Miro SCHÜPBACH 17-109-851
Marcel ZAUDER 16-124-836

1 Dezentralisierte Autonome Organisation - Definition

- Smart Contracts definieren die Regeln und die Operationen einer DAO
- Entscheidungsgewalt ist über alle Mitglieder verteilt
- Alle Transaktionen werden auf Blockchain festgehalten; Source Code und Blockchain ist Open Source
- **Protokoll-DAOs** kümmern sich um die Governance eines Protokolls, wie z.B. Aave (Kredit-Protokoll), Uniswap (DEX) oder MakerDAO (Stablecoin).
- In **Dienstleistungs-DAOs** finden sich Serviceanbieter und Nutzer zusammen, um verschiedene Dienstleistungen anzubieten und zu nutzen, beispielsweise Gitcoin.
- **Fundraising-DAOs** haben das Ziel ein gemeinschaftlichen Kapitals anzusammeln, um ein gemeinsames Ziel zu erreichen, z.B. ConstitutionDAO oder PleasrDAO.

2 Computerscience Teil

2.1 Dash DAO (DASH Blockchain)

- Users with at least 1000 DASH (≈ 80.000 US-$, May 2022) can establish Masternodes
- Masternodes enable different features (i.e. InstantSend, CoinJoin, ChainLocks etc.)
- Uses Proof-of-Work consensus by solving »X-11«-hash function
- Not everything of the mining reward goes to the miners:
  - 10% for Decentralized Governance Budget
  - 90% for miners and masternode owners (masternode owners get 60% of this reward in 2025)
- Only masternode owners can vote in proposals

2.2 ConstitutionDAO (Ethereum Blockchain - Juicebox Framwork)

- Uses Proof-of-Work consensus; Ethereum network plans to switch to Proof-of-Stake approach
- Donated money is stored in a multi-signature wallet
- Juicebox DAO have a funding goal and period → overflow is collected in separate treasury pool which can be accessed by the members by »burning« their tokens
- Voting rights are distributed across all members proportionally to the number of tokens they hold

2.3 Vulnerabilities and Potential Attack Opportunities

- 10.9 billion US-$ distributed across all DAOs
- 86 DAO attacks since January 2020 lead to a loss of 3.2 billion US-$
- **TheDAO Hack (2016)** – approx. 60 million US-$ siphoned; lead to hardfork of Ethereum blockchain
- **Ronin Network Attack (29. March 2022)** – 625 million US-$ lost
- **Beanstalk Farms (18. April 2022)** – 182 million US-$ lost

2.3.1 Reentrancy Exploits (TheDAO Hack)

- During execution the execution itself is interrupted, initiated, and both execution parts are terminating
- In TheDAO Hack example:
  - After the Ether was transferred a Fallback-Function is called
  - Initialized another withdrawal of same account
  - As balance was not yet updated, the same amount could be withdrawn several times

2.3.2 Rug Pulls

- If the private key for treasury/liquidity pool was not burned owner still has complete access over it
- After enough money was gathered the DAO's owner can transfer all the money to his wallet and »run«
- In Juicebox it is also possible to set the reconfiguration strategy to none → changes to settings of the DAO take effect immediately
- In 2021 over 2.8 billion US-$ were lost this way

2.3.3 Flash Loan (Governance) Attacks

- Flash loans are taken within the execution of a smart contract and must be paid back in full (plus interest) before the SC's termination
- Was commonly used to exploit differences in price between two exchange portals
- As tokens are most often proportionally to votes, one can use the flash loan in order to vote in proposals (**Flash Loan Governance Attack**)

2.3.4 Other Common Attacks

- If someone gathers hash power of over **51%** of the whole DAO, they would have full control over the blockchain.
- Wrong timestamped blocks can lead the blockchain to think that current mining processes take longer → decreases difficulty, and subsequent block mining becomes easier. (**Time Warp Exploit**)
- Ethereum was the target of a **DoS Attack** in 2016 → transactions took a lot of time to verify. Especially DAOs that use »*validation nodes*« (like Dash's Masternodes) are susceptible for this.

