Hochschule Neu-Ulm
University of Applied Sciences

Bachelorarbeit

im Bachelorstudiengang

Betriebswirtschaft

an der Hochschule für angewandte Wissenschaften Neu-Ulm

Einsatz von Kryptowährungen für wirtschaftskriminelle Vorhaben

Erstkorrektor/-in: Prof.Dr.Elmar Steurer

Betreuer/-in: Prof.Dr.Erik Rederer

Verfasser/-in: Esra Aksoy (Matrikel-Nr.: 253955)

Thema erhalten: 13.11.2022

Arbeit abgegeben: 13.03.2023

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

Vgl……Vergleiche

Bspw……beispielsweise

RDP……Remote Desktop Protocoll

FOMO……..Fear of missing out

GWG……Geldwäschegesetz

NFT……..Nicht fungible Token

AML……..Anti money laundering

KYC……..Know your customer

VPN……..Virtual private network

TOR……..The onion router

GASO……..Global anti scam organisation

POW……Proof of work

POS…… Proof of Stake

1 Einleitung

"The first generation of the digital revolution brought us the Internet of information. The second generation-powered by Blockchain technology-is bringing us the Internet of value: a new, distributed platform that can help us reshape the world of business and transform the old order of human affairs for the better." Don Tapscott[1]

Die Gesellschaft unterliegt gegenwärtig vielen disruptiven Technologien, welche die digitale Transformation vorantreiben. So macht beispielsweise Don Tapscott mit dem oben aufgeführten Zitat auf das aktuelle Potential der Digitalisierung aufmerksam[2].

Als Ende der 80er Jahre das World Wide Web entstand, ahnte niemand, wie sehr diese neue Technologie alle Lebensbereiche der Menschen umgestalten und revolutionieren würde. Zunächst war das Internet auf den digitalen Datenaustausch ausgerichtet. Heute sind die Anwendungsmöglichkeiten nahezu unbegrenzt[3].

Einhergehend mit der Entwicklung des Internets ist seit 15 Jahren eine neue Technologie in der Finanzwelt im Einsatz. Mit der Gründung der bisher ersten Kryptowährung Bitcoin 2009, wurde die Grundlage für ein Netzwerk gebildet, dessen Ausmaß damals kaum vorstellbar war. Wirtschaftsexperten zufolge wurde dadurch die zweite Generation der digitalen Revolution eingeleitet. Die Rede ist von der Blockchain-Technologie, einer dezentralisierten, transparenten und kryptographisch sicheren Datenverwaltung. Diese Technologie ist die Grundlage für ein Internet der Werte, in dem die Übertragung von Daten aller Art von einer Person zur anderen nahezu in Echtzeit möglich ist[4].

Basierend auf den Fortschritten des Internets, haben die Entwicklungen in der Finanzwelt in den letzten Jahren einen maßgeblichen Umschwung verzeichnet. In diesem Zusammenhang wird der Blockchain-Technologie ein disruptives Potential zugesprochen. Mit dem Aufkommen der digitalen Währung Bitcoin haben sich immer mehr Finanzinstitute mit dem Thema auseinandergesetzt und Anwendungen für den eigenen Markt gefunden. Zwar wurde ein Großteil der Finanzsysteme an die neuen Gegebenheiten der Digitalisierung angepasst, jedoch bestehen nach wie vor gravierende

[1] *Tapscott* (2022).
[2] Vgl.*Tapscott* (2022).
[3] Vgl.*Hofbauer* (2022).
[4] Vgl.*Hofbauer* (2022).

Schwächen, die diese Systeme undurchschaubar und aufgrund der Verantwortung einer zentralen Instanz sicherheitsgefährdend machen[5].

1.1 Problemstellung und Relevanz des Themas

Mit dem Aufkommen des Internets wurde es möglich, eine Vielzahl von bis dahin umständliche und langwierige Prozesse flexibel und einfach abzuwickeln. Durch die Vernetzung wurde die Möglichkeit geschaffen, Informationen massenhaft zu übertragen. Die Anonymität im World Wide Web ist in den letzten Jahren parallel zur Menge der übertragenen Daten rasant gestiegen. Zwei Parteien können Verträge verhandeln, ohne sich je zu begegnen. Seitdem Verträge auf Knopfdruck abgeschlossen werden, wurde eine Sicherheitslücke für Betrug und Manipulation geöffnet. Durch neue Technologien werden Transaktionen ohne Vertrauensbasis bei gleichzeitiger Vertragstransparenz ermöglicht[6].

Zu Beginn war Bitcoin als erste Kryptowährung nur eine Idee, um zu testen, ob eine digitale und dezentrale Währung von der Bevölkerung angenommen wird. Doch bald darauf stellte sich heraus, dass Bitcoin ein leistungsfähiger Ansatz ist, welcher enorme Entwicklungspotentiale nach sich zieht. Im Januar 2009 begann die praktische Umsetzung der Kryptowährung Bitcoin mit dem Ziel, eine virtuelle Währung zu erschaffen, die ohne die Hilfe einer zentralen Instanz erzeugt und gehandelt werden kann. Die grundlegende Intention der Entwickler war das Errichten eines dezentralen Geldsystems, welches ohne Zentralbanken und Geschäftsbanken auskommt, da deren Glaubwürdigkeit während der Finanzkrise von 2008 stark gelitten hatte. Die Blockchain-Technologie, die dem Bitcoin zugrunde liegt, hat zu einer Vielzahl weiterer Anwendungen und gleichzeitig zur Entstehung neuer Kryptowährungen geführt. Parallel zu den neuen Entwicklungen wurden auch immer mehr mögliche Schwachstellen der Kryptowährungen offengelegt. Dennoch stieg die Marktkapitalisierung in den letzten Jahren stetig an, sodass virtuelle Währungen weiter an Bedeutung und Bekanntheit gewinnen.

Als diese Währungen, insbesondere der Bitcoin, stark an Wert gewannen, fingen auch „normale“ Anleger an, sich für sie zu interessieren und sahen in den Kryptowährungen

[5] Vgl.*Schmlechen* (2019).
[6] Vgl.*Weise* (2019).

nicht nur ein reines Zahlungsmedium, sondern eine neuartige Vermögensanlage mit unerwartet hohen Renditechancen. Die ursprüngliche Absicht war es jedoch Kryptowährungen als alternatives Zahlungsmittel einzuführen. Doch bis heute konnten sich Kryptocoins nicht als gesetzliche Währung etablieren. Stattdessen wurden aus Kryptowährungen ein großes Business an Spekulationsobjekten. Trotz der enormen Kursschwankungen nutzen heute viele Menschen Kryptowährungen als Investitionsmöglichkeit. Zukunftsperspektivisch betrachtet, versprechen Anlagemöglichkeiten auf dem Gebiet der virtuellen Währung, den Investoren einen effizienten Nutzen. Jedoch geht das Anlegen von Digitalgeld auch mit gewissen Risiken und Gefahren einher, weshalb die zunehmende Kryptonutzung auch mit Zweifeln behaftet ist. Dies ist insbesondere auf die Zunahme der Kriminalität im Bezug auf den wachsenden Einsatz von Kryptowährungen zurückzuführen[7].

Trotz der möglichen Chancen betrachten Kritiker das Konzept des virtuellen Anlegens als kritisch, weshalb die Frage aufgeworfen wird: Welche wesentlichen Risiken verbergen sich hinter der zunehmenden Nutzung von Kryptowährungen? Der rasante Kursverlauf sowie die hohe Anzahl an unterschiedlichen Kryptowährungen und das zunehmende Interesse bei Anlegern, einschließlich des hierbei investierten Kapitals, führt dazu, dass neue Nutzer den Überblick verlieren. Eine zunehmende Anzahl von Neuanlegern hat bei vielen Unternehmern und darunter auch Betrügern das Interesse geweckt, Kapital aus der Unerfahrenheit der Nutzer zu schlagen. In diesem Kontext haben sich neue Geschäftszweige und Unternehmen im Hinblick auf Kryptowährungen etabliert. Dazu gehören Kryptowährungsbörsen und Bezahlsysteme, die es ermöglichen, mit Kryptowährungen zu handeln und mit ihnen zu bezahlen. Zudem ist es auch Privatpersonen zugänglich, ihre eigene Kryptowährung zu generieren. Einhergehend mit diesen Innovationen kursierten jüngst immer mehr Skandale in den Medien, bei welchen milliardengroße Geldmengen von Nutzern gestohlen wurden. Solche Vorfälle rufen in der Öffentlichkeit Skepsis hervor, weshalb die Potentiale und Gefahren der Technologie weiterhin im Mittelpunkt der Debatten stehen.

Es sind die grundlegenden Wesenszüge von Blockchain, welche gewisse Nischen für Kriminalität offerieren.

[7] Vgl.*Schmlechen* (2019).

So braucht es zum Beispiel zur Erzeugung von Kryptowährungen keine materiellen Ressourcen wie Metall, Plastik oder Papier. Für die Nutzung von Kryptowährungen wird lediglich Strom in Form von Rechenleistung benötigt. Darüber hinaus sind virtuelle Währungsformen einfach handzuhaben und zu übertragen. Sie werden nicht von einer Regierung ausgegeben und sind damit, zumindest prinzipiell, immun gegenüber staatlicher Beeinflussung. Genau diese Gegebenheiten bilden die perfekte Grundlage, um dieses System für inkrementelle Methoden des Betrugs auszunutzen. Denn statt der Nutzung als legales Zahlungsmittel werden vermehrt Kryptowährungen für internationale illegale Transaktionen, Betrug und vor allem zum Zwecke der Geldwäsche eingesetzt. Diese Gegebenheiten der Anonymität und der Wegfall von staatlicher Kontrolle bieten Kriminellen Raum, um ihre illegalen Aktivitäten und Geldwäschetransaktionen auszuleben, oftmals sogar ohne Konsequenzen[8].

In Anbetracht der oben formulierten Problemstellung resultiert auch die Relevanz zur Erarbeitung des angestrebten Themas. Das der wissenschaftlichen Arbeit zugrunde liegende Interesse umfasst die durch die fortschreitende Digitalisierung hervorgerufene Transformation der Finanzsysteme, die eine neuartige Ökonomie mit sich bringt. Diese verspricht durch die zunehmende Nutzung von Kryptowährungen neue Potentiale. Jedoch ist das Konzept der Blockchain-Technologie auch mit gewissen Gefahren und Kontroversen konnotiert, weshalb Aspekte in puncto Kriminalität weiterhin strittig sind.

1.2 Zielsetzung und Forschungsfrage

Dass der ökonomische und soziale Schaden durch die strafrechtliche, relevante Benutzung von Kryptowährungen ganz erheblich sein kann, wurde durch aktuelle Fälle belegt. Es sind massenhafte kriminelle Skandale im Einsatz mit Kryptowährungen aufgekommen.

So ergibt sich die Relevanz der Thematik hauptsächlich aus der Aktualität der beschriebenen Sachlage sowie aus den vorherrschenden Kontroversen in Bezug auf die Gefahren von kriminellen Aktivitäten im Kontext von Kryptowährungen, die es zu

[8] Vgl.*Chainanalysis* (2023).

klären gilt. Ebenso persönliches Interesse prägt die Auswahl des Themas, wie auch die Ausrichtung und Herangehensweise der Arbeit, entscheidend mit.

Die grundlegende Intention der angestrebten Ausarbeitung liegt darin, aktuelle Einflüsse von Kryptowährungen im Hinblick auf wirtschaftskriminelle Vorhaben aufzuzeigen. Zu diesem Zweck ist die wissenschaftliche Arbeit bemüht, die Möglichkeiten und Risiken von Digitalwährungen im Kontext von unrechtmäßigen Aktivitäten zu analysieren. Demnach besteht die Zielsetzung zum einen darin, den Status quo sowie Kontroversen bezüglich Kryptowährungen aufzudecken und herauszuarbeiten, inwieweit die Kriminalität in diesem Bereich vollzogen wird bzw. was die maßgeblichsten Diskussionspunkte hinsichtlich der Risiken sind. Im Zuge dessen soll die wesentliche Bedeutung und Entwicklung von Blockchain-Technologien betrachtet sowie aktuelle Fallbeispiele in diesem Zusammenhang aufgegriffen werden.

Das Forschungsinteresse basiert auf einer wesentlichen Hauptforschungsfrage sowie Leitfragen, dessen Beantwortung als Ziel der Arbeit definiert wird. Die Intention hierbei liegt zum einen darin, den Einfluss der Kryptowährung auf die vorab formulierte Forschungsfrage darzustellen und zum anderen grundsätzliche Aspekte in diesem Kontext zu erarbeiten, die im Hinblick auf die Ausarbeitung des Themas relevant sind. Vor diesem Hintergrund lautet die für die Untersuchung grundlegende Forschungsfrage:

Wie beeinflusst der Einsatz von Kryptowährungen die Effektivität und Durchführbarkeit von wirtschaftskriminellen Vorhaben wie Geldwäsche, Betrug und Cyberkriminalität?

Abgeleitet aus der Hauptfragestellung sowie der vorab definierten Zielsetzung, wird sich die Arbeit mit den folgenden Leitfragen befassen und versuchen eine möglichst umfassende Beantwortung darzulegen:

1. Welche Arten von wirtschaftskriminellen Handlungen werden typischerweise mithilfe von Kryptowährungen begangen?
2. Welche Vorteile bieten Kryptowährungen im Vergleich zu traditionellen Zahlungsmethoden für wirtschaftskriminelle Aktivitäten?
3. Wie können Kryptowährungen genutzt werden, um wirtschaftskriminelle Aktivitäten zu verschleiern oder zu erleichtern?

4. Welche Herausforderungen und Risiken gibt es bei der Bekämpfung von wirtschaftskriminellen Aktivitäten, die Kryptowährungen nutzen?
5. Welche Maßnahmen können ergriffen werden, um den Missbrauch von Kryptowährungen für wirtschaftskriminelle Zwecke zu verhindern oder zu verringern?

Das grundlegende Ziel dieser Untersuchung besteht darin, Erkenntnisse im Hinblick auf den Einsatz von Kryptowährungen zu gewinnen, die Ansätze zur Verbesserung der Prävention und Bekämpfung von wirtschaftskriminellen Aktivitäten schaffen können.

1.3 Aufbau der Arbeit und Methodik

Folgend wird die Kapitelstruktur der wissenschaftlichen Arbeit dargestellt. Wie oben bereits dargelegt, wird sich die angestrebte Ausarbeitung um eine Annäherung an die vorab formulierten Forschungs-/Leitfragen bemühen und sich mit dem Thema Kryptowährung sowie dessen Bezug zur Wirtschaftskriminalität befassen. Hierzu gliedert sich die Arbeit in zehn Abschnitte.

Der erste Teil der Arbeit wird sich in mehreren Unterkapiteln mit theoretischen Grundlagen der Kryptowährungen und für das Verständnis wesentlichen Begrifflichkeiten auseinandersetzen. Um sich der Materie zu nähern, werden zunächst zentrale Definitionen getätigt und die wesentlichen Zusammenhänge für ein besseres Verständnis aufgezeigt. Um zu definieren, welche Wesensmerkmale und Kerntechnologien der Blockchain innewohnen, wird vorab die elementare Bedeutung der Kryptowährung begrifflich abgegrenzt und darauf aufbauend die Kernpunkte der Funktionsweise herausgearbeitet.

Im Fokus des zweiten Kapitels steht die Entwicklung der Kryptowährungen, dazu wird die Entstehung und die Nachfrage nach kryptobasierten Vermögengegenständen beschrieben sowie die Schwachstellen der Blockchain aufgezeigt. Schließlich wird der Status quo anhand eines praxisnahen Fallbeispiels erläutert.

Basierend auf den vorab gewonnenen Erkenntnissen wird im Anschluss auf die Arten der Kryptokriminalität, wie etwa die Geldwäsche, Cyberkriminalität und Terrorismusfinanzierung, eingegangen.

Daran schließt sich eine Betrachtung der kryptobasierten Geldwäscheprozesse und dessen Eignung durch Eigenschaften der Kryptowährungen an. Abgerundet wird diese Analyse mit Warnsignalen der Krypto-Geldwäsche. Anschließend wird der Einsatz von Kryptowährungen zur Geldwäsche mithilfe des Drei-Phasen-Modells erläutert. Als nächstes wird das Thema des Krypto-Betrugs aufgezeigt und mit den verschiedenen Betrugsarten belegt. In diesem Zusammenhang folgt ein weiteres Fallbeispiel. Abschließend wird geprüft, welche Mittel und Methoden im Bereich der Kryptokriminalität eingesetzt werden.

Die letzten zwei Abschnitte beinhalten Möglichkeiten der Aufdeckung der im Verlauf der Arbeit aufgezeigten Kriminalitätsaktivitäten und deren strafrechtliche Regulierung.

Im letzten Teil erfolgt eine Schlussbetrachtung aus den Erkenntnissen der gesamten Untersuchung, bei welchem die Kernaspekte der Arbeit reflektiert und evaluiert werden. Hierzu komplettiert ein Fazit die wissenschaftliche Arbeit.

Um die Forschungsfrage sowie die darauf aufbauenden Leitfragen adäquat beantworten zu können, ist die Literaturrecherche eine essenzielle Herangehensweise. Die vorliegende wissenschaftliche Ausarbeitung verbleibt bei einer rein theoretischen Darlegung in Form einer Literaturarbeit und liefert Einblicke in praxisnahe Fallbeispiele. So wird eine klassische Recherchearbeit in Fachliteratur, Fachzeitschriften, wissenschaftlichen Publikationen, Berichten von Studien sowie im Internet betrieben, um nötige Informationen aus bereits vorangegangenen Forschungen zu generieren. Um relevante Studien und wissenschaftliche Beiträge zu erfassen, werden unter anderem digitale Bibliotheken (z. B. IEEE, ScienceDirect und Springer Link) sowie gängige Suchmaschinen für bibliografische Datenbanken (z. B. Google Scholar) herangezogen.

Das aus Gründen der besseren Lesbarkeit hauptsächlich verwendete generische Maskulin schließt gleichermaßen weibliche und männliche Personen ein. Wenn also beispielsweise von Nutzern gesprochen wird, sind damit auch Nutzerinnen gemeint, es sei denn das Geschlecht wird explizit hervorgehoben.

2 Theoretische Grundlagen

Einhergehend mit der digitalen Revolution, werden Kryptowährungen immer mehr zur Schlüsselkomponente des heutigen Finanzsystems. Gegenwärtig ist das Anwendungsspektrum von virtuellen Währungsformen umfangreich. Fortschritte auf dem Gebiet schufen nicht nur Raum für alternative Digitalwährungen, sondern ebneten auch den Weg für rechtswidrige Aktivitäten. Dies vertiefend, sind die nachfolgenden Unterkapitel bemüht, die wesentlichen Kernpunkte bezüglich Kryptowährungen aufzuarbeiten. Um der vorliegenden Arbeit eine Einleitung zu geben, werden vorab theoretische Begrifflichkeiten aufgeschlüsselt und im weiteren Verlauf die Funktionalität untersucht[9].

2.1 Definition Kryptowerte

Nach der Finanzkrise 2008 werden Krypto-Vermögenswerte von der EZB seit 2018 als eine neue Art von Vermögenswerten definiert, die in digitaler Form aufgezeichnet und durch Kryptografie ermöglicht werden[10].

Der Begriff der Kryptowerte bezieht sich in der Legaldefinition nach der Geldwäscherichtlinie Art.3 Nr.18 auf den Ausdruck der „virtuellen Währung“ und wird in §1 Abs. 11 S.1 Nr.10 KWG wie folgt definiert: „[…] eine digitale Darstellung eines Werts, die von keiner Zentralbank oder öffentlichen Stelle emittiert wurde,[…], und die nicht den gesetzlichen Status einer Währung oder von Geld besitzt, aber von natürlichen oder juristischen Personen als Tauschmittel akzeptiert wird und die auf elektronischem Wege übertragen, gespeichert und gehandelt werden kann.“[11]

Kryptowerte stellen eine Sammelbezeichnung für alle digitalen Vermögenswerte dar. Dazu gehören die Finanzinstrumente wie Kryptowährungen, sogenannte „Tokens“ oder „Coins“, die auf einer Blockchain wiedergegeben werden. Hierbei sollen Token ein Wirtschaftsgut und Coins digitale Münzen verkörpern. Sie repräsentieren lediglich digitalisierte Werte, die von keiner Zentralbankstelle oder öffentlichen Institution

[9] Vgl.*Bussac* (2019), S. 16.
[10] Vgl.*Chimienti* et al. (2019).
[11] *BaFin* (2020).

ausgegeben oder garantiert werden. Den rechtlichen Status einer Währung oder Geldeinheit haben sie daher noch nicht [12].

Der Fokus liegt dabei hauptsächlich auf den regulatorischen, wirtschaftlichen und geschäftlichen Aspekten und nicht auf der Nutzung von Technologien. Da ein Krypto-Wert keine finanzielle Forderung oder Verbindlichkeit an eine identifizierbare Einheit darstellt, basiert sein Wert nur auf der Erwartung, dass andere Nutzer bereit sind, in der Zukunft dafür zu zahlen, und nicht auf einem künftigen Cashflow, auf den die Nutzer ihre Erwartungen stützen können[13].

2.2 Definition und Bedeutung von Kryptowährungen

Das Wort Kryptowährung fügt sich aus den beiden Begriffen Kryptographie und Währung zusammen. Die Kryptographie ist die Wissenschaft der Datenverschlüsselung und eine Währung erfüllt die Aufgaben eines Zahlungsmittels, einer Recheneinheit und des Wertaufbewahrungsmittels[14]. Werden Bestandteile dieser Erklärungen zusammengesetzt, ergibt sich folgende Definition für Kryptowährungen: „Kryptowährungen sind digitale Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem."[15]

Somit stellen Kryptowährungen, auch virtuelle Währungen genannt, einen Sammelbegriff für Blockchain-basierte Zahlungsmittel dar, die durch die starke Verschlüsselungstechnologie gesichert werden und im Gegensatz zu bei den bisher bekannten Zahlungsmitteln typischerweise dezentral organisiert sind[16]. Anders als bei dem bisher verwendeten Buch- und Fiatgeld werden Kryptowährungen nicht von der Regierung geschaffen, sondern werden von nichtregulierenden Einrichtungen oder einem Computernetzwerk erzeugt. Kryptowährungen bilden einen dezentralen Finanzkreislauf, der ohne Zwischenschaltung von Aufsichtsbehörden oder Kreditinstituten funktioniert. Es kann daher auch keine Geldpolitik betrieben werden, da die Krypto-Geldmenge unabhängig von allen bestehenden wirtschaftlichen Gegebenheiten der Zentralbanken

[12] Vgl. *Chimienti* et al. (2019).
[13] Vgl.*Chimienti* et al. (2019).
[14] Vgl.*Bussac* (2019), S. 14–16.
[15] *Bendel* (2018).
[16] Vgl.*Heinze/Protschka* (2018), S. 67.

ist [17]. Die starke Verschlüsselung, die hohe Transparenz und Dezentralität gewährleisten die „Sicherheit“ der Kryptowährungen und bilden somit eine Grundlage für das Vertrauen der Nutzer in das Blockchain – Netzwerk[18].

Izzo-Wagner und Siering zufolge ist der Wert von Kryptowährungen nicht "intrinsisch" und vom Markt abhängig. Hierbei spielt es eine wesentliche Rolle, ob und von wie vielen Nutzern die Digitalwährung als Bezahl- oder Tauschmittel angenommen wird[19]. Der Gedanke hinter der Erfindung von Kryptowährungen war es eine virtuelle Zahlungsmethode für Kaufgeschäfte zu entwerfen und somit eine Alternative bei Transaktionen über das Internet zu haben, die durchgeführt werden können, ohne einen dritten überwachenden Beteiligten und nicht rückgängig gemacht werden können[20].

Dieser Ansatz wurde jedoch kaum genutzt, da bislang "noch keine Kryptowährung im Rechtsverkehr als Universaltausch- oder Zahlmittel" genügend verbreitet ist. Derzeit fungieren Kryptowährungen hauptsächlich als Spekulations- und Investitionsobjekt[21].

2.3 Funktionsweise

2.3.1 Blockchain-Technologie

Die Grundlage für das gesamte Kryptowährungs-System beruht auf der Blockchain-Technologie, dass sozusagen das Hauptverzeichnis des Kryptowährungssystems darstellt.[22] Die Blockchain ist eine Datenbank, die über ein etabliertes Netzwerk von Computersystemen verteilt wird und zur Speicherung sowie Aufzeichnung von Transaktionen dient. Diese Datenbank speichert alle Informationen über Transaktionen, die seit der Generierung der Blockchain ausgeführt wurden[23]. Das erste Mal wurde die Blockchain-Technologie von der ersten und bekanntesten Kryptowährung Bitcoin erfolgreich implementiert[24].

[17] Vgl.*Izzo-Wagner/Siering* (2020), S. 2.
[18] Vgl.*Soeteman* (2019), S. 37.
[19] Vgl.*Izzo-Wagner/Siering* (2020).
[20] Vgl.*Soeteman* (2019), S. 30–32.
[21] *Izzo-Wagner/Siering* (2020), S. 2.
[22] Vgl.*SCHMIDT* (2019), S. 2.
[23] Vgl.*Grzywotz* (2019), S. 31.
[24] Vgl.*Brünnler* (2018), S. 5.

Alle Transaktionen, die mit der zugehörigen Währung in einem bestimmten Zeitraum getätigt wurden, werden in Form von Blöcken gespeichert. Die Blockchain ist, wie dem Namen entnommen werden kann, eine ständig wachsende Verkettung solcher Blöcke mit Daten. Die Gesamtheit der Blöcke bildet die Blockchain[25].

Die Struktur und Entwicklung der Blockchain ergeben sich somit aus dem folgenden Prozedere. Jeder Block auf der Kette enthält mehrere Transaktionen und sobald eine neue Transaktion auf der Blockchain stattfindet, wird eine Aufzeichnung dieser erstellt.[26] Mithilfe eines kryptographischen Verfahrens werden diese Blöcke verkettet und können nachträglich nicht verändert oder manipuliert werden, wodurch die Integrität der Daten gewährleistet wird.[27] Die Blockchain-Datei ist transparent und für alle Netzwerknutzer verfügbar und aktualisiert sich bei Hinzufügen neuer Transaktionen dezentral auf allen im Netzwerk verwendeten Rechnern fort. Darin liegt die besondere Eigenschaft der Blockchain, denn durch den Verzicht auf eine zentrale Datenbank, die gehackt werden könnte, ist die Blockchain im Grunde manipulationssicher[28].

