Hochschule für Polizei und öffentliche Verwaltung NRW
Abteilung Gelsenkirchen
Studienort Gelsenkirchen
Fachbereich Polizeivollzugsdienst

Bachelorthesis zum Thema:

Kryptowährungen

Zukunftstechnologien oder kriminelles Werkzeug

Vorgelegt von:

Cedrik Mohr
Kurs: P20/51
Einstellungsjahrgang: 2020
Tel.: [redacted]
E-Mail: cedrik.mohr@studium.hspv.nrw.de

Abgabedatum: 10.05.2023

Erstgutachter/in: Patrick Rohde, M.A.
Zweitgutachter/in: Dr. Frank Kawelovski

Inhaltsverzeichnis

Abkürzungsverzeichnis

BKA ..... Bundeskriminalamt

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

BTC ..... Bitcoin

CEX ..... Centralized Exchange

DAO ..... Decentralized Autonomous Organization

DeFi ..... Decentralized Finance

DEX ..... Decentralized Exchange

ETH ..... Ether oder Ethereum

ICO ..... Initial Coin Offering

IPO ..... Initial Public Offering

KYC ..... Know Your Customer

LAFP NRW ..... Landesamt für Ausbildung, Fortbildung und
..... Personalangelegenheiten der Polizei NRW

NCFI ..... Nordic Computer Forensic Investigator

NFT ..... Non-Fungible Token

ONSINT ..... Open Source Intelligence

StGB ..... Strafgesetzbuch

1. Einleitung

Kryptowährungen haben sich in den letzten Jahren immer weiterverbreitet und haben somit teilweise unsere Denkweise über Finanzen und Währungen verändert. Doch mit der wachsenden Beliebtheit von Kryptowährungen, wie zum Beispiel Bitcoin oder Ethereum, entstanden auch kontroverse Debatten über diese. Einige Fachleute argumentieren, dass Kryptowährungen die Finanzwelt revolutionieren können. Andere Fachleute sind wiederum besorgt, dass Kryptowährungen nur von Kriminellen genutzt werden und sie ihnen ihre Machenschaften erleichtern.

1.1 Zielsetzung und erwartete Ergebnisse

Die vorliegende Bachelorarbeit verfolgt die folgenden Ziele:

Es sollen grundlegende Informationen rund um das Thema Kryptowährung auf eine verständliche Weise aufbereitet werden. Dazu wird neben dem theoretischen Hintergrund auch auf Anwendungsoptionen von Kryptowährungen eingegangen. Weiter sollen illegalen Handlungen, die mit Kryptowährungen durchgeführt werden, erläutert werden. Die grundlegenden Informationen und Anwendungsoptionen von Kryptowährungen sind dabei wichtig, um die illegalen Handlungen zu verstehen, beziehungsweise um nachzuvollziehen, welche Vorteile Kryptowährungen für Kriminelle haben. Ein weiteres Ziel ist, dass diese Bachelorarbeit als ein Nachschlagewerk für Laien auf dem Gebiet der Kryptowährungen fungieren soll. Gerade Strafverfolgungsbehörden sollen auf diese Weise einen guten Einblick in die Kryptowährungen und die kriminellen Handlungen, die mit diesen zusammenhängen, bekommen. Weiter soll vereinzelt auf Bereiche der Kryptowährungen eingegangen werden, die nicht zwangsläufig mit Kriminalität zu tun haben. Dies soll einen umfassenderen Blick auf Kryptowährungen gewährleisten, da bei Kryptowährungen vieles miteinander zusammenhängt.

Mit Blick auf die zu erwartenden Ergebnisse ist davon auszugehen, dass der Leser nach dem Lesen der Bachelorarbeit einen grundlegenden Einblick in Kryptowährungen erlangt hat und dadurch versteht, wie diese für illegale Handlungen verwendet werden können. Darüber hinaus hat der Leser auch grundsätzliches Wissen über Kryptowährungen erlangt. Gerade Personen, die für Strafverfolgungsbehörden arbeiten und vorher kaum Wissen über

Kryptowährungen hatten, können auf diese Weise mit den Opfern „mitreden“ und somit auch die zugrundeliegende kriminelle Handlung verstehen.

1.2 Aufbau der Bachelorarbeit

Die Bachelorarbeit besteht aus drei Hauptkapitel. Das erste Hauptkapitel beschreibt den theoretischen Hintergrund von Kryptowährungen, insbesondere wie diese vereinfacht funktionieren. Weiter werden in diesem Kapitel wichtige Begriffe in Zusammenhang mit Kryptowährungen erläutert. Im zweiten Hauptkapitel wird auf die Anwendungsoptionen und Potenziale von Kryptowährungen eingegangen. Im dritten Hauptkapitel werden die Informationen aus den ersten beiden Hauptkapiteln genutzt, um kriminelle Handlungen mit Kryptowährungen zu erläutern. Weiter wird exemplarisch auf die Polizeiarbeit im Zusammenhang mit Kryptowährungen, beziehungsweise Cybercrime, eingegangen. Am Ende dieser Arbeit steht ein Fazit.

1.3 Methodisches Vorgehen

Zu Kryptowährungen und zu Cybercrime ist zahlreiche Fachliteratur vorhanden und insbesondere in Bezug auf Kryptowährungskriminalität gibt es viele Internetquellen. Weiter gibt es zu allen Kryptowährungen so genannte „Whitepapers“, beziehungsweise Internetseiten. Die Whitepapers oder die Internetseiten enthalten grundsätzlich alle Informationen über legitime Kryptowährungen. Mit Hilfe der genannten Quellen können die Ziele der Bachelorarbeit vollumfänglich bearbeitet werden.

1.4 Wissenschaftlicher Stand

Kryptowährungen wurden in den letzten zehn Jahren immer größer und beliebter. Aus diesem Grund hat sich auch die Wissenschaft immer mehr für Kryptowährungen interessiert und somit ist zahlreiche Fachliteratur entstanden. Gleichzeitig sind auch kriminelle Handlungen in Zusammenhang mit Kryptowährungen gestiegen. Strafverfolgungsbehörden, Unternehmen und Privatpersonen haben dies auch bemerkt und sich in diese Richtung besser aufgestellt und diverse Dokumente zur Information erstellt.

2. Theoretischer Hintergrund

2.1 Definition und Grundlagen von Kryptowährungen

„Kryptowährungen sind digitale (Quasi-)Währungen mit einem meist dezentralen, stets verteilten und kryptografisch abgesicherten Zahlungssystem." (Bendel, 2021). Die wohl bekannteste Kryptowährung ist „Bitcoin". Bitcoin wurde 2008 von Satoshi Nakamoto erfunden. Satoshi Nakamoto ist ein Pseudonym und bis heute ist die Person oder Gruppe, welche das Pseudonym benutzt, nicht bekannt. Ziel dieser Währung war es, Geldtransaktionen ohne zentrale Instanz, wie zum Beispiel eine Bank von Person zu Person, beziehungsweise von Endgerät zu Endgerät durchführen zu können (Rosenberger, 2018, S. 9).

Die meisten Kryptowährungen, so auch Bitcoin, unterliegen gewissen Kernideen. Eine dieser Ideen ist die Dezentralisierung. Sie sorgt dafür, dass die Rechnungen, beziehungsweise die Blockchain, nicht an einem Ort gespeichert werden, sondern auf viele unterschiedliche Nutzer aufgeteilt werden, welche sich im Netzwerk befinden. Eine weitere Kernidee ist das Vertrauen, beziehungsweise das Nicht-Vertrauen. Es gibt grundsätzlich keine zentrale Instanz bei Kryptowährungen. Somit muss das Vertrauen auf eine andere Weise hergestellt werden. Dafür hat Nakamoto im Falle von Bitcoin, die Blockchain-Technologie angewandt. Die Blockchain ist eine chronologische Aneinanderreihung von sogenannten Blöcken. In jedem Block werden neue Transaktionen niedergeschrieben und dieser wird der Blockchain angehangen. Somit speichert die Blockchain sämtliche Transaktionen, die jemals getätigt wurden. Die Bitcoin-Blockchain und ihr Inhalt können jederzeit über Online-Plattformen wie blockchain.info eingesehen werden. Die Transaktionen werden nicht im Klarnamen ausgeführt, sondern über eine Art Pseudonym. Die Blockchain im Falle von Bitcoin ist somit fast vollständig anonym (pseudonym) und transparent. Anonymität und Transparenz sind weitere Kernideen von Kryptowährungen. Doch wie schafft die Blockchain nun Vertrauen? Jeder neue Block wird von allen Instanzen im Netzwerk überprüft, verifiziert und anschließend an das Ende der Blockchain angehangen und verkettet. Somit ist es faktisch nicht möglich die Blockchain zu manipulieren (Rosenberger, 2018, S. 18–20). Im nächsten Kapitel wird das genannte Vorgehen technisch weiter erläutert.

Bitcoin ist die größte Kryptowährung nach der Marktkapitalisierung. Die zweitgrößte ist Ethereum (Coinmarketcap, 2023d). Ethereum wird oftmals als 2. Generation der

Blockchain bezeichnet, da diese nicht nur Transaktionen auf der Blockchain ausführen kann, sondern sogenannte Smart Contracts. Smart Contracts sind Programme, die zwischen den Vertragsparteien gewisse Bedingungen und Vereinbarungen prüfen und durchsetzen können. Weiter gibt es noch viele weitere Anwendungsmöglichkeiten für Smart Contracts (Hönig, 2020, S. 117–118). Smart Contracts werden im Kapitel 2.2.5 näher erläutert.

Kryptowährung ist der Überbegriff für viele verschiedene Arten von Kryptowährungen. Die sogenannten echten Kryptowährungen (Zahlungstoken) haben den Zweck, dass sie als alternative Zahlungsmittel eingesetzt werden sollen, also um Waren oder Dienstleistungen zu erwerben. Ein solche Währung ist Bitcoin. Weiter gibt es Plattform-Token, diese werden benötigt, um an der zugrunde liegenden Plattform teilzunehmen. Eine solche Kryptowährung ist Ethereum (oder Ether genannt), um Transaktionen und Smart Contracts auf Plattform auszuführen, wird Ether als Gebühr verlangt. Ether kann zwar auch als Zahlungstoken verwendet werden, dafür ist er aber hauptsächlich nicht bestimmt. Eine weitere Kryptowährungsart sind die Utility-Token. Sie können als eine Art Eintrittskarte gesehen werden. Sie ermöglichen Zugriff auf bestimmte Dienstleistungen oder Produkte. Des Weiteren gibt es Security-Token. Diese können als Anteile an einem Projekt, Unternehmen oder System gesehen werden. Besitzer von Security-Token bekommen oftmals eine Art Dividende ausgezahlt. Diese wird durch Transaktionsgebühren oder durch den erwirtschafteten Umsatz des Projekts bezahlt (Izzo-Wagner & Siering, 2020, S. 7–8).

Weiter können Kryptowährungen noch in „Coins“ und „Token“ unterschieden werden. Coins sind Kryptowährungen, welche über eine eigenen Blockchain verfügen. Beispiele hierfür sind Bitcoin und Ethereum. Tokens hingegen sind Kryptowährungen, die durch Smart Contracts auf einer bestehenden Blockchain generiert werden. Sie profitieren von der zugrundeliegende Blockchain. So gibt es zum Beispiel zahlreiche Token, welche auf der Ethereum-Blockchain laufen (Moreland, 2022).

Die in diesem Kapitel genannten Zahlungstoken, Plattform-Token, Utility-Token und Security-Token sind nicht zwangsläufig Token, sondern können entgegen ihrem Namen auch Coins sein. Bitcoin zum Beispiel ist ein klassischer Zahlungstoken, hat aber eine eigene Blockchain und ist somit ein Coin.

