

Trends in der Krypto-Ökonomie

Non-Fungible Tokens und Dezentralisierte Autonome Organisationen

Autoren: Dr. Lukas Wiewiorra
Dr. Niklas Fourberg

Impressum

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik.org
www.wik.org

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin und Direktorin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzender des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7225
Steuer-Nr.	222/5751/0722
Umsatzsteueridentifikations-Nr.	DE 123 383 795

Inhaltsverzeichnis

1 Einleitung	1
1.1 Blockchain & Bitcoin	1
1.2 Smart Contracts	2
1.3 Dezentralisierte Applikationen und Autonome Organisationen	4
1.4 Non-fungible Tokens	5
1.5 Dezentralisiertes und Zentralisiertes Finanzwesen	5
1.6 Web3	6
1.7 Kritik	6
2 Entwicklung der Krypto-Ökonomie	8
2.1 Marktentwicklung und Volatilität	8
2.2 Die Krypto-Krise in 2022	11
2.3 Regulierung der Krypto-Ökonomie	13
3 Non-fungible Tokens (NFT)	17
3.1 Technische Umsetzung	17
3.2 Marktentwicklung	18
3.3 Herausforderungen und Potenziale	20
4 Dezentralisierte Autonome Organisationen (DAO)	22
4.1 Abgrenzungsversuch und Definition	22
4.2 Ziele von DAOs	23
4.3 Herausforderungen und Potenziale	24
5 Schlussfolgerungen & Ausblick	26
Literaturverzeichnis	27

1 Einleitung

Der Markt für Krypto-Produkte wird aktuell auf ein Volumen von über 2,5 Milliarden EUR geschätzt und zählt mittlerweile mehr als 12.000 Krypto-Projekte weltweit.¹ Seit der Veröffentlichung von Bitcoin im Januar 2009 durch einen (oder mehrere) Entwickler unter dem Pseudonym „Satoshi Nakamoto“, wurden eine Vielzahl weiterer Krypto-Währungen (sog. „Altcoins“ bzw. Alternativkryptowährungen zum Bitcoin) veröffentlicht. Als sogenannte „Stablecoins“ werden dabei Kryptowährungen bezeichnet, deren Preise an die Kurse von Fiatwährungen gekoppelt sind. Diese Kopplung wird durch (teilweise automatisierte) Preisbindungsmechanismen an einen Währungskorb oder andere Vermögenswerte erzielt. Daneben existieren auch sogenannte „Meme-Münzen“ die aus verschiedenen Gründen Bekanntheit unter Internetnutzern erlangt haben. Da ihr Wert aber fast ausschließlich von ihrer Popularität abhängt, sind Meme-Münzen spekulative und meist sehr volatile Kryptowährungen. Einige Beispiele für Meme-Münzen sind Dogecoin (DOGE) und Shiba Inu (SHIB).² Krypto-Währungen verwenden eine dezentralisierte Architektur auf Grundlage einer „Distributed-Ledger-Technologie“ (DLT) mit Tausenden von verteilten Knoten und einem Konsensmechanismus. In diesem digitalen dezentralen Transaktionsverzeichnis wird jede Transaktion aufgezeichnet, die jemals in einem spezifischen Netzwerk getätigt wurde.

1.1 Blockchain & Bitcoin

Das Bitcoin-Netzwerk zeichnet Transaktionen in Blöcken auf, versieht sie mit einem Zeitstempel, und verschlüsselt („hasht“) sie in einer fortlaufenden Kette. Dabei wird ein „Hash“ aus dem vorherigen Block (und damit implizit auch aus allen vorherigen Blöcken) generiert. Diese Kette aus miteinander verknüpften Blöcken wird Blockchain genannt. Eine Vielzahl von sogenannten Knoten im Bitcoin-Netzwerk halten dabei eine lokale Replik der Blockchain vor, validieren neue Transaktionen im Netzwerk und leiten diese an andere Knoten weiter. Dabei ist die Technologie für jeden zugänglich und jeder kann ohne Genehmigung am Netz teilnehmen und einen Knoten betreiben. Diese im gesamten Netz propagierten und validierten Transaktionen sind allerdings zunächst in einem Wartezustand, da die Blockchain nicht geändert werden kann ohne den festgelegten Konsensmechanismus zu erfüllen. Im Falle des Bitcoin-Netzwerkes ist dafür ein sogenannter „Proof-of-Work“ (Arbeitsnachweis) durch spezialisierte Netzwerkknoten, sogenannte Miner, zu erbringen. Dieser Nachweis erfolgt prinzipiell nach dem Konzept „eine CPU - eine Stimme“ (Nakamoto, 2008). Dabei beweisen Miner, dass sie Kapital riskieren, indem sie geeignete Hardware erwerben und Energie (d. h. Stromkosten) für das Mining aufwenden. Dabei ist der Proof-of-Work, den Miner erbringen, nicht mit der Lösung eines komplexen mathematischen Problems, sondern eher mit einem „Brute-Force“-Ansatz zu vergleichen. Miner erstellen in schneller Abfolge potenzielle Blöcke aus Transaktionen im Wartezustand und einem zusätzlichen Wert, welcher „Nonce“ (Number used once) genannt wird. Diese potenziellen Blöcke werden als Input für eine SHA256-Hash-Funktion verwendet. Die Ausgabe dieser Funktion ist ein Hash, welcher von spezialisierter Hardware in wenigen Millisekunden berechnet werden kann. Allerdings gibt es für den Hashwert eine Schwierigkeitsvorgabe, die sich durch eine bestimmte Anzahl von Nullen zu Beginn des Hashes, also eine Größe welche es zu unterbieten gilt, ausdrückt. Die Miner müssen daher den Nonce finden, welcher zusammen mit den Daten der wartenden Transaktionen im potenziellen Block einen Hash ergibt, der den aktuellen Schwierigkeitsgrad unterbietet. Um den richtigen Nonce zu finden, versucht die Mining-Hardware so lange durch Trial-and-Error verschiedene Zahlen als Nonce zu verwenden, bis eine Zahl gefunden ist, mit der ein Hash generiert werden kann, der der aktuellen Schwierigkeitsvorgabe entspricht. Dann kann erfolgreich ein neuer Block der Blockchain hinzugefügt werden und der Miner wird mit der aktuell

¹ <https://www.rolandberger.com/en/Insights/Publications/The-rise-of-the-Crypto-Economy.html>

² <https://bitpay.com/blog/guide-to-altcoins/>

geltenden Anzahl Bitcoin für einen neuen Block (zzgl. im Block enthaltener Transaktionsgebühren) belohnt. Die in einem neuen Block enthaltenen Transaktionen gelten damit als bestätigt bzw. verifiziert und sind nicht länger im Wartezustand. Die Belohnung schafft den Anreiz zum Mining und sorgt damit für den Aufbau der Netzwerk-Infrastruktur und den Betrieb des Netzwerks. Der Schwierigkeitsgrad des Bitcoin-Netzwerkes wird dabei so austariert, dass im Schnitt alle 10 Minuten ein neuer Block akzeptiert werden kann. Das bedeutet, Miner stehen in einem Wettbewerb um wartende Transaktionen in neuen Blöcken zu bestätigen. Daher stellt das schnellere Berechnen von Hashes einen Wettbewerbsvorteil dar. Um das Risiko durch teure Hardwareinvestitionen zu senken sind viele Miner daher in Pools organisiert, bei dem Rechenkapazitäten kombiniert werden.

Die Mehrheitsentscheidung in der Blockchain wird prinzipiell durch die längste Kette repräsentiert, in die der größte Proof-of-Work-Aufwand investiert wurde. Um einen bestehenden Block zu modifizieren, müsste ein Angreifer den Proof-of-Work für den betreffenden zu ändernden Block und alle nachfolgenden Blöcke neu erbringen und den Arbeitsnachweis „ehrlicher“ Knoten im Netzwerk übertreffen. Die Wahrscheinlichkeit dafür ist (insbesondere für älter werdende Einträge) verschwindend gering. Im Gegensatz dazu muss bei dem „Proof-of-Stake“ Ansatz Kapital in Form der Kryptowährung hinterlegt werden, welches als Sicherheit dient und vernichtet werden kann, wenn sich ein sogenannter „Validierer“ unehrlich oder unzuverlässig verhält. Das Konzept von Proof-of-Stake ist allerdings noch sehr jung. Insbesondere da keine rechenintensiven Operationen ausgeführt werden müssen um neue Blöcke zu erzeugen und Validatoren an erfolgreichen Validierungen verdienen, kann beispielsweise der Anreiz bestehen bei mehreren konkurrierenden Zweigen einer Blockchain auf allen Zweigen Blöcke erzeugen zu wollen. Dieses sogenannte „nothing-at-stake“ Problem kann daher die Stabilität des Systems gefährden. Theoretisch sind auch andere denkbare Angriffsszenarien möglich und die Branche verfeinert und entwickelt diesen Ansatz ständig auf unterschiedliche Arten und Weisen weiter. Vor Kurzem hat Ethereum sein Blockchain-Netzwerk erfolgreich vom Proof-of-Work-Ansatz auf den Proof-of-Stake-Ansatz umgestellt. Bisher ist das Netzwerk stabil und die Umstellung scheint erfolgreich verlaufen zu sein. Da Proof-of-Stake nicht auf eine hohe Rechenleistung angewiesen ist, hat es erhebliche Vorteile im Gegensatz zum Proof-of-Work-Ansatz im Hinblick auf den globalen Stromverbrauch und damit die Auswirkungen des Betriebs eines Blockchain-Netzwerks auf die Umwelt.

Allerdings muss ein Blockchain-Netzwerk nicht notwendigerweise immer öffentlich sein. Auch private Netzwerke, die nur mit Genehmigung genutzt werden können sind möglich. Da es sich um ähnliche Konzepte handelt, werden die Begriffe "privat" und "mit Genehmigung" sowie "öffentlich" und "ohne Genehmigung" in der Kryptowährungsbranche oft synonym verwendet. Im Allgemeinen sind zwar genehmigungsfreie Blockchains öffentlich (offener Lese- und Schreibzugriff), und private Blockchains bedürfen einer Genehmigung (geschlossener Lese- und Schreibzugriff). Allerdings sind nicht alle öffentlichen Blockchains genehmigungsfrei, da es öffentliche DLT-Netzwerke gibt, die es jedem erlauben, Daten in der Blockchain zu prüfen, die aber den Zugang zur Validierung von Blöcken einschränken.³

1.2 Smart Contracts

Mit dieser grundlegenden Architektur lassen sich in bestimmten Blockchains (z. B. Ethereum) aber auch vollständige Finanzinstrumente mittels sogenannter „Smart Contracts“⁴ abbilden. Diese intelligenten Verträge sind Programme, die automatisiert Aktionen ausführen, wenn bestimmte Bedingungen erfüllt

³ <https://polymesh.network/blog/public-permissioned-bridging-the-best-of-both-worlds>

⁴ <https://ethereum.org/de/developers/docs/smart-contracts/>

sind. Die Fähigkeit Smart Contracts in einer Blockchain abbilden zu können bildet dabei das Fundament für weiterführende Produkte und Organisationsformen, die in diesem Kurzbericht vorgestellt werden.

Die Idee von Smart Contracts geht auf Nick Szabo zurück, welcher bereits 1996 die konzeptionelle Grundlage für das Konzept verschriftlicht hat (Szabo, 1996). Bereits in dieser Arbeit wird die Vision von „Smart Properties“ umrissen, bei denen Smart Contracts mit physischen Gütern verknüpft werden. Szabo beschreibt dabei das Beispiel eines Autos, welches auf Raten erworben wurde und im Fall nicht bezahlter Raten automatisch die Rechte am Zugang zum Auto (z. B. digitale Schlüssel) an die Bank übergibt. Aktuelle Beispiele aus der Autoindustrie zeigen, dass Szabos Überlegungen durch existierende Krypto-Produkte in der Autoindustrie bereits teilweise umgesetzt werden.

Alfa Romeo verwendet beispielsweise NFTs (non-fungible tokens, s. Abschnitt 1.4) als Nachweis für den Wartungszustand eines Fahrzeugs. Der Elektro-Hybrid-SUV Tonale ist das erste Auto in der Branche, das mit einem digitalen NFT-Zertifikat ausgestattet ist. Nach Angaben des Unternehmens werden mit Zustimmung des Kunden Fahrzeugdaten aufgezeichnet, die als unveränderlicher Nachweis für den Wartungsstatus des Fahrzeugs in der Blockchain gespeichert werden sollen. So können Käufer auf dem Gebrauchtwagenmarkt z. B. sicher erfahren, ob das Auto gut gewartet ist, bevor sie ihre Kaufentscheidung treffen.⁵

Technisch setzt die Umsetzung intelligenter Verträge „Turing-Vollständigkeit“ und „Statefulness“ voraus, was zum Beispiel von Ethereum mit der Programmiersprache „Solidity“ erfüllt wird. Im Prinzip bedeutet Turing-Vollständigkeit, dass ein System oder Programmiersprache einen Computer simulieren kann und mit genug Ressourcen jeden denkbaren Algorithmus ausführen kann. Statefulness bezeichnet die Fähigkeit eines Systems sich an Zustände auf dem Blockchainlevel zu erinnern. Solidity ist eine objektorientierte Programmiersprache zum Entwickeln von Smart Contracts für Blockchain-Plattformen wie Ethereum oder Tron.⁶ Aber auch eine Reihe anderer Blockchain-Projekte ermöglichen Smart Contracts (z.B. „Diem DLT“ mit der Sprache „Move“). Das Bitcoin-Netzwerk erfüllt diese Kriterien allerdings nicht und kann daher keine Smart Contracts und daher auch keine der im Folgenden beschriebenen darauf aufbauenden Produkte und Organisationsformen abbilden.

