DECENTRALIZED FINANCES

-

HOW CAN DECENTRALIZED STRUCTURES AND THEIR DEFI ACTIVITIES BE CLASSIFIED UNDER CORPORATE AND/OR CIVIL LAW?

Miro Schüpbach (17-109-851)[1] Marcel Zauder (16-124-836)[2]

SUPERVISOR(S):
Prof. Dr. Christian Cachin
Prof. Dr. Mirjam Eggen
Dr. Christian Sillaber

ASSISTANT:
Semir Hermidas

22. APRIL 2022

SEMINAR LAW AND COMPUTER SCIENCE - REPORT

[1] miro.schuepbach@students.unibe.ch, University of Bern
[2] marcel.zauder@students.unibe.ch, University of Bern

Abstrakt

Mit dem Aufkommen der Blockchain Technologie und Kryptowährungen bekam die Finanzwelt eine ganz neue Facette im Bezug auf die Technologisierung. Schnell stellte sich die Frage, wie man mit Kryptowährungen wie Bitcoin oder Ethereum Gewinne durch Investitionen erzielen und maximieren kann. Aus dieser Problemstellung heraus entstanden Dezentrale Autonome Organisationen, welche wie die dazugehörige Währung in einer Blockchain eingebettet sind, um die Notwendigkeit einer zentralen Autorität vernachlässigen zu können. Diese erhielten schnell Zustimmung und Millionen von Dollar an Investitionen fanden sich bald in der digitalen Welt wieder.
Durch das schnelle Aufkommen dieser neuen Technologie sind natürlich Probleme vorprogrammiert und sowohl in technischer als auch in juristischer Hinsicht sollten diese schnell aufgearbeitet werden, um jegweiligen Konflikten zuvorzukommen. Nicht zuletzt durch die Bekanntwerdung des »*The DAO-Hack*« im Jahr 2016 wurde schnell klar, dass diese Technologie noch nicht ausgereift und mit vielen Fehlern behaftet ist. Auch im juristischen Sinne ist noch nicht geklärt inwiefern sich die neue technologisierte Welt in die Gesetzbücher, welche noch auf klassischen Tatsachen beruht, eingliedern lässt.
Dieses Paper befasst sich sowohl mit den technischen Verwundbarkeiten, Problemen und potentiellen Angriffsmöglichkeiten dieser DAOs, sowie mit der juristischen Einordnung in das schweizerische Gesellschaftsrecht. Dabei wird auf einige reale Beispiele von verschiedenen DAOs eingegangen und die größten Probleme erläutert. Weiterhin wird ein Vergleich zur kollektiven Kapitalanlage durchgeführt und mögliche Parallelen zwischen technologisierter und klassischer Welt erläutert.

Inhaltsverzeichnis

Literaturverzeichnis

ADAMS HAYDEN / ZINSMEISTER NOAH / ROBINSON DAN: *"Uniswap V2 Core"*. URL: https://uniswap.org/whitepaper.pdf (BESUCHT AM: 16. 04. 2022). (2020).

ARSENAULT ERIC: *"Voting Options in DAOs"*, in: DAOstack. URL: https://medium.com/daostack/voting-options-in-daos-b86e5c69a3e3 (BESUCHT AM: 21. 03. 2022). (2020).

AUFDERHEIDE SOPHIE C.: *"Dezentrale Autonome Organisationen (DAO) – Smart Contracts aus der Perspektive des Gesellschaftsrechts"*, in: WM Heft, S. 264–271. (2022).

BÄRTSCHI HARALD: *"Vom papierlosen Wertpapier zum Robo-Verwaltungsrat: Gesellschaftsrecht im digitalen Wandel"*, in: Peter Jung, Frédéric Krauskopf, Conradin Cramer (Hrsg.), Theorie und Praxis des Unternehmensrechts, Festschrift zu Ehren von Lukas Handschin, S. 60–77. (2020).

BUTERIN VITALIK: *"Ethereum Whitepaper, Decentralized Autonomous Organizations"*. URL: https://ethereum.org/en/whitepaper/ (BESUCHT AM: 24. 03. 2022). (2014).

CHITRA TARUN et al.: *"DeFi liquidity management via Optimal Control: Ohm as a case study"*. URL: https://web.stanford.edu/~guillean/papers/ohm-paper.pdf (BESUCHT AM: 14. 04. 2022). (2022).

EGGEN MIRJAM: *"Smart Contracts und allgemeine Geschäftsbedingungen"*, in: Susan Emmenegger, Stephanie Hrubesch-Millauer, Frédéric Krauskopf, Stephan Wolf (Hrsg.), Brücken bauen: Festschrift für Thomas Koller, S. 60–77. (2018).

EGOROV MICHAEL: *"StableSwap - efficient mechanism for Stablecoin liquidity"*. URL: https://curve.fi/files/stableswap-paper.pdf (BESUCHT AM: 16. 04. 2022). (2019).

ETIENNE TRANDAFIR: *"Immobilieninvestitionen und Blockchain"*, in: AJP, S. 19–29. (2020).

FAQIR-RHAZOUI YOUSSEF / ARROYO JAVIER / HASSAN SAMER: *"A comparative analysis of the platforms for decentralized autonomous organizations in the Ethereum blockchain"*, in: Journal of Internet Services and Applications. URL: https://doi.org/10.1186/s13174-021-00139-6. (2021).

FENWICK MARK / KAAL WULF A. / VERMEULEN ERIK P.M.: *"Why 'Blockchain' Will Disrupt Corporate Organizations"*, in: European Corporate Governance Institute (ECGI), Law Working Paper No. 419. URL: https://ssrn.com/abstract=3227933 (BESUCHT AM: 31. 03. 2022). (2018).

FORRER LUCAS / ZUUR FLORIS / MÜLLER MATTHIAS P. A.: *"Das Aktienrecht im Wandel der Digitalisierung - Entstehung der Gesellschaft, Willensbildung der Organe und Blockchain-Technologie"*, in: Lucas Forrer and Floris Zuur and Matthias P. A. Müller (Hrsg.), Das Aktienrecht im Wandel, Zum 50. Geburtstag von Hans-Ueli Vogt, S. 1–27. (2020).

GLARNER ANDREAS et al.: *"Decentralized Autonomous Association (DAA)"*, in: MME Magazin. URL: https://www.mme.ch/de-ch/magazin/artikel/decentralized-autonomous-association-daa (BESUCHT AM: 01. 04. 2022). (2020).

GUILLAUME FLORENCE: *"Art. 150"*, in: Bucher Andreas (Hrsg.), Commentaire Romand, Loi sur le droit international privé, Convention de Lugano. (2011).

GYR ELEONOR: *"Dezentrale Autonome Organisation DAO, Eine juristische Betrachtungsweise"*, in: Jusletter. URL: https://jusletter.weblaw.ch/jus-lissues/2017/917/dezentrale-autonome-_ad06f55b2f.html__ONCE&login=false. (2017).

HANDSCHIN LUKAS: *"Art. 530"*, in: Heinrich Honsell, Nedim Peter Vogt, Rolf Watter (Hrsg.), Basler Kommentar, Obligationenrecht II, 5. Auflage. (2016).

HASSAN SAMER / DE FILIPPI PRIMAVERA: *"Decentralized Autonomous Organization"*, in: Internet Policy Review 10 Nr. 2. URL: https://doi.org/10.14763/2021.2.1556. (2021).

HAUSHEER HEINZ / AEBI-MÜLLER REGINA E.: *"Das Personenrecht des Schweizerischen Zivilgesetzbuches"*. 5. Auflage. (2020).

HESS MARTIN / SPIELMANN PATRICK: *"Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht"*, in: Thomas U. Reutter and Thomas Werlen, Kapitalmarkt - Recht und Transaktionen XII, S. 174–202. (2017).

JUNG PETER / KUNZ PETER V. / BÄRTSCHI HARALD: *"Gesellschaftsrecht"*. 3. Auflage. (2021).

JUTZI THOMAS / SIERADZKI DAMIAN: *"Geltungsbereich des Kollektivanlagenrechts"*. (2022).

KOLLER ALFRED: *"Art. 184"*, in: Heinrich Honsell, Nedim Peter Vogt, Rolf Watter (Hrsg.), Basler Kommentar, Obligationenrecht II, 5. Auflage. (2016).

KULECHOV STANI: *"Aave Protocol Whitepaper V1.0"*. URL: https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf (BESUCHT AM: 16. 04. 2022). (2020).

LEHMANN MATTHIAS: *"Kryptowährungen und Token"*, in: Sebastian Omlor, Mathias Link (Hrsg.), Recht Wirtschaft Steuern. (2021).

LUSAR MARCUS / SATOR CLARA: *"Blockchain: Rechtsfragen rund um DAO & Co"*, in: Extrajournal. URL: https://extrajournal.net/2022/02/23/blockchain-rechtsfragen-rund-um-dao-co/ (BESUCHT AM: 06. 04. 2022). (2022).

MAKRIDIS CHRISTOS et al.: *"The Rise of Decentralized Cryptocurrency Exchanges: Evaluating the Role of Airdrops and Governance Tokens"*. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3915140 (BESUCHT AM: 24. 03. 2022). (2021).

MEIER JULIA / SCHUPPLI BENEDIKT: *"Grundlagen des Rechts / The DAO Hack and the Living Law of Blockchain"*, in: Alexandra Dal Molin-Kränzlin et al. (Hrsg.), Digitalisierung – Gesellschaft – Recht, S. 25–43. (2019).

MEIER-HAYOZ ARTHUER / FORSTMOSER PETER / SETHE ROLF: *"Schweizerisches Gesellschaftsrecht"*. 12. Auflage. (2018).

MICHAEL BAIER: *"Unregulierte Rechtsformen zur Strukturierung von Private Equity-Investitionen"*. (2019).

MÜLLER MATTHIAS P.A.: *"Blockchain und Gesellschaftsrecht: Ein Streifzug durch Möglichkeiten und Hürden"*, in: Expert Focus, S. 485–490. (2019).

OWOCKI KEVIN: *"It's Time To Decentralize Gitcoin"*. URL: https://gitcoin.co/blog/its-time-to-decentralize-gitcoin/ (BESUCHT AM: 28. 03. 2022). (2021).

PATEL NILAY: *"From a meme to $47 million: ConstitutionDAO, crypto, and the future of crowdfunding"*. URL: https://www.theverge.com/22820563/constitution-meme-47-million-crypto-crowdfunding-blockchain-ethereum-constitution (BESUCHT AM: 14. 04. 2022). (2021).

PFENNINGER MARKUS / NÜESCH MARTINA: *"Art. 2"*, in: René Bösch, François Rayroux, Christoph Winzeler, Eric Stupp (Hrsg.), Basler Kommentar, Kollektivanlagengesetz, 2. Auflage. (2016).

RAYROUX FRANÇOIS / PASQUIER SHELBY DU: *"Art. 7"*, in: René Bösch, François Rayroux, Christoph Winzeler, Eric Stupp (Hrsg.), Basler Kommentar, Kollektivanlagengesetz, 2. Auflage. (2016).

REIFF NATHAN: *"Decentralized Autonomous Organization (DAO)"*. URL: https://www.investopedia.com/tech/what-dao/ (BESUCHT AM: 16. 03. 2022). (2021).

RIVA SVEN: *"Decentralized Autonomous Organizations (DAOs) as subjects of law - The recognition of DAOs in the Swiss legal order"*. Masterarbeit der Universität Neuchatel (2019).

SCHILLER KAI: *"Was ist eine DAO (Dezentrale Autonome Organisation)?"* URL: https://blockchainwelt.de/dao-dezentrale-autonome-organisation-was-ist-das/ (BESUCHT AM: 20. 04. 2022). (2022).

SISARIO BEN: *"Meet the New Owners of the Wu-Tang Clan's One-of-a-Kind Album"*, in: New York Times, Ausgabe vom 21. Oktober, Teil C S. 3. (2021).

WOOD GAVIN: *"Ethereum: A secure decentralised generalised transaction ledger"*, in: Ethereum project yellow paper, vol. 151, S. 1–32. URL: https://ethereum.github.io/yellowpaper/paper.pdf (BESUCHT AM: 24. 03. 2022). (2014).

Materialliste

"Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070)". (vom 25. Juni 2014).

