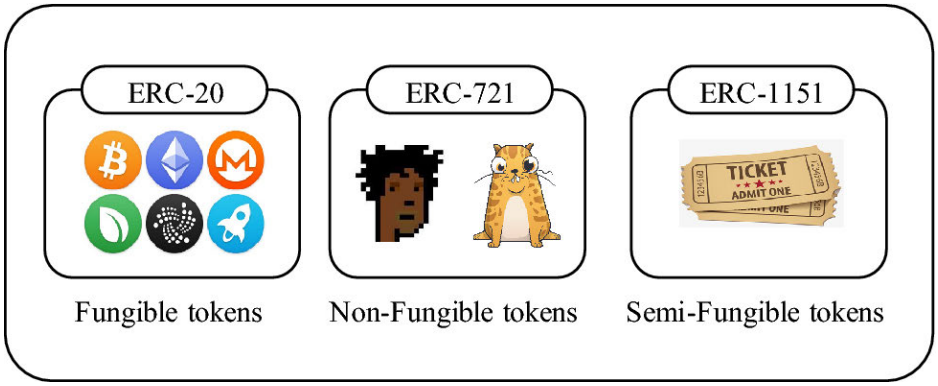

Abbildung 7: Von links nach rechts (fungible, non-fungible, semi-fungible) (vgl. Bamakan et al. 2022, 3)

Fungible Tokens sind austauschbar und nicht eindeutig. Währungen wie Bitcoin, Ethereum oder der Euro sind fungible. Ein Bitcoin ist ein Bitcoin wert, egal wo es ausgegeben wurde. Hierfür wird der ERC-20 Token Standard für auf Ethereum basierte Tokens genutzt (vgl. ethereum.org 2015, introduction-to-smart-contracts).

Non-Fungible Tokens (NFTs) sind hingegen digitale Vermögenswerte mit eindeutiger Kennung. NFTs ermöglichen es, dass der Besitzer sein digitales Eigentum verifizieren kann. Sie können außerdem ein Objekt in der echten Welt digital repräsentieren (vgl. Bamakan et al. 2022, 1).

Semi-Fungible Tokens sind in derselben Klasse oder zu einem bestimmten Zeitpunkt fungible und in anderen Klassen oder unterschiedlichen Zeiten non-fungible. Dies ist sinnvoll bei z. B. Konzerttickets. Das Ticket kann vor dem Konzert noch mit anderen Tickets getauscht werden oder verkauft werden. Sobald das Konzert endet, wird aus dem fungible Token ein NFT. Es kann damit nicht mehr gegen ein neues Konzertticket getauscht werden und existiert als Sammlerstück weiter (vgl. Bamakan et al. 2022, 3).

Tokens sind der Treiber für ein funktionierendes Web3 und geben wirtschaftliche Anreize, die Blockchain-Netzwerke zu verwalten. Sie geben zudem die Möglichkeit in DAOs demokratisch mitzuwirken (vgl. Voshmgir 2018).

2.6.4 Kritik an Web3

Web3 wird scharf kritisiert und argumentiert unter anderem mit den folgenden Punkten:

Das Dilemma der Dezentralität

Web3 verspricht, die Macht an die Menschen zurückzugeben. Jedoch dominieren zentrale Dienste den Markt. Jack Dorsey, ehemaliger CEO von Twitter, beschreibt Web3 als „ultimately a centralized entity with a different label.“ (Dorsey 2021).

Wie in Kapitel 2.5.2 erwähnt, benötigen DApps eine Verbindung zum Blockchain-Netzwerk. Jedoch verwenden fast alle DApps Provider, wie Infura oder Alchemy. Solche Dienste verkaufen den API-Zugriff und geben ohne eine Verifizierung auf

Anfragen der DApp einen einfach JSON-Blob mit dem Output zurück. Fast alle Clients vertrauen auf solche Provider und der Aufwand mit Konsensmechanismen scheinen obsolet (vgl. Marlinspike 2022).

Diese Entwicklung lässt sich auf den Grund für Zentralität in Web2 zurückführen: „People don't want to run their own servers, and never will." (vgl. Marlinspike 2022). Selbst Unternehmen outsourcen ihre Server. Dasselbe passiert zurzeit mit Web3.

Z. B. ist der größte NFT Onlinemarkt für digitale Kunst (OpenSea) und die größten Marktplätze für Kryptowährungen zentralisiert (Binance, Coinbase, …). Viele sehen dies jedoch nicht als Hauptaufgabe von Web3. Chris Dixon, ein Web3 Entrepreneur, sieht in solchen zentralisierten Diensten keine Schwäche von Web3. Er sieht die Hauptaufgabe in der Dezentralisierung von Netzwerken.

OpenSea blockiert Berichten zufolge iranische Benutzer von seiner Plattform. Mehrere NFT-Künstler haben auf Twitter bekannt gegeben, dass sie nicht auf ihre Konten zugreifen konnten. MetaMask blockierte ebenfalls iranische und venezuelische Nutzer aufgrund von „rechtlichen Rahmenbedingungen". Zentrale Dienste verbannen Anwender vom angeblichen dezentralen Web3, das Web, das die Macht an den Nutzer zurückgeben soll (vgl. Butler 2022).

Energieverbrauch

Die Branche hat durch den hohen Energieverbrauch von Bitcoin ein schlechtes Image und dasselbe gilt für Ethereum. Eine Ethereum-Transaktion verbraucht ~240 kWh. Im Vergleich dazu verbrauchen 100.000 VISA Transaktionen ~150 kWh (vgl. Statista 2022). Wie in vorherigen Kapiteln erwähnt, plant Ethereum ein Umsteigen auf Proof-of-Stake und damit eine drastische Verringerung des Carbon Footprint. In Zeiten von Klimapolitik fordern erste Europapolitiker das Verbot von Kryptowährungen und China hat das Bitcoin-Mining schon komplett verboten. Viele Länder gehen das Thema jedoch noch nicht an. „Wahrscheinlich ist vielen das Thema zu neu oder zu kompliziert", sagte Jean-Pierre Schweitzer vom europäischen Umweltbüro EEB (vgl. Herwartz und Steuer 2022).

Auto-enforceable code

Mit Blockchains und Smart Contracts, ist es fast unmöglich eine Transaktion rückgängig zu machen. Smart Contracts werden von Menschen geschrieben und Statistiken zeigen, dass Programmcodes eine große Anzahl von Fehler enthalten. Eine Schätzung gibt eine durchschnittliche Anzahl von 1-25 Fehlern pro 1000 Zeilen Code an (vgl. McConnell 2004, 521).

Fehler in Smart Contracts führten z. B. im Januar 2020 dazu, dass ein Hacker $320 Millionen aus der Verbindung der Blockchain Solana und dem Wormhole-Netzwerk stahl. Im Oktober 2021 erlaubte ein Bug das Erstellen und Senden von COMP, den Token von Compound (ein algorithmisches, autonomes Zinsprotokoll), an zufällige Adressen. Nachdem $80 Millionen an falsche Personen gesendet wurde, musste eine Behebung des Problems erst von den Nutzern des Netzwerks über ein Governance-Vorschlag bestätigt werden. Dies dauerte eine Woche und der Bug sorgte für weitere Verluste von $68 Millionen. Die dezentrale Struktur von Compound sorgte für eine langsame Verarbeitung und Bürokratie während einer Krise (vgl. Genç und Graves 2022).

“Smart contracts need testable evidence that they do what you intend, and only what you intend. That means defined security properties and techniques employed to evaluate them.” – Dan Guido, Experte in Smart Contract Sicherheit.

Ende der Anonymität

Kritik wird laut, dass Web3 nicht so verschieden zum Web2 ist in Bezug auf die Datenprivatsphäre. Infura ist das neue Amazon und Alchemy das neue Facebook. Die zuvor genannten Provider sammeln zwar keine Namen, Geburtstage oder Kreditkarten, jedoch speichern sie IP-Adressen und Geolokalisierungen. Es gibt denen die Macht, Benutzer aus dem Netzwerk zu verbannen. „Web3 would fall back to the same old crusty behaviors of Web2 companies (censorship, rent-seeking business models, data collection, unilateral control)” (particl.news 2022).

Außerdem laufen knapp 66 % der Ethereum Knoten auf Cloud Server und davon 2/3 mit AWS. Während andere Knoten ebenfalls auf Anbieter von Web2 Giganten laufen (s. Kapitel 5.1.1).

Ein weiteres Problem ist der vollständige Mangel an finanzieller Privatsphäre. Alle Transaktionen dezentraler Finanzapplikationen sind standardgemäß öffentlich auf der Blockchain. Sobald jemand deine kryptografische Adresse kennt, sind alle vergangenen und zukünftige Transaktionen für immer zuordbar. Ein Beispiel: Du kaufst ein Haus mit Kryptowährung und erhältst zusätzlich noch die rechtlichen Dokumente als NFT auf deine, von der Regierung verifizierten, Ethereum Adresse. Der Verkäufer des Hauses kann nun jedoch all deine Transaktionen auf dem Ethereum-Netzwerk zurückverfolgen (vgl. particl.news 2022).

Goldrausch und Fake-Hype

„OpenSea would actually be much `better` in the immediate sense if all the web3 parts were gone. It would be faster, cheaper for everyone, and easier to use." (vgl. Marlinspike 2022).

Moxie Marlinspike, CEO der Signal-App, ist der Meinung, dass digitale Kunst nur ein Hype ist, da es auf Kryptowährungen aufbaut. Das Verkaufen von digitaler Kunst wäre auch ohne Blockchain möglich. Menschen möchten auf den neuen Hype aufspringen, nachdem sie gesehen haben, wie viel Geld in Kryptowährungen verdient wurde. Es geht denen dabei nicht um Dezentralität oder die Zukunft des Internets, sondern um Wertschöpfung (vgl. Marlinspike 2022).

Kryptowährungen und NFTs haben zurzeit keinen wahren Zweck in der echten Welt und basieren auf reiner Spekulation (vgl. Shevchuk 2022).

Komplexität

Die vorherigen genannten Probleme zielen auf eines ab: Web3 Entwicklung ist komplex. Vollkommen dezentrale Applikationen können in der Benutzerfreundlichkeit nicht mit zentralen Diensten mithalten. Die Interaktion mit verteilten Systemen ist kompliziert, umso mehr, wenn zusätzliche Anforderungen wie die Verwaltung von

mehreren Signaturen oder die Verwendung von Zero-Knowledge-Proofs zur Wahrung der Privatsphäre und Sicherheit hinzukommen (vgl. Brody 2022).

Kapitalismus auf Steroiden

Kritiker sehen Gefahren in DAOs durch schlechtes Design und unbedachte Programmierung. Zurzeit entscheiden Informatiker über essenzielle Governance-Fragen. “While many engineers are working on this cutting edge technology and they´re super smart, they are not governance experts” (Voshmgir 2018). Governance-Experten und Informatiker sollten in dieser Thematik zusammenarbeiten und entscheiden, wie der Quellcode aussehen muss. Es ist nicht nur eine technologische Frage, es ist eine Governance-Frage, Ethikfrage, Wirtschaftsfrage, organisatorische Frage etc. (vgl. Voshmgir 2018). Laut Vochmgir muss diese Zusammenarbeit zustande kommen, ansonsten geschehen die gleichen Fehler wie bei der Entwicklung von Web2 mit Protokoll-bias und Algorithmischen-bias.

Oftmals sind DAOs auch an gewissen Voraussetzungen gebunden. Im Beispiel der dezentralen Kryptowährungsbörse Uniswap, benötigt ein Nutzer 10.000.000 des Tokens UNI, um einen Vorschlag machen zu dürfen. Diese Art von DAO und Nutzung des Tokens löst jedoch Kritik aus. Der obige Mechanismus gleicht einer Plutokratie. Je mehr UNI ein Nutzer besitzt, desto höher sein Einfluss (vgl. Eichholz 2020). Diese Anreizmechanismen sind „Kapitalismus auf Steroiden“ (Voshmgir, 2018).

Interoperabilität

Die Web3 Foundation ist, wie Vitalik Buterin, ein großer Spieler in der Entwicklung von Web3 Technologien. Gegründet von Dr. Gavin Wood, damaliger Co-Founder von Ethereum. Die Foundation entwickelt Polkadot, eine open source Blockchain Plattform, die es ermöglicht, dass öffentliche und private Blockchains sich einer Konnektivitätsschicht anschließen und harmonieren (vgl. Web3 Foundation o. J.). Wood verließ 2016 Ethereum und kritisierte die langsame Entwicklung von Ethereum 2.0. Interoperabilität und massive Anzahl von unabhängigen Blockchain-Projekten ist eine zentrale Herausforderung von Web3 und spezifischer Ethereum. Viele

Plattformen sind derzeit nicht in der Lage, miteinander zu interagieren. Polkadot möchte Blockchain übergreifende Transaktionen so nahtlos wie möglich gestalten.

Gavin Wood sieht Interoperabilität von individuellen Blockchains als kritischen Faktor eines funktionierenden Web3 Ökosystems und schlägt daher Polkadot als Fundament vor. Diese These von Interoperabilität wird von anderen Experten bestätigt: „a secure interoperability platform to hyperconnect these isolated state publishers (both decentralized and federated / central ones) is the final building block to enable Web3“ (Zhuotao et al. 2021, 3).

Interoperabilität ist ein Hauptkritikpunkt an Ethereum (s. Kapitel 2.6.4). Und es ist unwahrscheinlich, dass das Problem in naher Zukunft gelöst wird. Trotz der Kritikpunkte, sind 70 % aller DApps auf der Basis von Ethereum gebaut (vgl. Yatchenko 2022). Aufgrund der heutigen Popularität von Ethereum (Stand 2022), wird sich diese Bachelorarbeit auf Ethereum basierende DApps spezialisieren.

3 Konzeption zur Evaluierung von Web3

Das vorherige Kapitel gibt ein grundlegendes Wissen über den Aufbau und Nutzen von Web3. Befürworter sehen DApps auf Basis von Blockchains als die Zukunft des Internets. Um Web3 zu evaluieren ist es demnach essenziell, diese DApps, deren Fundamente, Anwendernutzen und Entwicklung zu bewerten. Diese Bewertung findet mit einer Untersuchung auf vorher definierten Metriken statt.

Anwender, Investoren und Entwickler profitieren von einem Standardsatz von Maßnahmen, die Grundlagen eines Systems messen und bewerten. Die richtige Auswahl dieser Metriken ist keine leichte Aufgabe und dies ist z. B. zu erkennen im Fall der Dezentralität. Viele Protokolle sehen die Dezentralität als Kernziel ihres Projektes, können nach direkten Nachfragen jedoch nicht genau definieren, was dies beinhaltet. „Some aim for a minimum number of participating miners (…) while others suggest gauging decentralization indirectly through profitability or governance" (Hurder 2020).

Diese Bachelorarbeit zeigt ein Konzept zur Bewertung von Web3 Anwendungen in Bezug auf die Versprechen und Kritikpunkte von Web3. Entwickler können dies nutzen, um die Ziele einer DApp im Auge zu behalten und Verbesserungen vorzunehmen. Benutzer haben nach erfolgreicher Anwendung dieses Verfahrens auf mehrere Projekte eine fundierte Übersicht, die zur Entscheidungsfindung der Nutzung von DApps helfen kann. Auch Investoren können durch den Vergleich von ähnlichen Projekten eine Unterstützungshilfe für die Entscheidung einer Investition erhalten.

3.1 Methodik

Zur Konzipierung wird der Goal-Question-Metric-Ansatz (GQM) von Victor Basili und Dieter Rombach angewendet (s. Abb. 8). GQM soll in dieser kritischen experimentellen Bachelorarbeit auf der obersten konzeptuellen Ebene Ziele

definieren. Auf der operativen Ebene werden daraufhin Fragen erörtert, um diese Ziele besser zu charakterisieren. Die letzte Ebene (quantitative Ebene) assoziiert objektive oder subjektive Metriken zu der definierten Frage, um eine quantitative Antwort zu erhalten (vgl. Basili et al. 1994, 528–530).

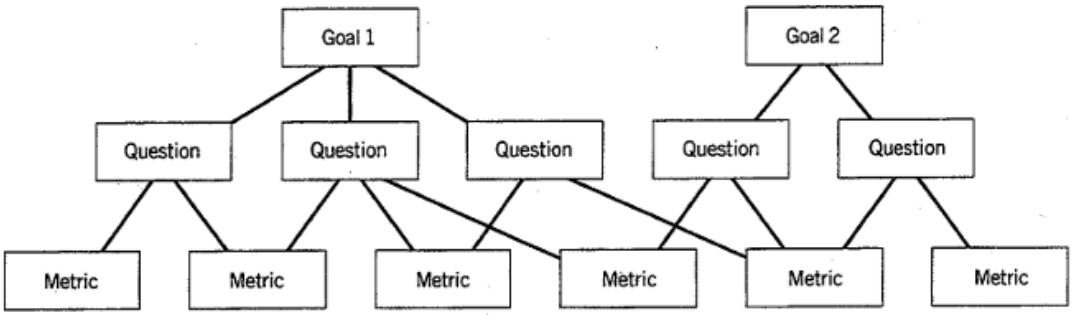

Abbildung 8: Hierarchische Struktur des GQM Models (vgl. Basili et. al. 1994, 529)

Das Erstellen von Zielen wird mit Hilfe von vier Schritten unterstützt:

1. **Zweck**: Verbesserung, Charakterisierung, Evaluierung, Vorhersagung, etc.
2. **Merkmal**: Benutzerfreundlichkeit, Korrektheit, Dezentralität, Flexibilität, Effizienz, Integrität, Testbarkeit, etc.
3. **Objekt (Prozess)**: Unternehmensprozesse, Software, etc.
4. **Perspektive**: Entwickler, Anwender, Manager, etc.

Aus dieser Spezifikation aller Ziele, können dann sinnvolle Fragen abgeleitet werden (vgl. Basili et al. 1994, 528–530).

3.1.1 Messung der Metriken

Um am Ende des GQM-Verfahrens ein aussagekräftiges Ergebnis zu erhalten, muss jede Metrik eine angemessene Messgröße haben und eine Vorgabe, wie die Messwerte ermittelt werden. Dies ist bei subjektiven Metriken schwer zu definieren und wird abhängig von der Metrik von dem jeweiligen Anwender des Konzepts bewertet. Objektive Metriken können jedoch durch Formeln ermittelt und berechnet werden. Diese klaren Ergebnisse der einzelnen Metriken werden für eine endgültige

Bewertung des Ziels zusammengetragen und gegebenenfalls gewichtet (vgl. Rumpel 2015, 15).

Die Anforderung des Messverfahrens muss dabei definiert werden. Verschiedene Ziele haben verschiedene Anforderungen. Die Metriken können binär betrachtet werden:

$$M_1 = \begin{cases} 0\ wenn\ x = y \\ 1\ wenn\ x \neq y \end{cases}$$

Eine weitere Möglichkeit für einen präziseren Wert ist es, zusätzliche Werte einzuführen. Es wird davon ausgegangen, dass alle x-Werte zwischen 0 und 1 liegen sollen. Dann lässt sich folgend definieren:

$$M_1 = \begin{cases} 0 & wenn \quad x = 0 \\ 0{,}5 & wenn \quad x > 0\ und\ x < 1 \\ 1 & wenn \quad x = 1 \end{cases}$$

Bestimmte Metriken können auch direkt verwendet werden und brauchen keine weiteren Aufteilungen oder Abfragen. Beispiel:

$$M_1 = \% - Anteil\ der\ Häuser\ in\ DE\ mit\ Solar$$

Solch eine Metrik gibt eine direkte Rückmeldung. Hat Deutschland 100 % Solar auf den Dächern, ist dies durch eine Teilung mit 100 als eine 1 (den höchstmöglichen Wert) repräsentiert. Eine Aufteilung mit einer „wenn“-Abfrage ist hier nicht nötig.

Die Zahlen stehen dabei für einen Erfüllungsgrad (s. Kapitel 3.1.2). Es muss erörtert werden, ob etwas „teilweise erfüllt“ sein kann. Bei der Frage, ob ein DApp-Entwickler für die Einhaltung der Dezentralität einen eigenen Ethereum-Knoten aufgestellt hat oder nicht, gibt es ein klares *erfüllt* oder *nicht erfüllt* (vgl. Rumpel 2015, 16).

Nicht für jede Frage lässt sich diese Art von Messung anwenden. In vielen Fällen ist es nötig, ein eigenes Zielerreichungsmaß abzuleiten. Dieser muss die Anforderung des Effektivitätsindikators einhalten, der hier verlangt, dass das Ergebnis einer Messung eine Zahl zwischen 0 und 1 ist. Dieser Indikator bestimmt abschließend die Zielerreichung in Prozent. Ein Beispiel:

Ziel 1 beinhaltet zwei Fragen (F1 und F2). F1 hat nur eine Metrik mit dem Wertebereich 0 bis 3 und dadurch folgendes Messverfahren zur Ermittlung des Zielerreichungsgrades (ZEG):

$$ZEG_1 = M_1 = \begin{cases} 0 & wenn\ x < 2 \\ 0{,}5 & wenn\ x = 2 \\ 1 & wenn\ x = 3 \end{cases}$$

Ziel 2 hat vier Metriken und ist daher etwas komplizierter (hier mit konkreten Metriken für das Verständnis):

M_2: Anzahl der besuchten Städte in Deutschland mit über 1 Million Einwohner

M_3: Anzahl der Städte in Deutschland mit über 1 Million Einwohner

M_4: Anzahl der besuchten Städte in der EU mit über 1 Million Einwohner

M_5: Anzahl der Städte in der EU mit über 1 Million Einwohner

Daraus lässt sich folgendes Zielerreichungsmaß erstellen, um einen Erfüllungsgrad zwischen 0 und 1 zu erhalten:

$$ZEG_2 = (\frac{M_2}{M_3} + \frac{M_4}{M_5})/2$$

Besteht die Möglichkeit, dass eine Formel die Gesetze der Mathematik brechen könnte, müssen für diese Situationen Regeln aufgestellt werden. Für den Fall, dass der Nenner Null wird und ein Gesetz gebrochen wird, soll hier der betroffene Summand entfernt werden.

In diesem Beispiel lässt sich für das Ziel Z1 den folgenden Effektivitätsindikator einführen:

$$I_1 = (ZEG_1 + ZEG_2)\ /\ 2$$

Im Falle von ZEG_1 =1 und ZEG_2 = 1, ist auch der Effektivitätsindikator I_1 = 1 und die Zielerreichung für Ziel 1 wäre 100 Prozent.

3.1.2 Deutung des Effektivitätsindexes

Die Deutung erfolgt über ein Spektrum von 0 bis 1 (s. Abb. 9). 0 ist dabei das schlechtmöglichste und 1 das bestmögliche Ergebnis. Dieses Ergebnis quantifiziert verschiedene Ziele für die detailreichere Diskussion in Kapitel 6.

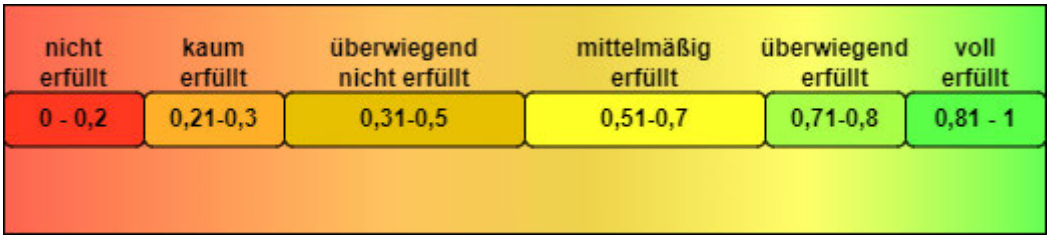

Abbildung 9: Spektrum zur Deutung des Effektivitätsindexes

3.2 GQM-Verfahren für eine DApp

Die Ziele für eine Evaluierung einer DApp lassen sich unter anderem aus den Versprechen der Befürworter und den Kritikpunkten der Skeptiker ableiten. Diese wurden in Kapitel 2.6 ausführlich erörtert. Im Folgenden werden alle Ziele, Fragen und Metriken aufgezeigt und mithilfe einer tabellarischen Struktur visualisiert. Dieses Konzept kann damit universell auf alle (PoW) DApps angewendet werden und eine Bewertung des Web3 Ökosystems herleiten.

Es beginnt mit dem Versprechen, dass Web3 charakterisiert: Dezentralität.

3.2.1 Dezentralität

Um die Dezentralität einer DApp zu untersuchen, müssen alle Teile der Architektur analysiert werden. Dabei spielt die fundamentale Blockchain eine große Rolle, sowie die angebundenen Protokolle und Funktionalitäten. Des Weiteren gilt es zu untersuchen, ob zentralisierte Dienste genutzt wurden, um die Entwicklung der DApp zu vereinfachen (s. Tabelle 1). Dezentralität ist keine binäre ist oder ist-nicht Kondition, „but a very complex and emergent process that will change as the network grows“ (Muzzy und Anderson 2022). Eine Blockchain erlangt oftmals Dezentralität mit der

Zeit. Es wird nicht immer möglich sein, Dezentralität zu quantifizieren und vieles hängt von der Interpretation der Daten und Graphen ab (Muzzy und Anderson 2022).

GQM Model für Ziel 1, eine Dezentrale DApp			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Dezentralität der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Entwicklers		
Frage	F1.1	Wie dezentral ist die fundamentale Blockchain?		
Metriken	M1	Herfindahl-Hirschman Index (HHI)	Formel	objektiv
	M2	Gini-Koeffizient (Miner)	Formel	objektiv
	M3	Nakamoto Koeffizient (51%)	Formel	objektiv
	M4	Zentralität EIPs	Skala	subjektiv
	M5	Gini-Koeffizient (Knoten - Länder)	Formel	objektiv
	M6	%-Anteil Top Land	Statistik	objektiv
	M7	Blockchain-Größe in GB	Daten	objektiv
	M8	Blockchain-Wachstumsrate	Daten	objektiv
	M9	Zentralität Speicher	Skala	subjektiv
	M10	Anzahl Knoten in Cloud	Daten	objektiv
	M11	Anzahl Knoten	Daten	objektiv
	M12	Anteil Knoten des Top Cloud-Anbieter	Daten	objektiv
Frage	F1.2	Ist ein eigener Knoten aufgestellt?		
Metriken	M13	Binäre Abfrage (Ja/Nein)	Binär	objektiv
Frage	F1.3	Wie dezentral sind die benutzten Provider?		
Metriken	M14	Zentralität des Providers	Skala	subjektiv
Frage	F1.4	Wie dezentral sind die angebundenen Dienste/Protokolle?		
Metriken	M15	Zentralität des Dienstes/Protokolls	Skala	subjektiv
	M16	Herfindahl-Hirschman Index (HHI)	Formel	objektiv
	M17	Gini-Koeffizient (Miner/Validator)	Formel	objektiv
	M18	Nakamoto Koeffizient (51%)	Formel	objektiv

Tabelle 1: Tabelle für die Fragen und Metriken der Dezentralität

Frage 1.1: Wie dezentral ist die fundamentale Blockchain?

Die Dezentralität einer Blockchain ist schwer zu messen und ist stark von Analysetools und transparenten Daten abhängig. Es ist daher sinnvoll, alle möglichen Faktoren zu analysieren, die einen zentralisierten Engpass haben könnten (s. Tabelle 1).

Verschiedene Experten haben dort eine andere Herangehensweise. Eine Möglichkeit wäre einzelne Unterkategorien zu bilden und diese zu bewerten (vgl. Muzzy und Anderson 2022; Srinivasan 2017). Andere bilden Metriken für die einzelnen architekturalen Schichten einer öffentlichen Blockchain (vgl. Gochhayat et al. 2020) oder führen eine empirische Studie und Literaturrecherche durch, zur Erfassung von Meinungen verschiedener Experten (vgl. Sai et al. 2021).