Um Abläufe basierend auf Smart Contracts realisieren zu können gibt es verschiedene spezialisierte Formen von Token, die sich in zwei funktionale Gruppen gliedern lassen, welche sich überschneiden können, sogenannte „Utility Token“ und „Governance Token“.

Utility Token erlauben es den Inhabern Zugang zu Dienstleistungen oder ausgewählten Funktionen in einem Blockchainnetzwerk zu erhalten. Da alle Aktionen auf der Blockchain Aufwand für das Netzwerk erzeugen und dieser Aufwand dezentral von Teilnehmern des Netzwerk erbracht werden muss, müssen Transaktionen mit sogenanntem **Gas** bzw. Transaktionsgebühren bezahlt werden. **Gaspreise** fallen mit höherem Aufwand und kürzerer Fristigkeit von Transaktionen höher aus. Mit diesen Tokens können daher Belohnungen ausgezahlt werden, Dienstleistungen erworben werden oder Netzwerkgebühren beglichen werden. Einige Beispiele für Utility Token sind ether (ETH), Basic Attention Token (BAT) und Funfair (FUN). **Governance Token** erfüllen eine vergleichbare Funktion, geben Inhabern aber das spezifische Recht, Vorschläge oder Änderungswünsche im Blockchainnetzwerk zu erstellen und darüber

⁵ <https://www.jumpstartmag.com/what-are-the-latest-nfts-in-the-car-industry/>

⁶ <https://de.wikipedia.org/wiki/Solidity>

abzustimmen. Beispiele für Governance Token sind z. B. Maker (MKR) und der Uniswap-Protokoll-Token (UNI).⁷

1.3 Dezentralisierte Applikationen und Autonome Organisationen

Mit der Möglichkeit Wert über Krypto-Tokens zu allokalieren und der Fähigkeit Regeln über Smart Contracts zu automatisieren, lassen sich „Dezentralisierte Applikationen“ (DApps) abbilden. Johnston et al. (2014) schlagen eine Klassifizierung vor, nach der sie folgende Typen von Dapps unterscheiden:

- **Dezentralisierte Applikationen des Typ I** haben eine eigene Blockchain. (z. B. Bitcoin, Litecoin)
- **Dezentralisierte Applikationen des Typs II** nutzen die Blockchain einer dezentralisierten Anwendung des Typs I. Dezentrale Anwendungen vom Typ II sind Protokolle und haben Token, die für ihre Funktion notwendig sind. (z. B. Omni)
- **Dezentrale Applikationen des Typ III** verwenden das Protokoll einer dezentralisierten Anwendung vom Typ II. Dezentralisierte Anwendungen vom Typ III sind Protokolle und haben Token, die für ihre Funktion notwendig sind (z. B. das SAFE-Netzwerk, welches das Omni-Protokoll verwendet um "Safecoins" auszugeben, die zum Erwerb von verteiltem Dateispeicher verwendet werden können)

Johnston et al. (2014) erläutern diese Klassifizierung anhand einer hilfreichen Analogie: „Eine Dapp des Typs I ist vergleichbar mit einem Computerbetriebssystem (wie Windows, Mac OS X, Linux, Android, iOS), eine Dapp des Typs II ist vergleichbar mit einem allgemeinen Softwareprogramm (wie ein Textverarbeitungsprogramm, eine Tabellenkalkulationssoftware, ein Dateisynchronisationssystem wie Dropbox) und eine Dapp des Typs III ist vergleichbar mit einer spezialisierten Softwarelösung (wie ein Tool zum Zusammenführen von E-Mails, das ein Textverarbeitungsprogramm verwendet oder ein Makro für die Kostenabrechnung, das eine Tabellenkalkulation verwendet).

Mit diesen Werkzeugen können ebenfalls neue virtuelle Organisationsformen umgesetzt werden, sogenannte Dezentralisierter Autonome Organisationen (DAO). Das Konzept wurde ursprünglich unter dem Begriff Dezentralisierter Autonome Corporation (DAC) in einem Beitrag von Daniel Larimer⁸ zum Thema Sicherheit in blockchainbasierten Systemen angedacht. Der Autor beschreibt das Konzept in diesem Kontext folgendermaßen:

“Think of a crypto-currency as shares in a Decentralized Autonomous Corporation (DAC) where the source code defines the bylaws. The goal of the DAC is to earn a profit for the shareholders by performing valuable services for the free market. With this goal in mind set out to maximize shareholder value at every stage as you design the bylaws that govern operation of the DAC. [...] The goal of a for-profit DAC is to maximize value and minimize costs. In this case, we only want the DAC to pay for useful security, but no more than necessary to maximize shareholder value.”

Bei einer DAO werden die Regeln und Ziele einer Organisation in Form von Smart Contracts in der Blockchain hinterlegt. Vitalik Buterin, Mitbegründer und Erfinder von Ethereum, geht davon aus, dass eine DAO nach dem Start ohne menschliche Intervention eines Managers funktionieren könne (Buterin,

⁷ <https://bitpay.com/blog/guide-to-altcoins/>

⁸ <https://letstalkbitcoin.com/is-bitcoin-overpaying-for-false-security>

2014). Änderungen an diesem Set aus Regeln können nur durch Abstimmung der Mitglieder einer DAO erfolgen. Das Stimmgewicht der Mitglieder einer DAO bemisst sich dabei in der Regel an der Anzahl der Token, die ein Teilnehmer hält. Diese Entscheidungen können damit die weitere Entwicklung und Ausrichtung eines Projekts oder die Ziele einer dezentralen autonomen Organisation bestimmen. Mittlerweile haben sich eine Vielzahl von DAOs mit unterschiedlichen Zielen, Absichten und Regelwerken gebildet, welche im Rahmen dieser Kurzstudie in Kapitel 4 näher erläutert werden.

1.4 Non-fungible Tokens

Daneben haben in der Krypto-Ökonomie sogenannte Non-fungible Tokens (NFT) stark an Popularität gewonnen. NFTs sind einmalige digitale Eigentumsnachweise, welche in einer Blockchain gespeichert werden. NFTs haben in den letzten Jahren insbesondere durch kreative Anwendungsszenarien (z. B. digitale Kunst) stark an Bedeutung gewonnen und der Markt für NFTs wächst seit 2021 rasant. Viele bekannte Marken und klassische Unternehmen strömen in den Markt und versuchen dort durch den Vertrieb von Sammlerobjekten und gestützt von ihrer Position im allgemeinen Markenbewusstsein Fuß zu fassen. Allerdings werden NFTs auch kritisch beobachtet, da rechtliche Fragen im Hinblick auf die tatsächlichen Eigentumsverhältnisse der Bezugsgüter (z. B. Bilder, Bücher Videos) immer noch mit Unsicherheiten behaftet sind.

1.5 Dezentralisiertes und Zentralisiertes Finanzwesen

Mittlerweile bieten eine Vielzahl von Plattformen und Applikationen Krypto-Finanzprodukte und -dienstleistungen an, mit deren Hilfe es möglich ist, innerhalb von Minuten Krypto-Vermögenswerte zu verleihen, zu leihen, zu handeln und zu kaufen, ohne eine Genehmigung von zentralen Behörden einholen zu müssen. Dabei wird zwischen Dezentralisiertem Finanzwesen (DeFi) und zentralisiertem Finanzwesen (CeFi) unterschieden. DeFi bezeichnet den Handel mit Vermögenswerten auf Grundlage der Blockchain und die Umsetzung von Finanzinstrumenten mittels sogenannter „Smart Contracts“. Eine Reihe von DeFi-Plattformen bieten mittlerweile auch NFT-Darlehen an. In einigen Fällen können NFT-Besitzer die Kredite nutzen, um Kryptowährungen oder Fiat-Währung gegen ihre NFTs einzutauschen. CeFi bezeichnet den Handel mit Kryptowährungen und -gütern (z. B. NFTs) über zentralisierte private Akteure, welche z. B. Krypto-Börsen und -Plattformen betreiben. Im Gegensatz zu DeFi werden durch CeFi-Akteure die Regeln einer Plattform nicht mittels Smart Contracts festgelegt, sind daher auch nicht über die Blockchain transparent nachvollziehbar und können beispielsweise durch den Plattformbetreiber einseitig verändert werden. Die folgende Tabelle verdeutlicht diesen Zusammenhang im Vergleich zur klassischen Finanzindustrie (TradFi).

Tabelle 1–1: DeFi, CeFi und TradFi – Beispielunternehmen

Funktion	DeFi	CeFi	TradFi
Spot trade	Uniswap, Curve	Coinbase, Kraken	New York Stock Exchange, NASDAQ
Handel mit Derivaten	dYdX, GMX	Bybit, FTX	Chicago Mercantile Exchange
Verwaltung von Vermögenswerten	The Index Co-op, Yearn	Galaxy, Grayscale Bitcoin Trust	BlackRock
Kreditvergabe und Kreditaufnahme	Aave, Compound	Celsius, Nexo	Bank of America

Quelle: <https://www.coindesk.com/learn/defi-vs-cefi-in-crypto/>

1.6 Web3

Der Begriff „Web3“ (oder Web 3.0) wurde von Ethereum-Mitbegründer Gavin Wood geprägt und bezeichnet ein dezentrales digitales Ökosystem auf Basis der Blockchain.⁹ Häufig wird der Begriff vom Web 2.0 dadurch abgegrenzt, dass ein Gegensatz zwischen Zentralisierung und Dezentralisierung suggeriert wird. Web 2.0 steht nach diesem Erklärungsansatz für eine Plattformökonomie mit großen zentralistischen Playern, welche den Zugang zu und die Spielregeln auf ihren Plattformen bestimmen und von den zentral verwalteten Datensätzen profitieren. Für das Web 3.0 gehen die konkreten Vorstellungen unterschiedlicher Akteure auseinander und es existiert keine einheitliche Definition. Gemein ist allen Erklärungsansätzen, dass das Schlüsselkonzept der Dezentralisierung im Fokus steht und die Verteilung von Rechten und Werten über kryptographische Token. Daher werden von vielen Erklärungsansätzen NFTs, DeFi und DAOs erfasst. Teilweise werden auch die Konzepte einer selbstbestimmten digitalen Identität, die Transparenz des Ökosystems und eine Demokratisierung im Hinblick auf den Besitz und Zugang zu Daten in die Definition mit eingeschlossen.

Kritiker halten Web 3.0 für einen Marketingbegriff und die aktuellen Entwicklungen in diesem Bereich für weniger dezentralisiert, als es die Akteure dieser Branche darstellen. Insbesondere da ein Großteil der Umsätze in der Krypto-Ökonomie derzeit noch von großen Unternehmen aus dem CeFi-Segment erwirtschaftet werden, erscheint die Vision eines umfassenden dezentralisierten digitalen Ökosystems, welches auch weniger technikversierten Nutzern zugänglich ist, noch in weiter Ferne. Einige Marktbeobachter schlussfolgern sogar, dass man durch die Dominanz von Risikokapitalfirmen in diesem Segment zukünftig lediglich die etablierten Big-Tech-Player durch neue große Spieler aus dem Finanzmarkt-bereich austauschen wird.

1.7 Kritik

Die Krypto-Ökonomie im Allgemeinen steht unter regulatorischer Beobachtung und erntet auch in der Öffentlichkeit viel Kritik. Insbesondere der „Proof-of-Work“-Ansatz benötigt in der aggregierten Betrachtung weltweit ein sehr hohes Maß an Energie und hat damit erhebliche negative Auswirkungen auf die Umwelt. Der jährliche Energieaufwand alleine für das Bitcoin-Netzwerk wird auf 114,9 TWh geschätzt. Dies entspricht 64,09 Megatonnen CO₂, was ungefähr dem CO₂-Ausstoß von Serbien und Montenegro entspricht.¹⁰ Der negative Effekt schwankt dabei stark entsprechend der globalen Verteilung von Minern und dem lokal verfügbaren Energieerzeugungsmix. Analysen legen nahe, dass beispielsweise das harte Durchgreifen gegen Krypto-Miner in China¹¹ zu einer Verlagerung der Mining-Aktivitäten in die USA und Kasachstan geführt hat, was sich negativ auf den Anteil regenerativer Energien auswirkte, welcher für das Mining aufgewendet wird. Allerdings steigen die Mining-Aktivitäten in China derzeit wieder an und übertreffen sogar mittlerweile das Niveau vor dem harten Durchgreifen der Regierung.¹²

Ein vergleichbarer Effekt lässt sich auch bei Hardwarepreisen beobachten. Für das „Mining“ geeignete Hardwarekomponenten für Endanwender (z. B. Grafikkarten) waren insbesondere zu Hochzeiten der globalen Chip-Knappheit für Verbraucher kaum erschwinglich und werden von der Profitabilität von Krypto-Werten beeinflusst.¹³ Die Gesamtnachfrage nach diesen Komponenten und der damit verbundene Elektroschrott, der nach der Lebensdauer dieser Komponenten anfällt, steigt damit drastisch an.