Abkürzungsverzeichnis

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
approx.	approximately
Art.	Artikel
BGer	Bundesgericht
ca.	circa
DAO	Dezentralisierte Autonome Organisation
DeFi	Decentralized Finances
DEX	Decentralized Exchange
DLT	Digital-Ledger Technologie
eG	einfache Gesellschaft
GV	Generalversammlung
Hrsg.	Herausgeber
i.d.R.	in der Regel
i.S.d.	im Sinne des
insb.	insbesondere
IPRG	Bundesgesetz über das Internationale Privatrecht vom 18. Dezember 1987 (Stand am 1. Januar 2022)(SR 291)
KAG	Bundesgesetz über die kollektiven Kapitalanlagen vom 23. Juni 2006 (Stand am 1. Januar 2020)(951.31)
KKV	Verordnung über die kollektiven Kapitalanlagen vom 22. November 2006 (Stand am 1. Januar 2022)(951.311)
N	Randnummer
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (Stand am 1. Januar 2022)(SR 220)
PoA	Proof-of-Authority

PoS . . . . . Proof-of-Stake

PoW . . . . . Proof-of-Work

Rz. . . . . . Randzeile

s. . . . . . siehe

S. . . . . . Seite

sog. . . . . . sogenannt

u. E. . . . . . unseres Erachtens

Vgl. . . . . . Vergleiche

VR . . . . . Verwaltungsrat

Kapitel 1: Einleitung

1.1 Allgemeines

1.1.1 Was ist eine Dezentralisierte Autonome Organisation?

Eine einheitliche Definition für den Begriff der Dezentralisierten Autonomen Organisation konnte sich bisher nicht durchsetzen[1]. Allgemein wird eine DAO aus Regeln definiert, welche in einem Open-Source Code festgeschrieben sind. Die Entscheidungsgewalt ist dabei über alle DAO-Mitglieder verteilt und ist weder an einen zentralen Entscheider gebunden noch haben Aktionäre oder Zentralregierungen einen Einfluss auf die Entscheidungen der DAO. Alle getätigten Finanztransaktionen sowie die Regeln werden auf einer Blockchain, eine Digital-Ledger Technologie, die durch trusted timestamps und der Nutzung einer verteilten Datenbank gegen Fälschungen geschützt ist, festgehalten und durch Smart Contracts verwaltet. Dieser Ansatz hat den Vorteil, dass eine DAO die komplette Entscheidungsmacht auf alle Teilhaber verteilt, wodurch ansonsten notwendige Drittparteien nicht erforderlich sind, sodass der Ablauf vereinfacht wird und damit verbundene Nebenkosten verringert werden können[2].
Um einer DAO anzugehören, wird in der Regel der Besitz eines Tokens vorausgesetzt, z.B. eines Ethereum-Tokens. Mit diesem wird ein Mitglied als solches in der DAO verifiziert und kann an Abstimmungen und Erstellungen von Proposals, wie z.B. Governance-Proposals, teilnehmen. Die Annahme oder Ablehnung solcher Proposals wird durch die Mehrheit der Mitglieder bestimmt, wodurch zwischen diesen ein Consensus geschaffen wird. Die Implementierung, wie die Mehrheit bestimmt wird, ist in den Smart Contracts einer DAO festgelegt. Da der Quellcode einer jeden DAO Open-Source ist, kann sich jeder diesen anzeigen lassen und auch den Inhalt der DAO, den sogenannten treasury, prüfen, da alle Transaktionen auf der Blockchain aufgezeichnet werden[3].

1.1.2 Erscheinungsformen einer DAO

In den letzten Jahren bildeten sich in der Praxis bereits über tausend verschiedene DAOs jeglicher Art.[4] Obwohl sich die Projekte aufgrund ihrer Natur gewisse Eigenschaften teilen, ist die DAO Landschaft keineswegs homogen. Entgegen einer früheren Auffassung[5] dienen DAOs nicht ausschliesslich dazu, gemeinsam Kapital zu beschaffen und Investitionen zu tätigen. Die modernere Definition umfasst eine Vielzahl von DAOs, wobei der dezentralisierte Entscheidungsfindungsprozess sowie die technische und soziale Zusammenarbeit im Fokus steht.[6] Des Weiteren werden die meisten DeFi-

[1] RIVA, S. 25 f.
[2] SCHILLER.
[3] »What is a decentralized autonomous organization, and how does a DAO work?«, https://cointelegraph.com/ethereum-for-beginners/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work (Besucht am: 16.03.2022).
[4] FAQIR-RHAZOUI et al., S. 9 f.; AUFDERHEIDE, S. 266..
[5] HASSAN / DE FILIPPI, S. 2 ff.
[6] BUTERIN, S. 23; »MakerDAO Whitepaper«, https://makerdao.com/en/whitepaper/ (Besucht am: 25.03.2022).

Protokolle durch einen DAO beherrscht. Eine mögliche Kategorisierung kann u. E. anhand der Zweckbestimmung von DAOs vorgenommen werden. Trotz grosser Unterschiede zwischen den einzelnen DAOs, können sie gesamtheitlich betrachtet in drei Hauptkategorien unterteilt werden.[7] Diese werdem im Folgenden kurz erläutert.

Protokoll-Dao
Unter diese Kategorie fallen grundsätzlich alle DAOs, deren Zweck die Governance eines Protokolls ist. Der Begriff Governance ist in diesem Sinne weit zu verstehen und kann nebst Abstimmungen auch die gemeinsame Entwicklung und Instandhaltung des Protokolls beinhalten. Insb. bei Protokoll-DAOs ist des Öfteren zu beobachten, dass erst nach Veröffentlichung des Protokolls die Umwandlung zum DAO erfolgt.[8] Als bekannte Protokoll-DAOs auf der Ethereum Blockchain gelten beispielsweise Aave (Kredit-Protokoll), Uniswap (DEX) oder MakerDAO (Stablecoin).[9] Sofern man die Ansicht vertritt, dass auch Blockchains wie Ethereum als DAOs gelten, würden diese als *ground layer DAOs* wohl auch unter diese Kategorie fallen.[10]

Dienstleistungs-DAO
Dienstleistungs-DAOs zeichnen sich dadurch aus, dass sich eine Gemeinschaft von Entwicklern, Benutzern und Künstlern etc. zusammen findet und als DAO gewisse Dienstleistungen anbietet. Dabei kann es sich sowohl um For-Profit als auch um Non-Profit Organisationen handeln. Ein berühmtes Beispiel dafür ist Gitcoin[11], ein Unternehmen welches sich erfolgreich zu einem DAO umstrukturiert[12] und bereits tausende open-source Projekte mit insgesamt über 50 Millionen Dollar unterstützt hat. Als weitereres äusserst interessantes Modell experimentiert der LexDAO[13] als *decentralized legal engineering guild* mit der Abwicklung von Verträgen durch Code und dezentralisierter Rechtsberatung.

Fundraising-DAO
Die vermutlich grösste mediale Aufmerksamkeit erhalten die sog. Fundraising-DAOs. Während der »*The DAO-Hack*« zu einer Hardfork der Ethereum Blockchain führte, kaufte die PleasrDAO für vier Millionen Dollar die einzige Kopie des Wu-Tang Clan Albums *Once Upon a Time in Shaolin* von der amerikanischen Regierung.[14] Für weitere Schlagzeilen sorgte die ConstitutionDAO[15], welche versuchte, bei Sotheby's eine

[7] »Your DAO guide - the most important DAO categories defining the space«, https://www.ledger.com/academy/your-dao-guide (Besucht am: 21.03.2022).
[8] MAKRIDIS et al., S. 10.
[9] KULECHOV; ADAMS et al.; »MakerDAO Whitepaper, https://makerdao.com/en/whitepaper/« (Besucht am: 25.03.2022).
[10] RIVA, S. 30 f.; WOOD.
[11] »Gitcoin«, https://gitcoin.co/ (Besucht am: 25.03.2022).
[12] OWOCKI.
[13] »LexDAO«, https://www.lexdao.coop/#/ (Besucht am: 28.03.2022).
[14] MEIER / SCHUPPLI, S. 32 ff.; SISARIO; »PleasrDAO«, https://pleasr.org/# (Besucht am: 28.03.2022).
[15] ConstitutionDAO, https://www.constitutiondao.com/ (Besucht am: 28.03.2022).

Originalversion der amerikanischen Verfassung zu ersteigern. Unter diese Kategorie können somit DAOs subsumiert werden, bei welchen gemeinschaftlich Kapital gesammelt wird, um Investitionen jeglicher Art zu tätigen.

Zusammenfassend kann festgehalten werden, dass eine Vielzahl von DAOs mit verschiedensten Zweckbestimmungen bestehen. Als neue Form der Arbeitsteilung, Kapitalbeschaffung und Entscheidungsfindung führen DAOs zu neuen technischen und juristischen Herausforderungen.

1.1.3 Vor- und Nachteile von DAOs

Einer der grossen Vorteile von DAOs besteht darin, dass sie transparent und unveränderlich sind. Dies bedeutet, dass jede einst getätigte Transaktion in der Blockchain gespeichert wird und jeder auf sie zugreifen kann, wodurch Streitigkeiten und Unstimmigkeiten über die vergangenen Transaktionen über die DAO vermieden werden. Darüber hinaus kann jede hierarchische Führung ausser Acht gelassen werden, da jedes Mitglied gleichberechtigt ist – wobei es möglich ist, das Gewicht der Entscheidung proportional an die Anzahl der Token, die es besitzt, anzupassen. Dieser Ansatz löst das *Principal-Agent Dilemma*, da keine Repräsentanten oder Mittelsmänner benötigt werden, die zu Prioritätskonflikten führen können. Abschliessend ist noch hervorzuheben, dass jede und jeder Mitglied einer DAO werden kann.
Andererseits besteht eine Rechtsunsicherheit in Bezug auf DAOs, da es sich um eine neue Technologie handelt und der schweizerische Gesetzgeber derzeit keine expliziten Regulierungen bezüglich DAOs erlassen hat. Darüber hinaus kann man DAOs, da sie sich über das gesamte Internet spannen, fast unmöglich einer nationalen Juristiktion zuordnen, was zu Schwierigkeiten in Bezug auf das anwendbare Recht führt. Insb. ist darauf hinzuweisen, dass die DAO aus Smart Contracts aufgebaut ist, Codezeilen, die von (einer Gruppe von) Programmierern entwickelt wurden, wobei das Problem darin liegt, dass niemand garantieren kann, dass dieser Code fehlerfrei ist und auch keine Hintertüren offen lässt. Ein gutes Beispiel für diese Unsicherheit ist der The DAO Hack, dessen Smart Contracts eine Hintertür hatten, durch die Millionen von Dollar an Finanzmitteln aus der *Treasury* dieser DAO gestohlen wurden.[16] Weitere Angriffsmöglichkeiten werden in Abschnitt 3.5 vorgestellt.

[16] REIFF.

1.2 Zielsetzung

Da DAOs auf einer neuartigen Technologie aufbauen und daher kaum in juristischer Hinsicht erforscht wurden, wird in diesem Paper versucht, eine Verbindung zwischen der technischen Implementation und der Schweizerischen Gesetzgebung zu erstellen. Mit Hilfe des technischen Know-Hows und den korrespondierenden Gesetzestexten des schweizerischen Privatrechts werden zum Schluss mögliche Lösungsansätze zu wiederkehrenden Problemen bei der Nutzung von DAOs untersucht.

Das Ziel ist die Evaluierung der technischen und rechtlichen Probleme von DAOs sowie die Vorstellung von möglichen Lösungsansätzen.

Kapitel 2: Vorgehen

2.1 Methodologie

Dieses Paper wird in zwei Hauptteile aufgegliedert, welche von der jeweiligen Fachperson bearbeitet wird (der überfachliche Teil - Einleitung und Schlussfolgerung - entstand in Kooperation beider Autoren):

1. **Informations-Technischer Teil**
   Es werden zwei Implementationsmöglichkeiten von DAOs anhand der ConstitutionDAO und der DashDAO dokumentiert und verglichen. Auch werden potentielle Sicherheitslücken und damit verbundenene Angriffsmöglichkeiten auf die jeweiligen DAOs, aber auch generelle Schwachstellen, aufgezeigt.
2. **Juristischer Teil**
   Es wird vorerst genauer definiert, mit welcher Art von DAO sich der juristische Teil befasst und welche möglichen Problematiken bezüglich des anwendbaren Rechts auftreten könnten. Darauf wird versucht, das Phänomen der DAO in das schweizerische Gesellschaftsrecht einzuordnen, mit Fokus auf den Vergleich zur Kollektiven Kapitalanlage. Sodann werden die verschiedenen Stakeholder einer DAO analysiert und zuletzt auf mögliche Ansprüche sowie auftretende Haftungsfragen eingegangen.

Als Ergebnis werden Lösungsmöglichkeiten zu sowohl technischen als auch zu juristischen Problemen vorgestellt.

2.2 Limitationen

Da dieses Paper in Zusammenarbeit von Studenten unterschiedlicher Fachrichtungen, explizit von jenen der Juristischen und Informatischen Fakultät, entstanden ist, sind folgende Limitationen aufgetreten:

1. Da ein juristisches Paper sehr viele Kriterien in Bezug auf Formalität und Gestaltung erfüllen muss, werden diese sowohl in den spezifischen Kapiteln als auch in den fachlich übergreifenden Kapiteln beachtet. Der informatische Teil hingegen beachtet diese Kriterien nicht vollständig.
2. In rechtlicher Hinsicht ist der Fachbereich der Blockchain und der darauf aufbauenden Kryptowährungen sowie der hier näher betrachteten DAOs kaum erforscht. Dies führt dazu, dass vergleichsweise nur wenige wissenschaftliche Quellen zu diesem Thema existieren.
3. Die jeweiligen Autoren besitzen unterschiedliche Expertisen in den jeweiligen Spezifikation dieses Papers, wodurch eine Kohärenz zwischen beiden Teilen angestrebt, aber unter Umständen nicht ganz erreicht wird.
4. Da es sich bei dem Thema der Blockchains, Kryptowährungen und DAOs um einen grossen Bereich in der Informatik handelt, sind sehr viele englische Fachbegriffe in diesem Paper vorhanden, die bei der Übersetzung ins Deutsche unter Umständen ihre Bedeutung verlieren. Deshalb werden diese nicht übersetzt und ihre englische Form wird beibehalten. Des Weiteren wird der technische Teil dieses Papers auf Englisch verfasst sein, um jegweilige Bedeutungsverluste oder -veränderungen zu verhindern.

Kapitel 3: DAO - Computer Science

In the following chapter, different ways of implementing DAOs and how they operate are shown and explained using the DashDAO and the ConstitutionDAO. The ConstitutionDao is running on Ethereum built with the Juicebox protocol. DashDAO on the other hand uses its own blockchain and network. The similarities and differences of these two approaches are then evaluated and potential flaws and attack opportunities of DAOs in general are pointed out.