3 Juristischer Teil

DAOs können in *top-* und *ground-layer* DAOs eingeteilt werden. *Ground-layer* DAOs sind ganze Blockchains wie Ethereum oder Bitcoin. Die *top-layer* basieren auf einer *ground-layer* DAO und bedienen sich derer Infrastruktur, indem sie Smart Contracts auf der Blockchain ablegen.

3.1 DAOs im Gesellschaftsrecht

Aufgrund des numerus clausus des schweizerischen Gesellschaftsrechts müssten DAOs entweder als Personengesellschaft oder als Körperschaft qualifiziert werden.

Körperschaft

Für eine Qualifikation als Körperschaft spricht die unbegrenzte Mitgliederzahl, die fehlenden Treuepflichten sowie dass grundsätzlich die Stimmkraft dem eingebrachten Kapital entspricht. Dagegen sprechen mögliche Organisationsmängel sowie das Fehlen von Statuten und HR-Eintrag.

Personengesellschaft

Sowohl die grosse Gestaltungsfreiheit bezüglich der vertraglichen Grundlage als auch das Prinzip der Selbstorganschaft deuten auf eine Qualifikation als Personengesellschaft hin. Dagegen spricht die persönliche Beziehung und die weitgehenden Treuepflichten der Gesellschafter.

3.2 DAOs als einfache Gesellschaft

Es ist durchaus vertretbar, dass eine vertragsmässige Verbindung von mehreren Personen, die sich gemeinsamen Mittel bedienen, vorliegt. Da das Bewusstsein der Qualifikation als eG nicht erforderlich ist, müsste jedoch ein Wille zur gemeinsamen Zweckverfolgung gegeben sein. Gerade dieser Rechtsbindungswille ist u.E. jedoch bei DAOs nicht vorhanden.

3.3 DAOs als kollektive Kapitalanlage

Eine kollektive Kapitalanlage ist ein Vermögen, das durch die Anleger zur kollektiven Kapitalanlage aufgebracht und in Fremdverwaltung für deren Rechnung verwaltet werden, wobei die Anlegerinteressen gleichmässig befriedigt werden. DAOs erfüllen drei dieser vier Kriterien. Diese Qualifikation scheitert an dem Kriterium der Selbstverwaltung, da DAOs definitionsgemäss selbstverwaltet sind und die Mitwirkung der Anlegerinnen und Anleger im Zentrum steht.

3.4 Stakeholder einer DAO

Die Stakeholder einer DAO sind grundsätzlich in Entwickler, Benutzer, DAO Mitglieder und möglicherweise Delegates einzuteilen. Zentral sind dabei die DAO Mitglieder, da diese das entscheidungsbefugte Organ einer DAO sind.

3.5 Ansprüche der Investoren

Die DAO Token vermitteln den DAO Mitglieder primär Stimmrechte. Verschiedene DAOs experimentieren ebenfalls mit Mechanismen welche Dividendenausschüttungen oder Bezugsrechten ähneln. Ebenfalls gibt es DAOs die Rückerstattungsrechte garantieren.

3.6 Haftung von DAOs

Haftung der DAO als solche

Da es der DAO an einer eigenen Rechtspersönlichkeit mangelt, ist eine Haftung der DAO als solche de lege lata nicht möglich.

Haftung der DAO Mitglieder

Wird die DAO als einfache Gesellschaft qualifiziert, würde dies zu einer solidarischen, persönlichen und unbeschränkten Haftung der einzelnen Mitglieder führen. Fehlt es an einem Rechtsbindungswillen, schlagen gewisse Autorinnen und Autoren vor, die Regeln der einfachen Gesellschaft analog anzuwenden. U.E. ist dies nicht zielführend, insbesondere da es sich bereits um einen Auffangstatbestand handelt und sich Probleme bei der Durchsetzbarkeit stellen würden.

Haftung de lege ferenda

De lege ferenda wäre es wünschenswert, den DAOs eine eigene Rechtspersönlichkeit zu gewähren und das Betriebsrisiko auf die DAO als solche zu überwälzen. Dies könnte mit gewissen Eigenkapital- und Auditvorschriften kombiniert werden.