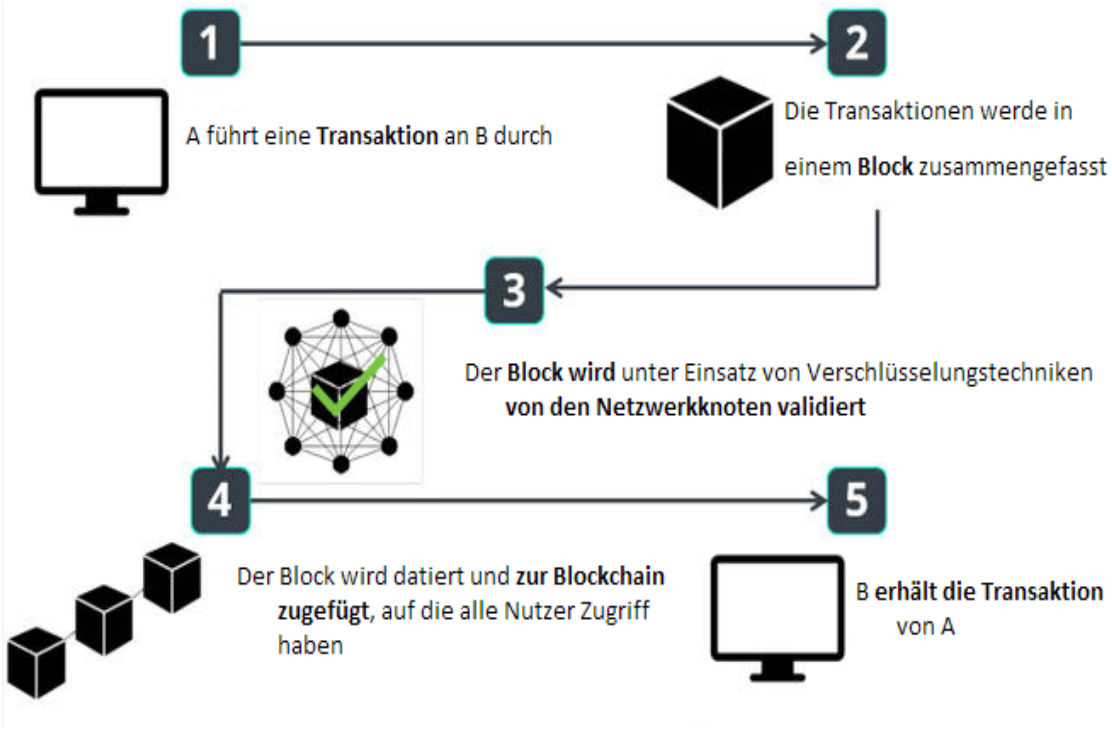


Abbildung 1: Funktionsweise der Blockchain[29]

[25] Vgl.*SCHMIDT* (2019), S. 2.
[26] Vgl.*Grzywotz* (2019), S. 31.
[27] Vgl.*Bundesamt für Sicherheit in der Informationstechnik* (2022).
[28] Vgl.*Soeteman* (2019), S. 31.
[29] Vgl.*Central Charts*.

Doch trotz der Manipulationssicherheit der Blockchain ergeben sich genau aus dem Grund der fehlenden zentralen Instanz Möglichkeiten für Kriminelle, die Blockchain für ihre eigenen Zwecke zu nutzen.

2.3.2 Ablauf von Transaktionen

Transaktionen, welche über die Blockchain ablaufen, funktionieren mithilfe von Computer- Codes. Für die Verwendung des Krypto-Systems wird zunächst für jeden Nutzer jeweils ein privater und ein öffentlicher Schlüssel, aus zufällig gebildeten Zahlen- und Buchstabenkombinationen, generiert[30]. Der private Schlüssel ist nur dem Nutzer allein zugänglich, er fungiert als Passwort und ermöglicht den Zugang und den Besitz über die Kryptocoins. Der Schutz dieses Passworts in Form der Zeichenkette vor anderen ist von grundlegender Bedeutung, da bei verlorenem oder gestohlenem privatem Schlüssel der Nutzer den Zugang und somit die komplette Macht über sein digitales Vermögen verliert. Daher sollte dieses Passwort, sowie der Pin-Code eines Bankkontos, stets privat gehalten und nur zum Übertragen und Signieren der Transaktionen genutzt werden[31].

Der öffentliche Schlüssel wiederum stellt die „Adresse“ des Nutzers dar, vergleichsweise wie die IBAN, jedoch wird zur Person selbst keinerlei Angabe gemacht, der Nutzer bleibt also hinter diesem „Pseudonym“ versteckt. Somit ist dem Netzwerk nur dieser öffentliche Schlüssel und nicht die dahinterstehende Person bekannt[32]. Für den Erhalt der Kryptocoins bei einer Transaktion, muss dieser öffentliche Schlüssel dem Absender bekannt gegeben werden, damit von der Gegenpartei an diese Adresse die Kryptowährungen gesendet werden können. Mithilfe des jeweils eigenen privaten Schlüssels wird die Transaktion von beiden Seiten freigegeben und signiert. Innerhalb eines Krypto-Netzwerks können die Benutzer ihre Kryptowährung also willkürlich zwischen ihren Adressen hin- und herschieben, wobei der Vorgang insgesamt anonym bleibt, damit nicht erkennbar ist, wer der Besitzer eine Adresse ist[33]. Diese Codes

[30] Vgl.*Grzywotz* (2019), S. 31.
[31] Vgl.*SCHMIDT* (2019), S. 1.
[32] Vgl.*Grzywotz* (2019), S. 35.
[33] Vgl.*Grzywotz* (2019), S. 35.

werden derweil von der einen Partei zur anderen übertragen, die Transaktion wird kryptografisch signiert und in der Blockchain notiert[34].

Die Verwaltung, sowie Speicherung dieser Schlüsselpaare und die dazugehörigen Kryptowährungen erfolgt in sogenannten „Wallets“. Eine Wallet stellt eine digitale Geldbörse für Kryptowährungen dar, die den Besitz und auch den Austausch von Kryptocoins zwischen den Adressen ermöglicht. Es ist jedem Nutzer möglich sich eine unbegrenzte Anzahl an Wallets zuzulegen und sich somit eine unbegrenzte Anzahl von Schlüsselpaaren zu erzeugen und zu speichern. Die Option der unbeschränkten Anzahl an Wallets, verknüpft mit den Pseudonymen, auf der Basis der öffentlichen Schlüssel, bietet dem Nutzer des Kryptowährungssystems die erhoffte Privatsphäre und Anonymität.[35] Transaktionen können somit anonym erfolgen, da außer dieser Adresse keine Informationen über den Empfänger bekannt sind. Die Verbuchung dieser Transaktionen wird jedoch in der öffentlich zugreifbaren Blockchain gespeichert[36].

Dennoch kann durch die manipulationssichere Erfassung aller Transaktionen in der Blockchain jeder Wallet-Adresse eine exakte Anzahl der im Besitz gehaltenen Kryptocoins zugeordnet werden. Der Wallet dient zu diesem Zweck vielmehr zur Verwaltung der digitalen Identität im System. Denn, die im Besitz befindlichen Kryptocoins existieren nicht als Datei und können daher in dem Wallet nicht abgelegt oder gespeichert werden. Ein Rückschluss auf die tatsächliche Person ist nur sehr beschränkt und ungenau möglich, bspw. über die genutzte IP-Adresse. Die Bestätigung der Transaktion erfolgt durch die Rechner im Netzwerk, die diese Signatur prüfen. Ist die Signatur korrekt, kann über das entsprechende Guthaben verfügt werden[37].

Eine Rückbuchung einer bereits durchgeführten Transaktion ist aus technischen Gründen nicht möglich, da aufgrund der immer wieder neu generierten Zahlenketten der Blockchain die vorherige IP-Adresse nach Durchführung einer Transaktion veraltet ist. Aufgrund der technologischen Eigenschaften des Systems ist das Kopieren von Kryptocoins oder deren Vermehrung in betrügerischer Absicht nicht möglich. Dies verleiht dem Gesamtsystem insgesamt eine hohe Zuverlässigkeit[38].

[34] Vgl.*SCHMIDT* (2019), S. 2.
[35] Vgl.*Grzywotz* (2019), S. 35.
[36] Vgl.*Koenig* (2018b), S. 122.
[37] Vgl.*Koenig* (2018b), S. 120–126.
[38] Vgl.*Koenig* (2018b), S. 126.

2.3.3 Mining

Die Art des Schaffens neuer Coins wird Mining genannt. Im Gegensatz zu den Einheiten der klassischen Währungen, die von Zentralbanken ausgegeben werden, erfolgt die Erzeugung der neuen Kryptowährungen durch das sogenannte „Mining“. Dabei handelt es sich um ein vorgegebenes kryptographisches Verfahren, in dem eine komplexe mathematische Aufgabe in den Diensten des Blockchain-Systems gelöst wird, wodurch neue Kryptocoins einer jeweiligen Kryptowährung geschöpft werden. Hier dürfen allerdings nicht die notwendige Elektrizität für das Bereitstellen der Rechenleistung und die erforderlichen Kosten für die Hardware vergessen werden[39].

2.3.4 Konsens-Algorithmen

Die Erzeugung der Kryptowährungen erfolgen nach einem Konsensalgorithmus. Dieser Konsens-Algorithmus verschafft Nutzern die Koordination in einer verteilten Umgebung, welche die verschiedenen Knoten in einem Peer-to-Peer-Netzwerk umfasst. Durch das Konsensverfahren wird der Zusammenschluss zwischen den gleichgestellten Teilnehmern im gesamten Netzwerk erreicht[40]. Die grundlegenden Funktionen, die der Algorithmus erfüllt, sind zum einen die Sicherstellung der Kontinuität und des ordnungsgemäßen Betriebs des Systems, und zum anderen die Definition der Regeln für die Erstellung neuer Blöcke[41]. Die sogenannten Konsensalgorithmen lassen sich in folgende zwei Hauptgruppen unterteilen.

Der Proof-of-Work-Mechanismus (POW) zielt darauf ab, die Rechenleistung zu nutzen, um Hashwerte zu berechnen. Im Rahmen dieses Minings versuchen alle Computer im Netzwerk eine mathematische Aufgabe zu lösen, die in der Berechnung der Hash-Werte der Blöcke liegt. Sobald die Aufgabe von einem Rechner gelöst wird, darf dieser seinen Block an die Blockchain anhängen. Der Gewinn erfolgt in Form der entsprechenden Kryptowährung. Die Kryptowährung generiert einen Wert durch den Nachweis der Arbeit [42].

[39] Vgl.*Izzo-Wagner/Siering* (2020), S. 10.
[40] Vgl.*Metzger* (2022).
[41] Vgl.*Bussac* (2019), S. 54.
[42] Vgl.*Koenig* (2018b).

Die neue Alternative zu PoW ist der Konsensalgorithmus Proof of Stake. Statt Rechenleistung werden durch den Einsatz von bestehenden Coins neue Blöcke generiert. Im Gegensatz zu PoW werden bei PoS keine Hashwerte berechnet. Das Ziel ist ausschließlich die Überprüfung der richtigen Bestätigung der Transaktionen. Bei POS wird nach dem Zufallsprinzip ein Knoten ausgewählt, der für die Validierung des nächsten Blocks zuständig ist und anschließend den Gewinn in der Kryptowährung erhält[43].

2.4 Dezentralität

Wie bereits erwähnt werden die Währungstransaktionen und Guthaben der Kryptowährungen in dezentralen Netzwerken verwaltet. Durch diese Dezentralität zeichnet sich die Blockchain-Technologie aus, denn bei jeglichen Transaktionen von Kryptowährungen sind immer nur der Absender und Empfänger beteiligt. Darüber hinaus wird keine dritte Partei benötigt[44].

Die herkömmliche Methode der Geldschöpfung einer Währung ist die Steuerung durch die Zentralbanken und die anschließende Verteilung sowie der Umlauf des Geldes durch die Geschäftsbanken. Bei klassischen Finanzaktivitäten steht somit immer eine zentrale Partei im Mittelpunkt, die für die Regelungen, Kontrolle und Überwachung von Transaktionen zuständig ist. Bei Kryptowährungen hingegen fällt diese zentrale Instanz weg, stattdessen sind Software-Algorithmen und dezentrale Architekturen für die Krypto-Geldschöpfung und dessen Kontrolle / Verwaltung verantwortlich[45].

Kryptowährungen werden daher der Kategorie „Decentralized Finance“ zugeordnet. Dieses ist der Sammelbegriff für klassische Finanzdienstleistungen, deren Abwicklung über eine dezentrale Plattform, beispielsweise eine Blockchain, abläuft[46]. Der Begriff bezeichnet demnach Finanzanwendungen, die keine zentrale Instanz benötigen, beispielsweise eine Bank. Die Aufgaben dieser Zentrale übernehmen die Netzwerkteilnehmer im dezentralen System. Das System der Kryptowährungen zeichnet sich durch

[43] Vgl.*Bundesnetzagentur* (2019).
[44] Vgl.*Koenig* (2018b), S. 127.
[45] Vgl.*Izzo-Wagner/Siering* (2020), S. 14.
[46] Vgl.*BTC-ECHO* (2022).

vollständige Dezentralität aus, was bedeutet, dass es keinen zentralen Server oder eine kontrollierende Autorität gibt[47].

Das ursprüngliche Ziel von Kryptowährungen war es, eine universelle digitale Währung zu kreieren, die als Zahlungsinstrument verwendet werden kann, ohne von einer zentralen Institution kontrolliert zu werden. Da Kryptowährungen nicht vom Staat, sondern von unregulierten Organisationen oder einem Computer-Netzwerk herausgegeben werden, kann beispielsweise keine Geldmengensteuerung erfolgen. Das Geldvolumen muss nicht an die aktuelle Wirtschaftslage angepasst werden. Aus diesem Grund können Kryptowährungen am besten als „virtuelles Geld“ beschrieben werden, da sie im Gegensatz zu den klassischen, gesetzlichen Währungen nicht von Zentralbanken herausgegeben und kontrolliert werden und auch nicht von Geschäftsbanken an die Bevölkerung verteilt werden[48]. Darüber hinaus gibt es grundsätzlich keine Hierarchien zwischen den Nutzerinnen und Nutzern[49]. Kryptowährungen existieren nicht physisch oder in Form von Dateien, sondern als kodierte Transaktionsdaten in einem dezentralisierten Buchführungssystem, der Blockchain[50].

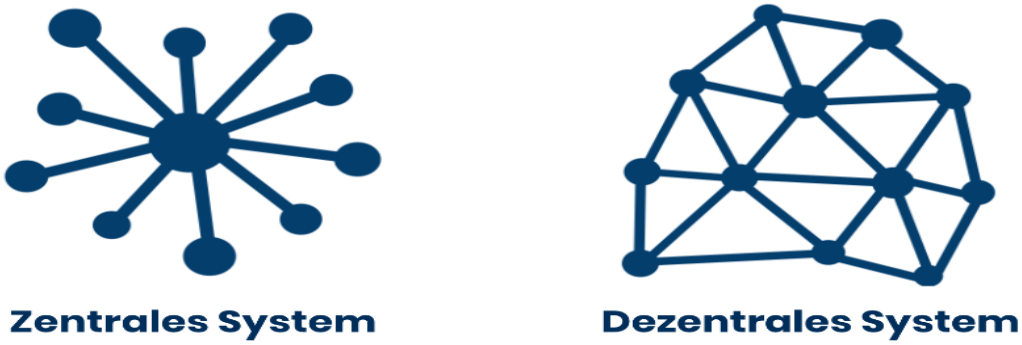


Abbildung 2: Unterschied zentrales und dezentrales System[51]

Die obige Abbildung zeigt den Unterschied zwischen einem zentralen und einem dezentralen System auf. Zentrale Systeme zeichnen sich durch einen einzigen Knoten aus, über diesen jede Transaktion oder Aktivität ablaufen muss. Aufgrund dessen

[47] Vgl.*Heinze/Protschka* (2018), S. 67.
[48] Vgl.*Izzo-Wagner/Siering* (2020), S. 3.
[49] Vgl.*Hudson Intelligence* (2022a).
[50] Vgl.*Heinze/Protschka* (2018), S. 67.
[51] Vgl.*Breitsprecher* (2018).

verfügt dieser Knoten sehr viel Macht über, während alle anderen Punkte dazu verpflichtet sind, diesem einen Knoten zu vertrauen[52].

Das dezentrale System hingegen, besteht aus mehreren Knoten, ohne einen zentralen Knoten, der das System leitet und kontrolliert. Selbst wenn ein Knoten ausfallen sollte, besteht nicht die Gefahr, dass das System versagt. Demzufolge gibt es keine Bedingtheit einer einzigen Autorität. So können Zahlungen ohne Zwischenschaltung einer dritten Partei, wie z.B. einer Bank, direkt von einer Kryptowährungspartei an eine andere Partei transferiert werden [53].

2.5 Peer-to-Peer Netzwerk

Die Blockchain wird aufgrund ihrer Dezentralität in Peer-to-Peer-Netzwerk eingebettet und wird im technischen Zusammenhang als Peer-to-Peer-Modell bezeichnet [54]. Der Begriff leitet sich vom englischen „peer“ ab und wird im Allgemeinen mit „Gleichgestellter“ übersetzt. Peer-to-Peer-Netzwerke sind gleichberechtigte Computernetzwerke, in denen die Nutzer untereinander Ressourcen anbieten und nutzen können. Es gibt keinen zentralen Server oder Host, die Struktur des Netzwerks wird durch die Nutzer aufrechterhalten**.** Jeder einzelne Computer, indem Fall „Peer“ stellt einen Netzwerkknoten dar, der mit allen anderen Knoten verbunden ist, ohne dass es eine zentrale Koordinierungsstelle gibt, die erhöhte Berechtigungen hat [55]. Dabei agiert jeder Knoten sowohl als Client als auch als Server gegenüber den anderen Knoten. Beim Empfangen und Senden von digitalen Daten spielen alle Peers die gleiche Rolle.

Die folgende Abbildung stellt den Vergleich zum herkömmlichen Client-Server-Modell dar.

[52] Vgl.*Breitsprecher* (2018).
[53] Vgl.*Graf* (2017).
[54] Vgl.*Hudson Intelligence* (2022a).
[55] *Hudson Intelligence* (2022a).

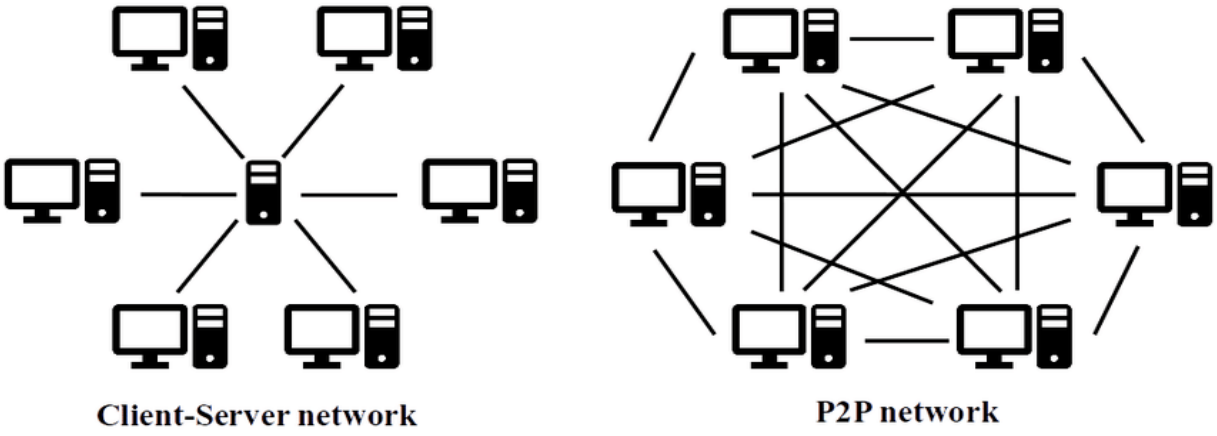


Abbildung 3: Client-Server vs. Peer-to-Peer-Netzwerke[56]

Der maßgebende Unterschied zwischen P2P-Systemen und herkömmlichen Client-Server-Modellen ist die Datenverteilung[57]. Beim zentralisierten Client-Server-Modell erfolgt die Verwaltung und Speicherung der Daten unidirektional von einem zentralen Server zu den Clients, während bei Peer-to-Peer jeder Benutzer seine eigenen Daten verwaltet und aufbewahrt. Auf technischer Ebene fällt also beim P2P-Konstrukt die autoritäre Macht weg, die sich beim Client-Server Modell im Mittelpunkt befindet[58].

In einem Peer-to-Peer-Netzwerk gibt es zudem keine Unterscheidung zwischen Client und Server, jeder Knoten kann beide vertreten. Aufgabe des Servers ist die Bereitstellung von Diensten[59]. Es ist wichtig, dass alle Netzknoten in ihren Rechten und Rollen im System gleichgestellt werden, damit das System innerhalb der Regeln selbstorganisierend und nicht hierarchisch ist[60].

In der Blockchain- und Kryptowährungsindustrie nimmt die P2P-Technologie eine wichtige Rolle ein. Dieses Modell ermöglicht es den Nutzern, Kryptowährungen international zu versenden und zu empfangen, ohne auf einen zentralen Datenserver oder einen Intermediär angewiesen zu sein. Somit sind Kryptowährungen die Antwort auf ein stark dezentralisiertes Währungssystem, in dem es keine großen Akteure gibt, die Geldwährungen proaktiv manipulieren können, was der Grund ist, dass Kryptowährungen einen enormen Popularitätsschub erfahren haben [61].

---

[56] *Jaganathan/Veeramani*.
[57] Vgl.*Howard* (2022).
[58] Vgl.*Hudson Intelligence* (2022a).
[59] Vgl.*Hudson Intelligence* (2022a).
[60] Vgl.*Duthel* (2017).
[61] Vgl.*Hudson Intelligence* (2022a).

2.6 Smart Contracts

Ein essenzieller Teil der Funktionsweise der Decentralized Finance, auf der Grundlage der Blockchain-Technologie, sind die digitalen Verträge, die sogenannten „Smart Contracts“ [62]. Darunter werden automatisierte Verträge verstanden, die mit vordefinierten und programmierten Vereinbarungen zwischen zwei Vertragspartnern auf der Blockchain gespeichert werden. Die Verwaltung der Einzelheiten des Vertrags wird von künstlicher Intelligenz geprüft und ausgeführt, nicht von Juristen oder Notaren. Die Datenübermittlung erfolgt nur, wenn die Bedingungen beider Parteien im Vertrag erfüllt sind, so dass ein Vertragsbruch nicht möglich ist[63]. Nachdem ein Smart Contract zustande kommt, ist dieser nicht mehr veränderbar. Durch die Speicherung auf der Blockchain soll sichergestellt werden, dass beide Parteien den Vertrag einhalten[64]. Die Blockchain übernimmt somit die transparente Funktion eines Mechanismus zum Austausch von Daten zwischen Parteien, ohne dass ein Intermediär zwischengeschaltet werden muss. Keine der zentralen Instanzen wie bspw. die Bank oder das Gericht haben die Befugnis, die Einhaltung der Verträge zu kontrollieren[65].

2.7 Arten von Token

Der Begriff Kryptowährungen wird als Überbegriff für alle digitalisierten Token genutzt, die wie Bitcoin und Ethereum auf der Blockchain basieren. Die Kryptowährungen unterscheiden sich jedoch teilweise in der Zielrichtung und dem Zweck der einzelnen Coins bzw. Tokens[66].

Ein **Utility-Token** ist ein digitaler Vermögenswert, der eine Blockchain-Plattform nutzt, um Zugang zu einem bestimmten Produkt oder einer Dienstleistung zu gewähren, der zum Kauf dieses Produkts oder dieser Dienstleistung verwendet werden kann. Utility Token sind am wenigsten reguliert.

[62] Vgl.*Dr.Burgwinkel* (2016).
[63] Vgl.*Koenig* (2018a), S. 164.
[64] Vgl.*Wyss* (2021).
[65] *ethereum.org* (2022).
[66] *Izzo-Wagner/Siering* (2020), S. 7.

Sicherheits-Token werden häufig im Rahmen eines „Initial Token/Coin Offering“ verkauft oder versteigert, was den Unternehmen ermöglicht, Mittel zur Unterstützung einer neuen Idee oder eines neuen Geschäftsmodells zu generieren; dies ist die gleiche Funktion wie bei einem herkömmlichen Börsengang. Das Unternehmen tauscht Sicherheits-Token gegen Fiat-Geld oder andere Krypto-Vermögenswerte ein. Sicherheitstoken können daher als Anteile an einem Unternehmen, einem System oder einem Projekt verstanden werden. Ähnlich wie bei Aktien erhalten diese Anteile ihren Wert in erster Linie dadurch, dass ein Teil des Systems erworben wird, welches hinter diesen Anteilen steht. Die stärkste Regulierung erfahren daher in der Regel Security Token.[67]

Nicht fungible Token (NFTs) sind Blockchain-basierte digitale Elemente, deren Einheiten einzigartig sind, im Gegensatz zu traditionellen Kryptowährungen, deren Einheiten austauschbar sein sollen. NFTs können Datensätze auf der Blockchain abspeichern. Diese Daten können mit Bildern, Videos, physischen Gegenständen, Mitgliedschaften und zahllosen anderen Anwendungen verbunden werden. NFTs verleihen dem Inhaber das Eigentum an den Daten oder Medien, mit denen der Token verknüpft ist, und werden üblicherweise auf spezialisierten Marktplätzen gekauft und verkauft. [68]

Plattform-Token umfassen Kryptowährungen, die benötigt werden, um an der zugrundeliegenden Plattform teilzunehmen, beispielsweise Ethereum, bei dem man die zugehörige Kryptowährung „Ether“ verwendet, um Smart Contracts abzuschließen. Obwohl Plattformtoken als Zahlungsmittel dienen könnten, ist dies nicht zwangsläufig beabsichtigt. Um die Token zu klassifizieren, muss in diesen Fällen darauf geachtet werden, auf welche Funktionen der jeweilige Token fokussiert.[69]

Echte Kryptowährungen **(Zahlungs-Token)** haben primär nur den Zweck, als alternatives Zahlungsmittel für den Kauf von Waren oder Dienstleistungen eingesetzt zu werden[70].

[67] Vgl.*Izzo-Wagner/Siering* (2020), S. 8.
[68] Vgl.*Izzo-Wagner/Siering* (2020), S. 8.
[69] Vgl.*Izzo-Wagner/Siering* (2020).
[70] Vgl.*Izzo-Wagner/Siering* (2020), S. 8.