Die verwendeten Metriken sind alle on-Chain Daten und ebenfalls bedeutende off-Chain Daten wurden bewusst weggelassen. Die Quantifizierung von off-Chain Daten

wie die Stärke und Verteilung der Stromnetze, auf denen Knoten laufen, sowie die rechtlichen Zuständigkeiten und ökonomischen/politischen Stabilität der Länder sprengt den Rahmen dieser Bachelorarbeit (vgl. Muzzy und Anderson 2022).

Eine Blockchain kann im Bereich Dezentralität äußerst detailreich untersucht werden. Diese Bachelorarbeit befasst sich jedoch mit dem gesamten Umfeld von Web3 und kann daher bewusst viele Metriken nicht beachten. Es wird daher eine architektonische Herangehensweise nach Gochhayat gewählt (s. Abb. 10) (vgl. Gochhayat et al. 2020). Es werden angemessene Metriken hinzugefügt und weniger relevante Faktoren entfernt (s. Tabelle 2). Eine ausführliche Analyse und Literaturrecherche zu diesem Thema bietet Sai (vgl. Sai et al. 2021).

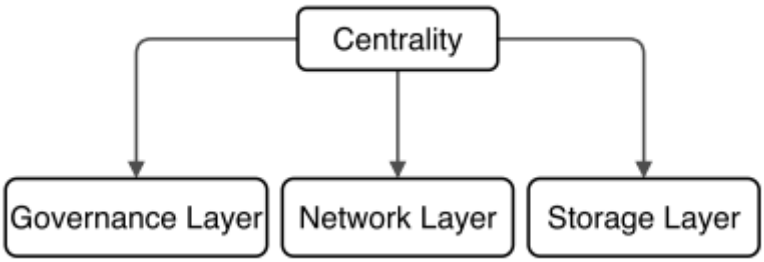

Abbildung 10: Die drei Schichten der Dezentralität (Gochhayat et al. 2020, 178374)

Schicht	Zentralisierungsfaktor	wichtige Metriken
Operative Schicht (Storage Layer)	Speicherbeschränkung	Größe in GB & Wachstumsrate
	Knotenverteilung	Individuelle/Cloud Knoten
Netzwerkschicht (Network Layer)	Geografische Verteilung	Gini-Koeffizient %-Anteil Top Land
Governance-Schicht (Governance Layer)	Machtverteilung	Gini-Koeffizienten, HHI & Nakamoto-Koeffizienten
	Verbesserungsprotokoll	Skala Zentralität

Tabelle 2: Aufteilung der Metriken in die Schichten der Blockchain

Die **Governance-Schicht** beinhaltet folgende Messbarkeiten:

Machtverteilung: *M_1 (HHI)*; *M_2 (Gini), M_3 (Nakamoto)*

$$ZEG_1 = \left(M_1 + (1 - M_2) + \frac{M_3}{10}\right) / 3$$

Dabei gilt, $M_1 = \begin{cases} 0 \; wenn \; HHI > 2500 \\ 0{,}33 \; wenn \; HHI > 1500 \leq 2500 \\ 0{,}66 \; wenn \; HHI > 100 \leq 1500 \\ 1 \; wenn \; HHI \leq 100 \end{cases}$ $HHI = \sum_{i=1}^{N} s_i^2$

$s_i = Prozent \; des \; Miners \; i \; im \; Netzwerk \quad N = Totale \; Anzahl \; der \; Teilnehmer$

Der HHI ist ein Hinweis auf das Ausmaß des Wettbewerbs. Im Falle einer PoW Blockchain bedeutet das den Wettbewerb unter Miner und Mining-Pools. Es berechnet alle quadrierten Marktanteile der einzelnen Wettbewerber eines bestimmten Marktes. Folgende Werte können gedeutet werden: HHI unter 100 bedeutet eine hart umkämpfte Branche, zwischen 100 und 1500 eine unkonzentrierte Industrie, zwischen 1500 und 2500 eine mäßige Konzentration und ein Wert über 2500 bedeutet eine hohe Konzentration. Je wettbewerbsreicher, desto dezentraler (vgl. Sridhar 2021).

$$M_2 = Gini - Koeffizient = \frac{A}{A + B}$$

Der Gini-Koeffizient oder Gini-Index ist ein Maß für Vermögungsungleichheiten, die innerhalb einer bestimmten Bevölkerung bestehen. Dieser Index wird mithilfe der Lorenzkurve berechnet (s. Abb. 11).

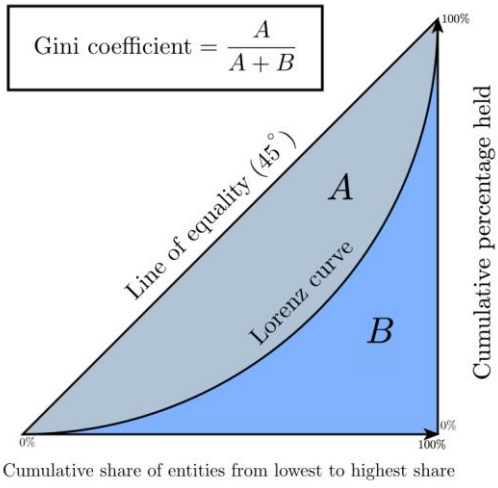

Abbildung 11: Lorenz-Kurve und Formel für Gini-Koeffizienten (vgl. Sridhar 2021)

Die Lorenzkurve ist der Graph, der durch das Abbilden des kumulativen Prozentsatzes der Bevölkerung zum Prozentsatz des Vermögens oder der Beteiligung entsteht. Es bildet damit Disparitäten ab und der Gini-Koeffizient fasst diese Informationen in einer einzelnen Zahl zusammen (s. Abb. 12) (vgl. Sridhar 2021). Im Falle einer Blockchain bedeutet das, der Gini-Koeffizient ist 0, wenn alle Knoten Blöcke gleichermaßen generieren. Je höher der Wert steigt, desto zentralisierter (vgl. Gochhayat et al. 2020, 178380).

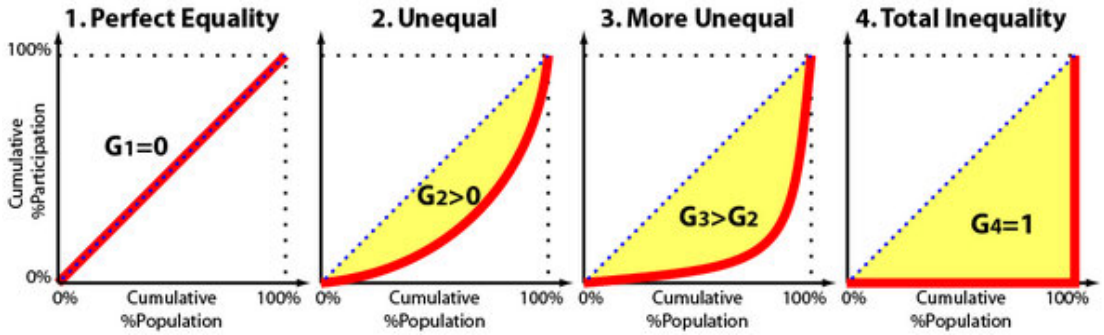

Abbildung 12: Die Ergebnisse der Lorenzkurve (Sridhar 2021)

$$M_3 = Nakamoto * 2 \qquad Nakamoto = \min\left\{k \in [1, \dots, k]: \sum_{i=1}^{k} p_i \geq 0{,}51\right\}$$

Falls $M_3 > 10$ dann $M_3 = 10$. Der Nakamoto-Koeffizient ermittelt die minimale Nummer von Entitäten für eine Rechenleistung von 51%. Dies ist nicht nur eine Metrik der Dezentralität, sondern auch ein bedeutungsvolles Ergebnis für die Sicherheit der Blockchain. Dies kann zu einer sogenannten „51%-Attacke“ führen und großen Schaden an der Blockchain verrichten (vgl. Bunin 2019).

Verbesserungsprotokolle: *M_4 (Skala Zentralität der EIPs)*

$$ZEG_2 = \frac{M_4}{10}$$

M_4 evaluiert die Zentralität der EIPs auf einer Skala von 0 bis 10. Wobei 10 vollkommen dezentral und 0 vollkommen zentral bedeutet. Die Antwort basiert auf Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Effektivitätsindikator: $I_1 = (ZEG_1 + ZEG_2)/2$

Die **Netzwerkschicht** beinhaltet folgende Messbarkeit:

Geografische Verteilung: *M_5 (Gini)*; *M_6 (%-Anteil Top Land)*

$$ZEG_3 = \left((1 - M_5) + \left(1 - \frac{M_6}{100}\right)\right) / 2$$

Dabei gilt, $M_5 = Gini - Koeffizient = \frac{A}{A+B}$ $(s. Abb. 19 \,\&\, 20)$

Der Gini-Koeffizient beschreibt hier die Ungleichheiten der Knotenverteilung auf den verschiedenen Ländern. *M_6* ist der Anteil des Landes mit den meisten Knoten in Prozent.

Effektivitätsindikator: $I_2 = ZEG_3$

Die **Operative Schicht** beinhaltet folgende Messbarkeit:

Speicherbeschränkung: *M_7 (Größe in GB)*; *M_8 (Wachstumsrate)*; *M_9 (Zentralität Speicher)*

$$ZEG_4 = \frac{M_9}{10}$$

Dabei gilt, dass die Bewertung der Speicherbeschränkung abhängig ist von der Technologie und den Kosten für Festplatten. Dies kann sich durch ansteigende Blockchain-Aktivität, mangelnder Rohstoffe oder weiteres ändern. Auch durch eventuell langsamen Fortschritt in der Erhöhung von Speicher, ist es schwer, eine einheitliche Messung zu erstellen. Es ist daher vorteilhaft, eine subjektive Einschätzung im Bereich der Größe und Wachstumsrate zu geben.

M_9 evaluiert die Größe und Wachstumsrate auf einer Skala von 0 bis 10. Wobei 10 eine Situation darstellt, bei der die Mehrheit der Nutzer sich das finanziell leisten kann

und 0 bedeutet, dass das Aufstellen ein reines Luxusgut ist. Die Antwort basiert auf Literaturrecherche der aktuellen Situation und den Metriken $M_{7,8}$.

Knotenverteilung: *M_{10} (Anzahl Knoten in Cloud); M_{11} (Anzahl Knoten); M_{12} (Anteil Knoten des Top Cloud-Anbieter)*

$$ZEG_5 = \left(\left(1 - \frac{M_{10}}{M_{11}}\right) + \left(1 - \frac{M_{12}}{100}\right)\right)/2$$

M_{10} ist die Anzahl aller Knoten, die über eine beliebige Online-Cloud laufen und M_{11} die Anzahl aller Knoten der Blockchain. M_{12} ist der Anteil der Knoten des Top-Cloud Anbieters in Relation zu allen Knoten der Blockchain.

Effektivitätsindikator: $I_3 = (ZEG_4 + ZEG_5)/2$

Frage 1.2: Ist ein eigener Knoten aufgestellt?

Knoten: *M_{13} (binäre Abfrage)*

$$ZEG_6 = M_{13}$$

Dabei gilt, $M_{16} = \begin{cases} 0\ wenn\ x\ =\ 0 \\ 1\ wenn\ x\ \neq\ 0 \end{cases}$

x = 0 wenn „Nein“ und x = 1 wenn „Ja“. Wurde ein eigener Knoten aufgestellt und somit auf einen Provider verzichtet, kann die Frage 1.3 übersprungen werden und der *Effektivitätsindikator* ist: $I_4 = ZEG_6$

Frage 1.3: Wie dezentral sind benutzte Provider?

Provider: *M_{13} (Skala Zentralität des Providers)*

$$ZEG_7 = \frac{M_{13}}{20}$$

Wurde kein eigener Knoten aufgestellt und dadurch ein Provider genutzt, muss dieser auf Dezentralität bewertet werden. M_{13} evaluiert die Zentralität auf einer Skala von 0 bis 10. Wobei 10 vollkommen dezentral und 0 vollkommen zentral bedeutet. Die Antwort basiert auf Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Alternativer *Effektivitätsindikator:* $I_4 = (ZEG_6 + ZEG_7)/2$

Frage 1.4: Wie dezentral sind die angebundenen Dienste/Protokolle?

Die verwendeten Dienste/Protokolle können ebenfalls tief im Detail untersucht werden. Dies ist jedoch nicht zwingend notwendig. Weitere Protokolle wie The Graph oder IPFS dienen dazu, die DApp weiter zu dezentralisieren oder den Entwicklern hinter den Kulissen mehr Spielraum zu geben. Eine Literaturrecherche mit aktueller Bewertung der Lage ist für Dienste und Protokolle ohne eigener Blockchain ausreichend. Wird ein weiteres Blockchain-Protokoll in die DApp eingebaut, gilt es dieses mit einigen essenziellen Metriken (HHI, Gini, Nakamoto) zu untersuchen.

Dienste/Protokolle: *M_{14+i} (Skala Zentralität des Dienstes/Protokolls)*

$$ZEG_8 = k \in [1, \dots, k]: \left(\sum_{i=1}^{k} \frac{M_{14+i}}{10} \right) / k$$

Dabei ist k die Anzahl der genutzten Dienste und Protokolle ohne Blockchain. M_{13+i} evaluiert die Zentralität auf einer Skala von 0 bis 10. Wobei 10 vollkommen dezentral und 0 vollkommen zentral bedeutet. Die Antwort basiert auf Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Blockchain-Protokolle: *M_{15+k} (Gini); M_{16+k} (HHI); M_{17+k} (Nakamoto);*

$$j \in [1, \dots, n]: ZEG_{8+j} = \left((1 - M_{15+k}) + (1 - M_{16+k}) + \frac{M_{17+k}}{10} \right) / 3$$

Dabei gilt, n ist die Anzahl aller angebundenen Protokolle und j das jeweilige Protokoll. Jedes Protokoll bekommt einen eigenen Zielerreichungsgrad. Siehe Kapitel 3.2.1 unter dem Unterpunkt „Machtverteilung“ für die Formeln der Metriken.

Effektivitätsindikator:

$$I_5 = \left(ZEG_8 + \sum_{j=1}^{n} ZEG_{8+j} \right) / (n + 1)$$

3.2.2 Sicherheit

Die Sicherheit der DApp hat eine äußerst hohe Priorität in der Web3 Entwicklung. Aufgrund der Token-Ökonomie und das damit verbundene Kapital, gilt es die Tokens der Benutzer zu schützen. Wie in Kapitel 2.6.4 erwähnt, steigt die Anzahl der Hacker-Angriffe und Exploits in DApps und Blockchain-Protokollen an. Es ist daher essenziel, die Sicherheitslage zu überprüfen und dies mithilfe von Metriken zu untersuchen.

Wie bei der Dezentralität ist es vorteilhaft, hier die einzelnen architektonischen Elemente zu untersuchen (s. Tabelle 3).

GQM Model für Ziel 2, eine sichere DApp			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Sicherheit der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Entwicklers		
Frage	F2.1	Wie sicher ist die fundamentale Blockchain?		
Metriken	M1	Nakamoto-Koeffizient (33%)	Formel	objektiv
	M2	Nakamoto-Koeffizient (51%)	Formel	objektiv
	M3	Nakamoto-Koeffizient (66%)	Formel	objektiv
	M4	Sicherheit der Blockchain	Skala	subjektiv
Frage	F2.2	Wie sicher sind die Smart Contracts?		
Metriken	M5	Smart Contract Audit	Analyse	objektiv

Tabelle 3: Tabelle für die Fragen und Metriken der Sicherheit

Frage 2.1: Wie sicher ist die fundamentale Blockchain?

Das Grundgerüst von Web3 und der DApp müssen höchste Sicherheitsstandards aufweisen. Auf Grund dessen, sind subjektive Einschätzungen umso kritischer zu betrachten.

Blockchain-Sicherheit: *M_1 (Nakamoto >33%); M_2 (Nakamoto >51%); M_3 (Nakamoto >66%); M_4 (Skala Sicherheit der Blockchain)*

$$ZEG_1 = \left(\frac{M_1}{10} + \frac{M_2}{10} + \frac{M_3}{10} + \frac{M_4}{10}\right) / 4$$

Dabei gilt,

$$M_1 = \min\left\{k \in [1, \dots, k]: \sum_{i=1}^{k} p_i \geq 0{,}33\right\} * 4 \quad M_2 = \min\left\{k \in [1, \dots, k]: \sum_{i=1}^{k} p_i \geq 0{,}51\right\} * 2$$

$$M_3 = \min\left\{k \in [1, \dots, k]: \sum_{i=1}^{k} p_i \geq 0{,}66\right\} * 1{,}5 \qquad M_4 = Skala\ 0 - 10$$

Falls $M_{1,2,3} > 10$ dann $M_{1,2,3} = 10$. Die Multiplizierung mit 4, 2 und 1,5 bei $M_{1,2,3}$ gilt für den Ausgleich der Formel. *M_4* evaluiert die Sicherheit auf einer Skala von 0 bis 10. Wobei 10 vollkommen sicher und 0 unsicher bedeutet. Die Antwort basiert auf Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Frage 2.2: Wie sicher sind die Smart Contracts?

Smart Contracts: *M_{4+i} (Audit)*

$$ZEG_2 = k \in [1, \dots, k]: \sum_{i=1}^{k} M_{4+i}$$

Dabei gilt, $M_{4+i} = \begin{cases} 0\ wenn\ x\ =\ 0 \\ 1\ wenn\ x\ \neq\ 0 \end{cases}$

k ist die Anzahl der zu untersuchenden Smart Contracts. x = 0 wenn Smart Contract Audit nicht bestanden (ein Fehler kritischer Natur reicht aus) und x = 1 wenn Audit bestanden. Jeder Smart Contract wird individuell als eigene Metrik betrachtet.

Für die Untersuchung der Smart Contracts hat sich ein neuer Zweig in der Wirtschaft aufgetan. Smart Contract Audits sind heutzutage ein wesentlicher Bestandteil des Entwicklungsprozesses. Die meisten Smart Contracts arbeiten mit Vermögenswerten und ein einziger Bug oder kritischer Fehler kann für Verluste in Millionenhöhe sorgen (vgl. Kapitel 2.6.4).

Abschließend lässt sich folgender *Effektivitätsindikator* für die Sicherheit bilden:

$$I_6 = (ZEG_1 + ZEG_2)\ /\ 2$$

3.2.3 Funktionalität

Durch die Natur der Smart Contracts und der Unwiderruflichkeit, ist es umso bedeutender, dass die Funktionalitäten getestet werden. Dies gilt aus der Sicht des

Entwicklers (s. Tabelle 4) und des Anwenders (s. Tabelle 5). Die Website muss funktionieren, sowie die Schnittstellen zu Protokollen und weiteren Diensten.

GQM Model für Ziel 3, eine funktionale DApp			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Funktionalität der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Entwicklers		
Frage	F3.1	Funktionieren die Smart Contracts?		
Metriken	M1	%-Anteil Test-Coverage	Analyse	objektiv
	M2	Unit und Integrations-Tests	Testung	objektiv
Frage	F3.2	Funktionieren die angebundenen Dienste/Protokolle?		
Metriken	M3	Testen der Funktionalitäten	Skala	objektiv

Tabelle 4: Tabelle für die Fragen und Metriken der Funktionalität

Frage 3.1: Funktionieren die Smart Contracts?

Smart Contract: *M_1 (%-Anteil Test-Coverage); M_2 (%-Anteil erfolgreiche Unit und Integrationstests)*

$$ZEG_1 = \left(\frac{M_1}{100} + \frac{M_2}{100}\right)/2$$

Dabei ist M_1 der gemeinsame Prozentanteil der zusammenrechneten Kategorien des jeweiligen „Coverage Checkers“ aller Smart Contracts. M_2 ist ebenfalls die gesamte Prozentzahl der funktionierenden Unit & Integrationstests aller Smart Contracts.

Frage 3.2: Funktionieren die angebundenen Dienste/Protokolle?

Dienste/Protokolle: *M_{2+j} (Funktionalität der Dienste/Protokolle)*

$$j \in [1, \dots, m]: ZEG_{1+j} = \frac{M_{2+j}}{10}$$

Dabei gilt, m ist die Anzahl der Dienste/Protokolle, die untersucht werden sollen und j ist der zu untersuchende Dienst oder das zu untersuchende Protokoll. M_{2+j} ist jeweils eine Skala von 0 bis 10, dass die Funktionalität der Dienste/Protokolle Mithilfe einer Testung der Funktionen bewertet. 10 bedeutet, dass alles zu 100% funktioniert und 0, dass das Anbinden gescheitert ist.

Effektivitätsindikator für die Funktionalität aus der Sicht des Entwicklers:

$$I_7 = \left(ZEG_1 + \left(\sum_{j=1}^{m} ZEG_{1+j} \right) \right) / (m+1)$$

Es folgt die Untersuchung der Funktionalität aus der Sicht des Anwenders:

GQM Model für Ziel 3, eine funktionale Dapp (Anwender)			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Funktionalität der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Anwenders		
Frage	F3.3	Funktioniert die Website?		
Metriken	M4	Gesamt %-Anteil funktionierender Funktionen (lokal)	Analyse	objektiv
	M5	Gesamt %-Anteil funktionierender Funktionen (Testnetzwerk)	Analyse	objektiv

Tabelle 5: Tabelle für die Fragen und Metriken der Funktionalität aus der Sicht des Anwenders

Frage 3.2: funktioniert die Website?

Website: *M_3 (Gesamt %-Anteil funktionierenden Funktionen lokal); M_4 (Gesamt %-Anteil funktionierenden Funktionen Testnetzwerk);*

$$I_8 = ZEG_{n+1} = \left(\frac{M_3}{100} + \frac{M_4}{100} \right) / 2$$

3.2.4 Effizienz

Die Effizienz ist ein universelles Merkmal und sollte in Verbindung mit Software untersucht werden. Kritiker in Kapitel 2.6.4 machen klar, dass die Dezentralität zu langsamen und teuren Transaktionen führen kann. Es muss daher untersucht werden, ob DApps in diesen Bereich mit Web2 Anwendungen mithalten können. Auch hier muss wieder auf die Sicht des Entwicklers (s. Tabelle 6) und des Anwenders (s. Tabelle 7) geschaut werden.

GQM Model für Ziel 4, eine effiziente DApp			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Effizienz der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Entwicklers		
Frage	F4.1	Wie schnell kann die Blockchain Transaktionen validieren?		
Metriken	M1	TPS (Vergleich)	Statistik	objektiv
	M2	Effizienz der Transaktionen	Skala	subjektiv
Frage	F4.2	Wie hoch ist der Energieverbrauch?		
Metriken	M3	Terrawattstunden	Statistik	objektiv
	M4	Effizienz der Energie	Skala	subjektiv
Frage	F4.3	Wie hoch sind die Kosten für den Entwickler?		
	M5	Kosten für das Deployen des Smart Contracts	Daten	objektiv
	M6	Effizienz des Deployen	Skala	subjektiv

Tabelle 6: Tabelle für Fragen und Metriken der Effizienz

Frage 4.1: Wie schnell kann die Blockchain Transaktionen validieren?

Transaktionen: *M_1 (TPS); M_2 (Skala Effizienz der Transaktionen)*

$$ZEG_1 = \frac{M_2}{100}$$

Die Effizienz der Blockchain Transaktionen wird mit einer Skala von 0 bis 10 bewertet. Dabei ist 10 eine außerordentliche Effizienz im Vergleich zu Konkurrenten und 0 eine äußerst langsame Transaktionszeit. Die Antwort basiert auf dem Vergleich der Metrik M_1, durch Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Frage 4.2: Wie hoch ist der Energieverbrauch?

Energie: *M_3 (Terrawattstunden); M_4 (Skala Effizienz der Energie)*

$$ZEG_2 = \frac{M_4}{100}$$

Die Effizienz des Energieverbrauches wird mit einer Skala von 0 bis 10 bewertet. Dabei ist 10 ein klimafreundlicher Verbrauch und 0 umweltschädlich. Die Antwort basiert auf der Metrik M_3, durch Literaturrecherche der aktuellen Situation und subjektiver Bewertung.

Frage 4.3: Wie hoch sind die Kosten für den Entwickler?

Kosten: *M_5 (Kosten in US-Dollar); M_6 (Skala Effizienz des Deployen)*

$$ZEG_3 = \frac{M_6}{100}$$

Die Effizienz des Deployen und dessen Kosten werden mit einer Skala von 0 bis 10 evaluiert. Dabei wird die Metrik 5 berechnet und dient als Grundlage für die Bewertung.

Effektivitätsindikator der Effizienz aus der Sicht des Entwicklers:

$$I_9 = (ZEG_1 + ZEG_2 + ZEG_3)/3$$

Es folgt die Untersuchung der Effizienz aus der Sicht des Anwenders.

GQM Model für Ziel 4, eine effiziente Dapp (Anwender)			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Effizienz der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Anwenders		
Frage	F4.3	Wie effizient ist die Anwendung?		
Metriken	M5	Transaktionsgebühren	Testung	objektiv
	M6	Effizienz der Anwendung	Skala	subjektiv

Tabelle 7: Tabelle für Fragen und Metriken der Effizienz aus der Sicht des Anwenders

Frage 5.4: Wie effizient ist die Anwendung?

Anwendung: *M_7 (Transaktionsgebühren); M_8 (Effizienz der Anwendung)*

$$I_{10} = ZEG_4 = \frac{M_6}{10}$$

M_6 ist dabei eine Skala von 0 bis 10. Diese bewertet die Effizient der Anwendung basierend auf den Daten von M_7, sowie Literaturrecherche und subjektiver Bewertung. 10 steht dabei für eine ausgesprochen effiziente DApp und 0 für eine teure und langsame DApp.

3.2.5 Benutzerfreundlichkeit

Die Benutzerfreundlichkeit einer neuen Technologie ist für zukünftige Entwickler eine essenzielle Messung. Wie in Kapitel **Error! Reference source not found.** erläutert, ist der Tech-Stack für den Web3 Entwickler deutlich komplexer als für Web2. Lohnt sich der Mehraufwand? Und wird der durchschnittliche Anwender sich dafür begeistern können, ohne dass es zu kompliziert wird? Die Benutzerfreundlichkeit von

Web3 muss daher aus Sicht des Entwicklers (s. Tabelle 8) und des Anwenders (s. Tabelle 9) betrachtet werden.

GQM Model für Ziel 5, eine benutzerfreundliche DApp			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Benutzerfreundlichkeit der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Entwicklers		
Frage	F5.1	Wie hoch ist der Lernaufwand für den Web 3.0 Tech-Stack?		
Metriken	M1	Anzahl Stunden	Daten	objektiv
	M2	Komplexität & Lernaufwand Web 3.0	Skala	subjektiv

Tabelle 8: Tabelle für Fragen und Metriken der Benutzerfreundlichkeit

Frage 5.1: Wie hoch ist der Lernaufwand für den Web3 Tech-Stack?

Lernaufwand: *M_1 (Anzahl Stunden); M_2 (Skala Komplexität & Lernaufwand Web3);*

$$I_{11} = ZEG_1 = \frac{M_2}{10}$$

M_2 evaluiert den Aufwand anhand der Anzahl der Stunden und den damit verbundenen Aufwand nach subjektiver Bewertung. 0 bedeutet, dass der Aufwand exorbitant groß ist und 10, dass der Aufwand im Vergleich zum Ergebnis gering ist.