2.2 Technische Grundlagen von Kryptowährungen

2.2.1 Bitcoin und Proof-of-Work

Sobald eine Person eine Bitcoin Transaktion ausführt, passiert Folgendes: Die Bitcoin Software auf dem Endgerät der Person verschickt an alle bekannten Netzwerkknotenpunkte (Nodes) die Transaktion. Die Nodes überprüfen und verifizieren die Transaktion, unter anderem die Bitcoin-Adressen des Empfängers und Versenders, die Höhe des Betrags an Bitcoin und ob der Versender über die zu versendenden Bitcoins verfügt. Anschließend senden die Nodes die Transaktion an andere Nodes, mit denen sie verknüpft sind. Auf diese Weise verbreitet sich die Transaktion über das gesamte Bitcoin-Netzwerk aus, sodass jede Node Kenntnis von der Transaktion hat. Doch wie kommen die Transaktionen nun in einen Block der Blockchain? Diese Aufgabe übernehmen die sogenannten Miner. Die Miner sind für die Überwachung, die Einmaligkeit der Transaktion und für die Blockerschaffung zuständig. Jeder Miner im Netzwerk versucht zeitgleich den nächsten Block zu erschaffen, indem er eine kryptografische-mathematische Berechnung durchführt. Der erste Miner der die richtige Lösung generiert, darf den nächsten Block erschaffen und die Transaktionen in diesem niederschreiben. Bevor der Block endgültig an die Blockchain angehangen wird, überprüft ein gewisser Prozentsatz der anderen Miner die Rechnung und den Block. Wenn diese Überprüfung erfolgreich ist, wird der Block angehangen. Der Miner, welcher den Block erschaffen hat, bekommt zum aktuelle Zeitpunkt 12,5 Bitcoins ausgezahlt. Anschließend wird die neue Blockchain über das Netzwerk durch die Nodes verbreitet und wieder auf Gültigkeit überprüft. Dabei gilt das Mehrheitsprinzip. Die Rechenaufgabe wird etwa alle 10 Minuten gelöst, somit wird auch alle 10 Minuten ein neuer Block generiert. Das gerade beschriebene Verfahren nennt sich „Proof-of-Work“ und ist ein sogenannter Konsensmechanismus. Er ist sehr rechen- und stromintensiv (Rosenberger, 2018, S. 19–20).

2.2.2 Ethereum und Proof-of-Stake

Ethereum benutzte wie Bitcoin ein Proof-of-Work Konsensmechanismus. Seit 2022 benutzt Ethereum den sogenannten „Proof-of-Stake“ Konsensmechanismus. Bei Proof-of-Stake bekommt nicht der Miner, in Proof-of-Stake Konzepten Validator genannt, der zuerst eine Rechnung löst, das Recht einen neuen Block zu generieren, sondern es wird durch eine Art Zufallssystem entschieden. Ein Validator kann jeder werden, der Ether (ETH) mit Hilfe eines Smart Contracts hinterlegt, das sogenannte „Staken“. Je mehr ETH hinterlegt wurden,

desto höher ist die Chance das Recht zum Generieren des nächsten Blocks zu bekommen. Ein wesentlicher Vorteil von Proof-of-Stake im Gegensatz zu Proof-of-Work ist, dass die Validatoren (Miner) nicht miteinander konkurrieren. Das heißt, sie benötigen nur Rechenleistung, wenn sie als neue Blockersteller ausgewählt wurden und müssen nicht wie bei Proof-of-Work unentwegt Rechnungen lösen. Sollte ein Validator nicht als nächster Blockersteller ausgewählt werden, so validiert er die Erstellung des Blocks, also überprüft sie. Sollte er dabei „bösartige“ oder falsche Blöcke validieren, kann er die anfänglich hinterlegten ETH verlieren. Validatoren bekommen einmal durch das Erstellen von Blöcken ETH und einmal durch das Validieren von Blöcken. Des Weiteren zahlen die Benutzer bei Transaktionen eine Gebühr in ETH, die auch „Gas“ genannt wird (Ethereum, o.D.b).

2.2.3 Private Key und Public Key

Wie bereits erwähnt, erfolgen Krypto-Transaktion nicht über Klarnamen, sondern mit Hilfe von Pseudonymen, diese werden öffentliche Schlüssel, beziehungsweise Public Key genannt. Die öffentlichen Schlüssel können grob mit einer IBAN-Nummer aus der klassischen Finanzwelt verglichen werden. Das Gegenstück des öffentlichen Schlüssels ist der private Schlüssel, beziehungsweise Private Key. Der private Schlüssel sollte immer geheim bleiben, denn jeder, der den privaten Schlüssel kennt, kann Transaktionen einleiten und die zugrunde liegenden Vermögenswerte verwalten. Aus dem privaten Schlüssel kann immer wieder der öffentliche Schlüssel generiert werden, andersrum ist dies grundsätzlich unmöglich. Eine Transaktion wird mit Hilfe des öffentlichen Schlüssels des Empfängers verschlüsselt. Nur der private Schlüssel des Empfängers kann die Transaktion entschlüsseln und somit über die Vermögenswerte der Transaktion verfügen (Kurt & Kurt, 2022, S. 21).

2.2.4 Wallets

Der private Schlüssel und der öffentliche Schlüssel sind in einem sogenannten Wallet gespeichert. Ein Wallet ist grundsätzlich ein Programm, welches mit der jeweiligen Blockchain kommuniziert und unter anderem Transaktionen durchführen kann. Es gibt verschiedene Arten von Wallets, die sich durch Datensicherheit, Benutzerfreundlichkeit und technischer Einfachheit unterscheiden. Grob kann man drei Wallet-Arten unterscheiden, zum einen die Hardware-Wallets, zum anderen die Software-Wallets und die Online-E-Wallets. Die Hardware-Wallets gelten als besonders sicher, da sie nicht permanent mit einem Computer oder Netzwerk verbunden sind, sondern wie eine Art USB-Stick nur benutzt werden, wenn eine

Transaktion durchgeführt werden soll. Weiter sind die meisten Hardware-Wallets nochmals intern gesichert und verschlüsselt. Software-Wallets sind Programme auf dem PC des Benutzers. Sie speichern den öffentlichen und privaten Schlüssel auf der Festplatte des Benutzers. Diese Wallets sind einfach zu bedienen. Der Nachteil ist, dass diese Wallets anfällig für Schadsoftware sind. Somit sollten sie nur für kleine Mengen von Kryptowährungen benutzt werden. Online-E-Wallets sind Wallets, welche sich auf einem Server befinden, der mit dem Internet verbunden ist. Somit kann auf diese Wallets von überall zugegriffen werden, wenn eine Internetverbindung besteht. Dabei muss aber auf den Hersteller dieser Wallets vertraut werden, da es zu einem Datenleck kommen kann und jemand anderer Zugriff auf die Wallets bekommen könnte. Eine Unterform der Online-E-Wallets sind die Börsen-Wallets. Die Börsen-Wallets liegen auf einem Unternehmensserver und werden über das Unternehmen als Zwischenhändler durch den jeweiligen Benutzer verwaltet. Der große Nachteil ist, dass das Wallet nicht dem Benutzer gehört, sondern dem Unternehmen. Somit muss dem Unternehmen vertraut werden. Die Hardware-Wallets und die meisten Software-Wallets können mit einem sogenannten Wiederherstellungs-Seed rekonstruiert werden. Dieser Seed besteht aus 12 oder 24 Wörtern aus einem vordefinierten Wörterbuch. Das heißt, wenn jemand diese Wörter hat, kann er das Wallet wiederherstellen und über die Vermögenswerte eines anderen verfügen (Hellwig et al., 2021, S. 46–49).

Des Weiteren werden Hardware-Wallets als Cold-Wallets und Software-Wallets als Hot-Wallets bezeichnet (Mathys & Gimeno, 2021, S. 141).

Eine besonders sichere Art der Cold-Wallets sind die Paper-Wallets. Hierbei wird der Private Key und manchmal auch der Public Key auf ein Papier geschrieben oder gedruckt. Somit ist ein Paper-Wallet sicher vor Hacking oder technischen Fehlfunktionen. Der Nachteil ist, dass das Papier zerstört oder gestohlen werden kann (Gomzin, 2022, S. 178).

2.2.5 Smart Contracts

Smart Contracts können innerhalb einer Transaktion niedergeschrieben und ausgeführt werden. Diese Programme sind, wie die Transaktionen, für jedermann einsehbar. Weiter können diese Programme nicht ohne weiteres verändert werden. Somit ist es wichtig, dass diese von Anfang an ordnungsgemäß funktionieren, da es sonst zu Angriffen und weitreichenden Folgen für die Blockchain kommen kann (Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., 2017, S. 19–20). Durch Smart Contracts können eine

Reihe von Anwendungen realisiert werden. Auf Grundlage von Ethereum können neue Kryptowährungen erschaffen werden (Token), welche eigenen Regelungen unterliegen. Weiter können sogenannte Decentralized Finance (DeFi) Anwendungen programmiert werden. Mit diesen können Finanzsysteme aufgebaut werden. Ein weiterer bekannterer Anwendungsfall der Smart Contracts sind Non-Fungible-Tokens (NFTs). Mit NFTs können Besitzansprüche von Dateien, wie Bild- oder Musikdateien auf der Blockchain abgebildet werden. Somit wird eine Art Einzigartigkeit in der digitalen Welt erzeugt. Weiter können sogenannte Dezentrale Autonome Organisationen (DAOs) gegründet werden. Mit Hilfe von DAOs können Projekte in einem Kollektiv mit flachen Hierarchien organisiert werden. Sämtliche Entscheidungen werden durch eine Abstimmung getroffen. Eine einzelne Instanz hat keine alleinige Entscheidungsmacht. Auch die finanziellen Mittel einer solchen Organisation werden durch festgeschriebene Regeln verwaltet (Kurt & Kurt, 2022, S. 30–31). Dies waren nur einzelne Beispiele für den Anwendungsbereich von Smart Contracts. Im 3. Kapitel dieser Arbeit, werden die gerade genannten Anwendungen und weitere Anwendungsbereiche im Detail erläutert.

2.2.6 Krypto-Börsen

Die sogenannten Krypto-Börsen sind keine Börsen im rechtlichen Sinne. Sie sind Unternehmen, die zentralisierte Handelsplätze anbieten. Auf Krypto-Börsen können Landeswährungen in Kryptowährungen und umgekehrt getauscht werden oder auch Kryptowährung gegen Kryptowährung. Eine weitere Art der Krypto-Börsen sind sogenannte DEXs (Decentralized Exchanges). Diese funktionieren ohne zentrale Partei, sodass Benutzer mit Hilfe von Smart Contracs Kryptowährungen tauschen können. DEX funktionieren nur mit Kryptowährungen und nicht mit Landeswährungen (Kurt & Kurt, 2022, S. 122–123).

Die größte Krypto-Börse nach Handelsvolumen in 24 Stunden ist Binance (Coinmarketcap, 2023a).

Die meisten zentralisierten Krypto-Börsen (auch Centralized Exchanges (CEX) genannt), wie Binance, führen bei ihren Kunden eine Know Your Customer (KYC) Verifizierung durch. Dies ist eine Identitätsverifizierung des Kunden. KYC ist in vielen Ländern für Banken und anderen Finanzunternehmen Pflicht. Dies geschieht um Betrug, Geldwäsche und andere kriminelle Handlungen zu bekämpfen. Ein Account, welcher nicht durch den KYC-Prozess verifiziert wurde, hat auf der Binance-Plattform starke Limitierungen (Binance, 2021). Somit

haben es Kriminelle schwerer, illegal erhaltene Kryptowährungen in Landeswährungen zu tauschen. Diese müssten somit vor der Einzahlung auf eine solche Krypto-Börse gewaschen werden. Dies wird in Kapitel 4.1 erläutert.