3 Entwicklung von Kryptowährungen

Täglich steigt die Anzahl der verfügbaren Kryptowährungen, trotzdem ist die Menge der Kryptocoins auf sehr wenige große Player konzentriert. Zum einen profiliert sich Bitcoin mit einem Marktanteil von 46,2 %, der mit Abstand den größten Teil ausmacht. Zum anderen stellt sich in diesem Zusammenhang auch Ethereum mit 17,6 % Marktanteil als erwähnenswert heraus. Mittlerweile gibt es über 10.000 verschiedenen Kryptowährungen[71]. Allerdings ist dies nur die offizielle Anzahl an Kryptowährungen. Über das Ethereum-Netzwerk können Token ganz einfach erzeugt werden. Dadurch können für einen bestimmten Einsatzzweck eigene Kryptowährung erstellt und dabei die Sicherheit des Ethereum-Netzwerks genutzt werden[72].

3.1 Entstehung von Kryptowährungen

Neben dem Vorreiter der Kryptowährungen, dem Bitcoin, gibt es mittlerweile tausende weitere Kryptowährungen. Diese Kryptowährungen vereinen derzeit eine Gesamtmarktkapitalisierung von 111 Milliarden US-Dollar. Dabei verfolgen die einzelnen Kryptowährungen zum Teil unterschiedliche Ziele[73].

Bitcoin ist die erste und bekannteste Kryptowährung, auf der Blockchain-Basis. Sie ist auch die umstrittenste Anwendung, da sie einen globalen Marktplatz für anonyme Transaktionen im Wert von mehreren Milliarden Dollar ohne staatliche Aufsicht ermöglicht[74]. Der Gründer des Bitcoins ist unter dem Pseudonym „Satoshi Nakamoto“ bekannt, dessen Identität immer noch unentdeckt ist[75]. Die Finanzkrise im Jahr 2008 führte zur enormen Unzufriedenheit in der Bevölkerung und der Glaube an die Funktionstüchtigkeit der Banken sank täglich. Anfang 2009 veröffentliche Satoshi Nakamoto dann sein „Whitepaper“, ein Dokument welches Bitcoin als neues technisches Zahlungssystem bekannt machte. Nakomoto präsentierte Bitcoin als die neue digitale Währung, auf Basis der Blockchain-Technologie, in dem Transkationen zwischen Benutzern getätigt werden können[76]. Diese Währung sollte eine dezentrale Alternative zu

[71] Vgl.*Coin Market cap* (2022).
[72] Vgl.*Soeteman* (2019), S. 42.
[73] Vgl.*Heinze/Protschka* (2018).
[74] Vgl.*Ayed* (2017).
[75] Vgl.*Financial and consumer services comission* (2022).
[76] Vgl.*Ayed* (2017).

den bestehenden Papierwährungen sein, die unabhängig von einer zentralen Institution existiert, nicht manipulierbar ist, den Datenschutz in Zeiten elektronischer Zahlungen in den Vordergrund stellt und eine Lösung für die Finanzkrise darstellt[77]. Obwohl sie als Ersatz für Papiergeld gedacht war, wird Bitcoin immer noch in den meisten Ländern nicht als gesetzliche Währung anerkannt[78].

3.2 Nachfrage nach kryptobezogenen Vermögenswerten

In den letzten zehn Jahren ist die Nachfrage nach dem Handel mit Kryptowährungen erheblich gestiegen. Diese Nachfragesteigerung hat Innovationen in diesem Sektor ermöglicht und den Zugang zur Blockchain in einem ständig wachsenden Kreislauf erleichtert. Mit der steigenden Nachfrage der Nutzer hat auch das Angebot auf dem Markt zugenommen. Diese enorme Nachfrage lässt sich auf den Siegeszug von Bitcoin zurückführen, der in nur zehn Jahren von einem Wert von 50 Euro auf einen Höchststand von 67.000 Euro gestiegen ist. Anleger, die diesen Sprung verpasst hatten, begannen schnell, Geld in den Markt zu investieren, in der Hoffnung, dass sich eine ähnliche Geschichte wie bei Bitcoin wiederholen würde[79].

Gegenwärtig erkennt eine große Mehrheit der Länder Kryptowährungen nicht als gesetzliches Zahlungsmittel an, sondern sehen sie eher als spekulative Wertpapiere. Aus dem ursprünglichen Ziel einer neuen Währung, womit Menschen im Alltag bezahlen können, ist nichts beigeblieben[80]. Zu Beginn gab es sogenannte Cold Wallets, worauf die Kryptocoins offline auf Datenträgern gespeichert wurden, wodurch Sie erstens durch andere Hacker- und Betrugsangriffe geschützt waren und hauptsächlich die Funktion zum Zahlen hatten. Dafür war die Essenz einer „sicheren“ und unabhängigen Kryptowährung vorteilhaft. Nun sind sie jedoch nahezu vollständig raus aus dem offline Cold-Wallet zum online Hot-Wallet übergegangen, die Menschen lediglich zum Betrügen einladen. Es ist fast unmöglich sich mit Online-Wallets vor systematischen Betrug zu schützen[81].

[77] Vgl.*Heinze/Protschka* (2018), S. 105.
[78] Vgl.*Financial and consumer services comission* (2022).
[79] Vgl.*Coin Market cap* (2022).
[80] Vgl.*Coin Market cap* (2022).
[81] Vgl.Entwicklung der Kryptowährungen (2023).

Aus dem Grund ist es sehr wichtig zu beachten, dass es neben wachsenden Markt dieser neuen Geldanlage, der für einige Nutzer zwar erhebliche Gewinne verspricht, gleichzeitig der Missbrauch dieses Marktes zunimmt, womit die große Mehrheit der Nutzer viel Geld verlieren. Der Markt ist so groß geworden, dass er nicht anders kann, als kontinuierlich Investitionen und neues Geld anzuziehen, da die Leute versuchen, einen Teil der Gewinne zu erwirtschaften, die alle anderen zu erzielen scheinen[82].

3.3 Sicht der deutschen Bevölkerung auf Kryptowährungen

Im Jahr 2022 besaßen circa 8 Millionen deutsche Erwachsene, also etwa 9,8 Prozent der deutschen Bevölkerung, Kryptowährungen. Deutschland belegt im Krypto-Ranking den 28. Platz von insgesamt 47 Ländern, und die Besitzquote von Kryptowährungen liegt unter dem weltweiten Durchschnitt von 10,7 Prozent[83].

Im Gegensatz zu den hohen Risikobereitschaften in Asien, Afrika und Lateinamerika herrscht in Europa eine eher skeptische und zögerliche Haltung gegenüber Kryptowährungen. Insbesondere Deutschland gilt als das Land mit dem größten Misstrauen gegenüber Kryptovermögen, wobei 76 Prozent der Bevölkerung eine Investition ausschließen. In Deutschland ist der Bitcoin nach wie vor die am weitesten verbreitete Kryptowährung. Mehr als 69 Prozent der deutschen Kryptobesitzer besitzen Kryptowährungen mit Bitcoin. Mit seinen umfangreichen Anwendungsfällen folgt Ethereum direkt nach Bitcoin, gefolgt von Tether (USDT), Ripple (XRP) und anderen Altcoins. Die meisten deutschen Besitzer von Kryptowährungen haben im Durchschnitt mehr als 1.000 EUR in Krypto-Assets[84].

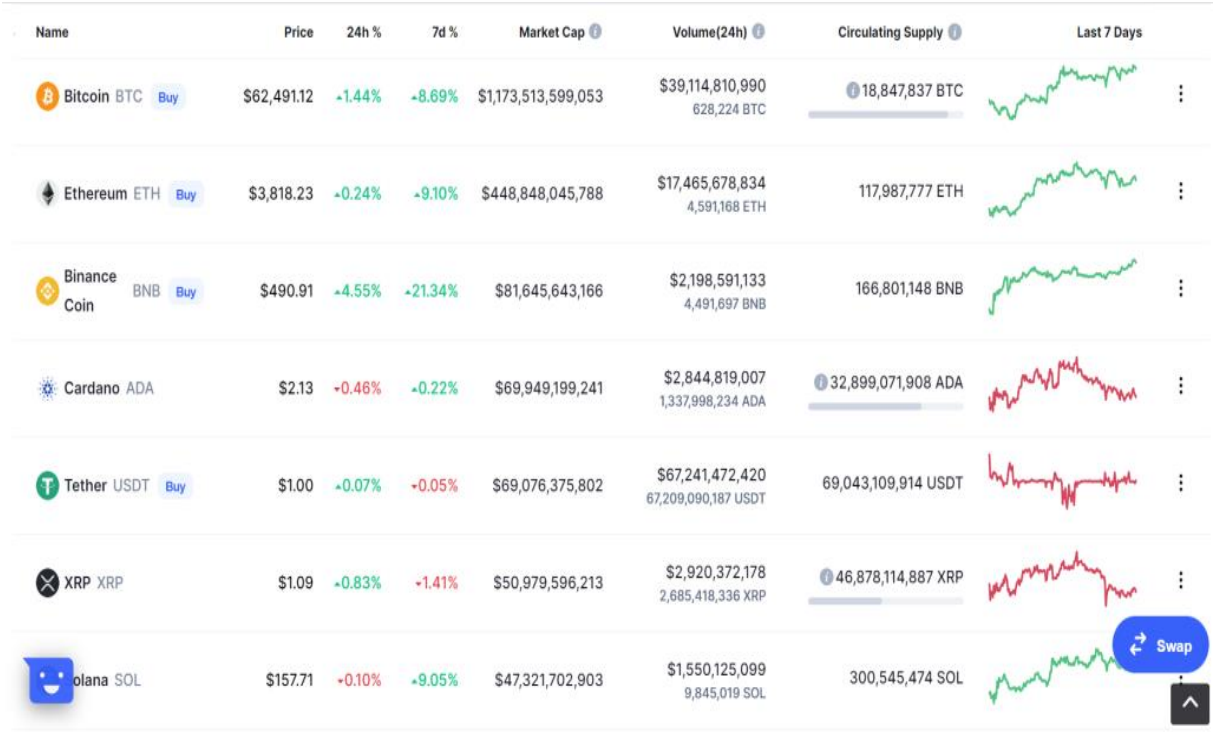
3.4 Aktueller Einbruch des Kryptomarktes

Die Zeiten für Digitalwährungen waren lange günstig, denn die niedrigen Zinsen der Notenbanken sorgten dafür, dass gefragt war, was mehr Rendite versprach als Sparkonten. Das Jahr 2021 brachte für viele bekannt Kryptowährungen ein Allzeithoch[85].

[82] Vgl.*Coin Market cap* (2022).
[83] Vgl.*Retzer* (2022).
[84] Vgl.*Retzer* (2022).
[85] Vgl.*Buchter/Tönnesmann*.

So stieg beispielweise der Kurs des Bitcoins vor einem Jahr auf fast 60.000 Euro. Anfang 2020 hatte er einen Wert von circa 8.000 Euro. Auch Ethereum und andere bekannte Kryptowährungen waren Teil dieses Wachstums, wodurch bei vielen Menschen das Interesse geweckt wurde, in Kryptowährungen zu investieren. Der Grund hierfür waren die massenweise wachsenden Neuanleger und die Hoffnung auf weitere steigende Zahlen. Kryptowährungen waren eine vielversprechende Geldanlage, die schnelle und hohe Gewinne auswiesen. Die mehr als 10.000 verschiedenen Kryptowährungen weltweit erreichten auf ihrem Höhepunkt im Jahr 2021 in Summe einen Wert von drei Billionen Euro[86].

Die nachfolgend dargestellte Abbildung zeigt die Kurswerte der Top 7 Kryptowährungen im Jahr 2021.



Name	Price	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
Bitcoin BTC Buy	$62,491.12	1.44%	8.69%	$1,173,513,599,053	$39,114,810,990 628,224 BTC	18,847,837 BTC	
Ethereum ETH Buy	$3,818.23	0.24%	9.10%	$448,848,045,788	$17,465,678,834 4,591,168 ETH	117,987,777 ETH	
Binance Coin BNB Buy	$490.91	4.55%	21.34%	$81,645,643,166	$2,198,591,133 4,491,697 BNB	166,801,148 BNB	
Cardano ADA	$2.13	0.46%	0.22%	$69,949,199,241	$2,844,819,007 1,337,998,234 ADA	32,899,071,908 ADA	
Tether USDT Buy	$1.00	0.07%	0.05%	$69,076,375,802	$67,241,472,420 67,209,090,187 USDT	69,043,109,914 USDT	
XRP XRP	$1.09	0.83%	1.41%	$50,979,596,213	$2,920,372,178 2,685,418,336 XRP	46,878,114,887 XRP	
olana SOL	$157.71	0.10%	9.05%	$47,321,702,903	$1,550,125,099 9,845,019 SOL	300,545,474 SOL	

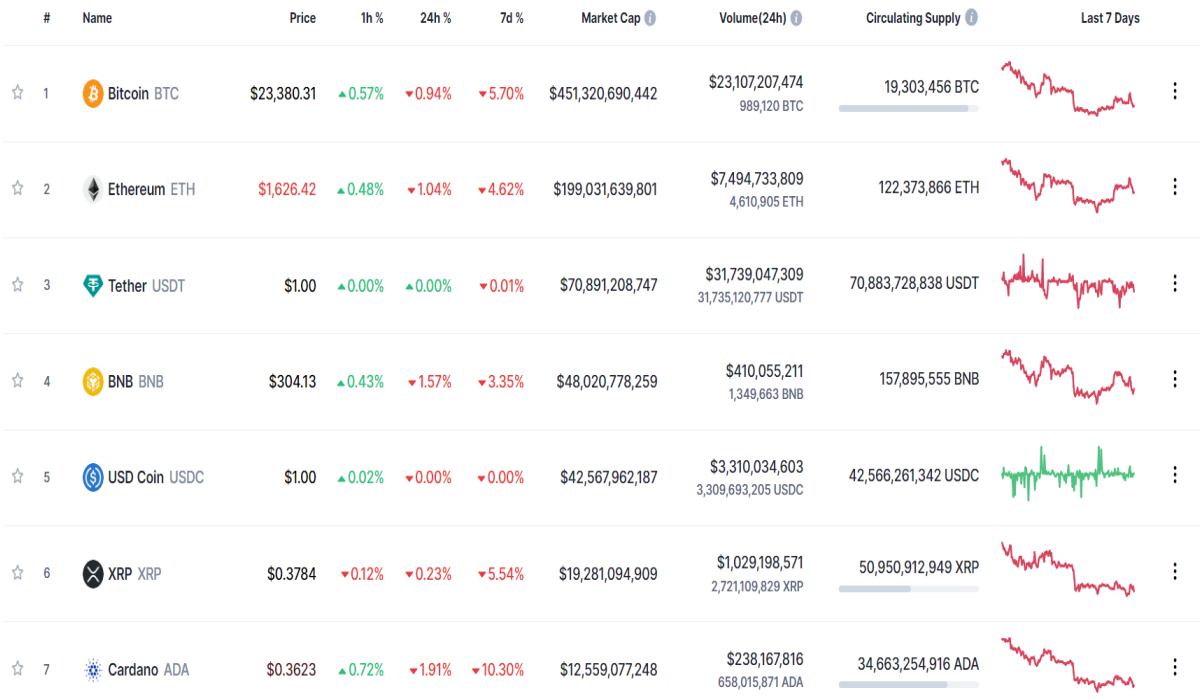
Swap

Abbildung 4: Kurs der Kryptowährungen 2021[87]

Das enorme Wachstum der Kryptovermögensanlagen führte zu dem Anstieg der Nachfrage nach kryptobasierten Vermögensanlagen, was zur Folge hatte, dass das Angebot zunahm. Dazu gehört die Gründung von neuen Kryptobörsen, sogenannte digitale Handelsplattformen, auf der sich Kryptowährungen kaufen, verkaufen und

[86] Vgl.*Buchter/Tönnesmann*.
[87] Vgl.*Coin Market cap* (2022).

tauschen lassen. Die erworbenen oder im Besitz befindlichen Kryptowährungen werden in diesen Börsen abgelegt und können auf das eigene Börsenwallet ein- und ausgezahlt werden. Die Kryptobörsen werben damit frei über die Kryptocoins verfügen zu können, während ein breites Angebotsspektrum an zahlreichen Produkten aus dem Kryptosektor zur Verfügung gestellt wird[88].



#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$23,380.31	▲0.57%	▼0.94%	▼5.70%	$451,320,690,442	$23,107,207,474 989,120 BTC	19,303,456 BTC	
2	Ethereum ETH	$1,626.42	▲0.48%	▼1.04%	▼4.62%	$199,031,639,801	$7,494,733,809 4,610,905 ETH	122,373,866 ETH	
3	Tether USDT	$1.00	▲0.00%	▲0.00%	▼0.01%	$70,891,208,747	$31,739,047,309 31,735,120,777 USDT	70,883,728,838 USDT	
4	BNB BNB	$304.13	▲0.43%	▼1.57%	▼3.35%	$48,020,778,259	$410,055,211 1,349,663 BNB	157,895,555 BNB	
5	USD Coin USDC	$1.00	▲0.02%	▼0.00%	▼0.00%	$42,567,962,187	$3,310,034,603 3,309,693,205 USDC	42,566,261,342 USDC	
6	XRP XRP	$0.3784	▼0.12%	▼0.23%	▼5.54%	$19,281,094,909	$1,029,198,571 2,721,109,829 XRP	50,950,912,949 XRP	
7	Cardano ADA	$0.3623	▲0.72%	▼1.91%	▼10.30%	$12,559,077,248	$238,167,816 658,015,871 ADA	34,663,254,916 ADA	

Abbildung 5: Kursverluste Kryptowährungen[89]

Im Jahr 2022 jedoch, war eine bedeutende Transformation auf dem Gebiet der Kryptowährungen festzustellen, da die Kurse erheblich gefallen sind.

Der Bitcoin verlor von seinem Allzeithoch wiederum fast 50% und fiel von 68.000 Dollar (Anfang September 2021) auf 35.000 Dollar (Februar 2022) ab**.** Wie in der obigen Abbildung dargestellt, liegt der aktuelle Wert des Bitcoins bei 23.380 Dollar, das sind ein Drittel des Höhepunktes im Jahr 2021. Andere Kryptowährungen verloren noch mehr an Wert im Vergleich zu ihren jeweiligen Allzeithochs[90].

Für den Absturz der Kryptokurse gibt es im Wesentlichen mehrere Gründe. Zum einen sind es die hohen Inflationsraten und die steigenden Zinserhöhungen von

[88] Vgl.*Handelsblatt GmbH* (2023).
[89] Vgl.*Coin Market cap* (2022).
[90] Vgl.*Coin Market cap* (2022).

Zentralbanken, die sich negativ auf die Finanzmärkte insgesamt und damit auch auf den Kryptomarkt auswirken. Das liegt daran, dass die meisten Menschen Kryptowährungen mit dem Geld kaufen, das ihnen nach allen Ausgaben für Investitionen bleibt. In Phasen hoher Inflation sind diese jedoch weniger vorhanden. Außerdem machen höhere Zinsen Investitionen auf Kredit uninteressant und Investitionen in andere Anlageklassen, selbst in klassisches Tagesgeld, generell wieder interessanter.

Die Bitcoin-Währung schien im Hinblick auf Inflationen eine wertbeständige Position einzunehmen, jedoch stellte sich dies als ein Irrtum heraus. Stattdessen scheint ein Zusammenhang zwischen Kryptowährungen und Technologieaktien zu existieren. Gegenwärtig hat die Kryptowelt mit einer hohen Volatilität zu kämpfen[91].

Eines der Hauptgründe für den Kurssturz um nahezu 50%, der im November 2022 zu beobachten war, ist auf die finanziellen Problemen der Kryptobörse FTX zuruckzuführen. Es handelte sich hierbei um einer der größten Kryptobörsen der Welt, die jedoch unter massiven Liquiditätsproblemen litt. Dies wiederum ließ die Investoren an der Zuverlässigkeit der virtuellen Währungsform im Allgemeinen zweifeln, weshalb zunehmend mehr Nutzer von ihren digitalen Coins abwanden. Durch den Zusammenbruch der FTX wurde die gesamte Branche erschüttert[92]. Nachfolgend soll näher auf diesen Börsenskandal eingegangen werden.

3.5 Fallbeispiel Börsenskandal FTX

Die meisten Krypto-Investoren nutzten Plattformen wie FTX oder Binance, um ihre Coins zu verwahren. „Sie vertrauen genau den Intermediären, denen der Bitcoin-Erfinder misstraute.“[93]

Samuel Bankman-Fried, auch SBF genannt, steht im Mittelpunkt des FTX-Börsenskandals. Es handelt sich hierbei um den Gründer der weltweitbekannten Kryptobörse, die noch im November 2022 ein Vermögen von 26 Milliarden Dollar auswies. Um sich auf dem Börsenmarkt zu profilieren, fand SBF potente Geldgeber, darunter den

[91] Vgl.*Sackmann* (2022).
[92] Vgl.*Sackmann* (2022).
[93] *Kirchner* (2022a).

weltgrößten Vermögensverwalter BlackRock, der sich an FTX beteiligte. Auf diese Weise stieg der Wert des noch jungen Unternehmens innerhalb kürzester Zeit auf mehr als 30 Milliarden US-Dollar an, wodurch er als größter Anteilseigner zum Multimilliardär wurde. Einen großen Teil des Kapitals seiner Investoren setzte SBF für die Bekanntmachung seines Unternehmens ein, zum Beispiel als Sponsor eines Formel-1-Teams und in der Politik. Das Crash in der Kryptowelt begann somit durch die Kryptobörse FTX, auf der mehr als fünf Millionen Menschen mit digitalen Währungen handelten, die 2021 einen Wert von 719 Milliarden Dollar betrugen[94].

Der FTX-Skandal markierte seinen Ausgangspunkt, als die Kryptobörse im November 2022 Konkurs anmelden musste. In Panik versuchten die Kunden, ihr Geld von der Plattform abzuziehen. Wie viel Geld die Börse für die Nutzer im Depot hatte und wie viel noch übrig ist, ist nun Gegenstand der Ermittlungen eines Insolvenzverwalters. Bei der Analyse der Buchhaltung von FTX stellte sich heraus, dass diese bei weitem nicht den Umfang und die Komplexität aufwies, wie sie in den Finanzberichten eines großen Unternehmens zu finden sind. So zeigte sich, dass FTX zuletzt Verbindlichkeiten von neun Milliarden Dollar, aber nur Aktiva von 900 Millionen Dollar auswies. Die Financial Times berichtete zudem über ein Dokument, in dem auch von einem „versteckten, falsch deklarierten internen Konto“ mit einem Fehlbetrag von acht Milliarden Dollar die Rede war[95].

Dies führt zum Kern der FTX-Pleite: Die Börse hatte einen Teil der Kryptowährungseinlagen ihrer Nutzer an ihre Tochtergesellschaft Alameda ausgeliehen, ein Vorgang der für US-Börsen strikt verboten ist. FTX war auf den Bahamas ansässig und Alameda hat ihrerseits das Geld im Kryptomarkt verloren. Das Portal CoinDesk veröffentlichte einen Bericht über die Sicherheiten, die Alameda für den Kredit von FTX hinterlegt hatte. Diese Sicherheiten waren eine Kryptowährung namens FTT, die von FTX selbst ausgegeben wurde. Die Tochtergesellschaft der Kryptobörse wettete mit Kundengeldern und hinterlegte als Sicherheit eine von der Börse erfundene Währung-Daraufhin brach der Kurs der selbst erfundenen Währung FTT ein und die Kunden

[94] Vgl.*Buchter/Tönnesmann*.
[95] Vgl.*Buchter/Tönnesmann*.

versuchten, ihre Anlagen abzuziehen. Dies war jedoch nicht möglich, da FTX keine mehr Reserven hatte[96].

Statt um fünf Milliarden Verbindlichkeiten handelte es sich in Wirklichkeit um 13 Milliarden. FTX überwies „irrtümlich“ acht Milliarden an Kundengeldern an einen Hedge-Fund, der sich im Besitz von SBF selbst befindet. Darüber hinaus wurden weitere unangemessene Aktivitäten unternommen. So gab es bspw. keine Aufsichtsratssitzungen, keine klar definierten Zuständigkeiten und keine geregelte Buchführung. Zudem wurden Zahlungen mit Hilfe von Emojis in Online-Chats autorisiert. Besonders fragwürdig für eine milliardenschwere Kryptobörse ist außerdem die Missachtung von Grundregeln der IT-Sicherheit. Der Zugriff auf die digitalen Währungen erfolgte über einen nicht gesicherten E-Mail-Posteingang, auf den mehrere Mitarbeiter gleichzeitig Zugriff hatten. Über einen Zugang in der Software hatte SBF Zugang auf die Gelder der Kunden.

Bei dem FTX-Skandal handelte es sich zudem um ein Fall von Überbewertung. Die Firma setzte im Jahr 2021 Kryptowährungen mit einem Volumen von 719 Milliarden Dollar um und erzielte bei einem Umsatz von einer Milliarde einen Gewinn von 388 Millionen. Die Investoren bewerteten das Unternehmen hingegen mit 32 Milliarden Dollar. Die Deutsche Börse wird mit einem Gewinn von 1,2 Milliarden Euro im Jahr 2021 und einem Volumen von 98 Milliarden Euro allein im Oktober etwa gleich hoch bewertet. Angesichts des hohen Wachstums der FTX, der geringeren Margen von Kryptowährungen im Vergleich zu traditionellen Wertpapieren, der sich ständig ändernden Krypto-Technologie und der häufigen Millionenverluste durch Hackerangriffe sollte die FTX deutlich niedriger bewertet werden als eine traditionelle Börse[97].

All diese Inkonsistenzen auf FTX waren so groß, dass andere Krypto-Unternehmen und Coins unter Druck gerieten. Vom Crash waren auch Unternehmen betroffen, die an der FTX gehandelt haben. Aufgrund dessen, dass auch institutionelle Anleger wie Staatsfonds und Pensionskassen in Krypto investieren, stellt sich aktuell die Frage, ob die Implosion die ganze Finanzwelt infizieren könnte. Die Pleite der FTX wurde als „der

[96] Vgl.*Buchter/Tönnesmann*.
[97] Vgl.*Kirchner* (2022b).

größte Zusammenbruch in der Geschichte der Kryptowährungen“ bezeichnet. Der FTX-Konkurs sei jedoch ein entscheidender Moment für die Szene, weil er ein „regulatorisches Beben“ auslösen wird, dass viele Staaten bisher versäumt haben[98].

Die Wissenschaftler sind skeptisch, dass sich die Krypto-Unternehmer selbst plötzlich für mehr Regulierung aussprechen und transparenter werden wollen. Sie vermuten einen Versuch der Industrie, ihre Geschäfte als behördlich genehmigt darzustellen, damit noch mehr Großanleger, Pensionsfonds und Banken in das Coin-Business einsteigen und bei Erreichen einer kritischen Masse die digitalen Währungen als Spekulationsobjekt etabliert und systemrelevant werden[99].

