Hochschule RheinMain
Fachbereich Design Informatik Medien
Studiengang Angewandte Informatik

Bachelor-Arbeit
zur Erlangung des akademischen Grades
Bachelor of Science - B.Sc.

Untersuchung von DAOs mit Fokus auf Dezentralität

vorgelegt von **Kiril Shterjov**
Matrikelnummer 1124394
Eichendorffstr. / 16
65187 Wiesbaden

am 06.12.2022

Referent: Prof. Dr. Marc-Alexander Zschiegner
Korreferent: Prof. Dr. Michael Ricken
Betreuer extern: Alexander Krahl

Durchgeführt bei der Daubit GmbH
Riederbergstraße. / 3, 65197 Wiesbaden

Formales

Erklärung gem. ABPO, Ziff. 4.1.5.4 (3)

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

Ort, Datum Unterschrift Studierender

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

Verbreitungsform	**ja**	**nein**
Veröffentlichung des Titels der Arbeit im Internet	X	
Veröffentlichung der Arbeit im Internet	X	

Ort, Datum Unterschrift Studierender

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Motivation

Die Entwicklung der Blockchain-Technologie hat gezeigt, dass die Anwendung dieser Spitzentechnologie vielseitig ist. Diese bietet wesentlich mehr Potenziale als die Schaffung und Verwaltung von Kryptowährungen.
Eines dieser Potenziale ist die **Dezentrale Autonome Organisation (DAO)**. In dieser Arbeit wird das untersucht, besonders wird Akzent auf die Governance von DAO geben. Ziel dieser Arbeit ist es, einen guten Eindruck zu bekommen, was DAO bedeutet und was ihre Stärken, Schwächen und Herausforderungen sind, in der dezentralisierten Welt, die in der Öffentlichkeit immer mehr an Beliebtheit gewinnt.

1.2 Umfeld

Diese Arbeit wurde beim Unternehmen Daubit Programmierung Service GmbH durchgeführt. Daubit, ein inhabergeführtes Unternehmen mit Sitz in Wiesbaden, existiert seit 2008 und bietet Dienstleistungen im Bereich der App- und Web-Programmierung, sowie von Blockchainprojekten. Seit der Gründung im Jahr 2008 haben sich seine Tätigkeitsfelder kontinuierlich ausgebaut. Momentan besteht es aus ungefähr 10 Personen, die in verschiedenen Bereichen tätig sind. Mehr Informationen lassen sich über Daubit Webseite, `www.daubit.org`, erfahren.

Kapitel 2

Grundlagen

Dieses Kapitel ist in vier Unterkapitel geteilt. Das Erste wird die Blockchain-Technologie, das Zweite die Ethereum-Blockchain, das Dritte die DAO und das Vierte die Unterschiede zwischen DAO und traditionelle Unternehmen beschreiben.

2.1 Blockchain

In diesem Abschnitt wird die Blockchain-Technologie als Baustein für die Dezentralität erklärt.

Die Entwicklung dieser Technologie ist mit der Idee auf elektronisches Geld verknüpft. Der erste Gedanke für die Dezentralität existierte seit geraumer Zeit. Die Blockchain-Technologie ist keine neue Technologie, häufig wird die Erscheinung von Bitcoin als Anfang dieser Technologie bezeichnet. In der Vergangenheit haben viele Wissenschaftler versucht, ein geeignetes Protokoll für die Dezentralität zu entwickeln. Das erfolgreichste und bis jetzt sicherste Protokoll hat Satoshi Nakamoto in 2008 in White Paper veröffentlicht (vgl. [Sat08]). Es erläutert die Grundlagen von **Bitcoin** - digitales Währungssystem und beschreibt die Blockchain-Technologie als Zusammenspiel mehrerer bereits bestehender Technologien.

Eine Blockchain bezeichnet eine kontinuierlich erweiterbare Liste von Datensätzen "Blöcke", die mittels kryptografischer Verfahren miteinander verkettet sind. Jeder Block enthält dabei typischerweise einen kryptografisch sicheren Hash (Streuwert) des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten (vgl. [Luc20, S.221]). Anders gesagt, Blockchain ist eine Reihe von digitalen Datenblöcken, die in eine Kette hintereinander geschaltet werden.

Da es keine universelle Blockchain gibt und um ihre Definition und Funktion zu verdeutlichen, wird die Anwendung der Blockchain anhand des Bitcoin-Protokolls erklärt.

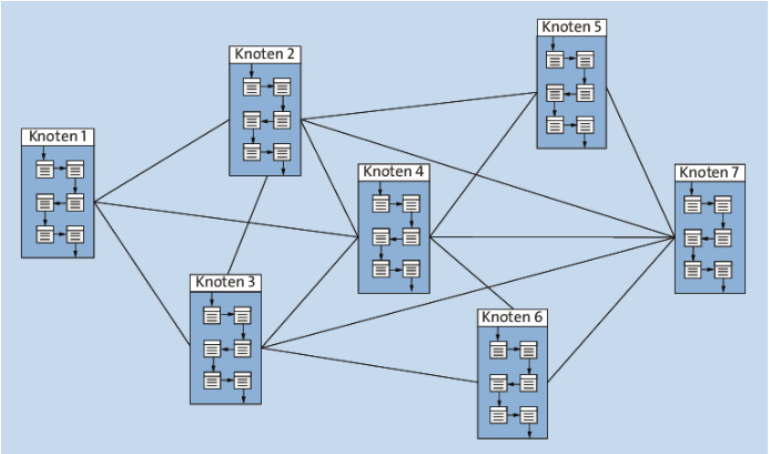


Abbildung 2.1: Übersicht eines Blockchain-Netzwerks (vgl. [SF19, S.27])

In Abbildung 2.1 lässt sich erkennen, dass es keine zentrale Instanz gibt. Um Dezentralität zu erschaffen, werden kryptografische Methoden, wie asymmetrische Verschlüsselungsverfahren (AV) bzw. Public Private Key-Verfahren, kryptografische Hashfunktionen, Merkle-Bäume, Elliptic Curve Cryptography (ECC) etc., verwendet.

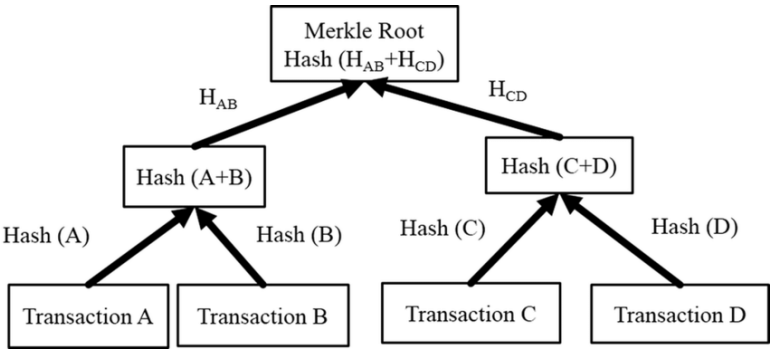


Abbildung 2.2: Merkle Tree [Nnk+18]

Ein Block besteht aus zwei wichtigen Komponenten, Block-Header und Transaktionen. Auf der untersten Ebene sind die Transaktionen, die je nach Art der Blockchain-Plattform in einem eigenen Format codiert sind. Damit die einzelnen Teilnehmer durch Transaktionen, Datensätze oder Ereignisse mit dem Netzwerk interagieren können, benötigen sie Adressen. Zudem müssen sie beweisen, dass sie wirklich der Inhaber dieser Adresse sind. Hier wird das AV benutzt, um Adresse aus Public Key zu erzeugen. Das System generiert dem Teilnehmer einen zufälligen Private Key und berechnet daraus den zugehörigen Public Key (vgl. [SF19, S.27]). Außer AV wird hier auch ein Merkle-Baum verwendet. Merkle-Baum besteht aus mehreren Hash-Werten. Jeder Hash-Wert ist eine Transaktion des Blocks und ist als Blatt im Merkle-Baum dargestellt. Es werden zwei Hash-Werte verkettet, indem sie wieder gehasht werden. Das Ergebnis dieser Verkettung wird in die nächste Ebene geschrieben (siehe Abbildung 2.2). In dem obersten Wert, genannt Root-Hash, sind Informationen aller im Block befindlichen Transaktio-

nen verschmolzen. Dieser Wert ist bei Block-Header repräsentiert. Der Hauptgrund, warum hier Merkle-Baum verwendet wird, ist die Reduzierung des Aufwands für die Überprüfung der Transaktionen. Statt eines Aufwands von n (n=Anzahl der Transaktionen) benötigt der Merkle-Baum einen Aufwand von log(n) (vgl. [SF19, S.91]). Wenn es z. B. Transaction C in Abbildung 2.2 überprüft werden muss, benötigt man nur den Hashwert von Transaktion D, Hashwert von (A+B) und den Roothash.

Der Block-Header besteht auch aus Zeitstempel, Target, voriger Block-Hash, Nonce (number used only one) und Version. In Abbildung 2.3 kann man die Struktur und Verkettung von Blöcken betrachten. Der vorige Block-Hash wird aus den Daten des vorherigen Blocks gebildet und in den nächsten Block-Header mitaufgenommen. Die einzige Ausnahme ist der erste Block. Hier wird kein voriger Block-Hash zur Verfügung stehen. Als Hash-Wert bekommt er üblicherweise den Hashcode 0x0 (vgl. [SF19, S.184]). Dieser Block kann genutzt werden, um eine eigene private Blockchain zu erstellen und wird deshalb auch Genesis Block genannt. Ein weiteres wichtiges Merkmal ist die Non-

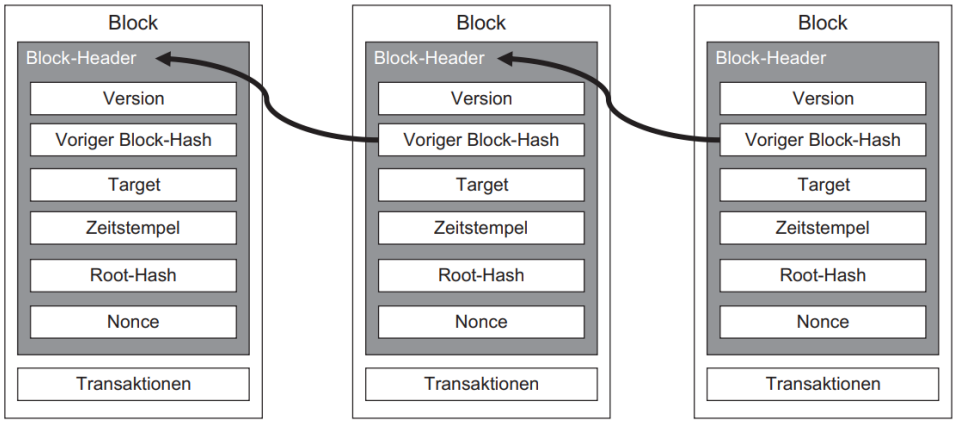


Abbildung 2.3: Struktur und Verkettung von Blöcken (vgl. [FM20, S.12])

ce. Nonce ist die beliebige Zahl und ist sehr bedeutend für den Konsensmechanismus von Bitcoin. Diese Nummer ist der Hauptgrund für die Verteilung der Teilnehmer von Bitcoin-Blockchain in passive und aktive Teilnehmer. Die aktiven Teilnehmer (Miner) müssen eine Zahl finden, sodass der Hashwert des Blocks kleiner als eine bestimmte Obergrenze ist (Mining). Diejenige, die nicht teilnehmen möchten, heißen passive Teilnehmer. Ein passende Nonce ist der Arbeitsnachweis (Proof of Work) der Miner (vgl. [Ant18, S.233]). Die passende Nonce zu finden, kostet viel Geld aufgrund der Strom- und Hardwarekosten, weil es komplexe Berechnung ist. Miner arbeiten daher in Form von Mining-Pools zusammen. Sie bündeln ihre Hashing-Leistung und teilen die Belohnung unter den Teilnehmern auf [Ant18, S.253].