3. Anwendungsbereiche und Potenziale von Kryptowährungen

Wie bereits in den vorgegangenen Kapiteln erwähnt, bieten Kryptowährungen viele Anwendungsbereiche und Potenziale. In diesem Kapitel werden die einzelnen Anwendungsoptionen näher erläutert.

3.1 Decentralized Autonomous Organization (DAO)

DAOs werden kollektiv geführt und mit Hilfe einer Blockchain organisiert. Das Kollektiv hat grundsätzlich ein einheitliches Ziel. Mit einer DAO können Menschen weltweit an einem Projekt arbeiten, ohne einer Führungskraft zu vertrauen, welche zum Beispiel das Vermögen der Organisation verwaltet. DAOs haben keine Geschäftsführer, welche aus Versehen oder böswillig Fehler machen. Stattdessen bestimmt der auf der Blockchain niedergeschriebene Programmiercode, welche Regeln die Organisation hat, wie sie arbeitet und wie das Vermögen genutzt werden kann. Dieser Programmiercode wird mit Hilfe von Smart Contract umgesetzt. Diese Smart Contracts können nur durch eine mehrheitliche Entscheidung im Nachhinein geändert werden. Alle Entscheidungen der Organisation werden durch das Kollektiv durch Vorschläge und Abstimmungen geregelt. All diese Entscheidungen passieren offen auf der Blockchain. Wenn eine Person finanzielle Mittel der DAO nutzen möchte, muss dies durch eine Abstimmung bestätigt werden. Keine Einzelperson kann alleinige Entscheidungen über die DAO treffen. Somit bieten DAOs eine neue Form der globalen Zusammenarbeit. Die Personen, welche Zusammenarbeiten wollen, müssen sich nicht gegenseitig vertrauen, sondern nur dem Programmiercode, welcher für jede Person öffentlich auf der Blockchain einsehbar ist. Eine Person bekommt ein Stimmrecht in einer DAO, wenn sie die dafür vorgesehen Token in ihrem Wallet besitzt. Die meisten DAO-Token können berechtigungsfrei gekauft werden. Andere DAO-Token werden nur durch bestimmte Regelungen ausgegeben. Es gibt zahlreiche Projekte bei denen DAOs sinnvoll sind. Wohltätigkeitsorganisation sind ein Beispiel. Durch eine DAO können weltweit Spenden angenommen werden und diese können öffentlich und transparent verteilt werden. Ein weiteres Beispiel ist kollektives Eigentum. Auf diese Weise können Menschen weltweit in

physische oder digitale Vermögenswerte investieren und die Mitglieder können transparent und als kollektiv über die weitere Verwendung entscheiden (Ethereum, o.D.a).

Viele Krypto-Projekte setzten auf das DAO-Prinzip, so auch eine der größten Decentralized Exchanges (DEX) Uniswap (Uniswap, o.D.). Was eine DEX ist, wird in Kapitel 3.3 erläutert.

3.2 Decentralized Finance (DeFi)

„DeFi wants to enable an alternative financial system that is built bottom-up, completely decentralized, censorship-free, low-fee, fully-automated, and without counterparty risk." (Grigo et al., 2020, S. 9).

Jede Person, unabhängig von ihrer Herkunft oder sozialem Status, kann DeFi-Anwendungen nutzen. Dies funktioniert im traditionellen Bankensystem nicht. Doch welche Vorteile hat DeFi neben den gerade genannten, gegenüber dem traditionellen Banksystemen? Zum einen sind alle DeFi-Anwendungen Open-Source, das heißt jeder kann den Programmiercode einsehen, zum anderen sind alle jemals getätigten Transaktionen einsehbar und somit transparent. Im Gegensatz dazu, sind traditionelle Banken eine Art Black Box. Eine außenstehende Person hat kaum Einblick in die bankinternen Prozesse. Sie muss auf das vertrauen, was die Bank angibt zu tun. Die Banken werden von diversen Einrichtungen, wie zum Beispiel die BaFin überwacht, dennoch kann gesagt werden, dass traditionelle Banken weniger transparent in Bezug auf ihre eigenen Investitionen sind als dezentrale und Open Source DeFi-Anwendungen (Grigo et al., 2020, S. 9–10).

Ein Beispiel für ein DeFi-Projekt ist Maker und seinem Stablecoin namens DAI. Ein Stablecoin ist eine Kryptowährung, welche an eine Landeswährung gebunden ist. In diesem Fall ist die Kryptowährung an den US-Dollar gebunden. Das heißt, ein DAI ist einen US-Dollar wert. DAI werden generiert, indem ein Benutzer Ether durch einen Smart Contract hinterlegt. Die hinterlegte Kryptowährung muss immer mindestens 150 % der generierten DAI entsprechen, damit eine Preisstabilität entsteht. In diesem Beispiel ist Ether die hinterlegte Kryptowährung und diese schwankt im Preis. Das heißt, wenn die Kryptowährung unter die 150 % Marke im Vergleich zu den ausgezahlten DAI fällt, dann muss die Person weitere Ether hinterlegen. Sollte sie dies nicht tun, wird sie liquidiert. Somit werden ihre hinterlegten Ether verkauft und sie erhält eine Art Vertragsstrafe. Zusammengerechnet verliert die Person 16 % des Wertes der anfänglich generierten DAI. Dies geschieht alles automatisch

durch einen Smart Contract. Der Verkaufsprozess der hinterlegten Ether wird durch eine automatische Auktion geregelt. Die Bieter bezahlen in DAI und bekommen 3 % von der genannten Vertragsstrafe als Vorteil. Die DAI, welche zum Bezahlen der Auktion benutzt wurden, werden „verbrannt“, das heißt sie werden für immer unbrauchbar gemacht. Somit wird einer Inflation von DAI entgegengewirkt. Ein Beispiel: Person A hinterlegt Ether im Wert von 150 $. Somit bekommt sie maximal 100 Dai im Wert von 100 $. Sollte sie die maximale Anzahl an DAI nehmen, so sind genau 150 % der ausgezahlten DAI als Ether, umgerechnet in Dollar, hinterlegt. Sobald der Preis von Ether nun fällt, ist die 150 % Bedingung nicht mehr gegeben und Person A müsste mehr Ether hinterlegen, um die Bedingung wieder zu erfüllen. Sollte sie dies nicht tun, werden die hinterlegten Ether in Wert von 100 DAI (100 $), wie oben beschrieben, verkauft und eine 16 % Strafe wird angerechnet. Die anfänglich generierten 100 DAI kann Person A nun behalten. Sie bekommt aber nicht mehr die Ether im Wert von 150 $ zurück, sondern nur noch Ether im Wert von 36 $ (150 – 100 – (100 * 16 / 100)). Aus diesem Grund sollte ein höherer Betrag als 150 % hinterlegt werden. Im umgekehrten Fall steigt Ether, so dass der hinterlegte Ether nicht mehr 150 $, sondern 300 $ wert ist. Person A kann nun die 100 geliehenen DAI gegen die ursprüngliche Menge an Ether eintauschen. Diese sind aber nicht mehr 150 $, sondern 300 $ wert. Mit dem letzten Beispiel wurde auch die Antwort auf die Frage genannt, warum eine Person Ether hinterlegen soll, um viel weniger DAI zu bekommen. Die Antwort ist, dass die Person auf einen Kursanstieg hofft. Mit diesem System kann die Kryptowährung Ether weiter gehalten werden und Kursgewinne können in Zukunft verwirklicht werden. Währenddessen kann DAI für unzählige andere Projekte und Anwendungen verwendet werden oder über eine Krypto-Börse ausgezahlt oder getauscht werden. Somit liegt die Kryptowährung nicht nur auf dem Wallet herum, sondern mit einem Teil des Wertes von ihr kann gearbeitet werden. Es gibt noch viele weitere Stablecoin Projekte, wie Maker. Doch Maker ist zurzeit einer der wichtigsten Projekte. Das ganze Projekt ist dezentral und läuft automatisiert. Somit ist das Projekt an kein Unternehmen gebunden, welches unter Umstände bankrottgehen könnte (Grigo et al., 2020, S. 11–12). Stablecoins können auch direkt getauscht, beziehungsweise erworben werden. Auf diese Weise können Kryptowährungen ohne die hohe Volatilität von anderen Kryptowährungen gehalten werden. Dies können sich auch Kriminelle zu nutzen machen. Mit Stablecoins besteht nicht die Gefahr, dass die erbeuteten Kryptowährungen an Wert verlieren.

Wie bereits erwähnt, funktionieren solche Projekte automatisch durch Smart Contracts. Diese Smart Contracts sind zwar für jede Person einsehbar, aber für den Laien schwer bis kaum zu verstehen. Somit kann es sein, dass die Smart Contracts entweder Lücken haben, welche böswillig ausgenutzt werden können oder der Smart Contract selbst ist böswillig und betrügerisch programmiert. Gerade DeFi-Anwendungen sind beliebtes Angriffsziel für Kriminelle. Dies wird in Kapitel 4.5 näher erläutert. Aus diesem Grund ist es für einen Krypto-Anfänger ratsam an größeren Projekten teilzunehmen, da es bei diesen wahrscheinlicher ist, dass Lücken im Programmiercode oder böswillige Programmiercodes erkannt und veröffentlicht werden.

3.3 Decentralized Exchange (DEX)

Die meisten DEX haben zwei Hauptanwendungsoptionen, zum einen ermöglichen sie den Tausch zwischen zwei Kryptowährungen und zum anderen können die Nutzer Liquidität für den Tausch bereitstellen und bekommen im Gegenzug eine Vergütung. Eine bekannte DEX ist Uniswap. Uniswap funktioniert auf der Ethereum-Blockchain und mit einem Ethereum-basierten Token (Grigo et al., 2020, S. 13). Der Uniswap-Token besitzt 2023 eine Marktkapitalisierung von 2,8 Milliarden US-Dollar und ist somit eine der größte DEXs und eine der größten DAOs im Jahr 2023 (Coinmarketcap, 2023f). Gerade noch sehr kleine und unbekannte Kryptowährungen können ausschließlich über DEX getauscht/erworben werden. Somit sind DEX auch der Hauptzugangspunkt für betrügerische Kryptowährungen.

3.4 Initial Coin Offering (ICO)

Der Begriff Initial Coin Offering (ICO) ist von dem Börsenbegriff Initial Public Offering (IPO) abgeleitet. Bei einem IPO geht ein Unternehmen an die Börse und verkauft somit Unternehmensanteile. Ein ICO kann als Crowdfunding gesehen werden, nur ohne Crowdfunding-Plattform. Bei einem ICO versucht ein Projekt Finanzmittel zu beschaffen, um eine neue Kryptowährung zu erschaffen, beziehungsweise sie zu etablieren. Die Investoren eines ICO bekommen im Gegenzug diese neue Währung auf ihre Wallets. ICOs sind meistens durch Smart Contracts geregelt. Auf diese Weise wurde auch anfänglich Ethereum finanziert. 2014 wurden Ether im Gegenwert von 18,4 Millionen US-Dollar gekauft. Im Jahr 2017 wurden etwa 5,5 Milliarden US-Dollar in ICOs investiert. Ein Jahr zuvor waren es lediglich 295 Millionen US-Dollar. Somit gab es einen regelrechten Hype um ICOs. ICOs stellen ein hohes Potential für Spekulanten aber auch ein extremes Risiko für die Investoren dar.

Traditionelle Finanzmärkte sind durch Behörden und Aufsichtsstellen reguliert. Dies trifft auf ICOs nicht zu (Rosenberger, 2018, S. 95–97).