Doch während Banken seit Hunderten von Jahren gelernt haben, mit Bilanzen umzugehen und Betrüger fernzuhalten, ist die Kryptowelt noch schwach reguliert. Schätzungen zufolge müssen Krypto-Unternehmen jeden Monat eine Milliarde Dollar für ihre Stromkosten zahlen und dafür neu erzeugte Coins verkaufen. Das ist nur möglich, wenn die Anleger mindestens die gleiche Summe investieren. Was geschieht, wenn kein neues Geld mehr in Kryptowährungen strömt, ist noch nicht geklärt[100].
Die Pleite der FTX ist bei weitem kein Einzelfall. Angefangen hat es mit dem Diebstahl von neun Milliarden Dollar bei der japanischen Bitcoin-Handelsplattform Mt. Gox im Jahr 2014. Die Kette der Milliarden-Diebstähle findet bisher noch kein Ende.
All die Risiken, die Kryptowährungen ursprünglich vermeiden sollten, finden sich bei dem FTX-Skandal wieder. Spekulationsverluste, Bankenpanik, langfristige Anlagen für kurzfristige Verbindlichkeiten, mangelndes Eigenkapital, möglicherweise Veruntreuung von Kundengeldern und dazu noch Hackerangriffe[101].

Solange Kryptowährungen nicht als Zahlungsmittel im Einsatz sind, sondern reine Spekulationsobjekte, sind sie nur überlebensfähig, wenn ständig neues Kapital eingezahlt wird. Damit sind laut Wirtschaftsforschern weitere Pleiten an den Börsen vorprogrammiert. Wie bei Finanzkrisen üblich ist, greift die Angst nun auch Kryptoinvestoren an. Krypto-Anleger: Sie tauschen ihr digitales Vermögen wieder gegen Fiatwährungen,

[98] Vgl.*Kirchner* (2022b).
[99] Vgl.*Buchter/Tönnesmann*.
[100] Vgl.*Kirchner* (2022a).
[101] Vgl.*Kirchner* (2022a).

etwa Dollar oder Euro. Auch Bitcoin verlor rund ein Viertel seines Wertes in den vergangenen Monaten[102].

Zusammenfassend wirft Tönnesmann die wichtige Frage auf: „Wozu braucht man Kryptowährungen, wenn sie keine echte Alternative zum Währungssystem sind, sondern lediglich ein paralleles hochriskantes Finanzsystem?“[103]

3.6 Schwachstellen der Blockchain-Technologie

Fortschritte in der Computertechnologie können, wie in den obigen Abschnitten bereits umrisshaft dargelegt, auch als Herausforderung betrachtet werden, da die Sicherheit der Blockchain auf der Tatsache beruht, dass sie mit den heutigen modernen Computersystemen verschlüsselt bleiben kann. Doch mit der Entwicklung leistungsfähiger Quanten-Computer wird dieses unknackbare System jedoch weniger sicher. Laut eines Berichts von Ben Ayed heißt es, dass insbesondere die Blockchain aufgrund der Anonymität und der Möglichkeit, Geld zu empfangen und zu übermitteln, ohne die Identität preisgeben zu müssen, sind Bitcoin-Adressen mit einem Pseudonym und nicht mit einer realen Person verbunden. Dieses Pseudonym kann jedoch auf andere Weise mit Personen verknüpft sein, wodurch sich Angreifer in der Lage befinden, alle Transaktionen der Person einzusehen[104].

Schließlich gibt es noch das erhebliche Problem des Betrugs, da immer mehr Menschen auf dem Gebiet der Kryptowährungen agieren. Ben Ayed führt weiter aus, dass die Krypto-Technologie eine noch neue Entwicklung ist und die Nutzer nicht über die vollständigen Kenntnisse verfügen, so dass Hacker einen Vorteil aus uninformierten Menschen ziehen können[105].

[102] Vgl.*Buchter/Tönnesmann*.
[103] Vgl.*Kirchner* (2022a).
[104] Vgl.*Ayed* (2017).
[105] Vgl.*Ayed* (2017).

4 Krypto-Vermögenskriminalität

4.1 Trends in der Finanzkriminalität

Im Jahr 2021 erreichte die Kriminalität in Verbindung mit Kryptowährungen einen neuen Höhepunkt: 14 Milliarden Dollar wurden in diesem Jahr mit illegalen Kryptowährungsaktivitäten erwirtschaftet, verglichen mit 7,8 Milliarden Dollar im Jahr 2020. Die kriminelle Nutzung von Kryptowährungen erhöht weiterhin die Hürden für die Akzeptanz von Kryptowährungen, vergrößert die Möglichkeit staatlicher Verbote und schadet Menschen, die die Technologie für völlig legale Zwecke nutzen wollen[106].

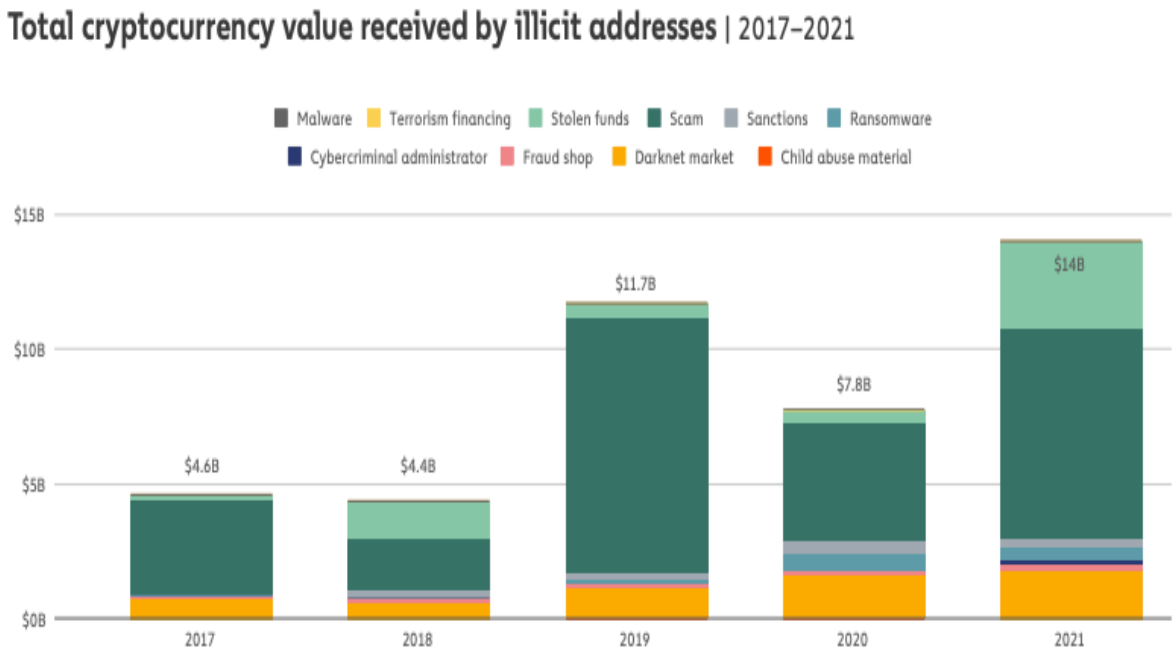


Abbildung 6: Jährliche Übersicht der Betrugsarten (Chainanalysis Crypto Crime Report)[107]

Die Einnahmen aus Betrug stiegen 2021 ganze 82 % im Vergleich zum Vorjahr. Dies ist auf Kryptowährungen zurückzuführen, die von anderen Kryptowährungsnutzern, in diesem Fall „Opfern“, gestohlen wurden[108]. Laut dem Chainalysis-Bericht (2022) wurden im Jahr 2021 fast 2,8 Milliarden US-Dollar an gestohlenen Geldern durch „Rug Pulls“, eine neue Betrugsmethode, erbeutet, was fast der Gesamtheit des Finanzdiebstahls im Jahr 2020 entspricht. Insgesamt wurden im Jahr 2021 Kryptowährungs-diebstähle im Wert von etwa 3,2 Milliarden US-Dollar verzeichnet, ein Anstieg von 516

[106] Vgl.*Grauer* et al. (2022).
[107] Vgl.*Chainanalysis* (2023).
[108] Vgl.*Grauer* et al. (2022).

Prozent gegenüber dem Vorjahr. Im Jahr 2020 wurden knapp 162 Millionen Dollar an Kryptowährungen von Defi-Systemen gestohlen, was 31 % des angegebenen Gesamtbetrags vom Vorjahr entspricht. Auch dieser Betrag ist im Jahr 2021 vergleichsweise um 330 Prozent gestiegen[109].

Die Darknet-Märkte stellten 2021 einen neuen Umsatzrekord auf und brachten insgesamt 2,1 Milliarden US-Dollar an Kryptowährung ein. Ungefähr 300 Millionen US-Dollar dieser Gesamtsumme wurden von Betrugsshops erwirtschaftet, die den Verkauf gestohlener Logins, Kreditkarten, Exploit-Kits und mehr vermittelten. Der Rest – mehr als 1,8 Milliarden US-Dollar – wurde von drogenorientierten Märkten erwirtschaftet[110].

Mit anderen Worten: Mit dem Wachstum des dezentralen Finanzmarktes hat auch die Kriminalität im Zusammenhang mit Kryptowährungen enorm zugenommen.

4.1.1 Ransomware-Angriffe

Der englische Begriff „Ransom“ steht für Lösegeld und beschreibt die Absicht dieser Schadsoftware sehr treffend. Ransomware sind Computerviren, die einzelne Dateien auf dem Computer verschlüsseln oder gleich das ganze Gerät sperren. Die Opfer werden zur Zahlung eines Lösegeldes aufgefordert, um wieder Zugriff auf Ihre Dateien zu erhalten. Nicht nur Unternehmen, sondern auch Privatpersonen sind von solchen Angriffen betroffen[111].

Die durchschnittliche Höhe der Zahlungen für Ransomware belief sich im Jahr 2021 auf mehr als 118.000 US-Dollar. Große Zahlungen wie die Rekordsumme von 40 Millionen US-Dollar, die Kryptohacker erhielten, haben zu diesem Allzeithoch der durchschnittlichen Zahlungshöhe beigetragen. Ein Grund für den Anstieg der Lösegeldsummen ist, dass sich Ransomware-Angreifer auf sehr gezielte Attacken auf große Organisationen konzentrieren. Diese „Big Game Hunting“-Strategie wird zum Teil dadurch ermöglicht, dass Ransomware-Angreifer Tools von Drittanbietern verwenden, um ihre Angriffe effektiver zu gestalten[112]. Diese Tools reichen von illegalen Hacking-Tools bis hin zu legitimen Produkten und umfassen eine Reihe von Elementen: Zum einen

[109] Vgl.*Grauer* et al. (2022).
[110] Vgl.*Grauer* et al. (2022).
[111] Vgl.*F-Secure* (2023).
[112] Vgl.*Grauer* et al. (2022).

gemietete Infrastrukturen wie Webhosting, Proxy-Dienste und E-Mail-Dienste zur Durchführung von Angriffen. Zum anderen Hacking-Tools wie Netzwerkzugänge, die die Netzwerke der Opfer auf Schwachstellen scannen. Die gestohlenen Daten wie Passwörter, personenbezogener Daten von Einzelpersonen und kompromittierter RDP-Anmeldeinformationen (Remote Desktop Protocol), helfen Angreifern, in die Computernetzwerke der Opfer einzudringen. Einer der wichtigsten Aspekte bei der Überwachung von Ransomware ist die Geldwäsche. In der folgenden Grafik ist dargestellt, wohin die Angreifer die Kryptowährung, die sie von den Opfern erpressen, transferieren[113].

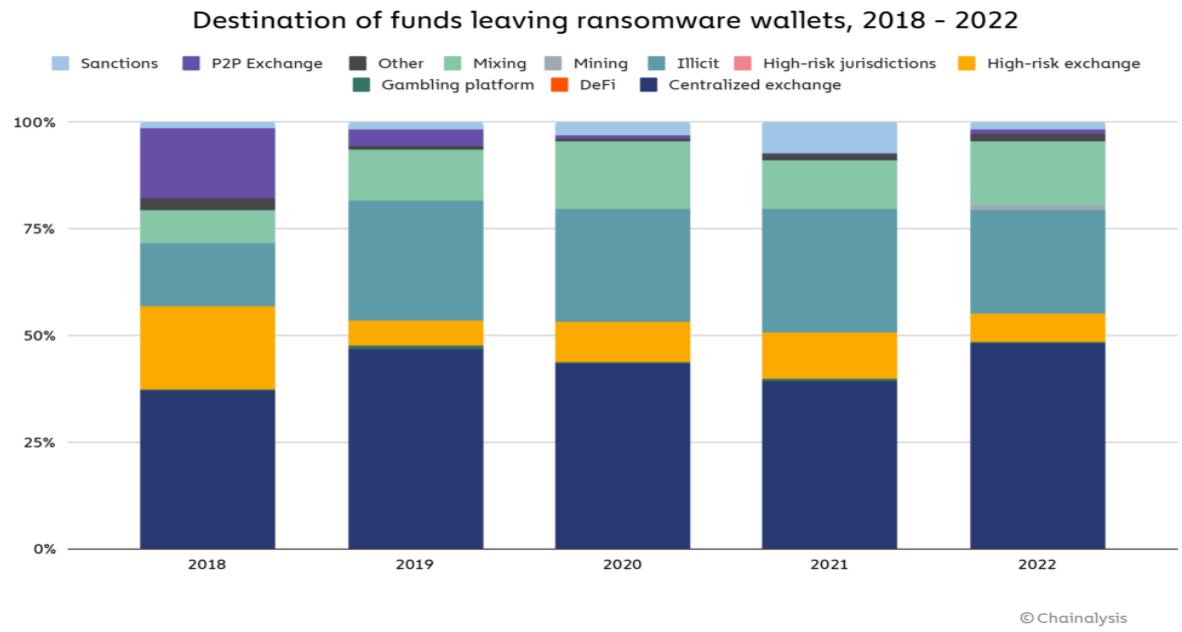


Abbildung 7: Geldfluss aus Ransomware-Angriffen (Chainanalysis 2022)[114]

4.1.2 Darknet-Transaktionen

Die Darknet-Märkte stellten 2021 einen neuen Umsatzrekord auf und brachten insgesamt 2,1 Milliarden US-Dollar an Kryptowährung ein. Ungefähr 300 Millionen US-Dollar dieser Gesamtsumme wurden von Betrugsshops erwirtschaftet, die den Verkauf

[113] *Chainanalysis* (2023).
[114] *Chainanalysis* (2023).

gestohlener Logins, Kreditkarten, Exploit-Kits und mehr vermittelten. Der Rest – mehr als 1,8 Milliarden US-Dollar – wurde von drogenorientierten Märkten erwirtschaftet.[115]

4.1.3 Terrorismusfinanzierung auf der Blockchain

Der Chainalysis-Bericht (2022) stellt zudem fest, dass sie bei ihren Nachforschungen massenweise terroristische Organisationen entdeckt haben, die versucht haben, ihre Aktivitäten mit Kryptowährungen im Jahr 2021 zu finanzieren. Es ist es jedoch schwieriger, die Gruppen ausfindig zu machen, die damit durchgekommen ist. Die Terrororganisation Al-Qaida sammelte im Jahr 2019 und 2020 Kryptowährungen über Telegram Kanäle und Facebook-Gruppen. Mehr als eine Million Dollar wurden auf einem Geld Service Company-Betreiber aufgedeckt, der einige dieser Transaktionen ermöglichte[116].

4.2 Geldwäsche durch Kryptowährungen

Bei den meisten Straftaten im Zusammenhang mit Kryptowährungen steht die Geldwäsche im Mittelpunkt[117]. Unter dem Begriff Geldwäsche wird laut dem Bundesministerium für Innern und für Heimat "die Einschleusung von illegal erwirtschafteten Geldern in den legalen Finanz- und Wirtschaftskreislauf" verstanden[118].

Cyberkriminelle, die mit Kryptowährungen handeln, haben in der Regel ein grundlegendes Ziel: ihre illegal erzielten Gewinne an Orte zu transferieren, an denen das Geld vor den Behörden verborgen bleiben und in Bargeld umgewandelt werden kann. Wenn das Geld nicht zugänglich ist, gibt es keine Motivation, Verbrechen im Zusammenhang mit Kryptowährungen überhaupt zu begehen[119]. Während Kryptowährungen im Wert von Milliarden von Dollar von illegalen Adressen transferiert werden, findet sich das meiste davon in einer kleinen Zahl von Unternehmen wieder, wovon die meisten aufgrund ihrer Transaktionsgeschichte speziell auf Geldwäsche ausgelegt sind[120].

[115] Vgl.*Grauer* et al. (2022).
[116] Vgl.*Chainanalysis* (2023).
[117] Vgl.*Grauer* et al. (2022).
[118] Vgl.*Bundesministerium für Innern und für Heimat*.
[119] Vgl.*Grauer* et al. (2022).
[120] Vgl.*Grauer* et al. (2022).

In der folgenden Abbildung werden die jährlichen Geldwäschebeträge durch Kryptowährungen aufgezeigt.

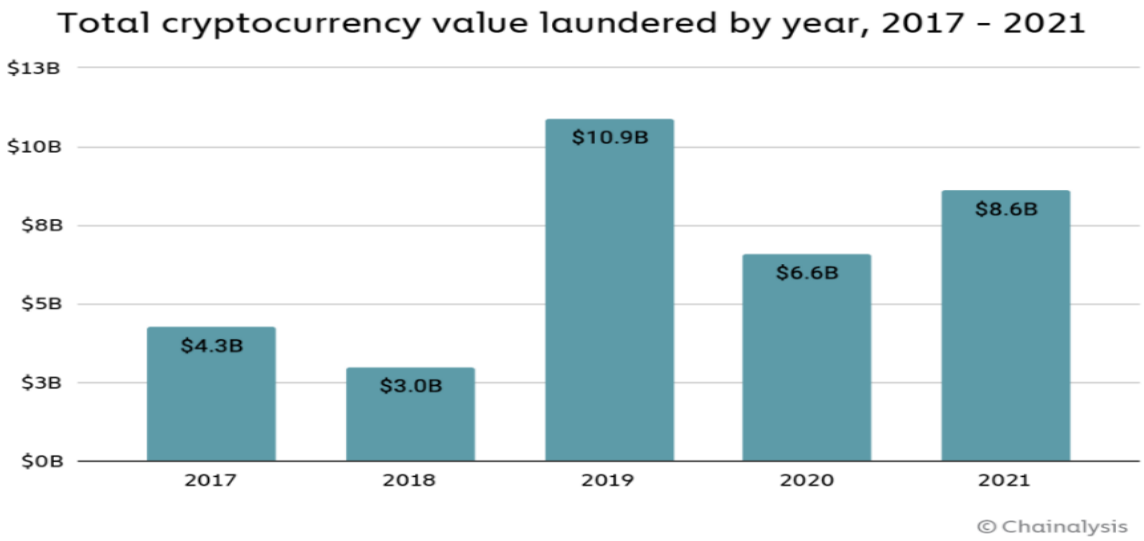


Abbildung 8: Geldwäsche durch Kryptowährungen (Chainanalysis Crypto Crime Report)

Im Jahr 2021 wurden Kryptowährungen im Wert von 8,6 Milliarden US-Dollar gewaschen. Diese wurden von Cyberkriminellen unter Verwendung illegaler Adressen an gehostete Dienste übertragen. Insgesamt bedeutet dies auch hier einen Anstieg der Geldwäscheaktivitäten um 30 Prozent zum Vorjahr. Angesichts der Zunahme legaler und illegaler Kryptowährungsaktivitäten im Jahr 2021 ist ein Anstieg der Geldwäsche jedoch nicht überraschend. Der größte Teil der gewaschenen Kryptogelder stammt aus Verkäufen im Darknet und aus dem Online-Handel mit Drogen[121]. Laut dem Bericht von Chainanalysis (2022) haben Kriminelle seit dem Jahr 2017 insgesamt etwa 33 Milliarden Dollar in Kryptowährungen gewaschen, wobei der größte Teil der Summe im Laufe der Zeit an zentrale Kryptobörsen verlagert wurde[122].

Der Hauptunterschied zwischen Geldwäsche und Fiatwährungen und Geldwäsche mit Kryptowährungen liegt darin, dass die Transparenz der Blockchain es noch einfacher macht, nachzuverfolgen, wie Kriminelle Kryptowährungen zwischen Wallets und Diensten transferieren, um ihre Vermögenswerte in Bargeld umzuwandeln. Wie bereits im ersten Abschnitt erwähnt, ist das Hauptbuch für jedermann einsehbar, was den Forschern eine genauere Schätzung des Wertbereichs ermöglicht. Doch aufgrund der

[121] Vgl.*Grauer* et al. (2022).
[122] Vgl.*Grauer* et al. (2022).

Anonymität der Transaktionen ist es umso schwieriger die Identität der Menschen ausfindig zu machen, die illegale Transaktionen vollzogen haben[123].

4.3 Trends der Geldwäsche in NFTs

Im Jahr 2021 ist die Popularität von nicht fungiblen Token (NFT) explodiert. Einem Bericht von Chainanalysis (2022) zu folge, wurden Kryptowährungen, die einen Wert von 44,2 Milliarden US-Dollar aufweisen, auf Ethereum Smart Contracts übertragen, die mit NFT-Märkten und -Sammlungen verbunden sind[124].

Ein Bereich, der im Zusammenhang mit NFTs als besorgniserregend gilt, ist die als „Wash Trading“ bekannte Methode zur künstlichen Erhöhung des Wertes von NFTs und somit Geldwäsche durch den Kauf von NFTs zu betreiben. Das Wash Trading stellt somit eine Form der Marktmanipulation dar. Hierbei wird eine Transaktion durchgeführt, bei der der Verkäufer auf beiden Handelsseiten vertreten ist. Dadurch wird ein irreführender Eindruck über den Wert und die Liquidität eines Vermögenswertes vermittelt[125]. Erkennbar ist diese Manipulation beispielsweise durch wiederholte Käufe und Verkäufe auf einer Kryptobörse, die automatisiert erscheinen, mengenmäßig übereinstimmen und sich im Wesentlichen auswaschen.[126] In der Vergangenheit stellte das Wash-Trading ebenfalls ein großes Problem dar, da die Kryptowährungsbörsen versuchten, die Handelsvolumina größer erscheinen zu lassen, als es in Wirklichkeit der Fall war. Ziel des NFT-Wash-Tradings ist es somit, die eigenen NFT wertvoller erscheinen zu lassen als der reale Wert, indem diese an eine neue, vom ursprünglichen Besitzer kontrollierte Wallet verkauft wird, wodurch der Marktpreis des Vermögenswerts in die Höhe getrieben wird[127].

Tatsächlich sind diese Arten von Finanzmanipulation mit NFTs relativ unkompliziert, da viele NFT-Handelsplattformen den Benutzern den Handel ermöglichen, indem sie ihre Brieftasche mit der Plattform verbinden, ohne sich identifizieren zu müssen[128]. Mit Hilfe der Blockchain-Analyse ist es jedoch möglich, den NFT-Wash-Handel zu

[123] Vgl.*Grauer* et al. (2022).
[124] Vgl.*Grauer* et al. (2022).
[125] Vgl.*Bluemel* (2023).
[126] Vgl.*Küster* (2022).
[127] Vgl.*Bluemel* (2023)..
[128] Vgl.*Grauer* et al. (2022).

verfolgen, indem die NFT-Verkäufe an selbstfinanzierte Adressen analysiert werden. Die Analyse der NFT-Verkäufe an selbstfinanzierte Adressen zeigt, dass einige NFT-Verkäufer Hunderte von Verkäufen an sich selbst getätigt haben[129]. Durch die manipulierten steigenden Zahlen mancher NFT-Werte werden immer mehr ahnungslose Käufer angelockt, während Besitzer der NFTs glauben, dass der gekaufte NFT, an Wert gewonnen hat und von einem Käufer an einen anderen verkauft wurde[130].

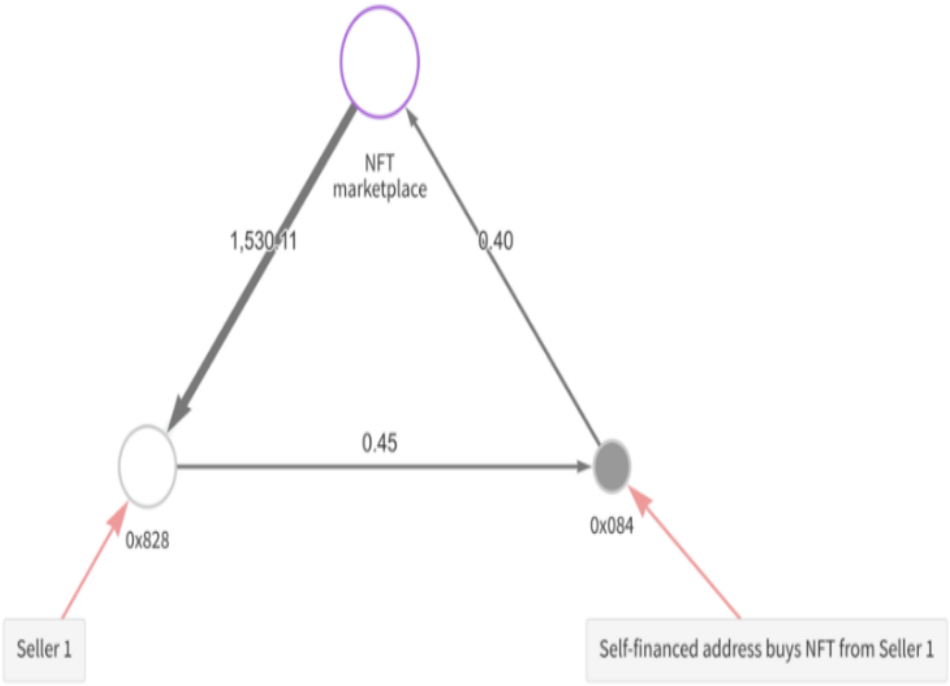


Abbildung 9: NFT Wash-Trading Beispiel[131]

In der obigen Abbildung ist erkennbar, wie ein NFT durch das Wash-Trading von einem Verkäufer an die selbstfinanzierte Adresse übertragen wird.

NFT-Wash-Trading bewegt sich in einer rechtlichen Grauzone. Obwohl Wash-Trading bei herkömmlichen zentralisierten Wertpapieren und Termingeschäften in hohem Maße illegal ist, wurden bisher keine Durchsetzungsmaßnahmen gegen Wash-Trading bei NFTs ergriffen. Dies könnte sich jedoch ändern, wenn die Regulierungsbehörden ihre Aufmerksamkeit und die geltenden Betrugsbekämpfungsgesetze auf neu entstehende NFT-Marktplätze anwenden. Wash-Trading bei NFTs erschafft im

[129] Vgl.*Bluemel* (2023).
[130] Vgl.*Grauer* et al. (2022).
[131] Vgl.*Ledger Academy*.