Wenn jemand versucht, ein Block zu manipulieren, verändert sich der Hashwert dieses Blocks und damit die Hashwerte von folgenden Blöcken. Man kann also leicht erkennen, an welcher Stelle genau die Änderung ist. Damit ist Manipulation an beliebiger Stelle nicht möglich.

Diese Erfindung von Satoshi Nakamoto ist der dezentralisierte Mechanismus für entstehenden Konsens. Entstehend, weil der Konsens nicht explizit erreicht wird. Vielmehr ist der Konsens ein entstehendes Artefakt der asynchronen Interaktion Tausender unabhängiger Nodes[1], die alle einfachen Regeln folgen (vgl. [Ant18, S.219]). Bitcoins Konsensmechanismus ist, zumindest theoretisch, anfällig für Angriffe durch Miner (oder Pools). Ein Angriffsszenario gegen den Konsensmechanismus wird 51-%-Angriff genannt. Bei diesem Szenario tut sich eine Gruppe von Minern zusammen, die den Großteil der Hashing-Leistung des Netzwerks (51 %) unter ihrer Kontrolle haben, um Bitcoin anzugreifen. Da sie den Großteil der Blöcke schürfen, können sie bewusst Forks erzeugen und Transaktionen doppelt einlösen (Double-Spending) oder DoS-Angriffe gegen bestimmte Transaktionen oder Adressen fahren. Bei einem Fork/Double-Spend-Angriff sorgt der Angreifer dafür, dass bereits bestätigte Blöcke für ungültig erklärt werden, indem er einen Fork und den Wechsel zu einer anderen Chain erzwingt (vgl. [Ant18, S.257]). Die massive Zunahme der Hashing-Leistung macht den Bitcoin gegen Angriffe durch einzelne Miner immun. Ein Solo-Miner kann nur einen kleinen Prozentsatz der gesamten Hashing-Leistung kontrollieren. Allerdings birgt die durch die Mining-Pools erfolgte Zentralisierung das Risiko gewinnorientierter Angriffe durch Poolbetreiber. Der Betreiber eines Managed Pools kontrolliert die Erzeugung von Anwärterblöcken, und er kontrolliert auch, welche Transaktionen enthalten sind. Der Poolbetreiber hat die Möglichkeit, Transaktionen auszuschließen oder Double-Spending-Angriffe durchzuführen. Erfolgt dieser Missbrauch der Leistung in eingeschränkter und unauffälliger Form, kann ein Poolbetreiber nachhaltig Profit aus dem Konsensangriff schlagen, ohne weiter aufzufallen (vgl. [Ant18, S.259]). Beispiele für erfolgreiche Forks sind Bitcoin Cash und Bitcoin Gold (vgl. [Ant18, S.262]).

Seit der Veröffentlichung von Bitcoin wurden die Ideen von Satoshi Nakamoto in zahlreichen Projekten verändert und aufgebaut. Ein solches erfolgreiches Projekt ist die Plattform Ethereum mit seiner Smart Contracts. Bei Ethereum ist nicht nur möglich, Zahlungsvorgänge abzubilden, sondern auch einen Programmiercode in der Blockchain zu speichern (vgl. [SF19, S.113]). An diese Weise entstanden im Lauf der Zeit viele unterschiedliche Blockchains.

2.2 Ethereum

Ethereum wird als Blockchain der zweiten Generation - *Blockchain 2.0* bezeichnet, da hier mehr Funktionen möglich sind.

Dieses Projekt ist im Jahr 2013 von Vitalik Buterin in einem Whitepaper vorgestellt worden [Vit22]. Vitalik hatte die Idee, eine Plattform zu erstellen, die auf Blockchain-Technologie basierend und zusätzlich die Erstellung von dezentralen verteilten Applikationen zu ermöglichen.

[1] `https://nodes.com/#nodes-definition`

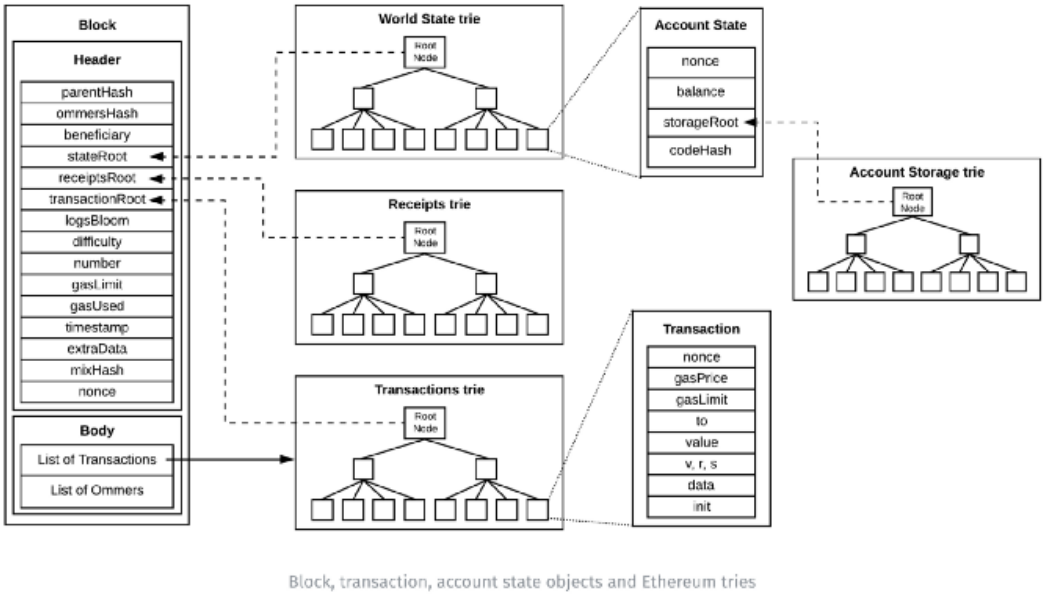


Abbildung 2.4: Blocks Struktur in Ethereum [luc22]

Ähnlich wie bei Bitcoin besteht bei Ethereum ein Block aus Header und Transaktion (siehe Abbildung 2.4). Im Unterschied zu Bitcoin ist bei Ethereum der Block-Header erweitert. Es gibt insgesamt drei Roothashes, einen für Transaktionen, einen für Empfänger und einen für den Zustand. Der Hauptunterschied zwischen Ethereum und Bitcoin in Bezug auf die Blockchain-Architektur besteht darin, dass Ethereum-Blöcke im Gegensatz zu Bitcoin-Blöcken eine Kopie, sowohl der Transaktionsliste, als auch des neuesten Zustands, enthalten. Außerdem werden noch zwei weitere Werte im Block gespeichert, die Blocknummer und die Schwierigkeit(difficulty)[Vit22].

Die Ethereum-Blockchain ermöglicht, im Unterschied zu Bitcoin, das Erstellen von Programmen auf der Blockchain (Smart Contracts). Die Smart Contracts in Ethereum bestehen aus Code, der in sogenannten Contract Accounts gespeichert wird und in der Ethereum Virtual Machine (EVM) ausgeführt wird. Um Smart Contracts zu programmieren, wird am häufigsten mit Abstand die Programmiersprache Solidity verwendet (vgl. [SF19, S.315]). Das Zahlungsmittel und die Währung im Netzwerk wird Ether genannt.

Die EVM ist der Teil von Ethereum, der das Deployment und die Ausführung von Smart Contracts übernimmt. Auf hohem Niveau kann man sich die EVM, die auf der Ethereum-Blockchain läuft, als globalen, dezentralisierten Computer mit Millionen ausführbarer Objekte mit eigenem permanentem Datenspeicher vorstellen (vgl.[AW19, S.297]). In Abbildung 2.4 kann man bemerken, dass die Transaktionen Gasprice und Gaslimit enthalten. Gas ist Ethereums Maßeinheit für die Rechen- und Speicherressourcen, die nötig sind, um Aktionen in der Ethereum-Blockchain durchzuführen. Gas erfüllt zwei Aufgaben: Es dient als Puffer zwischen dem Ethereum-Preis und der Belohnung, die Miner für ihre Arbeit erhalten, und als Schutz vor Denial-of-Service-Angriffen

(vgl.[AW19, S.313]). Soll die EVM eine Transaktion abschließen, wird ihr im ersten Schritt die Gasmenge zugewiesen, die als Gaslimit in der Transaktion festgelegt wurde (vgl.[AW19, S.314]).

Die Smart Contracts sind das Herzstück einer DAO. DAO ist erst mal von Vitalik in gleichem Whitepaper vorgestellt. Diese Art von Organisationen wird in nächsten Kapiteln detailliert beschrieben.

2.3 DAO

Dieses Kapitel taucht kurz in die Welt der DAOs ein. In letztem Unterkapitel wird ein Überblick über die Unterschiede zwischen einer DAO und einer traditionellen Organisation gegeben.

2.3.1 Geschichte

Das erste DAO-Projekt - *The DAO* wurde im April 2016 erstellt. Diese DAO war ein kollektives Investitionsvehikel, das als rationalistische Form des Crowdfundings, als dezentraler Risikofonds konzipiert war und zum ersten Mal zeigte, wie sich eine solche dezentrale Organisation, die durch einen Code betrieben wird, selbst verwalten kann. Die Teilnehmer zahlen ETH in die DAO ein und erhalten DAO-Token, die den finanziellen Anteil des Inhabers an der DAO, sowie das Stimmrecht repräsentieren (vgl. [Pat21]).