Die Bundesanstalt für Finanzdienstleistungsaufsicht (Bundesanstalt für Finanzdienstleistungsaufsicht [BaFin], 2017) sieht bei ICOs ein hohes Risiko für Verbraucher. Somit muss der Verbraucher sich über einen Totalverlust seiner Investition klar sein. Dieser Totalverlust kann entweder durch große Preisschwankungen entstehen oder auch durch Betrüger geschehen. Betrüger können den zugrundeliegenden Smart Contract so programmieren, dass die Investition direkt an den Betrüger gesendet wird und somit kann der Verbraucher nicht mehr über die Investition verfügen. Der Programmiercode solcher Smart Contracts ist zwar öffentlich, aber nur die wenigsten Verbraucher können die geschriebenen Codezeilen verstehen und somit abwägen, ob das Projekt kein Betrug ist. Weiter sind große Preisschwankungen nicht selten, da die Geschäftsmodelle und die Entwicklung der ICO-Projekte meist experimentell sind und somit fällt es teilweise auch Experten schwer, ein solch neues Projekt richtig zu beurteilen.

Zusammenfassend lässt sich sagen, dass ICOs eines der höchsten Risiken im Kryptobereich darstellen. Nichtsdestotrotz können sie eine hohe Chance für Spekulanten und kleine Projekte sein. Investoren sollten sich aber immer über die hohen Risiken bewusst sein. ICOs sind also eher etwas für erfahrenere Krypto-Nutzer. Des Weiteren bieten sie eine gute Möglichkeit für Betrüger, um an Vermögenswerte zu kommen. Dies wird in Kapitel 4.6 näher erläutert.

3.5 Non-Fungible Tokens (NFTs)

Zwischen dem ersten Quartal 2021 und dem ersten Quartal 2022 gab es einen Anstieg des Handelsvolumens von NFTs um 714 %. Das Handelsvolumen ist von 2 Milliarden US-Dollar auf 16,5 Milliarden US-Dollar gestiegen. Weiter ist die Anzahl der Käufer um 1489 % gestiegen, von 73 777 auf 1 172 235 und die Anzahl der Verkäufer um 2345 %, von 33 377 auf 816 027 (Bocksch, 2022). Zwischen 2021 und 2022 hatten NFTs einen regelrechten Hype. Doch dieser Hype hat auch zahlreiche Betrüger angezogen. Welche kriminellen Handlungen mit NFTs durchgeführt werden, wird im Kapitel 4.7 dieser Arbeit erläutert.

Viele Menschen besitzen digitale Wertgegenstände, wie Internetdomains, Computerspiele auf einem Account oder Lieder auf iTunes. Doch all diese Gegenstände sind oftmals nur in

der vorgegebenen Umgebung nutzbar. Es kann nicht frei über diese verfügt werden. Sie können weder transferiert, noch verkauft werden. Weiter gibt es keine Garantie, dass der erworbene Gegenstand einzigartig ist. All diese Probleme können NFTs lösen. NFTs repräsentieren Eigentumsansprüche von (digitalen) Wertgegenständen. Diese Eigentumsansprüche werden durch Smart Contracts auf einer Blockchain geschrieben. Solche Wertgegenstände können mp3-Dateien, ein JPEG-Bild, eine Domain oder auch physische Gegenstände wie Häuser oder Gemälde sein. Das Wichtigste an Non-Fungible Tokens ist, dass sie „nicht fungibel“ sind, also nicht austauschbar. Ein 10-Euroschein ist zum Beispiel fungibel, da er beliebig durch einen anderen 10-Euroschein ersetzt werden kann. Ein Mehrfamilienhaus, welches an einer bestimmen Stelle erbaut wurde, ist nicht fungibel, da es nicht durch ein anderes Haus austauschbar ist. Weiter hat ein NFT immer nur einen Eigentümer, beziehungsweise ist nur einem öffentlichen Schlüssel zugeordnet. Der Eigentumsanspruch ist auf der Blockchain niedergeschrieben und kann nicht manipuliert werden. Auf diese Weise kann der Eigentümer seinen Anspruch eindeutig beweisen. Weiter kann nur er frei über das NFT verfügen (Kurt & Kurt, 2022, S. 92–93).

Der Kerngedanke von NFTs war, dass Künstler Kontrolle über ihre Werke haben und mit ihnen Geld erwirtschaften können (Dash, 2021).

NFTs können auf NTF-Markplätzen erworben werden. Dort können NTF-Ersteller oder auch NFT-Besitzer ihre NFTs gegen Kryptowährung anbieten und tauschen. Einer der größten NFT-Markplätze ist OpenSea (OpenSea, o.D.).

Zusammenfassend lässt sich sagen, dass NFTs Einzigartigkeit im virtuellen Bereich ermöglichen. Dies war vor NFTs nicht möglich. Aus diesem Grund können NFTs noch für viele weitere Dinge benutzt werden. So können akademische Bescheinigungen, Anwesenheitslisten oder abgeschlossene Kurse mit NFTs ersetzt werden. Weiter kann auf NFTs von überall mit dem Handy zugegriffen werden. Weiter sind solche Systeme in Folge der Blockchain-Technik nur schwer zu manipulieren oder zu hacken (Pravin, 2022, S. 13).

3.6 Metaverse

> Das Metaverse (dt. "Metaversum") ist ein virtueller Raum, in dem sich Benutzer mit Hilfe von Avataren bewegen und in dem sie virtuelle Artefakte beeinflussen und nutzen können, etwa wenn sie sich Kleidung überziehen, ein Haus bauen und dieses einrichten, eine Tür öffnen und auf die Straße hinaustreten und dort Mitspieler und Gleichgesinnte treffen. Wie in der realen Welt kann man dort leben, arbeiten, lernen, Handel treiben, Gespräche führen und Beziehungen aufbauen. (Bendel, 2023)

Das Metaverse gilt aktuell als Megatrend. Spätestens seitdem Mark Zuckerberg Facebook zu einem allumfassenden virtuellen Ökosystem umbauen möchte, ist der Begriff Metaverse vielen Menschen ein Begriff. Auch andere große Konzerne, wie Microsoft und Epic Games arbeiten an einem Metaverse. In den meisten Metaversen kann mit Hilfe von Kryptowährung sicher und transparent bezahlt werden (Pfeiffer et al., 2022, S. 28–29).

Decentraland ist mit seiner Kryptowährung „MANA“ zurzeit einer der größten Metaverses nach Marktkapitalisierung (Coinmarketcap, 2023e). Decentraland läuft auf der Ethereum-Blockchain und ist eine „virtual reality platform“. Das Projekt ist eine DAO und wird somit durch die Community geregelt und geleitet. Mit Decentraland können virtuelle 3D-Parzellen mit MANA erworben werden, diese Parzellen sind NFTs, welche auf Smart Contracts basieren. Innerhalb der Parzellen kann der Eigentümer Videospiele oder 3D-Szenen implementieren. Die Eigentümer können bestimmen, welche Mitspieler diese Parzellen betreten können. Weiter können die Eigentümer ihre Parzellen monetarisieren, sodass andere Spieler bezahlen müssen, um dies zu betreten (Decentraland, 2023).

So wie bei jedem Krypto-Trend, gibt es auch hierbei Möglichkeiten, wie Kriminelle diesen ausnutzen. Dies wird in Kapitel 4.8 näher erläutert.

3.7 Risiken im Umgang mit Kryptowährungen

Die Risiken von Kryptowährungen sind im Vergleich zu klassischen Anlagemöglichkeiten hoch. Kryptowährungen sind sehr volatil. Preisschwankungen von hohen zweistelligen Prozentsätzen sind teilweise normal. Bitcoin ist zum Beispiel in der Zeitspanne von November 2021 bis November 2022 von ca. 57 000 Euro/BTC auf ca. 16 000 Euro/BTC gefallen. Mittlerweile, im April 2023, ist Bitcoin wieder auf ca. 25 000 Euro/BTC gestiegen (Coinmarketcap, 2023b). Nichtsdestotrotz haben Personen, welche im November 2021 Bitcoin

erworben haben und bis jetzt nicht verkauft haben, mehr als 50 % Verlust in ihrem Portfolio zu verzeichnen. Doch es gibt nicht nur hohe Preisschwankungen, sondern auch Totalverluste. Diese treten oftmals auf, wenn die Smart Contracts von Krypto-Projekten fehlerhaft sind. So auch bei der Kryptowährung Terra Luna. Zwischen dem 05.05.2022 und dem 13.05.2022 ist der Wert von Luna von ca. 81 Euro/Luna auf 0,006 Euro/Luna gefallen (Coinmarketcap, 2023c). Die Investoren von Terra Luna haben schätzungsweise durch den Crash insgesamt 42 Milliarden US-Dollar verloren. Gerade Kleinanleger aus Südkorea waren betroffen (Költzsch, 2022). Der Crash wurde durch eine Lücke in den Smart Contracts von Terra Luna ausgelöst. Vereinfacht gesagt, hat eine große Abhebung im Luna-Netzwerk im Wert von 2 Milliarden US-Dollar einen Teufelskreis ausgelöst, durch diesen wurden immer mehr Luna generiert und dadurch gab es die oben genannte Inflation der Luna Kryptowährung (Q.ai, 2022). Eine Person, die sich nicht intensiv mit Kryptowährungen beschäftigt, kann Kryptowährungen nur schwer bewerten. Damit geht ein hohes Risiko des Vermögensverlusts einher. Somit ist es nicht unüblich, dass ein hoher Vermögensverlust auch auf legale Weise passiert. Zusätzlich zu den generellen Risiken bei Kryptowährungen, welche nicht auf illegales Handeln zurückzuführen sind, gibt es noch zahlreiche Betrügereien im Kryptobereich, die einen Totalverlust der Investition zur Folge haben können. Mit diesen wird sich im nächsten Kapitel dieser Arbeit befasst.

4. Kryptowährungen und Kriminalität

In den vorherigen Kapiteln wurden wichtige Begriffe und Anwendungsoptionen von Kryptowährungen erläutert. Diese sind nötig, um zu verstehen, wie gewisse kriminelle Handlungen im Kryptobereich entstehen. Die Handlungen werden in den nachfolgenden Kapiteln behandelt. Zunächst wird jedoch auf grundlegende Statistiken im Zusammenhang mit Kriminalität und Kryptowährungen eingegangen: 2022 betrug das Transaktionsvolumen von illegaler Kryptowährung 0,24 % des gesamten Transaktionsvolumens von Kryptowährung. 2021 waren es 0,12 % und 2019 waren es 1,9 %. Das Transaktionsvolumen von illegalen Kryptowährungen hat sich von 2021 auf 2022 zwar verdoppelt, dennoch ist über die Jahre ein Abwärtstrend zu erkennen (Chainalysis, 2023, S. 7).