3.1 General

As this paper is created in a collaboration between the Computer Science and Law faculty first some general information about important notations and mechanisms regarding cryptocurrencies are listed.

3.1.1 Blockchain [HA22]

A blockchain can be understood as a database shared among various nodes within a computer network. The information is stored within blocks that are linked together using cryptographic mechanisms. If new information, like in a DAOs case a new transaction, is generated, a new block with this information is initialized and after its validation is chained onto the previous block, ensuring a chronological order on the blockchain.
For cryptocurrency like Bitcoin, it is of most importance that the blockchain is used in a decentralized way, such that no single individual or a small group of participants gather the control of the whole blockchain but its control is retained by all users collectively. Furthermore, already chained blocks are immutable by any means so that all information that was validated is irreversibly saved on the blockchain.

3.1.2 Smart Contracts

A smart contract can be defined as a program that runs on a blockchain implementing and running functions based on the corresponding data, and its state, located at a specified address on the blockchain. Smart contracts are typically used to automate execution when certain pre-established conditions are met to ensure all participants get the right outcome and can neglect trusted third parties which would also coincide with a performance loss [IBMSmartCon].
The most common metaphor for how a smart contract is working is the vending machine [SN18]:

> When certain preconditions are met, i.e. for the vending machine when the money is inserted and a snack is selected, a certain output is guaranteed, in this example, the snack is dispensed. With the use of this vending machine the need of any third party, here a vendor employee, is removed.

3.1.3 Consensus and Consensus Mechanisms [RE21]

Every cryptocurrency, like Bitcoin and Ethereum, needs a mechanism to ensure and validate the authenticity of each transaction and the security of the underlying blockchain. This also guarantees that the blockchain contains all the valid transactions ever made and every transaction that was successfully carried out is recorded on the blockchain. The validation process of these is performed by computers, so-called miners. The consensus mechanism then ensures that each miner agrees on the validity of the next block and therefore the »new« blockchain. There are many different types of these consensus mechanisms. Following, some of the most common are listed:

1. *Proof-of-Work (PoW)*
   The miners are competing against each other which block of transactions gets validated next. The »winner« is then rewarded with a mining fee, which is paid by the performers of the transaction through a so-called »*gas fee*«. However, this approach is highly energy-intensive but brings a high degree of trust. This mechanism is used by Bitcoin and Ethereum.
   Author's note: On the 21st of April 2022, the European Commission under the direction of Swedish financial regulators discussed the possibility of banning the PoW approach used by cryptocurrencies, especially Bitcoin. The discussion was fueled due to its environmental impact stated in a paper published by netzpolitik.org as this consensus mechanism is very energy-hungry [SJ22].
2. *Proof-of-Stake (PoS)*
   The miners with the largest holdings, i.e. most amount of tokens or coins, can validate new blocks which lessens the transaction costs and is also fast than PoW. This rewards especially the users with the biggest stake in the network and motivates the for continued participation. Examples of this are BNB and Solana.
3. *Proof-of-Authority (PoA)*
   This approach is not as common as the first two but is used mainly in private organizations. So-called »vetted sources«, which have special permissions to access the network, create new blocks, therefore, using the means of reputation and authority rather than any public consent to ensure validity.

3.2 Dash [DashDocs]

Dash itself describes the DAO and its associated Cryptocurrency. The altcoin is a fork of the Bitcoin protocol and was initially released by Evan Duffield in January 2014. As of the 22. April 2022 its current market capitalization is around 1.1 billion US-$[1]. Its source code is publicly available via GitHub[2]. In order to run without any central authority, it uses peer-to-peer technology and is able to manage transactions and issue money anywhere in the world.

[1] https://coinmarketcap.com/
[2] https://github.com/dashpay/dash

3.2.1 Masternodes

Users that possess at least 1000 DASH (approx. 100'000 US-$ as of 22. April 2022) can establish a so-called masternode, whereas the operation and maintenance of which is being rewarded. This reward becomes much more lucrative over time as its allocation is modified from 50/50 between miners and masternodes to 40/60 respectively. As of now, the actual allocation lies within 44.8/55.2. If the user's possession becomes less than 1000 DASH the masternode is rejected for any future decision makings and does not earn any rewards. The controllers of these masternodes are additionally given voting rights that can be used on budget proposals or any important decision that affects Dash itself. Through the implementation of such a two-tier network, multiple features are enabled and can be offered in a trustless and decentralized way:

1. *InstantSend*
   Lessens transaction validation time from up to an hour to 2 seconds by using a quorum of masternodes.
2. *CoinJoin*
   Establishes financial privacy within the network.
3. *ChainLocks*
   Protection against 51% mining attacks, by instantly signing the blocks as they are mined.
4. *Governance and Treasury*
5. *Dash Evolution*

3.2.2 Consensus and Mining

Mining coins makes use of a proof-of-work (see section 3.1.3) algorithm by solving a hash function called »X11«. This hash function makes use of eleven different scientific hash algorithms in order to mitigate the threat of ASICs and centralized mining. An ASIC is an application-specific integrated circuit that is customized to be used for a very particular computation [WikiASIC]. As many various hash algorithms are used in »X11« it is much more difficult to create such an ASIC that is capable to solve every single one of them. However, as of today »X11«-ASICs are emerging and comprise the hash rate of the Dash network, but not as much as is the case for Bitcoin.
As previously mentioned different to Bitcoin the reward for mining is not exclusively allocated to the miners but is split up in three different categories:

- *10% of reward for Decentralized Governance Budget*
  Dash uses this part of the block reward in order to fund itself hence not being dependent on any donations or premined endowments.
- *90% of reward for Mining and Masternode Reward*
  The remaining part of the reward is distributed among the miners and masternode owners. In August 2020 the network approved a distribution table that will reward masternode owners up to 60% of the remainder in 2025 as this innovative two-tier network approach separates this cryptocurrency from others and is a very important asset for the Dash network.

3.2.3 Operations and Smart Contracts

Proposals and ideas regarding the Dash DAO network usually come into life in its Dash forum. In this publicly accessible forum, feedback and suggestions can be stated by everyone part of the DAO's community. Once the proposer is certain that his proposal has a valid and reasonable chance of defying a vote, he can establish it as a governance object on the blockchain by paying a 5 DASH fee. If the net vote count for »YES« is at least 10% of the total masternode count the proposal is passed and given there is enough block reward available is saved on the blockchain. The budget for the proposals is allocated every 16616 blocks, approximately a month, in so-called superblocks. These superblocks contain the information on which proposals did pass and according to the margin by which they were winning are awarded. This means that most often different proposals are competing against each other in order to receive the necessary votes in order to get passed and receive the funding in order to be integrated into the blockchain. This behaviour ensures that the proposal owners try to convince as many master node owners as possible to vote in favor of their idea, hence, needing to deal with the Dash community and possibly adjust their proposal.
As the number of participants, and therefore also the number of ideas, is said to be increasing, the masternode owners would be expected to evaluate a massive amount of proposals which is simply not possible. Therefore, the possibility of creating funding organizations is made possible that act as a contractor for the allocation of budget for smaller decentralized projects according to votings or requirements of the Dash network and its community.

3.2.4 Coin Ownership and Voting

In the Dash network, not everyone is allowed to vote on proposals. A user must be an owner of a masternode, which requires possession of at least 1000 DASH, in order to get a voting right in the Dash network. Each masternode is hence equivalent to one vote. This vastly decreases the time a vote takes as only a fraction of users are allowed to approve or disapprove of a certain proposal regarding the budget or the whole Dash network.

3.3 ConstitutionDAO

The ConstitutionDAO is based on the Ethereum blockchain and was released in November 2021 with the goal to purchase an original copy of the United States Constitution. However, this goal was never achieved and the raised 47 million US-$ was said to be reimbursed minus the Ethereum transaction fees. This reimbursement step got messy as the median donation was around 217 US-$ but the fees summed up to approximately 140 US-$ therefore at least 1.2 million US-$ of the raised funds were lost due to transaction fees and most reimbursements were never performed [KJ21]. After losing the bidding the DAO was disbanded and became defunct with no intentions to invest in other projects [FM22].

3.3.1 Juicebox Protocol [JuiceBoxDoc]

Juicebox is a framework with which a developer can distribute his services and develop a programmable treasury accessible to everyone. It uses the ERC20, an Ethereum token, as the equivalent currency for its fundraising and money distributions.
With Juicebox one can set a funding target with a corresponding duration, similar to a crowdfunding process, just with the use of cryptocurrency. Any surplus that is made during the funding period is defined as overflow and locked into the treasuries reserved pool. The participants can use their tokens in order to claim a portion of that overflow for themselves [DoDAOJB]. More about the operations of Juicebox platforms can be read in Section 3.3.3.

3.3.2 Consensus [EthDocs]

As JuiceBox is a framework built on the Ethereum blockchain it uses the same consensus mechanism as the Ethereum network itself - namely a Proof-of-Work approach. The protocol used for this mechanism is called Ethash and requires the miner based on the block difficulty to create a mixHash below a target nonce. It is easy to verify the correctness of such a mixHash, therefore any other miner or client can detect fraud nearly instantaneously.
However, Ethereum does work on moving to a Proof-of-Stake consensus mechanism (as of 22. April 2022). There are several reasons why implementing a PoS approach is preferred over a PoW approach for Ethereum:

- It becomes easier to run a node as no investments in hardware or energy are needed
- PoS is more decentralized as more nodes do not lead to an increased percentage return as it is with mining
- Enables the use of secure sharding, creation of multiple blocks at the same time, which increases the transaction throughput, also lowering the power needed and therefore the amount of gas fees needed to pay the node owners.

For both approaches, Ethereum will mark the transaction to have »finality« when these are part of the blockchain that cannot be altered or deleted. This is needed, especially in the PoW mechanism, but for consensus mechanisms in general as they work in a decentralized way, as two valid blocks can be generated at the same time. Therefore, the majority of nodes need to confirm a certain block to be the subsequent block in the chain. For the PoW approach finality can be usually assured after approx. 1 minute or six blocks. For the PoS mechanism, on the other hand, finality is ensured by the »Casper protocol« which uses checkpoints to get at least 2/3 of all validators to agree on the state of a block. It also implements a kind of defense against 51% attacks as a validator will lose their entire stake if they participate in such malicious operations.

3.3.3 Operations and Smart Contracts [DoDAOJB]

All donations are collected in a so-called multi-signature wallet, which requires in the case of the ConstitutionDAO an agreement of the majority of 13 authorized signers in

order to move the money in it.
As previously stated each Juicebox project has a funding target - which can also be 0$ - and a possible funding period. The funding while being below the goal is stored in a certain treasury from which the predetermined workers and developers are paid. The surplus, the so-called overflow, is stored in another pool and every member of the DAO can access it by using their own token.
Juicebox also provides an interface for the reconfiguration process meaning how much time needs to pass before any changes to the configurations are implemented in the project. This is mainly to protect the investors from being »rug-pulled« (see Section 3.5.5) by the owner as it would be the case if the changes can be implemented immediately. Therefore a 3 or 7-delay strategy would be advisable to use as this ensures more safety for the members that are therefore more willing to spend money on the funding project. In order to bond users to the project incentives as »Discount Rate« and »Bonding Curves« can be configured. The discount rate incentivizes the supporters to buy into the project early as the number of tokens rewarded per payment is lowered with each funding cycle and therefore the same amount of money is less valuable the later a potential member is buying into the project. The bonding rate defines how much of the overflow a token can be redeemed. The higher the percentage the less the deviation over time is, meaning if a low percentage value is chosen a token that is redeemed at a later point in time will return more value than a token that is redeemed right after it was obtained.

3.3.4 Token Ownership and Voting

The ConstitutionDAO used its own token called $PEOPLE which is directly connected with the Ethereum token ERC-20. The governance model was not fully settled as the DAO was created in a hurry and not all details of how it should work were figured out at the time the auction was lost. Many different models like »one token, one vote«, »one wallet, one vote«, or a »quadratic voting model« were discussed [PN21].
The most common governance model for an Ethereum-based DAO, and therefore also for a DAO that uses Juicebox, is that each member has votes based on the proportion of how much he paid in the first place, hence, how many tokens he has [EthDocs].

3.4 Similarities and Differences

In regards to consensus currently (22. April 2022) both examples use a Proof-of-Work approach, however, the Ethereum-based DAOs are converging towards a Proof-of-Stake mechanism as this provides various advantages like a lower entrance investment to partake in the consensus and much lower energy consumption needed to generate new blocks. Nevertheless, already in the PoW approach, there are notable differences between both DAOs. Ethereum-based DAOs as the ConstitutionDAO use a simple hash function in order to ensure the validity of a new block whereas the DashDAO uses its own »X11« hash function which is built up from eleven different hash algorithms, hence, being more difficult to solve and more secure against ASICs or Multipool attacks. Additionally, the reward allocation differs between both organizations as in most

Ethereum-based DAOs the whole amount that is mined is rewarded to the miner whereas in the DashDAO miner gets nowadays less than 45% of the value mined as 10% is reserved for the governance budget and masternode owners, which are a crucial part of the Dash network, receive more than half of what is left as compensation for running and maintaining such masternodes.
These masternodes are possibly the biggest selling point of DashDAO. They enable certain features that simplify or increase the speed of transactions and further ensure security against malicious intent or attacks. The masternode owners also have sole decision-making power, whereas, in Ethereum-based DAOs, anyone who owns a token from the DAO can usually participate in voting. The DashDAO approach is much quicker as less votes are gathered and it additionally ensures that the members that can vote are voting in favor of the development of the DAO as they have a huge stake invested into it.

