

Rainer Gievers

Das Praxisbuch Kryptowährungen für Einsteiger

Ausgabe 2022/23

www.das-praxisbuch.de

Vorwort

Der Finanzmarkt wird staatlich streng reguliert, was auch kein Wunder ist, wenn man bedenkt, was alles davon abhängt: Egal, ob Sie beim Supermarkt bezahlen, einen Kredit aufnehmen oder Ihren Lohn vom Arbeitgeber erhalten, überall sind Banken und das Geldsystem im Spiel.

Umso erstaunlicher ist es, dass nur eine Handvoll Kryptografen und Programmierer mit dem Bitcoin eine Digitalwährung aus der Taufe gehoben haben, die seit über 10 Jahren vollkommen unabhängig von staatlichen Institutionen funktioniert. Inzwischen legen auch Börseninvestoren und Unternehmen einen Teil ihrer Gelder in Bitcoin an.

Während Bitcoin sich zunehmend als Wertspeicher und Alternative zu Gold etabliert, haben weitergedachte Digitalwährungen wie Ethereum sogar Eingang in Industrie und Handel als Kontroll- und Abwicklungssystem gefunden.

Dieses Buch erläutert zunächst die Bedeutung und Funktionsweise von Bitcoin. Danach erfahren Sie, wie man direkt oder indirekt in die Digitalwährung investiert. Auch die steuerlichen Aspekte kommen nicht zu kurz.

Bitte beachten Sie, dass sich einige Beschreibungen in diesem Buch wiederholen, denn das Buch sind so aufgebaut, dass jedes Kapitel in sich abgeschlossen ist.

Falls Sie im Buch irgendwo einen Fehler entdecken oder eine Frage zum Inhalt haben, schicken Sie bitte eine E-Mail an info@das-praxisbuch.de.

Rainer Gievers, 04.02.2022

1. Auflage, Februar 2022

1. Inhaltsverzeichnis

2. Was sind Bitcoin?	7
2.1 Grundlagen	7
2.2 Das Wallet	10
2.3 Fachbegriffe	10
2.4 Illegal eingesetzte Kryptowährungen	11
2.5 NFT	11
2.6 DeFi	14
2.6.1 Gefahren beim DeFi	14
3. Kryptobörsen	16
3.1 Kryptobörsen im Überblick	17
3.2 Arbitrage-Geschäfte	18
3.3 Staking	20
3.3.1 Vor- und Nachteile des Stakings für Anleger	20
4. Krypto-Finanzprodukte	22
4.1 CFD	22
4.2 ETC und ETN	23
5. Besteuerung von Kryptowährungen	24
5.1 Privatanleger	24
5.1.1 Kauf von Waren und Dienstleistungen	25
5.1.2 Probleme mit Coins auf Kryptobörsen	25
5.2 Steuerberechnung durchführen	26
5.2.1 FIFO-Methode	28
5.3 Gewerblicher Kryptohandel	29
5.4 Steuerreporting durch externe Dienstleister	29
5.4.1 Steuerermittlung mit Accounting	30
5.4.1.a Manuelle Transaktionenerfassung	31
5.4.1.b Steuerberechnung	37
5.4.1.c Direktverbindung mit Coinbase	40
6. Wallets	47
6.1 Online-Wallet	47
6.1.1 Bison App	47
6.2 Coinbase-Wallet	48
6.3 Software-Wallets	49
6.4 Paper-Wallet	50
6.5 Hardware-Wallet	53
7. Exodus-Multi-Wallet	57
7.1 Installation und Einrichtung	57
7.2 Benutzeroberfläche	60
7.3 Exodus-Wallet-Software auf dem Handy	62
7.3.1 Installation	62
7.3.2 Vorhandenes Exodus-Wallet übernehmen	64
7.3.3 Erste Einrichtung	66
7.3.4 Benutzeroberfläche	70
8. Kryptowährungen im Überblick	73
8.1 Bitcoin	73
8.1.1 Energieverbrauch	73
8.1.2 Transaktionskosten und Abwicklungsdauer	76
8.1.3 Was ist Bitcoin wert?	77
8.1.3.a Stock-to-Flow-Modell	78
8.1.4 Risiken	80
8.2 Bitcoin Cash und Bitcoin SV	80
8.3 Litecoin	81
8.4 Ripple	81
8.5 Ethereum	82