4.1 Geldwäsche mit Kryptowährungen

Sobald ein Betrüger Kryptowährungen erbeutet hat oder durch eine andere kriminelle Handlung bekommen hat, steht er vor dem Problem, dass diese Kryptowährungen über die zugrundeliegende Blockchain verfolgt werden können. Dieses Problem versprach „ChipMixer“ zu lösen. ChipMixer startete seinen Dienst Mitte 2017. Die Nutzer des Dienstes konnten Bitcoin auf die Plattform transferieren. Dort wurden anschließend Verschleierungsvorgänge (Mixing) durchgeführt und die Kryptowährung im Anschluss wieder ausgezahlt. Seit 2017 sollen dabei mehr als 2,8 Milliarden Euro gewaschen worden sein. Ein großer Teil stammt aus Darknet-Marktplätzen, aus betrügerisch erlangten Kryptowährungen von Ransomware-Gruppierungen und anderen kriminellen Taten. Am 15.03.2023 konnten die Server der Plattform durch die Generalstaatsanwaltschaft Frankfurt – Zentralstelle zur Bekämpfung der Internetkriminalität und dem Bundeskriminalamt beschlagnahmt werden. Weiter konnten Bitcoin im Wert von 44 Millionen Euro sichergestellt werden (BKA, 2023). Doch es gibt noch viele andere Plattformen, die einen ähnlichen Dienst wie ChipMixer anbieten. Zum Beispiel „UniJoin“. UniJoin verspricht nach dem Mixvorgang anonyme Kryptowährungen. Weiter sollen keine Kundendaten gespeichert werden. Die eingezahlten Bitcoins können nach dem Mixen auf bis zu acht neue Bitcoin-Wallets gesendet werden. Die neuen Wallets haben anschließende keine Verbindung mehr zu dem Wallet, welches ursprünglich die Bitcoins eingezahlt hat und sind somit nicht weiter verfolgbar. Im Vordergrund des Unternehmens steht die Privatsphäre und die Anonymität. Sobald eine Person es schafft den öffentlichen Schlüssel, beziehungsweise das Wallet mit einem Klarnamen zu verbinden, kann die Person sämtliche Aktivitäten der anderen Person über die Blockchain einsehen und verfolgen. Sollte so etwas passieren, kann die betroffene Person durch einen CoinMixer, wie UniJoin, wieder Anonymität erreichen (Unijoin, o.D.). Somit haben UniJoin und ähnliche Unternehmen ihre Daseinsberechtigung im Kryptobereich. Nichtdestotrotz nutzen Kriminelle solche Plattformen für Geldwäsche. Im Jahr 2022 waren 24 % des Volumens, welche an die CoinMixer-Unternehmen gesendet wurde, aus illegalen Quellen. Im Jahr 2021 waren es lediglich 10 %. Diese 24 % aus dem Jahr 2022 setzen sich mit 85,1 % aus gestohlenen Kryptowährungen, mit 6,3 % aus Darknet-Markterträgen, mit 3 % aus Ransomware Lösegeld, mit 2,7 % aus generellem Betrug, mit 2,3 % aus Online-Betrugsshops und mit 0,6 % mit sonstigen Betrugsarten zusammen (Chainalysis, 2023, S. 46–47).

Die beschriebene Geldwäsche von Kryptowährungen könnte gemäß § 261 strafbar sein (Kaufmann, 2021).

4.2 Kryptowährungen und die sozialen Medien

Die meisten Kryptowährungen sind eng mit den sozialen Medien verbunden, insbesondere Twitter wird oft genutzt, um Informationen über die Krypto-Projekte zu verbreiten und für diese zu werben. Doch in den sozialen Medien wird nicht nur für legitime Kryptowährungen geworben, sondern auch für betrügerische Projekte. Bei der sogenannten Pump and Dump Betrugsmasche wird primär Twitter benutzt. Dort werden von Accounts mit vielen Followern „Trading-Tipps" gepostet, welche vorwiegend Krypto-Einsteiger ansprechen sollen. Diese Trading-Tipps versprechen oftmals hohe Gewinne. Die Käufer sollen nur lange genug die beworbene Kryptowährung halten. Diese beworbenen Kryptowährungen können meisten ausschließlich auf DEXs getauscht/erworben werden. Sobald die Personen die Kryptowährung kaufen, steigt diese im Wert (Pump). Im Vorfeld haben die Betrüger einen großen Teil der Kryptowährung günstig gekauft. Dieser Teil wird anschließend verkauft (Dump), wenn genug Personen in die Kryptowährung investiert haben und der Preis hoch genug ist. Dadurch fällt die Kryptowährung im Preis und das kann wiederum dazu führen, dass andere Personen aus Angst vor noch größerem Verlust, ebenfalls verkaufen. Das kann zur Folge haben, dass die Kryptowährung so stark fällt, dass die Weiterbetreibung der Kryptowährung unwirtschaftlich ist und diese nicht weiter handelbar ist (Pfeiffer et al., 2022, S. 14). Solche Betrügereien sind leichter zu durchschauen als andere, da sämtliche Wallets, die die Kryptowährung halten, auf der Blockchain einsehbar sind. Somit sollten potenzielle Investoren skeptisch werden, wenn ein Wallet hohe Prozentzahlen der verfügbaren Kryptowährung hält. Aus diesem Grund ist dies eine Betrügerei, die auf Krypto-Einsteiger abzielt. Hierbei kann es sich um einen Kapitalanlagenbetrug handeln, wenn durch die oben genannten Trading Tipps Versprechungen über die weitere Preissteigerung gemacht wurden (Wilms, o.D.). Diese Betrugsmasche funktioniert in der Regel nur bei kleineren Kryptowährungen, da dort die Preisveränderung auch schon bei wenigen Käufern hoch sein kann.

Eine weitere Betrugsform, welche sehr leicht durchzuführen war, ist der „Gewinnspiel-Scam", hierbei wurden ab 2017 Kommentare unter Twitter Beiträgen von berühmten Persönlichkeiten des Kryptobereichs geschrieben, die für ein Gewinnspiel warben. Um an dem

Gewinnspiel teilzunehmen, mussten die Nutzer eine Kryptowährung auf eine gewisse Wallet schicken. Diese Kommentare wirkten auf den ersten Blick echt, da sie von Twitter-Accounts geschrieben wurden, welche sich ähnlich wie der Twitter-Account der berühmten Persönlichkeit lasen. Die Gewinnspiele waren jedoch nicht echt und die gesendete Kryptowährung war verloren. Mittlerweile können die Ersteller eines Twitter-Beitrags einstellen, wer unter ihren Beiträgen schreiben kann, somit ist es schwerer für die Betrüger geworden (Pfeiffer et al., 2022, S. 19–20). Gewinnspiel-Scams können gemäß § 263 StGB als Betrug strafbar sein.

Eine weitere häufige Betrugsart ist der „Rug Pull". Bei diesem Betrug leiten die Betrüger die Opfer dazu, ihre Kryptowährung zu kaufen. Die Werbung dafür passiert regelmäßig über Soziale Medien. Diese Kryptowährung sieht auf den ersten Blick legitim aus und der Handel mit ihr funktioniert ebenfalls. Die Betrüger/Entwickler der Kryptowährung nehmen im Zuge des Betrugs allerdings die Investitionen der Opfer, die eigentlich für die weitere Entwicklung des Projekts gedacht war und beenden das Projekt. Die Opfer besitzen zwar noch die erworbene Kryptowährung und können weiter mit dieser Handeln, aber sie verliert kurze Zeit nach einem Rug Pull durch die Entwickler enorm an Wert. Somit liegt teilweise ein Totalverlust der Investition vor (Scharfman, 2023, S. 9). Bei einem Rug Pull könnte es sich je nach Umstand um einen Betrug gemäß § 263 StGB oder um einen Kapitalanlagebetrug gemäß § 264a StGB handeln (Wilms, o.D.).

Ein Betrug, der durch Dating Plattformen durchgeführt wird, ist der sogenannte „Crypto Romance Scam". Hierbei lernt das Opfer den Betrüger über Dating Plattformen kennen. Die Betrüger geben sich dabei oftmals als eine andere Person aus. Im Verlauf des Kennenlernens der beiden Personen überzeugt der Betrüger das Opfer, in Kryptowährungen zu investieren. Dafür sendet der Betrüger dem Opfer eine vermeintliche Webseite einer Krypto-Börse, bei der das Opfer anschließend Geld in Kryptowährungen investieren soll. Diese Internetseite ist allerdings eine Fälschung und wird von dem Betrüger kontrolliert. Das investierte Geld geht somit direkt an den Betrüger. Der Betrüger versucht anschließend, dass das Opfer immer mehr Geld investiert. Sobald das Opfer die Investition von der vermeintlichen Krypto-Börse abheben möchte, wird der Account gesperrt. Um den Account zu entsperren, soll das Opfer den Kundenservice kontaktieren. Der vermeintliche Kundenservice ist wieder der Betrüger. Der Kundenservice sagt nun, dass das Opfer mehr Geld investieren

soll, damit der Account entsperrt wird. Auf diese Weise können die Opfer um sehr viel Geld gebracht werden (Scharfman, 2023, S. 9–10). Bei einem Crypto Romance Scam könnte es sich ebenfalls je nach Umstand um einen Betrug gemäß § 263 StGB oder um einen Kapitalanlagebetrug gemäß § 264a StGB handeln (Wilms, o.D.).

4.3 Kryptowährungen als Lösegeld

Bei Ransomware handelt es sich um Schadprogramme. Sobald der Computer des Opfers mit solch einem Programm infiziert ist, verschlüsselt das Programm viele Daten auf dem Rechner. Nach der Zahlung eines Lösegeldes (engl. ransom), werden gemäß dem Betrüger, die Daten wieder entschlüsselt. Das Lösegeld wird oftmals in Form von Kryptowährung verlangt (Dreißigacker et al., 2020, S. 322).

Ransomware-Angriffe richten sich nicht nur gegen Privatpersonen, sondern vorwiegend gegen Unternehmen. Bei Unternehmen können diese Angriffe verheerende Folgen haben. Nachfolgende sind Beispiele genannt, bei denen Unternehmen Opfer von diesen Angriffen geworden sind. Colonial Pipeline ist der größte Bezinpipeline Betreiber der USA und wurde Opfer einer Ransomware, die zur Folge hatte, dass die Kraftstoffversorgung des Landes eingeschränkt war. Das Unternehmen zahlte den Hackern 4,4 Millionen US-Dollar Lösegeld. Das Uniklinikum Düsseldorf wurde ebenfalls Opfer einer Ransomware. Es gelang den Angreifern ca. dreißig Server des Uniklinikums zu verschlüsseln. Dies hatte zur Folge, dass das Klinikum die Notfallversorgung nicht mehr aufrechterhalten konnte und ca. eintausend Patienten mussten in umliegende Krankenhäuser transportiert werden. Dabei ist eine Notfallpatientin verstorben. Ein weiteres Beispiel ist das Kammergericht Berlin. Dort wurden mehr als fünfhundert Computer und über hundert Server infiziert. Das hatte zur Folge, dass das Kammergericht über Monate nicht über das Internet erreichbar war. Somit funktionierte die Kommunikation nur über Telefon, Fax und die Post. Es kann nicht nur Lösegeld für die Entschlüsselung verlangt werden, sondern auch Schweigegeld für das Unterlassen der Verbreitung von den gestohlenen Daten (Pohlmann, 2022, S. 2–3).

Die Ransomware kann auf viele verschiede Arten in die Netzwerke oder auf die Computer der Opfer gelangen. So kann die Infizierung über Phishing-E-Mails geschehen. Bei Phishing-E-Mails wird versucht, dass der Benutzer auf gewisse Links oder Anhänge klickt. Des Weiteren kann die Schadsoftware über Drive-By-Downloads von kompromittierten Webseiten geschehen. Dabei wird die Schadsoftware automatisch heruntergeladen, wenn eine solche

Website besucht wird. Bei Unternehmen kann auch das Remote-Desktop-Protokoll ausgenutzt werden. Dieses ist eigentlich dafür da, dass die IT-Abteilung eines Unternehmens aus der Ferne auf die Computer der Mitarbeiter zugreifen kann. Ist dieses Protokoll aber falsch eingestellt, können Angreifer ebenfalls auf die Computer zugreifen und Schadsoftware hochladen. Des Weiteren können Computer und Netzwerke auch über USB-Sticks oder ähnliche Datenträger infiziert werden (Bloomer, 2022, S. 47).

Gerade Privatpersonen können Glück haben und die genutzte Ransomware wurde in der Vergangenheit schon entschlüsselt. Somit können die verschlüsselten Daten wiederhergestellt werden. Auf der Webseite „bleib-virenfrei.de“ werden zurzeit 847 Ransomware-Varianten gelistet und viele von diesen wurden bereits entschlüsselt. Des Weiteren wird grundsätzlich von der Zahlung des Lösegelds abgeraten. Es ist nicht sicher, ob nach der Zahlung die Daten entschlüsselt werden. Weiter werden die Angreifer ermutigt, in Zukunft weitere Angriffe auszuführen (Bauer & Hifinger, 2023).