3.5 Vulnerabilities and Potential Attack Opportunities

Since the start of recording in January 2020 as of the 22. April 2022 in total 86 DeFi attacks have occurred in which approximately 3.2 billion US-$ have been lost.[3] The largest one took place on the 29th of March 2022 as approximately 625 million US-$ in USDC and Ether were lost due to an exploit in the Ronin network's validator nodes[4] which have a similar function as the previous mentioned Masternodes (see Section 3.2.1) in the Dash network.
With approximately 10.9 billion US-$ distributed across various DAOs[5], this is a worrying fact as a bug-free and exploit-safe code implementation of a DAO network and its smart contracts cannot be guaranteed. In the following subsection, some of the most concerning vulnerabilities of DAOs and their networks are mentioned and explained.

3.5.1 The Re-Entrancy Problem - The DAO Hack

One of the most famous attacks on DAOs in recent history was the »The DAO Hack« in 2016 in which approx. 60 million US-$ was siphoned off and in the end, lead to a hard fork of the Ethereum blockchain in order to roll back the Ethereum network to before the attack happened [CS22].
This attack was possible because of an »*Re-Entrancy Exploit*« within the Dao's smart contracts. A re-entrant procedure is given if during the execution it is interrupted, initiated again - the actual re-entrance step -, and both execution parts can terminate without raising any error. As can be seen in Figure 3.1 until the Ether is transferred everything is running as it would for a non-malicious contract. However, when the Ether was transferred the Smart Contract will call a »Fallback Function« which initializes another withdrawal from the same account. Due to an implementation error, the balance state on

[3] https://cryptosec.info/defi-hacks/
[4] https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit/
[5] https://deepdao.io/organizations (as of 18.04.2022)

the server is only updated **after** the process has terminated, the malicious attacker is able to withdraw the same amount several times not needing to have the actual amount of currency in his balance. As the smart contract always withdraws money from the DAO but the actual balance is never updated the attacker can easily siphon large amounts of ether [QL19].

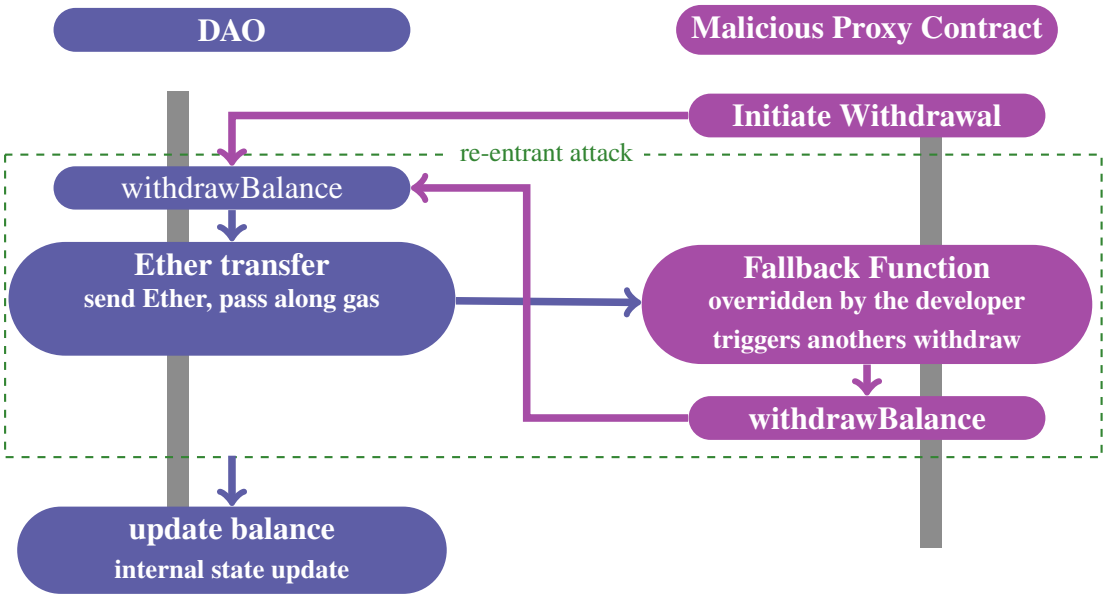

Abbildung 3.1: Re-Entrancy Attacks

3.5.2 51% Attacks

As DAOs and the underlying blockchains are built on the fact that in decentralization not a single person or a small group of people do have control over the whole network. Therefore consensus mechanisms are integrated in order to verify a block's validity in which the majority of all nodes need to agree on one state of the blockchain which is then considered to be the correct state. The 51% or majority attack does use the fact that if one has control over more than 50% of a blockchain's hashing power the group has total control over which transactions are performed and validated and also can rewrite already validated parts of the blockchain. This approach is usually a problem in the early stages of a DAO when the hashing power is not sufficiently large, hence, a group can rent hash power from a third party in order to flood the network with »miners« in order to perform such an attack and gain control of a blockchain. For larger networks like Bitcoin or Ethereum this attack becomes infeasible as the hashing power required for a 51% attack would cost more than a potential attack would eventually return.
Ethereum also tries to limit the success of 51% attacks by converting to a consensus mechanism using the PoS approach. As this requires having a lot of stakes invested into that cryptocurrency in order to perform a majority attack there is very little incentive to destroy or harm the cryptocurrency as this would directly affect the huge amount of money invested into it. It is of more advantage to keep the network secure and healthy

if a huge investment is at stake [EthDocs].
DashDAO also implemented a feature, especially against 51% mining attacks in ChainLocks. By forming a Quorum of masternodes, which is responsible for observing and affirming newly mined blocks and only validates a new block when over 60% of all master nodes see the same block, reorganization attacks before that block are made impossible.

3.5.3 Time Warp Exploit (Kimoto Gravity Well)

A time warp attack is performed by adding a wrong timestamp to a newly mined block. This becomes critical as this would decrease the difficulty of mining subsequent blocks. This is caused by the network itself as it updates the difficulty of blocks periodically in order to keep the average generation rate stable, i.e. for Bitcoin it is 10 minutes per block. When a miner is deceiving the algorithm that the mining did take a long time the network will decrease the difficulty, therefore, making the creation of a new block faster, which in the worst-case lead to an increase in the inflation rate of the cryptocurrency [PM19]. Especially the Kimoto Gravity Well algorithm, which was introduced in order to prevent spikes in difficulty when huge multipools were emerging, had an inbuilt time-warp exploit which was discovered in 2014 [BitFor], hence for example Dash created their own difficulty adjustment algorithm called Dark Gravity Wave in order to manage both problems [DashDocs].

3.5.4 Flash Loan Attacks

On the 18th of April 2022, the credit-based protocol Beanstalk Farms had become the victim of two sinister governance proposals and a flash loan attack, hence losing roughly 182 million US-$. Both proposals contained a malicious rider which created a sinkhole of funds. During the voting period for both proposals, the attacker took a flash loan of approximately 1 billion US-$, therefore accumulating enough assets, around 67% of the Beanstalk Farms governance, in order to approve both proposals [NB22].
A flash loan is similar to a traditional loan whereas a borrower lends money and is assumed to pay it back in full plus interest. However, there are additionally some unique terms and premises as whenever during an execution of a smart contract a flash loan is obtained the full amount must be paid back before the smart contract terminates otherwise the transaction is reversed by the smart contract and the loan is nullified. Also, in order to obtain a flash loan, no collateral is needed as the time frame of the execution of a smart contract is at most a couple of minutes, hence the borrower must return the flash loan right away anyway. One of the most common flash loan attacks is an arbitrage attack which exploits the fact that exchange markets lack the tool to perform instantaneous synchronizations, hence the exchange value may differ between two of those. Therefore, a borrower can get a flash loan, sell them at the exchange market with a higher price and buy them at the other one that has a lower price tag on those tokens. Then the flash loan is paid back with low interest, usually 0.09%, and the borrower made a profit out of literally nothing [DM22].

However, the attacker used another vulnerability that flash loans expose for the previously stated attack. As tokens, especially on an Ethereum-based DAO, can be equated with several votes a flash loan is, therefore, a fast and cheap way to gather a huge amount of votes in order to approve any proposal. These kinds of attacks are usually called »Flash Loan Governance Attacks« as they are targeting the governance and the approval step of proposals of a DAO network. This means that if there are enough tokens in any treasury or pool from which a person can take a flash loan anyone can use those tokens to vote in favor of their most-regarded proposal and after that can pay the loan back with minimal interest rate [FW20].

3.5.5 Rug-Pull Attacks

An attack on a DAO is not always solely performed by an outside member of the network but can also be performed by the owner of the DAO. A so-called»rug-pull« is performed by setting up a DAO network with for example the Juicebox framework (see Section 3.3.1) which on first inspection looks like a legitimate organization in order to gather funding. However, eventually the »scammer« pulls all the liquidity out of the DAO and adds his to his ledger. Especially in Juicebox with which it is possible to build a project with no reconfiguration strategy making changes take into effect immediately after they are changed, hence, being susceptible to such malicious intent. Another way to perform rug-pulls is not to »burn« the private key which was used to instantiate the liquidity pool in order to lock the owner from the control of it. Therefore it is important to ensure that such scams are not made possible and investors may need to be cautious if such exploits are not dealt with, as in 2021 alone over 2.8 billion US-$ were lost due to rug pulls [MS21].

3.5.6 DoS Attacks

In 2016 the Ethereum network became the target of a DoS attack with the result that transaction verification and block creation were immensely slowed down and the syncing of nodes with the network became delayed. This attack was performed by flooding the network with a »barrage of small transactions« which therefore paralyzed the network and made it a nuisance to work with and the network overall became more vulnerable to other attacks as a majority of its nodes were not functioning properly [HA16]. This type of attack could also be mounted against for example the Dash network (see Section 3.2) as it uses solely Masternodes in order to perform votings or check the validity of the blockchain and offers various other features. As they are most often run and maintained by members of the DAO, which might not have the full perspective of how to set a node up correctly, these might get susceptible to such DoS attacks. As the masternodes are a crucial link in the Dash network a failure of the majority of them would lead to an inability to perform the common operations and a potential breakdown of the functioning of the DashDAO.

Kapitel 4: DAO - Law

Im Rahmen des juristischen Teils dieser Arbeit beschränkt sich der Fokus im Folgenden auf sog. *top layer DAOs*, welche auf einem *ground layer DAO* (hauptsächlich Ethereum) basieren und sich dessen Infrastruktur bedienen.[1] Unterschieden wird dabei zwischen einer geringen Anzahl von *regulated DAOs*, die von Regulierungen einzelner Nationen erfasst werden, und sogenannten *maverik DAOs*.[2] Aus juristischer Perspektive interessant sind dabei die *maverik DAOs*, da diese ausschliesslich online existieren, weder einen rechtlichen Sitz noch einen physischen Standort haben[3] und sich aufgrund ihrer vollständig dezentralisierten und autonomen Art die Zuordnung zu einer einzelnen staatlichen Jurisdiktion als äusserst schwierig erweist.[4] Im Sinne dieser Arbeit entspricht der Begriff DAO somit einem *maverik DAO*.

4.1 Anwendbares Recht nach IPRG

Bis anhin ungeklärt ist, welches nationale Recht auf die DAOs angewendet wird, da die einzelnen DAO-Mitglieder auf der ganzen Welt verstreut sein können, formell und faktisch kein Sitz besteht und die administrative Verwaltung durch Smart Contracts wahrgenommen wird.[5] Aufgrund ihrer Dezentralität sind DAOs als länderübergreifende und somit weltweite Erscheinung inhärent transnational.[6] Zur Bestimmung des Rechts, welches im Einzelfall zur Anwendung kommt, muss folglich eine kollisionsrechtliche Einordnung anhanden des IPRG vorgenommen werden.[7]

4.1.1 Lex Fori

Das IPRG stellt bei der Bestimmung des anwendbaren Rechts normalerweise auf die Rechtswahl der Parteien oder auf den Ort (Niederlassung, Wohnsitz, Ort der charakteristischen Leistung) ab.[8] Obwohl eine Rechtswahl die Suche nach dem anwendbaren Recht um einiges vereinfachen würde, wird eine solche regelmässig nicht erfüllt sein.[9] Ein eindeutig bestimmbarer Ort als Anknüpfspunkt für die Gerichtsbarkeit liegt in der dezentralen, digitalen Welt nicht mehr vor und stellt die bestehenden Rechtsordnungen vor eine grosse Herausforderung.[10] Ist eine räumliche Zuordnung unmöglich, verbleibt nur noch die Anwendung der lex fori (Recht des angerufenen Gerichts).[11] Ein Rückgriff auf die lex fori scheint bei Versagen von Gründungs- und Sitztheorie jedoch aus mehreren Gründen nicht zu überzeugen.[12] Erstens würde dies dem Prinzip der engsten Ver-

[1] RIVA, S. 30 f.
[2] RIVA, S. 35.
[3] FENWICK et al., S. 11 f.
[4] RIVA, S. 36 ff.
[5] LEHMANN, S. 249 f.; GYR, S. 17; LUSAR / SATOR.
[6] HESS / SPIELMANN, S. 196; RIVA, S. 36.
[7] LEHMANN, S. 179 f.; HESS / SPIELMANN, S. 196.
[8] HESS / SPIELMANN, S. 196.
[9] LEHMANN, S. 225 f.
[10] HESS / SPIELMANN, S. 196 f.; LEHMANN, S. 235 f.
[11] LEHMANN, S. 235; AUFDERHEIDE, S. 271.
[12] AUFDERHEIDE, S. 267; LEHMANN, S. 235; LUSAR / SATOR.