⁹ <https://www.wired.com/story/web3-gavin-wood-interview/>

¹⁰ <https://digiconomist.net/bitcoin-energy-consumption>

¹¹ <https://www.npr.org/2022/02/24/1081252187/bitcoin-cryptocurrency-china-us>

¹² <https://www.jbs.cam.ac.uk/insight/2022/bitcoin-mining-new-data-reveal-a-surprising-resurgence/>

¹³ <https://www.tomshardware.com/news/gpu-prices-plummet-along-with-crypto>

Daneben wird ebenfalls die Obsoleszenz von Hardware für den Zweck des Minings kritisiert. Da der Aufwand des Minings über die Zeit ansteigt, wird der Einsatz älterer und damit weniger leistungsfähigen Hardwarekomponenten immer unattraktiver, was ebenfalls zu mehr Elektroschrott beitragen kann, falls die Komponenten nicht einer Zweitverwertung zugeführt werden können. Auch drastische Kursverluste von Kryptowährungen wie in 2022 können das Mining unattraktiv werden lassen und zu Abverkäufen von Komponenten führen, die vorher zu Mining-Zwecken eingesetzt wurden.¹⁴

Darüber hinaus werden durch die Anonymität von Krypto-Produkten illegale Finanztransaktionen vereinfacht. Daher steht die Krypto-Branche regelmäßig in der Kritik Geldwäsche zu erleichtern¹⁵ und betrügerischen Akteuren ein neues Spielfeld zu eröffnen. Dies lässt sich unter anderem dadurch nachweisen, dass die Anzahl von sogenannten „Ransomware-Attacken“ (d. h. Verschlüsseln von geschäfts- bzw. betriebsrelevanten Daten unter Lösegeldforderung) mit steigenden Kursen von bekannten Kryptowährungen zunehmen.¹⁶

Allerdings werden von Befürwortern auch die ungenutzten Potenziale von Krypto-Assets hervorgehoben. Gerade in Entwicklungsländern gibt es eine Vielzahl von Menschen ohne Zugang zu einem Bankensystem. Von einigen Marktbeobachtern werden daher Krypto-Finanzprodukte als eine technologische Innovation angesehen, um diesen Menschen die Teilhabe an Finanzdienstleistungen zu ermöglichen.¹⁷

In dieser Kurzstudie wird im Folgenden ein Überblick über die Entwicklung der Krypto-Ökonomie gegeben und anschließend auf die beiden Phänomene NFTs und DAOs näher eingegangen.

¹⁴ <https://videocardz.com/newz/crypto-crash-forces-miners-to-sell-hundreds-of-graphics-cards-during-livestreamed-auctions>

¹⁵ <https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/05/money-laundering-non-fungible-tokens>

¹⁶ <https://venturebeat.com/security/the-surprising-relationship-between-bitcoin-and-ransomware-is-investigated-in-white-house-summit/>

¹⁷ <https://www.finews.ch/news/finanzplatz/54822-ftx-bit-capital-ha-duong-krypto-crypto-crash-bitcoin-ethereum>

2 Entwicklung der Krypto-Ökonomie

2.1 Marktentwicklung und Volatilität

Aus ökonomischer Perspektive handelt es sich bei blockchainbasierten Produkten um eine Netzwerkökonomie. Je nach Netzwerktopologie existieren verschiedene Ansätze um Netzwerkeffekte und damit den Wert eines Netzwerks zu bestimmen. Für Bitcoin hat sich beispielsweise (wie auch bei Telekommunikationsnetzen) das Metcalfesche Gesetz bestätigt. Danach erhöht sich der Wert eines Netzwerkes nicht linear, wenn mehr Menschen dem Netzwerk beitreten, sondern proportional zum Quadrat der Anzahl der Nutzer. Peterson (2018) zeigt in einer empirischen Analyse, dass der Bitcoin-Preis mittel- bis langfristig tatsächlich dem Metcalfeschen Gesetz zu folgen scheint.

Mit Blick auf die Marktkapitalisierung führen aktuell (Dezember 2022) Bitcoin und Ethereum den weltweiten Markt der Kryptowährungen an. Allerdings fallen in der Momentaufnahme (Abbildung 2-1) die auch kurzfristig deutlich schwankenden Kurse für die dargestellten Kryptowährungen (sortiert nach Marktkapitalisierung) auf. Ausnahme bilden in diesem Beispiel die Währungen „Tether“ und „USD Coin“, welche in die in der Einleitung beschriebene Gruppe der Stablecoins fallen und an den Kurs des US-Dollars gekoppelt sind. Daher ergeben sich bei diesen beiden Kryptowährungen nicht die sonst deutlich sichtbaren Kursschwankungen im dargestellten Wochenverlauf.

Abbildung 2-1: Top Kryptowährungen nach Marktkapitalisierung (11.12.2022)

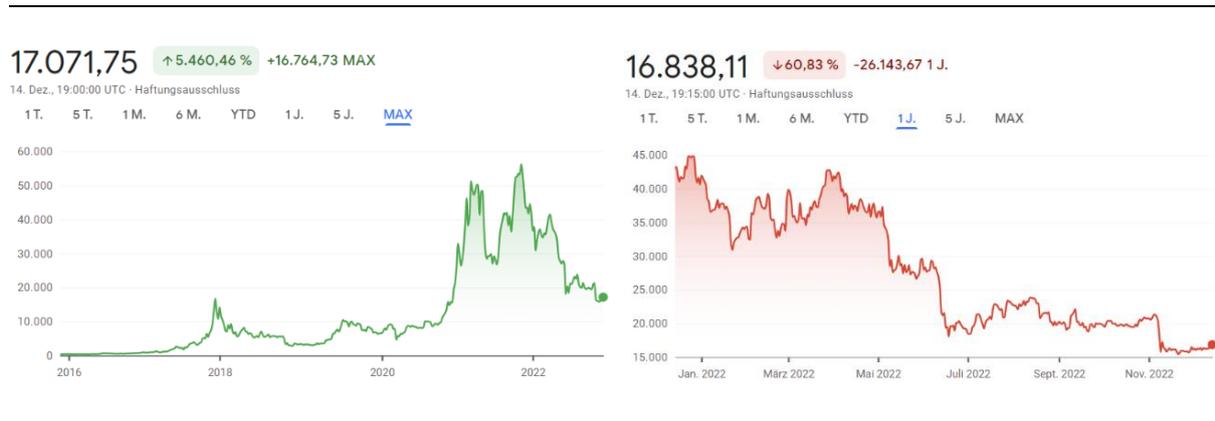
☆ 1	 (BTC) BITCOIN	€16,272.17	€313.85 B	€13.27 B	19.23 M BTC	
☆ 2	 (ETH) ETHEREUM	€1,208.10	€145.98 B	€2.66 B	120.52 M ETH	
☆ 3	 (USDT) TETHER	€0.95	€62.52 B	€15.44 B	65.71 B USDT	
☆ 4	 (BNB) BNB	€274.72	€45.02 B	€381.22 M	163.28 M BNB	
☆ 5	 (USDC) USD COIN	€0.95	€40.69 B	€957.79 M	42.75 B USDC	
☆ 6	 (BUSD) BINANCE USD	€0.949	€21.03 B	€3.84 B	22.10 B BUSD	
☆ 7	 (XRP) XRP	€0.3663	€18.56 B	€306.78 M	50.40 B XRP	
☆ 8	 (DOGE) DOGECOIN	€0.0913	€12.60 B	€252.06 M	137.26 B DOGE	
☆ 9	 (ADA) CARDANO	€0.2964	€10.44 B	€74.53 M	35.05 B ADA	
☆ 10	 (MATIC) POLYGON	€0.860	€7.74 B	€108.81 M	8.96 B MATIC	

Quelle: <https://crypto-economy.com/markets/> (Aufgerufen: 11.12.2022)

Allerdings unterliegen Kryptowährungen nicht nur kurzfristigen Kursschwankungen, sondern auch langfristigen, teils drastischen, Wertveränderungen. Abbildung 2-2 verdeutlicht dies anhand der Gegenüberstellung der Kursentwicklung von Bitcoin (BTC) von 11/2015-12/2022 im Vergleich zur Kursentwicklung im Jahresverlauf 2022. Auch nach starken Kursverlusten in 2022 hat Bitcoin im Vergleich zu 2016 immer noch um 5460% an Wert gewonnen (vgl. Abbildung 2-2a), ein Vorteil für Akteure, die früh in die Technologie investiert haben. Im Gegensatz dazu haben Anleger, die beispielsweise in 2021 auf einem hohen Kursniveau in Bitcoin investiert haben, bis Dezember 2022 einen Wertverlust von bis zu 60% erlitten (vgl. Abbildung 2-2b). Der bisher höchste Kurs des Bitcoin lag bei 59.717,00 €.¹⁸

¹⁸ <https://kriptomat.io/de/kryptowaehrungen-kurse/bitcoin-btc-kurs/>

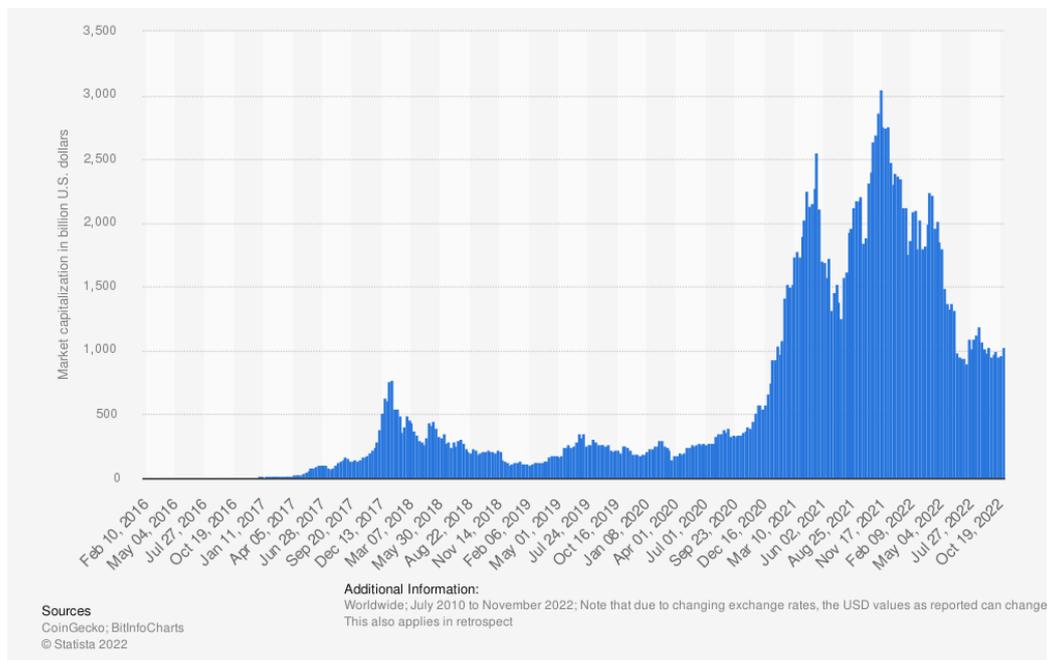
Abbildung 2-2: Bitcoin (BTC) in Euro (EUR) –11/2015-12/2022 vs. 2022



Quelle: <https://www.google.com/finance/quote/BTC-EUR> (Abgerufen 11.12.2022)

Die Entwicklung der Gesamtmarktkapitalisierung von Kryptowährungen erreichte ihren bisherigen Höchstwert im November 2021 mit 3058 Mrd. US-Dollar (Statista, 2022b). Die Marktkapitalisierung ist bis Oktober 2022 auf ein Niveau von ca. 1000 Mrd. US-Dollar gefallen. Nach dem Kollaps der Kryptowährung(en) „Terra/Luna“ und der Börse „FTX“ in 2022 befindet sich die Kryptoökonomie aktuell auf einer Talfahrt.

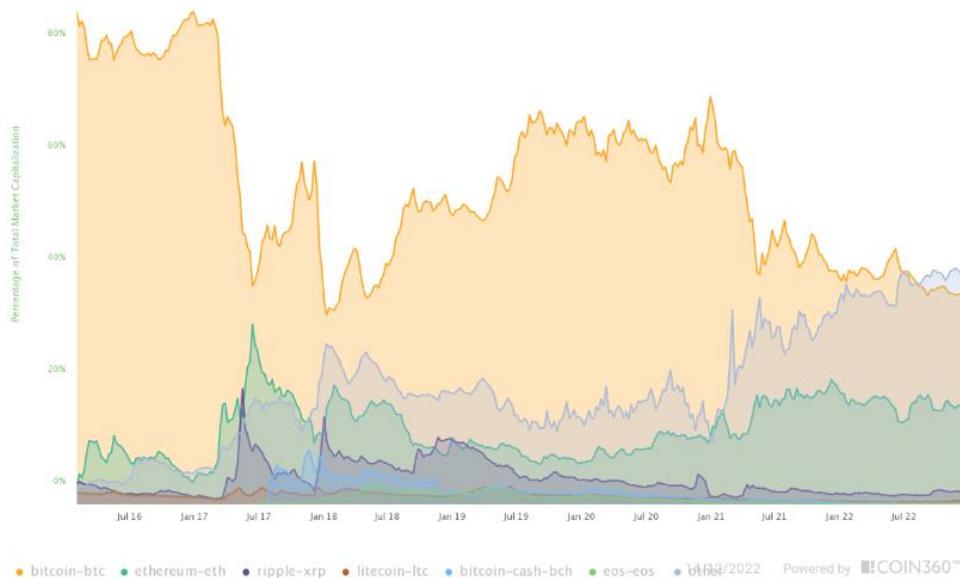
Abbildung 2-3: Gesamtmarktkapitalisierung von Kryptowährungen pro Woche von Juli 2010 bis November 2022



Quelle: Statista (2022b).