8.5.1	Andere Kryptowährungen auf der Ethereum-Blockchain.....	82
8.5.2	Umstellung auf Proof-of-Stake.....	83
8.6	Weitere Digitalwährungen.....	83
8.6.1	Stablecoins.....	84
8.6.2	Shitcoins.....	85
9.	Bison App.....	87
9.1	Der erste Kauf.....	89
9.2	Über Kurse informieren.....	91
9.3	Echtgeldhandel.....	94
9.4	Gewinnachweis.....	95
10.	Coinbase.....	97
10.1	Erste Schritte.....	97
10.2	An- und Abmelden.....	103
10.3	Fiat-Geld einzahlen.....	105
10.3.1	Bankkonto ändern.....	106
10.4	Fiat-Geld auszahlen.....	108
10.5	Handeln.....	109
10.5.1	Kryptokauf.....	110
10.5.2	Kryptoverkauf.....	112
10.5.3	Coinbase-Zinsen deaktivieren.....	113
10.6	Coinbase Pro.....	114
10.6.1	Kauf auf Coinbase Pro.....	115
10.6.2	Coins von Coinbase Pro nach Coinbase transferieren.....	119
10.7	Kennenlernen und verdienen.....	120
10.8	Watchlist.....	121
10.9	Coinbase auf dem Handy.....	122
11.	Tipps und Tricks.....	125
11.1	Kontostand.....	125
11.2	Bitcoin vom Paper-Wallet entnehmen.....	126
11.3	Wert eines Bitcoin-Paper-Wallets ermitteln.....	128
11.4	Bitcoin-Wale.....	129
11.5	Sicherer Umgang mit Kryptowährungen.....	129
11.6	Nachrichtenseiten zu Kryptowährungen.....	130
11.7	Betrugsversuche auf YouTube.....	130
11.8	Kryptowährungen handeln ohne KYC.....	131
12.	Handelsstrategien.....	134
12.1	Moderne Portfoliotheorie.....	135
12.2	HODL.....	136
12.3	Durchschnittsmethode.....	136
12.3.1	Sparplan mit Coinbase.....	137
12.3.2	Sparplan mit der Bison App.....	139
12.4	Kaufen, wenn unterbewertet.....	141
12.5	Aktives Handeln.....	142
12.6	Automatisiertes Handeln.....	144
12.7	Weitere Handelstipps.....	146
13.	Stichwortverzeichnis.....	147
	Weitere Bücher des Autors.....	149

Hinweis

Die Informationen in diesem Buch wurden mit größter Sorgfalt erarbeitet und zusammengestellt. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Verlag und Autor übernehmen daher keine juristische Verantwortung oder irgendeine Haftung für eventuell verbliebene Fehler oder deren Folgen.

Die in diesem Buch dargestellten Inhalte dienen ausschließlich der Information und stellen keine Kauf- bzw. Verkaufsempfehlungen dar. Sie sind weder explizit noch implizit als Zusicherung einer bestimmten Kursentwicklung der genannten Finanzinstrumente oder als Handlungsaufforderung zu verstehen. Der Erwerb von Wertpapieren oder Kryptowährungen birgt Risiken, die zum Totalverlust des eingesetzten Kapitals führen können. Die Informationen ersetzen keine, auf die individuellen Bedürfnisse ausgerichtete, fachkundige Anlageberatung. Eine Haftung oder Garantie für die Aktualität, Richtigkeit, Angemessenheit und Vollständigkeit der zur Verfügung gestellten Informationen sowie für Vermögensschäden wird weder ausdrücklich noch stillschweigend übernommen.

Alle erwähnten Warennamen und Bezeichnungen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen.

Alle Rechte vorbehalten. Das Werk einschließlich aller Teile ist urheberrechtlich geschützt. Kein Teil darf ohne schriftliche Genehmigung durch den Autor Rainer Gievers, Borgentreich, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Copyright © 2022 Rainer Gievers, D-34434 Borgentreich

ISBN: 978-3-96469-184-2

2. Was sind Bitcoin?

In diesem Kapitel stellen wir das Konzept der Kryptowährung Bitcoin genauer vor.