bindung widersprechen, wonach Sachverhalte anhand der Regeln der räumlich nächsten Rechtsordnung beurteilt werden sollen. Zweitens würde dies die Rechtssicherheit beeinträchtigen, da dies zu sog. *forum shopping* führt, wobei die Parteien je nach angerufenem Gericht ein unterschiedliches Ergebnis herbeiführen können. Folglich führt die lex fori auch als ultima ratio nicht zu einem zufriedenstellenden Resultat.[13]

4.1.2 Das Internet als örtliche Jurisdiktion

Dass die DAOs keiner Rechtsordnung zugeordnet werden können, führt zu einer unbefriedigenden Lösung. Ein Autor schlägt diesbezüglich als kreative Lösung vor, das Internet als örtliche Jurisdiktion anzuerkennen, um das Problem der rechtlichen Anerkennung von DAOs zu lösen.[14] Diese Unsicherheit kann seiner Ansicht nach mithilfe einer modernen Auslegung einer Gesellschaft gemäss Art. 150 IPRG, sowie einer innovativen Interpretation des Staatsbegriffes gemäss Art. 154 IPRG und was als Recht gilt, behoben werden.[15] Erwähnenswert ist vorerst, dass der Begriff einer Gesellschaft i.S.d. internationalen Privatrechts autonom ist und somit nicht an den gesellschaftsrechtlichen numerus clausus gebunden ist.[16] Während es konkret auf den Einzelfall ankommt, sollte eine DAO - sofern sie sich einer ausreichenden Organisationsstruktur bedient - regelmässig unter den Begriff einer Gesellschaft gem. Art. 150 IPRG subsumiert werden können.[17] Ist eine Gesellschaft nach Art. 150 IPRG ausreichend organisiert, muss sodann geprüft werden, ob sie i.S.v. Art. 154 Abs. 1 IPRG gemäss dem Recht des Staates, nach wessen Vorschriften sie organisiert ist, gültig konstituiert wurde. Bestehen keine solche Vorschriften, untersteht sie dem Recht eines Staates, wenn sie sich nach diesem organisiert hat. Erfüllt eine Gesellschaft diese Voraussetzungen nicht, so untersteht sie gemäss Art. 154 Abs. 2 IPRG dem Recht des Staates, in dem sie tatsächlich verwaltet wird. Definitionsgemäss sind DAOs jedoch nicht nach dem Recht eines einzelnen Staates organisiert, da sie ausschliesslich im Internet existieren und keiner staatlichen Jurisdiktion zugeordnet werden können.[18] Folglich sei bei DAOs auf den Ort der tatsächlichen Verwaltung abzustellen. Der Autor zeigt daraufhin anhand verschiedener Beispiele, dass bei DAOs der Ort der tatsächlichen Verwaltung kein anderer als das Internet sein kann.[19] Folgt man der traditionellen Interpretation des Staatsbegriffs nach Art. 154 IPRG, hätten DAOs folglich keine rechtliche Existenz in der Schweiz und würden sich folglich ausserhalb des Rechtssystems befinden.[20] Aus diesem Grund wurde in der Lehre durch weite Auslegung und kreative Methoden versucht, die DAOs einer der privatrechtlichen Gesellschaftsformen zuzuordnen. Obwohl die DAOs in vielen Aspekten den Gesellschaften des schweizerischen Rechts gleichen, blieb den Autoren keine andere Wahl als einzusehen, dass DAOs schlecht unter eine

[13] LEHMANN, S. 235.
[14] RIVA, S. 54 ff.
[15] RIVA, S. 36.
[16] CoRo-LDIP/CL GUILLAUME, S. 1282.
[17] RIVA, S. 43 ff.
[18] RIVA, S. 52.
[19] RIVA, S. 52 ff.
[20] RIVA, S. 54.

einzige Gesellschaftsform subsumiert werden können.[21] Der Autor schlägt daraufhin vor, den Geltungsbereich der Definitionen von Staat und Recht i.S.v. Art. 154 IPRG zu öffnen und um den online-Bereich und den dazugehörenden Code zu erweitern. In Analogie dazu, wie Gründer sich dazu entscheiden, sich nach dem Recht eines Staates i.S.v. Art. 154 Abs. 1 IPRG zu organisieren, scheinen Gründer und Mitglieder einer DAO zu entscheiden, sich nach dem Recht des Codes zu organisieren und sich der örtlichen Gerichtsbarkeit des Internets zu unterwerfen.[22] Ein anderer Ansatz wäre das Prinzip der Funktionalen Äquivalenz.[23] Eine vertiefte Auseinandersetzung damit würde den Rahmen dieser Arbeit jedoch sprengen, weshalb nicht weiter darauf eingegangen werden kann.

4.1.3 Zwischenfazit

Die Bestimmung der Juristiktion von DAOs gestaltet sich aufgrund derer Dezentralität als äusserst schwierig. Weder die Anwendung von Gründungs- oder Sitztheorie noch die Anwendung von lex fori scheint zu einem zufriedenstellenden Ergebnis zu führen. Als innovativer Ansatz wird von einem Autor eine online Jurisdiktion vorgeschlagen. Dies würde dazu führen, dass eine DAO allein durch seine Existenz im Internet ausreichend konstituiert ist und ihr somit in der Schweiz eine rechtliche Existenz gewährt wird. Im folgenden Teil dieser Arbeit wird jedoch unbeachtlich dieser Problematik von der Anwendbarkeit des schweizerischen Rechts ausgegangen.

4.2 Eingliederung in das Gesellschaftsrecht

Bevor die verschiedenen Stakeholder identifiziert und mögliche Haftungsfragen geklärt werden können, muss eine Einordnung von DAOs in das schweizerische Gesellschaftsrecht vorgenommen werden. In der Schweiz besteht ein durch das Gesetz vorgegebener numerus clausus von zehn möglichen Gesellschaftsformen.[24] Gesellschafter können durch ihre Vertrags- oder Vereinigungsfreiheit keine neuen Gesellschaftsformen schaffen oder bestehende kombinieren.[25] DAOs müssten folglich unter eine der bestehenden Gesellschaftsformen subsumiert werden. Im Folgenden wird somit evaluiert, ob DAOs einer der gesetzlich vorgegebenen Rechtsformen zugeordnet werden können.

4.2.1 Qualifikation als Körperschaft

Es ist nach wie vor offen, ob den DAOs eine eigene Rechtspersönlichkeit zukommt. Die Idealform wäre, dass DAOs unabhängig von anderen natürlichen oder juristischen Personen von der Rechtsordnung als Rechtssubjekt anerkannt werden.[26] Für eine Qua-

[21] RIVA, S. 54; BÄRTSCHI, S. 14 f.; AUFDERHEIDE; HESS / SPIELMANN, S. 191 ff.
[22] RIVA, S. 54 ff.
[23] RIVA, S. 57 ff.
[24] MEIER-HAYOZ et al., S. 45 f.
[25] JUNG et al., S. 107 f.
[26] BÄRTSCHI, S. 11.

lifikation einer DAO als Körperschaft spricht auf der einen Seite die unbegrenzte Anzahl möglicher Beteiligten (*token holder*), die zumeist fehlende persönliche Beziehung sowie das Nichtbestehen von Treuepflichten der einzelnen Gesellschafter. Auch die Trennung von Kapital und Gesellschafter sollte gegeben sein, da die DAO-Mitglieder keinen direkten Zugriff auf die *protocol-treasury* haben.[27] Ebenso gilt als Indiz die Unabhängigkeit der DAO-Mitglieder, die regelmässige kapitalistische Beteiligung sowie die grundsätzlich dem investierten Kapital entsprechenden Stimmkraft (sog. *token voting*). Die Qualifikation des Erwerbs von Tokens als Gewähr von Fremdkapital ist der hiernach vertretenen Ansicht abzulehnen.[28] Zudem erinnert die grundsätzlich freie Übertragbarkeit der Gesellschafterstellung, d.h. der Token, an eine Körperschaft. Hierbei ist jedoch festzuhalten, dass auch nicht übertragbare *governance tokens* existieren.[29] Auf der anderen Seite sprechen jedoch ebenso viele Gründe gegen eine Qualifikation als Körperschaft. Während ein mögliches Whitepaper möglicherweise durch analoge Auslegung den Statuten entsprechen könnte, liegt diesbezogen bei DAOs eine weitreichende Gestaltungsfreiheit vor, wogegen diese bei Körperschaften vergleichsweise eingeschränkt ist. Ebenso dagegen spricht das Erfordernis von natürlichen Personen als Verwaltungsratsmitglieder von Aktiengesellschaften und Geschäftsführer von Gesellschaften mit beschränkter Haftung gemäss Art. 707 Abs. 3 und Art. 809 Abs. 2 OR. Bei Fehlen der erforderlichen Organen würde gemäss Art. 731b und Art 819 OR ein Organisationsmangel vorliegen.[30]. Bei einer DAO liegt aufgrund der dezentralen Struktur und meist eher flächeren Hierarchie weder ein Verwaltungsrat, noch eine Geschäftsführung vor. Ferner wird ein für Körperschaften zwingend notwendiger Handelsregistereintrag bei DAOs vermutlich regelmässig ausbleiben.[31] Auch bei Vereinen bestehen von Gesetzes wegen in verschiedenen Bereichen zwingende Anforderungen an Statuten und Organe.[32]. Experimente wie eine DAA[33], bei welchen zwar der Entscheidungsprozess und das operative Geschäft als DAO getätigt werden, elementare Prozesse aber aufgrund von zwingenden gesetzlichen Vorschriften trotzdem zentralisiert vorgenommen werden, erfüllen die Ansprüche an die Dezentralität einer DAO nicht, sondern entsprechen eher der Idee einer *regulated-DAO*.[34]

4.2.2 Personengesellschaften

Wird nicht von einer eigenen Rechtspersönlichkeit einer DAO ausgegangen, wäre zu prüfen, ob eine Personengesellschaft vorliegt. Dafür sprechen würde lediglich die weitreichende Gestaltungsfreiheit der vertraglichen Grundlage sowie die Selbstorganschaft bzw. das Fehlen von Leitungs- oder Verwaltungsorganen.[35] Personengesellschaften bil-

[27] GYR, S. 9.
[28] BÄRTSCHI, S. 13.
[29] ARSENAULT.
[30] BÄRTSCHI, S. 12.
[31] MEIER-HAYOZ et al., S. 169.
[32] HAUSHEER / AEBI-MÜLLER, S. 378 ff.
[33] GLARNER et al..
[34] Zum Ganzen JUNG et al., S. 102 f.
[35] BÄRTSCHI, S. 14.

den sich i.d.R. aus wenigen Gesellschafter, gekoppelt an eine persönliche Beziehung und intensiven Treuepflichten. Des Weiteren besteht eine grundsätzliche Abhängigkeit der Existenz der Gesellschaft von jedem Mitglied (vgl. Art. 545 Abs. 1 Ziff. 2 OR). Gesellschafterwechsel sind im Sinne einer Vertragsänderung eingeschränkt. Ebenfalls zeichnen sich Personengesellschaften durch das Einstimmigkeitsprinzip bei der Beschlussfassung und einer starken persönlichen Haftung aus.[36] Die Anzahl DAO-Mitglieder ist stark vom Einzelfall abhängig. Es kommt jedoch nicht selten vor, dass die Mitgliederzahl von erheblicher Höhe ist und sich in einem stetigen Wechsel befindet.[37] Die *governance tokens* werden rund um die Uhr gehandelt und selbst bei DAO-Migliedern im Besitz eines hohen Anteils dieser Tokens - inklusiv daraus resultierender starker Stimmkraft - ist die Wahrung derer Anonymität eine gängige Praxis. Keiner dieser Punkte spricht für eine starke persönliche Beziehung zwischen allen DAO-Mitgliedern und auch Treuepflichten liegen im klassischen Sinne keine vor. Zwar wird in der Praxis mit neuen Formen der Governance experimentiert[38], jedoch ist das Modell des *token votings* im Sinne eines Mehrheitsprinzips nach wie vor vorherrschend. Werden konkret die Voraussetzungen des Auffangstatbestands der einfachen Gesellschaft[39] geprüft, ist nach Art. 530 Abs. 1 OR eine vertragsmässige Verbindung von zwei oder mehreren Personen zur Erreichung eines gemeinsamen Zweckes mit gemeinsamen Kräften oder Mitteln erforderlich. Die vertragliche Bindung kann formfrei und durch konkludentes Verhalten eingegangen werden.[40] Entscheidend ist nicht das Bewusstsein der Qualifikation als eG, sondern der Wille der Parteien zur vertraglich bekräftigten gemeinsamen Zweckverfolgung.[41] Obschon die Annahme vertretbar ist, dass die DAO-Mitglieder auf ein gemeinsames Ziel hinarbeiten, dafür gemeinsam Kapital bereitstellen und sich dafür Smart Contracts zunutze machen[42], darf nicht ohne Weiteres angenommen werden, dass diese den Willen gefasst haben, sich zu einer Gesellschaft zusammenzuschliessen und alle damit einhergehenden Konsequenzen in Kauf zu nehmen.[43] Insbesondere aufgrund der Tatsache, dass das einzelne DAO-Mitglied die anderen Beteiligten nicht persönlich kennt und diese sogar häufig unter einem Pseudonym auftreten, kann im Bezug auf die damit verbundenen Treuepflichten sowie den solidarischen, persönlichen und unbeschränkten Haftungsrisiken nicht von einem Rechtsbindungswillen ausgegangen werden.[44] Zudem scheint es verkehrt, bei einem System, welches *trustless* ist und daher dazu dient, sich nicht binden zu müssen, einen Rechtsbindungswillen anzunehmen. Analog ist - bei Annahme eines kaufmännisch geführten Gewerbes - auch die Qualifikation als Kollektiv- oder Kommanditgesellschaft nicht zielführend.[45]

[36] JUNG et al., S. 102 f.
[37] AUFDERHEIDE, S. 268 f.
[38] ARSENAULT.
[39] HESS / SPIELMANN, S. 190 ff.; BÄRTSCHI, S. 14 f.
[40] BSK-OR HANDSCHIN, N 2.
[41] BSK-OR HANDSCHIN, N 17.
[42] GYR, S. 10 ff.
[43] BÄRTSCHI, S. 14 f.
[44] MÜLLER, S. 488.
[45] BÄRTSCHI, S. 15; GYR, S. 10 Rz. 24.