Allgemeinen einen ungerechten Markt für Einzelpersonen, die künstlich aufgewertete Token kaufen. Ebenso kann dessen Häufigkeit das Vertrauen in das NFT-Ökosystem untergraben und das zukünftige Wachstum einschränken[132]. Die unvorhersehbare Preisgestaltung von NFTs ist für Geldwäscher besonders attraktiv. Obwohl der Preis von Bitcoin und ähnlichen Kryptowährungen den Gesetzen von Angebot und Nachfrage auf dem Markt folgt, ist der Preis von NFTs extrem spekulativ[133]. Eine für 1 EUR gekaufte NFT kann am nächsten Tag für 1 Mio. EUR verkauft werden. Dies macht NFTs einsetzbar für die Wäsche von Schwarzgeld mit „legalen“ Mitteln[134].

4.4 FOMO bei Kryptovermögen

Um zu verstehen, warum es trotz des hohen Risikos für den durchschnittlichen Nutzer immer wieder Bestrebungen gibt, weiterhin in verschiedene Krypto-Assets zu investieren, unabhängig davon, wie fragwürdig das Produkt insgesamt ist, muss ein Phänomen betrachtet werden, das im Englischen als Fear-of-missing out FOMO bekannt ist. Dabei handelt es sich um den psychologischen Aspekt der Angst, etwas zu verpassen[135]. Die Versäumnisangst ist der Trieb des Menschen, der sich in einer sozialen Gemeinschaft befindet. Es liegt in der Natur des Menschen, neidisch zu sein und sich nach dem zu sehnen, was andere haben, und das Aufkommen der sozialen Medien hat dieses Feuer nur noch mehr angefacht. Die Kombination dieser beiden Triebkräfte kann daher zu dem Gedanken führen, nicht zurückzubleiben, wenn andere Menschen durch die Anlage in Kryptowährungen vermeintlich hohe Gewinne erzielen[136].

[132] Vgl.*Bluemel* (2023).
[133] Vgl.*Bluemel* (2023).
[134] Vgl.*IT-Daily* (2022).
[135] Vgl.*King University Online* (2019).
[136] Vgl.*King University Online* (2019).

5 Geldwäsche mit Kryptowährungen

5.1 Digitalisierung als Treiber

Der Ursprung der Geldwäsche ist als soziales Delikt ausgestaltet und erfordert die Zusammenarbeit mehrerer Akteure. Vor der Entwicklung des Internets war die räumliche Ausbreitung begrenzt, aber durch die Erweiterung des digitalen Raums haben Geldwäscher neue Möglichkeiten erhalten. Die Digitalisierung bietet Anonymität und schnelle, weltweite Transaktionen, die es Geldwäschern erleichtern, ihre Tätigkeiten zu verschleiern. Das Darknet und virtuelle Währungen, insbesondere die Blockchain-Technologie, werden von Geldwäschern genutzt, um Transaktionen zu verschleiern. Die fehlende Identifikation von Personen ist ein wichtiger Faktor, der dazu führt, dass Geldwäscher ihre Tätigkeiten ins digitale Umfeld verlagern. Die globale Vernetzung erleichtert auch das Auffinden von Geldkurieren für Straftäter[137].

5.2 Zweck der Geldwäscherei

Die Nutzung von Kryptowährungen zur Geldwäsche zielt darauf ab, illegal verschaffte Gelder über Handelsplattformen in den legalen Wirtschaftskreislauf einzuschleusen. Geldwäsche ist ein Straftatbestand nach § 261 StGB und kann mit einer Freiheitsstrafe von bis zu zehn Jahren geahndet werden. Um nicht in den Verdacht der Geldwäsche zu geraten, investieren Geldwäscher größere Geldbeträge in Kryptowährungssysteme auf verschiedenen Handelsplattformen. Die Kryptowährungen werden dann in gesetzliche Zahlungsmittel umgewandelt, um sie in den regulären Wirtschaftskreislauf einzubringen. Transaktionen können problemlos grenzüberschreitend abgewickelt werden, wobei der Tausch von Kryptowährungen in Fiatgeld weltweit möglich ist, auch zwischen Privatpersonen gegen Bargeld. Um die Nachvollziehbarkeit der Transaktionen zu erschweren, bedienen sich Geldwäscher spezieller illegaler Anonymisierungsdienste, um den Weg der Transaktionen zu verschleiern[138].

Geldwäscher haben unterschiedliche Platzierungs-, Stapelungs- und Integrationstaktiken. Je mehr Verfahren angewandt werden, desto mehr Geld kann effektiv

[137] Vgl.*Fiedler* et al. (2017).
[138] Vgl.*LHP* (2018).

gewaschen oder versteckt werden. Jedoch ziehen sie es vor, einige Strategien anzuwenden die Anonymität bewahren und harmlos aussehen[139].

Im Folgenden sollen die meistgenutzten Geldwäsche-Strategien näher erläutert werden.

5.3 Strategische Prozesse bei der Geldwäsche

Bei der Geldwäsche handelt es sich nicht um eine einmalige Handlung, sondern vielmehr um einen Prozess, der in drei Phasen unterteilt werden kann.

Abbildung 10: 3-Phasen der Geldwäsche[140]

Der erste Schritt bei der Geldwäsche ist die **Platzierungsphase**, bei der das Geld, das aus illegalen Einkünften erworben wurde, in den legalen Witschaftskreislauf eingeschleust wird[141]. Dies kann durch den Kauf von Wertgegenständen, wie z.B. Kunstwerken, Immobilien oder Kryptowährungen, erfolgen. In dieser Phase wird das Geld auch oft in kleineren Beträgen geteilt, um keine Aufmerksamkeit zu erwecken. Infolgedessen erfordert die Einzahlung unrechtmäßig erzielter Gewinne aus Bargeschäften eine Reihe von winzigen Einzahlungen über einen längeren Zeitraum und häufig auf viele Konten; diese Methode wird „Smurfing“ genannt[142]. Aufgrund der hohen Meldepflichten für Einlagen und der unvermeidlichen Bedenken, die entstehen, wenn

[139] Vgl.*Turner/Irwin* (2017).
[140] Vgl.*Dahmen* (2022).
[141] Vgl.*Martucci* (2022).
[142] *Martucci* (2022).

erhebliche Geldbeträge aus dem Nichts auftauchen, ist das Entdeckungsrisiko in der Platzierungsphase am höchsten[143].

Nach § 51 Abs. 8 GwG gilt „Bei Bartransaktionen, die von Kreditinstituten innerhalb einer Geschäftsbeziehung (z.B. Bareinzahlung auf ein Kundenkonto) durchgeführt werden, und die einen Betrag von 10.000 Euro überschreiten, ist grundsätzlich die Herkunft der Vermögenswerte durch aussagekräftige Belege nachzuweisen“[144]. Hat die Bank bereits bei einem geringeren Betrag Zweifel an der rechtmäßigen Herkunft des Bargeldes, kann auch bei einem geringeren Einzahlungsbetrag einen Herkunftsnachweis verlangt werden[145]. Es ist wichtig zu beachten, dass EU-weit ähnliche Anforderungen herrschen. Zusätzlich zu den oben genannten Anforderungen müssen die Banken auch Aufzeichnungen aufbewahren oder Berichte über verdächtige Aktivitäten erstellen, wie z. B. unerwartete Bareinzahlungen von Kontoinhabern, die solche Einzahlungen nicht regelmäßig vornehmen[146].

Die zweite Phase umfasst die **Verschleierungsphase**. Sie beinhaltet eine Reihe komplizierter und verwirrender finanzieller Manipulationen, welches die ursprüngliche Platzierung des Geldes in einzelne Teile zerlegt[147]. Ziel dieser Phase ist es, das illegal erworbene Geld so zu verändern, dass es seine Verbindung zur illegalen Ursprungquelle verliert. Dies ist ein komplexer Prozess, der häufig internationale Finanztransaktionen erfordert. Dies kann durch den Transfer von Geldern zwischen verschiedenen Konten oder die Übertragung in andere Währungen erfolgen. In dieser Phase können auch Scheinfirmen und Briefkastenfirmen eingesetzt werden, um die Herkunft des Geldes zu verbergen. Überweisungen zwischen Bankkonten, die manchmal unter mehreren Namen und bei vielen Institutionen in mehreren Ländern geführt werden, Immobilien- oder Dienstleistungstransaktionen mit Firmen oder legalen Unternehmensorganisationen, die nur auf dem Papier existieren und keine echte wirtschaftliche Rolle spielen, sind gängige Verschleierungsaktivitäten[148].

Kryptowährungen wie Bitcoin werden als Geldwäschemethode immer attraktiver, da sie nicht denselben regulatorischen Beschränkungen unterliegen wie traditionellere

[143] Vgl.*Martucci* (2022).
[144] *BaFin* (2021).
[145] Vgl.*BaFin* (2021)..
[146] Vgl.*Martucci* (2022).
[147] Vgl.*Martucci* (2022).
[148] Vgl.*Martucci* (2022).

Finanzderivate und Fiat-Währungen. Hier wird das Geld über eine Reihe von Transaktionen gestapelt oder transferiert, um die Ermittler zu verwirren und den Papierweg zu verkomplizieren[149]. Martucci (2018) merkt in diesem Kontext außerdem an, dass diese Manöver immer schwieriger und vielfältiger werden, je größer die Summen sind. Eine gängige Taktik in dieser Phase besteht darin, dass Kriminelle ihr Geld ins Ausland in mehrere Länder verschieben, in denen die Steuergesetze weniger streng sind; die Caymen-Inseln, Zypern und Panama sind einige Namen, die es den Kontoinhabern ermöglichen, ihre Namen und damit die Herkunft des potenziell kriminellen Geldes vor den Behörden zu verbergen. Bei grenzüberschreitenden Transaktionen sind die Gelder zur Vermeidung von Aufdeckung in Bewegung. Zu diesem Zweck werden Schlupflöcher in der Gesetzgebung der jeweiligen Länder ausgenutzt[150].

In der letzten Phase, der sogenannten **Integrationphase**, wird das gewaschene Geld schließlich „gereinigt“, indem das Geld aus einer scheinbar legalen Herkunft mit dem ursprünglichen Besitzer vereint wird. Die Integration gilt als die am wenigsten riskante Phase des dreistufigen Geldwäscheprozesses, da sie häufig legitime wirtschaftliche Interessen berührt[151]. Hier besteht die Absicht darin, das Geld wieder in die legale Wirtschaft einzuführen und es für legitime Zwecke zu verwenden. In dieser Phase kann das Geld beispw. in Investitionen in Luxusgüter, Immobilien und Firmeranteile fließen. Dazu gehört laut Martucci (2018) der Kauf von legitimen Wertpapieren oder anderen Finanzinstrumenten im Namen des Geldwäschers oder seiner legalen Geschäftsgesellschaften. Dieser Prozess ist zwar für den Kriminellen am sichersten, aber es gibt dennoch Methoden, mit denen die Behörden das gewaschene Geld aufspüren, verfolgen und beschlagnahmen können[152].

Kriminelle nutzen Kryptowährungen für Geldwäsche, da sie aufgrund ihrer Dezentralisierung und mangelnden Regulierung besonders beliebt bei Kriminellen sind. Die Anonymität von Kryptowährungen erschwert die Identifizierung des wirtschaftlich Berechtigten und ermöglicht es, Gelder mit krimineller Herkunft zu verschleiern. Kriminelle investieren einen Teil ihrer inkriminierten Gelder in Kryptowährungen und verschieben diese während des Layering-Prozesses zwischen verschiedenen Wallets, um die

[149] Vgl.*Martucci* (2022).
[150] Vgl.*Martucci* (2022).
[151] Vgl.*Martucci* (2022).
[152] Vgl.*Martucci* (2022).

Herkunft der Gelder zu verschleiern. Nach diesem Prozess können die Kryptowährungen an Tauschbörsen gegen andere Cyberwährungen oder Fiatgeld eingetauscht werden, was das Risiko für die Kriminellen verringert. Obwohl die Blockchain eine gewisse Transparenz bietet, bleibt die hohe Anonymität ein erhöhter Risikofaktor. Geldwäsche ist eine globale Bedrohung für die Wirtschaft, die auch vor der Existenz von Kryptowährungen bestand. Schätzungen zufolge wurden seit 2009 mehr als 2,5 Billionen US-Dollar mit Bitcoin gewaschen[153].

5.4 Eignung von Kryptowährungen zur Geldwäsche

Kryptowährungen bieten für Kriminelle im Hinblick auf die Geldwäsche eine Reihe von Vorteilen, die sich mitunter aus der weltweiten Verfügbarkeit und der Schnelligkeit der Transaktionen ergeben. „Aufgrund dieser großen Attraktivität auf der Täterseite werden Kryptowährungen mittlerweile in nahezu jedem Ermittlungsverfahren zur Internetkriminalität im festgestellt"[154], so das BKA. Die meisten Geldwäscheaktivitäten werden nach und nach aufgedeckt und so wird nach effektiveren Möglichkeiten zur Verschleierung und Tarnung der eigenen Machenschaften gesucht. Gerade die neuen Kryptowährungen bieten ein neues Spektrum an Möglichkeiten, um den Behörden die Aufdeckung zu erschweren[155].

Nachfolgend sollen das Bitcoin-System und die möglichen Geldwäschetechniken im Hinblick auf ihre Vorteile untersucht werden.

5.4.1 Anonymität

Die Anonymität der kryptographischen Währungen, vor allem der Bitcoin, ist ein wesentlicher Grund dafür, dass sie sich zur Durchführung krimineller Aktivitäten eignen. Transaktionen mit Kryptowährungen erfolgen verschlüsselt und können nur auf das Börsenkonto oder die Krypto-Wallet eines Nutzers zurückverfolgt werden. Während einige Kryptobörsen und Wallet-Anbieter von ihren Kunden die Angabe persönlicher Daten verlangen, bieten Tumbler- und Mixing-Dienste einen zusätzlichen Schutz für

[153] Vgl.*Teichmann International* (2021).
[154] *Littmann* (2021).
[155] Vgl.*ComplyAdvantage* (2022).

Transaktionen. Schließlich können Geldwäscher diese Tauschdienste für Kryptowährungen nutzen, um mehrere strukturierte Einzahlungen von unrechtmäßig erworbenem Geld in Mengen vorzunehmen, die keine AML-Meldekriterien auslösen[156]. Mit anderen Worten, er erleichtert die Schichtungsphase des Geldwäscheprozesses. Diese Dienste verschleiern die Spuren von Kryptowährungstransaktionen, indem sie diese auf mehrere Nutzer aufteilen und Coins aus verschiedenen Wallets mischen[157].

Dieser Vorteil der Anonymität bringt daher auch Risiken in Bezug auf illegale Aktivitäten wie Betrug mit sich, da Kryptowährungen Pseudo-Anonymität bieten. So ist es zum Beispiel möglich, sich lokal ein eigenes Wallet zu erstellen und von einer beliebigen Person Coins auf dieses einzahlen zu lassen, ohne persönliche Daten preisgeben zu müssen. Auch der Erwerb von Bitcoins oder anderen Währungen durch Mining kann ohne Angabe persönlicher Daten sein[158].

Anders als bei einem Bankkonto, bei dem sich der Kunde ausweisen und persönlich erscheinen muss, reicht bei Bitcoin ein Internetzugang aus, um Transaktionen durchzuführen. Bei einer Krypto-Adresse handelt es sich lediglich um eine Folge von Zahlen und Buchstaben, von denen es nahezu unendliche Kombinationen gibt. Einen Hinweis darauf zu finden, wer sich hinter einer bestimmten Bitcoin-Adresse verbirgt, ist daher schwierig[159]. Diese Pseudoanonymität kann jedoch leicht durchbrochen werden, wenn der Nutzer irgendwann eine Spur hinterlässt. Sobald eine Bitcoin-Adresse mit einer realen Identität verknüpft ist, kann die Identität des Nutzers, der mit dieser Adresse agiert, aufgedeckt werden. Aus diesem Grund bleibt die Anonymität von Kryptowährungen ein umstrittenes Thema, insbesondere wenn es um illegale Aktivitäten wie Geldwäsche geht[160].

5.4.2 Schwere Rückverfolgbarkeit

Die Schwierigkeit der Rückverfolgbarkeit hängt auch mit der Pseudoanonymität bzw. der Funktionsweise der Blockchain an sich zusammen. Es bedarf einen enormen

[156] Vgl.*ComplyAdvantage* (2022).
[157] Vgl.*ComplyAdvantage* (2022).
[158] Vgl.*ComplyAdvantage* (2022).
[159] Vgl.*Grzywotz* (2019), S. 99.
[160] Vgl.*ComplyAdvantage* (2022).

technischen Aufwand, einen Token zu einer bestimmten Person zurückzuverfolgen. Nur in schwerwiegenden Fällen wäre ein solches Verfahren lohnend. Allerdings ist es beim heutigen Stand der Technik nicht möglich, jeden Token und Wallet ständig zu überwachen. Noch weniger ist es möglich, dass jede Transaktion einer Person zugeordnet werden kann. Wie bereits erwähnt, ist es verschiedenen Forschergruppen bereits gelungen, die Adressen von Wallets auch über das Darknet hinweg zu lokalisieren und einer IP-Adresse zuzuweisen. Allerding ist das nur in einer experimentellen Umgebung und nicht mit einer absoluten Genauigkeit möglich. Die Zukunft bietet jedoch viele Möglichkeiten, insbesondere im Gebiet der künstlichen Intelligenz[161].

5.4.3 Datenschutz

Eine breit angelegte Überwachung der Transaktionen von Personen bedeutet nicht nur einen immensen technischen und kostenintensiven Aufwand, sondern auch einen massiven Eingriff in die Privatsphäre der Nutzer. Sowohl das Privatrecht als auch das Verfassungsrecht schützen das Recht auf Privatsphäre, wobei der Staat nur dann in die privaten Aktivitäten eingreifen darf, wenn dies gesetzlich vorgesehen und ausreichend notwendig für die Gewährleistung öffentliche Sicherheit, die Vorbeugung von Straftaten, oder der Schutz der Rechte und Freiheiten ist. Allerdings müssen auch in diesen Fällen bestimmte Voraussetzungen erfüllt sein, und es besteht immer das Risiko einer Verletzung der Privatsphäre und anderer Grundfreiheiten[162].

5.4.4 Dezentralität

Wie bereits im Kapitel 2.4 erläutert, gibt es im Kryptovermögens-System im Gegensatz zu Kredit- und Finanzinstituten keine zentralisierte Verwaltung, die verdächtige Transaktionen prüfen und an Geldwäschemeldestellen melden kann. Intermediäre spielen hier eine wichtige Rolle, da sie eine Schnittstelle zwischen Geldwäschern und Behörden darstellen und verdächtige Aktivitäten aufdecken können. Folglich hat ein

[161] Vgl.*ComplyAdvantage* (2022).
[162] Vgl.*ComplyAdvantage* (2022).

Geldwäscher durch die Verwendung der Kryptowährung einen Vorteil, da keine Überwachung durch eine zentrale Macht herrscht[163].

5.4.5 Globalität

Kryptowährungen ermöglichen grenzüberschreitende Transaktionen ohne Hindernisse und erleichtern somit das Waschen inkriminierter Gelder in Ländern mit hohem Geldwäscherisiko. Die Eigenschaften des Kryptowährungs-Systems fördern das Waschen von Geldern, indem sie das Drei-Phasen-Modell der Geldwäsche unterstützen. Kryptowährungen sind ein neues Werkzeug in diesem Prozess, dass zwei Fallkonstellationen ermöglicht: die Unterbringung der beanstandeten Werten im Blockchain-System und die Platzierung von strafbaren Kryptocoins. In der Verschleierungsphase können Geldwäscher eine Vielzahl von Transaktionen durchführen, um inkriminierte Coins zu verschleiern, indem sie zwischen Adressen verschoben oder durch Finanzagenten einbezogen werden. In der Integrationsphase können Geldwäscher ihre Auszahlungen unkompliziert in Ländern mit geringeren Anforderungen zur Geldwäscheprävention verlegen, indem sie den Tausch von Kryptocoins in Fiat-Währungen nutzen. Neue Coins können auch durch den Kauf von Wertobjekten oder Mining-Hardware mit inkriminierten Kryptowährungen generiert werden[164].

5.4.6 Effizienz

Schließlich ist die Effizienz ein weiterer wesentlicher Aspekt, den es in diesem Zusammenhang zu erwähnen gilt. Die Tatsache, dass Transaktionsraten schnell durchgeführt werden können, in einigen Fällen innerhalb von Sekunden, bieten Geldwäschern ein höheres Maß an Effizienz als Fiat-Währungen und die Möglichkeit, Gelder zu verschleiern, bevor Geldwäschebekämpungsverfahren („Anti-Money-Laundering (AML)“) sie bemerken.[165]

[163] Vgl.*Grzywotz* (2019), S. 98.
[164] Vgl.*Grzywotz* (2019), S. 100.
[165] Vgl.*ComplyAdvantage* (2022).

5.5 Warnsignale der Krypto-Geldwäsche

Es gibt einige Warnsignale, die auf eine potenzielle Geldwäsche mit Kryptowährungen hinweisen können. Dazu gehören das Transaktionsverhalten, die Identität des Kunden, der Einsatz von Geldkurieren oder der Ort, an dem der Krypto-Vermögenswert ursprünglich gefunden wurde[166].

Zu den Transaktionsarten und -mustern gehören mehrere Transaktionen mit kleinen Beträgen, Transaktionen, die nicht zum Risiko- oder Vermögensprofil eines Kunden passen, und regelmäßige Transaktionen, die zu häufigen Verlusten führen. Außerdem ist das Transaktionsvolumen zu beachten, wenn ein Konto ungewöhnlich hohe Transaktionen in kurzer Zeit tätigt. Ungewöhnliche und unregelmäßige Muster wie häufige Transaktionen zwischen Fiat- und Kryptowährungen ohne offensichtlichen geschäftlichen Grund können auch Anzeichen für illegale Aktivitäten darstellen[167].

Weitere rote Fahnen sind auch Geldkuriere, deren Finanzdaten nicht mit ihrem derzeitigen Lebensstil übereinstimmen oder letztlich Gelder aus Quellen beziehen, die mit illegalen Operationen, Darknet und Webseiten mit unzureichenden AML-Verfahren[168]. Auch kann die Verwendung von Mixing Services darauf hindeuten, dass es beabsichtig wurde die Transaktion zu verheimlichen, um die Herkunft von Kryptowährungen zu verschleiern. Wenn eine Kryptowährungstransaktion in Länder mit schwachen Regulierungen stattfindet, kann dies ein auch Hinweis sein, da solche Länder oft als Zufluchtsort für illegale Aktivitäten genutzt werden. Es ist wichtig zu beachten, dass keines dieser Warnsignale allein ausreicht, um sicherzustellen, dass eine Transaktion tatsächlich eine Geldwäsche darstellt. Eine sorgfältige Untersuchung aller Fakten und Umstände ist notwendig, um eine angemessene Entscheidung zu treffen[169].

5.6 Mittel und Methoden für Geldwäsche

Die folgenden Abschnitte beleuchten einige der Methoden, die von Kriminellen verwendet werden, um ihre unrechtmäßig erworbenen Gewinne auszunutzen.

[166] Vgl.*ComplyAdvantage* (2022).
[167] Vgl.*ComplyAdvantage* (2022).
[168] Vgl.*ComplyAdvantage* (2022).
[169] Vgl.*ComplyAdvantage* (2022).

Da Banken und andere Finanzinstitute ihre Fähigkeiten zur Aufdeckung von Geldwäsche weiter verbessern, tun dies auch Kriminelle, die davon profitieren wollen. Das heutige Geldwäschesystem ist so komplex, dass es viele Menschen davon abschreckt, sich illegal Geld zu beschaffen, doch der Aufstieg der Blockchain und von Krypto-Vermögenswerten auf der globalen Ebene hat diese Barriere beseitigt[170].

In den vorangegangenen Abschnitten war zu erkennen, wie die Finanzwelt es kriminellen Organisationen ermöglicht hat, von den dezentralisierten Märkten zu profitieren, indem sie durch Betrugsmaschen naive Verbraucher und Schlupflöcher des Staates ausnutzen. In den folgenden Abschnitten werden einige der Instrumente vorgestellt, die auf dem Markt eingesetzt werden, um die Bewegung von illegal erlangten Gewinnen zu erleichtern, die für jeden mit einem Grundverständnis von Krypto zugänglich sind. Außerdem wird ein Einblick in einige der gängigsten Methoden gegeben, die auf dem Markt vorherrschend sind, um Geld über verschiedene Krypto-Vermögenswerte zu waschen, mit geringen bis gar keinen Auswirkungen, zu waschen.

5.6.1 Mixing-Dienste

Eine, für Kriminelle gängige Methode, mit der Krypto-Nutzer ihre Blockchain-Transaktionen verschleiern können, besteht darin ihre unrechtmäßig erworbenen Gewinne an einen zentralen oder dezentralen "Mixer" zu senden[171]. Bereits zahlreiche Unternehmen haben diese Chance für sich ergriffen und angefangen mit der Verschlüsselung von Kryptotransaktionen einen neuen Markt zu erobern. Sogenannte Mixer fungieren als Zwischenstufe im Geldwäscheprozess und erfordern deutlich weniger Zeit und Kosten als herkömmliche Geldwäscheprozesse[172].

Ein Kryptowährungs-Mixer, auch Tumbler genannt, ist ein Dienst, der zur Verbesserung der Anonymität von Kryptowährungstransaktionen beiträgt, indem er die Coins mehrerer Nutzer zu einem großen Geldbestand mischt. Dabei wird die Verbindung zwischen den Adressen des Senders und des Empfängers unterbrochen und die Rückverfolgbarkeit der Transaktion erschwert. Um die Rückverfolgung des Transaktionsverlaufs zu erschweren, kann der Mischvorgang mehrfach wiederholt werden.

[170] Vgl.*ComplyAdvantage* (2022).
[171] Vgl.*Stevens* (2022).
[172] Vgl.*Stevens* (2022).

Dazu können die Coins über mehrere Adressen geleitet und mehrfach mit Coins anderer Teilnehmer vermischt werden. Dazu sendet der Nutzer den entsprechenden Geldbetrag in Form seiner Kryptowährung an den Mixer-Dienst, der diesen über weitere Umwege an den eigentlichen Empfänger weiterleitet. Meist wird eine Off-Chain-Stückelung mit einer zeitversetzten Ausgabe des zu mischenden Betrags kombiniert. Die Herkunft des Zahlungsmittels kann umso besser verschleiert werden, je mehr Nutzer in diesem Off-Chain-Netzwerk ihre Kryptowährung mischen[173].