Kryptowährungen sind ein wesentlicher Bestandteil von Ransomware. Die Kernkonzepte von Kryptowährungen eignen sich sehr gut für solche illegalen Handlungen, da es auch für Strafverfolgungsbehörden schwer ist, die Klarnamen der Täter zu ermitteln. Die Blockchains der Kryptowährungen sind zwar transparent und das gezahlte Lösegeld kann von Wallet zu Wallet verfolgt werden, doch sobald es zu einer Krypto-Börse transferiert wird, kann es nur noch mit Hilfe dieser verfolgt werden. Weiter gibt es die CoinMixing-Dienste, welche ebenfalls die Herkunft von Kryptowährungen verschleiern können.

Im Falle von Ransomware Angriffen können viele Straftatbestände einschlägig sein. Wenn ein Täter eine E-Mail mit der Absicht versendet, dass der Computer des Opfers gesperrt wird, um anschließend Geld zu fordern, so könnte dies einen versuchten Computerbetrug gemäß § 263 a StGB i.V.m. § 263 Abs. 2 StGB darstellen. Weiter könnte es sich zusätzlich um eine Fälschung beweiserheblicher Daten gemäß §269 StGB handeln, wenn ein Name einer existierenden Firma oder Organisation missbraucht wird und somit der Eindruck bei dem Opfer entsteht, einen Anhang öffnen zu müssen. Sollte der Computer des Opfers infiziert werden, so könnte es sich gemäß § 303a StGB um eine Datenveränderung, beziehungsweise gemäß §303b StGB um eine Computersabotage handeln. Sollte das Opfer das Lösegeld zahlen, so könnte es sich um einen vollendeten Computerbetrug nach § 263a StGB handeln. Sollte das Opfer nicht zahlen, bleibt es bei den vorhergenannten Straftaten. Im

Falle einer Infizierung mit Ransomware durch eine inkriminierte Internetseite könnte es sich ebenfalls um eine Datenveränderung gemäß § 303a StGB, beziehungsweise um eine Computersabotage gemäß § 303b StGB handeln. Weiter könnte es sich in beiden Fällen zusätzlich um das Vorbereiten des Ausspähens und Abfangens von Daten gemäß § 202c StGB handeln und um eine Erpressung gemäß § 253 StGB, wenn mit einem empfindlichen Übel gedroht wird, damit Geld gezahlt wird (Büchel & Hirsch, 2014, S. 89–90).

4.4 Kryptowährungen und das Darknet

Das Darknet ist ein Teil des Internets, welcher nicht über einen Standard-Browser besucht werden kann und nicht von Suchmaschinen gefunden werden kann. Das Darknet sollte nicht mit dem Deep Web verwechselt werden. Das Deep Web ist der Teil des Internets, welcher ausschließlich nicht mit Suchmaschinen gefunden werden kann. Dies sind zum Beispiel Datenbanken oder andere zugangsgeschützte Bereiche. Somit ist das Darknet Teil des Deep Webs. Des Weiteren kann das Darknet nur über das Tor-Netzwerk besucht werden. Dazu wird zum Beispiel der Tor-Browser benötigt. Bei einem Standard-Browser gehen die Anfragen direkt zu dem Webserver der gewünschten Internetseite, werden dort bearbeitet und anschließend zurückgesendet. Bei dem Tor-Browser wird die Anfrage verschlüsselt über mehrere Knoten/Server gesendet, bis sie am Webserver der gewünschten Internetseite angekommen ist. Nur die Knoten, die direkt miteinander kommunizieren, kennen einander. Somit kann nur schwer nachvollzogen werden, von wo und von wem die Anfrage ursprünglich gesendet wurde. Mit dem Tor-Browser können auch normale Internetseiten anonym besucht werden. Doch eigentlich ist der Browser für Internetseiten gedacht, die auf „.onion“ enden und nicht mit normalen Browsern geöffnet werden können. Es gibt grundsätzlich zwei Gruppen, für die das Darknet interessant ist: Zum einen sind das Personen, welche eine anonyme Kommunikation benötigen. Dies sind zum Beispiel Journalisten in gewissen Staaten, welche um ihr Leben fürchten müssen, wenn sie sensible Information oder Daten öffentlich verbreiten. Zum anderen sind es Personen, die versuchen durch die Anonymität negative Konsequenzen von Strafverfolgungsbehörden zu entgehen. Im sichtbaren Bereich des Internets würde die Handlungen solcher Personen schnell zu Anzeigen und Strafen führen. Aus diesem Grund befinden sich im Darknet zahlreiche illegale Foren, Webshops und Handelsplattformen für Dienstleistungen und Waren. Es wird davon ausgegangen, dass im Jahr 2017 nur 37,5 % der Inhalte im Darknet legal sind. Der Rest ist somit

illegal. Im Darknet kann fast alles, was illegal ist, gekauft werden. Darunter Drogen, Waffen, diverse Urkunden, Auftragskiller, Uran oder auch Gift. Da es im Darknet keinen Käuferschutz oder ähnliches gibt, ist es fraglich wie viele dieser Angebote echt sind. Aus diesem Grund wird oftmals eine Art Empfehlungssystem genutzt. Neue Händler müssen dabei von aktiven Händlern als vertrauenswürdig eingestuft werden, damit sie Waren oder Dienstleistungen anbieten können. Im Darknet wird grundsätzlich mit einer der verschiedenen Kryptowährungen bezahlt (Eckermann, 2017). Kryptowährungen passen durch ihre Anonymität sehr gut mit dem Darknet zusammen. So können Kriminelle die Kryptowährung, wie oben beschrieben, Mixen lassen und sie anschließend auf eine Krypto-Börse senden und dort in eine Landeswährung umtauschen.

Im Darknet können viele Straftatbestände einschlägig sein. Darunter viele Straftaten des Strafgesetzbuches, des Waffengesetzes und auch des Betäubungsmittelgesetzes.

4.5 Gestohlene Kryptowährungen

Im Jahr 2022 wurden Kryptowährungen im Wert von 3,8 Milliarden US-Dollar gestohlen. Im Jahr 2021 waren es Kryptowährungen im Wert von 3,3 Milliarden US-Dollar und 2020 waren es lediglich 0,5 Milliarden US-Dollar (Chainalysis, 2023, S. 56). Der größte Teil der gestohlenen Kryptowährungen wird meistens über Hacking und Ausnutzen von Lücken in Smart Contracts erbeutet. Aus diesem Grund sind auch besonders oft DeFi-Projekte betroffen. 82,1 % von den gestohlenen Kryptowährungen im Jahr 2022 wurde von DeFi-Projekten erbeutet. Die gestohlenen Kryptowährungen von Privatpersonen haben im Jahr 2021 ca. 15 % der gesamten gestohlenen Kryptowährungen ausgemacht. Im Jahr 2022 waren es lediglich ca. 1 % (Chainalysis, 2023, S. 58). Sollten Lücken oder Hacking benutzt worden sein, um Kryptowährungen eines anderen zu erhalten, so kann es sich um einen Computerbetrug gemäß § 263a StGB handeln. Ein Diebstahl kommt bei Kryptowährungen nicht in Betracht, da Kryptowährungen keine Gegenstände im Sinne des Diebstahls sind.

Die Kriminellen bekommen unter anderem durch Phishing Zugang zu den Krypto-Vermögenswerten ihrer privaten Opfer. Hierbei versucht der Betrüger an die Zugangsdaten eines Online-Wallets oder an den Wiederherstellungs-Seed seiner Opfer zu bekommen. Die Opfer bekommen eine E-Mail oder eine Nachricht auf den Sozialen Medien mit einer gefälschten Internetseiten. Dort sollen die Opfer dann ihren Wiederherstellungs-Seed oder die Zugangsdaten zu dem Online-Wallet eingeben. Sollte ein Opfer dies machen, können die

Hacker frei über die Krypto-Vermögenswerte des Opfers verfügen (Kaspersky, o.D.). Somit sind auch hier die Sozialen Medien ein wichtiger Faktor für die Begehung krimineller Handlungen. Beim Phishing kann es sich um Fälschung von beweiserheblichen Daten gemäß § 269 StGB handeln, beziehungsweise um einen besonders schweren Fall der Fälschung von beweiserheblichen Daten gemäß § 269 Abs. 3 i.V.m. 267 Abs. 4 StGB (Kujus, 2023).

4.6 Betrügerische ICOs

Wie bereits erwähnt, gab es in der Vergangenheit einen regelrechten Hype um ICOs. Dies hat auch viele Betrüger angezogen. Diese Betrügereien funktionieren, wie die oben beschrieben Rug Pulls. Nur in diesem Fall gibt es keine funktionierende Kryptowährung, sondern nur das Versprechen, dass es nach dem ICO eine funktionierende Kryptowährung wird. Auch hier werden die Investitionen, die eigentlich für die Weiterentwicklung des Projekts gedacht sind, von den Betrügern entwendet.

Im Jahr 2017 waren ca. 78 % der ICOs betrügerische Handlungen und es konnte im weiteren Verlauf nicht mit ihnen gehandelt werden (Dowlat, 2018, S. 24). Somit verloren die Investoren ihre gesamte Investition.

Bei betrügerischen ICOs könnte es sich je nach Umstand um einen Betrug gemäß § 263 StGB oder um einen Kapitalanlagebetrug gemäß § 264a StGB handeln (Wilms, o.D.).

4.7 Betrügerische NFTs

Wie bei Kryptowährungen ist der Handelsmarkt bei NFTs weitestgehend unkontrolliert und unüberwacht. Es gibt zwar internationale Bemühungen Kryptowährungen und auch NFTs zu regulieren, doch zurzeit ist ein großer Bereich der Kryptowährungen unreguliert. Aus diesem Grund fällt es Kriminellen auch leicht NFT-Scams (engl. für Betrug) auszuführen. Jede Person, die das technische Verständnis über NTFs mitbringt, kann NFTs erschaffen. Diese NFTs können jedes Objekt abbilden, ohne dass der Ersteller im Besitz des Objekts ist. Weiter können NFTs zu einem beliebigen Preis auf den NFT-Markplätzen angeboten werden. (Wilms, o.D.). Es gibt Betrüger, die Kunstwerke, Lieder oder ähnliches von Künstlern als NFT erstellen und diese anschließend verkaufen. Des Weiteren können auch bei NFTs, wie weiter oben beschrieben, Rug Pulls oder Phishing-Attacken geschehen (Dörner & Müller, 2022).

Bei betrügerischen NFTs könnte es sich je nach Umstand um einen Betrug gemäß § 263 StGB oder um einen Kapitalanlagebetrug gemäß § 264a StGB handeln (Wilms, o.D.).

4.8 Kriminelle Handlungen im Metaverse

Es ist nur eine Frage der Zeit, bis Kriminelle auch das Metaverse für kriminelle Handlungen benutzen. Es könnte sich für Geldwäsche gut eignen. So können virtuelle Grundstücke, beziehungsweise Parzellen im Falle von Decentraland, von Kriminellen mit illegal erhaltenen Kryptowährungen gekauft werden. Mit diesen wird anschließend so lange gehandelt, bis die ursprüngliche illegale Finanzierung verschleiert worden ist. Im Anschluss werden die Gewinne als legitime Gewinne durch den Handel von NFTs deklariert (Annison, 2022, S. 18). Der Vorteil des Metaverses besteht darin, dass die Kriminellen auch ein hohes Volumen von Kryptowährungen zu virtuellen Grundstücken tauschen können, ohne dass sie einen Identifikationsprozess, wie zum Beispiel auf Krypto-Börsen durchlaufen müssen. Ein weiterer Vorteil ist, dass sie die illegal erhaltenen Kryptowährungen im weiteren Verlauf als Gewinne aus dem NFT-Handel deklarieren können und somit frei über die Kryptowährungen verfügen können. Somit können die Kryptowährungen anschließend auf Krypto-Börsen gesendet und in Landeswährungen umgetauscht werden.