Das Ziel ist, dass jeder seine Ideen und Projekte der DAO-Community vorstellen kann und potenziell Investitionsgelder von der DAO erhalten kann. Auch jeder, der einen DAO-Token besitzt, kann über den Investitionsplan abstimmen.

Mit mehr als 11.000 Mitgliedern, hat *The DAO* es geschafft, mehr als 150 Millionen Dollar zu sammeln. Aber wegen eines Programmierfehlers, "*recursive call vulnerability*", in einem Code des Smart Contract, wurde diese im Juni des gleichen Jahres gehackt. Der Angreifer konnte etwa 3,6 Millionen ETH stehlen. Das spielte auch eine Rolle beim Hard Forking (vgl. [Ant18, S.257]) von Ethereum, das notwendig war, um das ganze Geld zu retten.

Diese Sicherheitsprobleme haben die Entwicklung von DAO stark eingeschränkt [Wan+19]. Trotz des Misserfolgs der ersten DAO, gab es eine Reihe wichtiger Experimente, die den Weg für moderne DAOs ebneten. In letzter Zeit sind mehrere Plattformen entstanden, um den Einsatz von DAOs auf der Blockchain zu erleichtern. Die Hauptplattformen heute sind *Aragon, Colony, DAOstack* and *DAOhaus* [EFAH20].

Aragon ist eine Plattform für die Erzeugung einer DAO. Es ist eine Suite von Anwendungen und Diensten, die neue Formen globaler Gemeinschaften ermöglichen. *Aragon* kann eine lange Reihe von DAOs freischalten, die nicht nur auf Protokolle wie Ethere-

um oder Bitcoin beschränkt sind [Ara22].

Colony ist ein umfassendes Framework für DAOs, die auf Ethereum implementiert ist. Es ist vollständig dezentralisiert, völlig vertrauenswürdig und zu 100 % Open Source.[Col22] Im Gegensatz zu anderen DAOs, befürwortet Colony das Erfordernis der Stimmabgabe der Mitglieder zu beseitigen. Stattdessen, konzentriert es sich auf Mechanismen, die Menschen dazu zwingen, ihren Job zu erledigen.

DAOstack ist ein Open-Source-Software-Stack, der zur Unterstützung eines globalen kollaborativen Netzwerks entwickelt wurde. Der Stack kann verwendet werden, um Organisationen für jede Art von kollektiver Arbeit aufzubauen, und er enthält auch Tools, um diese Organisationen miteinander zu verbinden, sodass alle seine Mitgliedsorganisationen gestärkt werden, wenn das Netzwerk wächst[DAO22].

DAOhaus ist ein Fork der Smart Contracts von Moloch DAO. Moloch, der als alter Opfergott bezeichnet wird, versucht eine Infrastruktur zu fördern, in der der kollektive Nutzen immer größer ist als der individuelle Nutzen einer bestimmten Einheit. Moloch DAOs haben ein Abstimmungssystem, das versucht, Angriffe und Missbrauch zu minimieren. Im August 2019 wurde DAOhaus als Schnittstelle geschaffen, um dies zu ermöglichen, jedermann ein Moloch-ähnliches DAO einzusetzen, indem er ein paar Parameter einstellt, wie Name, Währung, Tributgröße usw.[EFAH20]

2.3.2 Definition

Es gibt keine einheitliche Definition von DAO. DAO kann man beschreiben als eine Art Blockchain-basierter Anwendungen, die durch eine Reihe von Regeln reguliert wird, die von ihren gewählten Mitgliedern geschrieben wurden und automatisch bestimmte Aufgaben ausführen [Wan+19]. Eine DAO ist eine Organisation, die autonom agiert, ohne eine zentrale Instanz zu benötigen. Der wichtigste Aspekt von DAOs ist, dass sie sich im gemeinsamen Besitz ihrer Mitglieder befinden und von ihnen verwaltet werden (durch den Besitz digitaler Token).

Der Hauptteil einer DAO ist der Governance Contract. Außer den Governance Contract, könnte eine DAO auch weitere Contracts besitzen, die bestimmte Zwecke erfüllen. Da DAO eine Blockchain-Plattform ist und damit alles einwandfrei funktioniert, besteht diese auch aus Minern, Benutzern und Entwicklern. Alle Mitglieder besitzen Governance Token. Sie können sie benutzen, um Änderungen in Organisation vorzuschlagen (Proposals). Dieser Token bestimmt auch, ob die Organisation diese Proposals abnimmt oder ablehnt, denn das Votingsystem ist nur mit dem Governance Token möglich. Jede DAO hat eigene Regeln, die im Governance Contract beschrieben sind und analog beschreibt, wie das System reguliert ist. Wenn jemand dem DAO beitritt, stimmt er normalerweise dem Smart Code bzw. diesen Regeln zu. Jede Änderung des Codes erfordert normalerweise eine Abstimmung unter den Mitgliedern (vgl. [Eje22, S.32]).

Abbildung 2.5 gibt einen Überblick dafür, wie die Smart Contracts eine DAO regulieren.

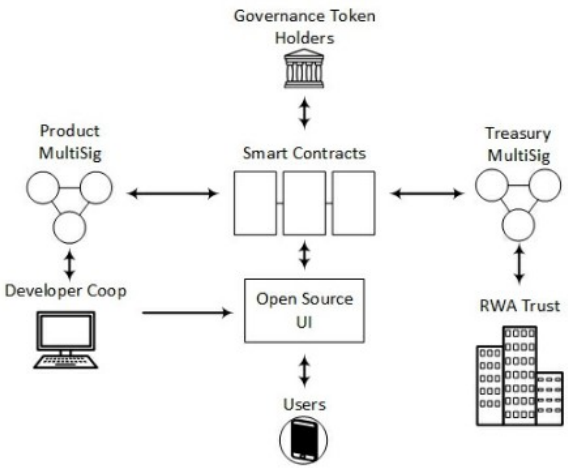


Abbildung 2.5: Die Struktur von DAO (vgl. [Eje22, S.33])

Der Vorgang zum Starten eines DAO-Projekts umfasst folgende Schritte (vgl. [Liu+21]):

1. Entwicklung und Einsatz von Smart Contracts nach vordefinierten Regeln
2. Behandlung von Token-Problemen (über ICO) in der anfänglichen Finanzierungsphase
3. Am Ende der Finanzierungsphase beginnt eine DAO zu laufen
4. Es werden Proposals gemacht und die Mitglieder können darüber abstimmen

Neben diesen vier Hauptschritten müssen noch weitere Entscheidungen während der Erstellung getroffen werden, wie z.B. auf welche Blockchain die Organisation laufen soll, die Definition der Dao-Ziele und die Bildung der DAO-Community etc. [Eje22, S.63ff]

Je nach Zweck dieser Organisationen werden sie häufig in acht Typen eingeteilt: Protocol DAOs, Grant DAOs, Philantropy DAOs, Social DAOs, Collector DAOs, Venture DAOs, Media DAOs und Sub DAOs[Eje22, S.48f]. Ein Beispiel für Protocol DAOs sind in dieser Studie untersuchte DAOs, Compound ,Uniswap und Evmos.

2.4 DAOs vs Traditionelle Organisationen

DAOs	**Traditionelle Organisationen**
sind in der Regel demokratisch und vollständig	haben in der Regel eine klare Hierarchie
Änderungen werden nur mit Abstimmung der Mitglieder durchgeführt	Änderungen werden mit Abstimmung der Mitglieder oder können mit der Entscheidung einiger Personen durchgeführt werden
die Stimmen werden ohne vertrauenswürdigen Vermittler automatisch berechnet	die Stimmen werden manuell gezählt
Dienstleistungen werden automatisch und dezentral erbracht	erfordert manuelle Verarbeitung oder automatische zentrale Kontrolle
alle Aktivitäten sind offen und transparent	in der Regel werden die Äktivitäten werden privat durchgefürt und sind nicht öffentlich zugänglich

Tabelle 2.1: Vergleich zwischen DAO und traditionelle Organisationen

Die DAOs haben viele Vorteile gegenüber traditionellen Organisationen. Sobald die Governance Smart Contract von DAO deployed ist, gehört die Organisation keiner einzelnen Person, sondern allen Mitgliedern der DAO. Deshalb lässt sich daraus schließen, dass DAO keine Hierarchie ist bzw. kein Direktor oder Vorsitzenden hat. Dies trägt dazu bei, dass jeder in der Organisation an wichtigen Entscheidungen mitwirken (mit Abstimmung) kann, was nicht der Fall bei traditionellen Organisationen ist. Ein weiterer Vorteil ist, dass die Abstimmungen jeder Zeit möglich sind und die Stimme während der Abstimmung von Mitgliedern automatisch gezählt werden. Darüber hinaus können die Voters die Ergebnisse verfolgen, egal ob die Abstimmung beendet ist oder nicht. Das, was die DAO besonders attraktiv macht, ist seine dezentrale Natur. Im Unterschied zu einer traditionellen Organisation, sind bei der DAO alle Aktivitäten offen und transparent.

Wie bei jeder Organisation, hat die DAO auch Nachteile. Die DAOs existieren nur online, was sie von Internet und Strom abhängig macht. Ein anderer Nachteil sind die rechtlichen Fragen der DAO. Bevor man eine DAO erstellt, muss sich die Frage beant-

worten, wie und ob diese Organisationen rechtlich erlaubt sind bzw. ob es solche Form von Organisationen in dem Staat der Erstellung überhaupt gibt. Außerdem ist die DAO eine neue institutionelle Form, was dazu beiträgt, auf die Chancen um einen Erfolg der Organisation zu zweifeln.

In Abbildung 2.1 lassen sich die Hauptunterschiede zwischen DAO und traditionelle Organisation einsehen.

Kapitel 3

Untersuchung des DAOs

In diesem Kapitel werden alle untersuchten DAOs vorgestellt. Darüber hinaus werden die Untersuchungskriterien beschrieben und schließlich die Untersuchungsergebnisse dargestellt.

3.1 Vorstellung des untersuchten DAOs

Untersucht werden drei DAOs, *Compound DAO, Uniswap DAO* und *Evmos DAO*. Es handelt sich um drei verschiedene DAOs, die unterschiedliche Ziele als Organisation haben und differente Governance Regelungen. Alle drei DAOs haben einen On-Chain Governance Mechanismus.