Es folgt die Evaluierung der Benutzerfreundlichkeit aus der Sicht des Anwenders.

GQM Model für Ziel 5, eine benutzerfreundliche DApp (Anwender)			Messung	Art
Ziel	Zweck	Evaluiere		
	Merkmal	die Benutzerfreundlichkeit der		
	Objekt (Prozess)	DApp		
	Perspektive	aus der Perspektive des Anwenders		
Frage	F5.2	Wie leicht kann der Benutzer die Anwendung bedienen?		
Metriken	M3	Trainierbarkeit	Skala	subjektiv

Tabelle 9: Tabelle für Fragen und Metriken der Benutzerfreundlichkeit aus der Sicht des Anwenders

Frage 5.2: Wie leicht kann der Benutzer die Anwendung bedienen?

Bedienung: *M_3 (Trainierbarkeit)*

$$I_{12} = ZEG_2 = M_3$$

M_3 evaluiert die Trainierbarkeit und Einfachheit der Web3 Bedienung aus der Sicht des Anwenders. 0 bedeutet, dass die Bedienbarkeit für die Mehrheit der Menschen nicht zumutbar ist und 10, dass die Bedienbarkeit auf dem Level von Web2 oder besser ist.

4 Entwurf und Implementierung einer prototypischen Web3-Anwendung

4.1 Vorhaben

Das Ziel dieser Bachelorarbeit ist die Evaluierung von Web3 mithilfe eines Konzepts zur Bewertung von DApps. Dieses Kapitel führt eine eigen erstellte DApp auf Basis von Ethereum ein. Dabei werden die grundlegenden Bausteine von Web3 verwendet. Der Prototyp hat keine wahren Funktionalitäten und ist ein Beispiel zur Veranschaulichung des Konzeptes aus Kapitel 3.

4.2 Entwurf

Das Ziel dieses Prototyps ist es, die aktuellen Möglichkeiten einer klassischen DApp abzubilden. Dabei kommt es nicht auf Komplexität oder Funktionalität an. Es geht um das Erforschen der aktuellen Technologien und Dienste in Web3. Eine DApp in zwei Jahren kann einen komplett anderen Entwurfsplan haben und die heutigen beliebten Dienste in den Schatten stellen. Es geht hierbei nicht darum, die perfekt DApp zu erschaffen, sondern genau das abzubilden, was in der heutigen Zeit (Stand 2022) von der Mehrheit genutzt wird und dies zu bewerten.

Angefangen mit dem Fundament von Web3, der Blockchain. Wie in Kapitel 2.4.6 erwähnt, ist Ethereum zurzeit die mit Abstand beliebteste Blockchain zur Erstellung von DApps und bildet daher auch das Kerngerüst dieses Prototyps. Der Smart Contract wird in Solidity geschrieben.

Die Aufstellung eines Knotens ist, wie in Kapitel 2.6.4 erläutert, kein leichtes Vorhaben. Viele Entwickler arbeiten daher mit Providern wie Infura oder Alchemy. Die Kritik an Providern ist groß, die in dieser Arbeit untersucht wird.

Ein weiterer wesentlicher Punkt ist die Verbindung des Nutzers mit der DApp über Wallets und im engeren Sinne „MetaMask“. Gegründet von ConsenSys, die Entwickler

hinter Infura, ist MetaMask die populärste Wallet und spielt mit ~21 Millionen aktiven Nutzern eine relevante Rolle in Web3. Sie ist ebenfalls Bestandteil des Prototyps.

Genau wie Web2, braucht die Applikation eine Art der Datenspeicherung und Datenabfrage. IPFS ist der Standard unter vielen Web3 Projekten und wird hier verwendet. Die Datenabfrage erfolgt über The Graph. Siehe Abbildung 13 für eine Visualisierung.

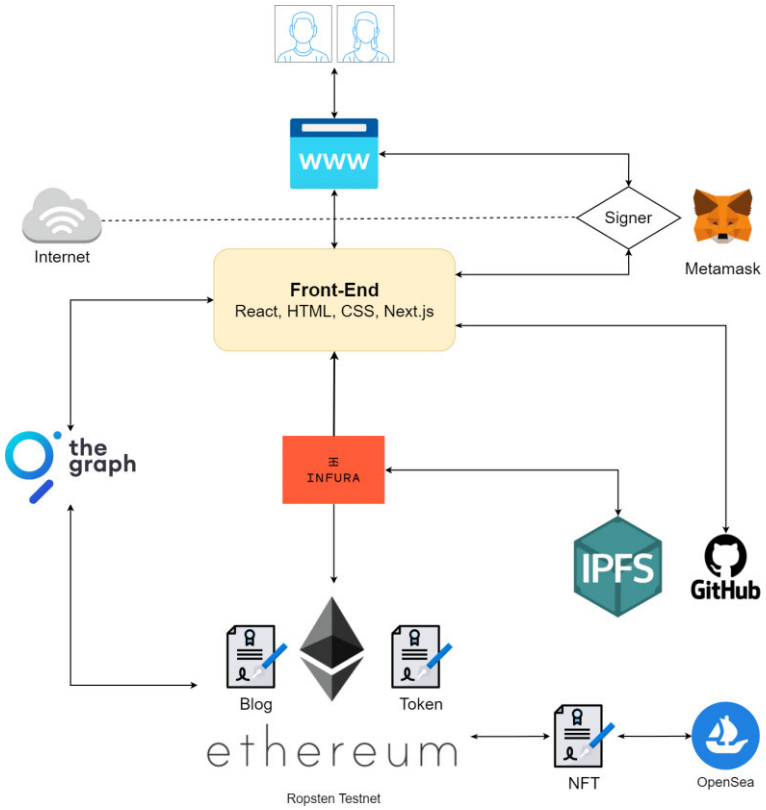

Abbildung 13: Visualisierung des Prototyps

4.3 Prototyp

Die Idee hinter den Prototypen ist ein Web3 Blog für die Hochschule für Angewandte Wissenschaften Hamburg (HAW), wo Studenten eigene Beiträge veröffentlichen können. Die Daten werden dabei nicht auf einer zentralen Datenbank gespeichert, sondern mithilfe von IPFS dezentral. Dies ist nicht die beste Umsetzung der neuen Web3 Technologien, gibt jedoch einen vereinfachten Überblick über die

Funktionalitäten. Aufgrund der fehlenden Erfahrungen mit Web-Entwicklung (JavaScript, Next.js, CSS, React, …), ist der Blog eine Mischung aus mehreren Tutorials von Nader Dabit. Mit dem Hauptmerkmal auf seine Polygon-basierende „Full Stack Web3 Development“-Reihe (vgl. Dabit 2022).

Zugehörig wird unabhängig von dem Blog ein eigener HAW NFT nach dem ERC-1155 Token Standard erstellt. Ein ERC-1155 Token hat mehr Funktionen als ein klassischer NFT nach ERC-721. Diese Funktionen sind jedoch nicht für diese Bachelorarbeit relevant. Für die Entwicklung des NFT wird mit OpenSea gearbeitet, die nur ERC-1155 anbieten. Zusätzlich wurde ein eigener HAW Token nach dem ERC-20 Standard erstellt.

4.3.1 Entwicklung

Für die Entwicklung dieser DApp kommen verschiedene Bausteine zum Einsatz.

Hardhat

Die Entwicklung des Prototyps wird mithilfe von Hardhat durchgeführt. Hardhat ist eine Entwicklerumgebung für die Ethereum-Blockchain, die es ermöglicht, DApps zu testen, kompilieren, deployen und debuggen. Es kreiert ein lokales Ethereum Netzwerk, um die Funktionalitäten ohne jegliche Kosten zu testen (vgl. hardhat.org 2022).

Ethers.js

Die Verbindung der Webapp mit den Funktionalitäten der Blockchain geschieht über Ethers.js, eine Bibliothek für die Ethereum-Entwicklung. Es ermöglicht die Verbindung zu Providern und damit den Knoten, sowie Interaktionen mit dem Smart Contract und der Wallet (vgl. Moore 2022).

Front End Frameworks

Für das Front End wird das Next.js Framework in Verbindung mit React verwendet.

4.3.2 Web3 HAW Blog

4.3.2.1 Front End

Das Front End ist einfach gehalten und beinhaltet eine Startseite (s. Abb. 14) mit einem Button zum Verbinden, Erstellen eines Beitrages und ein Home-Button. Des Weiteren gibt es eine Seite für das Hinzufügen eines Beitrages. Eine genaue Erläuterung der Funktionalitäten befindet sich im Anhang 2.1: Front End.

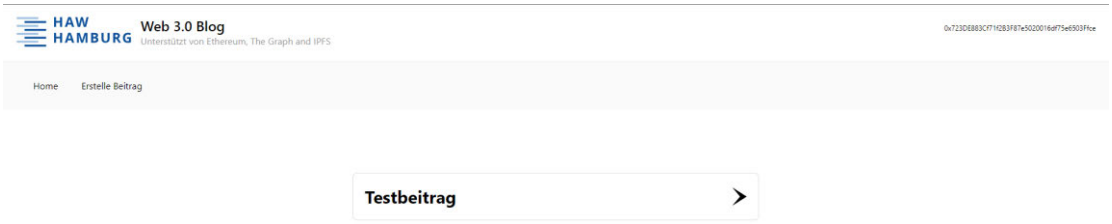

Abbildung 14: Startseite Web3 Blog

4.3.2.2 Back End

Der Smart Contract ist das Herz einer DApp und beinhaltet die wesentlichen Funktionalitäten. Der Smart Contract des Blogs beinhaltet insgesamt 93 Lines of Code.

Der Code-Abschnitt unter Listing 2 ist Standard für viele Smart Contracts und bildet die Basis für die darauffolgenden Funktionen. Der Blog hat die Variablen „name“ und „owner“ in Zeile 8 & 9. Zeile 11 & 12 ist eine importierte Funktion zum Zählen der Beiträge. Die Struktur eines Beitrages beinhaltet die ID, den Titel, den Inhalt (IPFS Hash) und ein boolean, ob es veröffentlicht ist oder nicht. Die Mappings sind Lookups für Beiträge anhand der ID und des IPFS Hashes. Die darunter folgenden Events in Zeile 24 & 25 ermöglichen die Kommunikation vom Smart Contract mit dem Interface. Sie fungieren als ein „Listener“ für Events im Client und updaten den Subgraph in The Graph. Der Konstruktor gibt dem Blog einen Namen und Besitzer (Owner).

contracts > Blog.sol

```
1   //SPDX-License-Identifier: Unlicense
2   pragma solidity ^0.8.0;
3
4   import "hardhat/console.sol";
5   import "@openzeppelin/contracts/utils/Counters.sol";
6
7   contract Blog {
8       string public name;
9       address public owner;
10
11      using Counters for Counters.Counter;
12      Counters.Counter private _postids;
13
14      struct Post {
15          uint id;
16          string title;
17          string content;
18          bool published;
19      }
20
21      mapping(uint => Post) private idToPost;
22      mapping(string => Post) private hashToPost;
23
24      event PostCreated(uint id, string title, string hash);
25      event PostUpdated(uint id, string title, string hash, bool published);
26
27      constructor(string memory _name) {
28          name = _name;
29          owner = msg.sender;
30      }
```

Listing 1: Code-Abschnit des Smart Contracts

Siehe Anhang 2.2: Back End für weitere Erläuterungen einzelner Funktionen und die Integration mit Infura.

4.3.3 HAW NFT

Zusätzlich wurde ein 3D-NFT erstellt, um weitere Elemente von Web3 zu testen. Ein NFT kann in diesem Beispiel als Zugangselement für den Blog gebraucht werden. Dies wurde hier Aufgrund der Komplexität nicht programmiert.

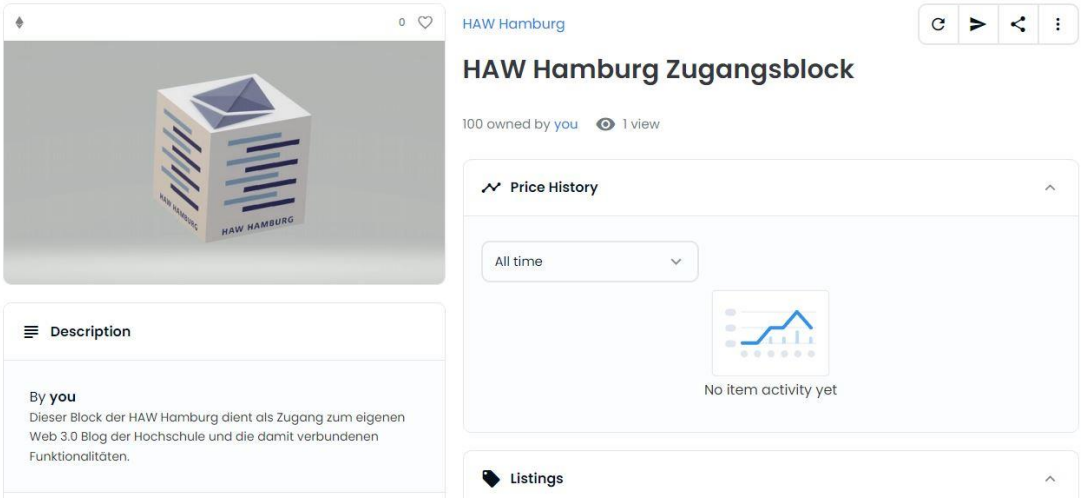

Abbildung 15: HAW NFT auf OpenSea Testnet (testnet.opensea.io 2022)

Dieser NFT wurde 100-mal erschaffen (s. Abb. 15) und ist als Block designt, der sich automatisch um die eigene Achse dreht.

Die Idee hinter einem NFT könnte im Falle einer Universität sein, dass jeder immatrikulierte Student ein NFT bekommt und damit Zugriff auf den Blog erhält. Des Weiteren wäre eine erweiterte Form des Blogs möglich, in der Studenten im Besitz eines solchen Zugangsblockes die Wahlen innerhalb der Universität online transparent abhalten könnten. Masterstudenten der Universität Malta sind zusammengekommen und haben solch eine DApp erstellt, die auch zum ersten Mal von der Universität in Betrieb genommen wurde (vgl. Haig 2020).

4.3.4 HAW Token

Mithilfe des ERC-20 Token Standards wurde ein eigener HAW Token auf Ethereum-Basis deployt (s. Abb. 16). Die Funktionalitäten eines solchen Tokens sind in der Testumgebung eingeschränkt und haben im Rahmen dieser Bachelorarbeit eine rein experimentelle Natur.

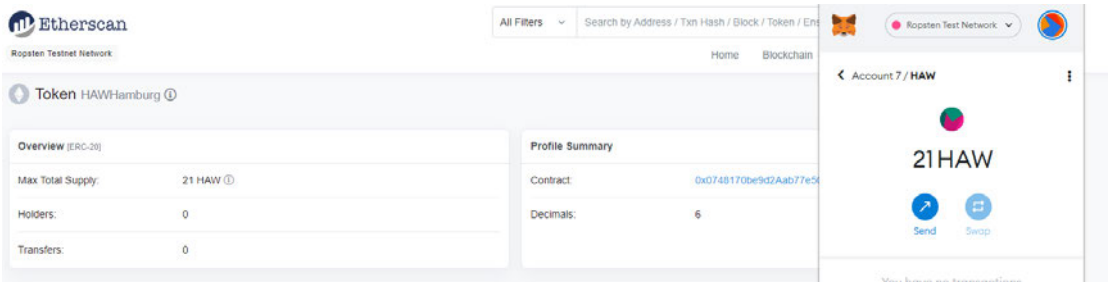

Abbildung 16: HAW-Token Smart Contract Info (vgl. Etherscan.io 2022d)

Einsatzmöglichkeiten wären ein eigener HAW Online-Shop, in welchem der hauseigene HAW Token zum Einsatz kommt. Solch eine Implementierung bedarf jedoch einer fortgeschrittenen Wirtschaftserfahrung rund um das Thema Blockchain und DeFi (decentralized finance).

5 Ergebnisse

5.1 Evaluierung der HAW DApp

Im Folgenden wird die HAW DApp aus Kapitel 4.3 Mithilfe des erstellten Konzepts aus Kapitel 3 evaluiert. Eine Diskussion der Ergebnisse folgt in Kapitel 6. Dieses Kapitel beschäftigt sich hauptsächlich mit dem Blog, jedoch wird der HAW Zugangsblock NFT und der HAW Token ebenfalls teilweise experimentell untersucht.

5.1.1 Evaluierung der Dezentralität

Wie dezentral ist die Ethereum-Blockchain?

Governance-Schicht

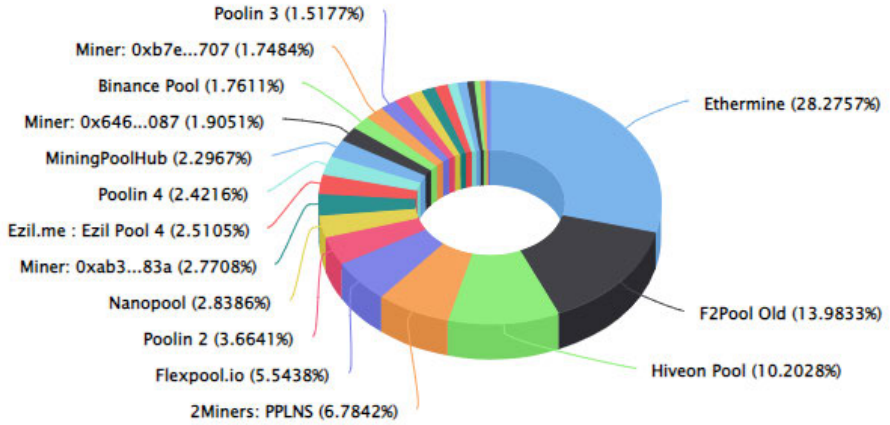

Abbildung 17: Top 25 Miners in den letzten 7 Tagen (Etherscan.io)

Die erste Metrik ist der HHI. Es gibt insgesamt 64 registrierte Miner in den letzten 7 Tagen (Stand 03.08.2022). Zur Berechnung des HHI muss der jeweilige Anteil jedes Miners quadriert und summiert werden.

$$HHI = \sum_{i=1}^{64} (28{,}2757)^2 + (13{,}9833)^2 + (10{,}2028)^2 + \cdots + (0{,}0021)^2 = \mathbf{1244{,}24}$$

Diese Rechnung ergibt laut dem HHI einen „unkonzentrierten Markt“ und damit ein mittleres Maß an Wettbewerb. Um auszuschließen, dass das Ergebnis durch viele einzelne kleine Miner verfälscht ist, ist eine Analyse des Wettbewerbs unter den Top 10 Miner (s. Abb. 17) ebenfalls sinnvoll:

$$HHI = \sum_{i=1}^{10} (36{,}1674)^2 + (17{,}6012)^2 + (12{,}9143)^2 + \cdots + (2{,}7416)^2 = \mathbf{1973{,}91}$$

Die Werte haben einen signifikanten Unterschied und zeigen, dass viele kleine Miner das Ergebnis verfälschen. Es ist daher zum Vorteil, den Wert des HHI der Top 10 für den Zielerreichungsgrad zu verwenden. Die erste Metrik hat einen Wert von $M_1 = 0{,}33$ nach den Vorgaben in Kapitel 3.2.1.

Die zweite Metrik ist der Gini-Koeffizient. Folgende Lorenzkurven lassen sich bilden (s. Abb. 18 & 19).

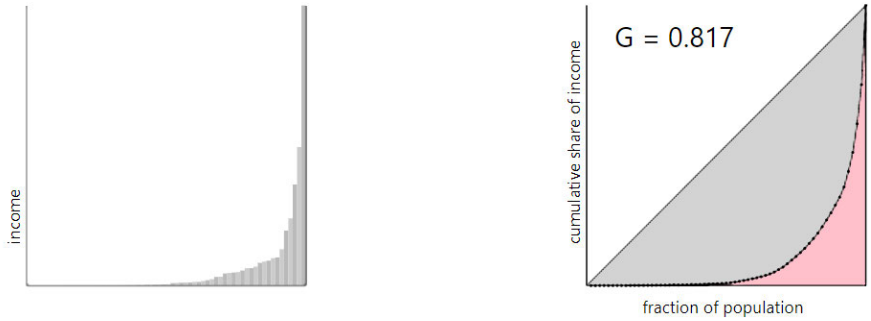

Abbildung 18: Verteilung und Lorenzkurve der 64 Miner (vgl. Shlegeris 2022)

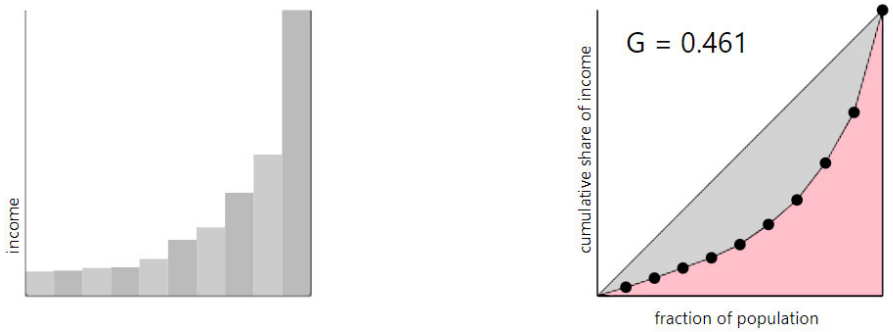

Abbildung 19: Verteilung und Lorenzkurve der Top 10 Miner (vgl. Shlegeris 2022)

Hier lässt sich wiedererkennen, dass die kleinen Miner, die z. T. nur einen Block erstellen, eine große Auswirkung auf das Ergebnis haben. Aufgrund der Tatsache, dass jede Person ein eigener Miner und damit Teil dieser Statistik sein kann, wird für die Evaluierung das Ergebnis der Top 10 Miner gewählt. Einzelne private Personen, die sich keinen Mining-Pool anschließen und dadurch einen kleinen Nebenverdienst verdienen, verfälschen die eigentliche Konkurrenz der großen Mining-Pools. Daher ist *M_2 = 0,46.*

Die letzte Metrik zur Bestimmung der Machtverteilung ist der Nakamoto-Koeffizient.

$$Nakamoto = \min\left\{k \in [1, \dots, k]: \sum_{i=1}^{k} p_i \geq 0{,}51\right\} = 3$$

Anhand der Top 15 Miner lässt sich erkennen, dass Ethermine, F2Pool Old und Hiveon Pool eine gesamte Hashpower von 52,5% haben und es somit die Top 3 Mining-Pools benötigt, um das Netzwerk zu übernehmen (s. Abb. 17). Die letzte Metrik ist daher nach den Vorgaben aus Kapitel 3.2.1 *M_3 = 3 * 2 = 6*.

Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_1 = \left(0{,}66 + (1 - 0{,}46) + \frac{6}{10}\right)/3 = \frac{0{,}66 + 0{,}54 + 0{,}6}{3} = \mathbf{0,6}$$

Verbesserungsprotokoll

Die folgende Metrik ist eine subjektive Bewertung von 0 bis 10. Anhand des Kapitels 2.4.6.1 wurde der Governance-Prozess der Protokollvorschläge erläutert. Trotz der umfangreichen Vertreter der Entscheidungsträger gibt es keine wahre Dezentralität und Demokratie. Eines der Kernversprechen von Web3 ist jedoch die Demokratie (s. Kapitel 2.6.1). Diese Entscheidungsart ist bei Ethereum gescheitert. Der zuvor erwähnte DAO-Hack hat die Governance-Landschaft weiter zentralisiert. Trotz dieses Bruches ist die jetzige Lösung eine gute Alternative. Experten in allen Bereichen besprechen Änderungsvorschläge der Netzwerkteilnehmer. Es ist außerdem im Interesse aller, Kompromisse zu finden und das Netzwerk aufgrund der Token-

Ökonomie aufrechtzuhalten (s. Kapitel 2.6.3). Die abschließende Bewertung der Dezentralität beträgt 6/10 und somit *M_4 = 6.*

Eingesetzt in die Formel des Zielerreichungsgrades: $ZEG_2 = \frac{6}{10} = \mathbf{0,6}$

Der Effektivitätsindikator für die Governance-Schicht:

$$I_1 = (ZEG_1 + ZEG_2)/2 = \frac{(0{,}6 + 0{,}6)}{2} = \mathbf{0,6}$$

Netzwerkschicht

Die Knoten zum Aufrechterhalten des Netzwerkes können weltweit aufgestellt werden. Oftmals gibt es jedoch eine Konzentration der Knoten in Ländern mit attraktiverer Kondition. Dies gilt es zu untersuchen.

Eine Zentralität im Bereich der Knotenaufstellung kann ein Risiko sein. China hat z. B. das Bitcoin-Mining 2021 verboten und verschiedene große Mining-Operationen gestoppt. Die Regierung begründet dies mit dem Streben nach Kohlenstoffneutralität und sieht Krypto-Mining als „extrem schädlich“ (vgl. Schesswendter 2022). China hatte bis zu einem gewissen Punkt 65 % der Hashpower von Bitcoin und ein Abstellen aller Knoten hätte starke Konsequenzen für das Netzwerk. Trotz des Verbots macht China 2022 noch immer 21 % der weltweiten Bitcoin-Hashpower aus. Operationen wurden in den Untergrund verlegt. Sollte ein Land folglich das Krypto-Mining verbieten, hängt die Auswirkung stark von der Motivation der jeweiligen Regierung ab, es durchzusetzen (vgl. Schesswendter 2022).

Für Ethereum gibt es eine starke Konzentration in den USA mit knapp ~50 % der bereitgestellten Knoten (vgl. Etherscan.io 2022c). Metrik 6 bestimmt den Prozentanteil des Top-Landes und beträgt daher *M_6 = 50,87 %*. Zur Bestimmung der Ungleichheit wird der Gini-Koeffizient verwendet (s. Abb. 20). Es wird sich auf die Ungleichheit der Top 10 Länder fokussiert.

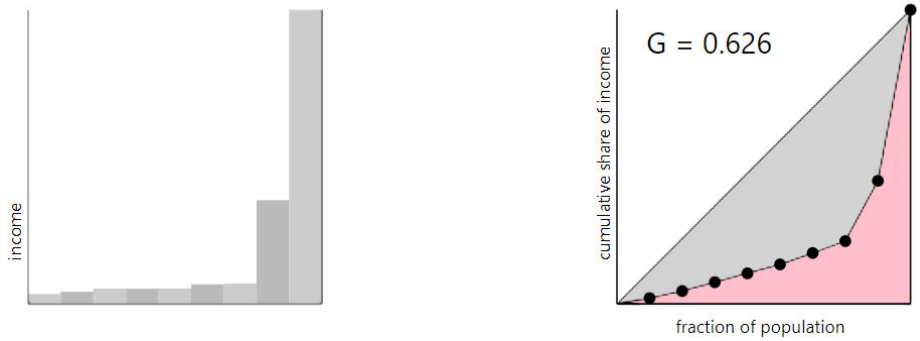

Abbildung 20: Distribution und Lorenzkurve der Top 10 Länder und dessen Knotenaufstellung (vgl. Shlegeris 2022)

Das Ergebnis zeigt eine klare Ungleichheit mit einem Koeffizienten von *G = 0,626* (s. Abb. 20). Metrik 5 ist daher $M_5 = 0,63$.