Allerdings lässt sich an Abbildung 2-4 erkennen, dass Bitcoin mittlerweile weniger als 40% der gesamten Marktkapitalisierung ausmacht. Dies liegt unter anderem daran, dass sich immer mehr Kapital auf andere Kryptowährungen wie Ether und eine Vielzahl anderer Altcoins und Krypto-Produkte verteilt.

Abbildung 2-4: Prozentsätze der gesamten Marktkapitalisierung der beliebtesten Kryptowährungen



Quelle: <https://coin360.com/charts> (Aufgerufen: 14.12.2022)

Im Gegensatz dazu ist die DeFi-Branche erst seit 2020 in starkem Wachstum begriffen. Dabei hat sich die Anzahl der eindeutigen Adressen, die weltweit einen Vermögenswert im DeFi-Segment gekauft oder verkauft haben, von Ende 2020 bis Mitte 2022 auf fast 5 Millionen vervielfacht (Dune Analytics, 2022). Der Anteil von DeFi am gesamten Krypto-Handelsvolumen und relevanten Krypto-Börsen ist allerdings noch vergleichsweise gering, wie die folgende Tabelle aufzeigt.

Tabelle 2–1: Top 10 (von 184) Krypto-Börsen nach 24h Handelsvolumen am 18.12.2022

Börse	24h Handelsvolumen	Märkte ¹⁹	Dezentralisiert
Binance	5,43 Mrd. USD	1375	Nein
Coinbase Pro	672,43 Mio USD	537	Nein
Changeelly PRO	504,80 Mio USD	105	Nein
Upbit	428,17 Mio USD	287	Nein
Bitget	387,51 Mio USD	422	Nein
Uniswap v3	368,66 Mio USD	513	JA
Bybit	250,41 Mio USD	302	Nein
Kucoin	250,13 Mio USD	1129	Nein
OKX	242,31 Mio USD	625	Nein
BitMart	240,56 Mio USD	526	Nein

Quelle: <https://coinranking.com/de/exchanges> (Aufgerufen: 18.12.2022)

¹⁹ Die Spalte „Märkte“ bezeichnet die Anzahl der Märkte die eine Börse bedient (z.B. Bitcoin (BTC) zu Tether USD (USDT)).

2.2 Die Krypto-Krise in 2022

Mit dem Crash der drittgrößten Krypto-Börse „FTX“ unter der Führung von Sam Bankman-Fried Ende 2022 wurden innerhalb kürzester Zeit 200 Milliarden USD Marktkapitalisierung von Krypto-Assets vernichtet.²⁰ Im Sog dieses Kollapses melden immer mehr Krypto-Firmen Insolvenzen an (z. B. BlockFi²¹). Allerdings ist der Zusammenbruch der dem CeFi-Bereich zuzuordnenden Krypto-Börse FTX auf Misswirtschaft, fehlendes Risikomanagement und potenziellen Betrug zurückzuführen.

Sam Bankman-Fried, Sohn von Barbara und Joseph Bankman-Fried, beide Juraprofessoren an der Stanford Law School, im Fox Hill Gefängnis auf den Bahamas, wurde vor einem Gericht in Nassau zu seiner Freilassung auf Kautions und der Auslieferung an die USA angehört.²² Er wurde von US-Behörden in mehreren Fällen wegen Betrugs und Geldwäscherei angeklagt. Der Antrag auf Freilassung auf Kautions wurde abgelehnt.²³ Mittlerweile wurde er an die USA ausgeliefert.²⁴

Nach Presseberichten hat die Partnerin von Sam Bankman-Fried, Stanford-Absolventin Caroline Ellison, Tochter von Sara Fisher Ellison, MIT-Dozentin für VWL, und Glenn Ellison, MIT-Head of Economics, als hochrangige Händlerin für das ebenfalls von Bankman-Fried gegründete Unternehmen Alameda gearbeitet.²⁵ Dort stieg die hochbegabte Mathematikerin mit dem Erfolg von FTX zum Co-CEO auf, da sich Bankman-Fried auf seine Rolle als CEO von FTX konzentrierte, als der Krypto-Boom die Bewertung des Unternehmens bis auf 32 Milliarden USD trieb.²⁶ Allerdings hielt Bankman-Fried weiterhin 90% der Anteile an Alameda und man geht aktuell davon aus, dass FTX ein Volumen von mindestens 4 Milliarden USD an Kundengeldern genutzt hat, um die hoch riskanten Geschäfte Alamedas zu finanzieren.²⁷ Alameda Research ist mit rund 30 Firmen verflochten, verteilt in Staaten wie Panama, Nigeria, Türkei, Antigua, Singapur oder Hongkong.²⁸ Nach Aussagen des derzeitigen Insolvenzverwalters von FTX, John J Ray III, haben auch Bankman-Frieds Eltern von FTX Gelder erhalten.²⁹ Nach Gerichtsunterlagen gab er ebenfalls an, in seiner Laufbahn noch nie ein „vollständiges Versagen der Unternehmenskontrollen und ein so vollständiges Fehlen vertrauenswürdiger Finanzinformationen erlebt [zu haben] wie in diesem Fall“ und beklagt die Machtkonzentration "in den Händen einer sehr kleinen Gruppe unerfahrener und unbedarfter Personen".³⁰

20 <https://www.finews.ch/news/finanzplatz/54822-ftx-bit-capital-ha-duong-krypto-crypto-crash-bitcoin-ethereum>

21 <https://cryptopotato.com/blockfi-files-for-bankruptcy-following-ftx-crash/>

22 <https://www.businessinsider.de/wirtschaft/finanzen/die-mutter-von-sam-bankman-fried-lachte-waehrend-der-anhoerung-vor-gericht-ihres-sohnes-so-ein-medienbericht-b/>

23 <https://www.businessinsider.com/sam-bankman-fried-arrogant-scared-at-bahamas-prison-official-2022-12>

24 <https://www.spiegel.de/wirtschaft/unternehmen/pleite-von-kryptoboerse-ftx-zwei-topmanager-bekennen-sich-wegen-betrugs-schuldig-a-95e24959-3b57-4763-a03e-030d7e21c46f>

25 <https://www.manager-magazin.de/finanzen/carolne-ellison-bei-ftx-und-alameda-research-die-mysterioese-rolle-der-hedgefonds-chefin-a-5db14370-3cdf-497e-ba8f-f0d4bd7a8c7d>

26 <https://www.finanzen.ch/nachrichten/devisen/das-weiss-man-ueber-caroline-ellison-die-ehemalige-ceo-von-alameda-research-1031947075>

27 <https://markets.businessinsider.com/news/currencies/ftx-crash-client-funds-alameda-binance-sbf-sec-cftc-probe-2022-11>

28 <https://www.manager-magazin.de/finanzen/carolne-ellison-bei-ftx-und-alameda-research-die-mysterioese-rolle-der-hedgefonds-chefin-a-5db14370-3cdf-497e-ba8f-f0d4bd7a8c7d>

29 <https://www.businessinsider.de/wirtschaft/finanzen/die-mutter-von-sam-bankman-fried-lachte-waehrend-der-anhoerung-vor-gericht-ihres-sohnes-so-ein-medienbericht-b/>

30 <https://financialservices.house.gov/uploadedfiles/hhrg-117-ba00-wstate-rayj-20221213.pdf>

Zum Zeitpunkt der Verschriftlichung dieser Studie ist noch unklar, wie nachhaltig dieser Kollaps die Krypto-Industrie verändern oder beeinträchtigen wird. Allerdings ist dies nicht der erste Skandal, den die Branche bisher erlebt hat.

Bereits im Mai 2022 kollabierte die koreanische Krypto-Währung Terra. Terraform Labs betreibt die Terra-Blockchain und gab darüber sowohl die Krypto-Währung terraUSD (UST), als auch Luna aus. Dabei war terraUSD als algorithmischer Stablecoin konzipiert. Allerdings handelte es sich bei terraUSD im Gegensatz zu anderen Stablecoins (z. B. Tether, USDC) nicht um eine fiat-gestützte Kryptowährung. Statt realer Vermögenswerte wurde der Wert von terraUSD durch die zweite Kryptowährung Luna gestützt. Gleichzeitig bot der Betreiber mit „Anchor“ eine Darlehensplattform an, in welche Kunden Einlagen in der eigenen Krypto-Währung terraUSD einstellen konnten und dafür von der Plattform eine feste Zinsrate von 20% in Aussicht gestellt bekamen. Dieser Anreiz führte zu großer Popularität der Plattform im Heimatmarkt Südkorea und Berichte über erste Terra-Millionäre führten ebenfalls zu großer Bekanntheit des Gründers Do Kwon.³¹

Kunden mussten in Luna investieren um terraUSD zu erhalten. Der Wechselkurs wurde von dem aktuellen Luna-Kurs in US Dollar bestimmt. Allerdings konnten zu jeder Zeit eine Einheit terraUSD in eine Einheit Luna umgewandelt werden. Als im Mai 2022 die algorithmische Bindung von terraUSD and den US Dollar nicht mehr stabil gehalten werden konnte, fiel der Preis von terraUSD unter einen US Dollar. Damit wurde es für Anleger attraktiv ihre terraUSD Reserven zum festgelegten Kurs von 1:1 in Luna zu tauschen. Daraufhin brach der Kurs von terraUSD zusammen. Da Luna aber ohne terraUSD ebenfalls wertlos ist, brach daraufhin auch die Krypto-Währung Luna zusammen.³² Nach Schätzungen der Firma Elicptic gingen dabei 42 Milliarden US Dollar verloren.³³ Do Kwon wurde wegen Betrugs und Verstößen gegen das Kapitalmarktrecht angeklagt und befindet sich nach einem Zwischenstopp in Dubai derzeit auf der Flucht. Nach Berichten befindet er sich aktuell in Serbien³⁴ und wird seit September, ebenso wie fünf seiner Mitarbeiter, mit einem internationalen Haftbefehl (Interpol "Red Notice") gesucht.³⁵ Da die Krypto-Währung selbst dezentral über eine Blockchain realisiert wird, kann sie aber auch nach dem Absturz weiter gehandelt werden und der Kurs scheint sich aktuell sogar zu erholen.³⁶

Ein weiteres prominentes Beispiel der Vergangenheit ist der Zusammenbruch der Handelsplattform „Mt. Gox“ in 2014, die zu dem Zeitpunkt ca. 60% des weltweiten Bitcoin-Handels abwickelte. Das Unternehmen meldete am 28. Februar 2014 Insolvenz an und gab an, es seien 750.000 Bitcoins von Kunden sowie 100.000 Bitcoins des Unternehmens durch Hackerangriffe verloren gegangen. Im weiteren Verlauf des Verfahrens gab das Unternehmen an, 200.000 Bitcoins seien wieder aufgetaucht.³⁷ Bei späteren Ermittlungen konnte allerdings festgestellt werden, dass von den immer noch fehlenden 650.000 Bitcoins nur 7000 durch Hackerangriffe entwendet wurden. Verdächtige Kontenbewegungen legen nahe, dass diese durch bestens mit dem System vertraute Insider im Unternehmen veruntreut wurden.³⁸ Auch hier stand mit dem CEO Mark Karpeles eine Person im Rampenlicht, die direkt oder indirekt von den illegalen Machenschaften profitiert haben könnte. Zwar wurde er in 2019 von einem Gericht in Tokio für schuldig befunden, elektronische Aufzeichnungen im Zusammenhang mit den Büchern von

31 <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=2d7f8ef04ff1>

32 <https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=2d7f8ef04ff1>

33 <https://www.bbc.com/news/business-63940181>

34 <https://www.btc-echo.de/schlagzeilen/do-kwon-haelt-sich-womoeiglich-in-serbien-versteckt-155899/>

35 <https://t3n.de/news/terra-chef-do-kwon-auf-der-flucht-interpol-sucht-mit-internationalem-haftbefehl-1501468/>

36 <https://www.nasdaq.com/articles/is-terra-luna-token-coming-back-from-the-dead>

37 <http://www.mtgox.com/img/pdf/20140320-btc-announce.pdf>

38 <https://www.heise.de/newsticker/meldung/Untergang-der-Bitcoin-Boerse-Mt-Gox-Ermittlungen-deuten-auf-Insider-Tat-2507602.html>

Mt. Gox gefälscht zu haben, aber für unschuldig in Bezug auf die Anklagepunkte Veruntreuung und Vertrauensbruch. Karpeles wurde zu einer Bewährungsstrafe von zwei Jahren und sechs Monaten verurteilt.³⁹

Insgesamt ist der Kurs des Bitcoin seit 2012 mehr als 10 Mal gecrasht und teilweise von fast 20.000 USD auf etwa 3.000 USD gefallen.⁴⁰ Auch zu diesen Zeitpunkten waren viele Beobachter kritisch. Allerdings hat sich auch nach Mt. Gox der Bitcoin Kurs trotz aller Befürchtungen von Analysten wieder erholt und sogar neue Höchststände erreicht. Auch jetzt wird von unterschiedlichen Seiten der Niedergang der Krypto-Branche beschworen.⁴¹ Die Beispiele der Vergangenheit zeigen allerdings, dass nicht davon auszugehen ist, dass die aktuelle Krise das Fortbestehen der Krypto-Branche essenziell gefährdet.