Compound ist ein EVM-kompatibles Protokoll. Das Hauptziel von Compound ist, seinen Nutzern zu ermöglichen, Zinsen von ihren Kryptowährungen zu erhalten, indem sie diese in einen Pool, der von der Plattform unterstützt werden, einzahlen. Wenn ein Nutzer Tokens in einen Compound-Pool einzahlt, erhält er im Gegenzug cTokens. Wenn man zum Beispiel ETH in einen Pool einzahlt, erhält man dafür cETH. Im Laufe der Zeit steigt der Wechselkurs der cTokens des ursprünglichen Assets, was bedeutet, dass man für sie eine höhere Summe des ursprünglichen Vermögenswerts einlösen kann als man anfangs eingesetzt hat — auf diese Weise werden Zinsen verteilt[Com22e].

Compound wurde 2017 von Robert Leshner und Geoffrey Hayes gegründet. Am Anfang wurde das Protokoll zentral kontrolliert und im Laufe der Zeit wurde die Kontrolle dezentral durch die DAO übernommen.

Das Compound-Protokoll wird von COMP-Token-Inhabern geregelt und aktualisiert, wobei drei verschiedene Komponenten verwendet werden: der COMP-Token, das Governance Modul und Timelock. Zusammen ermöglichen diese Smart Contracts der Community, Änderungen (Proposals) durch die Verwaltungsfunktionen eines cToken oder des Comptrollers vorzuschlagen, abzustimmen und umzusetzen. CTokens sind das primäre Mittel zur Interaktion mit dem Compound Protocol. Wenn ein User einen cTo-

ken minted, einlöst, ausleiht, zurückzahlt, oder überträgt, tut er dies unter Verwendung des cToken-Contract [Com22d]. Auf der anderen Seite ist der Comptroller die Risikomanagementlayer des Compound-Protokolls, die bestimmt, wie viel kollateral ein User halten muss und ob (und um wieviel) ein Benutzer liquidiert werden kann [Com22c]. Die Proposals können Systemparameter ändern, neue Märkte unterstützen oder dem Protokoll völlig neue Funktionen hinzufügen(vgl. [Com22b]). Die Governance Smart Contract von Compound hat zwei Versionen: Governance Alpha und Governance Bravo.

Uniswap ist ein Protokoll für den automatisierten Token-Austausch auf Ethereum [Hay22]. Der Schöpfer der Plattform ist der Ethereum-Entwickler Hayden Adams. Er hat in 2018 zum erstmal Automated Market Maker (AMM)[1] in Blockchain-basierten dezentralen Börsen eingeführt. Der Unterschied mit anderen Börsen ist, dass hier man keine Auftragsbücher(eng. *order books*) benutzt, sondern Liquidität.

Das Uniswap-Protokoll ist dezentral durch die DAO kontrolliert. Ähnlich wie bei Compound, wird das gesammte Protokoll von UNI-Token-Inhabern gesteuert und aktualisiert. Die drei wichtigsten Smart Contracts sind Uni-Token, das Governance Modul und Timelock. Diese zusammen ermöglichen, Änderungen am Uniswap-Protokoll vorzuschlagen, abzustimmen und umzusetzen. Die Governance Smart Contract von Uniswap hat drei Versionen: Governance Alpha, Governance Alpha2 und Governance Bravo.

Im Unterschied zu Compound und Uniswap, wurde **Evmos** nicht mit Ethereum, sondern mit Cosmos SDK[2] entwickelt. Aber die Applikationen von Evmos basieren auf EVM. Das macht Evmos besonders attraktiv für die Ethereum Entwickler.

Die Evmos-Blockchain bietet Ethereum-Entwicklern die Möglichkeit, ihre Smart Contracts auf dem Evmos EVM bereitzustellen und die Vorteile einer ProofofStake (PoS)-chain mit schneller Endgültigkeit zu nutzen. Entwickler profitieren auch von hochzuverlässigen Clients von Testnets, die zum Testen und Bereitstellen ihrer Verträge verwendet werden können. Evmos ist aber trotzdem an das Cosmos ökösystem anbegunden und mit diesem föderiert. Entwickler können auch von der Verwendung eines Bridge-Netzwerks (EVMOS als Tokenbridge ETH <-> Cosmos) profitieren, um die Interoperabilität zwischen Mainnet Ethereum und Evmos zu ermöglichen [Evm22b].

Der andere Unterschied zu Compound und Uniswap ist, dass es keine separate Governance Smart Contract gibt, sondern alle Regelungen als Code in die Blockchain Node Software beschrieben sind.

[1] `https://coinmarketcap.com/alexandria/glossary/automated-market-maker-amm`
[2] `https://github.com/cosmos/cosmos-sdk`

3.2 Untersuchungskriterien

Um eine bessere Ansicht des DAOs zu schaffen, werden seine Governance Regelungen untersucht.

Dabei werden folgende Kriterien berücksichtigt:

Votes: Hier werden die Regelungen des Votingmechanismus betrachtet. Welche Voraussetzungen müssen erfüllt werden, um die User an das Votingsystem teilnehmen zu lassen. Es werden außerdem alle mögliche Stimmoptionen der Voters und die Quorum und Threshold der Proposals untersucht.

Proposals: Es werden die Nummer der erstellten Proposals und ihre durchschnittliche Schaffung per Monat untersucht. Sobald die Nummer vorhanden ist wird die Erfolgsquote der Proposals berechnet. Darüber hinaus wird auch die Nummer der Proposers untersucht (alle Adressen, die mindestens ein Proposal erstellt haben).

Voters: Die Voters vermitteln ein klares Bild davon, wie der gesamte Prozess des dezentralisierten Wahlsystems abgelaufen ist. Deshalb dürfen sie bei der Untersuchung nicht vernachlässigt werden. Es werden die Anzahl der Voters per Proposal und gesamte unterschiedliche Voters, die am Voting System des DAOs beteiligt sind, untersucht. Es wird außerdem ein Überblick der Abstimmung geben.

Mithilfe von diesen drei Kriterien lässt sich die Statistik des DAOs darstellen. In der Tabelle 3.1 erhält man einen Überblick darüber, woraus die Statistik besteht.

Statistik	
Votes	• Voraussetzungen für die Teilnahme eines Votingsystems • Gesamte Stimmoptionen • Quorum • Threshold
Proposals	• Erstellte Propolsals • Erstellte Propolsals monatlich • Erfolgsquote • Unterschiedliche Proposers insgesamt
Voters	• Unterschiedliche Voters Adresse • Durchschnittliche Voters per Proposal • Erfolgsquote • Überblick der Abstimmung

Tabelle 3.1: Übersicht der Statistik

3.3 Aufbau der Untersuchung

Die Untersuchung des DAOs ist tatsächlich Datenanalyse. Um die gesamte Untersuchung durchzuführen, müssen große Mengen von Daten empfangen werden. Der gesamte Prozess ist im Next JS-Projekt durchgeführt und dargestellt. Während des Aufbaus dieses Frontend-Projektes werden TypeScript bzw. JavaScript und CSS (Tailwind CSS) Programmiersprachen benutzt. Die Quellen für den Aufbau sind online verfügbar[1]

Grundsätzlich ist der Untersuchungsaufbau in drei Teilen aufgeteilt. Die Informationen darüber wie z. B. das Votingssystem eines DAO geregelt ist und wieviele Stimmoptionen ein Voter hat, kann man von der Webseite des jeweiligen DAOs erhalten. Deshalb ist dieser Schritt der erste Teil der Untersuchung. Da Compound und Uniswap Governance Regelungen im separaten Smart Contract geschrieben sind, ist die Interaktion mit diesen zwei Smart Contracts der zweite Teil. Der dritte Schritt ist eine API-Anfrage, die die Daten von Evmos verfügt. Es wird WEB 3.0 benutzt, um die Interaktion mit Smart Contract zu machen und WEB 2.0 für die API-Anfrage. Es wurde versucht, so viele Daten wie möglich für Votes, Voters und Proposals zu sammeln. Um die dargestellten Ergebnisse zu bekommen, muss man die erzeugte Webseite über locale Server (localhost) starten.

3.3.1 Interaktion mit Smart Contract

Die beiden Ethereum kompatiblen Governance-Smart Contracts von Compound und Uniswap sind mit Solidity Programmiersprache geschrieben. Hier muss man die Syntax von Solidity kennen, um in der Lage zu sein, den Code von deployte Smart Contract zu lesen. Der Code vom Smart Contract ist Open Source und falls der deployte Smart Contract verifiziert ist, kann man in Etherscan (`https://etherscan.io/`) seinen Code problemlos sehen. Etherscan ist das vertrauenswürdigste Tool zum Navigieren durch alle öffentlichen Daten in der Ethereum-Blockchain. Zu diesen Daten gehören Transaktionsdaten, Wallet-Adressen, Smart Contracts und vieles mehr [coi22].

Etherscan hat ein breites Anwendungsspektrum:

a) Berechnung der Gasgebühren mit Gas Tracker

b) Smart Contracts suchen und verifizieren

c) Beobachtung der Live-Transaktionen, die auf der Ethereum-Blockchain stattfindet.

d) Möglichkeit zu entdecken, welche Smart Contracts einen verifizierten Quellcode haben.

[1] `https://gitlab.cs.hs-rm.de/kshte001/Bachelorarbeit`

e) Möglichkeit zu suchen, eine einzelne Transaktion aus einer beliebigen Ethereum-Wallet

f) Möglichkeit zu verfolgen, wie viele Smart Contracts ein User mit seiner Wallet autorisiert hat

g) etc

Die Interaktion mit dem Smart Contract erfolgt mit Hilfe von Web3. Es werden die Funktionen und Events vom schon geschriebenen Smart Contract aufgerufen, damit man die gesuchten Daten bekommt. Die Interaktion könnte nicht funktionieren ohne die deployte Adresse der Smart Contract und ihre Application Binary Interface (ABI) zu wissen. Die Information, welche Adresse zu einem Smart Contract gehört, lässt sich von der Webseite des bestimmten DAO erfahren. Um ABI zu erhalten, wird den Etherscan benutzt.

Der nächste Schritt ist das Lesen des Codes. Man muss die Funktionen aus dem Smart Contract, die die bestimmten Daten liefert, mit Web3 übersetzten. Aber die gesamten Events-Daten eines Smart Contract zu bekommen, muss sein Startblock und Endblock bekannt sein. Der Startblock ist der Block, wo der Contract deployt ist und der Endblock ist der letzte Block bzw. der aktuellste Block eines Smart Contract. Alle beiden Blocks lassen sich wieder mithilfe von Etherscan finden. Als Endblock bei Compound und Uniswap ist der Block mit der Nummer 15875000, der am 01.11.2022 um 12:52 Uhr erstellt worden ist. Somit zeigt diese Untersuchung nur die Events-Daten, die bis zu diesem Zeitpunkt passiert sind.