Eingesetzt in die Formel für den Zielerreichungsgrades und Effektivitätsindikators:

$$I_2 = ZEG_3 = \left((1 - 0{,}63) + \left(1 - \frac{50{,}87}{100}\right)\right)/2 = \frac{0{,}37 + 0{,}49}{2} = \mathbf{0,43}$$

Operative Schicht

Speicherbeschränkung

Um Teil des Ethereum-Netzwerkes zu werden und als Miner zu fungieren, muss ein eigener Knoten aufgestellt werden. Es gibt „Full Nodes“ und „Archive Nodes“. Letzteres besitzt alle historischen Daten seitdem Genesis Block und eine Größe von 11,4 Terrabyte (Stand 04.08.2022). Um als Miner zu agieren, reicht jedoch ein „Full Node“ aus. Dieser bildet die letzten 128 Blöcke der Ethereum-Blockchain ab und ist zurzeit ~837 GB groß (Stand 04.08.2022) (vgl. Sen 2022; Etherscan.io 2022b). Damit ist $M_7 = 837\ GB$.

Die Wachstumsrate beträgt zurzeit ~0,54 GB pro Tag und damit etwas mehr als 15 GB pro Monat (s. Anhang 3.1: Berechnung der Wachstumsrate). Damit ist $M_8 = 0,54\ GB$.

Mithilfe der genannten Metriken lässt sich nun die Zentralität des Speichers bewerten. Für das Aufstellen eines Knotens werden 16 GB+ RAM, eine CPU mit 4+ Kernen, eine

Bandbreite von mindestens 25Mbits/s und eine schnelle SSD mit 1Tb Speicher empfohlen. Der gETH Client hat Möglichkeiten, die Größe von Zeit zu Zeit mithilfe des sogenannten „pruning“ zu reduzieren (vgl. Sen 2022). Trotz der Speichereinsparungen sind die Voraussetzungen noch hoch. Es wird angenommen, dass ein Computer vorhanden ist. Für die Erweiterung des Speichers wird hier eine SSD benötigt. Diese kosten zurzeit zwischen 100 und 150€ (1 TB, Stand 08.2022). Dies ist nach subjektiver Bewertung mit dem durchschnittlichen Gehalt vereinbar und folglich wird die Dezentralität des Speichers bzw. die Möglichkeiten an dem Netzwerk teilzunehmen mit einer 8/10 bewertet. Die Metrik 9 beträgt daher $M_9 = 8.$

Eingesetzt in die Formel für den Zielerreichungsgrades: $ZEG_4 = \frac{8}{10} = \mathbf{0,8}$

Knotenverteilung

Zurzeit gibt es 5411 Ethereum-Knoten (Stand 09.08.2022) und zwei Drittel werden auf Cloud-Anbietern gehostet (vgl. ethernodes.org 2022b). Dies ergibt $M_{10} = 3583$ und $M_{11} = 5411.$ Amazon dominiert das Hosting Geschäft und hostet 57,2% aller Knoten im Cloud-Bereich (vgl. ethernodes.org 2022a). Insgesamt stellt Amazon 35% aller Knoten des kompletten Ethereum-Netzwerkes bereit und damit ist M_{12} = 35%. Siehe Anhang **Error! Reference source not found.** für einen Snapshot der Statistiken.

Eingesetzt in die Formel für den Zielerreichungsgrades:

$$ZEG_5 = \left(\left(1 - \frac{3583}{5411}\right) + \left(1 - \frac{35}{100}\right)\right)/2 = \frac{0{,}34 + 0{,}65}{2} = \mathbf{0,5}$$

Effektivitätsindikator der operativen Schicht:

$$I_3 = (ZEG_4 + ZEG_5)/2 = \frac{0{,}8+0{,}5}{2} = \frac{1{,}3}{2} = \mathbf{0,65}$$

Ist ein eigener Knoten aufgestellt?

Für diese Anwendung wurde kein eigener Ethereum-Knoten aufgestellt und alternativ der Provider Infura genutzt. Metrik 13 ist daher $M_{13} = 0$ nach den Vorgaben der binären Abfrage aus Kapitel 3.2.1.

Eingesetzt in die Formel des Zielerreichungsgrades: $ZEG_6 = \mathbf{0}$

Sind die verwendeten Provider dezentral?

Infura ist ein bedeutsames Tool für die heutige Web3-Entwicklung und bietet „nodes-as-a-service“. Einen eigenen Knoten aufzustellen kann teuer, zeitaufwendig und schwer zu bedienen sein. Jedoch führt diese Abhängigkeit zu einem Machtungleichgewicht. Infura kann als einzelne Entität und Anbieter dieses Service alle Knoten vom Netz ziehen (vgl. Duperrin 2022). Dies ist im ersten Moment ein unrealistisches Szenario, führt jedoch zu weiteren Problemen.

Ausfälle haben in mehreren Beispielen für kurzzeitige Abschaltungen eines großen Teiles des Ethereum DApp-Ökosystems gesorgt. Große Namen wie Binance und MetaMask hatten limitierte Funktionen (vgl. Duperrin 2022).

Des Weiteren kann Infura als zentrale Einheit von Regierungen gesteuert werden und bestimmte Operationen zensieren. Das ist ein großer Verstoß gegen die Kernprinzipien von Web3. Insgesamt ist Infura ein nützliches Tool für Entwickler, das jedoch durch die hohe Nachfrage unausweichlich ein zentraler Punkt im Ökosystem wurde (vgl. Duperrin 2022). Daher erhält die Dezentralität des Providers Infura eine Bewertung von 3/10. Die Metrik hat einen Wert von $M_{14} = 3$.

Eingesetzt in die Formel für den Zielerreichungsgrades: $ZEG_7 = \frac{3}{10} = \mathbf{0,3}$

Effektivitätsindikator: $I_4 = (ZEG_6 + ZEG_7)/2 = \frac{0+0,3}{2} = \frac{0,3}{2} = \mathbf{0,15}$

Wie dezentral sind die angebundenen Dienste/Protokolle?

Dienste & Protokolle ohne Blockchain

Die Wallet MetaMask musste sich Sanktionen von Regierungen hingeben (s. Kapitel 2.6.4) und hat dadurch, dass MetaMask von ConsenSys entwickelt wurde, die gleichen Nachteile wie der Provider Infura. MetaMask verwendet für die Transaktion vordefinierte Knoten von Infura. Dies kann jedoch in den Einstellungen geändert

werden und bietet damit mehr Spielraum. Aufgrund dessen, bekommt MetaMask eine Bewertung von 6/10.

GitHub hingegen ist ein verteiltes System. Projekte sind im Falle eines Ausfalls nicht mehr erreichbar und die Arbeit kann nicht fortgesetzt werden. Im Falle eines totalen Shutdowns wäre der Code jedoch noch auf den lokalen Rechnern vorhanden und kann auf einer ähnlichen Plattform wechseln. GitHub ist daher nur für den Entwickler relevant und hat keine Auswirkung auf die DApp. Durch die fehlende Relevanz wird GitHub nicht evaluiert (vgl. Streza 2022).

Der NFT-Markplatz OpenSea ist eine vollkommen zentrale Einheit und unterliegt der Willkür des Unternehmens. OpenSea kann Kunst verbieten (vgl. Marlinspike 2022), bestimmte Nutzer mithilfe von Geolokalisierung ausschließen (s. Kapitel 2.6.4) und speichert Metadaten vieler NFTs zentral auf einem Server (vgl. George 2022). Aufgrund dessen, bekommt OpenSea eine Bewertung von 0/10.

Hinsichtlich zusätzlicher Protokolle, wurde IPFS genutzt. IPFS verwendet ähnliche Technologien wie eine Blockchain. Jeder kann dem Netzwerk beitreten und hochgeladen Daten können nicht mehr geändert werden. Lediglich eine Versionisierung ist möglich. Nicht jeder Teilnehmer des Netzwerkes hat alle Daten und Dokumente. Teilnehmer, die Zugriff auf ein Dokument möchten, speichern es ebenfalls mit dessen Hash im Cache. Die Datei geht dann verloren, sollten alle Teilnehmer mit der Datei sich vom Netzwerk trennen. Es ist daher vollkommen dezentral und erhält eine Bewertung der Dezentralität von 10/10.

Eingesetzt in die Formel für den Zielerreichungsgrades:

$$ZEG_8 = \sum_{i=1}^{3} \frac{M_{14+i}}{10} = \left(\frac{M_{15}}{10} + \frac{M_{16}}{10} + \frac{M_{17}}{10}\right)/3 = \left(\frac{6}{10} + \frac{0}{10} + \frac{10}{10}\right)/3 = \frac{1{,}6}{3} = \mathbf{0,53}$$

Protokolle (Blockchains)

The Graph		*Auswertung*
Konsensus	PoS	
HHI	$\sum_{i=1}^{10}(24{,}52)^2 + (24{,}45)^2 + \ldots + (2{,}39)^2 = \mathbf{1613{,}13}$	$M_{18} = 0{,}33$
Gini	**0,419**	$M_{19} = 0{,}42$
Nakamoto (>66)	$\min\left\{k \in [1,\ldots,168]: \sum_{i=1}^{168} p_i \geq 0{,}66\right\} = \mathbf{16}$	$M_{20} = 10$ (max. 10)

Tabelle 10: Berechnung der Metriken zur Evaluierung von Dezentralität

Die Erhebung der Daten erfolgt aus der offiziellen Liste der Netzwerkteilnehmer (vgl. Graph Explorer 2022). Dabei wurden die Top 10 aktuellen Indexer für den HHI und Gini-Koeffizenten genutzt (Stand 09.08.2022). Ein Indexer ist dabei ein Knotenbetreiber, welcher die Graph Tokens (GRT) staked. Eine ausführliche Erläuterung des Graph Explorers und die Deutung der Daten befindet sich in der offiziellen Dokumentation (vgl. The Graph Docs 2022).

Die Daten zeigen einen Mangel an Wettbewerb und eine überdurchschnittliche Ungleichheit. Durch den Einsatz von PoS ist die Möglichkeit einer Übernahme des Netzwerkes jedoch unwahrscheinlich. Es müssten die Top 16 Netzwerkteilnehmer zusammenkommen.

Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_9 = \left((1 - M_{18}) + (1 - M_{19}) + \frac{M_{20}}{10}\right)/3 = \left((1 - 0{,}33) + (1 - 0{,}42) + \frac{10}{10}\right)/3$$
$$= \frac{0{,}66 + 0{,}58 + 1}{3} = \frac{2{,}24}{3} = \mathbf{0{,}75}$$

Effektivitätsindikator:

$$I_5 = \frac{\left(ZEG_8 + \sum_{j=1}^{1} ZEG_{8+j}\right)}{n+1} = \frac{(0{,}3 + 0{,}75)}{1+1} = \mathbf{0{,}53}$$

5.1.2 Evaluierung der Sicherheit

Wie sicher ist die Ethereum-Blockchain?

Der Nakamoto-Koeffizient ist eine fundamentale Metrik zur Bestimmung der Sicherheit von Blockchain-Netzwerken (s. Kapitel 3.2.2). Im Folgenden wird untersucht, wie viele Miner sich zusammenschließen müssen, um eine bestimmte Anzahl der Hashpower zu erlangen (s. Tabelle 11).

Prozent	**Formel**	**Anzahl**	**Ausmaß**
>33% (Metrik 1)	28,3% + 14% = 42,3%	2	Eine 33% Attacke ist gefährlicher für PoS Netzwerke. Mit 33% der Hashpower kann das Netzwerk kurzzeitig lahmgelegt werden (Bunin 2019).
>50% (Metrik 2)	28,3% + 14% + 10,2% = 52,5%	3	Die drei Top Miningpools müssen zusammenkommen, um die Blockchain nach Belieben ändern zu können. >50% ermöglicht „double-spending“, das Benutzen von schon ausgegebenen ETH (Bunin 2019).
>66% (Metrik 3)	28,3% + 14% + 10,2% + 6,8% + 5,5% + 3,7% = 68,5%	6	Dies ist nötig, um einen „51% Angriff“ in einem PoS Netzwerk auszuführen. Das ist zurzeit noch nicht relevant. Ethereum wird jedoch in Zukunft auf PoS umsteigen (Bunin 2019)

Tabelle 11: Berechnung der Nakamoto-Koeffizienten und dessen Ausmaß

Ethereum wurde 2016 erfolgreich angegriffen (s. Kapitel 2.4.6). Heutzutage ist ein solcher Angriff um ein Vielfaches teurer und kaum profitabel. Es gibt jedoch immer

wieder Unstimmigkeiten in der Community, die mit Bedacht beobachtet werden sollten. Im Dezember 2021 wurde das „London Update“ eingeführt, das die Belohnungen für die Miner reduzierten, in einem Versuch, die Gas-Kosten zu senken. Dies hatte eine große Debatte ausgelöst und verschiedenen Miner haben für einen 51%-Angriff plädiert, um dieses Update zu verhindern. Angeblich hatte die Gruppe genug Hashpower, um diesen Angriff durchzuführen. Die Drohung wurde am Ende jedoch nicht erfüllt. Das Netzwerk blieb verschont und das Update wurde eingespielt. Solche Drohungen sollten jedoch nicht unterschätzt werden. Da Ethereum plant auf PoS zu wechseln und verschiedene defensive Mittel gegen einen solchen Angriff hat (vgl. CoinMarketCap 2021), wird die Sicherheit der Ethereum-Blockchain zurzeit mit einer 8/10 bewertet (Metrik 4). Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_1 = \left(\frac{2*4}{10} + \frac{3*2}{10} + \frac{6*1{,}5}{10} + \frac{8}{10}\right)/4 = \frac{(0{,}8 + 0{,}6 + 0{,}9 + 0{,}8)}{4} = \mathbf{0,78}$$

Wie sicher sind die Smart Contracts?

Die Ergebnisse des Scans ergeben, dass es keine kritischen Schwachstellen in den Smart Contracts gibt (s. Abb. 21).

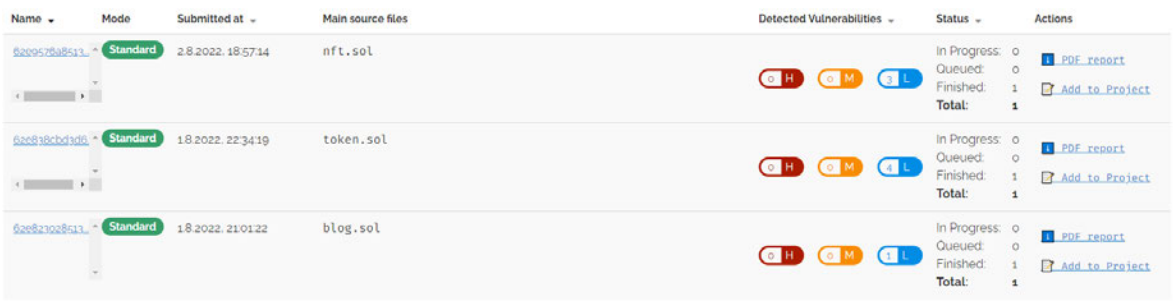

Abbildung 21: Ergebnisse der drei Smart Contract Audits (MythX.io)

Im Rahmen dieser Bachelorarbeit wurde für den Smart Contract Audit die automatische Erkennungssoftware MythX von ConsenSys gewählt. Die kostenlosen Anbieter sind oftmals nicht mehr in Betrieb oder nicht besonders aussagekräftig. Für die drei Smart Contracts des Blogs, des NFT und des Tokens belaufen sich die Kosten

auf $9,99 für eine automatische Untersuchung. Diese Untersuchung kann viele bekannte Schwachstellen wie unter anderem „Unchecked call“, „Re-entrancy“ oder „Bad coding patterns“ erkennen (vgl. Oualid 2022). Siehe Anhang 3.3: MythX Smart Contract Audit Report für den vollständigen Bericht des Blogs.

Da in keinem der Smart Contracts Schwachstellen gefunden wurden, erhalten die Metriken nach den Vorgaben in Kapitel 3.2.2 einen Wert von $M_{5,6,7} = 1$. Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_2 = \sum_{i=1}^{3} M_{4+i} = M_5 + M_6 + M_7 = 1 + 1 + 1 = \mathbf{1}$$

Effektivitätsindikator: $I_6 = (ZEG_1 + ZEG_2)/2 = \frac{0{,}775+1}{2} = \mathbf{0,89}$

5.1.3 Evaluierung der Funktionalität

Funktionieren die Smart Contracts?

Angewendet wird der Solidity Coverage Checker von sc-forks (cgewecke 2019). Ein Solidity Coverage Checker ist ebenso bedeutsam für die Funktionalität, als für die Sicherheit des Smart Contracts. Es untersucht, ob der gesamte Code mit Tests abgedeckt ist. Dies kann eine aktuelle Übersicht über alle Funktionalitäten schaffen. Der Solidity Coverage Checker hat nach dem zweiten Durchlauf eine Coverage von 90,65 % und damit ist $M_1 = 90{,}65\ \%$.

Nun gilt es zu untersuchen, ob diese Tests auch einwandfrei funktionieren. Das Ausführen der Unit-Tests funktioniert zu 100 %. Damit ist M_2 = 100 %. Für die genaue Vorgehensweise, sowie die Tabellen des Coverage Checkers und die Auflistung der Unit-Tests siehe Anhang 3.4: Smart Contracts.

Eingesetzt in die Formel für den Zielerreichungsgrades:

$$ZEG_1 = \left(\frac{90{,}65\%}{100} + \frac{100\%}{100}\right)/2 = \frac{0{,}91 + 1}{2} = \mathbf{0,96}$$

Funktionieren die angebundenen Dienste?

Die Datenspeicherung mit IPFS funktioniert im Testnetzwerk aus unerklärlichen Gründen nicht. Trotz einer vollständigen Integrierung und Analysierung der offiziellen Dokumentation scheint es Probleme beim public Gateway zu geben. Das public Gateway ist der Zugang zum öffentlichen Netzwerk. Trotz des Aufsetzens eines eigenen Knotens und der Implementierung nötiger Funktionen im Programmcode funktioniert der Upload nicht. Lokal klappt das Erstellen eines Beitrages und die Daten werden in einer lokalen Testumgebung gespeichert. IPFS funktioniert jedoch nicht und bekommt eine Bewertung von 0/10. Damit ist $M_3 = 0$. Siehe Anhang 3.5.1: IPFS für die genauere Problembeschreibung und die Aufstellung eines IPFS Knotens.

Die Installation und Integrierung von The Graph ist weniger komplex. Die Technologie dahinter ist jedoch kompliziert. Die Erstellung eines sogenannten „Subgraphs“ hat funktioniert und das dazugehörige GraphQL Schema zur Definierung der Daten wurde geschrieben. Siehe Anhang 3.5.2: The Graph für eine Erläuterung.

Jedoch funktionieren die Abfragen nicht, da es keine Daten gibt. The Graphs Funktionalität baut darauf auf, dass die Daten korrekt gespeichert werden. Aufgrund der Tatsache, dass dies mit einer funktionalen IPFS Datenspeicherung funktionieren würde, bekommt The Graph eine Bewertung von 6/10 und $M_4 = 6$.

Eingesetzt in die Formel des Zielerreichungsgrades: $j \in [1, \dots, m]: ZEG_{1+j} = \frac{M_{2+j}}{10}$

m = 2 (IPFS und The Graph). Für j = 1 (IPFS): $ZEG_2 = \frac{M_3}{10} = \frac{0}{10} = \mathbf{0}$

Für j = 2 (The Graph): $ZEG_3 = \frac{M_4}{10} = \frac{6}{10} = \mathbf{0,6}$

Effektivitätsindikator:

$$I_7 = \left(ZEG_1 + \left(\sum_{j=1}^{2} ZEG_j \right) \right) / (2+1) = \frac{0{,}96 + (0 + 0{,}6)}{3} = \mathbf{0,52}$$

Nun erfolgt die Evaluierung der Funktionalitäten aus der Sicht des Anwenders.

Funktionieren die einzelnen Elemente der Website?

Funktion	Lokal	Testnetzwerk	Gesamt
Verbinden	Ja – 100%	Ja – 100%	100%
Erstellen eines Beitrages	Ja – 100%	Ja – 100%	100%
Bild einfügen	Ja – 100%	Ja – 100%	100%
Auflistung der Beiträge	Ja – 100%	Ja – 100%	100%
Anzeigen eines Beitrages	Ja – 100%	Nein – 0%	50%
Bearbeiten eines Beitrages	Ja – 100%	Nein – 0%	50%
Home-Button	Ja – 100%	Ja – 100%	100%
Gesamt	**100%**	**~71%**	**~86%**

Tabelle 12: Evaluierung der Website und dessen Funktionalitäten

M_5 ist damit 86%. Eingesetzt in die Formel des Zielerreichungsgrades und Effektivitätsindex:

$$I_8 = ZEG_5 = \left(\frac{86}{10}\right) = \mathbf{0,86}$$

5.1.4 Evaluierung der Effizienz

Wie schnell kann die Blockchain Transaktionen validieren?

Um diese Metrik bewerten zu können, ist ein Vergleich mit den Konkurrenten von Ethereum nötig. Es wird im Folgenden die Transaktionen pro Sekunde (TPS) und der jeweilige Marktanteil der Blockchains in den letzten 4 Jahren verglichen (s. Tabelle 13).

Blockchain	TPS	Marktanteil				
		01.01.2019	01.01.2020	01.01.2021	01.01.2022	Heute 08.2022
Ethereum	13	11,90%	7,63%	10,70%	19,23%	18,47%
Solana	50k	/	/	0,01%	2,35%	1,26%
Cardano	266	0,80%	0,45%	0,70%	1,97%	1,57%
Binance Smart Chain	39	0,64%	1,14%	0,70%	3,76%	4,48%
Polkadot	100k - 1M	/	/	0,90%	1,20%	0,83%
Ethereum 2.0	100k	/	/	/	/	/

signifkante Steigerung
signifkanter Verlust
keine signifikante Veränderung

Tabelle 13: Vergleich der Effizienz von vier Ethereum-Konkurrenten und Marktanteil-Entwicklung

Ethereum hat als älteste Blockchain in diesem Vergleich die langsamste Transaktionszeit. Trotz der steigenden Skalierungsprobleme (s. Kapitel 2.6.4), dominiert Ethereum den Markt und sorgt sogar für einen Rückgang von Konkurrenten mit über 3500x mal schnellerer Transaktionszeit. Ein Grund könnte der Ruf sein und dass damit verbunde Upgrade auf Eth 2.0. Berechnungen zeigen, dass Ethereum 2.0 auf Basis von PoS über 100.000 Transaktion pro Sekunde ausführen kann. Diskutiert wird dies in Kapitel 6, in welchem die Marktanteile eine Rolle spielen werden.

Die objektive Betrachtung zeigt jedoch, dass das Ethereum-Netzwerk mit 13 TPS weit unter dem aktuellen Durchschnitt liegt. Metrik1 ist daher $M_1 = 13$. Demzufolge bekommt Ethereum zum jetzigen Zeitpunkt eine Bewertung von 4/10. Die Metrik ist $M_2 = 4$.

Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_1 = \frac{4}{10} = \mathbf{0,4}$$

Wie hoch ist der Energieaufwand?

Aufgrund des Konsensmechanismus benötigt Ethereum eine große Menge von Hashpower und den damit verbundenen Strom. Der Stromverbrauch ist seit 2021 stark angestiegen und liegt zurzeit bei knapp 85 TWh pro Jahr (s. Abb. 22). Metrik 3 liegt daher bei $M_3 = 85\ TWh$.

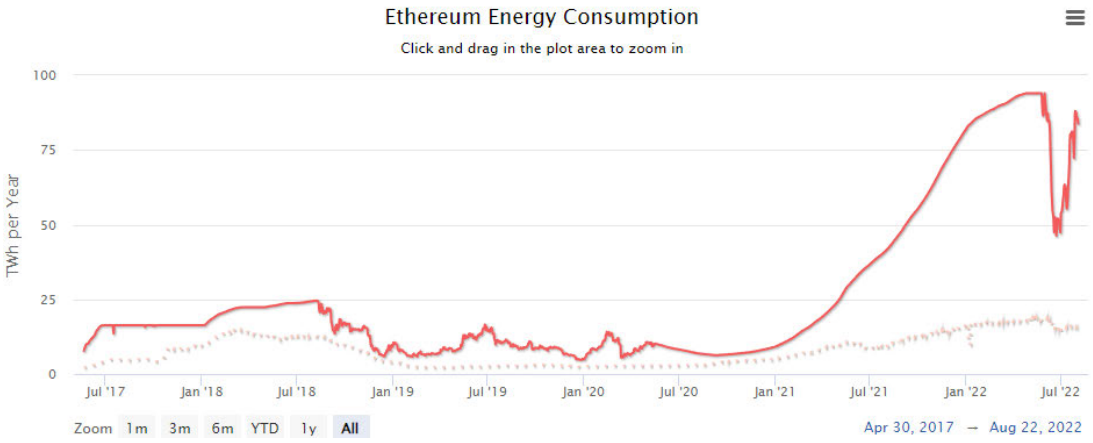

Abbildung 22: Ethereum Energy Consumption Index (Digiconomist 2022)

Dies ähnelt dem Stromverbrauch des Landes Finnland oder Belgien (vgl. countryeconomy.com 2021). Eine einzige Transaktion ist vergleichbar mit dem Streamen von 17,333 Stunden auf YouTube (vgl. Digiconomist 2022).

In der Zukunft soll Ethereum 2.0 diesen Stromverbrauch um 99,9% senken und nur 0,01 TWh pro Jahr an Strom benötigen (vgl. ethereum.org 2022). Diese Bewertung gilt jedoch der Gegenwart und Ethereum mit PoW bekommt eine 0/10 im Bereich des Energieverbrauchs. Metrik 2 hat daher einen Wert von $M_4 = 0$.

Eingesetzt in die Formel für den Zielerreichungsgrad: $ZEG_2 = \frac{4}{10} = \mathbf{0}$

Wie hoch sind die Kosten für den Entwickler?

Das Deployen eines Smart Contracts auf das Ethereum-Netzwerk kostet Gas und kann in Zeiten hoher Aktivitäten stark ansteigen. Diese Bachelorarbeit arbeitet auf Testnetzwerken, sodass der eigentliche Deployment-Preis berechnet werden muss. Jeder deployte Smart Contract hat einen Transaktions-Hash, der es mithilfe von Analyseseiten ermöglicht, Metadaten zu erfahren. Um den Smart Contract für den Blog auf das Ethereum-Mainnet zu deployen, würde es aktuell (04.08.2022) $ 86,33 kosten. Metrik 5 ist daher $M_5 = \$\ 86{,}33$. Der HAW Token Contract hingegen $ 49,02 und der HAW Zugangsblock $ 8,09. Siehe Anhang 3.6: Berechnung der Deployment-Kosten für die genaue Kalkulierung der Preise.

Dies sind die Kosten in einem unausgelasteten Netzwerk. Es sind neben eventueller Anschaffung eines Knotens oder die Nutzung eines Providers die einzigen Kosten für den Entwickler. Im Falle eines komplexeren Beispiels kann der Preis jedoch ansteigen. Es ist im Hinterkopf zu behalten, dass der Prototyp kaum Funktionalitäten hat. Durch die starken Schwankungen der Preise und die relativ hohen Kosten für 93 LOC wird die Effizienz des deployen mit 4/10 bewertet. Metrik 3 hat daher einen Wert von $M_6 = 4.$

Eingesetzt in die Formel für den Zielerreichungsgrad:

$$ZEG_3 = \frac{4}{10} = \mathbf{0,4}$$

Effektivitätsindikator:

$$I_9 = (ZEG_1 + ZEG_2 + ZEG_3) \,/\, 3 = (0{,}4 + 0 + 0{,}4)/3 = \frac{0{,}8}{3} = \mathbf{0,27}$$

Als nächstes folgt die Evaluierung der Effizienz aus der Sicht des Anwenders.