4.2.3 Zwischenfazit

Die DAO kombiniert Elemente einer Körperschaft sowie einer Personengesellschaft mit eigenen, dem Gesellschaftsrecht bisher fremden Charakterzügen. Durch den numerus clausus im Schweizer Gesellschaftsrecht ist jedoch eine DAO als Gesellschaft sui generis zurzeit nicht denkbar. Während gewisse Autoren[46] durch kreative Auslegung versuchen, sich die DAO durch bestehendes Recht zu erklären, bleibt offen, ob dies im Sinne einer verständlichen Rechtsordnung wirklich zielführend ist.

4.3 DAOs als kollektive Kapitalanlage

Wie bereits festgehalten[47], dienen DAOs zu zahlreichen Zwecken, wovon lediglich ein Teil davon als Investitionsvehikel agiert. Der in der Literatur öfters gezogene Vergleich zu den kollektiven Kapitalanlagen muss sich somit auf die sog. Fundraising-DAOs beschränken. Die Legaldefinition der kollektiven Kapitalanlagen befindet sich in Art. 7 KAG und beinhaltet vier Unterstellungskriterien. Art. 7 KAG beschreibt die kollektiven Kapitalanlagen als Vermögen, die durch die Anleger zur kollektiven Kapitalanlage aufgebracht und in Fremdverwaltung für deren Rechnung verwaltet werden, wobei die Anlegerinteressen gleichmässig befriedigt werden.[48] Im Folgenden wird anhand des Beispiels der ConstitutionDAO gezeigt, inwiefern eine Fundraising-DAO als Kollektive Kapitalanlage qualifiziert werden kann. Eine Qualifikation als kollektive Kapitalanlage hätte weitgehende Konsequenzen und würde eine Bewilligungs- und Genehmigungspflicht durch die FINMA, eine daraus folgende Restriktion auf im KAG vorgesehene Rechtsformen sowie eine Pflicht zur Beachtung zahlreicher weiterer Vorschriften mit sich führen.[49]

4.3.1 Vermögen

Eine kollektive Kapitalanlage setzt sich aus dem von den verschiedenen Anlegern zur Einlage aufgebrachten Vermögen zusammen. Unter dem Begriff des Vermögens ist eine Gesamtheit von Geld, geldwerten Sachen und Rechten gemeint, die sich zur Vermögensanlage durch die Anleger eignen und verwertbar sind. [50] Darunter fallen auch Kryptowerte.[51] Beim ConstitutionDAO wurden fast 50 Millionen Dollar in Ether an einen Smart Contract geschickt. Die Vermögensanlage bestand somit aus einer Kryptowährung.

[46] GYR; AUFDERHEIDE.
[47] s. Abschnitt 1.1.2.
[48] BSK-KAG RAYROUX / PASQUIER, N 3.
[49] MICHAEL, S. 76 f.; ETIENNE, S. 24 f.; GYR, Rz 37; BSK-KAG RAYROUX / PASQUIER, N 4.
[50] BSK-KAG RAYROUX / PASQUIER, N 11.
[51] Bericht des Bundesrat, S. 7 f.

4.3.2 Gemeinschaftliche Kapitalanlage

Unter gemeinschaftlicher Kapitalanlage versteht man jede aufgrund von identischen Verträgen getätigte Anlage zur Erzielung eines Ertrages, eines Wertzuwachses oder zumindest zur Erhaltung des Vermögens.[52] Erstens ist die Gemeinschaftlichkeit gegeben, wenn sich gemäss Art. 5 KKV mindestens zwei unabhängige Anlegerinnen oder Anleger beteiligen.[53] Zweitens liegen identische Verträge dann vor, wenn keine Individualisierung der Einlagen besteht und die Anleger ausschliesslich einen proportionalen Anspruch an dem Gesamtsaldo haben.[54] Die Kapitalanlage hat grundsätzlich passiv zu erfolgen, insb. damit die Anlagetätigkeit von rein unternehmerischen Tätigkeiten bestimmter Wirtschaftsakteuren abgegrenzt werden kann.[55] An der ConstitutionDAO waren zahlreiche Personen beteiligt, welche Vermögenswerte im Austausch für Tokens eingebracht haben. Die Tokens vermittelten Stimmrechte über den Verwendungszweck der Originalkopie bei erfolgreicher Ersteigerung sowie ein Rückerstattungsrecht bei Misserfolg.[56] Die Einlagen der einzelnen DAO-Mitglieder waren somit nicht mehr individualisierbar und die Mindestzahl von zwei unabhängigen Anlegerinnen und Anleger wurde erreicht. Es ist fraglich, ob durch den Erwerb einer Originalkopie der amerikanischen Verfassung eine Anlage zur Erzielung eines Ertrags oder eines Wertzuwachses oder zumindest zur Erhaltung des Vermögens vorliegt. Durch das Fehlen eines spezifischen Whitepapers ist der Zweck der ConstitutionDAO nicht abschliessend zu ermitteln. Obwohl der wahre Wert fast unmöglich zu ermitteln ist, kann argumentiert werden, dass Investitionen in historisch äusserst relevante Dokumente zumindest werterhaltend sind. Da es sich um eine einmalige Investition handelt, ist zudem die Passivität ebenfalls zu bejahen. Bei anderen DAOs mit stärkerem Fokus auf Investitionen (Vgl. The DAO) kann sogar davon ausgegangen werden, dass eine Vermehrung des Vermögens angestrebt wird.[57] Folglich ist die Ansicht vertretbar, dass es sich bei der ConstitutionDAO um eine gemeinsame Kapitalanlage handelt.

4.3.3 Gleichmässige Befriedigung der Anlegerinteressen

Aufgrund des supra-individuellen Leistungsinhalts der kollektiven Kapitalanlage müssen die Anlegerinteressen gleichmässig befriedigt werden.[58] Insbesondere im Bereich der Rücknahmebegehren ist die Gleichbehandlung strikt zu beachten.[59] Bei der ConstitutionDAO hatten die Tokeninhaber sowohl ein zukünftiges Stimmrecht als auch eine Rückerstattungsmöglichkeit proportional zum eingebrachten Betrag.[60] Die Anlegerinteressen wurden somit gleichwertig beachtet.

[52] BGE 116 Ib 73, S.79 E.2c; BSK-KAG RAYROUX / PASQUIER, N 13; GYR, Rz. 37 ff
[53] BSK-KAG RAYROUX / PASQUIER, N 21.
[54] BSK-KAG RAYROUX / PASQUIER, N 19; GYR, Rz. 41.
[55] BSK-KAG RAYROUX / PASQUIER, N 6 ff; GYR, Rz. 39; JUTZI / SIERADZKI, S. 121 f.
[56] PATEL.
[57] GYR, Rz. 40.
[58] BSK-KAG RAYROUX / PASQUIER, N 3.
[59] BSK-KAG RAYROUX / PASQUIER, N 24; GYR, Rz. 43.
[60] PATEL.

4.3.4 Fremdverwaltung

Bei kollektiven Kapitalanlagen gilt, mit Ausnahme der Einanlegerfonds, der Grundsatz der Fremdverwaltung.[61] Die Anlegerinnen und Anleger dürfen somit weder rechtlich noch wirtschaftlich in der Lage sein, die Anlageentscheide zu beeinflussen.[62] Obwohl dies bei der ConstitutionDAO aufgrund der nur einmaligen Investition nicht allzu klar ersichtlich ist, widerspricht dieses Kriterium dem inhärenten Begriff einer DAO. Bei DAOs spielen die Mitspracherechte eben gerade eine massgebende Rolle, da die DAO-Mitglieder bei wesentlichen Entscheiden Einfluss nehmen können. Dass zur Bewältigung administrativer Vorgänge auf Smart Contracts zurückgegriffen wird, ändert daran nichts.[63] Bei DAOs ist somit eine Selbst- und nicht eine Fremdverwaltung anzunehmen.

4.3.5 Exkurs: Investmentclub

Erfolgt eine kollektive Kapitalanlage durch Selbstverwaltung, ist zu prüfen, ob ein sog. Investmentclub vorliegt. Die Anzahl der Mitglieder eines Investmentclubs muss jedoch überschaubar sein d.h. die Mitgliederanzahl darf 20 Personen nicht überschreiten.[64] Die ConstitutionDAO sowie alle weiteren bekannten DAOs kennen keine Beschränkung der Mitglieder und überschreiten diese Zahl vermutlich bei Weitem.[65] Durch das Aufkommen von *protocol owned liquidity*[66] müsste zudem geklärt werden, ob als Mitglieder nur natürliche Personen in Frage kommen oder nicht.[67]

4.3.6 Zwischenfazit

Obwohl die sog. Fundraising-DAOs gewisse Parallelen zur kollektiven Kapitalanlage aufweisen, scheitert die Zuordnung zu einem rechtlichen Konstrukt auch in diesem Fall, da die DAOs definitionsgemäss selbstverwaltet werden. Obwohl gewisse Elemente eine Ähnlichkeit aufweisen, entsprechen die Merkmale eines DAOs gesamtheitlich betrachtet auch nicht den Eigenschaften eines Investmentclubs.[68]

4.4 DAOs als reines Vertragsnetz

Nach den erfolgten Ausführungen wird ersichtlich, dass sich die DAOs nicht ohne Weiteres unter bestehende Rechtsformen subsumieren lassen. Somit ist letztlich zu prüfen, ob es sich bei DAOs um ein rein vertragliches Austauschverhältnis handeln könnte.

[61] BSK-KAG RAYROUX / PASQUIER, N 25.
[62] JUTZI / SIERADZKI, Rz. 292.
[63] JUTZI / SIERADZKI, Rz. 425 f.; GYR, Rz. 44 f.
[64] JUTZI / SIERADZKI, Rz. 196; GYR, Rz. 46 f.
[65] GYR, Rz. 47; HESS / SPIELMANN, S. 192.
[66] CHITRA et al., S. 1.
[67] GYR, Rz 46; PFENNINGER / NÜESCH, N 19.
[68] GYR, Rz. 47.

4.4.1 Vertragsfunktion eines Smart Contracts

Fraglich ist somit vorerst, ob ein Smart Contract alleinstehend als rechtlich bindend betrachtet werden kann oder ob ein zusätzlicher Vertrag in der physischen Welt erforderlich ist. De lege lata werden Smart Contracts in der Schweiz nicht als formal verbindlich anerkannt.[69] Während der Ausdruck Smart Contract den Schluss nahelegt, dass es sich um einen Vertrag handelt, wird in der Literatur regelmässig vertreten, dass damit zwar ein Verfügungsgeschäft abgeschlossen werden kann, es jedoch nicht genügt, um ein Verpflichtungsgeschäft zu begründen.[70] Je nach Ausgestaltung kann sich ein Smart Contract jedoch auch auf das Verpflichtungsgeschäft auswirken.[71] Dies könnte dazu führen, dass ein Smart Contract als eine Art AGB in den Vertrag aufgenommen wird. Voraussetzung für das Zustandekommen eines Vertragsverhältnisses sind nach Art. 1 OR die übereinstimmenden und gegenseitigen, expliziten oder konkludenten Willensäusserungen der Parteien. Somit müsste der Smart Contract vom Konsens der Parteien getragen werden. Wird bei der Vereinbarung der Parteien nicht ausdrücklich auf die AGBs hingewiesen, werden Sie nicht Teil der vertraglichen Vereinbarung und können somit nur als Hilfsmittel für die Vertragserfüllung beigezogen werden.[72]

4.4.2 Vertragsqualifikation einer DAO

Der Beitritt zu einer DAO bzw. der Erwerb von Stimmrechten erfolgt in der Praxis meistens durch den Erwerb der entsprechenden Tokens an einer DEX. Es besteht somit regelmässig kein zusätzlicher Kaufvertrag in der physischen Welt. Zudem gibt es bei einer DEX praktisch keine Möglichkeit, die Identität des Verkäufers festzustellen. Dazu kommt die Problematik, dass die anderen *token holder* der DAOs regelmässig unter einem Pseudonym auftreten.[73] Es besteht somit auch keine Vereinbarung in der physischen Welt zwischen dem Käufer oder dem Verkäufer und den restlichen DAO-Mitgliedern. Der Abschluss eines Kaufvertrages mithilfe eines Smart Contracts kann und wird in der Praxis regelmässig konkludent erfolgen. Ein solcher konkludenter Abschluss eines Kaufvertrags ist auch möglich, wenn die Gegenpartei dem Käufer nicht bekannt ist, da es sich nicht um einen wesentlichen Punkt i.S.v. Art. 2 i.V.m. Art. 184 OR handelt.[74] Es könnte somit die Annahme vertreten werden, dass durch den Erwerb von DAO Tokens ein stillschweigender Konsens bezüglich dem Kaufvertrag zwischen Käufer und Verkäufer gegeben ist. Es könnte ebenfalls vertreten werden, dass der Smart Contract der DEX ein Teil dieses Vertrages wird bzw. als Hilfestellung beigezogen werden könnte. Die Annahme, dass neben dem Kaufvertrag zwischen Käufer und Verkäufer zusätzlich noch Verträge zwischen dem Käufer und jedem weiteren bestehenden DAO-Mitglied geschlossen werden, geht hingegen zu weit. Auch die Annahme eines Vertragsschlusses mit jedem DAO-Mitglied, sobald der Käufer seine erworbenen To-

[69] RIVA, S. 15.
[70] EGGEN, S. 157.
[71] EGGEN, S. 161.
[72] EGGEN, S. 162.
[73] RIVA, S. 15.
[74] BSK-OR KOLLER, N 43 f.

kens zur Governance der DAOs benutzt, erscheint nicht praktikabel. Die Problematik besteht hierbei weniger darin, ob der Smart Contract Teil des Vertrages wird, sondern dass der Wille zum Vertragsschluss regelmässig fehlen wird. Durch das Benutzen der Smart Contracts der DAOs signalisiert das einzelne DAO-Mitglied lediglich, in welche Richtung sich die DAO als solche fortbewegen soll. Dies spricht wiederum für eine Qualifizierung einer DAO als Gesellschaftsform und gegen ein Vertragsnetz zwischen den einzelnen DAO-Mitglieder.[75]

4.5 Stakeholder einer DAO

Entgegen einer geläufigen Auffassung sind DAOs nicht vollständig autonomisiert.[76] Es handelt sich dabei eher um eine neue Organisationsform, welcher sich die verschiedenen Stakeholder bedienen, um miteinander zu interagieren. Im Folgenden werden die verschiedenen Erscheinungsformen der Stakeholder von DAOs analysiert und mit bestehenden Stakeholdern des schweizerischen Gesellschaftsrechts verglichen. Insb. aufgrund der häufigen Pseudonymität der einzelnen Stakeholder ist der Vergleich mit den Akteuren der geltenden Rechtsformen nicht immer einfach. Während die folgende Einordnung allgemeiner Natur ist, sollte im Konkreten stets der Einzelfall betrachtet werden.