2.3 Regulierung der Krypto-Ökonomie

Allerdings lässt sich es aufgrund dieser Geschehnisse und der allgemeinen Kritik im Hinblick auf Geldwäsche, Steuerhinterziehung und Umweltschädigung auch nicht von der Hand weisen, dass Krypto-Märkte besser von Regulierungsvorhaben erfasst werden sollten. In den USA kündigte nach dem FTX-Crash bereits die Finanzministerin Janet Yellen an, dass eine effektivere Aufsicht über Krypto-Märkte erforderlich sei, ohne dabei FTX explizit zu nennen.⁴² Insgesamt beläuft sich der geschätzte Wert an verlorenen Krypto-Anlagen in der gesamten Industrie bisher auf ca. 74,5 Milliarden USD, davon konnten von den Betroffenen insgesamt nur ca. 6 Milliarden USD (8%) wiedergewonnen werden.

Abbildung 2-5: Kumulierte verlorene und wiedergewonnene Crypto-Anlagen



Quelle: <https://defiyield.app/rekt-database> (Aufgerufen: 11.12.2022)

³⁹ <https://www.coindesk.com/markets/2019/03/15/mt-goxs-mark-karpeles-found-guilty-over-data-manipulation-in-tokyo-court/>

⁴⁰ <https://www.finews.ch/news/finanzplatz/54822-ftx-bit-capital-ha-duong-krypto-crypto-crash-bitcoin-ethereum>

⁴¹ <https://www.economist.com/leaders/2022/11/17/is-this-the-end-of-crypto>

⁴² <https://www.manager-magazin.de/unternehmen/tech/ftx-und-sam-bankman-fried-die-abgruende-des-desasters-a-fa433527-292c-4140-bbe3-878c6afe377a>

Dabei zeichnen sich bereits erste Veränderungen ab. Die größte Krypto-Börse „Binance“ verzeichnet aktuell einen „Bank-Run“, bei dem Anleger sich im großen Stil von der Börse zurückziehen. Innerhalb eines Monats hat sich das Volumen von in öffentlichen Wallets (Krypto-Geldbörsen) gehaltenen Werten auf der Plattform von 69,5 Milliarden USD auf 54,7 Milliarden USD verringert. Das Unternehmen versucht das mangelnde Vertrauen durch Nachweise zu seinen Reserven zu beschwichtigen. Allerdings sollen die Hälfte der Reserven des Unternehmens in den eigenen Krypto-Währungen BUSD, einem Stablecoin, und binance coin (BNB) vorgehalten werden.⁴³ Nach aktuellen Berichten wird das US-Justizministerium gegen Binance auch wegen Finanzkriminalität ermitteln. Laut Reuters prüft die Staatsanwaltschaft, ob sie Anklage gegen den Gründer Changpeng Zhao und andere Führungskräfte erheben wird. Die Anklagen würden sich auf Verschwörung zur Geldwäsche, unerlaubte Geldübermittlung und Verstöße gegen strafrechtliche Sanktionen beziehen. Laut Schätzungen von Reuters hat Binance im Jahr 2022 über 10 Milliarden Dollar an illegalen Zahlungen abgewickelt.⁴⁴

Auf europäischer Ebene gibt es bereits eine Einigung über die seit 2020 geplante europäische Verordnung über Kryptowerte (Markets in Crypto-Assets - MiCA). Die Verordnung sollte ursprünglich bereits Ende 2022 in Kraft treten. Die Abstimmung darüber wird aber frühestens im Februar 2023 stattfinden, da die Komplexität des Gesetzestextes für Verzögerungen sorgte.⁴⁵ MiCA unterwirft zukünftig Kryptowerte, Emittenten von Kryptowerten und Anbieter von Krypto-Dienstleistungen einem europäischen Regelungsrahmen. Der Entwurf greift dabei bereits einen missverständlichen Begriff der Krypto-Branche auf und differenziert ihn juristisch basierend auf dem Referenzwert. Stablecoins sind ein allgemein sehr weit gefasster Begriff, wie insbesondere der Fall des Terra-Crashes belegt. Basierend auf der Verordnung wird daher zukünftig in der EU zwischen „E-Geld-Token“ und „wertreferenzierten Token“ unterschieden. E-Geld-Token nehmen dabei ausschließlich auf eine bestimmte offizielle Währung Bezug. Für wertreferenzierte Token können unterschiedliche offizielle Währungen oder andere (Kombinationen von) Assets und Kryptowerten als Bezugsgrundlage dienen. Eine Differenzierung nach dem Mechanismus, wie Wertstabilität faktisch erreicht werden soll, erfolgt in der Verordnung nicht. Algorithmische Stablecoins wie im Fall von Terraform Labs werden daher explizit von der Verordnung erfasst.⁴⁶ Grundsätzlich werden zukünftig folgende Punkte durch die MiCA-Verordnung adressiert:⁴⁷

- Anbieter von Krypto-Dienstleistungen benötigen zukünftig eine Zulassung, um in der EU tätig zu werden (es sei denn, der Wert aller Tokens in einem Jahr liegt unter 5 Mio EUR)
- Anbieter von Krypto-Dienstleistungen sind zukünftig verpflichtet, strenge Vorgaben zum Schutz der Wallets (Krypto-Geldbörsen) der Verbraucher zu erfüllen.
- Anbieter von Krypto-Dienstleistungen sind zukünftig haftbar, wenn sie Kryptowerte von Anlegern verlieren.
- Stablecoin-Besitzern wird vom Emittenten ein jederzeit ausübbarer, kostenloser Anspruch auf Umtausch eingeräumt

43 <https://markets.businessinsider.com/news/currencies/crypto-binance-scrutiny-collapse-ftx-exchange-chang-peng-zhao-bankman-fried-2022-12>

44 <https://www.reuters.com/markets/us/us-justice-dept-is-split-over-charging-binance-crypto-world-falters-sources-2022-12-12/>

45 <https://www.btc-echo.de/news/mica-abstimmung-zu-krypto-regulierung-im-eu-parlament-vertagt-153825/>

46 <https://www.cmshs-bloggt.de/rechtsthemen/die-neue-mica-verordnung/mica-entwurf-wertreferenzierten-tokens-und-e-geld-tokens/>

47 <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>

- Stablecoin-Emittenten werden Vorgaben zum Umgang mit ihrer Reserve gemacht und eine angemessene Mindestliquidität auferlegt.
- Emittenten von Kryptowerten müssen einen eingetragenen Sitz in der EU haben.
- Krypto-Betreiber müssen Informationen über ihren ökologischen und klimatischen Fußabdruck vorlegen.

Interessanterweise werden NFTs von dem Anwendungsbereich dieser Verordnung nicht erfasst, sofern sie nicht in eine der bestehenden Wertekategorien fallen. Der Proof-of-Work-Ansatz mit seinen negativen Auswirkungen auf die Umwelt ist dort ebenfalls bisher nicht adressiert worden. Daher hat es sich die EU zum Ziel gesetzt die Branche weiter zu beobachten, um nach dem Inkrafttreten von MiCA potenziell weitere Anpassungen vorzunehmen. Dazu soll auch ein regelmäßiges Monitoring großer Anbieter von Krypto-Dienstleistungen stattfinden:⁴⁸

- Die Europäische Kommission wird binnen 18 Monaten beauftragt, eine umfassende Bewertung sowie gegebenenfalls einen entsprechenden und verhältnismäßigen horizontalen Legislativvorschlag zur Schaffung einer Regelung für nicht austauschbare Token und zur Bewältigung der sich abzeichnenden Risiken eines solchen neuen Marktes auszuarbeiten.
- Die Europäische Kommission muss binnen zwei Jahren einen Bericht über die Umweltauswirkungen von Kryptowerten und die Einführung verbindlicher Mindeststandards für die Tragfähigkeit von Konsensmechanismen, einschließlich Proof-of-Work, vorlegen.
- Die nationalen Behörden müssen der Europäischen Wertpapier- und Marktaufsichtsbehörde (ESMA) regelmäßig einschlägige Informationen zu den größten Anbietern von Krypto-Dienstleistungen übermitteln.
- Die Europäische Bankenaufsichtsbehörde (EBA) wird beauftragt, ein öffentliches Register der nicht konformen Anbieter von Krypto-Dienstleistungen zu führen. Anbieter von Krypto-Dienstleistungen mit Bezug zu Drittländern mit hohem Risiko für Geldwäscheaktivitäten oder Ländern in der EU-Liste nicht kooperativer Länder und Gebiete für Steuerzwecke, werden verstärkt kontrolliert.

Neben der Ausarbeitung von MiCA wurden bereits die Rechtsvorschriften zur Bekämpfung der Geldwäsche (Anti money laundering - AML) in der EU angepasst und der Anwendungsbereich dieser Vorschriften auf Kryptowerte ausgeweitet. Die EU hat sich dabei an den Empfehlungen der „Financial Action Task Force“ (FATF), der globalen Aufsichtsbehörde für Geldwäsche und Terrorismusfinanzierung, orientiert. Mit diesen Anpassungen werden insbesondere folgende Punkte adressiert:⁴⁹

- Die Rückverfolgbarkeit von Kryptowert-Transfers soll sichergestellt werden, damit mögliche verdächtige Transaktionen besser erkannt und unterbunden werden können.
- Zu gegebener Zeit müssen die Mitgliedstaaten sicherstellen, dass alle Anbieter von Krypto-Dienstleistungen als Verpflichtete im Sinne der Vierten Geldwäscherichtlinie gelten. Damit wird eine Angleichung der Wettbewerbsbedingungen zwischen den Mitgliedstaaten angestrebt.

48 <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>

49 <https://www.consilium.europa.eu/de/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers/>

Durch die enge Beziehung zwischen AML und MiCA wurde beschlossen, den Zeitplan für die Anwendung dieser Verordnung an den Zeitplan von MiCA anzugleichen. Damit stehen der Krypto-Branche in der EU voraussichtlich ab 2023 neue Zeiten bevor. Bruno Le Maire, französischer Minister für Wirtschaft, Finanzen und industrielle und digitale Souveränität fasst die abgestimmte Gesetzesinitiative folgendermaßen zusammen:

„Die jüngsten Entwicklungen in diesem von rasanten Veränderungen geprägten Sektor haben bestätigt, dass eine EU-weite Regulierung dringend erforderlich ist. Die MiCA wird Europäer, die in diese Vermögenswerte investiert haben, besser schützen, den Missbrauch von Kryptowerten verhindern und dabei innovationsfreundlich sein, damit die EU diesbezüglich nicht an Attraktivität verliert. Die wegweisende Verordnung wird dem Wilden Westen, der bei Kryptowerten herrscht, ein Ende setzen und die Rolle der EU als Normgeber in digitalen Fragen festigen.“⁵⁰

Es ist zu erwarten, dass die initiale Version der MiCA-Regularien in Zukunft mehrere Änderungen erfahren wird. Der Markt für Krypto-Produkte mag aktuell angeschlagen wirken, wird sich aber durch technische Innovationen und neue Geschäftsmodelle schnell weiterentwickeln und Regulierer damit regelmäßig vor neue Herausforderungen stellen.

⁵⁰ <https://www.consilium.europa.eu/de/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica/>

3 Non-fungible Tokens (NFT)

Ursprünglich stammt das Konzept von NFTs aus dem Ethereum-Netzwerk und erlaubt es einzigartige Tokens auf einer Blockchain zu erzeugen. NFTs erlauben es daher digitale Güter mit einem Seltenheitswert zu versehen und handelbar zu machen. Damit ist es möglich ein Unikat zu schaffen, vergleichbar mit einem einzigartigen Gemälde, oder eine Limitierung abzubilden und beispielsweise das Konzept von Sammelbildern in einer digitalen Umgebung nachzubilden. Der weltweite Markt für physische Sammlerobjekte, Kunst und limitierte Markenartikel ist für viele Unternehmen ein lukratives Geschäft. Es verwundert daher nicht, dass das Konzept von NFTs, welches digitale Raritäten und Sammlerobjekte erst ermöglicht, für viele Marktakteure als ein reizvolles neues Geschäftsfeld erscheint. Allerdings kann das Erstellen von und der Handel mit NFTs auch dadurch kostspielig sein, dass sich der „Gaspreis“ (siehe Kapitel 1.2) in einer Blockchain ungünstig entwickelt. Im Oktober 2021 kostete das Mining eines NFT-Tokens mehr als 60 USD und die Kosten des Handelns konnten sich auf 60-100 USD pro Transaktion belaufen (Wang et al., 2021).