Ein entscheidender Punkt für den Anwender sind die Transaktionsgebühren. Jede Ausführung des Smart Contracts kostet den Nutzer Gas. Je nach Aktivitäten, kann der Preis exponentiell ansteigen, und der Konkurrenzkampf in den nächsten Block zu kommen ist hoch. Wie das Beispiel in Kapitel 2.6.4 gezeigt hat, in welcher die Gebühren für die Nutzer kurzzeitig fünf-stellig waren. Folgende Tabelle basiert auf einen Ethereum-Preis von $ 1.612,20 und 25 gwei pro Einheit Gas. Folgende Tabelle berechnet die Kosten für das Erstellen eines Beitrages:

Funktionalität	**Gas**	**Kosten**
Beitrag posten & Beitrag verändern	Min. 300.000	300.000 * 25 gwei = 7.500.000 gwei = 0,010685 ETH 0,0106585 ETH * $ 1.612,20 = **$ 19,18**

Tabelle 14: Berechnung der Kosten pro Funktionalität der Website (Etherscan.io 2022a)

Mit M_7 = *$ 19,18* ist dies ist ein hoher Preis für solch eine unkomplizierte Aktion. In dieser Hinsicht wird die Effizienz für den Anwender mit 1/10 bewertet. Damit ist M_8 = *1.*

Eingesetzt in die Formel für den Zielerreichungsgrad und Effektivitätsindikator:

$$I_{10} = ZEG_4 = \frac{1}{10} = \mathbf{0,1}$$

5.1.5 Evaluierung der Benutzerfreundlichkeit

Wie komplex ist die Web3 Entwicklung?

Das Erstellen eines Prototyps ist durch die verschiedenen neuen Technologien und Tools erschwert. Ebenfalls spielt die mangelnde Erfahrung mit JavaScript eine große Rolle. Es lässt sich eine Gesamtstundenzahl der Recherche der allgemeinen Thematik und Programmierung des Prototypens auf ca. 186 Stunden errechnen. Eine ausführliche Einteilung der Stunden mit Kommentaren zur Komplexität befindet sich im Anhang 3.7: Aktivitätstabelle.

Die Komplexität ist hoch. Tutorials für einfache DApps fangen bei zwei Stunden an und bieten ein absolutes Grundgerüst, wobei Erfahrung in JavaScript, React, HTML oder Node.js vorausgesetzt ist. Web3 führt viele neue Begriffe und Technologien ein. Entwickler müssen sich mit verschiedenen unausgereiften Tools zurechtfinden und neue Systeme wie IPFS verstehen und umsetzen können. Der Aufwand für eine einzelne Website zur Erstellung von einfachen Beiträgen ist höher als erwartet. Mehr zu dem Thema der Komplexität wird in Kapitel 6 diskutiert. Die Komplexität und Benutzerfreundlichkeit der Technologien und Tools wird mit 3,5/10 bewertet. Die Metrik hat daher einen Wert von M_1 = *3,5.*

Effektivitätsindikator: $I_{11} = ZEG_1 = \frac{3,5}{10} = \mathbf{0,35}$

Ebenso wie der Entwickler, muss der Anwender sich mit neuen Tools und Begriffen beschäftigen. Ein Anwender braucht kein grundlegendes Wissen über die eigentliche Technologie, sondern möchte in den meisten Fällen eine reibungslose und einfache

Bedienung. Der erste Punkt wäre das Installieren einer Wallet. Jeder Anwender braucht eine Ethereum-Adresse und MetaMask bietet eine einfache Anleitung. Jedoch wird der Anwender direkt mit der Möglichkeit konfrontiert, alles zu verlieren, sollte der private Schlüssel verloren gehen oder geklaut werden. Dies ist ein erheblicher Nachteil gegenüber Web2 Anwendungen und dessen „Passwort vergessen"-Möglichkeiten.

Außerdem sind die Marktplätze recht komplex. Das Kaufen von Ethereum benötigt mehrere Identifizierungen und Vertrauen in den Prozess. Nach dem Kauf von Ethereum muss es gegen Gebühren aus dem Marktplatz in die Wallet geschoben werden. Ist dies geschehen, kann der Nutzer sich anmelden und verschiedene Smart Contract Funktionalitäten nutzen. Jede Aktion kostet Gebühren und das kann bei größeren DApps recht komplex werden. Ein Beispiel ist das Kaufen eines NFTs. Vom Kauf des Ethereum bis hin zum Besitz des NFTs auf OpenSea muss der Käufer dreimal Gebühren zahlen. Das ist nicht praktikabel und benutzerfreundlich.

Der durchschnittliche Anwender wird diesen Prozess im jetzigen Zustand nicht dem Web2 bevorzugen und demenstsprechend bekommt die Benutzerfreundlichkeit für den Anwender eine Bewertung von 3/10. Die Metrik hat somit einen Wert von $M_2 = 3$.

$$I_1 = ZEG_1 = \frac{3}{10} = \mathbf{0,3}$$

5.2 Effektivitätsindex-Tabelle

Die Effektivitäts-Tabelle (s. Tabelle 15 & 16) gibt einen Gesamtüberblick aller relevanten Ergebnisse des Kapitels und ist die Grundlage der folgenden Diskussion in Kapitel 6. Die Legende der Tabelle beruht sich auf Kapitel 3.1 (s. Abb. 23).

0-0,2	0,21-0,3	0,31-0,5	0,51-0,7	0,71-0,8	0,81-1
nicht erfüllt	kaum erfüllt	überwiegend nicht erfüllt	mittelmäßig erfüllt	überwiegend erfüllt	voll erfüllt

Abbildung 23: Legende für die Deutung der Effektivitätsindex-Tabelle

Effektivitäts-Tabelle					
Dezentralität	Frage 1.1				
Governance-Schicht	Machtverteilung	ZEG_1	Verbesserungsp.	ZEG_2	
	$M_1 = 0,33$	0,6	$M_4 = 6$	0,6	
	$M_2 = 0,46$				
	$M_3 = 6$				
Effektivitätsindex	$I_1 = 0,6$				
Netzwerkschicht	Knoten	ZEG_3			
	$M_5 = 0,63$	0,43			
	$M_6 = 50,87\%$				
Effektivitätsindex	$I_2 = 0,43$				
Operative Schicht	Speicherbeschränkung	ZEG_4	Knotenverteilung	ZEG_5	
	$M_7 = 837$ GB	0,8	$M_{10} = 3585$	0,5	
	$M_8 = 0,54$ GB		$M_{11} = 5411$		
	$M_9 = 8$		$M_{12} = 35\%$		
Effektivitätsindex	$I_3 = 0,65$				
Knoten	Frage 1.2		Frage 1.3		
	eigener Knoten	ZEG_6	Provider	ZEG_7	
	$M_{13} = 0$	0	$M_{14} = 0,3$	0,3	
Effektivitätsindex	$I_4 = 0,15$				
Dienste/Protokolle	Frage 1.4				
	Dienste/Protokolle	ZEG_8	The Graph	ZEG_9	
	$M_{15} = 6$	0,3	$M_{18} = 0,33$	0,75	
	$M_{16} = 0$		$M_{19} = 0,42$		
	$M_{17} = 10$		$M_{20} = 10$		
Effektivitätsindex	$I_5 = 0,53$				
Sicherheit	Frage 2.1		Frage 2.2		
Blockchain/Smart Contracts	Ethereum	ZEG_1	Smart Contracts	ZEG_2	
	$M_1 = 2$	0,78	$M_5 = 1$	1	
	$M_2 = 3$		$M_6 = 1$		
	$M_3 = 6$		$M_7 = 1$		
	$M_4 = 8$				
Effektivitätsindex	$I_6 = 0,89$				

Tabelle 15: Teil eins der Effektivitäts-Tabelle

Funktionalität	Frage 3.1		Frage 3.2			
Smart Contracts & Dienste/Protokolle	Coverage	ZEG_1	IPFS	ZEG_2	The Graph	ZEG_3
	M_1 = 90,65%	0,96	M_3 = 0	0	M_4 = 6	0,6
	M_2 = 100%					
Effektivitätsindex	I_7 = 0,52					
Anwender	Frage 3.3					
	Website	ZEG_5				
	M_5 = 86%	0,86				
Effektivitätsindex	I_8 = 0,86					

Effizienz	Frage 4.1		Frage 4.2		Frage 4.3	
Blockchain & Entwicklung	Transaktionen	ZEG_1	Energie	ZEG_2	Kosten	ZEG_3
	M_1 = 13	0,4	M_3 = 85 TWh	0	M_5 = $86,33	0,4
	M_2 = 4		M_4 = 0		M_6 = 4	
Effektivitätsindex	I_9 = 0,27					
Anwender	Frage 4.4					
	Transaktionen	ZEG_4				
	M_7 = $19,18	0,1				
	M_8 = 1					
Effektivitätsindex	I_{10} = 0,1					

Benutzerfreundlichkeit	Frage 5.1	
Komplexität	Web 3.0 Tech-Stack	ZEG_1
	M_1 = 186 Stunden	0,35
	M_2 = 3,5	
Effektivitätsindex	I_{11} = 0,35	
Anwender	Frage 5.2	
	Trainierbarkeit	ZEG_1
	M_2 =3	0,3
Effektivitätsindex	I_{12} = 0,3	

Tabelle 16: Teil zwei der Effektivitätsindex-Tabelle

6 Diskussion

In dem vorangegangenen Kapitel wurden verschiedene Elemente der Web3-Technologien untersucht. Es wurden systematisch Metriken quantifiziert, um ein einheitliches Ergebnis zu erlangen. Es wurde ebenfalls ein breites Spektrum der möglichen Untersuchungskriterien evaluiert. Dieses Kapitel fasst die relevanten Ergebnisse zusammen und evaluiert diese hinsichtlich des übergeordneten Ziels dieser Bachelorarbeit: Die Evaluierung von Web3. Da Web3 ein Überbegriff für die Entwicklung von DApps ist, wurde in dieser These ein DApp-Prototyp erstellt und untersucht. Hinsichtlich dessen lassen sich über den allgemeinen Stand von Web3-Informationen herleiten.

6.1 Dezentralität im Kontext

Für die Dezentralität gibt es keine standardisierten Metriken. Dies erschwert die Quantifizierung. Es ist möglich, viele verschiedene Metriken aufzustellen und diese zu bewerten. Dabei ist es entscheidend, die Kennzahlen in einen Kontext zu stellen. Eine reine Zahl kann bei solch einem komplexen Untersuchungskriterium nicht das endgültige Ergebnis sein. Die Netzwerkebene hat beispielsweise einen Wert von 0,43, ein unterdurchschnittliches Resultat. Es muss geklärt werden, welche Bedeutung diese Zahl hat. Angela Welch beschreibt eine essenzielle Tatsache bei der Untersuchung der Dezentralität von Kryptowährungen: "succumbing to Gresham's Law of Measurement means allowing measurability to trump meaning-fulness. In other words, easily calculated quantitative metrics may provide the illusion of measurability while in actuality not being meaningful" (Walch 2019, 25).

Die Netzwerkebene, die von Web3-Unternehmern wie Chris Dixon als der kritischste Teil der Dezentralität angesehen wird (vgl. Dixon 2018), hat mit 0,43 den schlechtesten Wert unter den Ebenen. Das Netzwerk hat eine erhebliche Knotenlast in den USA. Um diese Metrik korrekt deuten zu können, hilft hier ein vergangenes Beispiel. Der schlimmste Fall wäre, dass die USA das Ethereum-Mining verbieten.

Genau das ist jedoch mit Bitcoin passiert. Bitcoin hatte 65 % der Hash-Power in China und das Mining wurde dort untersagt. Dies führte dazu, dass die Mining-Stationen in China abnahmen. Allerdings hatte es, wie zuerst befürchtet, keine nennenswerten Auswirkungen auf den Preis. Es erfordert eine große Menge an Ressourcen alle Mining-Stationen gleichzeitig abzuschalten. Viele Knoten wurden weiterhin illegal in China betrieben (s. Kapitel 5.1.1). Die großen Akteure würden das Land für ihre Operationen wechseln und das Ethereum-Netzwerk besteht weiter. Es herrscht damit eine klare Zentralität in den USA, im Kontext betrachtet ist dies jedoch keine direkte Bedrohung für das Ethereum-Netzwerk.

Eines der größten Herausforderungen von Ethereum ist die Konzentration von Minern und Mining-Pools. Mit etwas mehr als 50 % der Hash-Power sind die Top-3-MiningPools äußerst einflussreich. Die Struktur von Ethereum ermöglicht es, dass sich die Kette aufspaltet, sollten genügend Miner Einwände gegen Änderungen haben. Ein Plan, weniger Token an Miner auszuzahlen, hätte im Jahr 2021 beinahe dazu geführt. Eine Fraktion von Minern drohte, 51 % der Hash-Power zu kontrollieren und den Vorschlag zu boykottieren (vgl. Radmilac 2021). Obwohl die Drohung nicht wahr wurde, könnte sie in der Zukunft weiterhin ein Problem darstellen. Der Kontext in diesem Fall zeigt, wie stark sich diese Statistik auf die Dezentralität der Ethereum-Governance und -Sicherheit auswirkt.

Bei Ethereum ist das Governance-Problem historisch kompliziert. Die Ethereum-Gemeinschaft war 2016 nach dem DAO-Bruch sichtlich gespalten. wie in Abschnitt 2.6.4 dargelegt wurde, sind DAOs kein einfaches Instrument. Sie sind ein kompliziertes Konstrukt, das die Unterstützung von Governance-Spezialisten erfordert. Dezentralität und die damit einhergehende schwerfällige Bürokratie in Krisenzeiten (siehe Kapitel 2.6.4 Compound Hack) tragen zur wachsenden Kritik an DAOs bei. Die Community verändert sich aufgrund mangelnder Sicherheitsmaßnahmen und steigender Verluste (vgl. Schmalzried 2021). Derzeit sind "Dev Calls" die Governance-Alternative (siehe Kapitel 2.4.6.1). Ein Expertenrat ist ratsam, da viele Vorschläge höchst technisch veranlagt sind und die Mehrheit der Governance-Teilnehmer nur ein oberflächliches Verständnis der Technologie

besitzen. In ihrer derzeitigen Form ist die dezentrale Governance keine praktische Option. Aufgrund der Eigenschaften von Blockchains ist eine gewisse Zentralität kein großes Problem. Die Teilnehmer haben die Möglichkeit, sich zu trennen, und das Einspielen von Veränderungen ist nicht erforderlich. Aufgrund der Token-Ökonomie und der Anreize ist es jedoch im Interesse aller, einen Kompromiss zu finden, um Teil des Netzwerks zu sein.

Eine andere Art der Knotenverteilung zeigt ebenfalls eine klare Zentralität. 66 % aller Knoten befinden sich in der Cloud und sind somit von anderen Unternehmen abhängig. Im Grunde wäre dies kein großes Risiko, gäbe es keine eindeutige Konzentration auf AWS (s. Kapitel 5.1.1). Insgesamt laufen 35% aller Knoten auf AWS und widersprechen damit der Web3 Vision, sich von den Web2 Giganten wie Amazon zu lösen. Anders als bei der Verteilung über Länder, besteht hier die Möglichkeit einer direkten Abschaltung auf Wunsch eines einzelnen Unternehmens. Dies stellt rückwirkend ein Problem dar, sollte Amazon Aufgrund von Sanktionen zu Abschaltung gezwungen sein. Um Auswirkungen zu spüren, wäre dies jedoch nur dann der Fall, wenn die USA das Ethereum-Mining verbieten und Unternehmen zusätzlich dazu zwingen würde, diese von der Cloud abzukoppeln. Das ist jedoch kein realistisches Szenario.

Abschließend wurde deutlich, dass Metriken im Falle der Dezentralität der Blockchain nicht immer aussagekräftig sind. Hier kommt es auf den Kontext und die Realisierbarkeit der Risiken an. Objektiv betrachtet ist die Ethereum-Blockchain kein Vorzeigemodell für Dezentralität. Dabei ist zu beachten, dass die Dezentralität einer Blockchain ein stetig wandelnder Prozess ist. Dezentralität zu erreichen ist recht komplex und geschieht mit der Zeit (vgl. Muzzy und Anderson 2022). Demzufolge sind zentrale Funktionalitäten, wie hier bei der Ethereum-Blockchain, weiterhin Teil von Web3.

Im Zuge der Untersuchung der Dezentralität einer DApp, scheint die Konnektivität zwischen der DApp und der Blockchain das größte Problem zu sein. Viele DApps vertrauen auf Provider, wie Infura oder Alchemy. Infura wird von den größten DApps wie Uniswap oder Compound genutzt, die Dezentralität als Werbung für ihre

Anwendung nutzen. Gleichzeitig verbindet Infura die am weitesten verbreitete Web-Wallet, MetaMask, mit der Blockchain. Beide Anwendungen sind Bestandteil von ConsenSys, an dem JPMorgan Stimmrechte besitzt (vgl. Protos 2022). Ein fundamentales Web3-Entwicklungstool wird zum Teil von einer Investmentbank kontrolliert. Dies lässt erkennen, dass das Ziel der Unabhängigkeit von großen Unternehmen komprimiert ist. Auch ConsenSys muss sich an lokale Gesetze halten und hat bereits Verbraucher aufgrund verschiedener Sanktionen von der Nutzung seiner Dienste ausgeschlossen (s. Kapitel 2.6.4).

Die Vision von Web3 leidet unter der schnell wachsenden Nutzerbasis von Infura. Der Erfinder der Messaging-App Signal, Moxy Marlinspike, hat es passend zusammengefasst: "People don´t want to run their own servers, and never will" (Marlinspike 2022). Dezentralisierte Systeme sind nicht immer notwendig und viele Experten glauben, dass zentralisierte Plattformen im Web3 eine bedeutende Rolle spielen werden. Insbesondere müssen folgende Charakteristiken gelten: „(i) (…) verifiable proof to certify the correctness of the state (…), and (ii) all pub-lished state should have the concept of finality (..)" (Zhuotao et al. 2021, 3). Dies ist bei Infura derzeit nicht der Fall.

Es ist jedoch zu bedenken, dass diese Dienste auch Kreativität und Innovation fördern. Viele Entwickler werden durch die schwierige Konfiguration eines eigenen Knotens abgeschreckt und fügen der bereits komplexen Entwicklungsumgebung weitere Hindernisse hinzu. Damit Infura jedoch in der "matured Web3 era" (Zhuotao et al. 2021, 3) erfolgreich sein kann, muss es sich an die von den Experten festgelegten Standards anpassen.

Ein weiterer Punkt sind die Dienste und Protokolle. Darunter fallen Wallets wie MetaMask oder auch Marktplätze wie OpenSea. Die Web3-Community ist zurzeit in einer NFT-Bewegung und das Interesse an der eigentlichen Web3 Vision ist niedrig. Aus diesem Grund setzen viele Entwickler auf zentrale Dienste, um ihre Vision eines NFTs zu erfüllen. Dabei bieten zentrale Webseiten wie OpenSea einen benutzerfreundlichen Einstieg. Auch der HAW Zugangsblock NFT wurde Mithilfe von OpenSea erstellt. Der Vorgang benötigt keine Programmier- oder Blockchain-Kenntnisse. Hier herrscht das gleiche Dilemma. Zentrale Dienste schaffen einen

komfortablen Einstieg in die Web3-Entwicklung. Die Visionen von Web3 werden dabei kaum beachtet.

Es gibt auch positive Beispiele, wie IPFS und The Graph. Diese beiden Protokolle sind erste charakteristische Schritte für die Dezentralisierung des Internets und bieten eine gute Grundlage für weitere Entwicklungen.

6.2 Aufwendige Sicherheit

Die Sicherheit ist ein großes Thema im Web3 Bereich. Die Token-Ökonomie verlangt aufgrund der Wertschöpfung höchste Sicherheitsstandards. Seit dem DAO-Hack im Jahr 2016 unterlag die Ethereum-Blockchain keinem erfolgreichen Hackerangriff. Das Netzwerk hat durch die hohe Wachstums- und Erfolgsrate die Sicherheit gestärkt. Die nötige geliehene Hashpower würde zum jetzigen Zeitpunkt über $1 Millionen pro Stunde kosten, um das Netzwerk zu übernehmen (vgl. Crypto51.app o. J., Stand 12.08.2022). Dabei muss jedoch beachtet werden, dass es bei dieser Menge zu Komplikationen und Engpässen von gemieteter Hashpower kommen kann. Außerdem erweist sich die Wahrscheinlichkeit auf ein profitables Ergebnis als äußerst gering. Der Wechsel auf PoS ist ein bedeutendes Sicherheitsupgrade und erhöht die Kosten für einen Angriff auf über $15 Milliarden (vgl. ethereum.org 2022c, Proof-Of-Stake).

Durch die Komplexität eines direkten Angriffs auf die Blockchain, häufen sich die Sicherheitsexploits bei weiteren Web3 Diensten und Tools. Eine Zero-Knowledge-Proof Entwicklung ist daher besonders in den dezentralen Finanzen essenziell. Oftmals verlieren Nutzer ihre Kryptowährungen aufgrund von Tools wie unsichere Wallets, neue Marktplätze oder in Bridges zweier Blockchains, wie es bei Polygon und Ethereum möglich ist. Damit hat Ethereum selbst nichts zu verantworten, bildet jedoch ein schlechtes Licht auf die gesamte Web3-Community.

Smart Contracts sind dabei oftmals die Auslöser. Diese müssen ohne jegliche Loopholes erstellt werden. Im zweiten Quartal von 2022 wurden insgesamt über $700M aus Web3 Bridges gestohlen, davon $380M in Ethereum (vgl. Beosin & Footprint Analytics 2022, 3 & 5). Das ist nicht nur für die Anwender abschreckend,

sondern auch für Entwickler, die sich folglich die meiste Zeit ihrer Entwicklung mit der Sicherheit des Smart Contracts beschäftigen müssen.

Aus diesem Grund entsteht zurzeit ein neuer Wirtschaftszweig und viele Start Ups fokussieren sich auf Smart Contract Audits. Die Verantwortung ist oftmals zu hoch für einen einzelnen Entwickler oder einer Entwicklergruppe. Gibt das Budget jedoch eine professionale Sicherheitsanalyse nicht frei, ist die Entwicklung der Sicherheit für Smart Contracts limitiert. Es gibt einige automatische Audits online, welche die ausschlaggebendsten Sicherheitslücken der Vergangenheit kontrollieren. Das reicht für einen Prototypen aus Kapitel 4.3 aus, ist jedoch keine Alternative für große Projekte. Der HAW Blog hatte keine kritischen Fehler und könnte nun auf das Hauptnetzwerk von Ethereum deployt werden. Dessen Funktionalitäten bieten keine Angriffsfläche.

Abschließend lässt sich zum Thema Sicherheit sagen, dass die Ethereum-Blockchain für die Entwicklung von DApps sicher ist. Das zukünftige Upgrade auf PoS wird viele Sorgen nehmen. Jedoch ist die Sicherheit bei Smart Contracts ein komplexes und anstrengendes Verfahren für Entwickler. Wer kein Budget für Audits besitzt, sollte sich tiefgründig mit der Zero-Knowledge-Proof Entwicklung beschäftigen.

6.3 Marktführer trotz mangelhafter Effizienz

Die Gesamteffizienz der Ethereum-Blockchain wurde als „kaum erfüllt" eingestuft. Im Vergleich der Konkurrenten, hat die Ethereum-Blockchain die langsamste Transaktionsrate pro Sekunde. Die Konkurrenten erreichen bis zu 1.000.000 TPS und verlieren Marktanteile (s. Tabelle 14). Es stellt sich die Frage, wie dieses Phänomen entsteht.

Da Ethereum die erste Blockchain ihrer Art war, hat sie den Vorteil einer langen und stetigen Entwicklungsgeschichte. Es scheint, dass die Effektivität nicht die bedeutsamste Eigenschaft ist. Konkurrenten wie Cardano oder Polkadot haben ebenfalls bedeutende Fortschritte gemacht, jedoch hatten sie noch keine Gelegenheit ihre Fähigkeiten unter Beweis zu stellen. Der Ruf von Ethereum baut seine

Monopolstellung aus. Auch an den Konkurrenten wird Kritik geübt. Die NFT-Gemeinschaft erlebt derzeit ein Wiederaufleben der Blockchain Solana. Allerdings kommt es bei dem Netzwerk immer wieder zu längeren Ausfällen oder zu Hacker-Angriffen. Diese aufstrebende Blockchain wird häufig kritisiert, weil sie nicht ausreichend dezentralisiert sein soll. Dies ist auf die Tatsache zurückzuführen, dass etwa die Hälfte aller Solana-Token (SOL) an Insidern vergeben wurde (vgl. Watkins 2021).

Die fortschreitende Binance Smart Chain unterliegt der gleichen Kritik. Sie ist die einzige Blockchain, die von 2021 bis 2022 einen Zuwachs von 0,64 % Marktanteil auf 4,48 % verzeichnen konnte. Selbst der Marktanteil von Ethereum ist in diesem Zeitraum geringfügig gesunken (s. Tabelle 14). Die Popularität in diesem Beispiel kann auf die Aufnahme der Binance Smart Chain in Binance, der weltweit größten Kryptowährungsbörse, zurückgeführt werden.

Trotz seiner niedrigen Effizienz ist Ethereum weiterhin führend und tritt in die Fußstapfen von Bitcoin. Da Ethereum zu PoS übergeht und über 100.000 TPS verspricht, ist dies kein Grund zur Sorge. Es ist anzunehmen, dass es hier mehr um das Marketing als um den Fortschritt oder die Zukunft geht. Die Nutzer werden Ethereum weiterhin nutzen, weil es das erste System seiner Art ist. Das Gleiche gilt für Bitcoin. Objektiv gesehen ist Bitcoin eine der langsamsten, am wenigsten effizienten Kryptowährungen auf dem Markt und verschwendet genug Energie, um große Nationen zu versorgen (vgl. Yaga et al. 2018, 39). Konkurrenten von Bitcoin bieten keine Gebühren, keine Kohlenstoffemissionen und Soforttransaktionen. Dennoch folgt der gesamte Markt Bitcoin. Die Menschen investieren nicht in konkurrierende Anbieter, sondern in das Original, ohne auf dessen Eigenschaften zu achten. Ethereum befindet sich in der gleichen Situation. Trotz der angekündigten Umstellung auf PoS scheint es offensichtlich, dass Ethereum auch mit weiterführenden PoW der Marktführer bleiben würde. Das ist nicht gesund für den Fortschritt des Web3 als Ganzes.

Auch in Bezug auf die Energieverschwendung bietet Ethereum kein günstiges Bild. Ethereum ist mit einem Zielerreichungsgrad von 0 eine bedeutende Quelle von

Stromverschwendung. Dies ist ein Risiko, sollte Ethereum nicht auf PoS umsteigen. Der Klimawandel ist ein Thema, auf das sich die globale Politik immer mehr konzentriert. Wie in Kapitel 2.6.4 erörtert, befassen sich die ersten Politiker nun intensiv mit Kryptowährungen. Die Fehler des vergangenen Jahrzehnts dürfen von der künftigen Internetgeneration nicht wiederholt werden. Ethereum muss bei einer Energiewende ein Zeichen setzen und die Umstellung auf PoS vollziehen.

Ein weiteres Problem sind die Kosten, die den Verbrauchern und Entwicklern in Rechnung gestellt werden. Da die Token-Ökonomie auf Anreize angewiesen ist, müssen die Nutzer diese Anreize bieten. Die Bereitstellung der 93 LOC des HAW-Blog-Smart-Contracts für das Mainnet hätte im Durchschnitt 86 US-Dollar gekostet. Mit fast $1 pro LOC ist dies eine hohe Summe. Das ist kein wünschenswertes Ergebnis und erhöht die Einstiegshürde für zukünftige Entwickler.