Während der Interaktion ist ein Problem aufgetreten, die mithilfe von Programmierungslösungen behoben wurde. Das größte Problem ist, dass die Ethereum Nodes Limit eingesetzt worden sind, wie viele Blocks auf einmal angefragt werden können. Bei Compound und Uniswap ist dieses Limit auf 100 000 Blöcke eingesetzt. Hier wurde Iteration aufgebaut, die mehrere Requests (bei Compound circa 25 Requests) in einen Array speichert. In Realität braucht man viel Zeit und Geduld wegen des Rate Limits der Requests.

Wenn die notwendigen Daten da sind, werden sie in eine globale Konstante gespeichert, die jederzeit über die Daten, ohne neue Anfrage ,verfügt. Die einzige Ausnahme ist die Erhaltung der Daten aus den Votecastevents, da der Abstand zwischen Start- und Endblock nicht mehr als 100.000 Blöcke beträgt. Daher kann eine Anfrage problemlos gestellt werden.

3.3.2 Web API Anfrage

Wie schon erwähnt, sind die Daten von Evmos DAO direkt von der Blockchain Node möglich zu bekommen. Alle Governance Regelungen sind als Code bzw. Abschnitt in

Comsos SDK Netzwerk geschrieben. Hier braucht man entweder ein Node oder API Endpunkte, um die Daten zu erhalten. Evmos verfügt über eigene API Endpunkte - `https://api.evmos.dev/`, wo alle Daten abrufbar sind.

Weil während der Untersuchung die API-Endpunkte von Evmos auf bestimmten Endpunkten keine Daten geliefert haben bzw. die Daten nicht archiviert waren (aktuell kann man die Daten bekommen, außer Votes-Daten), sind bei dieser Untersuchung die Daten von Mintscan Exolorer(`https://www.mintscan.io/evmos`) genutzt worden. Es werden mehrere Endpunkte von Mintscan Web-API benutzt. Die Endpunkte sind dynamisch gebaut, da es für jede erstellte Proposal Endpunkte existiert.

Wie bei Smart Contract Interaktionen sind auch hier einige Probleme aufgetreten. Weil es um größe Menge Daten geht, wurde wegen des Rate Limitings die IP-Adresse, die die Request macht, blockiert. Das Problem konnte mit Virtual Private Network (VPN) gelöst werden.

Ein weiteres Problem ist die Aufbewahrung der Voter Daten jedes Proposals. Aufgrund der großen Anzahl von Votern ist es sehr schwierig, Daten von allen Proposals zu erhalten. Aber es ist nicht unmöglich. In dieser Studie werden nur zwei Proposals berücksichtigt und nur deren Voters werden angezeigt.

Am Ende ist eine Funktion geschrieben, die alle Daten filtriert, um die Proposals zu zeigen, die zum ersten November erstellt werden sind.

3.4 Untersuchungsergebnisse

In diesem Unterkapitel werden alle bekommenden Daten mithilfe von Diagrammen bildlich dargestellt und ausgewertet.

3.4.1 Votes

*- **Voraussetzungen für die Teilnahme eines Votingsystems***

Die Teilnahme beginnt mit dem Governance-Token. Die Governance-Tokens werden oft an aktive Benutzer für ihre Loyalität und Beiträge zur Community vergeben. Token-Inhaber wiederum stimmen über wichtige Themen ab, um eine robuste Entwicklung der Projekte sicherzustellen. Typischerweise erfolgt die Abstimmung über Smart Contracts, wobei die Ergebnisse automatisch umgesetzt werden[Bin22]. Die einzige Voraussetzung, um für einen Proposal zu voten, ist die Verfügung von Votes bzw. delegated Votes. Wenn der Voter über keine Votes verfügt, kann er nicht abstimmen. Um Votes zu bekommen, muss der Voter seine Tokens an sich selbst oder an jemand anderen delegieren. Somit kann nicht nur die Adresse, die Token besitzt, abstimmen, sondern auch ein anderer Voter, der die delegierten Votes erhalten hat.

Die Governance-Tokens der untersuchten DAOs sind: COMP-Token bei Compound, UNI-Token bei Uniswap und EVMOS-Token bei Evmos.

- ***Quorum und Threshold***

Quorum und Threshold sind wichtige Merkmale eines DAO. Sie sind bei jedem DAO unterschiedlich. Das Quorum ist die Anzahl der Votes die Voters zusammen erreichen müssen, um die Ergebnisse am Ende zu zählen. Das ist ähnlich wie einen normalen zentralen Votingmechanismus. Das Threshold ist auf anderer Seite die Anzahl der Votes eines Proposer, der in der Lage ist, Proposal zu erstellen. Diese Mindestgrenze der Votes meistens ist schwer zu erreichen.

Das Threshold bei Compound beträgt 25 000 delegated COMP (0,25% of total Supply). Für ein Quorum reichen 400 000 Votes (4% of total Supply) aus. Bei Uniswap die Voraussetzung, um ein Proposal zu erstellen, beträgt 2,5 Millionen delegated UNI (0,25% of total Supply) und das Quorum beträgt 4 Millionen Votes (4% of total Supply). Für diejenigen, die nicht Threshold erreichen können, haben beide DAOs ein anderes Protokoll gebaut, wo man Autonomous Proposal erstellen kann [Com22a] . Um solche Proposal zu erstellen, muss der Proposer 100 delegated COMP bei Compound bzw. 400 delegated UNI bei Uniswap verfügen. Wenn ein Autonomous Proposal 10 Millionen delegated Votes bei Uniswap bzw. 100 000 delegated Votes bei Compound erhält, wird er in einen formellen Governance-Proposal umgewandelt, über den die Organisation abstimmt.

Das Threshold repräsentiert bei Evmos nicht die Voraussetzung für die Erstellung des Proposal, sondern ist Anzahl der Ja-Stimmen, um das Proposal erfolgreich zu sein und beträgt 50 % der teilnehmenden Stimmen. Es sind mindestens 33,4 % der Stimmrechte des Netzwerks (Quorum) erforderlich, damit der Proposal gültig ist. Auf der anderen Seite ist die Voraussetzung für die Erstellung des Proposal ein Deposit, das 192 EVMOS beträgt. Es gibt eine Deposit-Periode und jeder kann zu diesem Deposit beitragen. Das Interessant zu erwähnen ist, dass die beitragende Adresse ihrem Deposit in drei Fällen verlieren könnte: wenn das mindestens Deposit während der Deposit-Periode nicht erreicht wird, das Quorum fehlschlägt oder 33.4 % der Stimmrechte des Netzwerks mit NoWithVeto gestimmt haben.

- ***Stimmoptionen***

Die Stimmoptionen sind eng mit dem Erfolg eines Proposal verbunden. Je mehr Optionen es gibt, desto größer ist die Wahrscheinlichkeit, dass der gegebene Vorschlag nicht in Erfüllung geht.

Die Abstimmungsmöglichkeiten bei Compound und Uniswap waren anfangs nur Ja und Nein, aber in der späteren Entwicklung der Organisationen kommt eine weitere Enthaltungsstimme hinzu. Während beim neu geschaffenen EVMOS DAO die Stimmoptionen ganz am Anfang auf 4 eingesetzt sind, gibt es eine sogenannte neue interessante Option "NeinMitVeto", die den Erfolg eines Proposal erschweren. Eine NeinMitVeto-

Abstimmung zeigt an, dass der Proposal entweder als Spam angesehen wird (für Cosmos Hub irrelevant ist), Minderheitsinteressen unverhältnismäßig schadet oder gegen die derzeit vom Management von Cosmos Hub festgelegten Einsatzregeln verstößt oder zu deren Verstoß ermutigt [Evm22a]. In der Tabelle 3.2 lassen sich die Stimmoptionen der untersuchten DAOs sehen.

Compound	**Uniswap**	**Evmos**
- Ja	- Ja	- Ja
- Nein	- Nein	- Nein
- Enthalten	- Enthalten	- Enthalten
		- NeinMitVeto

Tabelle 3.2: Übersicht der Stimmoptionen

3.4.2 Proposals

- Erstellte Proposals

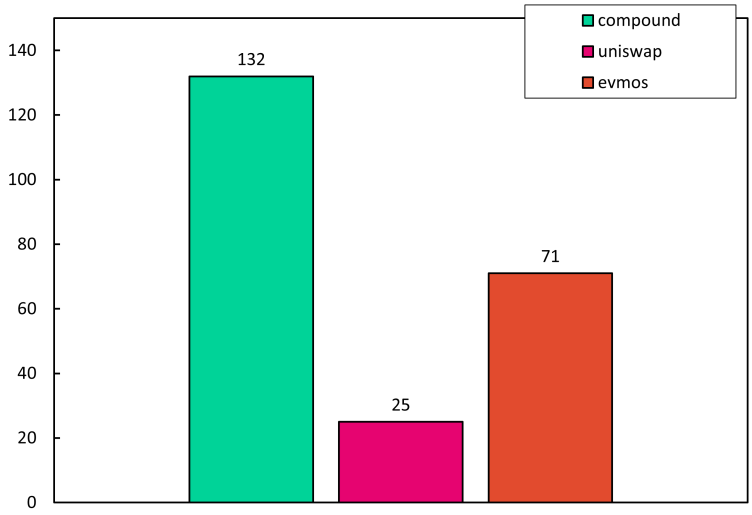


Abbildung 3.1: Erstellte Proposals

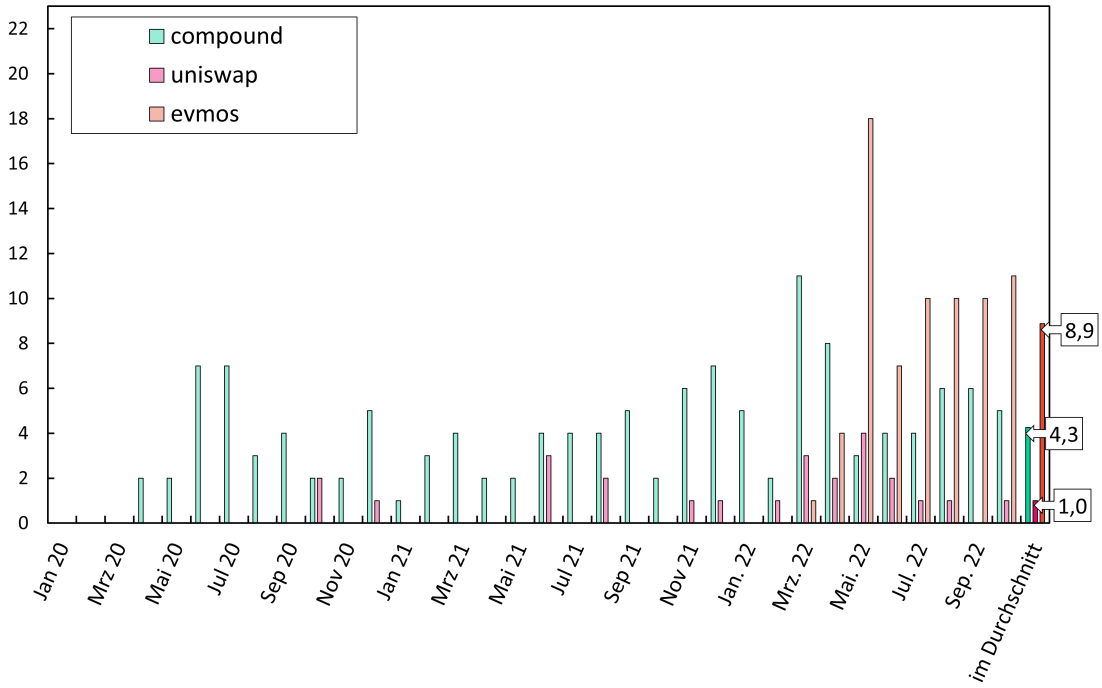


Abbildung 3.2: Erstellte Proposals monatlich

Das Diagramm 3.1 zeigt die Anzahl der erstellten Proposals bei allen drei DAOs. Um eine bessere Übersicht zu verschaffen, werden die Erstellung der Proposals monatlich untersucht. Die erzielten Ergebnisse sind in Diagramm 3.2 dargestellt. Man kann hier leicht erkennen, dass die Compound DAO die älteste DAO ist und deswegen deutlich mehr Proposals als die anderen DAOs hat. Aber wenn man die durchschnittliche Num-