4.5.1 Entwickler

Die Entwickler sind zuständig für die Erstellung der Smart Contracts. Sofern bereits eine entsprechende Governance Struktur eingerichtet wurde und Protokoll Updates nicht mehr alleinig in ihrer Macht stehen, entsprechen sie normalen DAO-Mitgliedern. Liegt keine Governance Struktur vor, handelt es sich technisch gesehen noch nicht um eine DAO. Bis zu diesem Punkt haben die Entwickler jedoch eine erhebliche Macht über die Smart Contracts und das damit einhergehende Produkt, da die einzelnen Updates nicht durch einen Governance Prozess legitimiert wurden.

4.5.2 Benutzer

Als reine Benutzer der DAOs gelten Personen, welche das Protokoll benutzen, ohne selbst DAO-Token zu halten. Solche kommen typischerweise bei Dienstleistungs- und Protokoll-DAOs vor und entsprechen schlussendlich den Kunden der DAOs. Des Öfteren besteht eine grössere Schnittstelle zwischen Benutzern und DAO-Mitgliedern, da letztere selbstverständlich das Protokoll ebenfalls benutzen. Rechtlich relevant sind diese im Bezug auf mögliche Exploits und die eventuell auftretenden Haftungsansprüche.

[75] BÄRTSCHI, S. 15.
[76] GYR, S. 1 und 7.

4.5.3 DAO-Mitglieder

Als DAO-Mitglieder gelten vorerst die Halter des entsprechenden DAO-Tokens, welches ihnen Stimmrechte und womöglich weitere Ansprüche verleiht.[77] Darunter fallen die Entwickler, Investoren, Mitglieder des Kernteams und sonstige Mitwirkende. Eine spezielle Eigenart einer DAO ist, dass sämtliche Mitwirkende durch die DAO-Token i.d.R. automatisch auch als Investoren involviert sind. Im Vergleich mit dem Gesellschaftsrecht besteht eine grosse Ähnlichkeit zwischen den stimmberechtigten DAO-Mitgliedern und einer Generalversammlung einer Aktiengesellschaft. Gleich wie die GV nach Art. 698 Abs. 1 OR sind die DAO-Mitglieder das oberste Organ einer DAO. Eine gängige Praxis ist zudem, dass bei Abstimmungen ebenfalls gewisse Quoren (Vgl. Art. 704 OR) in die Smart Contracts eingebaut werden.[78]

4.5.4 Delegates

Bei moderneren DAO Strukturen besteht die Möglichkeit der DAO-Mitglieder, ihr Stimmrecht an sogenannte *Delegates* zu delegieren.[79] Die Funktion der Delegates besteht in einer Mischform zwischen Verwaltungsrat und Stimmrechtsvertreter, da bei DAOs keine Kompetenzentrennung wie bei GV und VR besteht. Die *Delegates* können sodann im Namen der DAO-Mitglieder über die Zukunft der DAOs abstimmen. Diese sind dabei jedoch weder an Vorgaben der delegierenden DAO-Mitglieder noch an Vorgaben einer Institution gebunden, d.h. sie sind keiner Treuepflicht unterstellt.

4.6 Ansprüche der Investoren

Der Hauptanspruch von Investoren bzw. den Inhabern von DAO-Token sind die damit verbundenen Stimmrechte.[80] Interessant ist jedoch, ob den *token holder* noch weitere Rechte wie Dividenenausschüttungen oder Bezugsrechte gewährt werden.[81] Erste Annäherungen an Dividendenausschüttungen wurden durch die CurveDAO[82] erforscht, indem DAO-Mitglieder ihre Tokens für eine bestimmte Zeit in einem Smart Contract sperren und im Gegenzug einen prozentualen Betrag von 50 Prozent der Protokollgebühren sowie ein Mitspracherecht bezüglich der zukünftigen Emissionen der DAO-Tokens erhalten konnten.[83] Sowohl bei The DAO, als auch bei der ConstitutionDAO hatten die Investoren unter gewissen Voraussetzungen das Recht, ihre Einlagen zurückzuverlangen. Waren bei The DAO die Investoren mit einem Mehrheitsentscheid nicht

[77] GYR, S. 7.
[78] ARSENAULT.
[79] »DAOrayaki Research |Sybil: A Governance Tool for Discovering Delegates«, https://medium.com/@daorayaki/daorayaki-reserach-sybil-a-governance-tool-for-discovering-delegates-10ec4255b6a6 (Besucht am: 16.04.2022).
[80] BÄRTSCHI, S. 10 f.; ARSENAULT.
[81] BÄRTSCHI, S. 10.
[82] EGOROV.
[83] »What are veTokens?«, https://academy.stakedao.org/what-are-vetokens-2/ (Besucht am: 16.04.2022).

einverstanden, konnten sie mithilfe einer neuen DAO ihr ursprüngliches Investment zurücknehmen.[84] Bei der ConstitutionDAO hatten die DAO-Mitglieder nach der misslungenen Auktion die Möglichkeit einer Rückerstattung.[85] Diese Rechte sind de lege late jedoch nur faktisch vorhanden und ausschliesslich aufgrund der Smart Contracts durchsetzbar. Eine rechtliche Möglichkeit zum Enforcement ist unseres Erachtens zur Zeit nicht ersichtlich.

4.7 Haftung von DAOs

Mit dem Aufkommen von neuen autonomen Systemen stellen sich gleichzeitig zahlreiche Haftungsfragen. Im Folgenden wird die Haftung einer DAO als solche sowie eine mögliche Haftung der einzelnen DAO-Mitglieder analysiert.

4.7.1 Haftung der DAO als solche

Aufgrund der vielen Gemeinsamkeiten zu einer Kapitalgesellschaft liegt es nahe, das System als solches als primäres Haftungssubjekt zu behandeln.[86] Insb. im Bezug auf die fehlende Treuepflicht der DAO-Mitglieder und deren Pseudonymität wäre es wünschenswert, die DAO als solche schadenersatzpflichtig halten zu können. De lege lata genügt die DAO den Voraussetzungen einer Kapitalgesellschaft aus den bereits erwähnten Gründen nicht und kann somit nicht als solche haftbar gemacht werden.

4.7.2 Haftung der Beteiligten

Eine Haftung nach dem Recht der einfachen Gesellschaft würde eine solidarische, persönliche und unbeschränkte Haftung mit sich führen.[87] Gemäss den obigen Erwägungen ist die DAO aufgrund fehlendem Rechtsbindungswillen ebenfalls nicht als eG zu qualifizieren. Gelingt weder eine Qualifikation als Körperschaft, Personengesellschaft oder vertragliche Beziehung, schlägt ein Teil der Lehre eine analoge Betrachtung anhand der Regeln der einfachen Gesellschaft vor.[88] Dies wird insb. aus dem Grund vorgeschlagen, dass Gläubiger im Aussenverhältnis nicht dadurch benachteiligt werden sollten, dass es im Innenverhältnis an einem Rechtsbindungswillen fehle. Dies ist jedoch abzulehnen. Wenn der Auffangtatbestand der einfachen Gesellschaft aufgrund fehlendem Rechtsbindungswillen nicht erfüllt ist, kann dies nicht umgangen werden, indem eine Gesellschaft fingiert wird.[89] Zudem würde sich dabei wieder die Frage der Durchsetzbarkeit stellen, da sich dies mit Blick auf die Ausgestaltung der DAOs und insb. der fehlenden Identifizierbarkeit der DAO-Mitglieder als schwierig gestalten würde.[90] Sind sämtliche

[84] GYR, RZ. 13.
[85] PATEL.
[86] BÄRTSCHI, S. 15 f.; FORRER et al., S. 24 f.
[87] FORRER et al., S. 25; HESS / SPIELMANN, S. 191.
[88] GYR, RZ. 50; BÄRTSCHI, S. 16 f.
[89] BÄRTSCHI, S. 17.
[90] GYR, RZ. 51.

DAO-Mitglieder haftbar, würde dies zudem im Fall der Beteiligung von externen DAOs zur Ausdehnung der Haftbarkeit und weiteren rechtlichen Unsicherheiten führen. Im Sinne einer ausservertraglichen Haftung wäre des Weiteren der Rückgriff auf die beteiligten Personen nach Art. 50 OR denkbar.[91]

4.7.3 Blick in die Zukunft

Aus einer Perspektive de lege ferenda könnten die Eigenschaften einer DAO und deren Ähnlichkeiten zu einer körperschaftlichen Struktur als Anhaltspunkt für eine Gesellschaft sui generis gesehen werden.[92] Würde man den DAOs eine eigene Rechtspersönlichkeit gewähren, würde dies zu erheblich grösserer Rechtssicherheit führen. DAOs würden von der schweizerischen Gesetzgebung profitieren und die Schweiz würde als attraktiver Wirtschaftsstandort gestärkt werden.[93] Insbesondere würde dies die Möglichkeit der Einführung einer Haftung für DAOs als solche eröffnen. Durch eine gesetzliche Kausalhaftung könnte das Betriebsrisiko somit auf die DAOs als solche übergewälzt werden. Der Nutzen einer Schadenersatzpflicht der DAOs hängt jedoch davon ab, ob die einzelnen DAOs über ein genügendes Haftungssubstrat verfügen.[94] In der Praxis hat sich gezeigt, dass DAOs über erhebliche Geldbeträge verfügen. Der DeepDAO Website zufolge stehen zur Zeit insgesamt ca. 10.9 Milliarden US-$[95] unter der Verfügung verschiedener DAOs.[96] Eine gesetzliche Kausalhaftung könnte somit in Verbindung mit gewissen Eigenkapitalvorschriften umgesetzt werden. Dies könnte mit gewissen Audit Vorschriften kombiniert werden, um potentiellen Codefehler oder Backdoors der Entwickler entgegenzuwirken. Im Bereich des algorithmischen Börsenhandels bestehen solche Pflichten bereits heute.[97]

4.7.4 Zwischenfazit

Aufgrund fehlender Qualifikation als Rechtssubjekt kann de lege lata eine DAO nicht haftbar gemacht werden. Eine analoge Anwendbarkeit der Regeln der einfachen Gesellschaft würde hingegen zu erheblichen Risiken für DAO-Mitglieder, Schwierigkeiten bei der Durchsetzung und zu einer möglichen Ausdehnung der Haftung führen. Eine mögliche Lösung wäre de lege ferenda, die DAO als Rechtssubjekt anzuerkennen.

[91] BÄRTSCHI, S. 17.
[92] FORRER et al., S. 24 f.
[93] RIVA, S. 60.
[94] BÄRTSCHI, S. 16.
[95] Stand 18.04.2022 um 17:42:56.
[96] »Your DAO guide - the most important DAO categories defining the space«, http://deepdao.io/organizations (Besucht am: 16.04.2022).
[97] BÄRTSCHI, S. 16 und 18.