Ein Beitrag in dem hypothetischen Blog würde etwas weniger als 20 Dollar für die Veröffentlichung kosten. Dieser Preis ist zu hoch für diese Art von Funktionen. Die Behauptung, dass das Web3 nur noch für den Goldrausch genutzt würde, bestätigt sich hierdurch. Schnelles Profitieren und Ausnutzen des Hypes, bevor die Blase platzt. Mit solchen Gebühren wird das Web3 die Mehrheit der Nutzer nicht überzeugen können. Der Effektivitätsindex liegt daher bei 0,1.

6.4 Web3-Entwicklung ist zu komplex

Die letzten beiden großen Untersuchungsbereiche können besser zusammen diskutiert werden. Die Funktionalität hat durch die fehlerhafte Integration von IPFS nur einen Wert von 0,52. Da vieles von der Datenspeicherung abhängt, sind anderen Dienste wie The Graph ebenfalls betroffen. Den Grund dafür gilt es zu erörtern.

Web3 Entwicklung ist komplex und hat eine starke Lernkurve. Web3 Tech-Stacks gehen über das klassische Wissen der Web2 weit hinaus (vgl. Rivabella 2021). Es muss sich mit mehreren neuen Technologien auseinandergesetzt werden und insbesondere IPFS ist eine einzigartige Datenspeicherung. Der klassische Web2 Entwickler muss sich im Backend mit der jeweiligen Datenbank auseinandersetzen,

dessen Sprache beherrschen und die Prinzipien einer sowohl funktionierenden als auch optimierten Datenbank anwenden können.

Bei der Web3 Entwicklung muss der Entwickler die Grundprinzipien der Blockchain-Technologie verstehen. Ebenso essenziel ist ein Verständnis der Kryptographie und Sicherheit in IT. Hinzu kommt das Erlernen von Solidity im Falle von Ethereum. Smart Contracts zu schreiben ist ebenfalls kein einfaches Unterfangen. Neue Funktionalitäten müssen erlernt werden und die Sicherheit erfolgt nicht durch eine Firewall, sondern muss im Code eingebettet sein. Es ist ein fortgeschrittenes Wirtschaftswissen im Bereich der Blockchain nötig und es müssen Probleme wie „double-spending“ oder „re-entrance“ erforscht werden. Dazu kommt das Erlernen mit dem Umgang neuer Tools, Dienste und Protokolle. Eine DApp besteht nicht nur aus einem Smart Contract, sondern es muss die dezentrale Datenspeicherung studiert werden oder auch eine SQL-ähnliche Abfragesprache wie bei The Graph. Dies ist nur die Spitze des Eisberges. Dezentrale Kommunikation, Scaling-Solutions, Zero-Knowledge-Proof Entwicklung bei DeFi oder das Aufstellen eines Knotens sind ebenfalls mögliche Felder, die der Entwickler angehen muss (vgl. Rivabella 2021).

Der Tech-Stack ist für die kleinste Funktionalität ausgesprochen komplex und daher ein großes Problem. Aus eigener Sicht wurde ein Prototyp erstellt und nach über ~120 Stunden wurde die Entwicklung eingestellt. Dabei wurden die Ziele einer erfolgreichen Datenspeicherung mit IPFS nicht erreicht. Die Komplexität wurde mit 3,5/10 bewertet. Es wurden Foren-einträge studiert, Tutorials analysiert, Blog-Einträge und Whitepapers gelesen. Das Ziel ist nicht zwanghaft eine funktionierende DApp zu gestalten, sondern den Prozess hier darzulegen und dessen Schwierigkeiten zu zeigen. Und im jetzigen Zustand zeigt das Ergebnis der Funktionalität und Benutzerfreundlichkeit dieser Bachelorarbeit, dass die Web3 Entwicklung für einen Absolventen in Wirtschaftsinformatik zu komplex ist.

6.5 Fazit

Web3 versucht die Probleme des Web2 zu lösen, scheitert jedoch zurzeit an einem menschlichen Merkmal: der Komfortabilität. Web2 ist komfortabel und orientiert sich

stark an der Benutzerfreundlichkeit im Austausch für die Privatsphäre und Zentralität. Die wahre Vision von Web3 scheint unrealistisch zu wirken. In einer Welt voller Konsum und kapitalistischem Denken, ist diese Vision fremd. Zentrale Dienste und Webseiten dominieren den „Web3-Raum“ und es scheint der Mehrheit nicht relevant zu sein.

Es gibt eindeutige Indizien, dass dies einer Dotcom-Bubble ähnelt. Projekte versprechen unrealistisches, versprechen Dezentralität ohne diese definieren zu können. Projekte nennen sich eine DAO, obwohl sie einen zentralen Messenger mit Voting-Mechanismus benutzen. Das Argument „Web3 ist noch in den Anfängen“ kann im Rückblick auf die Dotcom-Bubble als valides Argument gesehen werden. Es scheint der normale Zyklus der Veränderung zu sein. Sollte die Web3-Bubble platzen, kommen dabei eventuell die wahren Funktionalitäten und Visionen wieder zum Vorschein.

Aus der Sicht des Entwicklers ist Web3 in einem Anfangsstadium. Viel Energie und Geld werden in digitale Kunst gesteckt, obwohl dieses Talent Web3 weiterbringen könnte. Das liegt auch daran, dass die Entwicklung neuere Technologien langsam und aufwendig ist. Digitale Kunst scheint zurzeit das einzige Thema in der Welt von Web3 zu sein.

Web3 ist noch nicht bereit Web2 ersetzen und ist weit davon entfernt. Zur jetzigen Zeit ist keine Zukunft für Web3 realistisch. Es gab einen guten Grund dafür, dass Web2 so existiert wie es existiert. Aus der Entwicklersicht ist Web3 eine katastrophale Verschlechterung gegenüber Web2. Es muss daran gearbeitet werden, Entwicklertools zu vereinfachen, Zentralitätsengpässe wie Infura zu verbessern und weg von dem Kapitalismus auf Steroiden zu kommen. Eine gewisse Zentralität wird immer existieren und das ist im Zusammenhang mit den von Experten definierten Bedingungen auch sinnvoll.

Außerdem ist die Token-Ökonomie in keinem Zustand für die Masse der Anwender. Schon jetzt gibt es starke Scaling-Probleme und Nutzer müssen zu hohe Gebühren zahlen. Satoshi Nakamoto hatte eine Vision, diese wurde von Vitalik Buterin mit Smart Contract expandiert. Beide möchten die Welt verändern, stehen jedoch vor der

größtmöglichen Hürde: die Menschheit und ihr komfortabler Lebensstil. Vielen Menschen ist die Lage der Zentralität und Verletzung der Privatsphäre in Web2 nicht bewusst. Infolgedessen kommt diese These zu dem Entschluss, dass es wahrscheinlich ein Subsystem des Internets geben wird, in der das Web3 seinen Platz bekommt. Web2 wird es jedoch auch in den nächsten Jahren nicht ersetzen.

7 Zusammenfassung & Ausblick

7.1 Zusammenfassung

Diese experimentelle Bachelorarbeit hat mithilfe eines eigen erstellten Konzepts Metriken anhand eines Prototyps quantifiziert und bewertet. Dabei wurde jeweils die Dezentralität, Sicherheit, Funktionalität, Effizienz und Benutzerfreundlichkeit der DApp analysiert. Die Dezentralität untersucht die verschieden architektonischen Ebenen der DApp und ist insgesamt unterdurchschnittlich schlecht bewertet worden. Dabei ist jedoch aufgefallen, dass insbesondere bei der fundamentalen Blockchain der Kontext der Metrik maßgebend ist. Ethereum hat einige zentralisierte Schwachstellen, wie die Verteilung der Knoten auf der Welt oder die Verteilung der Hashpower. In der Diskussion ist klargeworden, dass jedoch nur die Hashpower einer Metrik von Bedeutung ist.

Die Dezentralität der DApp dagegen ist ungenügend. Anstelle des Aufstellens eines eigenen Knotens, greifen viele Entwickler auf zentralisierte Provider zurück und vertrauen nicht verifizierbaren Informationen. Vorteilhaft ist jedoch die Entwicklung in die dezentrale Infrastruktur von Web3, durch die Erstellung von dezentraler Datenspeicherung (IPFS) oder das Ermöglichen von Abfragen innerhalb der Blockchain (The Graph).

Die Sicherheit ist im Falle des Prototyps ein Erfolg. Die automatischen Analysetools ergaben keine kritischen Fehler oder Bugs. Außerdem ist die Ethereum-Blockchain überdurchschnittlich sicher. Dies wird sich durch einen zukünftigen Wechsel des Konsensmechanismus von PoW auf PoS verfestigen. Das Gesamtbild der Sicherheit von Web3 ist jedoch fragwürdig. Kompliziertere Smart Contracts müssen mit präziser Untersuchung der Sicherheit geschrieben werden und können durch ihre unveränderbare Eigenschaft großen wirtschaftlichen Schaden anrichten. Zero-Knowledge-Proof Entwicklung und Smart Contract Audits gewinnen dabei an Bedeutung.

Die anhaltenden, immer wiederkehrenden Nachrichten über großangelegte Hackerangriffe und Phishing-Attacken vermindern die Chance einer Massenadoption der neuen Technologien. Der Anwender muss sich im Vergleich zu Web2 kompliziertes Wissen aneignen, um in Web3 sicher unterwegs zu sein. Es fallen zusätzlich hohe Gebühren für Entwickler und Anwender an, um diejenigen zu bezahlen, welche die Blockchain am Laufen halten.

Ein weiterer Punkt ist das mangelnde Umweltbewusstsein und die Effizienz der Blockchain. Die beliebteste Blockchain für DApp-Entwicklung ist nach Bitcoin die langsamste und energieaufwendigste. In einer progressiven Umweltpolitik sind PoW-Blockchains ein Dorn im Auge der Politik. Früher oder später wird diese Technologie im Rahmen der Klimapolitik ins Visier genommen und beschränkt. Eine erfolgreiche Migration der Ethereum-Blockchain auf PoS ist nötig, um in der Zukunft Teil von Web3 zu sein.

7.2 Ausblick & Weiterführung

Diese Bachelorarbeit arbeitete mit dem Minimum des möglichen in diesem Bereich. Eine Weiterführung der Dissertation könnte eine funktionsreichere Anwendung beinhalten. Dabei könnte aus dem Blog eine DAO kreiert werden, die durch den HAW NFT erreichbar ist und mit den HAW Token bedient wird. Diese DAO ist dezentral für alle Entscheidung und Wahlen innerhalb der Universität zuständig. Darauf folgt ein ergänzendes Konzept zur Untersuchung einer solchen DAO in Kombination mit der

Token-Ökonomie. Ebenfalls interessant wären eine empirische Studie und Interviews mit Governance-Experten oder die Evaluierung der Nutzung von öffentlichen Blockchains im Gegenzug zu privaten Blockchains für solche internen Projekte.

Insgesamt lohnt ebenfalls sich die Evaluierung einer möglichen PoS Ethereum-Blockchain, die trotz mehrfacher Verschiebung, noch im Jahre 2022 erscheinen soll. Im Zuge dessen können die Ergebnisse mit dieser Arbeit verglichen werden. Dieses Konzept gilt aus Grundbaustein für die Zukunft. Es kann prinzipiell erweitert und verändert werden, bleibt jedoch den fünf Grundpfeilern treu. Web3 wandelt sich schnell und Veränderungen an bestehenden Blockchains, Diensten oder neue Konkurrenten können mit dem Konzept untersucht werden.

Literaturverzeichnis

Antonopoulos, Andreas M./Wood, Gavin. (2019). Mastering Ethereum. Building smart contracts and DApps. Beijing, Boston, Farnham, Sebastopol, Tokyo/[München], O'Reilly; EBL. ISBN: 9781491971918. Online verfügbar unter https://github.com/ethereumbook/ethereumbook.

Bamakan, Seyed Mojtaba Hosseini/Nezhadsistani, Nasim/Bodaghi, Omid/Qu, Qiang (2022). Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Scientific reports 12 (1), 2178. https://doi.org/10.1038/s41598-022-05920-6.

Bambacht, Joost/Pouwelse, Johan (2022). Web3: A Decentralized Societal Infrastructure for Identity, Trust, Money, and Data. Delft University of Technology. Online verfügbar unter https://doi.org/10.48550/arXiv.2203.00398.

Bashir, Imran (2017). Mastering Blockchain. Distributed ledgers, decentralization and smart contracts explained. Birmingham, UK, Packt Publishing Ltd. ISBN: 1787129292. Online verfügbar unter https://books.google.de/books/about/Mastering_Blockchain.html?id=urkrDwAAQBAJ&redir_esc=y.

Basili, Victor R./Caldiera, Gianluigi/Rombach, H. Dieter (1994). Goal Question Metric Paradigm. Encyclopedia of Software Engineering 2, 528–532. Online verfügbar unter https://www.kiv.zcu.cz/~brada/files/aswi/cteni/basili92goal-question-metric.pdf.

Beck, Roman (2018). Beyond Bitcoin: The Rise of Blockchain World. Computer 51 (2), 54–58. https://doi.org/10.1109/MC.2018.1451660.

Benet, Juan (2014). IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3). Online verfügbar unter https://ipfs.io/ipfs/QmV9tSDx9UiPeWExXEeH6aoDvmihvx6jD5eLb4jbTaKGps.

Beosin & Footprint Analytics (2022). Beosin 2022 Q2 Web3 Security Report. Online verfügbar unter https://static.footprint.network/report/Q2_2022_Web3_Security_Report.pdf (abgerufen am 12.08.2022).

Berners-Lee, Tim/Cailliau, Robert (1990). WorldWideWeb: Proposal for a HyperText Project. CERN. Online verfügbar unter https://www.w3.org/Proposal.html (abgerufen am 24.04.2022).

Bit2Me Academy (2021). What is IPFS? Online verfügbar unter https://academy.bit2me.com/en/que-es-ipfs/ (abgerufen am 09.08.2022).

Bocksch, René (2022). Bitcoin-Stromverbrauch. Bitcoins Stromverbrauch übertrifft den der Ukraine. Statista vom 2022. Online verfügbar unter https://de.statista.com/infografik/18608/stromverbrauch-ausgewaehlter-laender-im-vergleich-mit-dem-des-bitcoins/ (abgerufen am 10.07.2022).

Brody, Paul (2022). Web 3.0 Is Too Complicated. Yahoo Finance vom 2022. Online verfügbar unter https://finance.yahoo.com/news/3-0-too-complicated-165752418.html (abgerufen am 22.05.2022).

Bunin, Viktor (2019). Proof of Stake's security model is being dramatically misunderstood. Medium vom 2019. Online verfügbar unter https://viktorbunin.medium.com/proof-of-stakes-security-model-is-being-dramatically-misunderstood-4ed7b19ca419 (abgerufen am 31.07.2022).

Buterin, Vitalik (2014). Ethereum Whitepaper. A Next-Generation Smart Contract and Decentralized Application Platform. Online verfügbar unter https://ethereum.org/en/whitepaper/ (abgerufen am 22.05.2022).

Butler, Brooks (2022). MetaMask, OpenSea Blocks Expose "Web3" Centralization. Crypto Briefing vom 2022. Online verfügbar unter https://cryptobriefing.com/metamask-opensea-blocks-expose-centralization-in-web3/ (abgerufen am 10.07.2022).

Bybit Learn (2022). Ethereum's Switch to PoS: What We Know So Far. Bybit. Online verfügbar unter https://learn.bybit.com/deep-dive/ethereum-proof-of-stake-pos/ (abgerufen am 22.05.2022).

cgewecke (2019). sc-forks · GitHub. Online verfügbar unter https://github.com/sc-forks (abgerufen am 02.08.2022).

Choudhury, Nupur (2014). World Wide Web and Its Journey from Web 1.0 to Web 4.0. (IJCSIT) International Journal of Computer Science and Information Technologies 5 (6), 8096–8100. Online verfügbar unter https://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf (abgerufen am 10.07.2022).

CoinMarketCap (2021). Ethereum's London Hard Fork: What Is It… and Why Is It Controversial? CoinMarketCap vom 2021. Online verfügbar unter https://coinmarketcap.com/alexandria/article/ethereums-london-hard-fork-what-is-it-and-why-is-it-controversial (abgerufen am 31.07.2022).

cointelegraph (2021). What is Ethereum and how does it work? Cointelegraph vom 2021. (abgerufen am 10.07.2022).

countryeconomy.com (2021). Electricity consumption 2021. Online verfügbar unter https://countryeconomy.com/energy-and-environment/electricity-consumption (abgerufen am 21.08.2022).

Crypto51.app (o. J.). Cost of a 51% Attack for Different Cryptocurrencies | Crypto51. Online verfügbar unter https://www.crypto51.app/ (abgerufen am 12.08.2022).

Dabit, Nader (2022). The Complete Guide to Full Stack Web3 Development. Online verfügbar unter https://www.youtube.com/watch?v=nRMo5jjgCr4 (abgerufen am 13.08.2022).

Digiconomist (2022). Ethereum Energy Consumption Index - Digiconomist. Online verfügbar unter https://digiconomist.net/ethereum-energy-consumption (abgerufen am 04.08.2022).

Dixon, Chris (2018). Why Decentralization Matters - OneZero. OneZero vom 2018. Online verfügbar unter https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e (abgerufen am 12.08.2022).

Dixon, Chris (2021). Why Web3 Matters. Future vom 2021. Online verfügbar unter https://future.com/why-web3-matters/ (abgerufen am 10.08.2022).

Dorsey, Jack (2021). jack auf Twitter: „You don’t own 'web3.'". Online verfügbar unter https://twitter.com/jack/status/1473139010197508098 (abgerufen am 10.08.2022).

Dreyer, Schürmann Rosenthal (2019). Smart Contracts: Rechtliche Voraussetzungen und Herausforderungen. SCHÜRMANN, ROSENTHAL, DREYER Partnerschaft von Rechtsanwälten mbB vom 2019. Online verfügbar unter https://www.srd-rechtsanwaelte.de/blog/smart-contracts-recht/ (abgerufen am 10.07.2022).

Duperrin, Pierre (2022). What is Infura? | Ledger. Online verfügbar unter https://www.ledger.com/academy/what-is-infura (abgerufen am 07.08.2022).

Dwivedi, Akhilesh/Kumar, Suresh/Dwivedi, Abhishek/Kumar, Raj/Singh, Manjeet (2011). Current Security Considerations for Issues and Challenges of Trustworthy Semantic Web. 0975-0290 03 (01). Online verfügbar unter https://www.researchgate.net/publication/247935415_Current_Security_Considerations_for_Issues_and_Challenges_of_Trustworthy_Semantic_Web.

Eichholz, Liesl (2020). The UNI Token: Is Uniswap Really Decentralized? Glassnode Insights - On-Chain Market Intelligence vom 2020. Online verfügbar unter https://insights.glassnode.com/uni-token-is-uniswap-really-decentralized/ (abgerufen am 19.08.2022).

ethereum GitHub (2022). Network Upgrades Specifications. Online verfügbar unter https://github.com/ethereum/execution-specs/tree/master/network-upgrades#getting-the-considered-for-inclusion-cfi-status (abgerufen am 02.08.2022).

ethereum GitHub (2022). Solidity — Solidity 0.8.16 documentation. Online verfügbar unter https://docs.soliditylang.org/en/v0.8.16/ (abgerufen am 10.08.2022).

ethereum.org (2015). Introduction to Smart Contracts. Online verfügbar unter https://github.com/ethereum/solidity/blob/v0.8.15/docs/introduction-to-smart-contracts.rst.

ethereum.org (2021). Sidechains. Online verfügbar unter https://ethereum.org/en/developers/docs/scaling/sidechains/ (abgerufen am 10.07.2022).

ethereum.org (2022). Ethereum Energy Consumption | ethereum.org. Online verfügbar unter https://ethereum.org/en/energy-consumption/ (abgerufen am 04.08.2022).

ethereum.org (2022). Governance bei Ethereum – eine Einführung. Online verfügbar unter https://ethereum.org/de/governance/ (abgerufen am 02.08.2022).

ethereum.org (2022c). Proof-of-stake (PoS) | ethereum.org. Online verfügbar unter https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (abgerufen am 12.08.2022).

ethernodes.org (2022a). Ethereum Mainnet Statistics | Hosting. Online verfügbar unter https://ethernodes.org/networkType/Hosting (abgerufen am 14.08.2022).

ethernodes.org (2022b). Ethereum Mainnet Statistics | Network Types. Online verfügbar unter https://ethernodes.org/network-types?synced=0 (abgerufen am 14.08.2022).

Etherscan.io (2022a). Contract Address (Blog.sol)0x96f06db1bc533b8982071423cc84aec6abdbaafd | Etherscan. Online verfügbar unter https://ropsten.etherscan.io/address/0x96f06db1bc533b8982071423cc84aec6abdbaafd (abgerufen am 08.08.2022).

Etherscan.io (2022b). Ethereum Charts and Statistics | Etherscan. Online verfügbar unter https://etherscan.io/charts#clientInfo (abgerufen am 14.08.2022).

Etherscan.io (2022c). Ethereum Node Tracker | Etherscan. Online verfügbar unter https://etherscan.io/nodetracker (abgerufen am 20.08.2022).

Etherscan.io (2022d). HAWHamburg (HAW) Token Tracker | Etherscan. Online verfügbar unter https://ropsten.etherscan.io/token/0x0748170be9d2Aab77e504676b497537a06c52d49 (abgerufen am 03.08.2022).

Filippi, Primavera de/Hassan, Samer (2016). Blockchain technology as a regulatory technology. From code is law to law is code. First Monday 21 (12). https://doi.org/10.5210/fm.v21i12.7113.

Fill, Hans-Georg/Meier, Andreas (Hg.) (2020). Blockchain. Grundlagen, Anwendungsszenarien und Nutzungspotenziale. Wiesbaden, Springer Vieweg. ISBN: 9783658280062. Online verfügbar unter https://link.springer.com/book/10.1007/978-3-658-28006-2.

Frankenfield, Jake (2016). Ethereum. Investopedia vom 2016. Online verfügbar unter https://www.investopedia.com/terms/e/ethereum.asp (abgerufen am 10.07.2022).

Fuchs, Christian/Hofkirchner, Wolfgang/Schafranek, Matthias/Raffl, Celina/Sandoval, Marisol/Bichler, Robert (2010). Theoretical Foundations of the Web: Cognition, Communication, and Co-Operation. Towards an Understanding of Web 1.0, 2.0, 3.0. Future Internet 2 (1), 41–59. https://doi.org/10.3390/fi2010041.

Genç, Ekin/Graves, Stephen (2022). 13 Biggest DeFi Hacks and Heists. Decrypt vom 2022. Online verfügbar unter https://decrypt.co/93874/biggest-defi-hacks-heists (abgerufen am 10.07.2022).

George, Chikku (2022). NFT Metadata Types on OpenSea Marketplace | Coinmonks. Coinmonks vom 2022. Online verfügbar unter https://medium.com/coinmonks/nft-metadata-types-on-opensea-marketplace-aaea1ff5987c (abgerufen am 07.08.2022).

Gochhayat, Sarada Prasad/Shetty, Sachin/Mukkamala, Ravi/Foytik, Peter/Kamhoua, Georges A./Njilla, Laurent (2020). Measuring Decentrality in Blockchain Based Systems. IEEE Access 8, 178372–178390. https://doi.org/10.1109/ACCESS.2020.3026577.

Graph Explorer (2022). Indexers | Graph Explorer. Online verfügbar unter https://thegraph.com/explorer/participants/indexers (abgerufen am 26.08.2022).

Haig, Samuel (2020). University Students Harness Blockchain for Elections Amid Lockdown. Cointelegraph vom 2020. Online verfügbar unter https://cointelegraph.com/news/university-students-harness-blockchain-for-elections-amid-lockdown (abgerufen am 02.08.2022).

hardhat.org (2022). Hardhat | Ethereum development environment for professionals. Online verfügbar unter https://hardhat.org/ (abgerufen am 31.07.2022).

Hassan, Samer/Filippi, Primavera de (2021). Decentralized Autonomous Organization. Internet Policy Review 10 (2). https://doi.org/10.14763/2021.2.1556.

Herwartz, Christoph/Steuer, Helmut (2022). Bitcoin: Ein Verbot würde die Energiewende vereinfachen. Handelsblatt vom 2022. Online verfügbar unter https://www.handelsblatt.com/politik/eu-klimaschutz-energetisch-ist-der-bitcoin-voelliger-irrsinn-erste-europapolitiker-fordern-verbot-von-kryptowaehrungen/28025224.html (abgerufen am 10.07.2022).

Hsieh, Ying-Ying/Vergne, Jean-Philippe/Anderson, Philip/Lakhani, Karim/Reitzig, Markus (2018). Bitcoin and the rise of decentralized autonomous organizations. Journal of Organization Design 7 (1). https://doi.org/10.1186/s41469-018-0038-1.

Hurder, Stephanie (2020). To Get Serious About Decentralization, We Need to Measure It. CoinDesk vom 2020. Online verfügbar unter https://www.coindesk.com/business/2020/05/29/to-get-serious-about-decentralization-we-need-to-measure-it/ (abgerufen am 11.07.2022).

ISO/TC 307 (2020). Blockchain and distributed ledger technologies. International Organization for Standardization. Online verfügbar unter https://www.iso.org/committee/6266604.html (abgerufen am 10.07.2022).

Kasireddy, Preethi (2022). The Architecture of a Web 3.0 application. Online verfügbar unter https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application (abgerufen am 10.07.2022).

Kirpal, Alfred/Vogel, Andreas (2006). Neue Medien in einer vernetzten Gesellschaft: Zur Geschichte des Internets und des World Wide Web. NTM International Journal of History and Ethics of Natural Sciences, Technology and Medicine 14 (3), 137–147. https://doi.org/10.1007/s00048-006-0239-5.

Lantz, Lorne/Cawrey, Daniel (2020). MASTERING BLOCKCHAIN. Unlocking the power of cryptocurrencies and smart contracts. O'REILLY MEDIA. ISBN:

9781492054658. Online verfügbar unter https://www.oreilly.com/library/view/mastering-blockchain/9781492054696/.

Leonhard, Robert Donald (2017). Corporate Governance on Ethereum's Blockchain. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2977522.

Marlinspike, Moxie (2022). My first impressions of web3. Online verfügbar unter https://moxie.org/2022/01/07/web3-first-impressions.html (abgerufen am 10.07.2022).

McConnell, Steve (2004). Code complete. A Practical Handbook of Software Construction. 2. Aufl. Redmond, Wash., Microsoft Press. ISBN: 9780735619678. Online verfügbar unter https://www.oreilly.com/library/view/code-complete-2nd/0735619670/.

Meinel, Christoph/Gayvoronskaya, Tatiana (2020). Blockchain. Hype Oder Innovation. Berlin, Heidelberg, Springer Berlin / Heidelberg. ISBN: 9783662619162. Online verfügbar unter https://link.springer.com/book/10.1007/978-3-662-61916-2.

Moore, Rick (2022). ethers.js Documentation. Online verfügbar unter https://docs.ethers.io/v5/ (abgerufen am 14.08.2022).

Muzzy, Everett/Anderson, Mally (2022). Measuring Blockchain Decentralization | ConsenSys Research | ConsenSys. Online verfügbar unter https://consensys.net/research/measuring-blockchain-decentralization/ (abgerufen am 11.07.2022).

Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org. Online verfügbar unter https://bitcoin.org/bitcoin.pdf (abgerufen am 10.07.2022).