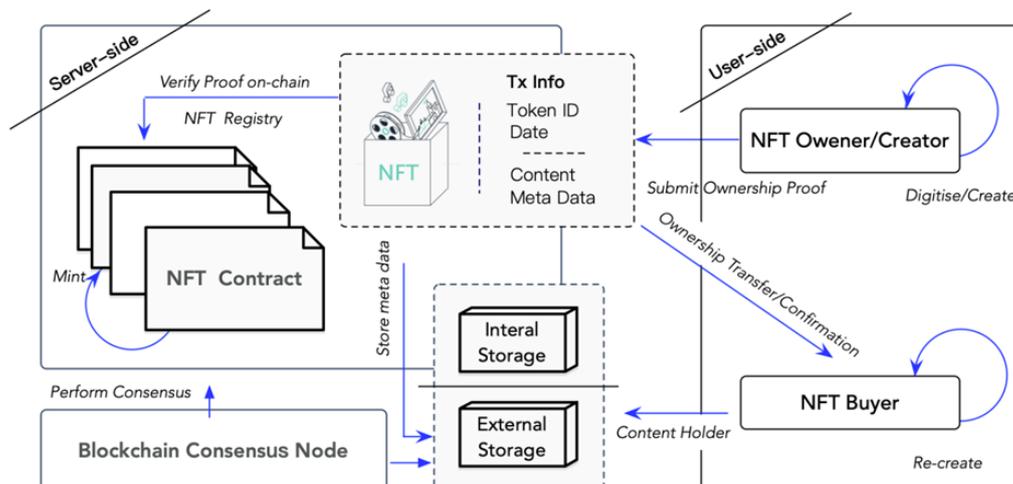
3.1 Technische Umsetzung

Im Folgenden wird ein üblicher Top-to-Bottom Prozess umrissen um ein NFT zu erstellen, zu veröffentlichen und handelbar zu machen. Die folgenden Ausführungen basieren dabei auf der Darstellung aus Wang et al. (2021) und werden nochmals in Abbildung 3-1 zusammengefasst.

Zunächst müssen Rohdaten bzw. das digitale Objekt (z. B. ein Bild oder Video) in ein geeignetes Dateiformat gebracht werden und mit einem korrekten und vollständigen Titel und einer Beschreibung ausgestattet werden. Danach kann die Datei auf einem externen Speicher abgelegt werden, oder direkt in der Blockchain gespeichert werden. Dies verbraucht allerdings „Gas“ (Transaktionsgebühren) und ist daher erheblich kostspieliger als die Speicherung auf einem externen Speicher. An dieser Stelle entscheidet der Eigentümer also bereits darüber, ob das später geprägte NFT nur als ein Verweis auf eine zentrale Ressource anzusehen ist, oder selbst dezentral in der Blockchain gespeichert wird.

Anschließend muss der Eigentümer des NFTs eine Transaktion mit einem Hash der Datei auf dem externen Speicher (oder der Datei selbst) signieren und an einen Smart Contract senden. Anschließend beginnt der Mining- bzw. der Prägeprozess des NFTs („Minting“). Sobald die Transaktion bestätigt wird, ist der Prägeprozess abgeschlossen und das NFT ab diesem Zeitpunkt mit einer eindeutigen Blockchain-Adresse verknüpft und damit persistent. Ob die Datei selbst ebenfalls persistent ist, hängt dabei davon ab, auf welche Weise die Speicherung vorgenommen wurde – innerhalb oder außerhalb der Blockchain.

Abbildung 3-1: NFT-System und Ablauf



Quelle: Wang et al. (2021, S. 6)

3.2 Marktentwicklung

Der Markt für NFTs hat sich in den letzten Jahren rasant entwickelt. Zwischen 2021 und 2022 erreichte der Handel mit Kunst-NFTs im August 2021 einen Höchststand von 117,4 Tausend NFTs. Dabei entfiel der größte Anteil des Handelsvolumens auf Sammlerobjekte und Kunst. Allerdings gewannen NFTs in 2021 insbesondere im Spiele-Segment an Bedeutung (z. B. das von Pokémon inspirierte Spiel „Axie Infinity“⁵¹). Dort müssen beispielsweise NFTs erworben werden um an dem Spiel mit den entsprechenden Spielfiguren teilnehmen zu können. Auch das Metaverse gewinnt im NFT-Segment zunehmend an Bedeutung, allerdings sind die Umsätze mit weniger als 5% im Vergleich zu anderen NFT-Einsatzgebieten noch sehr gering.

Tabelle 3–1: Volumen von Verkäufen, die ein NFT in unterschiedlichen Segmenten weltweit enthalten, 2018-2021 (in Mio. US-Dollar)

	2018	2019	2020	2021
All	36.77	24.02	66.78	13981.9
Collectible	13.86	2.71	16.45	7130.05
Game	5.19	11.59	15.26	2153.82
Art	0.05	0.45	17.11	2107.57
Metaverse	16.35	5.38	15.97	630.99
Utility	1.29	4.11	2.41	75.5
DeFi	0	0	0	19.75
Undefined	0.03	0	0	1864.22

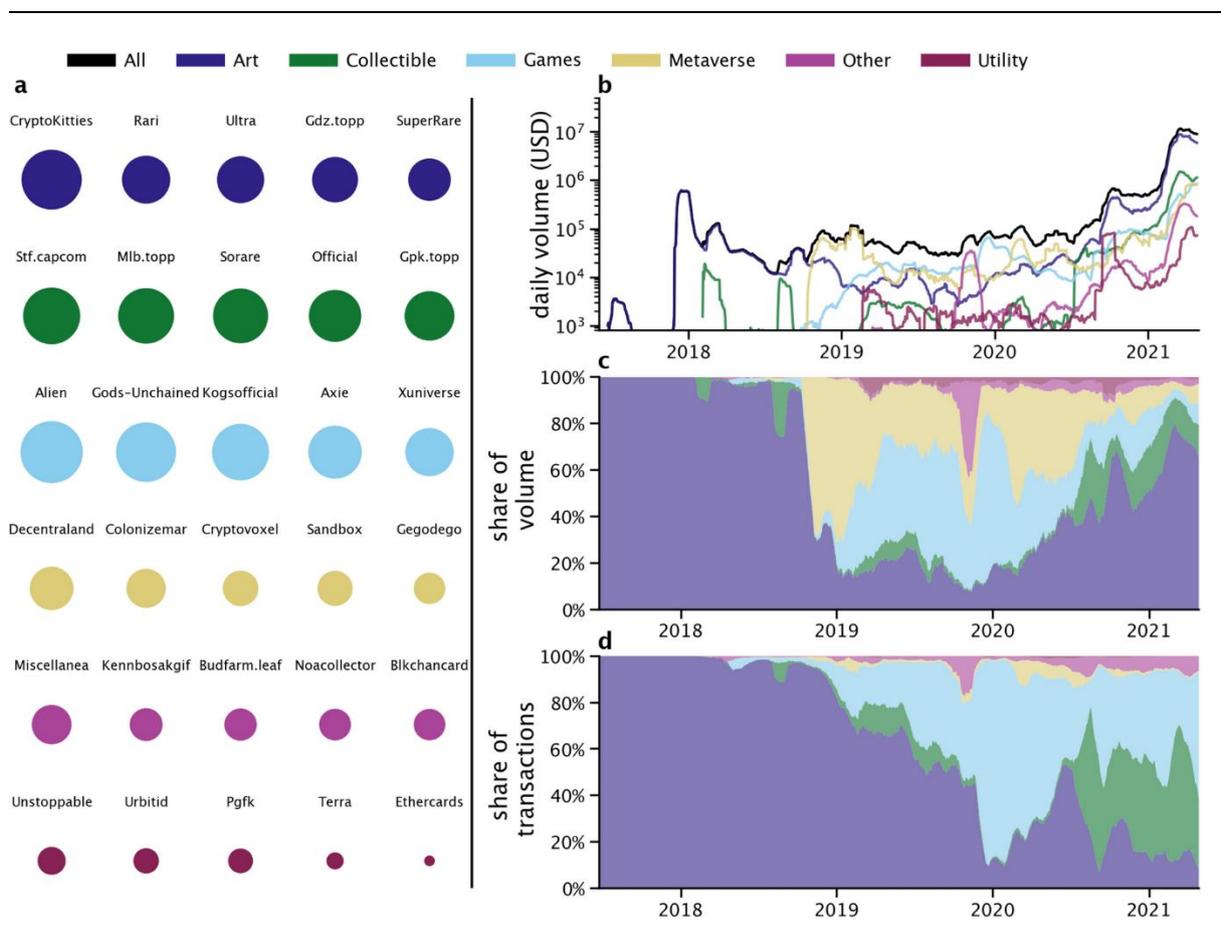
Quelle: Statista (2022a).

51 <https://coincierge.de/nft/axie-infinity/>

In der Studie von Nadini et al. (2021) wird der NFT-Markt zwischen Juni 2017 und April 2021 analysiert und die Ergebnisse grafisch aufgearbeitet. Dabei wurden Daten von der Ethereum und der WAX Blockchain verwendet.

Abbildung 3-2 stellt die Ergebnisse dieser Analyse der NFT-Landschaft dar, im Hinblick auf (a) die wichtigsten NFT-Sammlungen (nach Anzahl der Vermögenswerte) nach Kategorien und in der Größe proportional zur Anzahl der Vermögenswerte in jeder Sammlung, (b) das tägliche Handelsvolumen (in USD) nach Kategorie, (c) den Anteil des Handelsvolumens nach Kategorie und (d) den Anteil der Transaktionen nach Kategorie. Die Ergebnisse in diesen letzteren Feldern sind dabei Durchschnittswerte für ein rollendes Zeitfenster von 30 Tagen.

Abbildung 3-2: Überblick über die NFT-Landschaft (Juni 2017 bis April 2021)



Quelle: Nadini et al. (2021, S. 3)

Die Analyse verdeutlicht, dass NFTs aus dem Kunst- und Sammlerbereich einen hohen Anteil am Handelsvolumen ausmachen. Entsprechende NFTs können auch beliehen werden. Dabei müssen Kreditnehmer bei der Kreditvergabe NFTs als Sicherheiten verpfänden. Entsprechende Kreditangebote werden sowohl von Plattformen aus dem CeFi als auch aus dem DeFi-Bereich gemacht. Die meisten NFT-Kredite werden jedoch von DeFi-Plattformen angeboten, da dort die Kreditvereinbarung und die Einhaltung der vertraglichen Verpflichtungen über Smart Contracts sichergestellt werden können (z. B. dass die NFTs nach fristgerechter Rückzahlung automatisch wieder an den Kreditnehmer transferiert werden). Im Gegensatz zu den möglicherweise komplexeren Regelwerken von Dezentralisierten

Autonomen Organisationen (siehe Kapitel 4) sind die Konditionen und Modalitäten eines Kredits relativ einfach durch Smart Contracts abbildbar.

Über die vergangenen zwei Jahre haben eine lange Reihe von namhaften Unternehmen in das NFT-Segment investiert und eigene Produkte angekündigt oder bereits auf den Markt gebracht. Im Folgenden werden einige prominente Beispiele aufgelistet:

Tabelle 3–2: Beispiele – Investition bekannter Unternehmen in das NFT-Segment

DraftKings	verpflichtet echte NFL-Spieler für "gamifizierte NFT-Sammlungen" (The Verge, 12. Dezember 2021)
Samsung	integriert einen NFT-Marktplatz in seine Smart-TVs (Business Insider, 3. Januar 2022)
Nike	hat ein virtuelles Schuhunternehmen gekauft, das NFTs und Turnschuhe "für das Metaversum" herstellt (The Verge, 13. Dezember 2021)
GameStop	führt seinen eigenen NFT-Marktplatz ein (The Verge, 3. Februar 2022)
Coinbase	Ermöglicht es Nutzern NFTs auch mit Mastercard zu kaufen (Business Insider, 18. Januar 2022)
DFB	FANZONE wird Lizenzpartner des DFB für NFT-basierte Fußball-Sammelkarten (DFB, 2. März 2021)
Weitere: Adidas, Nike, GAP, Macy's, Konami u.v.m.	

Quelle: Zusammenstellung WIK (Einzelnachweise je Zeile).

Allerdings hat auch das NFT-Segment der Kryptobranche unter den turbulenten Marktgeschehnissen in 2022 (siehe Kapitel 2.2) stark gelitten. Der NFT-Markt schrumpfte nach aktuellen Analysen um 77% und fiel auf ein globales Volumen von etwa 1,7 Mrd. USD in Q3 2022.⁵²

3.3 Herausforderungen und Potenziale

In einer 2022 veröffentlichten Studie untersuchen Aharon & Demir (2022) die Beziehung von NFTs zu anderen Anlageklassen in der Zeitperiode zwischen Anfang 2018 und Mitte 2021. Die Ergebnisse dieser Studie deuten darauf hin, dass NFTs hauptsächlich unabhängig von Schocks in gängigen Anlageklassen (auch Ethereum) sind. Über den Zeitverlauf lässt sich feststellen, dass NFTs unter normalen Marktbedingungen bis zu einem gewissen Grad als Überträger von Systemrisiken fungieren können. Allerdings verlagert sich ihre Rolle in turbulenten Zeiten und sie wirken dann als Absorber von Risiko-Spillover-Effekten. Die Autoren schlussfolgern daraus, NFTs in turbulenten Zeiten (z. B. Pandemie) Diversifizierungsvorteile haben können. Umar et al. (2022) untersuchen in einer weiterführenden Studie die Sender und Empfänger von Spillovers für Rendite und Volatilität in unterschiedlichen NFT-Segmenten. Die Ergebnisse dieser Studie legen nahe, dass Utility-NFTs die wichtigsten Spillover-Sender in andere Segmente sind, während die Collectible-NFTs die wichtigsten Spillover-Empfänger sowohl im Hinblick auf Rendite als auch Volatilität sind.