mer betrachtet, die bei den letzten Balken mit der Beschriftung dargestellt ist, ist Evmos der Leader mit 8,9 erstellten Proposals per Monat, obwohl die Organisation seit März 2022 existiert.

Im Unterschied von Compound und Uniswap braucht die Evmos DAO viele Upgrades bzw. Code Änderungen, um Evmos geeignete Bridge für viele EVM kompatibel Blockchains zu machen. Darüber hinaus kann man hier viel leichter die Voraussetzung für die Erstellung eines Proposal erfüllen, weil der Depositsbeitrag geteilt werden kann. Zusammenfassend kann gesagt werden, dass die Anzahl der Proposals von der Art der DAO abhängt.

- ***Erfolgsquote***

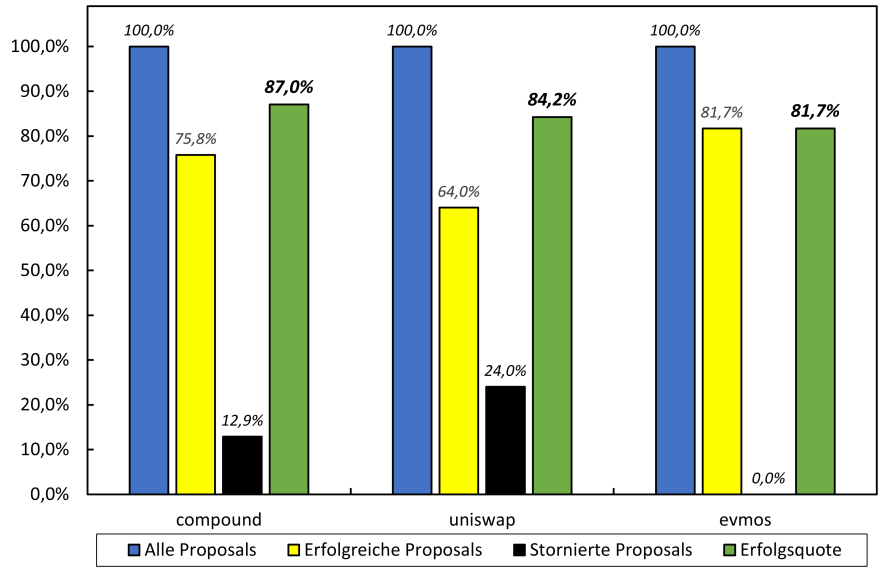


Abbildung 3.3: Erfolgsquote

Damit man die Erfolgsquote berechnen kann, werden auch die Anzahl der gelungenen und stornierten Proposals untersucht. Diagram 3.3 zeigt bei Evmos keine stornierten Proposals, weil diese DAO solche Proposals nicht verfügt bzw. es keine Möglichkeit für den Proposer gibt, ein Proposal zu stornieren. Die Endergebnisse zeigen, dass die Evmos Proposals die niedrigste Erfolgsquote von 81,7% haben. Das ist möglicherweise darauf zurückzuführen, dass aufgrund häufiger eingereichten Proposals nicht seriöse oder nicht gut bedachte Proposals kommen, die nicht unbedingt von der Community akzeptiert werden müssen.

- ***Unterschiedliche Proposers***

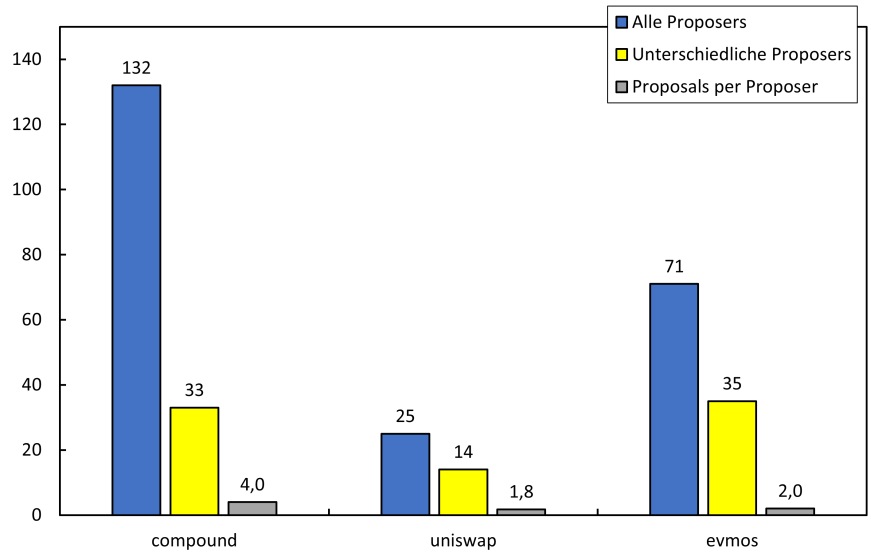


Abbildung 3.4: Unterschiedliche Proposers

Ein weiterer interessanter Faktor ist, wenn es um Proposal geht, von wem kommt der Proposal bzw. wer der Proposer ist. Hier werden alle Adressen, die mindestens ein Proposal gemacht haben, betrachtet und danach nach den unterschiedlichen Adressen gesucht. Aus den dargestellten Daten in Diagramm 3.4 lässt sich schließen, dass es bei Compound DAO mehr gleiche Proposers gibt, die Proposals gemacht haben, als bei der Uniswap und Evmos. Ein Grund dafür wäre, dass diese DAO aus dem Finanzsektor kommt und aus Mitgliedern besteht, die nicht genug ausgebildet sind, um in diesem Sektor tätig zu sein. Daher sind nur wenige Adresse in der Lage, Änderungen vorzustellen. Ein weiterer Grund wären auch die schwer erfüllbaren Voraussetzungen, 25 000 COMP, für die Erstellung des Proposal. Deshalb können Adressen, die das schon geschafft haben, dies wieder machen.