2.1 Grundlagen

Hinter der Entwicklung der ersten erfolgreichen Kryptowährung Bitcoin steckt Misstrauen gegenüber den traditionellen Bankinstitutionen. Der Bitcoin-Erfinder Satoshi Nakamoto schrieb in einem Diskussionsforum:

»Das Kernproblem konventioneller Währungen ist das Ausmaß an Vertrauen, das nötig ist, damit sie funktionieren. Der Zentralbank muss vertraut werden, dass sie die Währung nicht entwertet, doch die Geschichte des Fiatgeldes ist voll von Verrat an diesem Vertrauen. Banken muss vertraut werden, dass sie unser Geld aufbewahren und es elektronisch transferieren, doch sie verleihen es in Wellen von Kreditblasen mit einem kleinen Bruchteil an Deckung. Wir müssen den Banken unsere Privatsphäre anvertrauen, vertrauen, dass sie Identitätsdieben nicht die Möglichkeit geben, unsere Konten leerzuräumen. Ihre massiven Zusatzkosten machen Micropayments unmöglich.«¹

Schon vor Satoshi Nakamoto haben sich Entwickler Gedanken über eine dezentrale Währung gemacht, sind dabei aber immer am Aspekt der Vertrauenswürdigkeit und Praktikabilität gescheitert. »Harte« Währungen wie Euro und US-Dollar genießen Vertrauen, weil dahinter die Zentralbanken mit ihrer Autorität stehen. Man spricht deshalb auch vom **Fiat-Geld** (Fiat = lateinisch »Es werde«), das im Gegensatz zu Gold- und Silbermünzen keinen inneren Wert hat, sondern allein durch die Akzeptanz der Handelspartner Akzeptanz genießt².

Eine Digitalwährung muss ebenfalls Vertrauen genießen, sonst wird sie niemals als Zahlungsmittel oder Anlageobjekt von der breiten Bevölkerung akzeptiert. Gelöst wurde das Vertrauensproblem mit der sogenannten **Blockchain** (engl. Blockkette), eine beliebig erweiterbare Liste von Datenblöcken. Jeder enthaltene Datenblock enthält einen kryptographisch sicheren Hash (verschlüsselte Prüfsumme) des vorherigen Datenblocks, sowie Transaktionsdaten und Zeitstempel³. Dadurch fallen nachträgliche Manipulationen an den Datenblöcken auf und können verworfen werden. Die Nutzer der Blockchain können also der Blockchain vertrauen.

Die Verwaltung der Blockchain wurde nicht einer zentralen Stelle anvertraut. Stattdessen kommt die Technik des Distributed-**Ledger** (engl. verteiltes Hauptbuch) zum Einsatz. Der Ledger enthält mit der Blockchain alle jemals vorgenommenen Transaktionen und hat deshalb inzwischen eine Größe von 321 Gigabyte⁴ (Stand 02/2021). Lokal vorgehalten wird dieser Distributed-Ledger beispielsweise von allen Parteien, die Transaktionen in der Blockchain bestätigen oder auslesen.

Wie bereits erwähnt, gibt es beim Bitcoin keine zentrale Autorität. Stattdessen wird im Konsens gearbeitet: Die Mehrheit der beteiligten Bitcoin-Netzwerkteilnehmer muss sich regelmäßig auf die Regeln zur Gültigkeit und Bearbeitung von Transaktionen in der Blockchain einigen. Auch eine Transaktion selbst wird erst in die Blockchain aufgenommen, wenn die Mehrheit der Bitcoin-Netzwerkteilnehmer, auch als **Nodes** (engl. Knoten) bezeichnet, zustimmt. Diese Validierung wird als **Mining** (engl. Schürfen) bezeichnet.

Bitcoin ist eine digitale Währung, die eine Internetverbindung voraussetzt. Es wäre Ihnen also nicht ohne weiteres möglich, »offline« einem Freund einfach Bitcoin auszuhändigen.