Diese Mixer können als eine Art Tauschbörse für Kryptowährungen betrachtet werden. Eine Person hat bspw. den Wunsch, einen Bitcoin vollständig zu anonymisieren und seine Herkunft zu verschleiern. Wird dieser Bitcoin in einen Pool von bereits vermischten Bitcoins eines Bitcoin-Mixers eingebracht, ist nicht mehr nachverfolgbar, von wem diese Transaktion stammt. Mixer stellen somit ein großes Hindernis hinsichtlich der Nachvollziehbarkeit von Transaktionen dar und werden deshalb häufig für illegale Aktivitäten verwendet. Dies senkt die Einstiegshürde für Personen, die schwache staatliche Regulierungen ausnutzen wollen, um mehr Geld zu verdienen.

Mixer funktionieren, indem sie denselben Geldbetrag an mehrere Krypto Adressen überweisen, jegliche Blockchain-Verknüpfungen zwischen Mixer-Nutzern verbergen und die Rückverfolgbarkeit durch den Blockchain-Ledger so weit wie möglich zerstören[174]. Sie machen es für Rückverfolgungstools nahezu unmöglich die gestohlenen Kryptowährungen von den legitimen Währungen zu unterscheiden, und unterbrechen damit die Verbindung zu Möglichkeit, potenzielle Kriminelle herauszufinden. Es fügt eine zusätzliche Ebene des Schutzes für die Kriminellen hinzu, die verschiedene Strafverfolgungsbehörden durchbrechen müssen. Stevens (2022) betont, dass in Anbetracht der Tatsache, dass es sich bei der Blockchain noch um eine neue Technologie handelt, die sich in der Gesellschaft neu etabliert, die Kompetenz der Strafverfolgungsbehörden bestenfalls noch fraglich ist[175].

Als Beispiel kann in diesem Zusammenhang der sogenannte Tornado Cash herangezogen werden. Dieser war der bekannteste Mixer auf der Ethereum-Blockchain, der sowohl für legale als auch illegale Transaktionen genutzt wurde. Das System

[173] Vgl.*Stevens* (2022).
[174] Vgl.*Stevens* (2022).
[175] Vgl.*Stevens* (2022).

funktionierte durch den Einsatz von intelligenten Verträgen, die es ermöglichten, Anonymität zu wahren, indem Token-Einzahlungen von einer Adresse akzeptiert und Abhebungen von einer anderen Adresse vorgenommen wurden. Die intelligenten Verträge agierten als Pools für alle Vermögenswerte, die in eine zentrale Wallet eingezahlt wurden. Die Beziehung zwischen Quelle und Ziel wurde unterbrochen, wenn das Geld aus diesen Pools durch eine neue Adresse ersetzt wurde, wodurch die entnommenen Krypto-Vermögenswerte anonym waren. Die Nutzer hatten das Sorgerecht für ihre Token, solange sie sich in einem Tornado Cash-Pool befanden, und das System war dezentralisiert, so dass kein Akteur auf den Pool zugreifen oder sehen konnte, wo und welches Ethereum in den Pool gelangte. Dieser strukturelle Aufbau verhinderte auch, dass Regierungen Vorladungen für Informationen ausstellen konnten, und ermöglichte es Tornado Cash, der größte Anbieter von Mischdiensten auf der Ethereum-Blockchain zu werden[176].

In der folgenden Grafik wird der vereinfachte Aufbau eines solchen Mixers dargestellt.

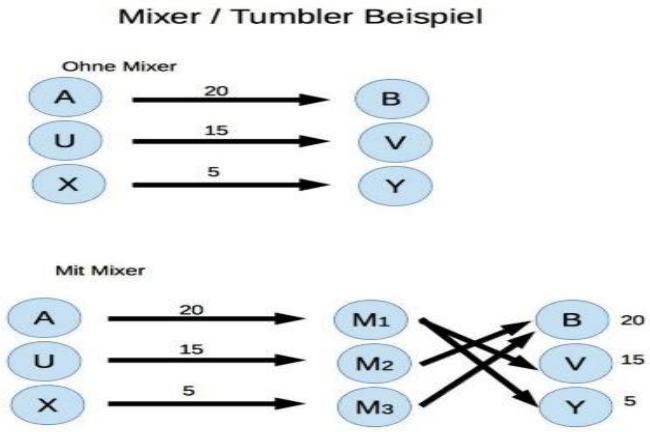


Abbildung 11:Mixer Struktur[177]

5.6.2 Peel Chains

Eine Peel Chain ist eine Methode zur Wäsche großer Geldbeträge durch eine Abfolge von kleinen Transaktionen[178]. Unter geringfügigen Überweisungen von den

[176] Vgl.*Maihofer* (2022).
[177] Vgl.*Compliance Blog*.
[178] Vgl.*Hudson Intelligence* (2022b).

ursprünglichen Beträgen wird ein kleines Stück der Kryptowährung in der Adresse des Kriminellen eingebracht. Diese inkrementellen Ausgaben werden häufig an Börsen geschickt, wo sie in Fiat-Währung wie Euro oder Dollar oder andere Vermögenswerte umgetauscht werden können[179]. Laut Hudson Intelligence (2022), werden die übrig gebliebenen Kryptowährungen aus der Hauptwallet dann an neue Adressen übertragen, und die anschließend wiederholt. Es ist weniger wahrscheinlich, dass die Ergebnisse der Peel-Kette bei Börsen für virtuelle Vermögenswerte Bedenken für die Einhaltung der AML-Vorschriften auslösen oder zu einer obligatorischen Meldung an Steuer- und Aufsichtsbehörden führen, aufgrund der winzigen Beträge jedes einzelnen Transfers[180]. Zur Erhöhung der Komplexität der Verfolgung von Vermögenswerten bis zu einem Fiat-Derivat oder Endziel entwickeln Kriminelle Kryptowährungen Schälketten von extremer Länge[181].

Forensische Methoden und Blockchain Intelligence-Technologien können die Effizienz der Verfolgung von Bargeldbewegungen in einer Betrugsuntersuchung erheblich verbessern. Allerdings ist der Prozess langwierig. Je komplexer die Kette wird, desto größer ist die Wahrscheinlichkeit von Fehlern[182].

In der unteren Abbildung wird die vereinfachte Vorgehensweise der Peel-Chains, am Beispiel von Bitcoins, dargestellt.

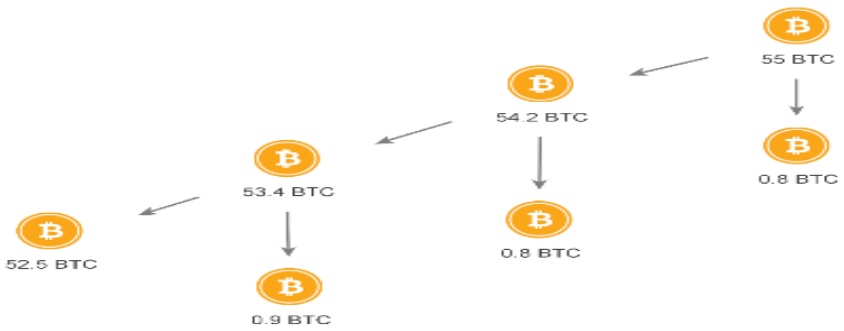


Abbildung 12: Peel Chains anhand Bitcoin[183]

[179] Vgl.*Hudson Intelligence* (2022b).
[180] Vgl.*Hudson Intelligence* (2022b).
[181] Vgl.*Hudson Intelligence* (2022b).
[182] Vgl.*Hudson Intelligence* (2022b).
[183] Vgl.*Maltego Team*.

5.6.3 Chain-Hopping

Das Chain-Hopping ist eine zusätzliche Methode, mit der Kriminelle versuchen, die Fähigkeit des Blockchain Tracking-Tool zu stören, um die Devisenbewegungen zu verfolgen, wenn die Layering-Phase im Geldwäscheprozess eintritt. Chawla (2017) erklärt, dass Chain Hopping im Wesentlichen dadurch funktioniert, dass die gestohlenen Kryptowährungen mehrmals in eine andere Kryptowährung umgewandelt werden, bis sie gegen Fiat-Geld ausgetauscht wird oder nicht mehr zu den ursprünglich gestohlenen Geldern zurückverfolgt werden kann[184].

Auch unregulierte Kryptowährungsbörsen ermöglichen es Kriminellen, Geld zu waschen durch den Einsatz von Kryptowährungen. Kryptowährungen können auf zahlreichen Marktplätzen platziert und auf unregulierten Börsen getauscht und für verschiedene Coins auf Börsen gehandelt werden, die keine strengen, strikten und rigorosen Identitätsprüfungen durchführen. Wiederholte Verschiebungen von einer Kryptowährung zur anderen können die Coins allmählich bereinigen, den Betrüger dann in eine Wallet eines Drittanbieters verschieben können[185].

5.6.4 CoinJoins

CoinJoin ist eine weitere Methode, mit der die Anonymität und Verschleierung von Kryptowährungstransaktionen erhöht werden kann. Der Grundgedanke ist, verschiedene Einträge von verschiedenen Benutzern in einer einzigen Transaktion zusammenzufassen, so dass nur schwer zu erkennen ist, welcher Eintrag zu welcher Ausgabe gehört. Dadurch wird die wahre Herkunft und Bestimmung von Geldern verschleiert und es wird schwieriger, Transaktionen zu verfolgen und nachzuvollziehen[186].

Die Implementierung des CoinJoin-Protokolls erfolgt durch Software oder Dienste, mit denen Nutzerinnen und Nutzer Teil des Prozesses werden können. Möchte ein Nutzer eine Transaktion durchführen, sendet er seine Eingaben an den CoinJoin-Dienst, der diese mit denen anderer Nutzer zu einer Transaktion zusammenführt. Diese

[184] Vgl.*Shivam Chavla* (2017).
[185] Vgl.*Elliptic* (2019).
[186] Vgl.*Hayes* et al. (2021).

Transaktion wird schließlich an das Netzwerk zur Verarbeitung und Bestätigung in Form einer einzigen Überweisung weitergeleitet[187].

5.6.5 Offline Kryptowechselautomaten

Der Wechsel von Kryptowährung zur klassischen Währung ist ein Vorgang, bei dem die Anonymität am meisten beeinträchtigt wird. Um dies zu vermeiden, sollte der Wechsel so durchgeführt werden, dass keine personenbezogenen Informationen angegeben werden müssen und der Geldfluss nicht später einer Person zugeordnet werden kann. Ein Wechselautomat eignet sich, wenn keine Registrierung mit echten Namen erforderlich ist. Es gibt jedoch Unterschiede in Bezug auf die Ausweispflicht und Registrierung bei der Nutzung solcher Automaten. Die meisten Automaten unterstützen nur den Wechsel von Fiatwährung zu Kryptowährung, nicht umgekehrt. Bei einigen Automaten müssen vor der Nutzung Registrierungsschritte durchgeführt werden. Über die meisten Automaten ist es jedoch möglich, bis zu einem Betrag von 500 Euro anonym Kryptowährungen zu erwerben. Beträge über 500 Euro erfordern eine Verifizierung mittels amtlichen Lichtbildausweises. Es gibt zwar wenige bis kaum Automaten in Deutschland, die den Tausch von Krypto- gegen Fiatwährung ermöglichen, aber solche Anbieter sind in der Schweiz, Slowenien und Österreich aktuell öfter zu finden. Beispiele hierfür sind „Coins2Go“ oder auch „Mr.Coin“. Es bleibt jedoch ein Risiko, dass im Wechselautomaten biometrische Erkennungssysteme von Personen aufzeichnen[188].

Bis September 2019 waren weltweit 5.457 Bitcoin-Geldautomaten im Betrieb[189]. Elliptic (2019) erklärt, dass Bitcoin-Geldautomaten es jedem mit einer Kredit- oder Debitkarte ermöglichen, Bitcoin zu kaufen, da diese Geldautomaten immer mit dem Internet verbunden sind. Auch können Geldautomaten Bitcoins in Bargeld umtauschen, indem sie eine einscannbare Wallet-Adresse verwenden. Darüber hinaus bieten Bitcoin-Geldautomaten zur Annahme von Bareinzahlungen auch einen QR-Code, der gescannt werden kann, um Bitcoin oder andere Kryptowährungen an einer herkömmlichen Börse abzuheben[190]. Die Gesetze, die Finanzinstitute zur Erstellung von Kunden-

[187] Vgl.*Hayes* et al. (2021).
[188] Vgl.*Elliptic* (2019).
[189] Vgl.*Elliptic* (2019).
[190] Vgl.*Elliptic* (2019).

und Transaktionslisten für diese Automaten verwenden, unterscheiden sich von Land zu Land und werden häufig nicht streng genug durchgesetzt[191].

5.6.6 Prepaid-Karten und Glücksspielseiten

Eine weitere Methode zum Waschen von Coins ist die Verwendung von Prepaid-Kreditkarten, auf welche die Kryptowährung geladen sind.[192] Prepaid-Karten können gegen andere Währungen getauscht, zur Finanzierung verschiedener rechtswidriger Operationen verwendet oder zusammen mit den entsprechenden PINs an Dritte weitergegeben werden[193]. Die Glücksspieltechniken, die zur Durchführung von Geldwäsche mit Kryptowährungen verwendet werden, bestehen darin, Online-Glücksspiele über Plattformen zu betreiben, die Bitcoin oder andere Kryptowährungen akzeptieren. Nutzer können mit Kryptowährungen virtuelle Guthaben oder Chips kaufen und diese dann nach einigen Transaktionen wieder einlösen[194].

5.6.7 Online-Kriminalität im Darknet

Ein weiterer großer Bereich des illegalen Einsatzes von Kryptowährungen ist der kriminelle Handel im Darknet. Das Internet wird zum besseren Verständnis in drei Bereiche unterteilt. Zum einen in das sichtbare und legale Web, zum anderen in das Deep Web, welches aus Seiten besteht, die nicht verzeichnet sind und daher nicht über Suchmaschinen gefunden werden können und zum Dritten in das Darknet. Unter dem Begriff Darknet wird ein kleiner Teil des sehr viel größeren Deep Web verstanden. Für den Zugriff auf die nicht verzeichneten Seiten des Deep Webs und damit auch auf die Webseiten des Darknets ist ein bestimmter Browser notwendig[195].

Dieser Browser ist der sogenannte TOR-Browser (The Onion Router). Das TOR-Netzwerk ist eine Art „Virtuelles Privates Netzwerk (VPN)“, bei dem es sich um ein in sich geschlossenes Kommunikationsnetzwerk handelt. Dieses Tor-Netzwerk hindert die Nachvollziehbarkeit von Daten, indem es alle Informationen durch das Netzwerk

[191] Vgl.*Elliptic* (2019).
[192] Vgl.*Elliptic* (2019).
[193] Vgl.*Elliptic* (2019).
[194] Vgl.*Elliptic* (2019).
[195] Vgl.*Eckermann* (2017)..

schickt, fragmentiert und am Schluss wieder zu einer verständlichen Information zusammensetzt. So wird verhindert, dass jemand nachverfolgen kann, welche Webseiten eine Person besucht hat, und dass die aufgerufenen Webseiten etwas über den Nutzer selbst aufdecken können[196]. Durch die Anonymität der Verbindung ist das Darknet besonders gut geeignet für die Abwicklung illegaler Geschäfte. In den unendlichen Bereichen des Darknets gibt es Internetseiten, auf denen alles Mögliche verhandelt werden kann, vor allem aber auch illegale Drogen und der Handel mit Waffen. Insbesondere in Verbindung mit Kryptowährungen, die noch eine zusätzliche „Anonymität“ bieten, kann dort alles nahezu risikolos gehandelt werden. Einzig die gekaufte Ware zu erhalten, kann für den Konsumenten risikobehaftet bleiben. Schließlich muss er einen Übergabeort angeben. Als Zahlungsmittel werden auf diesen Dark Sites sogar ausschließlich Kryptowährungen angeboten[197].

Um die Registrierungspflichten der Tauschbörsenbetreiber zu umgehen, sind Kriminelle auf die Nutzung eines VPN angewiesen. Mit Hilfe des Tor-Browsers kann die eigene IP-Adresse so verschleiert werden, dass keine Rückschlüsse auf eine bestimmte Person mehr möglich sind. Kombiniert mit der Nutzung öffentlicher Netze, bei denen auch keine Authentifizierung erforderlich ist, führt dies zu einer enormen Rückverfolgbarkeitssicherheit[198].

[196] Vgl.*Eckermann* (2017).
[197] *Eckermann* (2017).
[198] *Anonym im Netz* (2018).

6 Betrug mit Kryptowerten

Laut Chainanalysis entfällt die Mehrheit der illegalen Transaktionen durch Kryptowerte weiterhin auf den Betrug. Betrug mit Kryptowährungen ist fast so alt wie die Kryptowährung selbst. Eine Studie ergab, dass im Jahr 2020 Betrug die häufigste Art von Krypto-basiertem illegalen Handel ausmachte, gefolgt von Ransomware-Angriffen und Darknet-Marktplätzen. Betrug machte dabei fast 54% aller untersuchten illegalen Transaktionen aus. Neueste Untersuchungen zeigen einen Steigerung in der Komplexität und Ausgereiftheit der Attacken[199]. Chainalysis stellte jedoch auch fest, dass der Anteil von Betrugstransaktionen insgesamt im Jahr 2020 gegenüber 2019 zurückging. Dies könnte darauf hinweisen, dass die Einführung von verbesserten Anti-Geldwäsche- und Betrugsbekämpfungsmaßnahmen sowie die zunehmende Zusammenarbeit zwischen Regulierungsbehörden und Kryptowährungsunternehmen Wirkung zeigen. Trotzdem bleibt Betrug ein wichtiges Problem im Kryptowährungsraum[200].

Im Folgenden werden die gängigsten Betrugssysteme im Hinblick auf Kryptowährungen zusammengefasst.

Krypto Scams

Bei dem sogenannten Krypto Scams Betrugssystem werden potenziellen Anlegern schnelle und sichere Renditen für ihre Investitionen in Kryptowährungen versprochen. Die Betrüger nutzen gefälschte Websites, Social-Media-Plattformen, gefälschte Whitepapers und gefälschte App-Downloads, um die Nutzer dazu zu bringen, ihre Kryptowährungen an die Betrüger zu senden[201].

Phishing

Hierbei versuchen Kriminelle, Zugangsdaten und private Schlüssel zu stehlen, indem sie gefälschte E-Mails, Nachrichten oder Social-Media-Beiträge verwenden, um an vertrauliche Informationen zu gelangen[202].

[199] Vgl.*Grauer* et al. (2022)..
[200] Vgl.*Grauer* et al. (2022).
[201] Vgl.*Chainanalysis* (2023).
[202] Vgl.*Chainanalysis* (2023).

Ponzi-Systeme

Ein betrügerisches Unternehmen verspricht Anlegern, dass ihre Investitionen in Kryptowährungen durch eine hohe Rendite schnell vermehrt werden. Die Auszahlungen erfolgen jedoch nicht aus den Gewinnen, sondern aus den Einlagen neuer Investoren[203].

Fake Wallets

Betrüger entwickeln gefälschte Kryptowährungs-Wallets, die den Benutzer dazu bringen, private Schlüssel zu teilen. Die Betrüger können dann die Kontrolle über die Kryptowährungen des Opfers übernehmen[204].

Mining-Betrug

Kriminelle verkaufen gefälschte Mining-Geräte oder Mining-Pools, die vorgeben, hohe Erträge zu erzielen. In Wirklichkeit sammeln die Betrüger lediglich die Investitionen ein, ohne tatsächlich Mining-Aktivitäten durchzuführen[205].

Nachfolgend wird näher auf die einzelnen Anwendungsfälle dieser Betrugsarten eingegangen.

6.1 Betrugsarten

6.1.1 Pig-Butchering Betrug

„Pig Butchering“ ist der neueste Trend in der Krypto-Cyberkriminalität, dessen Ursprung in China liegt und sich aktuell international ausbreitet. Diese Betrugsmasche spielt sich hauptsächlich auf Online-Dating-Plattformen ab, bei denen Cyberkriminelle engen Kontakt zu ihren Zielpersonen herstellen. Die Emotionen der Opfer werden dann für ihren illegalen finanziellen Gewinn ausgenutzt, der mehrere Millionen Euro erreichen kann[206].

[203] Vgl.*Chainanalysis* (2023).
[204] Vgl.*Chainanalysis* (2023).
[205] Vgl.*Chainanalysis* (2023).
[206] Vgl.*Dewerne* (2023).

Die Betrüger beginnen, indem Sie ein ansprechendes Profilbild verwenden und versuchen mit Textnachrichten das Opfer, in dem Fall "Pig (=Schwein)", anzulocken. Durch mehrere Unterhaltungen locken sie ihre Opfer mit Komplimenten und erschwindeln so eine Bindung. Schließlich folgen Geld- und Anlagetipps über Gewinnmöglichkeiten mit Kryptowährungen. Der Betrüger informiert das Opfer schließlich über eine bedeutende Methode zum Geldverdienen mit Kryptowährungen und versucht es zu überzeugen, sich an der gefälschten Investitionsmöglichkeit zu beteiligen, die theoretisch profitabel erscheint. Sobald sich das Opfer auf diese Investition einlässt, wird es auf eine gefälschte Krypto-Plattform gelockt, welches wie ein vertrauenswürdiges, legitimes Finanzinstitut erscheint. Nach Registrierung auf dieser Plattform, wird eine Wallet eröffnet, auf welches das virtuelle Geld eingezahlt wird. Hier kann der Nutzer an gefälschten Echtzeit-Markdaten einsehen, wie sich die Investition rentiert. So versucht der Betrüger mittels verschiedener Methoden, sich große Geldsummen überweisen zu lassen[207]. Das eingezahlte Geld fließt auf direktem Wege dem Betrüger zu. Wenn das Wallet des Opfers voll genug ist, wird, wie es im Cyber-Jargon heißt, das Schwein „geschlachtet“. Der Betrüger verschwindet mit all dem eingezahlten Geld. Zum Schluss werden die Konten geschlossen und die Website der Kryptowährung ist nicht mehr erreichbar[208].

In der Finanzwelt ähnelt diese Methode dem so genannten Anlagebetrug, bei dem ein Angebot meist zu gut ist, um wahr zu sein, was der Grund ist, dass diese Betrugsmasche so hohe Erfolge erzielt. Der englische Ausdruck „Pig Butchering“ ist somit der Begriff für ein Betrugsschema in der Krypto-Welt, bei dem die ahnungslose Menschen durch emotionale Manipulation in die Falle gelockt und ausgebeutet werden[209].

Laut den Angaben der Global Anti Scam Organization (GASO), die von einem ehemaligen Opfer dieser Betrugsmasche gegründet wurde, ist der durchschnittliche Verlust pro Opfer etwa 122.000 US-Dollar, wobei die Mehrheit der Opfer Frauen im Alter zwischen 25 und 40 Jahren sind[210]. Der finanzielle Erfolg der Cyberkriminellen, der ihnen die Möglichkeit für eine weitere Ausweitung ihrer Aktivitäten verschafft, treibt die Verbreitung von "Pig Butchering" voran. Die Herausforderungen bei der Ermittlung und

[207] Vgl.*Bailey* (2022).
[208] Vgl.*datensicherheit.de* (2022).
[209] Vgl.*datensicherheit.de* (2022).
[210] Vgl.*IT-Daily* (2022)..

Untersuchung von Straftaten zeigen, dass die Täter über ein hohes Maß an Fachwissen verfügen[211].

Jüngst kursierten in den amerikanischen, aber auch deutschen Medien, immer mehr Meldungen zu Personen, die der Pig-Butchering Masche zum Opfer gefallen sind. Den Behörden zufolge werden die gemeldeten Verluste seit 2011 auf rund 575 Millionen Dollar geschätzt[212].

6.1.2 Pump-and-Dump-Betrug

Pump-and-Dump (PnD) ist ein Betrugsmodell im Zusammenhang mit dem Handel von Kryptowährungen, welches in den letzten Jahren bei Betrügern ebenfalls sehr gefragt ist. Ein PnD-Schema besteht darin, den Kurs einer Kryptowährung künstlich zu steigern (“pumping”), indem unrichtige, täuschende oder unzutreffende Darstellungen zum Kurs der Coins bzw. des Tokens gemacht werden, um neue Käufer für das Projekt zu gewinnen. In der Folge verkaufen die Betrüger ihre voreilig gekauften Anteile/Coins und lassen den Kurs wieder einbrechen. Pump-and-dump"-Betrügereien sind bei reguliertem Finanzwesen höchst illegal, aber durch den Mangel an Regulierungen, im Vergleich zu Aktien, die an den großen US-Börsen gehandelt werden, ist der „wilde Westen“ der Krypto-Welt voll von Betrug, einschließlich dem Pump-and-Dump-Schema[213].

Aufgrund der Tatsache, dass der Kryptowährungsmarkt noch weitgehend unreguliert ist und es sich um eine vergleichsweise überschaubare und geschlossene Nutzergemeinschaft handelt, ist die Organisation eines PnDs besonders einfach[214]. Häufig geht es darum, Kryptowährungen zu manipulieren, die eine sehr geringe Marktkapitalisierung aufweisen. Aus diesem Grund können Angaben über die Coins leicht Gegenstand von Manipulationen durch Betrüger sein. Der Informationsmangel begünstigt Betrüger

[211] Vgl.*IT-Daily* (2022).
[212] Vgl.*Dewerne* (2023).
[213] Vgl.*Levy* (2022).
[214] Vgl.*Levy* (2022).

zusätzlich, da es potentielle Anleger nicht genügend Quellen gibt, um alle vorhandenen Informationen über das Vorhaben zu überprüfen[215].

Es funktioniert, indem eine kleine Anzahl von Insidern, den Vermögenswert bereits mit einer digitalen Währung besitzen. Sie haben zum Beispiel zukünftige Kenntnisse über Handlungen, die sich auf den zugrunde liegenden Vermögenswert auswirken können, und nutzen dieses Wissen, um sich einen Wettbewerbsvorteil zu verschaffen[216]. Diese kaum gehandelten Vermögenswerte sind über soziale Netzwerke, Mundpropaganda oder andere Werbemittel öffentlich zugänglich. Insider beginnen, die Aktien zu hohen Preisen zu verkaufen oder abzustoßen, was zu einem dramatischen Ausverkauf führt und auf Kosten der getäuschten Masse profitiert. Wenn die ungebildete Anlegeröffentlichkeit die Kryptowährung ohne behördliche Maßnahmen aufnimmt, dürfte diese Betrugsmethode erheblich zunehmen[217].