Nath, Keshab/Dhar, Sourish/Basishtha, Subhash (2014). Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges. In: 2014 International Conference

on Reliability Optimization and Information Technology (ICROIT), 2014 International Conference on Optimization, Reliabilty, and Information Technology (ICROIT), Faridabad, Haryana, India, 2/6/2014 - 2/8/2014. IEEE, 86–89.

Norta, Alex/Othman, Anis Ben/Taveter, Kuldar (2015). Conflict-Resolution Lifecycles for Governed Decentralized Autonomous Organization Collaboration. In: Proceedings of the 2015 2nd International Conference on Electronic Governance and Open Society Challenges in Eurasia, EGOSE '15: Challenges in Eurasia, St. Petersburg Russian Federation, 2015. [Place of publication not identified], ACM, 244–257.

Nover, Scott (2022). Bored Ape Yacht Club's NFTs cost $181 million in "gas" fees. Quartz vom 2022. Online verfügbar unter https://qz.com/2161193/bored-ape-yacht-clubs-nfts-cost-181-million-in-gas-fees/ (abgerufen am 10.07.2022).

Oualid, Z. (2022). Top 10 solidity smart contract audit tools. Get Secure World vom 2022. Online verfügbar unter https://www.getsecureworld.com/blog/top-10-solidity-smart-contract-audit-tools/ (abgerufen am 02.08.2022).

particl.news (2022). Web3 Exposed! Is it Only a Mirage? Particl News. Online verfügbar unter https://particl.news/web3-exposed-is-it-only-a-mirage/ (abgerufen am 10.07.2022).

Protos (2022). ConsenSys lawsuit reveals JPMorgan owns critical Ethereum infrastructure. Protos vom 2022. Online verfügbar unter https://protos.com/consensys-lawsuit-jpmorgan-owns-critical-ethereum-infrastructure/ (abgerufen am 12.08.2022).

Radmilac, Andjela (2021). Ethereum Miners Threaten Strike Ahead of EIP-1559 - The Chain Bulletin. Online verfügbar unter https://chainbulletin.com/ethereum-miners-threaten-strike-ahead-of-eip-1559 (abgerufen am 12.08.2022).

Reijers, Wessel/Wuisman, Iris/Mannan, Morshed/Filippi, Primavera de (2018). Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain

Technologies. TOPOI: International Review of Philosophy 37 (17). https://doi.org/10.2139/ssrn.3340056.

Rikken, Olivier/Janssen, Marijn/Kwee, Zenlin (2019). Governance challenges of blockchain and decentralized autonomous organizations. Information Polity 24 (4), 397–417. https://doi.org/10.3233/IP-190154.

Rivabella, Vittorio (2021). Zero To Hero: Web3.0 and Solidity Development Roadmap. Online verfügbar unter https://vitto.cc/web3-and-solidity-smart-contracts-development-roadmap/ (abgerufen am 12.08.2022).

Rumpel, Rainer (2015). Das GQMS-Vorgehensmodell für das Messen der Wirksamkeit von Informationssicherheitsmanagementsystemen. Berlin: Hochschule für Wirtschaft und Recht Berlin, IMB Institute of Management Berlin. Working Paper 83. Online verfügbar unter https://www.econstor.eu/handle/10419/111285.

Sai, Ashish Rajendra/Buckley, Jim/Fitzgerald, Brian/Le Gear, Andrew (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. Information Processing & Management 58 (4), 102584. https://doi.org/10.1016/j.ipm.2021.102584.

Schesswendter, Raimund (2022). Trotz Verbot: China zweitgrößtes Land für Bitcoin-Mining. t3n Magazin vom 2022. Online verfügbar unter https://t3n.de/news/trotz-verbot-china-land-bitcoin-mining-1473721/ (abgerufen am 14.08.2022).

Schmalzried, Gregor (2021). Das neue Hype-Thema der Blockchain: Was sind DAOs? BR24 vom 2021. Online verfügbar unter https://www.br.de/nachrichten/netzwelt/das-neue-hype-thema-der-blockchain-was-sind-daos,SmqM4LK (abgerufen am 10.08.2022).

Scott, Brett/Loonam, John/Kumar, Vikas (2017). Exploring the rise of blockchain technology: Towards distributed collaborative organizations. Strategic Change 26 (5), 423–428. https://doi.org/10.1002/jsc.2142.

Selig, Jay (2022). The 8 Defining Features of Web 3.0. expert.ai vom 2022. Online verfügbar unter https://www.expert.ai/blog/web-3-0/ (abgerufen am 10.07.2022).

Sen, Sahil (2022). Ethereum full node vs archive node explained - step-by-step beginners guides | QuickNode. Online verfügbar unter https://www.quicknode.com/guides/infrastructure/ethereum-full-node-vs-archive-node (abgerufen am 14.08.2022).

Shevchuk, Vitalii (2022). 5 Reasons Why Web 3.0 will Fail? - ITNEXT. ITNEXT vom 2022. Online verfügbar unter https://itnext.io/top-5-reasons-why-web-3-will-fail-57237e4c3db (abgerufen am 10.07.2022).

Shlegeris, Buck (2022). Gini coefficient calculator. Online verfügbar unter https://shlegeris.com/gini.html (abgerufen am 03.08.2022).

Singh, Madhusudan/Kim, Shiho (2019). Blockchain technology for decentralized autonomous organizations. In: Shiho Kim/Ganesh Chandra Deka/Peng Zhang (Hg.). Role of Blockchain Technology in IoT Applications. Oxford, Academic Press [Imprint]; Elsevier Science & Technology, 115–140. Online verfügbar unter https://doi.org/10.1016/bs.adcom.2019.06.001.

Sridhar, Shyam (2021). Measuring Decentralization in PoS Ethereum. Ethereum Foundation, Robust Incentives Group. Online verfügbar unter https://shsr2001.github.io/beacondigest/notebooks/2021/07/19/measuring_decentralization.html#subsec-2-3 (abgerufen am 29.07.2022).

Srinivasan, Balaji S. (2017). Quantifying Decentralization - news.earn.com. news.earn.com vom 2017. Online verfügbar unter https://news.earn.com/quantifying-decentralization-e39db233c28e (abgerufen am 28.07.2022).

Statista (2022). Ethereum energy consumption 2022 | Statista. Online verfügbar unter https://www.statista.com/statistics/1265891/ethereum-energy-consumption-transaction-comparison-visa/ (abgerufen am 10.08.2022).

Stephen, DiRose/Mo, Mansouri (2018). Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations. In: 2018 13th Annual Conference on System of Systems Engineering (SoSE 2018). Paris, France, 19-22 June 2018, 2018 13th Annual Conference on System of Systems Engineering (SoSE), Paris, 2018. Piscataway, NJ, IEEE, 195–202.

Streza, Alex (2022). When GitHub Goes Down the World Comes Apart | JavaScript in Plain English. JavaScript in Plain English vom 2022. Online verfügbar unter https://javascript.plainenglish.io/when-github-goes-down-the-world-comes-apart-94d1c9bf75bf (abgerufen am 07.08.2022).

Tal, Yaniv/Ramirez, Brandon/Pohlmann, Jannis (2018). The Graph: A Decentralized Query Protocol for Blockchains. Online verfügbar unter https://github.com/graphprotocol/research/blob/master/papers/whitepaper/the-graph-whitepaper.pdf (abgerufen am 10.07.2022).

testnet.opensea.io (2022). HAW Hamburg Zugangsblock - HAW Hamburg | OpenSea. Online verfügbar unter https://testnets.opensea.io/assets/rinkeby/0x88b48f654c30e99bc2e4a1559b4dcf1ad93fa656/51673047168195838414032657087858036273270086711324709741734042965205258862692 (abgerufen am 02.08.2022).

The Graph Docs (2022). About The Graph - The Graph Docs. Online verfügbar unter https://thegraph.com/docs/en/about/ (abgerufen am 26.08.2022).

van de Velde, Jo/Scott, Angus/Sartorious, Katrina/Dalton, Ian (2016). Blockchain in Capital Markets. The Prize and the Journey. Online verfügbar unter https://www.oliverwyman.com/our-expertise/insights/2016/jan/blockchain-in-capital-markets.html.

Voshmgir, Shermin (2018). Web3, Blockchain, cryptocurrency: a threat or an opportunity? Genf, TEDxCERN, 2018. Online verfügbar unter https://www.ted.com/talks/shermin_voshmgir_web3_blockchain_cryptocurrency_a_threat_or_an_opportunity (abgerufen am 10.07.2022).

W3C.org (o .J.). Sematic Web. W3C.org. Online verfügbar unter https://www.w3.org/standards/semanticweb/ (abgerufen am 10.07.2022).

Walch, Angela (2019). Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems. In: Chris Brummer (Hg.). Chapter in Crypto Assets: Legal and Monetary Perspectives. Oxford University Press. Online verfügbar unter https://ssrn.com/abstract=3326244.

Wayner, Peter (2019). 23 blockchain languages driving the future of programming. TechBeacon vom 2019. Online verfügbar unter https://techbeacon.com/app-dev-testing/23-blockchain-languages-driving-future-programming (abgerufen am 10.07.2022).

Web3 Foundation (o. J.). Web 3.0 Technology Stack. Web3 Foundation. Online verfügbar unter https://web3.foundation/about/ (abgerufen am 10.07.2022).

Wietlisbach, Oliver (2018). Das sind alle Daten, die Facebook und Google von dir haben. watson vom 2018. Online verfügbar unter https://www.watson.ch/digital/best%20of%20watson/583783726-bist-du-bereit-auszuflippen-das-sind-alle-daten-die-facebook-und-google-von-dir-haben (abgerufen am 24.08.2022).

Wilson, David W./Lin, Xiaolin/Longstreet, Phil/Sarker, Saonee (2011). Web 2.0: A Definition, Literature Review, and Directions for Future Research. AMCIS. Online verfügbar unter https://www.semanticscholar.org/paper/Web-2.0%3A-A-Definition%2C-Literature-Review%2C-and-for-Wilson-Lin/f15acbb87c0302c4e22b473bbc9f65bf25cae01f.

Wood, Dr. Gavin/Buchanan, Aeron/Trinkler, Reto (2022). Web3 Foundation | About. Online verfügbar unter https://web3.foundation/about/ (abgerufen am 10.08.2022).

Yaga, Dylan/Mell, Peter/Roby, Nik/Scarfone, Karen (2018). Blockchain technology overview. 8202. Aufl. Gaithersburg, MD. Online verfügbar unter https://doi.org/10.6028/NIST.IR.8202.

Yatchenko, Darya (2022). Ethereum 2.0 vs Polkadot: Two Promising Platforms to Solve the Scalability Issue. PixelPlex vom 2022. Online verfügbar unter https://pixelplex.io/blog/ethereum-vs-polkadot-comparison/ (abgerufen am 10.07.2022).

Zhao, Huabing (2018). Digital Signature and Public Key as Identities - Huabing Zhao - Medium. Medium vom 2018. Online verfügbar unter https://zhaohuabing.medium.com/digital-signature-and-public-key-as-identities-94f8ecac2a24 (abgerufen am 10.08.2022).

Zheng, Zibin/Xie, Shaoan/Dai, Hong Ning/Chen, Xiangping/Wang, Huaimin (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services 14 (4), 352. https://doi.org/10.1504/IJWGS.2018.095647.

Zhuotao, Liu/Yangxi, Xiang/Shi, Jian/Gao, Peng/Wang, Haoyu/Xiao, Xusheng/Wen, Bihan/Li, Qi/Hu, Yih-Chun (2021). Make Web3.0 Connected. IEEE Transactions on Dependable and Secure Computing, 1. https://doi.org/10.1109/TDSC.2021.3079315.

Inhaltsverzeichnis Anhang

Anhang 1: Grundlagen

Anhang 1.1: Dezentrale Autonome Organisation (DAO)

In der akademischen Literatur gibt es mehrere Anläufe zur spezifischen Definition von DAOs. Einige geben keine Definition an (vgl. Norta et al. 2015) oder halten sich an Branchendefinitionen (vgl. Stephen und Mo 2018). Folgende Kerncharakteristiken lassen sich schlussfolgern:

- DAOs ermöglichen es Menschen, sich online selbst zu verwalten und koordinieren (vgl. Singh und Kim 2019, 119). Das Minimum einer Gruppe wird nicht erwähnt, wobei der Begriff „Organisation“ generell auf mehrere Menschen mit gleichen Zielen verweist.

- Der DAO-Quellcode wird in einer Blockchain mit Smart Contracts – wie Ethereum – bereitgestellt (vgl. Singh und Kim 2019, 119).

- Ein DAO Smart Contract, legt die Regeln zwischen den Interaktionen von Menschen fest (vgl. Filippi und Hassan 2016, 12), wobei es unklar ist, inwieweit es andere Governance-Mechanismen geben kann, die einen solchen Code beeinflussen oder außer Kraft setzen können (vgl. Singh und Kim 2019, 119).

- Da die Regeln in Smart Contracts definiert sind, werden sie unabhängig von dem Willen der Parteien selbst ausgeführt

- DAOs sollen unabhängig von zentraler Kontrolle agieren. Definitionen verweisen auf „self-governed“ (vgl. Filippi und Hassan 2016), „self-organising“ (vgl. Singh und Kim 2019) und „democratic control“ (vgl. Hsieh et al. 2018).

- Da DAOs auf Blockchain basieren, erben sie auch einige dessen Eigenschaften, wie Transparenz, Kryptografische Sicherheit und Dezentralität (vgl. Beck 2018, 57).

Eine große Anzahl von akademischer Literatur über DAOs ist aus dem Bereich der Informatik und fokussiert sich auf die Blockchain-Technologie und dessen

Geschäftsmodell. Jedoch können DAOs so viel mehr als digitale Marktplätze oder dezentrale Börsen sein. Eine DAO kann eine virtuelle Entität sein „that operates as a crowd-funding platform, a ride-sharing platform, a fully automated company, or a fully automated decision-making apparatus." (vgl. Hassan und Filippi 2021, 5).

Diverse Experten aus verschiedenen Bereichen beschäftigen sich vermehrt mit DAOs. Welche Möglichkeiten bieten „distributed governance structures" (Leonhard 2017; Hsieh et al. 2018), deren Limitationen und Herausforderungen (vgl. Scott et al. 2017), sowie im Bereich der Ökonomie und Governance (vgl. Rikken et al. 2019). Ebenfalls ist die Befassung der Gesetzmäßigkeit im Zusammenhang mit DAOs ein wesentliches Thema für die Weiterentwicklung. Smart Contracts werfen viele Rechtsfragen auf (Dreyer 2019) und werden auch juristisch unter die Lupe genommen (Reijers et al. 2018).

Anhang 1.2: Smart Contract

```
1  pragma solidity ^0.4.25;
2  contract SalesContract {
3    // Zustandsvariablen: stock, buyer
4    uint public stock; // verfügbare Menge
5    // Zuordnungen: erworbene Menge je Käufer
6    mapping (address => uint) public buyer;
7    // Konstruktor
8    constructor() public {
9      stock = 47; // initiale Menge
10   }
11   // Funktion, von Käufer aufzurufen
12   function order(uint quantity) public {
13     // Bedingungen: Verkaufszeitpunkt,
14     // max.-Menge 99, Prüfung Verfügbarkeit
15     if (block.timestamp > 1546038000 ||
16       quantity > 99 || stock < quantity) {
17       return;
18     }
19     // Preis: 1*10^18 Wei = 1 Ether
20     uint priceInWei = 1*10^18;
21     // Kauf, wenn Wert >= Menge*Preis
22     if (msg.value >= quantity*priceInWei) {
23       // Menge verfügbarer Artikel verringern
24       stock -= quantity;
25       // Kauf-Adresse mit Anzahl speichern
26       buyer[msg.sender] += quantity;
27     }
28   }
29 }
```

Listing 2: Beispiel Smart Contract Code (vgl. Fill und Meier 2020, 17)

Dies ist ein vereinfachte Smart Contract (s. Listing 2). Es können Variablen erstellt werden (s. Zeile 4 & 6), wobei die Zustandsvariable „buyer“ eine Hashtabelle ist, die in diesem Fall die erworbene Menge einen Käufer zuordnet (docs.soliditylang.org, o. J.). Der Konstruktor wird nach der Übersetzung des Smart Contracts in Bytecode ausgeführt und initialisiert hier die Variable „Stock“ auf die Menge 47 (s. Zeile 8 f.). Funktionen führe eine gewisse Aktivität aus. Hier das kaufen von Stocks. Die Funktion reduziert „stock“ um die angegebene Menge „quantity“, sofern sie nicht durch die angegebenen Bedingungen abgebrochen wird. Es bricht nach einem bestimmten Zeitpunkt, bei einer Menge > 99 oder bei zu geringerer Verfügbarkeit ab (s. Zeile 12-17). Ansonsten wird der Kauf ausgeführt, „Stock“ wird verringert und der Kauf wird in der Hashtabelle „buyer“ registriert (s. Zeile 20-26).

Anhang 2: Prototyp

Anhang 2.1: Front End

Die Startseite beinhaltet die Möglichkeit sich als Nutzer anzumelden (s. Abb. 24).

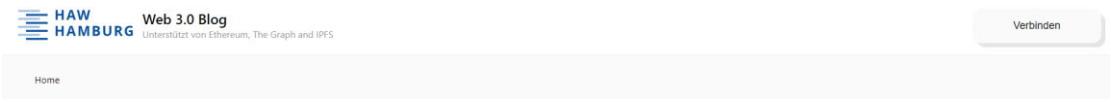

Abbildung 24: Startseite HAW Blog vor der Anmeldung

Nach der Anmeldung mit MetaMask über den Button „Verbinden“, erscheint eine erweiterte Startseite. Oben rechts zeigt den öffentlichen Schlüssel des eingeloggten Accounts an und es besteht nun die Möglichkeit einen Beitrag zu erstellen (s. Abb. 25).

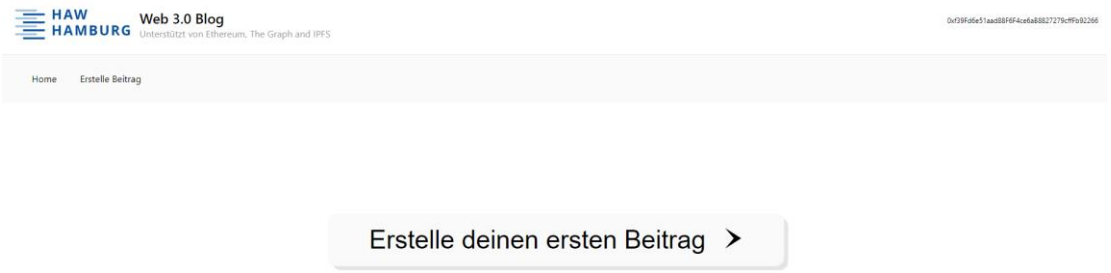

Abbildung 25: Startseite HAW Blog nach der Anmeldung

Nach dem Drücken des Buttons „Erstelle deinen ersten Beitrag“ erscheint eine Seite mit der Möglichkeit einen Beitrag zu erstellen (s. Abb. 26).

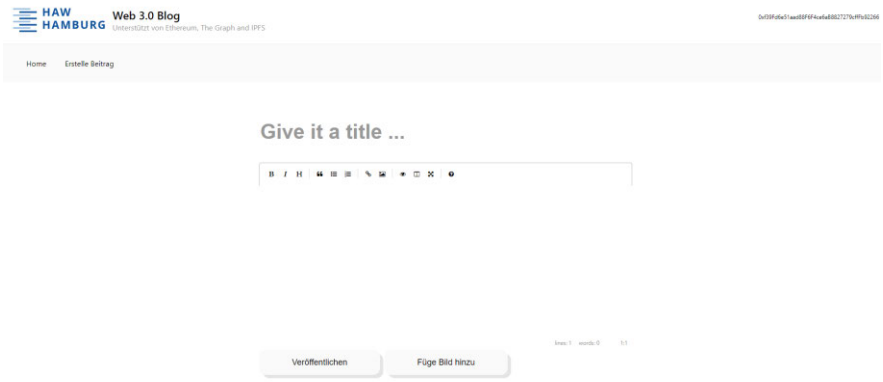

Abbildung 26: Seite zum Erstellen eines Beitrags

Daraufhin kann der Nutzer die Felder ausfüllen und ein Bild hinzufügen (s. Abb. 27).

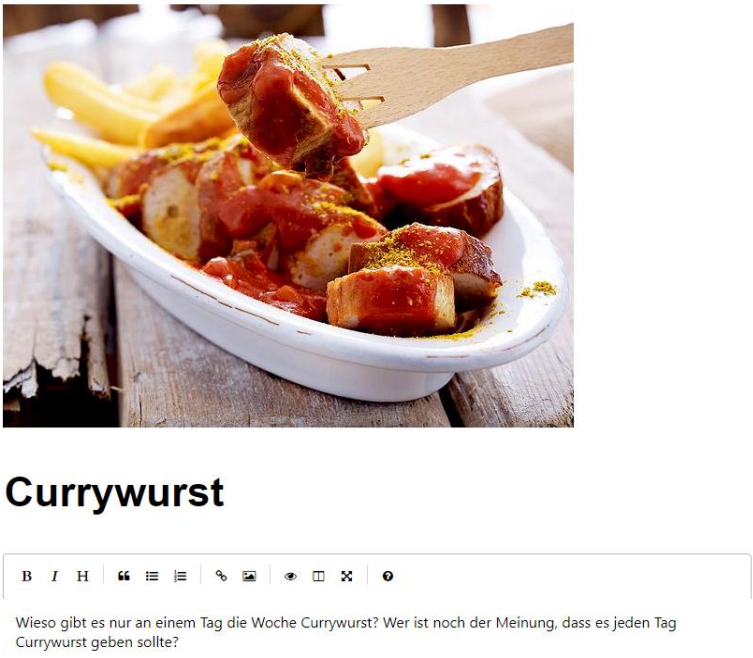

Abbildung 27: Ausgefüllter Beitragsvorschlag

Der Nutzer hat nun die Möglichkeit den Beitrag zu veröffentlichen. MetaMask öffnet sich daraufhin und verlangt eine Gebühr, um diese Smart Contract Funktionalität auszuführen und der Blockchain hinzuzufügen (s. Abb. 28).

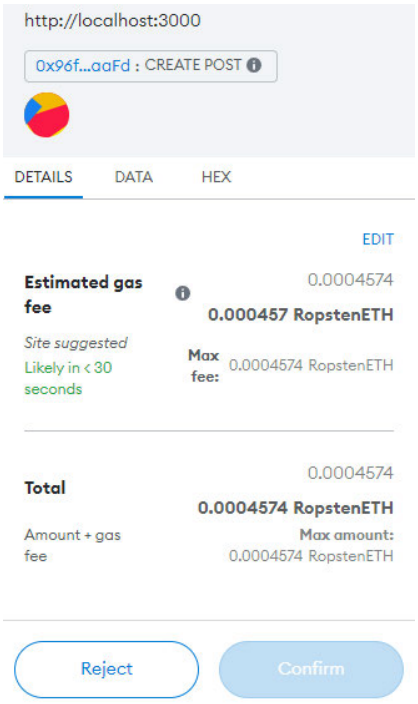

Abbildung 28: MetaMask Abfrage

Daraufhin erscheint Beitrag auf der Homepage.

Anhang 2.2: Back End

Die Beitragserstellung ist recht einfach gehalten (s. Listing 3).

```
53      function createPost(string memory title, string memory hash) public onlyOwner {
54          _postids.increment();
55          uint postid = _postids.current();
56          Post storage post = idToPost[postid];
57          post.id = postid;
58          post.title = title;
59          post.published = true;
60          post.content = hash;
61          hashToPost[hash] = post;
62          emit PostCreated(postid, title, hash);
63      }
```

Listing 3: Code-Abschnitt der Funktion zum Erstellen eines Beitrages

Das Erstellen von Beiträgen kann mit „public Owner“ in Zeile 53 nur dem Owner des Smart Contracts vorbehalten werden. Die ID wird erhöht und dessen Variable gesetzt. In Zeile 56 wird ein Beitrag, mit dem default „null“, erstellt. In den folgenden vier Zeilen werde diese Werte gesetzt. Daraufhin wird der Lookup für hashToPost gesetzt. Abschließend wird das PostCreated Event ausgelöst.

Dies läuft ähnlich bei dem Updaten eines Beitrages ab. Aus diesem Grund ist die nächste Funktion das Holen aller Beiträge (s. Listing 2).

```
77      function fetchPosts() public view returns (Post[] memory) {
78          uint itemCount = _postids.current();
79
80          Post[] memory posts = new Post[](itemCount);
81          for (uint i = 0; i < itemCount; i++) {
82              uint currentid = i + 1;
83              Post storage currentItem = idToPost[currentid];
84              posts[i] = currentItem;
85          }
86          return posts;
87      }
```

Listing 4: Code-Abschnitt der Funktion zum Holen aller Beiträge

Hier wird ein temporäres Array (memory) mit der Anzahl der Beiträge geschaffen. Anschließend wird durch den Lookup idToPost iteriert, bis alle Beiträge in dem temporären Array sind. Dieser wird am Ende zurückgegeben.

Daraufhin wird Mithilfe von Infura ein API-Schlüssel generiert, mit dessen entschieden werden kann, auf welches Netzwerk dieser Smart Contract deployt werden soll. Für Testzwecke gibt es das sogenannte „Ropsten Test Network“, das auf dem gleichen Protokoll wie Ethereum läuft. Da das deployen auf dem Ethereum-Mainnet echte Ethereum-Token kostet, ist dies eine kostenlose Alternative zum Testen der Funktionalitäten.

Wurde der Smart Contract deployt, gibt es einen Transaktionen Hash, mit welcher die Transaktion auf dem Blockchain-Netzwerk identifizieren kann und weitere Informationen erlangt (s. Abb. 29)

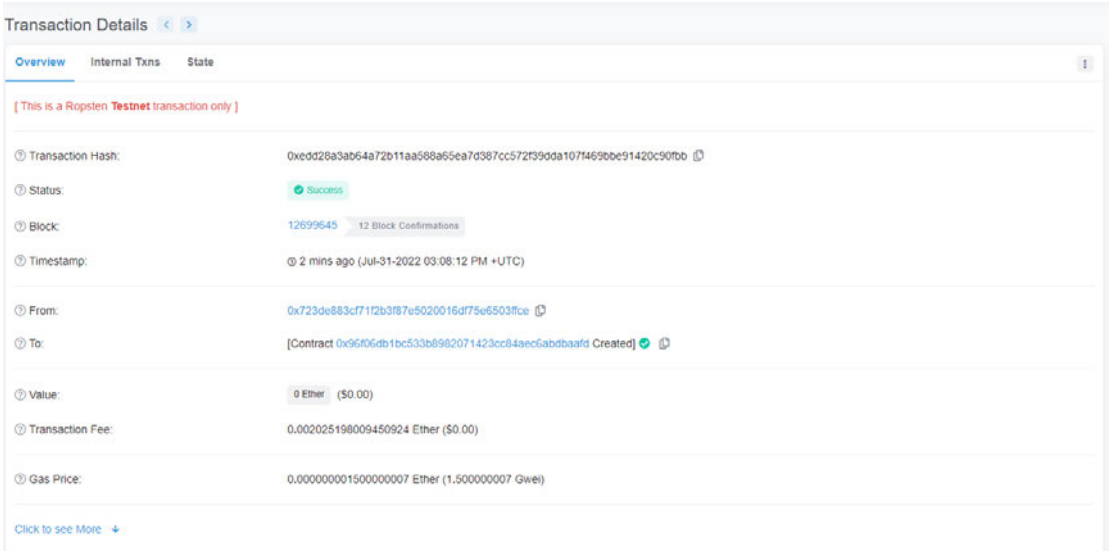

Abbildung 29: Transaktion für das deployen des Smart Contract (ropsten.etherscan.io)

Anhang 3: Ergebnisse

Anhang 3.1: Berechnung der Wachstumsrate

Um die Wachstumsrate zu bestimmen, muss bestimmt werde, wie viele Blöcke pro Tag erstellt werden und wie groß diese sind. Es werden täglich zwischen 6300-6500 Blöcke generiert (s. Abb. 30).