1 Zitiert aus <https://de.wikipedia.org/wiki/Bitcoin#Geschichte>

2 <https://de.wikipedia.org/wiki/Fiatgeld>


3 <https://de.wikipedia.org/wiki/Blockchain>

4 <https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/>

Krypto-Crash: Deutsche Abkühlung bei Bitcoin, Ether, Binance Coin und anderen

Pro News Wissen Themen Pioneers Jobs Firmen Events Shop Anmelden

🏠 Pocket Facebook Twitter WhatsApp E-Mail

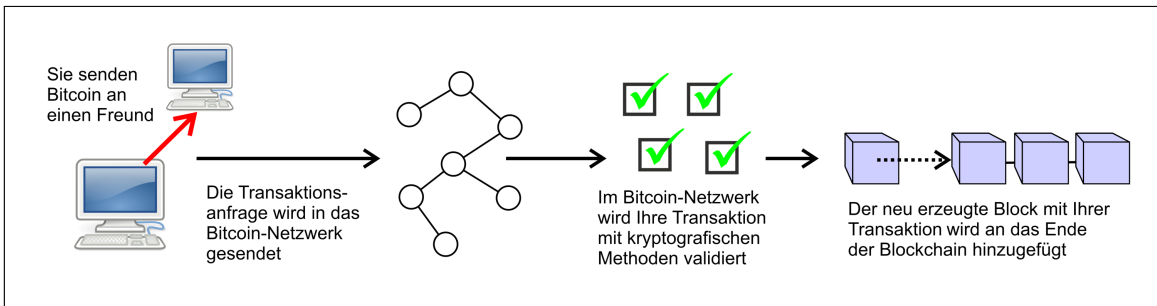


Dieter Petereit
Technikjournalist seit den Neunzigern | Dr. Web a.D.

Verwandte Themen

Bitcoin Elon Musk
Ethereum Uber

Die Medien illustrieren gerne Meldungen über Kryptowährungen mit »Bitcoin-Münzen«. Diese haben aber natürlich nur einen Materialwert und mit dem eigentlichen Zahlungsverkehr über die Blockchain nichts zu tun.

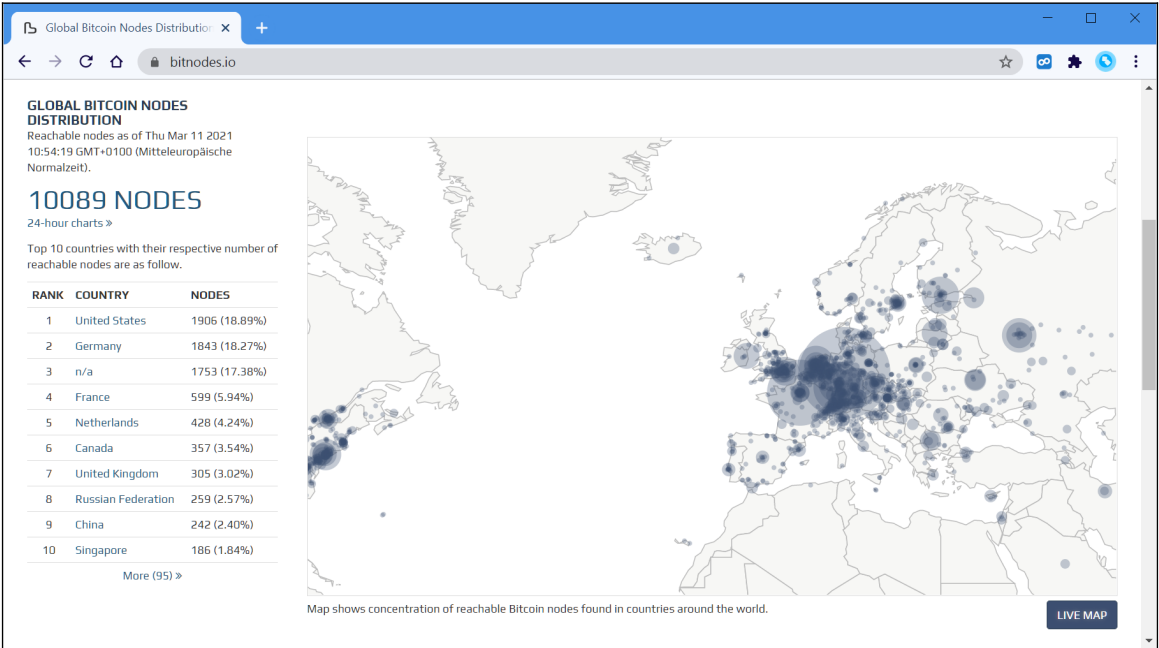


Stark vereinfachter schematischer Ablauf einer Bitcoin-Transaktion⁵

Da die Blockchain – vereinfacht gesagt – von jedem Node vorgehalten wird und neue Blöcke nur mit Zustimmung einer Node-Mehrheit von 51 Prozent in der Blockchain landen, ist das System sehr sicher.

Beim Bitcoin gibt es inzwischen mehr als 10.000 Nodes, deren Betreiber am reibungslosen Fortbestand der Blockchain interessiert sind. Es ist deshalb praktisch ausgeschlossen, dass sich jemals eine Mehrheit (über 51 Prozent) der Nodes für destruktive Änderungen an der Blockchain zusammenschließt.