4.9 Die 51 % Attacke

Diese Attacke kann durchgeführt werden, wenn sich in einem Proof-of-Work System Miner mit 51 % der Rechenleistung und böswilliger Absicht zusammentun. Zunächst wird eine parallele Blockchain der originalen Blockchain erschaffen. Bei dieser alternativen Blockchain senden sich die Kriminellen selbst Kryptowährung, somit wird ein neuer Block generiert. Als nächstes wiederholen sie die gerade genannte Sendung auf der originalen Blockchain, nur diesmal ist der Empfänger eine CEX. Auf dieser CEX tauschen sie die gesendete Kryptowährung in eine andere Kryptowährung und zahlen sich diese aus. Dieser Vorgang ist anschließend nicht reversibel. Nun beginnt der eigentliche Angriff. Die kriminellen Miner überschreiben nun die originale Blockchain mit der alternativen Blockchain. Diese alternative Blockchain ist durch die Rechenleistung (wahrscheinlich) länger als die originale Blockchain. Sollte das der Fall sein, wird sie vom übrigen Netzwerk übernommen, da immer die längste Blockchain genommen wird. Die anfängliche Sendung zu der CEX ist auf der neuen Blockchain nicht mehr verzeichnet. Auf diese Weise haben die Kriminellen einmal die versendete Kryptowährung in Form einer anderen Kryptowährung und die alte

Kryptowährung, da diese laut der neuen Blockchain nie versendet wurde. Sie haben somit den Wert ihrer Kryptowährungen verdoppelt. Unter Umständen kann solch ein Angriff auch bei Proof-of-Stake Systemen funktionieren (Gomzin, 2022, S. 92–93).

Ein solcher Angriff ist auf das Bitcoin-Netzwerk faktisch nicht möglich, beziehungsweise die Kosten sind zu hoch, so dass sich der Angriff nicht lohnen würde. Nichtdestotrotz können kleinere Kryptowährungen erfolgreich auf diese Weise angegriffen werden (Aras & Wenz, 2023).

4.10 Kryptowährungskriminalität und die Polizei

Cybercrime ist ein Kriminalitätsfeld, welches immer mehr Bedeutung gewinnt. Im Jahr 2021 stiegen Cybercrimes um 12 % zum Vorjahr an. Des Weiteren liegt die Aufklärungsquote mit 30 % weit unter der durchschnittlichen Aufklärungsquote (BKA, 2022).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem Leitfaden IT-Forensik ein Modell geschaffen, welche sich auf die Bearbeitung von Cybercrimedelikten übertragen lässt (BSI, 2021 nach Honekamp, 2019, S. 56). Zunächst werden sämtliche nützliche Informationen über einen Sachverhalt im Bereich Cybercrime zusammengetragen. Die Informationen stammen aus den polizeilichen Informationssystemen, aus der Akte und aus offenen Quellen, wie der ONSINT – Open Source Intelligence (Wehlte, 2016 nach Honekamp, 2019, S. 56). Weiter werden einzelne Maßnahmen, wie Durchsuchungen, Festnahmen, Sicherstellungen oder Beschlagnahmen vorbereitet (Honekamp, 2019, S. 56). Hierbei ist gerade bei Cybercrimestraftaten mit Bezug zu Kryptowährungen wichtig, dass auf Hardware-Wallets, Paper-Wallets oder Wiederherstellungs-Seeds geachtet wird. Weiter ist es erstrebenswert Computer im angeschalteten Zustand zu sichern, auf diese Weise kann gegebenenfalls auf offene Software-Wallets zugegriffen werden.

Die Verfolgung von Computerkriminalität erfordert von den Verfolgungsbehörden, dass ihr Personal gewisse Fähigkeiten und Kenntnisse in dem Bereich hat. So muss sichergestellt werden, dass das Personal Computerkriminalität erkennen und richtig aufnehmen kann, um keine Anhaltspunkte oder Beweise zu übersehen. Aus diesem Grund ist eine Grundqualifikation des Personals in der Fläche zur Bekämpfung von Computerkriminalität vonnöten. Des Weiteren muss es hochqualifiziertes Fachpersonal für die weitere Bearbeitung geben. Dies sind oftmals keine Polizeivollzugsbeamte, sondern Personen mit einer

entsprechenden (Fach-)Hochschulausbildung. Die Polizei Niedersachsen unterscheidet in ihrem Fortbildungskonzept zwischen den Ersteinschreitenden und den Verwaltungskräften Cybercrime. Die Ersteinschreitenden sollen „Phänomene von Cybercrime erkennen können sowie in die Lage versetzt werden, unaufschiebbare Feststellungen und Maßnahmen zur Aufklärung entsprechender Straftaten einzuleiten“. Die Verwaltungskräfte Cybercrime sollen „spezielle rechtliche, taktische, technische und kriminalistisch-kriminologische Kenntnisse zur Bearbeitung derartiger Ermittlungsverfahren erlangen und Handlungssicherheit bei der Bearbeitung von Ermittlungsverfahren im Zusammenhang Cybercrime“ erwerben (Herbst, 2017 nach Honekamp, 2019, S. 56–57). In Hamburg bekommen die Studierenden an der Akademie der Polizei Grundlagen der Informatik, der Betriebssysteme und der Netzwerktechnik vermittelt. Im weiteren Verlauf des Studiums werden bei der Schutz- und Kriminalpolizei in der Lehrveranstaltung „Computerkriminalität“ unterschiedliche Schwerpunkte gesetzt. Die Studierenden der Schutzpolizei erhalten eine Ersteinschreiterausbildung. Die Studierenden der Kriminalpolizei lernen zusätzlich die Grundsätze der digitalen Ermittlung. Die Bekämpfung von Computerkriminalität erfordert bundesländerübergreifende und auch internationale Kooperation (Honekamp, 2019, S. 57). Ein erster Grundstein der internationalen Zusammenarbeit in der Bekämpfung der Computerkriminalität wurde durch das Übereinkommen über Computerkriminalität gelegt (Europarat, 2001). Auf Basis dieses Übereinkommens erfolgt eine internationale Ausbildung zum Nordic Computer Forensic Investigator (NCFI). Diese Ausbildung findet an der Polizeihochschule in Oslo, Norwegen statt. Die Polizeihochschule in Oslo kooperiert mit ähnlichen Ausbildungseinrichtungen aus Schweden, Dänemark, Niedersachsen und Hamburg, um die Ausbildung durchzuführen (Herbst, 2017 nach Honekamp, 2019, S. 57). Mit solch einem Programm wird eine gemeinsame Basis für länderübergreifende Ermittlungen geschaffen. Auf diese Weise können Bitcoins oder IP-Adressen verfolgt, Händler im Darknet identifiziert und Botnetze bekämpft werden (Honekamp, 2019, S. 57).

In NRW wird die Fort- und Weiterbildung vom Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei NRW (LAFP NRW) geregelt. Dort können die Polizeivollzugsbeamten verschiedene Fortbildungen und Schulungen im Bereich der Cybercrime machen. Der Fortbildungsaufwand ist im Bereich der Cybercrime grundsätzlich sehr hoch, da sich die Technologie in diesem Bereich schnell weiterentwickelt. Weiter müssen sich die

Beamten aus diesem Grund regelmäßig weiterbilden. Die Fortbildungen für Polizeivollzugsbeamte, die einer Kreispolizeibehörde angehören, sind auf Sicherungs- und Ermittlungspersonal aufgeteilt (Kunze, 2022, S. 13). Somit wird auch hier die Ausbildung, beziehungsweise die Weiterbildung getrennt. Die Beamten des Wach- und Wechseldienstes werden als Sicherungspersonal ausgebildet und die Beamten der Kriminalpolizei als Ermittlungspersonal.

Zusammenfassend kann gesagt werden, dass die verschiedenen Polizeibehörden das Problem der Cyberkriminalität erkannt haben und dementsprechend ihr Personal ausgebildet wird. Weiter wurde erkannt, dass es Fachkräfte aus der privaten Wirtschaft bedarf und oftmals eine internationale Kooperation benötigt wird, um Cyberkriminalität zu bekämpfen. Nichtsdestotrotz dürfen die Polizeien in der Weiterbildung ihres Personals in diese Richtung nicht nachlassen. Gerade bei Kryptowährungen wird mit einem Anstieg an Nutzern in Deutschland gerechnet. Bis 2027 sollen ca. 23 Prozent der deutschen Bevölkerung Kryptowährungen besitzen. 2022 waren es noch 13 Prozent der deutschen Bevölkerung (Statista, o.D.). Somit wird wahrscheinlich auch die Kriminalität in diesem Bereich ansteigen und die Polizei benötigt dementsprechend mehr Personal.

5. Fazit

Kryptowährungen werden seit Jahren kontinuierlich beliebter und somit steigt auch die Anzahl der Nutzer. In der gleichen Geschwindigkeit steigt jedoch auch die Kriminalität in Zusammenhang mit Kryptowährungen. Die Finanzinstitute der einzelnen Länder arbeiten an Regulierungen, die die Kriminalität weiter eingrenzen soll. Zurzeit gibt es jedoch in jedem Bereich der Kryptowährungen Möglichkeiten, kriminelle Handlungen durchzuführen. Dies haben auch die Strafverfolgungsbehörden bemerkt und sich dementsprechend aufgestellt. Sie werden auch in Zukunft gefordert sein, sich den Gegebenheiten und immer neuen Technologien in dem Bereich anzupassen. Dies haben sie bis jetzt unter anderem durch internationale Zusammenarbeit und individueller Fort- und Weiterbildung geschafft. Weiter sind Kryptowährungen noch nicht massentauglich, da es einen hohen Lernaufwand benötigt, um sich im Kryptobereich zurechtzufinden. Gerade Krypto-Einsteiger lernen oftmals die Gegebenheiten von Kryptowährungen durch Verlust ihrer Investition kennen. Dies kann durch die teilweise extreme Volatilität von Kryptowährungen in Kombination mit

Unerfahrenheit, aber auch durch die zahlreichen Betrügereien geschehen. Ein weiterer nicht zu verkennender Punkt ist, dass Kryptowährungen als Bezahlmittel für Ransomware-Angriffe und für das Darknet benutzt werden. Hierfür und für andere kriminelle Handlungen eignen sie sich aufgrund ihrer Grundideen besonders gut. Nichtsdestotrotz haben Kryptowährungen ihre Daseinsberechtigung. Sie ermöglichen Dinge, die vor ihnen nur begrenzt möglich, beziehungsweise schwer umzusetzen waren. So können NFTs zum Beispiel für Einzigartigkeit in der digitalen Welt sorgen. Weiter können Menschen in Form von DAOs an Unternehmen und Projekten über den ganzen Globus verteilt arbeiten. Dabei wird gleichzeitig der Betrug innerhalb eines solchen Projekts durch Smart Contracts minimiert. Kryptowährungen können mit Stablecoins eine gute Sicherheit vor Inflation einer Landeswährung bieten. Gerade Smart Contracts bieten theoretisch unbegrenzt viele Möglichkeiten Kryptowährungen einzusetzen. So können Smart Contracts viele Vorgänge im Kryptobereich vereinfachen und zu einer leichteren Massenadaption führen. Zusammenfassend kann gesagt werden, dass Kryptowährungen nicht zu unterschätzende Erfindungen sind, welche vermutlich in Zukunft eine noch größere Rolle auf der Welt einnehmen werden. Zudem machen Kriminelle nur einen kleinen Teil des kompletten Handelsvolumens aus und sind somit auch zahlenmäßig eine absolute Minderheit im Kryptobereich. Außerdem wird kontinuierlich an Regulierungen und Gesetzen gearbeitet, um kriminelle Handlungen im Kryptobereich einzudämmen. Aufgrund der genannten Gründe hält der Autor dieser Arbeit Kryptowährungen für eine Zukunftstechnologie, die dennoch als kriminelles Werkzeug missbraucht werden kann. Die Vorteile von Kryptowährungen überwiegen dennoch für ihn.