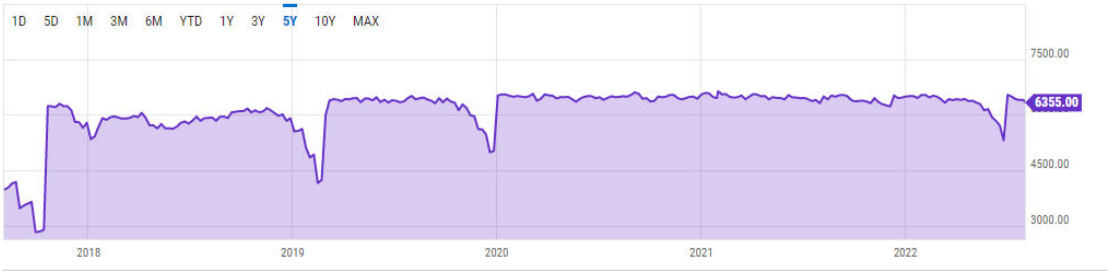

Abbildung 30: Blöcke produziert pro Tag in den letzten 5 Jahren (vgl. ycharts 2022)

Dessen Größe variiert und hängt von der Aktivität der Blockchain ab (s. Abb. 31). Es lohnt sich daher ein aktuelles Beispiel zu nehmen.

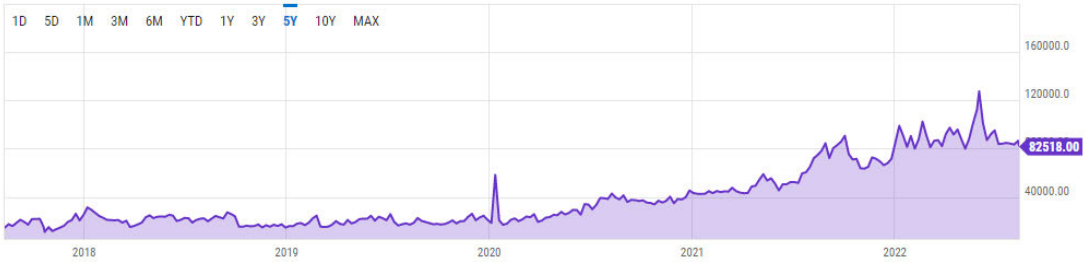

Abbildung 31: Durchschnittliche Block-Größe (vgl. ycharts 2022)

03.08.2022:

- Blöcke: 6355
- Block-Größe 84,139 Bytes

Wachstum: 6355 * 84,139 Bytes = 534.703.345 Bytes = 0.54 GB an dem Tag. Dies würde bei gleichbleibenden Daten ein Wachstum von über 15 GB pro Monat bedeuten.

Anhang 3.2: Knotenverteilung

Siehe Abbildung 32 für die Statistik der Knotenverteilung auf die verschiedenen Arten der Knotenaufstellung.

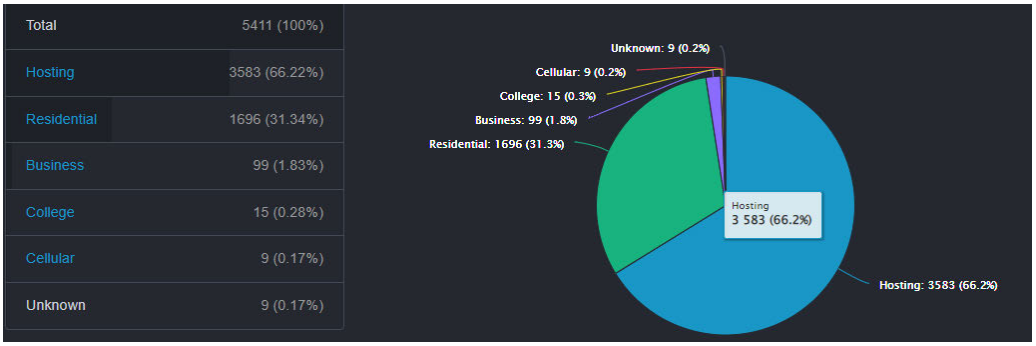

Abbildung 32: Aufteilung der Knotentypen (vgl. ethernodes.org 2022b)

Abbildung 33 visualisiert die Aufteilung der gehosteten Knoten und deren Anbieter.

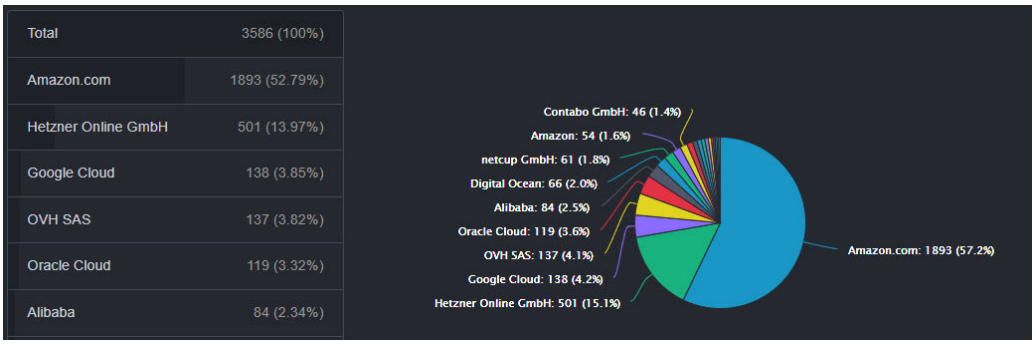

Abbildung 33: Aufteilung der Hostings (vgl. ethernodes.org 2022a)

Anhang 3.3: MythX Smart Contract Audit Report

Der MythX Report des Blogs (s. Abb. 34) hat nur eine „low vulnerability“ entdeckt (s. Abb. 35).

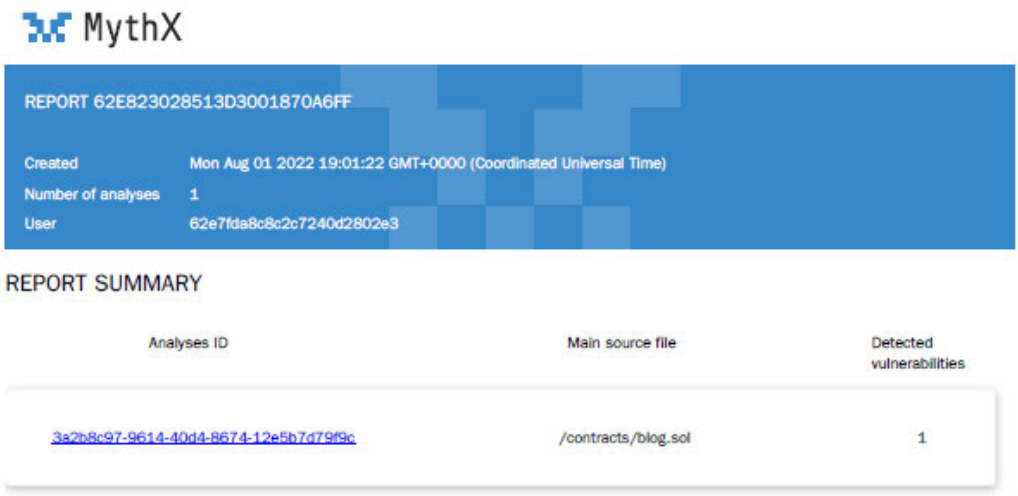

Abbildung 34: MythX Report Zusammenfassung

Diese Zusammenfassung erläutert in einem PDF alle möglichen Verbesserungsvorschläge.

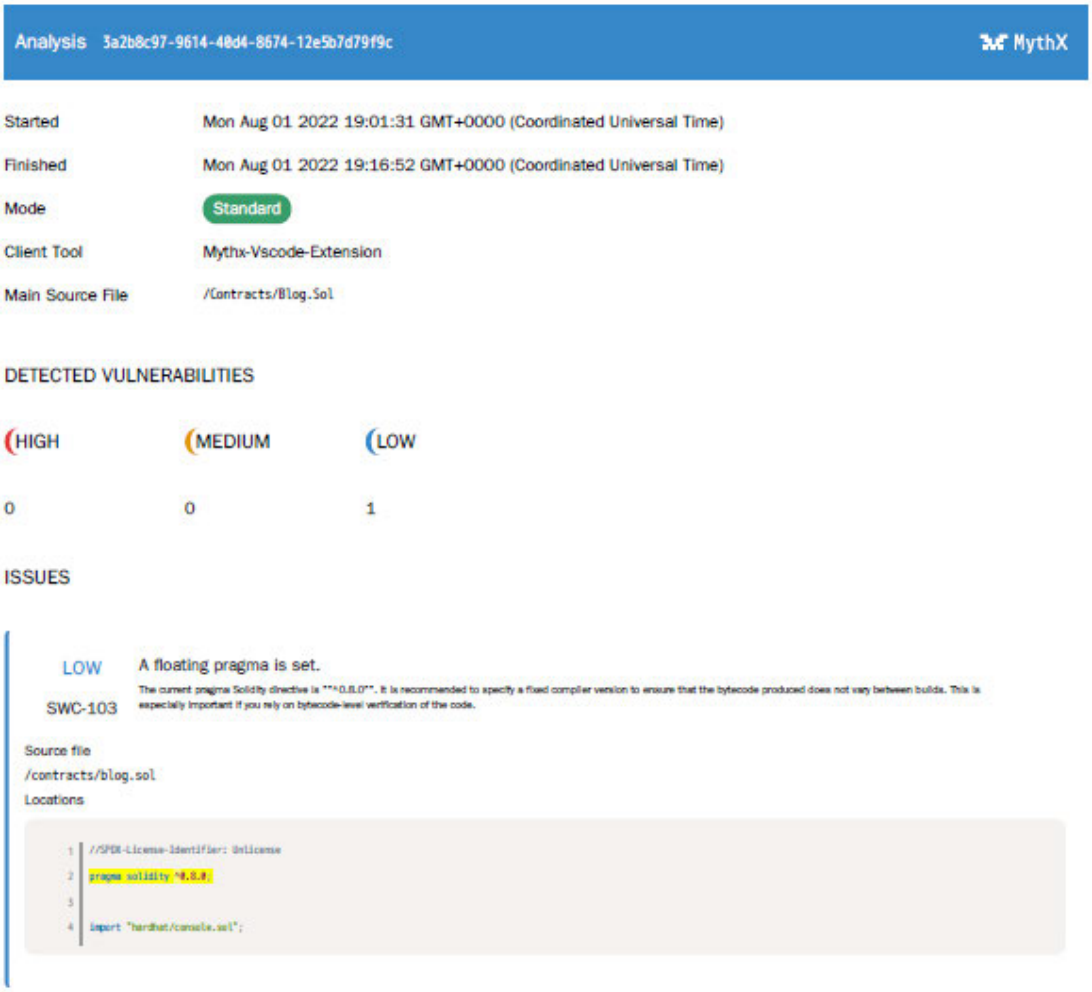

Abbildung 35: Analyse des Blogs

Anhang 3.4: Smart Contracts

Hier werden alle gefunden Vertrags- und Testdateien analysiert. Die Nutzung des Coverage Checker gibt eine Tabelle zurück. Die erste Spalte *Files* gibt jeweils die einzelnen Verträge an und alle zusammen. „% Stmts“ gibt die Prozentzahl der getesteten Statements, „% Branch“ der Control-Statements, „% Func“ der Funktionen und „% Lines“ der LOC.

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\	41.18	10	26.09	42.03	
Blog.sol	93.33	50	75	93.55	45,56
NFT.sol	0	0	0	0	... 81,82,83,97
Token.sol	0	0	0	0	... 55,56,57,58
All files	41.18	10	26.09	42.03	

Tabelle 17: Erster Durchlauf Solidity Coverage Checker

Durch das Anzeigen der „Uncovered Lines“ können nun fehlende Tests nachgearbeitet werden (s. Tabelle 17).

File	% Stmts	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\	97.62	75	92.31	97.67	
Blog.sol	96.67	50	87.5	96.77	56
NFT.sol	100	100	100	100	
Token.sol	100	100	100	100	
All files	97.62	75	92.31	97.67	

Tabelle 18: Zweiter Durchlauf Solidity Coverage Checker

Der Zweite Durchlauf (s. Tabelle 18) hat eine fast vollständige Coverage und ist somit für diese experimentelle Evaluierung ausreichend. Berechnung der Metrik 1 für den %-Anteil der Coverage für alle Smart Contracts gesamt: M_1 = *(%-Statements + %-Branch + %-Functions + %-Lines) / 4 = (97,62% + 75% + 92,31% + 97,67%) / 4 =* **90,65%**

Es wurde nun festgestellt, dass Tests für die jeweilige Funktion zu fast 100 % vorhanden sind. Nun gilt es zu testen, ob diese auch einwandfrei funktionieren:

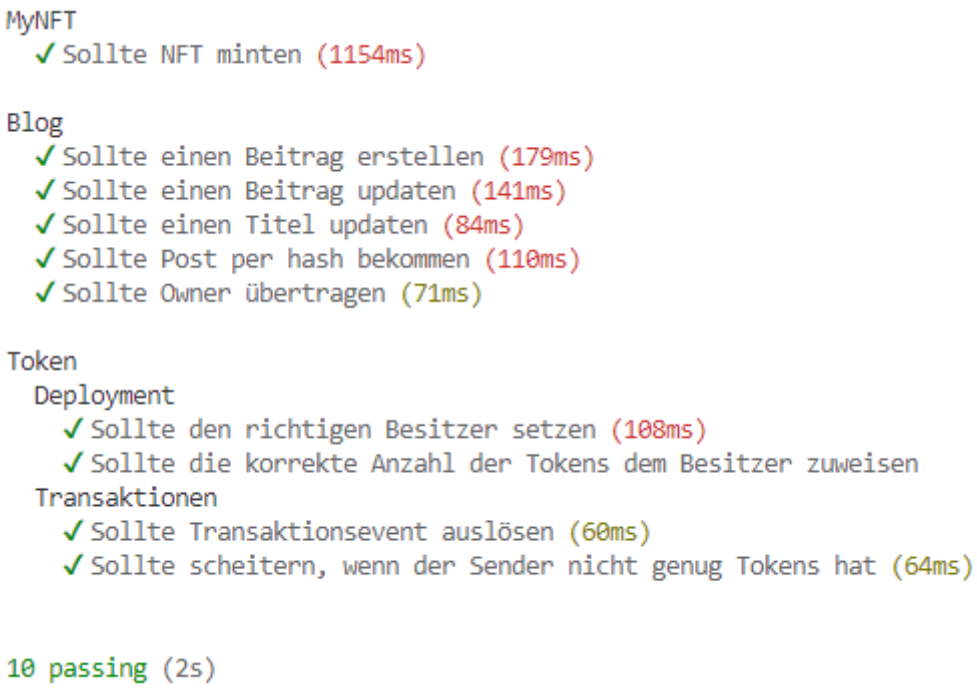

Abbildung 36: Erfolgreiches testen aller Unit-Tests mit Zeitangabe

Alle Tests funktionieren einwandfrei (s. Abb. 36) und M_2 ist damit 100 %.

Anhang 3.5: Funktionalität der Dienste

Anhang 3.5.1: IPFS

IPFS besitzt einen eigenen Desktop Client, der es ermöglicht, einen Knoten aufzustellen (s. Abb. 37).

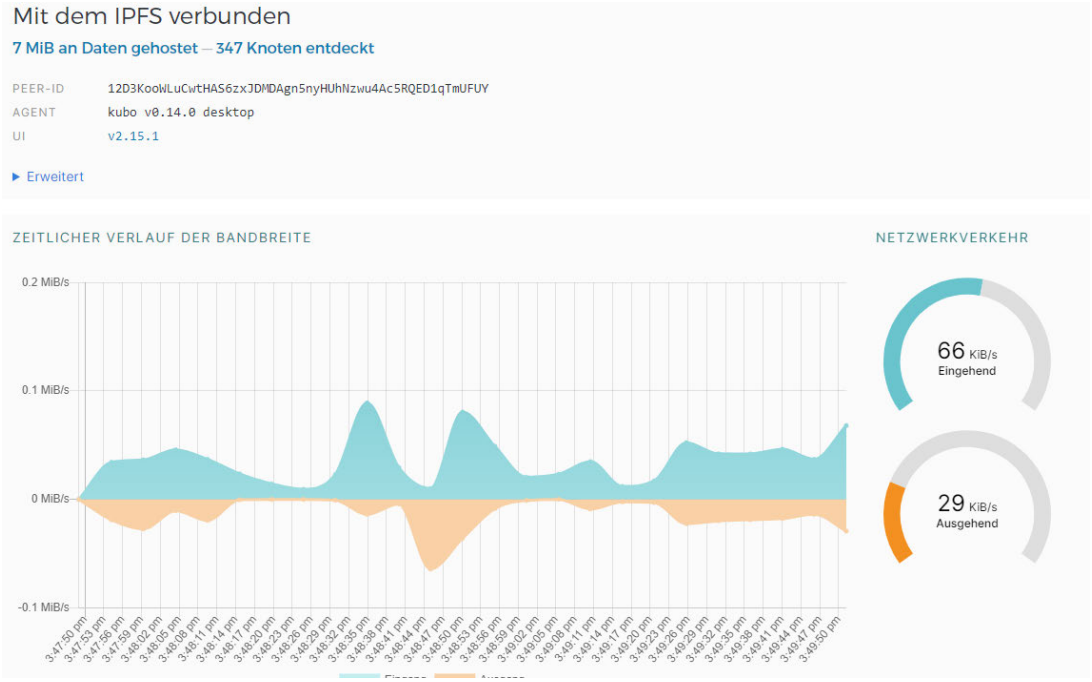

Abbildung 37: Verbindung zum IPFS-Netzwerk mithilfe eines eigenen Knotens

Das Problem bei der Integrierung in den Prototypen lag an der Verbindung zum public Gateway. Die Benutzung des öffentlichen Gateways (https://ipfs.io/ipfs/), des privaten (http://127.0.0.1:8080) und die Benutzung der Infura-API (https://ipfs.infura.io:5001/api/v0) haben nicht funktioniert. Dies lässt darauf schlussfolgern, dass es ein Problem im Programmcode gibt. Dieser konnte jedoch nicht identifiziert werden.

Anhang 3.5.2: The Graph

Die Integrierung von The Graph beinhaltet folgende Definierungen: GraphQL Schema und Subgraph Manifest.

Das GraphQL Schema beschreibt die Daten, die abgefragt werden können (s. Listing 5). Die einzige Entität des Blogs ist ein Beitrag.

```
type Post @entity {
  id: ID!
  title: String!
  contentHash: String!
  published: Boolean!
  postContent: String!
  createdAtTimestamp: BigInt!
  updatedAtTimestamp: BigInt!
}
```

Listing 5: Entität eines Beitrages

Dies ermöglicht es nun im folgenden „Playground“ mithilfe dieser Daten Abfragen zu schreiben (s. Abb. 38).

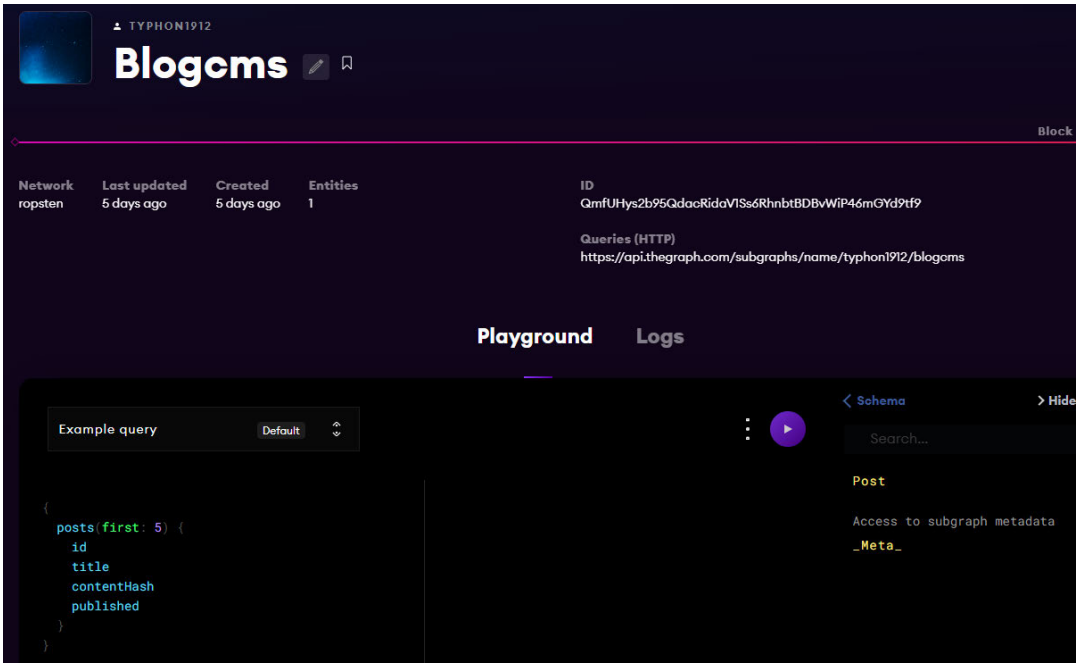

Abbildung 38: Subgraph des Blogs (thegraph.com)

Anhang 3.6: Berechnung der Deployment-Kosten

Die Errechnung der Entwicklerkosten lassen sich über die Transaktionsübersicht des Smart Contracts kalkulieren (s. Abb 39). Diese lassen sich mithilfe von Analyseseiten wie etherscan Aufrufen.

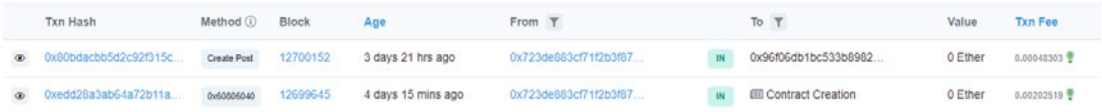

Abbildung 39: Transaktionsübersicht des Smart Contracts vom Web3-Blog (etherscan.io)

In der Übersicht der Transaktionsdetails des Smart Contracts befindet sich der Unterpunkt „Gas Limit & Usage by Txn“ (s. Abb. 40). Da die Preise für das Testnetzwerk um ein Vielfaches niedriger sind, muss diese Anzahl nun mit dem aktuellen Preis für Gas multipliziert werden.

Abbildung 40: Anzahl benutztes Gas für die Ausführung dieser Transaktion

Der aktuelle durchschnittliche Preis pro eine Einheit ist 25 gwei (1 gwei = 0,00000000159 ETH) (s. Abb. 41).

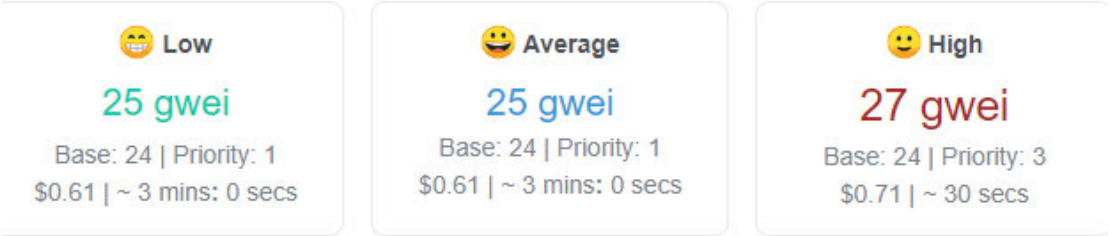

Abbildung 41: Gas-Preise am 04.08.2022 (5:33 pm)

Würde der Smart Contract in diesem Monat auf das Ethereum-Mainnet deployen kostet es:

1.350.132 * 25 gwei = 33.753.300 gwei = 0,053549 ETH

Mit dem aktuellen Preis von ETH multipliziert:

0,053549 ETH * $ 1.612,20 = **$ 86,33**

Der HAW Token würde 0,030407 ETH ($ 49,02) und der HAW Zugangsblock NFT 0,005021 ETH ($ 8,09) kosten.

Anhang 3.7: Aktivitätstabelle

Aktivität	**Dauer**	**Komplexität**
Recherche zur Ideenfindung	Ca. eine Woche für die Grundidee (~5 Stunden)	Mittel – dies beinhaltete Informationen durch Videos und Artikel zu sammeln. Wunsch nach sinnvollem Prototyp nicht erfüllbar, durch die Komplexität.
Back End des Blogs (Smart Contract, Tools)	Mithilfe verschiedener Tutorials und Foreneinträgen ca. eine Woche (~20 Stunden)	Hoch – viele neue Inhalte im Bereich des Codings. Grundverständnis für Solidity bekommen und JavaScript. Viele neue Konzepte in kurzem Zeitraum. Verschiedene Tools ausprobiert und am Ende für Hardhat entschieden.
Front End des Blogs	~ 3 Stunden Mithilfe von Vorlagen	Hoch/Niedrig – eigentlich Hoch durch das fehlende Verständnis mit React. Jedoch wurde sich hier auf Vorlagen bezogen.
IPFS	Ca. 3 Wochen, durchgängig präsent. Viele ungenaue Stunden für Error und Problemlösungsversuche (~20 Stunden)	Sehr hoch – IPFS ist ein komplett neuartiges System und für unerfahrene in dem Bereich komplex (vgl. Bit2Me Academy 2021). Das Aufsetzen des Clients und Netzwerkes ist nicht komplex. Das Einsetzen der Funktionalitäten im Smart Contract trotz Tutorials und privater Hilfe aus eigenen Foreneinträgen ist fehlgeschlagen.
The Graph	Ca. 3 Tage mit Error-Behandlungen (~ 8 Stunden)	Mittel – The Graph besitzt eine einsteigerfreundliche Dokumentation und kann beliebig tief komplex werden. Die Aufsetzung des Subgraphs ging Problemlos. Das Erstellen des GraphQL Schemas führte zu mehreren behebbaren Errors.

Token erstellen	Ca. 1 Tag (~5 Stunden)	Niedrig – Erstellung eines ERC-20 Standardtokens ist durch das Vorhandensein eines vorgefertigten Standards nicht komplex. Auch ohne Verständnis von Solidity lässt sich ein Token erstellen.
NFT erstellen und veröffentlichen	Ca. 1 Tag (~5 Stunden)	Niedrig – das Arbeiten mit OpenSea vereinfacht die Erstellung eines NFTs und ist ähnlich beim Token durch einen Standard Smart Contract leicht zu erstellen. Die kreative Arbeit der eigentlichen Animation hat die Mehrheit der Zeit in Anspruch genommen.
Allgemeine Recherche des Themas	Seit mehreren Monaten (ungenaue Stundenanzahl, mit ca. ~3 Stunden pro Tag (im Durchschnitt) min. 120 Stunden)	Hoch – Web3 ist ein stetig wandelnder Markt und von einem Tag auf den anderen können komplette Blockchains vom Markt verschwinden. Die Technologien hinter den Kulissen sind komplex und die Grundlagen dieser Bachelorarbeit kratzen nur an der Oberfläche des Möglichen.

Tabelle 19: Aktivitätstabelle mit jeweiliger Dauer und Komplexität

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

Ort	Datum	Unterschrift im Original