Kapitel 5: Schlussfolgerung

Schon jetzt sind insgesamt fast 11 Milliarden US-$[1] in den *treasuries* der verschiedenen DAOs zusammengekommen und die Tendenz ist, auch aufgrund der Niedrigzinslage in der westlichen Welt, stark steigend. Es ist dennoch zu bedenken, dass es sich bei DAOs um eine relativ neue Technologie handelt - die Entwicklung und Einführung der ersten DAOs liegt noch nicht ein Jahrzehnt zurück - und daher sind Bugs und Probleme im Code immer noch vielzählig vorhanden. Bei solch einer hohen Investitionssumme trifft eine Sicherheitslücke oder ein Siphoning-Angriff eine Vielzahl von Investoren und der monetäre Schaden könnte schnell in die Millionen gehen. Dies wird in einer gewissen Weise auch dadurch verschlimmert, dass der Source Code einer DAO Open Source ist und damit für jeden öffentlich zugänglich ist. Damit können Hacker Sicherheitslücken im Code schnell finden und ausnutzen. Auch sind Features, wie zum Beispiel Flash Loans, die auf den ersten Blick nützlich erscheinen und dies im bugfreien Zustand auch sind, in einer sehr neuen Umgebung häufig mit *Exploits* verbunden. So werden in diesem Fall schon Gegenmaßnahmen entwickelt, wie zum Beispiel dass neu erworbene Tokens nicht direkt für Abstimmungen genutzt werden können, sondern eine festgelegt »*Cooldown*« Zeit besitzen sollen, um die Gefahr von »*Flash Loan Governance Attacks*« zu reduzieren.
Dass der Code Open Source ist, ist aber auch die größte Stärke von DAOs und der Blockchain Technologie allgemein. Wenn ein Entwicklerteam eine Lösung zu einem spezifischen Problem findet, können andere DAO-Entwickler schnell die Funktionsweise des neuen Codes betrachten und ihn in ihr Netzwerk implementieren, um die Sicherheitslücke zu schließen. Beispielsweise wurde dem Problem des»*Time Warp Exploit*«, welcher durch den weit verbreiteten »*Kimoto Gravity Well*« Algorithmus rentabel wurde, so entgegen gewirkt, indem das Dash Entwicklerteam eine verbesserte Version in Form des »*Dark Gravity Waves*« Algorithmus implementierte, welcher sich schnell auch im Source Code anderer DAOs wiederfinden ließ.
In Hinsicht auf »*Re-Entrancy Attacks*«, welchem zum Beispiel *The DAO* zum Opfer fiel, sind die Entwickler der Smart Contracts gefordert, da dieses Problem rein auf einem fehlerhaften Verhalten dieser basiert. So muss versichert werden, dass häufig benutzte features, wie der Bezug von Tokens oder Cryptocurrency im informatischen Sinne »*atomar*« erfolgt, sodass während der Ausgabe und der Aktualisierung des Kontostands keine weitere Funktion aufgerufen oder anderer nicht dazugehöriger Code ausgeführt werden kann.
Da am 21.04.2022 erste Diskussionen in der Europäischen Komission auftraten[2], ob ein Bann des »*Proof-of-Work*« Consensus Konzepts aufgrund umwelttechnischer Gründe möglich ist und ein Wechsel auf einen »*Proof-of-Stake*« Consensus Mechanismus vorgeschrieben wird, können vor allem DoS Angriffe zu einem größeren Problem werden. Da in einem »*Proof-of-Work*« Ansatz sehr viele verschiedene »*Miner*« an der Blockchain arbeiten, welche nicht der DAO angehören müssen, ist die Zahl dieser deutlich höher, was solch einen DoS Angriff undurchführbar macht. Durch einen »*Proof-of-*

[1] Your DAO guide - the most important DAO categories defining the space, http://deepdao.io/organizations (Besucht am: 16.04.2022).
[2] Jack Schickler - »Sweden, EU Discussed Bitcoin Proof-of-Work Ban: Report«, https://www.coindesk.com/policy/2022/04/21/sweden-eu-discussed-bitcoin-proof-of-work-ban-report/ (Besucht am: 21.04.2022)

Stake« Ansatz wird die Anzahl der Nodes die einen neuen Block generieren und validieren geringer, könnte dies einer DoS Attacke in die Hände spielen und somit einem Angreifer ermöglichen das gesamte Netzwerk lahmzulegen, wie es schon in 2016 im Ethereum Netzwerk der Fall war.[3] Dies muss auf jeden Fall beachtet werden, falls eine solche Einschränkung, wie sie nun von der Europäischen Regierung diskutiert wird, wirklich durchgesetzt werden.
Heutzutage sind DAOs noch sehr anfällig gegenüber Angriffen - seit Anfang 2020 gab es immerhin 86 Angriffe auf DeFi Institutionen mit einem Gesamtschaden von ungefähr 3.2 Milliarden US-$.[4] - und es wird sicherlich noch lange dauern bis jede Sicherheitslücke geschlossen wurde - wenn dies überhaupt jemals der Fall sein wird. Wie dem auch sei, werden die Algorithmen und Smart Contracts immer ausgefeilter und der Code wird angepasst, um »*Backdoors*« zu schließen, um die Sicherheit und Stabilität der DAO Netzwerke zu erhöhen.

Innovative Technologien, wie die DAOs, stellen eine grosse Herausforderung für die schweizerische Rechtsordnung dar. Aufgrund derer inhärenten Dezentralität stellen sich bereits hinsichtlich des anwendbaren Rechts grundlegende Fragen. Jedoch auch aus der Sicht des schweizerischen Privatrechts bringen die sog. *maverik-DAOs* den numerus clausus des Gesellschaftsrechts an seine Grenzen. Im Sinne einer Gesamtbetrachtung führt weder eine Qualifikation als Körperschaft noch als Personengesellschaft zu einem zufriedenstellenden Resultat. Während bei den Körperschaften insbesondere formelle Mängel (Statuten, HR-Eintrag, Organe) dagegensprechen, fehlt es für eine Qualifikation als Personengesellschaft am Rechtsbindungswillen der einzelnen DAO-Mitglieder. Trotz grosser Ähnlichkeit von Fundraising-DAOs mit kollektiven Kapitalanlagen fehlt es ihnen per Definition am Erfordernis der Fremdverwaltung. Auch im Vergleich zu sog. Investmentclubs entsprechen DAOs nicht der Zweckbeschreibung des »privaten Investmentfonds für Hobby-Börsianer«, wie der Investmentclub von der Lehre gerne umschrieben wird.[5] Eine Qualifikation der DAOs als Vertragsnetz zwischen den einzelnen DAO-Mitgliedern ist ebenfalls nicht zielführend. Anhand einer genaueren Betrachtung der verschiedenen Stakeholder wurden insb. Ähnlichkeiten zu bestehenden Strukturen von Körperschaften festgehalten. Neben einem Recht zur Mitsprache werden den Investoren bzw. DAO-Mitgliedern vermehrt weitere Rechte gewährt, welche Gemeinsamkeiten zu Dividendenausschüttungen und Bezugsrechten aufweisen. Zuletzt wurden die möglichen Haftungsansprüche gegen die DAOs als solche sowie jene gegen die einzelnen Beteiligten analysiert. Während die Haftung der DAO als solche an mangelnder Rechtspersönlichkeit scheitert, führt auch eine analoge Anwendung der Regeln der einfachen Gesellschaften zu weiteren offenen Fragen. Eine diesbezüglich mögliche Lösung wäre de lege ferenda, die DAO als Rechtssubjekt anzuerkennen. Ob dies die Lücke zwischen Technologie und Recht zu schliessen vermag, bleibt bis auf Weiteres offen.

[3] Alyssa Hertig - »So, Ethereum's Blockchain is Still Under Attack...«, https://www.coindesk.com/markets/2016/10/06/so-ethereums-blockchain-is-still-under-attack/ (Besucht am: 14.04.2022)
[4] https://cryptosec.info/defi-hacks/ (Besucht am: 22. April 2022)
[5] BSK-KAG PFENNINGER / NÜESCH, N 18; GYR, Rz. 47.

Bibliography

[BitFor] BITCOIN FORUM: *"Forum about Timewarp Exploit in Kimoto Gravity Well"*. URL: https://bitcointalk.org/index.php?topic=552895 (BESUCHT AM: 14. 04. 2022)

[CS22] CRYPTOPEDIA STAFF: *"What Was The DAO?"* URL: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao (BESUCHT AM: 14. 04. 2022)

[DashDocs] DASH DORE GROUP INC.: *"Dash Documentation"*. URL: https://docs.dash.org/ (BESUCHT AM: 15. 03. 2022)

[DM22] DEER MARCEL: *"What are flash loans in DeFi?"* URL: https://cointelegraph.com/explained/what-are-flash-loans-in-defi (BESUCHT AM: 14. 04. 2022)

[DoDAOJB] DODAO.IO: *"Juicebox"*. URL: https://www.dodao.io/dao-frameworks/juicebox (BESUCHT AM: 30. 03. 2022)

[EthDocs] ETHEREUM: *"Ethereum Docs"*. URL: https://ethereum.org/en/developers/docs/ (BESUCHT AM: 30. 03. 2022)

[FM22] FOX MATTHEW: *"Tokens of the defunct DAO that failed to buy a copy of the constitution are worth $300 million even after disbanding"*. URL: https://news.yahoo.com/tokens-defunct-dao-failed-buy-171014991.html (BESUCHT AM: 14. 04. 2022)

[FW20] FOXLEY WILLIAM: *"'Flash Loans' Have Made Their Way to Manipulating Protocol Elections"*. URL: https://www.coindesk.com/tech/2020/10/29/flash-loans-have-made-their-way-to-manipulating-protocol-elections/ (BESUCHT AM: 14. 04. 2022)

[HA22] HAYES ADAM: *"What Is a Blockchain?"* URL: https://www.investopedia.com/terms/b/blockchain.asp (BESUCHT AM: 27. 03. 2022)

[HA16] HERTIG ALYSSA: *"So, Ethereum's Blockchain is Still Under Attack..."* URL: https://www.coindesk.com/markets/2016/10/06/so-ethereums-blockchain-is-still-under-attack/ (BESUCHT AM: 14. 04. 2022)

[IBMSmartCon] IBM: *"Smart contracts defined"*. URL: https://www.ibm.com/topics/smart-contracts#:~:text=Smart%20contracts%20are%20simply%20programs,intermediary's%20involvement%20or%20time%20loss. (BESUCHT AM: 10. 04. 2022)

[JuiceBoxDoc] JUICEBOX: *"Juicebox Documentation"*. URL: https://docs.juicebox.money/protocol/protocol (BESUCHT AM: 30. 03. 2022)

[KJ21] KASTRENAKES JACOB: *"Almost buying a copy of the Constitution is easy, but giving the money back is hard"*. URL: https://www.theverge.com/2021/11/24/22800995/constitutiondao-refund-progress-steep-gas-fees-cryptocurrency (BESUCHT AM: 14. 04. 2022)

[MS21] MALWA SHAURYA: *"DeFi 'Rug Pull' Scams Pulled In $2.8B This Year: Chainalysis"*. URL: https://www.coindesk.com/markets/2021/12/17/defi-rug-pull-scams-pulled-in-28b-this-year-chainalysis/ (BESUCHT AM: 14. 04. 2022)

[NB22] NEWAR BRIAN: *"Beanstalk Farms loses $182M in DeFi governance exploit"*. URL: https://cointelegraph.com/news/beanstalk-farms-loses-182m-in-defi-governance-exploit (BESUCHT AM: 20. 04. 2022)

[PN21] PATEL NILAY: *"From a meme to $47 million: ConstitutionDAO, crypto, and the future of crowdfunding"*. URL: https://www.theverge.com/22820563/constitution-meme-47-million-crypto-crowdfunding-blockchain-ethereum-constitution (BESUCHT AM: 10. 04. 2022)

[PM19] PORTA MICHELE: *"Timewarp Attack: how to reduce the mining difficulty"*. URL: https://en.cryptonomist.ch/2019/05/20/timewarp-attack-mining-difficulty/ (BESUCHT AM: 14. 04. 2022)

[QL19] QUANTSTAMP LABS: *"What is a Re-Entrancy Attack?"* URL: https://quantstamp.com/blog/what-is-a-re-entrancy-attack (BESUCHT AM: 14. 04. 2022)

[RE21] ROSENBERG ERIC: *"What is a Consensus Mechanism?"* URL: https://www.thebalance.com/what-is-a-consensus-mechanism-5211399 (BESUCHT AM: 27. 03. 2022)

[SJ22] SCHICKLER JACK: *"Sweden, EU Discussed Bitcoin Proof-of-Work Ban: Report"*. URL: https://www.coindesk.com/policy/2022/04/21/sweden-eu-discussed-bitcoin-proof-of-work-ban-report/ (BESUCHT AM: 21. 04. 2022)

[SN18] SZABO NICK: *"Unenumerated - An unending variety of topics"*. URL: https://unenumerated.blogspot.com/ (BESUCHT AM: 10. 04. 2022)

[WikiASIC] WIKIPEDIA: *"Application-specific integrated circuit"*. URL: https://en.wikipedia.org/wiki/Application-specific_integrated_circuit (BESUCHT AM: 27. 03. 2022)

Selbstständigkeitserklärung

»*Ich erkläre hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Alle Stellen, die wörtlich oder sinngemäss aus Quellen entnommen wurden, habe ich als solche gekennzeichnet. Mir ist bekannt, dass andernfalls die Arbeit mit der Note 1 bewertet wird und der Senat gemäss Artikel 36 Absatz 1 Buchstabe r des Gesetzes über die Universität vom 5. September 1996 und Artikel 69 des Statuts der Universität Bern vom 7. Juni 2011 zum Entzug des aufgrund dieser Arbeit verliehenen Titels berechtigt ist. Für die Zwecke der Begutachtung und der Überprüfung der Einhaltung der Selbständigkeitserklärung bzw. der Reglemente betreffend Plagiate erteile ich der Universität Bern das Recht, die dazu erforderlichen Personendaten zu bearbeiten und Nutzungshandlungen vorzunehmen, insbesondere die schriftliche Arbeit zu vervielfältigen und dauerhaft in einer Datenbank zu speichern sowie diese zur Überprüfung von Arbeiten Dritter zu verwenden oder hierzu zur Verfügung zu stellen.*«

[Fassung vom 22.5.2014]

Datum: 22. April 2022 Unterschrift: 

Miro Schüpbach

Datum: 22. April 2022 Unterschrift: 

Marcel Zauder