Chalmers et al. (2022) vergleichen NFTs mit dem ehemals erfolgreichen Konzept von Initial Coin Offerings (ICO), einem Ansatz zum Fund-Raising, der Ähnlichkeiten mit einem Börsengang aufweist, im Gegensatz dazu aber nicht von Aufsichtsbehörden genehmigt werden muss. Bei ICOs werden dazu Krypto-Token an Investoren ausgegeben und diese (austauschbaren, d. h. „fungiblen“) Token können anschließend von den Inhabern wie Anteile getauscht werden. Während die Autoren die Potenziale für

⁵² <https://nonfungible.com/reports/2022/en/q3-quarterly-nft-market-report>

die Kreativbranche herausarbeiten, leiten sie aus dem schnellen Aufstieg und Fall von ICOs auch ein Szenario ab, in dem NFTs in Zukunft weniger relevant werden könnten. Aus ihrer Sicht können Individuen in der Kreativbranche (z. B. Musik) insbesondere von dem dezentralen Ansatz profitieren, da sie durch diese Technologie bei der Vermarktung digitaler Produkte unabhängiger von großen Unternehmen (z. B. Produktionsfirmen) werden können. Allerdings könnte sich das Web 3.0 auch nur als eine Modeerscheinung herausstellen, und volatile und betrugsanfällige NFT-Märkte für Investoren an Attraktivität verlieren.

Auf EU-Ebene werden NFTs von der MiCA-Verordnung zunächst nicht erfasst (siehe Kapitel 2.3). Die Kommission wird den Sektor aber gesondert untersuchen und zukünftig basierend auf den Ergebnissen einen Regulierungsrahmen dafür entwickeln. Allerdings werden alle Kryptowertetransfers von der AML-Verordnung zukünftig abgedeckt. Dies kann dazu führen, dass der Markt transparenter wird und damit auch das Potenzial von NFTs zu illegalen Zwecken abnimmt. Da die Krypto-Branche allgemein als sehr spekulativ und volatil gilt, könnte auch das NFT-Segment von einem entsprechenden weiterführenden Regulierungsrahmen profitieren. Insbesondere das Potenzial für die Kreativwirtschaft ist groß, was zahlreiche Investitionen namhafter Unternehmen (siehe Tabelle 3–2) belegen. Es bleibt abzuwarten, ob durch diese Technologie zukünftig individuelle Künstler und Schaffende in der Kreativwirtschaft tatsächlich unmittelbarer und zu einem größeren Anteil von den Früchten ihrer Arbeit profitieren können. Dafür ist es allerdings notwendig, dass NFTs auch für eine breitere Masse von Verbrauchern zugänglich werden. Die einfache Zugänglichkeit von NFT-bezogenen Funktionalitäten in z. B. Smart-TVs und anderer Verbraucherelektronik könnte NFT-basierte Sammler- und Kunstobjekte auch für Verbraucher attraktiv machen, die weniger ein finanzielles Interesse an NFTs als Spekulations- und/oder Werterhaltungsobjekt, sondern vornehmlich an den Assets (z.B. Kunstwerk, Foto) der erworbenen NFTs selbst haben.

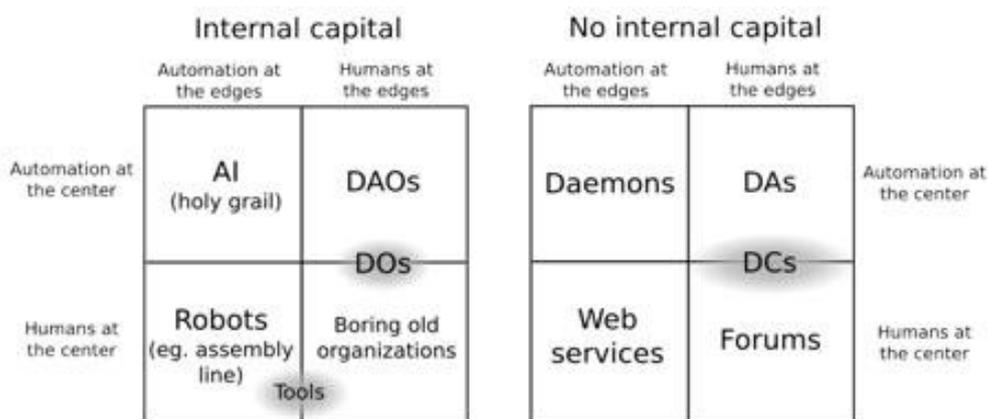
4 Dezentralisierte Autonome Organisationen (DAO)

4.1 Abgrenzungsversuch und Definition

Um das Phänomen von dezentralisierten autonomen Organisationen als eine vollständig über die Blockchain mit Hilfe von Smart Contracts abgebildete Organisationsform (siehe Kapitel 1.3) besser zu erfassen, ist zunächst eine Abgrenzung von verwandten Begrifflichkeiten und Konzepten notwendig. Eine zweckdienliche und umfängliche Diskussion dieses und verwandter Begriffe findet sich dazu bei Vitalik Buterin (2014).

Buterin unterscheidet verschiedene Organisationsformen zunächst anhand der Tatsache, ob eine Organisation internes Kapital besitzt oder nicht, und anschließend anhand der Frage, ob im Kern und an den Rändern der Organisation Menschen oder Automationen im Fokus stehen. Anhand dieser Unterscheidungen ergeben sich die in Abbildung 4-1 dargestellten Matrizen, welche einen Ansatz darstellen um verschiedene verwandte Organisationsformen voneinander abzugrenzen. Im Folgenden werden die Überlegungen von Buterin zusammengefasst:

Abbildung 4-1: Ansatz zur Abgrenzung von DAOs zu anderen Organisationsformen



Quelle: Buterin (2014).

Nach seiner Darstellung ist eine Organisation, die internes Kapital besitzt und eine Struktur hat, in der z. B. ein Management die Regeln für menschliche Akteure an den Rändern (z. B. Arbeitnehmer, Lieferanten, Kunden etc.) aufstellt und durchsetzt unter der Beschriftung „Boring old organizations“ verortet. In der rechten Matrix findet sich an derselben Stelle der Eintrag „Forum“, also eine Organisation mit Menschen im Kern und an den Rändern, welche aber kein internes Kapital besitzt (z. B. G8). Eine dezentralisierte Applikation (DA) wird im Gegensatz dazu nicht durch ein Management organisiert, sondern durch Smart Contracts, mit einer unbegrenzte Anzahl von menschlichen Teilnehmern auf allen Seiten eines Marktes und ist nicht notwendigerweise finanziell orientiert. Smart Contracts können in diesem Kontext als eine Art der „dezentralen Automatisierung“ aufgefasst werden. Ein Beispiel dafür ist z. B. BitTorrent. Das System verbindet Menschen miteinander und erlaubt ihnen nach einem bestimmten Protokoll miteinander Dateien dezentral auszutauschen. Eine dezentrale Community (DC) befindet sich in diesem Spektrum zwischen den Extremen eines Forums und einer DA und ist nicht eindeutig umrissen, besitzt aber kein internes Kapital. An dieser Stelle befindet sich nach Buterins Auffassung auf Seite der Organisationsformen mit internem Kapital die dezentrale Organisation (DO). Hier besteht anstatt einer hierarchischen Managementstruktur durch Menschen, welche in Präsenz miteinander

interagieren (z. B. Büro) ein kodifiziertes Protokoll, nach dem eine Gruppe von Menschen dezentral miteinander interagieren, welches über die Blockchain durchgesetzt wird. Allerdings entscheiden die Menschen in einer DO selbst über das weitere Vorgehen und die Aktionen der Organisation.

Buterins Abgrenzungsversuch konzentriert sich daher insbesondere darauf zu erklären was eine DAO nicht ist, um daraus abzuleiten, was als eine DAO anzusehen ist. Sein Versuch einer Abgrenzung ist daher an den folgenden drei Kernaussagen festzumachen:

1. Eine DAO hat (wie DOs) im Gegensatz zu einer DA "internes Kapital".
2. Eine DAO, im Gegensatz zu einer DO, besitzt ein System aus Smart Contracts, welches (nach seiner Implementierung) über sich selbst entscheidet („code is law“).
3. Eine DAO, im Gegensatz zu einer komplett autonomen KI, benötigt die Beteiligung von Menschen, die nach einem durch die DAO spezifizierten Protokoll agieren und Aufgaben übernehmen, welche die DAO nicht selbst ausführen kann.

Die mögliche „feindliche Übernahme“ einer DO und einer DAO ist z. B. möglich, falls ein signifikanter Anteil der Mitglieder miteinander kolludieren. Nach Vitalik Buterins Auffassung ist dieses Ergebnis bei einer DAO als ein Bug (also ein Fehler in den zugrundeliegenden Smart Contracts) anzusehen, bei einer DO hingegen als ein potenziell gewünschtes demokratisches Ergebnis.

Definitionsansätze von DAOs finden sich auch in der wissenschaftlichen Literatur. Hassan & De Filippi (2021) analysieren in ihrer Studie eine Vielzahl unterschiedlicher Begriffsabgrenzungen und Definitionen von DAOs, sowohl aus der Praxis, als auch aus der wissenschaftlichen Literatur. Basierend darauf schlagen die Autoren folgende vereinheitlichte Definition von DAOs vor:

“A DAO is a blockchain-based system that enables people to coordinate and govern themselves mediated by a set of self-executing rules deployed on a public blockchain, and whose governance is decentralised (i.e., independent from central control).” (Hassan & De Filippi, 2021, S.2)

4.2 Ziele von DAOs

Da DAOs im Prinzip als selbstausführender dezentralisierter Koordinations- und Steuerungsmechanismus dienen, können Gruppen von Menschen basierend auf diesem Ansatz unterschiedliche Ziele implementieren und gemeinsam verfolgen. Das Konzept einer DAO ist daher als allgemeine Organisationsform nicht einem bestimmten Einsatzzweck oder -gebiet zuzuordnen.

Bestimmte DAOs bewegen sich dabei sehr nah an der beschriebenen technischen Funktionsweise und werden als reine Protokolle genutzt, beispielsweise um Finanzinvestition zu tätigen und die Erträge unter den Mitgliedern zu verteilen.⁵³ Andere DAOs verfolgen primär philanthropische Ziele, um damit Geld für bestimmte wohltätige Zwecke zu sammeln (z.B. Big Green DAO⁵⁴). Die Mitglieder können in diesen Fällen mit ihren Governance-Token darüber abstimmen, welche Ziele finanziert werden sollen. Andere DAOs wiederum fokussieren sich primär auf den gemeinsamen Erwerb von Sammel- und/oder Kunstobjekten. In Tabelle 4–1 werden einige prominente Beispiel der jüngeren Vergangenheit aufgeführt. Bereits anhand der Eigenbezeichnung einer DAO lässt sich erkennen, dass DAOs nicht

⁵³ <https://milkroad.com/dao>

⁵⁴ <https://medium.com/impact-shakers/philanthropy-daos-the-future-of-giving-608cc7a829b4>

notwendigerweise als langfristig angelegte Organisationen verstanden werden müssen, sondern auch als Vehikel dienen können um gemeinsam kurzfristige und/oder einmalige Ziele zu erreichen.

Tabelle 4–1: Beispiele –DAOs

Spice DAO	kaufte eine seltene Kopie von Jodorowskys "Dune" für 3 Millionen Dollar (MorningBrew, 17. Januar 2022)
City DAO	kaufte 40 Hektar Land in Wyoming, um eine „Blockchain-Stadt“ zu bauen (Vice, 3. November 2021)
Consitution DAO	hat innerhalb einer Woche Ether im Wert von 47 Millionen Dollar gesammelt, um eine seltene Erstausgabe der US-Verfassung bei Sotheby's zu ersteigern - und verloren. (CNBC, 18. November 2021)
Blockbuster-DAO	wollte die Marke Blockbuster [US-amerikanische Videothekenkette] kaufen und als dezentralen Film-Streaming-Dienst wiederbeleben (Business Insider, 27. Dezember 2021)

Quelle: WIK (Einzelnachweise je Zeile)

Die erste DAO wurde „The DAO“ getauft und im April 2016 von einer Gruppe von Programmierern gegründet. Es war das erfolgreichste Investment Crowdfunding zu dieser Zeit und kann als eine Art Hedgefonds betrachtet werden, in dem die Teilnehmer entsprechend ihrem Investment über vorgeschlagene Projekte abstimmen konnten. Allerdings konnte ein Angreifer aufgrund einer Schwachstelle im Code (i.e. Smart Contracts) der DAO einen Teil der Einlagen in eine Tochter-DAO transferieren und damit unter seine Kontrolle bringen (vgl. El Faqir et al., 2020; Hassan & De Filippi, 2021).