Besonders bei Anfängern im Bereich der Kryptowährungen ist die Angst vor dem Verpassen möglicher Gewinne sehr ausgeprägt. Leider führt genau diese FOMO, wie bereits in Kapitel 4.4 näher erläutert, auch dazu, dass Menschen Opfer von Pump-and-Dump-Systemen werden. Wenn man als Neueinsteiger einen Coin sieht, der in kurzer Zeit um 100% oder mehr im Wert gestiegen ist, möchte man natürlich an den Gewinnen teilhaben. Leider ist eine Investition zu diesem Moment meist die falsche Entscheidung, da auf eine lange “Pump”-Phase oft eine schnelle “Dump”-Phase folgt.. Auf Indikatoren wie Handelsvolumen etc. wird als Neuling meist nicht geachtet, weshalb es immer wieder zu Betrugsfällen kommt[218].

6.1.3 Rug Pull-Betrug

Ein Rug Pull ist eine weitere Art von bösartigem Betrug in der Kryptowährungsbranche, bei dem kriminellen Krypto-Entwickler ein Blockchain-Projekt starten, mit der Absicht die Gelder der Investoren zu stehlen[219]. Der Begriff "Rug Pull" leitet sich von dem englischen Sprichwort "to pull the rug out" ab, was so viel bedeutet wie "jemandem den

[215] Vgl.*Blocktrainer* (2023).
[216] *Levy* (2022).
[217] *Levy* (2022).
[218] *Blocktrainer* (2023).
[219] Vgl.*Zero To Hundred* (2022).

Teppich unter den Füßen wegziehen", und ist eine treffende Beschreibung der aktuellen Situation[220].

Das genannte Phänomen beruht darauf, dass Cyberkriminelle selbst einen Token erstellen und ihn auf einem Handelsplatz für Kryptowährungen (den „Decentralized Exchange" DEX), bei dem die Akteure direkt dezentralisiert miteinander handeln, listen. Die Coin-/Token-Schöpfer entfachen meist einen vorübergehenden Hype auf Social-Media-Plattformen und „pumpen“ anfangs viel Liquidität in ihren Pool, um das Vertrauen der Anleger zu gewinnen. Rug Pulls entwickeln sich daher auf DEXs, da diese Arten von Börsen es ihren Nutzern ermöglichen, Token ohne Kosten und (AML)-Prüfung zu listen, im Gegensatz zu zentralisierten Kryptowährungsbörsen. Böswillige Teilnehmer profitieren von diesen unbeaufsichtigten Plattformen, die die Preise für Token in einem Pool durch Algorithmen auf der Grundlage des verfügbaren Guthabens bestimmen.[221].

Das Ziel ist es, den eigenen Token mit einer seriösen Kryptowährung wie Bitcoin auszutauschen. Nachdem eine große Menge nichtsahnender Anleger ihre seriösen werthaltigen Kryptowährungen gegen den gelisteten Token eintauscht und das Geld bei den Betrügern in Form von „echten“ Krypto-Assets eingetroffen ist, schließen die Gründer das Projekt wieder indem sie alles aus dem Liquiditätspool abziehen und den Wert des Coins auf null treiben. Die Anleger hingegen werden aufgrund ihrer Investition mit einem wertlosen Token zurückgelassen[222].

6.1.4 Phishing-Betrug

Eine spezielle Art des Krypto-Betrugs, das sogenannte Phishing, besteht darin, die Opfer zur Preisgabe ihrer privaten Schlüssel oder persönlichen Daten zu verleiten. Um das Vertrauen des Opfers zu gewinnen, gibt sich der Angreifer manchmal als Unternehmen oder Person aus, die an einem Unternehmen beteiligt ist, um legitim zu erscheinen[223]. Dabei gehen sie ähnlich vor wie beim klassischen Phishing und

[220] Vgl.*Würfel*..
[221] Vgl.*Zero To Hundred* (2022).
[222] Vgl.*Rosen* (2022).
[223] Vgl.*Cointelegraph* (2022).

verwenden gefälschte Webseiten, auf denen alle Benutzerangaben, wie das Passwort für die Kryptowährung, die Wiederherstellungsphrase und andere Finanzdaten, protokolliert werden und so in die Finger der Betrüger geraten. Mit Hilfe einer E-Mail werden die Betrugsopfer gelockt, so dass sich die Hacker einen Zugang zu den Wallets verschaffen können. Der Angreifer nutzt so die Daten des Nutzers, um dessen Bitcoin-Gelder zu erbeuten[224].Phishing-Methoden, die auch bei alltäglichem Identitätsdiebstahl und verschiedenen Arten von Unternehmenskriminalität zum Einsatz kommen, werden häufig per E-Mail verschickt, wobei sich die Kriminellen als Autoritätspersonen ausgeben und nach Anmeldeinformationen fragen. Auch diese Art von Betrug ist aktuell in den sozialen Medien weit verbreitet[225].

Die Auswirkungen auf die Opfer der Betrugssysteme sind beträchtlich, da die geschätzten Verluste im Zusammenhang mit Krypto-Betrügereien schwindelerregend sein können[226].

6.2 Fallbeispiel: Krypto-Betrug OneCoin

Laut CoinMarketCap wurde der „OneCoin“ Ende 2014 gegründet und in seinen Werbematerial als die kommende große Kryptowährung, ein "besseres Bitcoin", angepriesen. OneCoin wuchs schnell im Wert und in der Popularität, und zum Zeitpunkt des ersten Auftritts von der Gründerin Frau Ignatova auf der Bühne war er auf dem Markt deutlich mehr wert als Bitcoin Anstatt jedoch der bessere Bitcoin zu werden, wie seine Gründer angekündigt hatten, entpuppte sich diese neue Kryptowährung als ein massives Ponzi-Schema, das sich hinter einer MLM-artigen Marketingstrategie verbarg. Multi-Level-Marketing (MLM), auch Network-Marketing genannt, ist ein System, bei dem nicht nur bestimmte Produkte eines Unternehmens verkauft werden. Vielmehr werden auch neue Vertriebspartner angeworben. Es ist auch als Schneeballsystem bekannt[227].

In Vorbereitung auf die Veröffentlichung der Kryptomünze, wurden Hunderttausende von Anlegern durch den Kauf der gefälschten Produkte betrogen. Die Käufer konnten

[224] *Cointelegraph* (2022).
[225] Vgl.*Cointelegraph* (2022).
[226] Vgl.*Cointelegraph* (2022).
[227] Vgl.*Coin Market cap* (2022).

OneCoins schürfen, indem Sie die geworbenen Produkte kauften, die schließlich auf den Markt kommen und den internationalen Zahlungsverkehr revolutionieren würden. Der OneCoin selbst hatte jedoch nie einen tatsächlichen Wert. Die angebliche Blockchain, auf der die Währung aufgebaut werden sollte, existierte nicht; alles war eine Lüge[228].

Wie in CoinMarketCap's (2022) Artikel erwähnt, wurde den Nutzern Zugang zu einer Login-Plattform gegeben, auf der die Investoren sehen konnten, wie gut die einzelnen Portfolios liefen. In Wirklichkeit änderte das Unternehmen hinter OneCoin willkürlich die Preise. Es bestand nie eine Verbindung zu einem Marktpreis. Außerdem konnten die Anleger nie mit ihren Münzen auf der Plattform handeln. Das Unternehmen, dem OneCoin gehört, erzielte Einnahmen durch den Verkauf von Büchern und die Verwendung seiner Münze für Marketingzwecke. Es wurde belegt, dass der OneCoin-Betrug bis zu 15 Milliarden Dollar von seinen Nutzern gestohlen hat. Bevor das Unternehmen zusammenbrach, wurde OneCoin offiziell als Schneeballsystem angeklagt, und gegen die Gründer des Unternehmens wurden Haftbefehle ausgestellt[229].

Allerdings hatten bereits vor dem Zusammenbruch zahlreiche Zentralbanken damit begonnen, vor Investitionen in OneCoin zu warnen, da der Betrug weit verbreitet war, darunter die Kroatische Nationalbank im Jahr 2017 und die Zentralbanken von Lettland, Schweden und Norwegen im Jahr 2016. Das Bundesaufsichtsamt für Finanzdienstleistungsaufsicht (BaFin) in Deutschland erließ 2017 eine Unterlassungsverfügung gegen OneCoin und ordnete an, dass das Unternehmen seine Geschäftstätigkeit innerhalb des Landes sofort einstellt. Ignatova, das Gesicht von OneCoin, verschwand im selben Jahr und steht seitdem auf der FBI-Liste der meistgesuchten Personen[230].

Der Erfolg dieses One-Coin-Schwindels basiert auf den Perioden zuvor in der Kyrptogeschichte. In dieser Zeit begannen nämlich Kryptowährungen gerade, weltweit Aufmerksamkeit zu gewinnen, da der Bitcoin-Kurs knapp über 500 Dollar lag[231]. Interessant ist, OneCoin war nicht der einzige Bitcoin-Konkurrent. Viele andere Kryptomünzen tauchten plötzlich auf und versuchten, einen Anteil an der neuen Kryptowährungsbegeisterung auf dem Markt zu bekommen, doch die Münzen, die ähnliche Ansprüche

[228] Vgl.*Coin Market cap* (2022).
[229] Vgl.*Coin Market cap* (2022).
[230] Vgl.*Coin Market cap* (2022).
[231] Vgl.*Coin Market cap* (2022).

(einfache Zahlungen, niedrige Kosten, „sicher“), hatten jedoch nicht den Marketing-Appeal einer Frau mit einem Doktortitel und einem Hintergrund bei renommierten Beratungsunternehmen[232]. Dies war für viele neue Investoren der angebliche Beweis für die Legitimität des Projekts.

Die Verlockung des schnellen Geldes für diejenigen, die den Bitcoin-Zug verpasst hatten, war die treibende Kraft für viele, die am Aufstieg von Bitcoins zweifelten und Angst hatten, etwas zu verpassen, das sie potenziell reich hätte machen können[233]. OneCoin verkaufte "Bildungspakete" zu Kryptowährungen, um angehenden Anlegern zu helfen, informierte Fachleute zu werden und ihnen die Fähigkeiten zu vermitteln, die neuen Münzen zu schürfen, deren Wert später in die Höhe schießen sollte[234]. Die Pakete wurden mit verschiedenen unbegrenzten Preisspannen angeboten, um den Preisvorstellungen gerecht zu werden. Die Münzen wurden jedoch nie zum Verkauf an die breite Öffentlichkeit angeboten[235]. Die Nutzer konnten ihre Münzen nicht abheben und nur in kleinen Beträgen innerhalb des geschlossenen Systems übertragen, obwohl sie auf der OneCoin-Website einen nominalen internen Wert hatten[236].

Der OneCoin-Betrug war nach verschiedenen Einschätzungen sehr erfolgreich. Laut CoinMarketCap (2022) liegen die Umsätze zwischen bei 19,4 Milliarden Dollar. Im Jahr 2021 wurden die Seychellen Strafverfolgungsbehörden mit der Untersuchung von 230.000 Bitcoin-Transaktionen beauftragt, die angeblich mit dem Hack auf der kleinen Insel in Verbindung standen, durch den das Geld geschleust worden war[237].

Alle bis jetzt bekannten Beteiligten des Ponzi-Schemas werden weltweit gesucht. Es ist sehr schwer, dass die Identitäten aller an dem Verbrechen beteiligten Nutzer jemals bekannt werden, und die Blockchain-Gelder wurden wahrscheinlich an verschiedenen Börsen auf der ganzen Welt abgehoben. Das verlorene Geld ist scheint unwiederbringlich[238].

[232] Vgl.*Coin Market cap* (2022).
[233] Vgl.*Coin Market cap* (2022).
[234] Vgl.*Coin Market cap* (2022).
[235] Vgl.*Coin Market cap* (2022).
[236] Vgl.*Coin Market cap* (2022).
[237] Vgl.*Coin Market cap* (2022).
[238] Vgl.*Coin Market cap* (2022).

7 Aufdeckung von Kryptokriminalität

7.1 Technische Aufdeckungsmöglichkeiten

Um gegen die wachsende Finanz-Cyberkriminalität anzukämpfen, wurden über die Jahre einige technische Möglichkeiten zur Aufdeckung von Kriminalität mit Kryptowährungen entwickelt.

7.1.1 Blockchain-Analyse

Alle Kryptowährungstransaktionen werden auf der Blockchain aufgezeichnet. Daher können spezielle Software-Tools eingesetzt werden, um verdächtige Transaktionsmuster zu erkennen. Solche Muster können ein Warnsignal darauf sein, dass Kryptowährungen für illegale Aktivitäten wie Geldwäsche, Betrug, Drogenhandel verwendet werden. Bei der Blockchain-Analyse handelt es sich um einen Prozess, bei dem die Transaktionsdaten einer Blockchain untersucht werden, um Informationen über die Transaktionen und die daran beteiligten Parteien zu erhalten[239]. Mithilfe von Blockchain-Analysetools wie Chainalysis und Elliptic wird die Blockchain auf bestimmte Muster in den Transaktionen durchsucht. Diese Muster können zur Aufdeckung illegaler Aktivitäten und zur Identifikation verdächtiger Transaktionen genutzt werden[240].

Die Nachverfolgung gestohlener Kryptowährungen ist ein weiteres Beispiel für die Anwendung von Blockchain-Analysewerkzeugen. Wenn eine Börse für Kryptowährungen gehackt wird und Kryptowährungen gestohlen werden, können Blockchain-Analysewerkzeuge zur Identifizierung und Verfolgung der gestohlenen Kryptowährungen in der Blockchain eingesetzt werden[241].

Lösungsansätze für effektive Regulierungen

Eine gute Blockchain-Analyseplattform sollte in der Lage sein, potenziell risikoreiche Krypto-Aktivitäten in Echtzeit zu erkennen und zu identifizieren, sowie einen

[239] Vgl.*Chainanalysis* (2023).
[240] Vgl.*Elliptic* (2019).
[241] Vgl.*Chainanalysis* (2023).

umfassenden Überblick über das Organisations- und Benutzerrisiko zu gewährleisten. Die Plattform sollte Compliance-Teams ermöglichen, Warnmeldungen an ihren risikobasierten Ansatz anzupassen und ein Fallmanagement zur einfachen Berichterstattung und Zusammenarbeit mit Kollegen sowie Aufsichtsbehörden bieten[242].

Blockchain-Analysetools können Kryptounternehmen bei der Überwachung von Transaktionen unterstützen und manuelle Arbeitsabläufe reduzieren, indem sie potenziell verdächtige Aktivitäten identifizieren und Echtzeitwarnungen basierend auf den Anti-Geldwäsche-Richtlinien des Unternehmens konfigurieren. Eine effektive kontinuierliche Überwachung in einem Blockchain-Analysetool sollte automatische Warnungen und benutzerdefinierte Warnungsschwellenwerte umfassen, um Teams sowohl bei der Überwachung von eingehenden verdächtigen Aktivitäten als auch bei der Untersuchung historischer Transaktionen zu unterstützen, wenn neue Informationen als potenziell problematisch identifiziert werden[243].

Chainalysis Reactor

Es gibt mehrere Möglichkeiten, wie Kriminelle ihre Identitäten verschleiern und versuchen, ihre Transaktionen auf der Blockchain zu verbergen. Die Konnektivität und Offenheit der Kette ermöglichen es dennoch Forschungsunternehmen wie Chainalysis, Werkzeuge wie den Chainalysis Reactor zu entwickeln, um solche Geldwäsche Transaktionen zu verfolgen. Regierungen und Unternehmen nutzen das Reaktor-Tool weltweit, um den Kampf gegen Geldwäsche/Terrorismusfinanzierung zu erleichtern. Der Chainalysis Reactor ist eine Plattform, die Bitcoin-Transaktionen mit Aktivitäten in der realen Welt verknüpft. Sie untersuchen dabei die wichtigsten Gegenparteien und das Risiko für unrechtmäßige Tatbestände. Dabei wird eine "Überwachung" eingeführt, um zukünftige Transaktionen zu verfolgen oder es wird auf eine Anfrage mit automatischer Pfadfindung vorgegangen. Darüber hinaus ermöglicht die kanalübergreifende Untersuchungsfunktion des Reaktors den Nutzern, Geld über zahlreiche Vermögenswerte in einem einzigen Diagramm zu verfolgen, was die Analyse beschleunigt[244].

[242] Vgl.*Chainanalysis* (2023).
[243] Vgl.*Chainanalysis* (2023).
[244] Vgl.*Chainanalysis* (2023).

Kontrollbörse Luno

Luno ist eine Kryptowährungsbörse, die in verschiedenen Ländern auf der ganzen Welt vertreten ist. Sie hat eine Partnerschaft mit Chainalysis, einem führenden Unternehmen im Bereich Blockchain-Analyse, zur Erkennung und Verhinderung verdächtiger Aktivitäten[245]. Das von Luno eingesetzte Tool dient zur Identifizierung verdächtiger Transaktionen, einschließlich jenen, die mit illegalen Aktivitäten wie Geldwäsche und Betrug in Verbindung stehen könnten. Hierzu verwendet das Tool eine Kombination aus Algorithmen und manuellen Überprüfungen. Werden verdächtige Transaktionen festgestellt, wird das Luno-Team benachrichtigt und weitere Untersuchungen können durchgeführt werden, um den Hintergrund der Aktivitäten aufzuklären. Stellt sich heraus, dass es sich tatsächlich um eine illegale Transaktion handelt, müssen geeignete Maßnahmen getroffen werden, um den Benutzer von der Plattform zu sperren oder ihn bei den Strafbehörden anzuzeigen[246].

Cluster-Analysen

Eine Cluster-Analyse gruppiert ähnliche Transaktionen auf der Blockchain, um versteckte Beziehungen zwischen Adressen und Transaktionen zu identifizieren, was bei der Aufdeckung krimineller Aktivitäten helfen kann. Eine Clusteranalyse von Kryptowährungen identifiziert Ähnlichkeiten und Unterschiede zwischen verschiedenen Kryptowährungen und unterteilt sie in Gruppen oder Cluster mithilfe statistischer Algorithmen und maschinellem Lernen. Investoren und Händler können durch die Gruppierung von Kryptowährungen mit ähnlichen Eigenschaften Risiken minimieren und ihr Portfolio diversifizieren. Faktoren wie Marktkapitalisierung, Handelsvolumen, Volatilität, Beliebtheit, Technologie und Anwendungsfall können bei der Clusteranalyse berücksichtigt werden. Es ist jedoch wichtig zu beachten, dass die Ergebnisse nicht unbedingt objektiv oder endgültig sind und weitere Forschung notwendig ist, bevor Entscheidungen auf Basis dieser Analyse getroffen werden[247].

[245] Vgl.*Chainanalysis* (2023)..
[246] Vgl.*Chainanalysis* (2023).
[247] Vgl.*ComplyAdvantage* (2022).

7.2 Verstärkung der Börsenvorschriften

Die Unternehmen müssen das potenzielle Risiko verstehen, das mit ihrem Produktangebot verbunden ist, ebenso wie beim Handel mit Fiat-Währungen. Kryptowährungsunternehmen müssen sich an die Vorschriften der Rechtsprechung halten, in der sie operieren. Andernfalls drohen hohe Geldstrafen und andere negative Konsequenzen, einschließlich des Verlusts der Lizenz[248].

Um sicherzustellen, dass Kryptowährungsbörsen nicht für illegale Aktivitäten genutzt werden, müssen sie bestimmte KYC- (Know Your Customer) und AML- (Anti-Money-Laundering) Richtlinien einhalten. Die Überwachung von Kryptowährungsbörsen kann helfen, verdächtige Transaktionen zu erkennen und anzuzeigen. Während Coins nur zwischen Adressen übertragen werden, ohne dass ein Name in den Protokollen auftaucht, ist eine eindeutige Zuordnung zu einem Adressinhaber nicht möglich. Wenn jedoch an einer Stelle eine Verbindung zu der realen Identität hergestellt werden kann, ist die Anonymität verloren. Tauschbörsen sind daher strikt verpflichtet das **„Know-your-Costumer-Prinzip“** zu befolgen. Es ist nicht mehr möglich, dass ohne einen Identitätsnachweis durch ein Ausweisdokument, ein Account bei den bekanntesten Börsen wie „Bitpanda“ oder „Coinbase“ erstellt werden kann. Die Möglichkeit, anonym an Coins zu gelangen, ist damit weitaus eingeschränkt. Andere Online-Dienstleister und Handelsplätze, die Kryptowährungen als Zahlungsmöglichkeit akzeptieren, erfordern auch in der Regel aus Eigeninteresse einen Identitätsnachweis. Zusammenfassend ausgedrückt stellt die Anonymität der Kryptowährungen nur eine Verschleierung der Nutzeidentität dar, solange eine Schnittstelle zur realen Welt gefunden werden kann. Dabei kann es sich um einen digitalen Fingerabdruck, ein ausgelesenes Protokoll, eine IP-Adresse oder auch nur um eine Lieferadresse handeln[249].

Risikomanagement ist der Schlüssel zum Aufbau von Vertrauen bei neuen und bestehenden Nutzern angesichts der zunehmenden Medienberichterstattung über Krypto-Skandale. Voraussetzung für den Aufbau dieses Vertrauens ist die Einhaltung der internationalen Vorschriften zur Bekämpfung der Geldwäsche. Dazu zählen KYC-Anforderungen, Transaktionsüberwachung, Vorlage von Verdachtsberichten und Protokolle. Blockchain-Analyse-Tools können den Unternehmen einige der wichtigsten

[248] Vgl.*Chainanalysis* (2023).
[249] Vgl.*Sixt* (2017).

Informationen zur Verfügung stellen, die sie benötigen, um dies auf effiziente Weise zu tun[250].

7.3 Strafrechtliche Regulierung

Einige Unternehmen, die Analysewerkzeuge für Blockchains entwickeln, arbeiten eng mit Strafverfolgungsbehörden zusammen, um die Aufklärung von Straftaten zu unterstützen. Bei Bedarf sind sie auch in der Lage, rechtliche Schritte zur Unterbindung krimineller Aktivitäten einzuleiten[251]. Die fortschreitende Kompetenz der Strafverfolgungsbehörden, illegal beschaffte Kryptowährungen zu konfiszieren, ist eine vielversprechende Entwicklung bei der Bekämpfung der Kriminalität im Zusammenhang mit Kryptowährungen[252].

Im November 2021 gab die IRS (Criminal Investigations) bekannt, dass sie im Jahr 2021 Kryptowährungen im Wert von mehr als 3,5 Milliarden US-Dollar beschlagnahmt hatten , die alle im Rahmen nicht steuerlicher Ermittlungen gefunden wurden. Dies entspricht 93 Prozent aller von der Abteilung in diesem Zeitraum beschlagnahmten Gelder. Auch gab es mehrere andere Beispiele für erfolgreiche Beschlagnahmungen durch Behörden, darunter 56 Millionen US-Dollar, die vom Justizministerium im Rahmen einer Untersuchung zu Kryptowährungsbetrug beschlagnahmt wurden, 2,3 Millionen US-Dollar von Ransomware-Angriffen sowie ein nicht genannter Betrag, der vom israelischen National Bureau for Counter Terror Financing in einem Fall von Terrorismusfinanzierung konfisziert wurde[253].

Anfang 2022 bewahrten illegale Adressen in Kryptowährungen im Wert von mindestens 10 Milliarden US-Dollar auf, der Großteil davon in Wallets, die mit dem Diebstahl von Kryptowährungen in Verbindung stehen. Adressen, die mit Darknet-Märkten und Betrug in Verbindung gebracht werden, tragen ebenfalls erheblich zu dieser Zahl bei[254].

---

[250] *Chainanalysis* (2023)..
[251] Vgl.*ComplyAdvantage* (2022)..
[252] Vgl.*ComplyAdvantage* (2022).
[253] Vgl.*Chainanalysis* (2023).
[254] Vgl.*Chainanalysis* (2023).

7.4 Wichtige Strafbestimmungen im Zusammenhang mit Kryptowährungen

7.4.1 Geldwäschevorschriften

Um zu verhindern, dass das Finanzsystem zum Zwecke der Geldwäsche und der Terrorismusfinanzierung missbraucht wird, entstand im Zuge der Umsetzung der EU-Geldwäscherichtlinie das Geldwäschegesetz (GWG). Dieses Gesetz und weitere eingefügte Bestimmungen haben einerseits die Finanzmarktaufsicht mit der Wahrnehmung der Aufsichtstätigkeit betraut und andererseits durch das KYC-Prinzip versucht, die Anonymität der Geldwäscher so weit als möglich einzuschränken. Mit diesem Grundsatz soll ein Mindeststandard geschaffen werden, der Kreditinstitute und Versicherungsunternehmen verpflichtet, Neukunden zu identifizieren. Dazu gehört die Offenlegung, wer der Kunde ist, welches Geschäftsmodell er verfolgt und woher die Geldflüsse stammen[255]. In Deutschland besteht darüber hinaus eine Meldepflicht, um die Richtlinie umzusetzen. So muss das Finanzinstitut, wenn sich aufgrund verdächtiger Transaktionen ein Verdacht auf Geldwäsche ergibt, dies dem Finanzamt melden[256].

Diese Geldwäsche-Richtlinie enthält zahlreiche Vorgaben für die Mitgliedstaaten, die bei Umsetzung zum einen die Verfolgung dieser Delikte in den Vordergrund rücken und zum anderen die Begehung des Tatbestands der Terrorismusfinanzierung erheblich erschweren sollen. Durch behördliche Zusammenarbeit soll zudem eine grenzüberschreitende Verfolgung erreicht werden. Wie beim Geldwäschetatbestand verfolgt die Richtlinie auch hier das KYC-Prinzip und erhöht damit die Kontrolle des Delikts deutlich. So werden auch die Finanzinstitute verpflichtet, ihre Kunden zu überwachen und zu identifizieren[257].

7.5 Einbeziehung in die fünfte und sechste Geldwäscherichtlinie

Die 5. Geldwäscherichtlinie (5.GW-RL) hat mit ihrer Umsetzung im Jahr 2020 Kryptobörsen und Wallet-Anbieter in den Anwendungsbereich der EU-Geldwäscherichtlinien gebracht. Dies ist ein essenzieller Schritt zur Regulierung von

[255] Vgl.*Bundesministerium für Finanzen*.
[256] Vgl.*Bundesministerium für Justiz* (2022).
[257] Vgl.*Bundesministerium für Finanzen*.

Kryptowährungsvermögen. Kryptobörsen und Wallet-Anbieter werden damit zu den Unternehmen gezählt, die der 5.AMLD unterliegen. Damit sind sie auch verpflichtet, Sorgfaltspflichten gegenüber ihren Kunden und möglichen Neukunden zu erfüllen, diese laufend zu überwachen und bei Verdachtsmomenten schnell Meldung zu erstatten. Zudem müssen sich Unternehmen, die Börsen und Wallets anbieten, bei den entsprechenden Regierungsstellen eintragen lassen[258].