Quellenverzeichnis

Annison, T. (2022). *Elliptic Metaverse Report 2022: The Future of Financial Crime in the Metaverse.* Elliptic. https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf

Aras, B. & Wenz, D. (2023). *51 Prozent Attacke: Wie gefährlich ist sie für Bitcoin?* https://bitcoin-2go.de/51-prozent-attacke-bitcoin/

Bauer, F. & Hifinger, R. (2023). *Ransomware-Liste inkl. Decryptor (zum Entschlüsseln)*. https://www.bleib-virenfrei.de/it-sicherheit/ransomware/liste/

Bendel, O. (2021). *Kryptowährung: Definition: Was ist "Kryptowährung"?* https://wirtschaftslexikon.gabler.de/definition/kryptowaehrung-54160/version-384589

Bendel, O. (2023). *Metaverse: Definition: Was ist "Metaverse"?* https://wirtschaftslexikon.gabler.de/definition/metaverse-123520/version-388557

Binance (Hrsg.). (2021). *What Is KYC (Know Your Customer)?* https://academy.binance.com/en/articles/what-is-kyc-know-your-customer

BKA (Hrsg.). (2022). *Bundeslagebild Cybercrime 2021*. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.pdf?__blob=publicationFile&v=6

BKA (Hrsg.). (2023). *BKA schaltet weltweit größten Geldwäschedienst im Darknet ab*. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2023/Presse2023/230314_Geldwaesche_Darknet.html

Bloomer, T. (2022). 1.1 RANSOMWARE | Ransomware automatisch abwehren. *Digitale Welt*, *6*(1), 47–48. https://doi.org/10.1007/s42354-022-0435-z

Bocksch, R. (2022). *Non-Fungible Tokens: Starke Marktentwicklung*. https://de.statista.com/infografik/24807/kennzahlen-der-nft-industrie/

Büchel, M. & Hirsch, P. (2014). *Internetkriminalität: Phänomene - Ermittlungshilfen - Prävention*. *Grundlagen - Die Schriftenreihe der "Kriminalistik": [48]*. Kriminalistik.

Bundesanstalt für Finanzdienstleistungsaufsicht (Hrsg.). (2017). *Initial Coin Offerings: Hohe Risiken für Verbraucher*. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html

Chainalysis (Hrsg.). (2023). *The 2023 Crypto Crime Report*. https://go.chainalysis.com/2023-crypto-crime-report.html

Coinmarketcap (Hrsg.). (2023a). *Die besten Spot-Börsen für Kryptowährung*. https://coinmarketcap.com/de/rankings/exchanges/

Coinmarketcap (Hrsg.). (2023b). *Bitcoin*. https://coinmarketcap.com/de/currencies/bitcoin/

Coinmarketcap (Hrsg.). (2023c). *Terra Classic*. https://coinmarketcap.com/de/currencies/terra-luna/

Coinmarketcap (Hrsg.). (2023d). *Top 100 Kryptowährungen nach Börsenwert*. https://coinmarketcap.com/de/

Coinmarketcap (Hrsg.). (2023e). *Top-Metaverse-Tokens nach Marktkapitalisierung*. https://coinmarketcap.com/de/view/metaverse/

Coinmarketcap (Hrsg.). (2023f). *Uniswap*. https://coinmarketcap.com/de/currencies/uniswap/

Dash, A. (2021). *NFTs Weren't Supposed to End Like This.* The Atlantic. https://www.theatlantic.com/ideas/archive/2021/04/nfts-werent-supposed-end-like/618488/

Decentraland (Hrsg.). (2023). *Introduction*. https://docs.decentraland.org/player/general/introduction/

Dörner, A. & Müller, M. (22. Juni 2022). Die dunkle Seite der NFT-Welt. *Handelsblatt,* 2022(Nr. 118).

Dowlat, S. (2018). *Cryptoasset market coverage initiation: network creation*. https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ

Dreißigacker, A., Skarczinski, B. von, Bergmann, M. C. & Wollinger, G. R. (2020). Cyberangriffe gegen private Internetnutzer*innen. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie* (S. 319–344). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28507-4_13

Eckermann, I. M. (2017). *Was ist eigentlich das Darknet?* https://www.gdata.de/ratgeber/was-ist-eigentlich-das-darknet

Ethereum (Hrsg.). (o.D.a). *Dezentrale autonome Organisationen (DAO)*. https://ethereum.org/de/dao/

Ethereum (Hrsg.). (o.D.b). *PROOF-OF-STAKE (POS)*. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Europarat (Hrsg.). (2001). *Übereinkommen über Computerkriminalität*. https://rm.coe.int/168008157a

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Hrsg.). (2017). *Blockchain und Smart Contracts – Technologien, Forschungsfragen und Anwendungen*. https://www.fraunhofer.de/content/dam/zv/de/forschung/artikel/2017/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts_v151.pdf

Gomzin, S. (2022). *Crypto Basics*. Apress. https://doi.org/10.1007/978-1-4842-8321-9

Grigo, J., Hansen, P., Patz, A. & Wachter, V. von. (2020). *Decentralized Finance (DeFi) – A new Fintech Revolution? The Blockchain Trend explained*. https://www.bitkom.org/sites/main/files/2020-07/200729_whitepaper_decentralized-finance.pdf

Hellwig, D., Karlic, G. & Huchzermeier, A. (2021). *Entwickeln Sie Ihre eigene Blockchain*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-62966-6

Honekamp, W. (2019). Cybercrime: Aktuelle Erscheinungsformen und deren Bekämpfung. In H.-J. Lange, T. Model & M. Wendekamm (Hrsg.), *Forum für Verwaltungs- und Polizeiwissenschaft. Zukunft der Polizei* (S. 47–59). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22591-9_4

Hönig, M. (2020). *ICO und Kryptowährungen*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-27688-1

Izzo-Wagner, A. & Siering, L. M. (2020). *Kryptowährungen und geldwäscherechtliche Regulierung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-29981-1

Kaspersky (Hrsg.). (o.D.). *Gängige Betrugsmaschen mit Kryptowährungen und wie Sie sich davor schützen*. https://www.kaspersky.de/resource-center/definitions/cryptocurrency-scams

Kaufmann, H. (2021). *Geldwäscheverdacht im Zusammenhang mit Kryptowährung*. https://www.anwalt.de/rechtstipps/geldwaescheverdacht-im-zusammenhang-mit-kryptowaehrung-189293.html

Költzsch. (2022). *Terra-Luna-Gründer nach Milliarden-Crash in Serbien*. https://www.golem.de/news/kryptowaehrung-terra-luna-gruender-nach-milliarden-crash-in-serbien-2212-170431.html

Kujus, T. (2023). *Fälschung beweiserheblicher Daten*. https://kujus-strafverteidigung.de/strafrechts-abc/faelschung-beweiserheblicher-daten/

Kunze, D. (2022). Bearbeitung von Cyberangriffen unter Berücksichtigung der polizeilichen Vorschriftenlage und fachliche, technische und rechtliche Determinanten erfolgreicher Cyberoperationen gegen angreifende Infrastrukturen und Tätergruppierungen (Hack Back). In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie* (S. 1–32). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-35450-3_22-1

Kurt, L. & Kurt, D. (2022). *Digitale Assets & Tokenisierung*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-37562-1

Mathys, M. & Gimeno, R. (2021). Integration von Kryptowährungen in das Angebot von Regionalbanken. In J. Schellinger, K. O. Tokarski & I. Kissling-Näf (Hrsg.), *Digital Business: Analysen und Handlungsfelder in der Praxis.* Springer Fachmedien Wiesbaden.

Moreland, K. (2022). *Der Unterschied zwischen Coins und Tokens*. https://www.ledger.com/de/academy/crypto/der-unterschied-zwischen-coins-und-tokens

OpenSea (Hrsg.). (o.D.). *Building an open digital economy*. https://opensea.io/about

Pfeiffer, A., Wernbacher, T., Koenig, N., Denk, N., Vella, V. & Dingli, A. (2022). Blockchains, Kryptowährungen, Utility-Token, NFTs und das Metaverse: Eine Einführung für den Bereich der Cyberkriminologie. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie* (S. 1–36). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-35450-3_19-1

Pohlmann, N. (2022). Ransomware. Eine aktuelle und stetig steigende Bedrohung. *Digitale Welt*, *6*(1), 2–3. https://doi.org/10.1007/s42354-022-0423-3

Pravin, V. (2022). Blockchain und NFTs: Wie kann Betrug verhindert werden? *Digitale Welt*, *6*(3), 12–13. https://doi.org/10.1007/s42354-022-0508-z

Q.ai. (2022). *What Really Happened To LUNA Crypto?* https://www.forbes.com/sites/qai/2022/09/20/what-really-happened-to-luna-crypto/?sh=199b7f994ff1

Rosenberger, P. (2018). *Bitcoin und Blockchain*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-56088-4

Scharfman, J. (2023). *The Cryptocurrency and Digital Asset Fraud Casebook*. Springer International Publishing. https://doi.org/10.1007/978-3-031-23679-2

Statista (Hrsg.). (o.D.). *Cryptocurrencies - Deutschland*. https://de.statista.com/outlook/dmo/fintech/digital-assets/cryptocurrencies/deutschland

Unijoin (Hrsg.). (o.D.). *Häufig gestellte Fragen*. https://unijoin.io/de/faq

Uniswap (Hrsg.). (o.D.). *Governance: The Uniswap Protocol is a public good owned and governed by UNI token holders*. https://uniswap.org/governance

Wilms, A. (o.D.). *NFT Scam*. https://kanzlei-herfurtner.de/betrug/nft-scam/

HSPVNRW

Hochschule für Polizei und öffentliche Verwaltung
Nordrhein-Westfalen

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig und ohne fremde Hilfe angefertigt habe und außer den im Quellen- und Literaturverzeichnis sowie in den Anmerkungen genannten Hilfsmitteln keine weiteren benutzt habe. Alle Stellen der Arbeit, die anderen Werken dem Wortlaut oder Sinn nach entnommen sind, habe ich unter Angabe der Quelle als Entlehnung kenntlich gemacht. Dies trifft insbesondere auch auf Informationen aus dem Internet zu.

Gleichzeitig erkläre ich, dass weder diese Arbeit – in dieser oder einer inhaltlich äquivalenten Form – noch Teile daraus von mir oder einer anderen Person als Studienleistung an anderer Stelle vorgelegt oder veröffentlicht wurde. Mir ist insofern bekannt, dass es sich bei der Abgabe eines Plagiats um ein schweres akademisches Fehlverhalten handelt.

Der Umfang der Arbeit (Haupttext inkl. Fußnoten, ohne Deckblatt, Inhaltsübersicht, Verzeichnisse etc.) beträgt insgesamt

9474 Wörter.

Zutreffendes bitte ankreuzen:

☒ Ich versichere, dass ich bei der Erstellung der Arbeit keine Quellen verwendet habe, die als „Verschlusssache – Nur für den Dienstgebrauch“ eingestuft sind.

☐ Ich habe bei der Erstellung der Arbeit Quellen verwendet, die als "Verschlusssache – Nur für den Dienstgebrauch" eingestuft sind. Mir ist bekannt, dass meine Arbeit daher ebenfalls als "Verschlusssache – Nur für den Dienstgebrauch" einzustufen ist. Ich verpflichte mich ausdrücklich, die Arbeit verschlossen aufzubewahren und unbefugten Personen nicht zugänglich zu machen. Mir ist bekannt, dass eine Veröffentlichung der Arbeit ausgeschlossen ist und die Arbeit bei der Einschreibung in einer anderen Hochschule nicht vorgelegt werden kann.

Name, Vorname: Mohr, Cedrik
Ort, Datum: Herne, 08.05.2023
Unterschrift: C. Mohr