3.4.3 Voters

- ***Voters Anzahl***

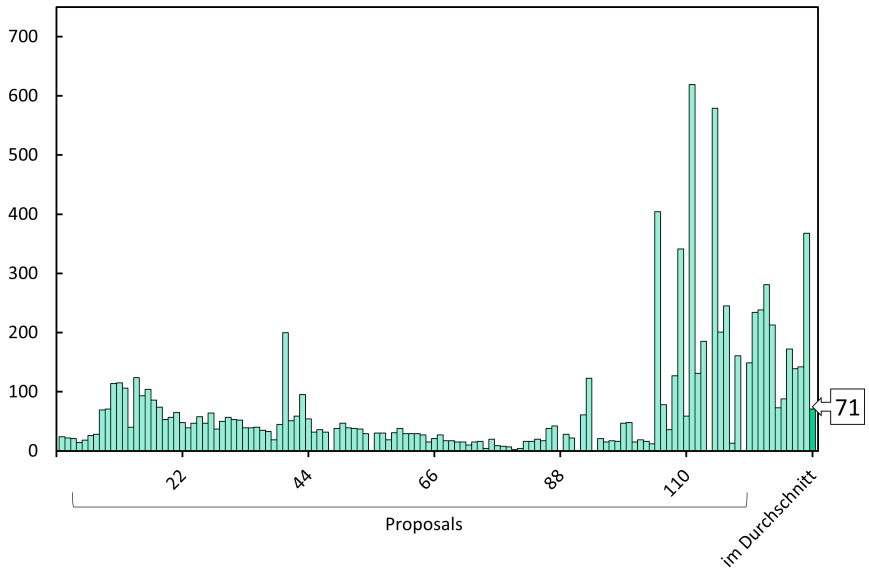


Abbildung 3.5: Compound Voters

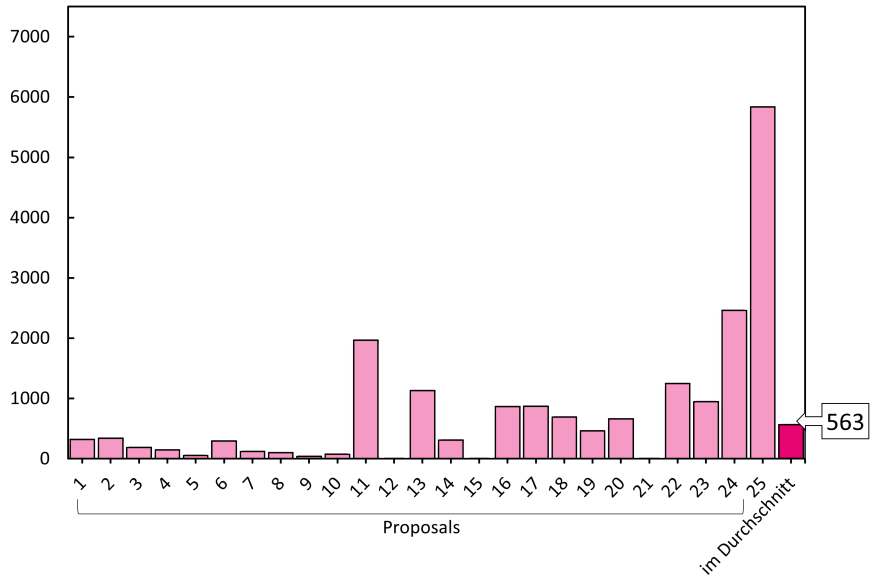


Abbildung 3.6: Uniswap Voters

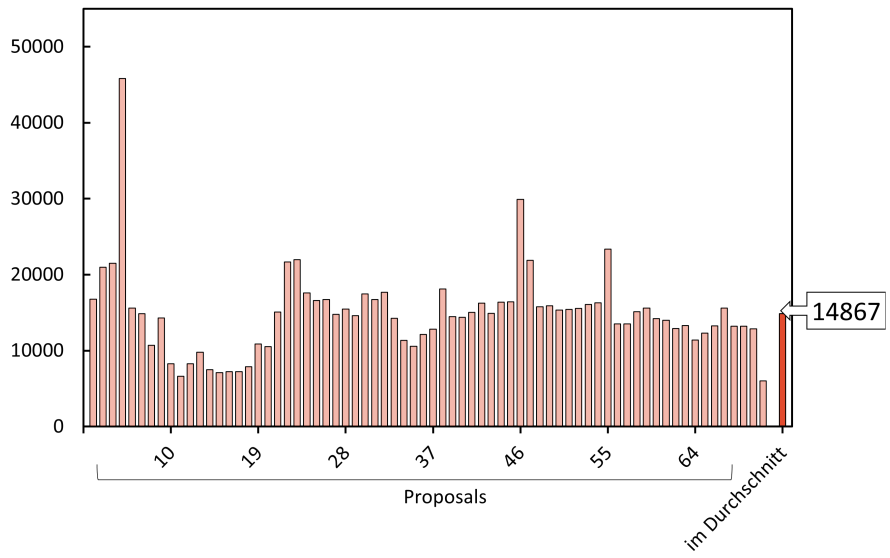


Abbildung 3.7: Evmos Voters

Die Diagramme 3.5, 3.6 und 3.7 zeigen die Anzahl der Voters per Proposals bei alle drei DAOs einzeln. Hier kann man bemerken, dass bei Compound und Uniswap im Laufe der Zeit die Anzahl der Voters kontinuierlich wächst, was bei Evmos nicht der Fall ist. Bei Evmos gibt es eine kontinuierliche, ungefähr gleiche Anzahl der Voters, die konstant bei jedem Proposal voten. Daher ist die durchschnittliche Anzahl der Voters bei Evmos viel größer im Vergleich mit Compound und Uniswap.

- ***Unterschiedliche Voters***

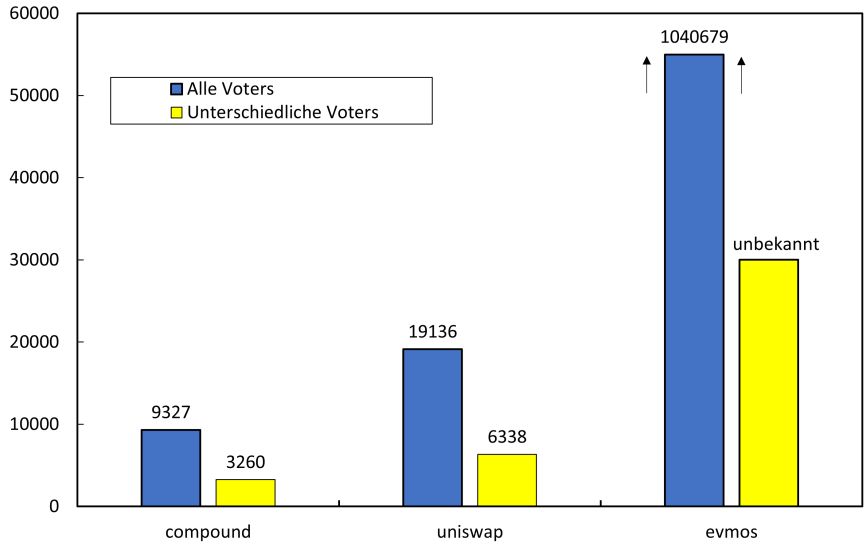


Abbildung 3.8: Unterschiedliche Voters

Aufgrund der großen Anzahl von Voters bei Evmos (über 1 Million) sind bei dieser Untersuchung nur die Voters-Daten von Compound und Uniswap untersucht und verglichen worden. Das Diagramm 3.8 stellt die Anzahl der Voters insgesamt und die Anzahl der unterschiedlichen Voters dar. Hier kann man daraus schließen, dass bei Uniswap viel mehr Adresse bzw. Users Governance-Token besitzen und somit Möglichkeit haben, an das Votingsystem teilzunehmen. Deshalb verfügt Uniswap mehr unterschiedliche Voters als bei Compound.

- ***Überblick der Abstimmung***

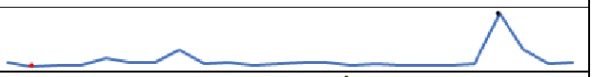
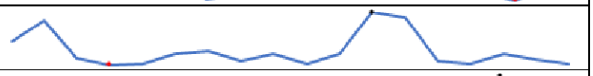
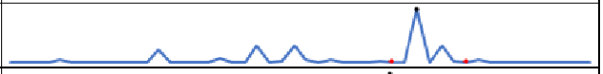
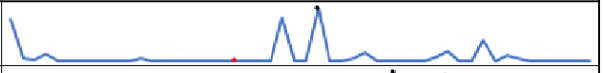
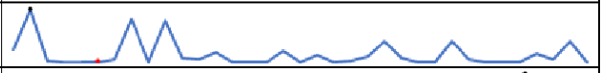
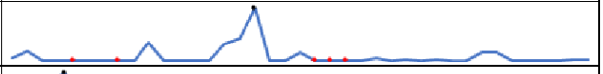
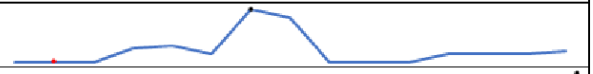
Proposals	Voters	Satus	Überblick der Abstimmung
Proposal 1	24	erfolgreich	
Proposal 3	21	erfolgreich	
Proposal 5	18	erfolgreich	
Proposal 11	115	erfolgreich	
Proposal 12	106	nicht erfolgreich	
Proposal 14	124	nicht erfolgreich	
Proposal 22	48	erfolgreich	
Proposal 23	39	erfolgreich	
Proposal 29	50	erfolgreich	
Proposal 30	57	erfolgreich	
Proposal 31	53	erfolgreich	
Proposal 32	52	nicht erfolgreich	
Proposal 35	40	erfolgreich	
Proposal 36	35	erfolgreich	
Proposal 50	47	erfolgreich	
Proposal 51	39	erfolgreich	
Proposal 70	15	nicht erfolgreich	
Proposal 71	15	erfolgreich	
Proposal 86	38	nicht erfolgreich	
Proposal 87	42	erfolgreich	

Abbildung 3.9: Überblick der Abstimmung (Compound)

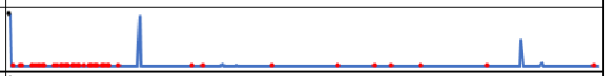
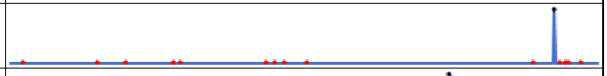
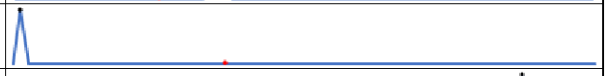
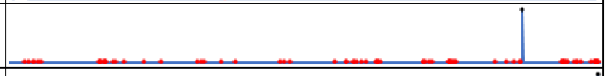
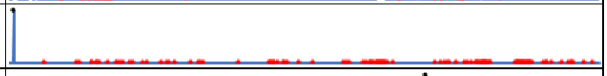
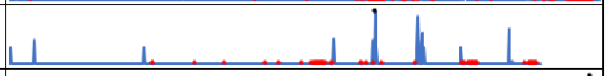
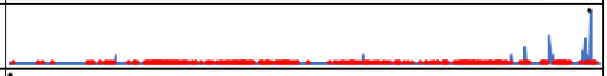
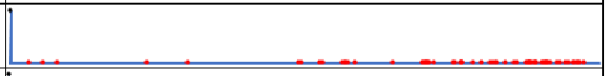
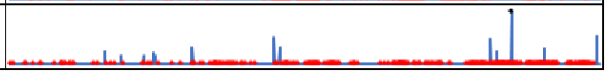
Proposals	Voters	Satus	Überblick der Abstimmung
Proposal 1	320	nicht erfolgreich	
Proposal 2	340	nicht erfolgreich	
Proposal 3	189	erfolgreich	
Proposal 4	148	erfolgreich	
Proposal 5	55	fortgesetz in 6	
Proposal 6	296	erfolgreich	
Proposal 8	101	erfolgreich	
Proposal 9	41	erfolgreich	
Proposal 10	75	erfolgreich	
Proposal 11	1965	erfolgreich	
Proposal 13	1131	erfolgreich	
Proposal 14	311	erfolgreich	
Proposal 16	863	erfolgreich	
Proposal 19	461	erfolgreich	
Proposal 20	663	erfolgreich	
Proposal 22	1248	erfolgreich	
Proposal 23	945	erfolgreich	
Proposal 24	2461	erfolgreich	
Proposal 25	5836	erfolgreich	

Abbildung 3.10: Überblick der Abstimmung (Uniswap)

Die letzten beiden Tabellen geben einen Überblick darüber, wie die Voters ihre Stimme bei Compound bzw. Uniswap gegeben haben. Die Tabelle zeigt auch, wieviele Voters bei einem Proposal gevotet haben und den Proposals Status am Ende. Aufgrund der nicht archivierten Votes-Daten bei den API-Endpunkten von Evmos, ist Evmos aus der Statistik rausgenommen worden. Es werden Proposals untersucht, die nicht storniert worden sind. Von insgesamt 132 sind zufällig nur 20 Proposals von Compound betrachtet. Bei Uniswap sind es 19, weil Uniswap sechs stornierte Proposals hat. Alle Linien in der Abstimmung-Spalte sind Sparklines, die anhand der Anzahl der Votes in Microsoft Excel erstellt worden sind. Die roten Punkte zeigen den minimalen Votes und der schwarzen den maximalen Votes. In diesem Falle sind die roten Punkte die Stimme mit

null Votes, weil es Voters gibt, die bestimmt haben, ohne ein Vote abzugeben. Auf der anderen Seite ist die flache Linie in Realität nicht flach. Dort sind alle Votes mit viel weniger Wert als der maximale Wert bzw. der Wert, der ungefähr groß wie der maximale Wert ist. Es werden nur die Votes betrachtet, unabhängig davon, ob der Voter mit ja, nein oder enthalten gevotet hat.