The DAO war zu diesem Zeitpunkt das größte Projekt in Ethereum-Netzwerk. Daraufhin entschloss sich die Ethereum Foundation nach Abstimmung aller Netzwerkteilnehmer für einen sogenannten Hard-Fork. Dabei stimmten 89% der Blockchain-Mitglieder von Ethereum für einen Hard-Fork und damit die Rückgabe des erbeuteten internen Kapitals der DAO an seine Mitglieder Ein Hard-Fork bedeutet, dass die Blockchain abgespalten wird und die „fehlerhafte“ Kette von dem Ethereum-Netzwerk nicht mehr akzeptiert wird. Der Rest der Ethereum-Nutzer spaltete sich allerdings ab, und unterstützen weiterhin die bisherige Blockchain.⁵⁵

Durch diese harte Abspaltung wurde das Image der Unveränderlichkeit der DLT stark beschädigt. Insbesondere die Befürworter der ursprünglichen Ethereum-Blockchain argumentieren, dass man mit Fehlern in Smart Contracts und den daraus resultierenden Konsequenzen leben müsse. Dieser Vorfall zeigt damit auch, dass eine Blockchain zwar als praktisch nicht manipulierbar gilt, aber der Konsensus der Netzwerk-Teilnehmer darüber entscheidet, was als eine Manipulation und was als ein zu behebender Fehler angesehen wird.

4.3 Herausforderungen und Potenziale

Im Kontext von DAOs ergeben sich eine Reihe von neuen juristischen, technischen und gesellschaftlichen Herausforderungen, insbesondere wenn die Aktivitäten von DAOs realweltliche Objekte und Aktionen betreffen. Beispielsweise ist in vielen Rechtsräumen noch nicht geklärt, ob DAOs als juristische Personen gelten.

⁵⁵ <https://btcdirect.eu/de-at/hard-fork>

In den USA haben Wyoming (Juli 2021)⁵⁶ und Tennessee (April 2022)⁵⁷ bereits Gesetze erlassen, die DAOs ausdrücklich als juristische Personen anerkennen. Anderenfalls wäre der rechtmäßige Erwerb der in Tabelle 4–1 aufgeführten „City DAO“ gar nicht möglich gewesen. Dabei werden spezifische und zweckgebundene Unternehmensformen geschaffen, in denen eine DAO als eine besondere Art von Gesellschaft, der „DAO LLC“ (Decentralized Autonomous Organization Limited Liability Company), gegründet werden kann. Dies soll eine Unterscheidung bei der Haftung zwischen stimmberechtigten DAO-Mitgliedern (i.e. Halter von Governance-Token) und anderen Inhabern von (Utility-)Token einer DAO erlauben.⁵⁸ Im US-Kongress sind darüber hinaus derzeit zwei überparteiliche Gesetzesvorlagen anhängig, die DAOs als juristische Personen anerkennen und einen Rahmen für deren Regulierung schaffen.⁵⁹ Dabei ist die Umsetzbarkeit vieler steuerrechtlicher Details noch unklar, allerdings wird explizit eine Steuerbefreiung bei DAOs zu Spendenzwecken aufgeführt.

Als weitere DAO-freundliche Länder gelten Malta, die Schweiz, Estland, Hong Kong, die Kaimaninseln und Gibraltar.⁶⁰ Auf EU-Ebene ist der Status von DAOs rechtlich noch nicht einheitlich geregelt.

Zusätzlich zu juristischen Herausforderungen identifizieren Wang et al. (2019) noch Sicherheitsprobleme und technische Beschränkungen als Herausforderungen für DAOs. Als häufige Sicherheits-Schwachstellen werden von den Autoren rekursive Aufrufe, Transaktionsreihenfolge-Abhängigkeit (TOD), Zeitstempel-Abhängigkeit und falsch behandelte Ausnahmen genannt. Aber auch technische Beschränkungen stellen nach Auffassung von Wang et al. (2019) eine Herausforderung dar. Dabei weisen die Autoren insbesondere darauf hin, dass eine „...große semantische Lücke zwischen gesetzlichen Regeln (bekannt als „wet code“) und den Regeln in intelligenten Verträgen („dry code“) bestehe“ (Wang et al. 2019, S. 876). Smart Contracts erfordern dabei einen semantisch expliziten Code in einer formalen Computersprache. Dabei sei es schwierig z.B. Randfälle in diesen Code zu übersetzen, was die Praktikabilität von DAOs einschränke.

⁵⁶ <https://en.cryptonomist.ch/2022/10/13/defi-mica-another-missed-opportunity>

⁵⁷ <https://www.crowdfundinsider.com/2022/05/191038-tennessee-follows-wyoming-to-become-second-state-to-recognize-daos/>

⁵⁸ <https://en.cryptonomist.ch/2022/10/13/defi-mica-another-missed-opportunity>

⁵⁹ <https://www.step.toe.com/en/news-publications/new-bipartisan-senate-legislation-seeks-to-address-cryptocurrency-and-digital-asset-tax-issues.html>

⁶⁰ <https://www.code2.io/blog/web3-dao-friendly-countries/>
<https://nomoretax.eu/legal-aspects-of-decentralized-autonomous-organisations-daos/>

5 Schlussfolgerungen & Ausblick

Die Krypto-Ökonomie durchläuft nach dem Zusammenbruch mehrerer Krypto-Börsen aus dem CeFi-Bereich aktuell eine schwierige Phase. Allerdings zeigen vergleichbare Fälle aus der Vergangenheit, dass sich der Krypto-Markt voraussichtlich auch davon wieder erholen wird. Viele der Vorfälle sind auf die Struktur und Intransparenz von profitorientierten CeFi-Spielern zurückzuführen, die ein sehr schnelles Wachstum erfahren haben und Macht in den Händen weniger Akteure bündeln. Dabei ist es fraglich, ob der DeFi-Ansatz vor vergleichbaren Problemen schützen kann, da auch hier Konzentrationstendenzen zu erwarten sind.⁶¹ Auch die Zugangshürden für nicht-technikaffine Marktteilnehmer sind derzeit noch als hoch einzuschätzen.

Die Krypto-Industrie steht dabei in der EU mit den MiCA/AML-Verordnungen ab 2023 vor neuen Herausforderungen. Dieser regulatorische Rahmen bietet der Branche aber gleichzeitig die Gelegenheit zu reifen, was sich langfristig positiv auf die Marktdurchdringung auswirken könnte. NFTs werden bisher allerdings von der MiCA-Verordnung nicht unmittelbar erfasst. Die Kommission wird den Sektor aber gesondert untersuchen und bei Bedarf einen Regulierungsrahmen dafür entwickeln. Sämtliche Kryptowertetransfers hingegen werden zukünftig von der AML-Verordnung abgedeckt. Dies kann dazu führen, dass der Markt transparenter wird und damit auch das Potenzial von NFTs zu illegalen Zwecken abnimmt. Da die Krypto-Branche allgemein als sehr spekulativ und volatil gilt, könnte auch das NFT-Segment von einem entsprechenden weiterführenden Regulierungsrahmen profitieren. Insbesondere das Potenzial von NFTs für die Kreativwirtschaft ist als groß einzuschätzen.

Der Einfluss des „Proof-of-Work“-Ansatzes auf die Umwelt wird von der Europäischen Kommission ebenfalls gesondert untersucht werden. Mit dem „Proof-of-Stake“-Ansatz existiert jedoch bereits ein erheblich weniger ressourcenintensiver Ansatz. Ethereum hat Proof-of-Stake bereits implementiert und seine Netzwerkumstellung auf diesen Ansatz erfolgreich durchlaufen.⁶² Allerdings haben auch geschlossene / zugangsbeschränkte Proof-of-Work-basierte DLT-Netzwerke einen geringeren Stromverbrauch als öffentliche DLT-Netze, übertreffen aber weiterhin den Stromverbrauch zentraler Architekturen (Sedlmeir et al. 2020).

Der Status von DAOs muss in vielen Ländern und auf EU-Ebene noch geklärt werden. Beispiele aus dem Ausland zeigen, dass Konstruktionen möglich sind mit denen DAOs als juristische Person in Erscheinung treten können. Neben technischen Restriktionen und Sicherheitsbedenken schränkt dieser Aspekt die Attraktivität von DAOs derzeit deutlich ein und macht diese Organisationsform für bestimmte Zwecke sogar impraktikabel. Es bleibt abzuwarten, ob ein geregelter rechtlicher Status von DAOs, welcher dieser Organisationsform auch in der EU weitere Möglichkeiten eröffnen könnte, tatsächlich zu einer weiteren Verbreitung von DAOs führen wird, da hiermit auch die Durchsetzbarkeit von Pflichten einhergehen wird (z.B. Steuerpflicht). Hinzu kommt die Frage, welcher Grad an strategischer und juristischer Komplexität in der Praxis zukünftig tatsächlich über Smart Contracts („dry code“) abgebildet werden kann.

⁶¹ <https://mitsloan.mit.edu/ideas-made-to-matter/decentralized-finance-4-challenges-to-consider>

⁶² <https://www.forbes.com/sites/qai/2022/09/27/proof-of-stake-will-the-ethereum-merge-really-lead-to-a-rally>

Literaturverzeichnis

- Aharon, D. Y., & Demir, E. (2022). NFTs and asset class spillovers: Lessons from the period around the COVID-19 pandemic. *Finance Research Letters*, 47, 102515.
- Buterin, V. (2014). DAOs, DACs, DAs and More: An Incomplete Terminology Guide. *Ethereum Foundation Blog*. 2014, May 6. <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> (Abgerufen am 22.12.2022)
- Chalmers, D., Fisch, C., Matthews, R., Quinn, W., & Recker, J. (2022). Beyond the bubble: Will NFTs and digital proof of ownership empower creative industry entrepreneurs?. *Journal of Business Venturing Insights*, 17, e00309.
- Dune Analytics (2022). Number of unique addresses that either bought or sold a Decentralized Finance (DeFi) asset worldwide from December 2017 to July 4, 2022 [Graph]. In Statista. <https://www.statista.com/statistics/1297745/defi-user-number/> (Abgerufen am 14.12.2022)
- El Faqir, Y., Arroyo, J., & Hassan, S. (2020). An overview of decentralized autonomous organizations on the blockchain. In *Proceedings of the 16th international symposium on open collaboration* (pp. 1-8).
- Fairfield, J. A. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*, 97, 1261.
- Hassan, S., & De Filippi, P. (2021). Decentralized autonomous organization. *Internet Policy Review*, 10(2), 1-10.
- Johnston, D., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., Wilkinson, S. & Mason, S. (2014). The General Theory of Decentralized Applications, DApps. <https://github.com/DavidJohnstonCEO/DecentralizedApplications> (Abgerufen am 22.12.2022)
- Katopodi, E. (2021). Blockchain Market: Regulatory Concerns Arising From The 'Diem' Example In The Field Of Free Competition. *EU and Comparative Law Issues and Challenges Series (ECLIC)*, 5, 197–216.
- Moringiello, J. M., & Odinet, C. K. (2022). The property law of tokens. *Florida Law Review*, 74, 607.
- Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L. M., & Baronchelli, A. (2021). Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific reports*, 11(1), 1-11.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, October.
- Peterson, T. (2018). Metcalfe's Law as a Model for Bitcoin's Value. *Alternative Investment Analyst Review Q*, 2.
- Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: Beyond myth. *Business & Information Systems Engineering*, 62(6), 599-608.
- Statista (2022a). Value of sales involving a non-fungible token (NFT) in gaming, art, sports and other segments from 2018 to 2021 (in million U.S. dollars). January 11, 2022. In Statista. <https://www.statista.com/statistics/1221400/nft-sales-revenue-by-segment/> (Abgerufen am 18.12.2022)
- Statista (2022). Overall cryptocurrency market capitalization per week from July 2010 to November 2022 (in billion U.S. dollars) [Graph]. November 14, 2022. In Statista. <https://www.statista.com/statistics/730876/cryptocurrency-market-value/> (Abgerufen am 14.12.2022)
- Stylianou, K., & Carter, N. (2020). The Size of the Crypto Economy: Calculating Market Shares of Cryptoassets, Exchanges and Mining Pools. *Journal of Competition Law & Economics*, 16(4), 511-551.
- Szabo, N. (1996). Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought*, (16), 18(2), 28.
- Umar, Z., Alwahedi, W., Zaremba, A., & Vo, X. V. (2022). Return and volatility connectedness of the non-fungible tokens segments. *Journal of Behavioral and Experimental Finance*, 35, 100692.
- Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L., & Wang, F. Y. (2019). Decentralized autonomous organizations: Concept, model, and applications. *IEEE Transactions on Computational Social Systems*, 6(5), 870-878.
- Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447.
- Yilmaz, M., Hacıoğlu, T., Clarke, P. (2022). Examining the Use of Non-fungible Tokens (NFTs) as a Trading Mechanism for the Metaverse. In: Yilmaz, M., Clarke, P., Messnarz, R., Wöran, B. (eds) *Systems, Software and Services Process Improvement. EuroSPI 2022. Communications in Computer and Information Science*, vol. 1646. Springer, Cham.