Anbieter von Kryptowährungs-Wallets und -Börsen standen mit der Implementierung dieser Anforderungen nach dem 5.Geldwäschegesetz vor einigen Herausforderungen. Schließlich erfordert das Paket aus effektiven Sorgfaltspflichten und laufender Überwachung Ressourcen unterschiedlicher Art. Die 6.GWG hat in Form der folgenden Änderungen die Anforderungen an die verpflichteten Unternehmen, wie z.B. Kryptobörsen und Wallets, weiter verschärft[259]. Ziel ist es insbesondere, das Recht der Mitgliedsländer in bestimmten Aspekten zu vereinheitlichen. Dazu gehört die Einführung von 22 Vortaten zur Geldwäsche und damit auch die neuen Straftatbestände Cyberkriminalität und Umweltkriminalität. Um ihrer Verdachtsmeldepflicht nachzukommen, müssen Krypto-Dienstleister sicherstellen, dass ihre Mitarbeiter im Erkennen von Risiken potenziell kriminellen Verhaltens geschult sind[260].

In der Praxis werden die betroffenen Unternehmen über wirksame Kontrollmechanismen verfügen müssen, um eine konsequente Einhaltung ihrer AML-Pflichten sicherzustellen. Durch die Ausweitung der Haftung wird sich auch der Druck auf das Management der Anbieter von Krypto-Wallets und Krypto-Börsen erhöhen, die AML-Richtlinien ausreichend zu kontrollieren und das Risikobewusstsein auf der Ebene des Vorstands und der Geschäftsführung zu schärfen[261].

7.5.1 Verschärfte Sanktionen

Auch für Personen, die sich der Geldwäsche schuldig machen, sieht das 6.GWG härtere Strafen vor. Beispielsweise wurde das Mindeststrafmaß von einem Jahr auf vier Jahre erweitert. Zudem können die Strafen für solche Delikte hohe Geldbußen oder sogar die dauerhafte Schließung eines Unternehmens vorsehen. Eine konsequente

[258] Vgl.*ComplyAdvantage* (2022).
[259] Vgl.*ComplyAdvantage* (2022).
[260] Vgl.*Bundesministerium für Justiz* (2022).
[261] Vgl.*ComplyAdvantage* (2022).

Umsetzung des 6.GWG ist für Kryptobörsen und Wallet-Anbieter als Verpflichtete unerlässlich[262]. Seitens der EU wurden beispielsweise Pläne zur weiteren Regulierung von Kryptowährungen angekündigt. Das Ziel, bis 2024 umfassende und „sehr klare" Regeln für Kryptowährungen zu schaffen, wurde in einem kürzlich veröffentlichten Dokument zur Priorität erklärt. Dazu gehört auch ein Rahmen für die Zulassung und gesetzliche Regulierung von Kryptoassets. Die Regulierungsbehörden weltweit werden weiterhin vor der Herausforderung stehen, Kryptowährungen in ihre regulatorische Landschaft zu integrieren, da sie ein breites Anwendungsgebiet haben und die Entwicklung der Technologie weiter voranschreitet[263].

7.5.2 Steuerhinterziehung

Sobald ein Geldwäschevorgang durch die Behörden aufgedeckt wird, stellt das einen strafrechtlichen Sachverhalt im Zusammenhang mit der Steuerhinterziehung dar. Zum einen der Tatbestand der verschleierten Einkünfte aus illegalen Aktivitäten, zum anderen werden die Verheimlichung der Einkünfte der Besteuerung. Diese strafrechtlichen Tatbestände werden je nach Land unterschiedlich geregelt[264].

Vor allem bei der Nutzung von Kryptowährungen und der damit zusammenhängenden Pseudoanonymität ist die Versuchung zur Verwirklichung des Tatbestandes der Steuerhinterziehung groß. Dies ist allerdings grob fahrlässig, da viele Steuerbürger den Begriff der Kryptowährung steuerrechtlich nicht einordnen und somit Gewinne, die sie aus „hobbymäßigen" Investments erzielen, nicht versteuern. Zumal die meisten Betreiber von Kryptobörsen bereits auf die Besteuerung von Gewinnen verweisen[265].

[262] Vgl.*ComplyAdvantage* (2022).
[263] Vgl.*ComplyAdvantage* (2022).
[264] Vgl.*Chainanalysis* (2023)..
[265] Vgl.*ComplyAdvantage* (2022).

8 Fazit

Die vorliegende Arbeit hat sich umfassend mit dem Thema Kryptowährung sowie dessen Bezug zur Wirtschaftskriminalität befasst. Das Forschungsinteresse basierte auf einer grundlegenden Forschungsfrage, dessen Beantwortung als Ziel der Arbeit definiert wurde. Die Intention hierbei lag zum einen darin, den Einfluss der Kryptowährung auf die vorab formulierte Forschungsfrage sowie Leitfragen darzustellen und zum anderen grundsätzliche Aspekte in diesem Kontext zu erarbeiten, die im Hinblick auf die Ausarbeitung des Themas als relevant gesehen wurden.

Der Fokus lag hierbei einerseits auf grundlegenden Begriffserläuterungen, Kernpunkten der zeitgemäßen Kryptowährung sowie dessen aktuelle Bedeutung im Kontext der Wirtschaftskriminalität. Die Ergebnisse zeigen im Allgemeinen, dass durch die Annonymität, Dezentralität und Effizienz Kryptowährungen den Raum für die verschiedensten Cyberkriminalitäten schaffen, wie etwa der Verkauf von wertlosen Coins und unzählige Hackerangriffe, welche die Absicht verfolgen die Nutzer zu bestehlen. Die Zunahme der kriminellen Aktivitäten auf dem Krypto-Gebiet sind insbesondere auf das plötzliche Wachstum der Branche zurückzuführen, welches eine Plattform für potenzielle Betrüger schuf.

Anhand des Fallbeispiels des FTX-Börsenskandals wird sichtbar, dass sogar weltweit bekannten Großkonzernen das Potenzial innewohnt, ihre Kunden zu bestehlen. Das Fallbeispiel des One-Coin-Betrugs veranschaulicht zudem, dass fast täglich neue Kryptocoins mit betrügerischen Absichten verbreitet werden. So entpuppt sich der seriöse Anschein vieler Unternehmen als bösartige Manipulation, um einen Profit aus der Naivität unerfahrener Anleger zu erwirtschaften. Da die Verbrechen immer größer und globaler werden und Millionen von Menschen betreffen, ziehen sie die Aufmerksamkeit der Aufsichtsbehörden weltweit auf sich. Im Blick auf die EU wurde mit der Einführung und Zusammenfassung der 5.GWG und 6.GWG ein Standpunkt eingeführt, auf dem die Grundlagen der Krypto-Verordnungen basieren.

Aus den Rechercheergebnissen geht zudem hervor, dass virtuelle Währungen besonders durch Hackerangriffe gefährdet sind. Hier ist festzuhalten, dass durch das Fehlen eines Intermediären durchgeführte Transaktionen endgültig sind und es bei einem Betrug unmöglich ist, das eingezahlte Geld zurückzuholen.

Ebenso die hohe Volatilität stellt einen wesentlichen Risikofaktor dar, dem insbesondere Investoren ausgesetzt sind. Bei neuen Kryptowährungen kann ein Schneebalsystem hervorgerufen werden, wodurch der Kurs einbricht und die Währung wertlos wird. Dabei hängen die größten Risiken, wie die Geldwäsche, Terrorismusfinanzierung und Kriminalität, mit der Anonymität bzw. Pseudoanonymität von virtuellen Währungen zusammen. Unter Berücksichtigung dieser Geldwäschetechniken kann die Eignung von Kryptowährungen zur Geldwäsche durchaus zugesprochen werden.

Einhergehend mit der zunehmenden Anzahl der Krypto-Verbrechen, die höhere Ansprüche an Sicherheitsmaßnahmen stellen sowie der steigenden Tendenz in virtuelle Währungen zu investieren, wird den Strafverfolgungsbehörden zur Bekämpfung von kryptobasierter Kriminalität eine zunehmende Bedeutung zugesprochen. So ist es bspw. durch den Einsatz von verschiedenen Blockchain-Analysetools möglich, die Herkunft illegaler Transaktionen zu verfolgen und bestenfalls Kriminelle zu identifizieren. Der Vorteil bei der Verfolgung von Kryptowährungen ist, dass der gesamte Transaktionsfluss bei Kryptowährungen im Gegensatz zu Bargeld viel leichter nachvollzogen werden kann und die öffentlichen Adressen durch die Überwachung der Blockchain aufgerufen werden können. Die Rückverfolgbarkeit der inkriminierten Gelder wird durch die Einschaltung professioneller Finanzagenten erschwert, was für den Geldwäscher wiederum das Gefahr mit sich bringt, für eine gewisse Zeit nicht über die inkriminierten Vermögenswerte verfügen zu können.

Eine große Herausforderung stellt die Geldwäsche mit Kryptowährungen dar, da diese oft anonym und dezentral sind und es für Kriminelle einfach ist, Geld durch verschiedene Adressen und Börsen zu waschen, so dass es nur schwer nachvollzogen werden kann. Um diesem Problem entgegenzuwirken, werden in einigen Ländern Regulierungen eingeführt, die Kryptobörsen verpflichten, die Identität ihrer Kunden zu überprüfen und Transaktionen zu überwachen, die als verdächtig gelten. Darüber hinaus gibt es private Unternehmen, die Kryptoanalyse-Tools anbieten, die Regulierungsbehörden und Finanzinstitute bei der Überwachung von Kryptowährungstransaktionen unterstützen können. Demzufolge werden Kryptowährungen oft in Verbindung mit illegalen Aktivitäten wie zum Beispiel Geldwäsche sowie Drogen- und Waffenhandel gebracht. Die Pseudoanonymität und Verwendung von TOR-Browsern und Bitcoin-Mixern machen es für die Behörden schwierig, diese Aktivitäten zu entdecken. Die Blockchain-Analyse

kann helfen, aber oft fällt die Geldwäsche erst bei der Umwandlung des virtuellen Geldes in eine klassische Währung auf. Es gibt einen Handlungsbedarf im Hinblick auf das virtuelle Währungssystem, da es eine wachsende Rolle im Wirtschaftsleben einnimmt.

Zusammenfassend ist es anzumerken, dass die Verwendung von Kryptowährungen für legitime Zwecke weiterhin unterstützt werden sollte, jedoch ist es notwendig, angemessene Maßnahmen zu ergreifen, um ihre Verwendung für illegale Aktivitäten zu verhindern. So ist beispielsweise Geldwäsche ein weit verbreitetes Problem, das nicht nur kriminelle Aktivitäten finanziert, sondern auch das Finanzsystem gefährdet. Aus diesem Grund werden Regulierungsbehörden und Finanzinstitute dazu aufgefordert, Maßnahmen zu ergreifen, um wirtschaftskriminelle Aktivitäten zu verhindern und zu bekämpfen, indem sie die Überwachung von Transaktionen verbessern und die Kundenidentifikation überprüfen.

Zurückblickend handelt es sich bei dem Thema Krypto-Kriminalität um ein aktuelles und kontroverses Thema, welches zukünftig noch weiterer Forschung bedarf. Ziel dieser Studienarbeit war es, mittels einer theoretischen Darlegung, Einblicke in die Hintergründe von Kryptowährungen basierend auf wirtschaftskriminellen Vorhaben zu gewinnen und auf deren Grundlage entsprechende Ansätze zur Verbesserung der Prävention und Bekämpfung von wirtschaftskriminellen Aktivitäten herauszuarbeiten. Zukunftsorientiert können die Ergebnisse dieser Dokumentation um bisher noch offene Themen erweitert werden.

Literaturverzeichnis

Anonym im Netz (2018), Bitcoin Wallet anonym benutzen, in: http://www.anonym-im-netz.com/bitcoin-wallet-anonym-benutzen/.

Ayed, B. (2017), The Blockchain Technology: Applications and Threats, in: https://www.academia.edu/42250813/The_Blockchain_Technology_Applications_and_Threats, abgerufen am 5. 12. 2022.

BaFin (2020), Merkblatt: Hinweise zum Tatbestand des Kryptoverwahrgeschäfts, in: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_200302_kryptoverwahrgeschaeft.html.

BaFin (2021), Auslegungs- undAnwendungshinweise, in: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2021/meldung_2021_06_08_AuA_Kreditinstitute.html.

Bailey, D. (2022), What is “pig butchering?”, in: https://www.businessofbusiness.com/articles/pig-butchering-crypto-romance-scam/.

Bendel, O. (2018), Kryptowährung. Definition: Was ist "Kryptowährung"?, in: https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160.

Blocktrainer (2023), Wie funktioniert ein Pump-and-Dump?, in: https://www.blocktrainer.de/blocktrainer-1x1/pump-and-dump/.

Bluemel, J. (2023), NFTs – the new art of money laundering?, in: https://www.idnow.io/blog/nft-non-fungible-tokens-new-art-money-laundering/.

Breitsprecher, M. (2018), Zentrale und dezentrale Systeme, in: https://blockruption.com/2018/06/welches-problem-lost-die-blockchain/.

Brünnler, K. (2018), Blockchain. Kurz & gut, Heidelberg.

BTC-ECHO (2022), Decentralized Finance, in: https://www.btc-echo.de/academy/bibliothek/defi/.

Buchter, H./Tönnesmann, J., Absturz der Zocker. Die Pleite der Kryptobörse FTX legt offen, was in der Branche schiefläuft. Wie gefährlich wird die Krise noch?, Die Zeit, Nr. 17.11.2022, S. 23.

Bundesamt für Sicherheit in der Informationstechnik (2022), Blockchain macht Daten praktisch unveränderbar, in: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung.html.

Bundesministerium für Finanzen, Geldwäscherei und Terrorismusfinanzierung. Rechtsgrundlagen in der EU, in: https://www.bmf.gv.at/themen/finanzmarkt/geldwaescherei-terrorismusfinanzierung.html, abgerufen am 2. 2. 2023.

Bundesministerium für Innern und für Heimat, Geldwäsche. Was ist Geldwäsche?, in: https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/geldwaesche/geldwaesche-node.html.

Bundesministerium für Justiz (2022), Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten.

Bundesnetzagentur (2019), Die Blockchain-Technologie. Potenziale und Herausforderungen in den Netzsektoren Energie und Telekommunikation, in: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/Links_Dokumente/einfuehrung_bc.pdf?__blob=publicationFile&v=12.

Bussac, E. (2019), Bitcoin, Ethereum & Co. Praxiswissen Kryptowährungen und Blockchain, Berlin.

Central Charts, Was ist eine Blockchain?, in: https://www.centralcharts.com/de/gm/1-lernen/1-kryptowahrung/42-trading/699-blockchain-funktionsweise-und-nutzung, abgerufen am 9. 12. 2022.

Chainanalysis (2023), How to Evaluate Blockchain Analysis Tools, in: https://blog.chainalysis.com/reports/how-to-evaluate-blockchain-analysis-tools/.

Chimienti, M. T./Kochanska, U./Pinna, A. (2019), Understanding the crypto-asset phenomenon, its risks and measurement issues, in: https://www.ecb.europa.eu//pub/economic-bulletin/articles/2019/html/ecb.ebart201905_03~c83aeaa44c.en.html.

Coin Market cap (2022), Kryptowährungspreise, Diagramme und Marktkapitalisierung, in: https://coinmarketcap.com/de/.

Cointelegraph (2022), What is a phishing attack in crypto, and how to prevent it?, in: https://cointelegraph.com/blockchain-for-beginners/what-is-a-phishing-attack-in-crypto-and-how-to-prevent-it.

Compliance Blog, Was sind Kryptowährungs-Mixer?, in: https://www.eurospider.com/de/know-how/compliance/210-was-sind-kryptow%C3%A4hrungs-mixer, abgerufen am 16. 1. 2023.

ComplyAdvantage (2022), Crypto Laundering - Money Laundering Through Cryptocurrency Exchanges, in: https://complyadvantage.com/insights/money-laundering-crypto-exchanges/.

Dahmen, K. (2022), Die 3 Phasen der Geldwäsche, in: https://exkulpa.de/geldwaeschepraevention/phasen-der-geldwaesche/, abgerufen am 17. 1. 2023.

datensicherheit.de (2022), Pig Butchering. Proofpoint-Warnung vor Ausbreitung einer Betrugsmasche aus Asien, in: https://www.datensicherheit.de/pig-butchering-proofpoint-warnung-ausbreitung-betrugsmasche-herkunft-asien.

Dewerne, Y. (2023), Nach Catfishing kommt Pig Butchering - bei dem Betrug haben es Kriminelle besonders auf Kryptowährungen abgesehen, in: https://www.esquire.de/news/gesellschaft/kryptowaehrung-pig-butchering-krypto-betrug-investitionen.

Dr.Burgwinkel, D. (2016), Blockchains und Smart Contracts, in: https://www.swissmadesoftware.org/blog/the-book-vol-5/fachartikel/blockchains-smart-contracts.html.

Duthel, H. (2017), "Be your own bank". "Bankgeschäfte sind notwendig, Banken sind es nicht" : Blockchain - Bitcoin : warum interessieren sich so viele dafür?, Norderstedt.

Eckermann, I. M. (2017), Was ist eigentlich das Darknet?, in: https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet, abgerufen am 29. 12. 2022.

Elliptic (2019), Bitcoin Money Laundering: How Criminals Use Crypto, in: https://www.elliptic.co/blog/bitcoin-money-laundering, abgerufen am 10. 2. 2023.

Entwicklung der Kryptowährungen (2023).

ethereum.org (2022), WAS IST EIN SMART CONTRACT?, in: https://ethereum.org/de/developers/docs/smart-contracts/.

Fiedler, I./Krumma, I./Zanconato, U. A./McCarthy, K. J./Reh, E. (2017), Das Geldwäscherisiko verschiedener Glücksspielarten, [Place of publication not identified].

Financial and consumer services comission (2022), Crypto assets and cryptocurrency, in: https://www.fcnb.ca/en/investing/high-risk-investments/crypto-assets-and-cryptocurrency, abgerufen am 25. 12. 2022.

F-Secure (2023), Was ist ein Ransomware-Angriff?, in: https://www.f-secure.com/de/articles/what-is-a-ransomware-attack.

Graf, H. (2017), Zentrale, dezentrale und verteilte Systeme, in: https://blog.novatrend.ch/2017/12/25/zentrale-dezentrale-und-verteilte-systeme/.

Grauer, K./Kueshner, W./Updegrave, H. (2022), The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime, in: https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

Grzywotz, J. (2019), Virtuelle Kryptowährungen und Geldwäsche, Berlin.

Handelsblatt GmbH (2023), Welche Kryptobörsen sind für den Kauf von Bitcoin und Co. geeignet?, in: https://www.handelsblatt.com/vergleich/krypto-boersen-vergleich/, abgerufen am 20. 2. 2023.

Hayes, A./Rasure, E./Logan, M. (2021), CoinJoin, in: https://www.investopedia.com/terms/c/coinjoin.asp.

Heinze, Y./Protschka, F. (2018), Blockchain ABC. Von A wie Altcoin bis Z wie ZCash, Berlin.

Hofbauer, W. (2022), Ein Tag schreibt Geschichte: Das WWW kommt auf die Welt, in: https://www.terramatermagazin.com/a/te/das-world-wide-web-kommt-auf-die-welt-ein-datum-schreibt-geschichte.

Howard (2022), Client-Server vs. Peer-to-Peer-Netzwerke (P2P), in: https://community.fs.com/de/blog/client-server-vs-peer-to-peer-networks.html.

Hudson Intelligence (2022a), P2P- Peer to Peer, in: https://www.google.com/search?q=unterschied+client-server+und+peer-to-peer&source=lnms&tbm=isch&sa=X&ved=2ahUKEwi1g7ulgvf7AhVe_7sIHTKnDaUQ_AUoAXoECAIQAw&biw=1490&bih=746&dpr=1.25.

Hudson Intelligence (2022b), Peel Chains, in: https://www.fraudinvestigation.net/cryptocurrency/tracing/peel-chain.

IT-Daily (2022), Crypto-Betrug: „Pig Butchering" ist die neue Modeerscheinung, in: https://www.it-daily.net/shortnews/crypto-betrug-pig-butchering-ist-die-neue-modeerscheinung.

Izzo-Wagner, A. L./Siering, L. M. (2020), Kryptowährungen und geldwäscherechtliche Regulierung, Wiesbaden.

Jaganathan, S./Veeramani, K., Client-server and P2P network models, in: https://www.researchgate.net/figure/Client-server-and-P2P-network-models_fig2_333160118, abgerufen am 15. 12. 2022.

King University Online (2019), What's FOMO?, in: https://online.king.edu/news/psychology-of-fomo/.

Kirchner, T. (2022a), Riskantes Paralleluniversum, Die Zeit, S. 10.

Kirchner, T. (2022b), Lexikon der Inkompetenz. Kryptobörsen: Die FTX-Insolvenz reißt andere Handelsplattformen, mit in den Abwärtsstrudel/ Milliarden-Gelder sind ähnlich wie im Fall Wirecard „verschwunden", Die Zeit.

Koenig, A. (2018a), BITCOIN - Geld ohne Staat. Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, München.

Koenig, A. (2018b), BITCOIN - Geld ohne Staat. Die digitale Währung aus Sicht der Wiener Schule der Volkswirtschaft, 3. Aufl., München.

Küster, F. (2022), Was ist Wash Trading an Krypto-Börsen?, in: https://kryptozeitung.com/was-ist-wash-trading/.

Ledger Academy, What is NFT wash-trading, in: https://www.ledger.com/academy/what-is-nft-wash-trading, abgerufen am 19. 1. 2023.

Levy, A. (2022), How to Spot a Pump-and-Dump Cryptocurrency Scam, in: https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/how-to-spot-crypto-scam/.

LHP (2018), Kryptowährungen: Bitcoin und Geldwäsche, in: https://www.lhp-rechtsanwaelte.de/themen/kryptowaehrungen-bitcoin-und-geldwaesche/.

Littmann, S. (2021), Geldwäsche mit Kryptowährungen. Bitcoin bleibt schmutzig, in: https://www.wiwo.de/finanzen/boerse/geldwaesche-mit-kryptowaehrungen-der-bitcoin-bleibt-schmutzig/27147874.html, abgerufen am 13. 1. 2023.

Maihofer, G. (2022), Das Verbotsdrama um Tornado Cash. Schlag gegen Cyberkriminelle – oder Kriegserklärung gegen Privatsphäre?, in: https://www.btc-echo.de/news/tornado-cash-verbot-kriegserklaerung-privatsphaere-148351/.

Maltego Team, Top Data Integrations & OSINT Tools for Cryptocurrency Investigations, in: https://www.maltego.com/blog/top-data-integrations-osint-tools-for-cryptocurrency-investigations/, abgerufen am 21. 1. 2023.

Martucci, B. (2022), Was ist Geldwäsche. Beispiele, Systeme und Vorschriften, in: https://www-moneycrashers-com.translate.goog/money-laundering-examples-schemes-regulations/.

Metzger, J. (2022), Konsensmechanismus, in: https://wirtschaftslexikon.gabler.de/definition/konsensmechanismus-54411.

Retzer, M. (2022), Kryptowährungen: Wo Deutschland im internationalen Vergleich steht, in: https://www.cash-online.de/a/kryptowaehrungen-wo-deutschland-im-internationalen-vergleich-steht-625343/.

Rosen, A. (2022), How to avoid 'rug pulls,' the latest cryptocurrency scam, in: https://economictimes.indiatimes.com/news/how-to/how-to-avoid-rug-pulls-the-latest-cryptocurrency-scam/articleshow/91499147.cms?from=mdr, abgerufen am 20. 1. 2023.

Sackmann, C. (2022), Bitcoin auf Zwei-Jahres-Tief: Was hinter dem Krypto-Crash steckt, in: https://www.focus.de/finanzen/boerse/kryptowaehrungen/handelsboerse-ftx-vor-der-pleite-bitcoin-auf-zwei-jahres-tief-das-steckt-hinter-dem-krypto-crash_id_179356439.html, abgerufen am 24. 2. 2023.

SCHMIDT, N. (2019), Kryptowährungen und Blockchains. Technologie, praxis, recht, steuern, [Place of publication not identified].

Schmlechen, F. (2019), Das Internet hebt die Finanzwelt aus den Angeln, in: https://www.welt.de/sonderthemen/noahberlin/article165739975/Das-Internet-hebt-die-Finanzwelt-aus-den-Angeln.html.

Shivam Chavla (2017), What is a Chain Hopping Attack?, in: https://blockchaind.net/chain-hopping-attack-bitcoin-cash-network/.

Sixt, E. (2017), Bitcoins und andere dezentrale Transaktionssysteme. Blockchains als Basis einer Kryptoökonomie, Wiesbaden.

Soeteman, K. (2019), Kryptowährungen für Dummies, Weinheim.

Stevens, R. (2022), Bitcoin Mixers: How Do They Work and Why Are They Used?, in: https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/.

Tapscott, D. (2022), The digital age, in: https://dontapscott.com/speaking/digital-age/.

Teichmann International (2021), Geldwäsche durch Kryptowährungen, in: https://www.teichmann-law.ch/publikationen/Geldwaesche-durch-Kryptowaehrungen.html.

Turner, A./Irwin, A. (2017), Bitcoin transactions: a digital discovery of illicit activity on the blockchain, in: https://www.researchgate.net/publication/321052607_Bitcoin_transactions_a_digital_discovery_of_illicit_activity_on_the_blockchain, abgerufen am 20. 1. 2023.

Weise, S. (2019), World Wide Web oder doch Wild Wild West?, in: https://www.kas.de/de/einzeltitel/-/content/world-wide-web-oder-doch-wild-wild-west.

Würfel, S., Was ist ein Rug Pull?, in: https://captainaltcoin.com/de/rug-pull-krypto/, abgerufen am 23. 1. 2023.

Wyss, M. (2021), Rosige Zukunft für Smart Contract und Kryptowährungen, in: https://morethandigital.info/die-wichtige-rolle-smart-contract-und-kryptowahrungen-zukunft/.

Zero To Hundred (2022), Rug Pull. Was ist ein Rug Pull?, in: https://0-100.io/glossar/rug-pull, abgerufen am 23. 1. 2022.

Eidesstaatliche Erklärung

Ich versichere, dass ich die vorliegende Bachelorarbeit selbständig angefertigt, nicht anderweitig für Prüfungszwecke vorgelegt, alle benutzten Quellen und Hilfsmittel angegeben, sowie wörtliche und sinngemäße Zitate als solche gekennzeichnet habe.

Ulm, den 12.03.2023