Die Ergebnisse zeigen, dass es sowohl bei Uniswap als auch bei Compound während der Stimmung unterschiedliche Votes von den Voters gevotet sind bzw. es gibt viel Voters mit wenig Votes als Voter mit viel Votes. Der Grund dafür ist die unterschiedliche Anzahl der Governance-Token bei jedem Voter. Jedem Voter ist freigegeben, mit welcher Menge an Votes er votet (1 Votes = 1 Token). Allerdings ist nicht jeder Voter in der Lage beliebig viele Votes abzugeben, weil nicht jeder über eine große Anzahl an Token verfügt. Zusätzlich kann man daraus schließen, dass eine Änderung in der Organisation nach eigenem Willen für einen Voter mit wenig Governance-Token schwer vorstellbar ist. Je mehr Governance Token man besitz, desto mehr Macht in der Organisation hat man.

Kapitel 4

Fazit und Ausblick

Diese Untersuchung ist ein Beweis für die Transparenz der DAO. Ohne eine Genehmigung von der untersuchten Organisation kann man alle benötigten Daten problemlos erhalten. Wenn man außerdem nicht genug Kenntnisse über den Ablauf der gesamten Prozesse verfügt, könnte man dies über die Dokumentation einer DAO in Erfahrung bringen. Auf der anderen Seite ermöglicht die Transparenz von DAO aber auch andere Angriffsflächen wie z.B.: Datamining in der Blockchain. Da der Code Open Source ist, könnten ihn viele Augen sehen, was dazu beiträgt, dass ein Fehler eher gefunden bzw. gefixed wird. Im Fall des Gegenteils ("Security through Obscurity"), wo man möglichst viel geheim hält, werden Schwächen vor den Entwicklern versteckt, was der Grund dafür ist, dass es im realen Leben nur mäßig funktioniert. Die in der Vergangenheit erfolgreiche Attack der ersten DAO - *The DAO* zeigt, dass die Gewährleistung der Sicherheit einer der größten Herausforderung der DAOs ist.

Diese Organisationen können nur online existieren und verbinden ihre Mitglieder unabhängig von ihrem Ort und es ist irrelevant, ob sie sich gegenseitig kennen, was bei traditionellen Unternehmen schwer vorstellbar ist. Sie haben Verwaltungsregeln, die in Smart Contract geschrieben und offen, fair und nicht manipulierbar sind.

Anhand dieser Untersuchung ist zu sehen, dass bei jeder solcher Organisationen unterschiedliche Regelung gelten. Jeder Organisation hat eigene Regeln geschrieben, wie die Organisation weiterentwickeln bzw. strukturieren soll. Diese Regeln müssen manchmal geändert bzw. ergänzt werden. Deshalb ermöglicht DAO mithilfe von Proposals an die Mitglieder ihre Meinung zu äußern und falls diese Meinung von den anderen Mitgliedern akzeptierbar bzw. nicht akzeptierbar ist, mit selbst definiertem Voting Mechanismus von DAO, das zu genehmigen bzw. abzulehnen.

Diese Untersuchung zeigt auch das eine DAO nicht unbedingt auf das Ethereum Netzwerk limitiert ist. Die frisch erstellte DAO, *Evmos DAO*, ist ein gutes Beispiel dafür, wie eine DAO auf Cosmos SDK erfolgreich existieren kann.

Die schon erwähnte in der Studie acht Typen von DAO sind nicht der einzigen Ty-

pen, die heutzutage existieren. Da ständig neue Formen von DAOs erfunden werden, könnte man nicht jede DAO-Kategorie abdecken. Eine solche neue Kategorie ist Decentralised Autonomous Gaming (DAG). DAG kann man als dezentralisiertes Spiel mit vordefinierten Regeln von Smart Contract definieren. Ein Beispiel für DAG ist das Spiel Schneeballschlacht. Schneeballschlacht wurde beim Unternehmen Daubit Programmierung Service GmbH entwickelt. Was dieses Spiel besonders macht, ist, dass die Spieler die Parameter des Spiels in der Zukunft (diese Eigenschaft ist noch nicht implementiert) durch die DAO ändern können. Mehr Informationen lässt sich über die Webseite `https://devpost.com/software/schneeballschlacht` erfahren.

Die DAOs sind noch am Anfang ihrer Entwicklung. Das Anwendungsspektrum dieser Organisation ist enorm groß und damit der Optimismus auch, dass diese Organisation in der dezentralen Welt bedeutende Rolle spielen kann.

An dieser Stelle möchte ich mich bei allen bedanken, die mich in den letzten drei Monaten unterstützt haben.

Besonders möchte ich mich bei Herrn Alexander KRAHL bedanken, der mich während der Erstellung dieser Arbeit regelmäßig betreut hat.

CD-Informationen

Informationen zu der beigefügten CD. Der Datenträger ist an der inneren hinteren Einbandseite zu finden.

Inhalt

- Bachelorarbeit als PDF
- Programmierungscode-Projekt als ZIP

Abkürzungsverzeichnis

DAO	Dezentrale Autonome Organisation
AV	asymmetrische Verschlüsselungsverfahren
ECC	Elliptic Curve Cryptography
EVM	Ethereum Virtual Machine
AMM	Automated Market Maker
ABI	Application Binary Interface
VPN	Virtual Private Network
DAG	Decentralised Autonomous Gaming

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur

[Ant18] Andreas M. Antonopoulos. *Bitcoin Blockchain - Grundlagen und Programmierung - Die Blockchain verstehen, Anwendungen entwickeln*. Sebastopol: O'Reilly, 2018. ISBN: 978-3-960-10172-7.

[Ara22] Aragon. *About Aragon*. https://aragon.org/about-aragon, Version: September. 2022.

[AW19] Andreas M Antonopoulos und Gavin Wood. *Ethereum – Grundlagen und Programmierung: Smart Contracts und DApps entwickeln*. O'Reilly, 2019. ISBN: 978-3-96010-348-6.

[Bin22] Binance Academy. *what are governance tokens*. https://academy.binance.com/en/articles/what-are-governance-tokens, Version: November. 2022.

[coi22] cointelegraph. *What is Etherscan, and how does it work?* https://cointelegraph.com/news/what-is-etherscan-and-how-does-it-work, Version: November. 2022.

[Col22] Colony. *About Colony*. https://colony.io/about-us, Version: September. 2022.

[Com22a] Compound. *Autonomous Proposals*. https://medium.com/compound-finance/compound-autonomous-proposals-354e7a2ad6b7, Version: November. 2022.

[Com22b] Compound. *Compound Governance*. https://docs.compound.finance/v2/governance/#governor-bravo, Version: Oktober. 2022.

[Com22c] Compound. *Comptroller Introduction*. https://docs.compound.finance/v2/comptroller/, Version: November. 2022.

[Com22d] Compound. *cToken Introduction*. https://docs.compound.finance/v2/ctokens/, Version: November. 2022.

[Com22e] Compound. *Was ist Compound?* https://coinmarketcap.com/de/currencies/compound/, Version: Oktober. 2022.

[DAO22] DAOStack. *An Explanation of DAOstack in Fairly Simple Terms*. https://medium.com/daostack/an-explanation-of-daostack-in-fairly-simple-terms-1956e26b374, Version: September. 2022.

[EFAH20] Youssef El Faqir, Javier Arroyo und Samer Hassan. “An overview of decentralized autonomous organizations on the blockchain”. In: *Proceedings of the 16th international symposium on open collaboration*. 2020, S. 1–8.

[Eje22] Patrick Ejeke. *DAO: What Is DAO? The Key to Democratizing The Metaverse Guide to Decentralized Autonomous Organizations: NFT, DEX, Gitcoin, Aragon, Crypto Investing Trading, Binance, BNB, BTC, ETH, Staking Crypto*. English. Hardcover. Independently published, 14. Apr. 2022, S. 143. ISBN: 979-8802414859. URL: https://lead.to/amazon/com/?op=bt&la=en&cu=usd&key=B09XZ5ZYNQ.

[Evm22a] Evmos. *Definition of NoWithVeto*. https://forum.cosmos.network/t/proposal-75-accepted-establishing-a-definition-of-nowithveto/6898,Version:November, urldate = 19.11.2022, 2022.

[Evm22b] Evmos. *Use Cases*. https://docs.evmos.org/about/intro/use_cases.html, Version: November. 2022.

[FM20] Hans-Georg Fill und Andreas Meier. *Blockchain - Grundlagen, Anwendungsszenarien und Nutzungspotenziale*. Berlin Heidelberg New York: Springer-Verlag, 2020. ISBN: 978-3-658-28006-2.

[Hay22] Hayden Adams. *Uniswap Whitepaper*. https://hackmd.io/@HaydenAdams/HJ9jLsfTz#%F0%9F%A6%84-Uniswap-Whitepaper, Version: Oktober. 2022.

[Liu+21] Lu Liu u. a. “From Technology to Society: An Overview of Blockchain-Based DAO”. In: *IEEE Open Journal of the Computer Society* 2 (2021), S. 204–215. DOI: 10.1109/OJCS.2021.3072661.

[Luc20] Kai Lucks. *Der Wettlauf um die Digitalisierung - Potenziale und Hürden in Industrie, Gesellschaft und Verwaltung*. Stuttgart: Schäffer-Poeschel, 2020. ISBN: 978-3-791-04676-1.

[luc22] lucass Aldanha. *Ethereum Yellow Paper Walkthrough (2/7)*. https://www.lucassaldanha.com/ethereum-yellow-paper-walkthrough-2/, Version: September. 2022.

[Nnk+18] Noe Nnko u. a. “A framework of blockchain-based secure and privacy-preserving E-government system”. In: *Wireless Networks* (Dez. 2018). DOI: 10.1007/s11276-018-1883-0.

[Pat21] Daniel Patterson. *Erstaunliche DAOs: Dezentrale autonome Organisationen für Einsteiger, NFT, Metaverse, DeFi, DEX, Gitcoin, Aragon, DeFi investieren, Krypto ... BNB, BTC, ETH, Ethereum (German Edition)*. German. Paperback. Independently published, 24. Dez. 2021, S. 83. ISBN: 979-8789745823. URL: https://lead.to/amazon/com/?op=bt&la=en&cu=usd&key=B09NSCWY1K.

[Sat08] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. `http://satoshinakamoto.me/bitcoin.pdf`, Version: November. 2008.

[SF19] Andreas Schütz und Tobias Fertig. *Blockchain für Entwickler - Grundlagen, Programmierung, Anwendung*. Bonn: Rheinwerk Verlag, 2019. ISBN: 978-3-836-26392-4.

[Vit22] Vitalik Buterin. *Ethereum Whitepaper*. `https://ethereum.org/en/whitepaper/`, Version: September. 2022.

[Wan+19] Shuai Wang u. a. "Decentralized autonomous organizations: Concept, model, and applications". In: *IEEE Transactions on Computational Social Systems* 6.5 (2019), S. 870–878.