⁵ Quelle Computersymbol: Gnome Project (www.gnome.org)



Die Website *bitnodes.io* listet für das Bitcoin-Netzwerk inzwischen mehr als 10.000 Nodes auf.

Neue Bitcoin entstehen beiläufig als Bezahlung für die Miner bei der Authentifizierung von Blockchain-Transaktionen als Blockprämie. Der Bitcoin-Algorithmus lässt maximal die Erzeugung von **21 Mio. Bitcoin** zu, wovon inzwischen 19 Mio. (Stand: 03/2021) bereits gewonnen wurden. Sobald alle Bitcoin »geschürft« sind – was noch 20 Jahre dauern kann – muss die Bezahlung der Miner geändert werden. Sie erhalten dann anstelle der Blockprämie eine Transaktionsgebühr, die von den Bitcoin-Nutzern erhoben wird.



Sie möchten wissen, wieviele Bitcoin aktuell im Umlauf sind? Dann hilft Ihnen die Website Buy Bitcoin Worldwide (*www.buybitcoinworldwide.com*) weiter.

2.2 Das Wallet

Damit Sie mit Bitcoin handeln können, benötigen Sie eine digitale Brieftasche, auf gut Englisch, die **Wallet**. Diese besteht aus einem **Private Key** (engl. privater Schlüssel) und **Public Key** (engl. öffentlicher Schlüssel). Der Public Key funktioniert wie eine IBAN-Kontonummer und kann beispielsweise so aussehen:

xJuw554yStgQa8Pszb5cQyERhDD2fL497F

Genau genommen verweist der **Public Key** auf eine Adresse im Blockchain, wo der Bitcoin-Betrag, den Sie besitzen, hinterlegt ist. In diesem Buch bezeichnen wir den Public Key als **Wallet-Adresse**. Andere Bitcoin-Besitzer, denen die Wallet-Adresse bekannt ist, können darauf Bitcoin »überweisen«.

Der **Private Key** besteht aus 51 Zeichen, die per Zufallsgenerator jeder Wallet zugeordnet werden. Um bei der Banking-Analogie zu bleiben, autorisiert der Private-Key wie eine PIN den Bitcoin-Transfer zu einer anderen Wallet. Der Private Key darf niemals an Dritte weitergegeben werden, weil andere sonst Zugriff auf seine Wallet erhalten. Damit wären eventuell auch die enthaltenen Bitcoin futsch!

Für die Aufbewahrung der Wallet gibt es verschiedene Möglichkeiten:

- Handy-App oder Desktop-PC-Anwendung
- Papieraufzeichnung
- Hardware-Wallet
- Online-Wallet

Sie dürfen beliebig viele Public-Keys und damit Wallet-Adressen erzeugen und nutzen. Das ist praktisch, um beispielsweise Bitcoin in kleiner Menge in einer Handy-App vorzuhalten und den Rest in einer sicheren Hardware-Wallet.

Im Kapitel 6 *Wallets* stellen wir einige Wallets genauer vor.

Für jede Digitalwährung ist eine Wallet nötig. Falls Sie neben Bitcoin zum Beispiel mit Bitcoin Cash handeln, benötigen Sie dafür ebenfalls eine eigene Wallet.

2.3 Fachbegriffe

Der Einfachheit halber greifen Krypto-Nutzer gerne auf Fachbegriffe aus dem Bankbereich zurück. Auch in diesem Buch verwenden wir statt »**Transfer** eines Werts von der Wallet-Adresse (Public Key)« einfach »**Überweisung**«.

Mit »**Coin**« (engl. Münze) sind meistens ausschließlich Bitcoin gemeint: »Ich überweise dir Coins«. **Altcoins** (Abk. alternative Coins) bezeichnet dagegen alle nach Bitcoin entstandenen Digitalwährungen.

Stablecoin (engl. Stabile Münze) sind fest mit einer nationalen Währung oder einem Währungskorb verknüpft, funktionieren aber ansonsten wie Kryptowährungen. Bekanntester Stablecoin ist Tether.

Token sind dagegen nicht mit den Coins zu verwechseln, sondern verbriefen häufig ein Recht oder einen Eigentumsnachweis⁶. Auch eine eigene Blockchain gibt es bei den Token nicht, sondern sie werden auf einer vorhandenen Blockchain, häufig der von Ethereum, aufgesetzt. Zu den Token zählen unter anderem Binance Coin und Tether. In der Praxis werden Sie allerdings Token meistens wie Coins als Wertanlage nutzen und keine weitergehenden Funktionen einsetzen.

⁶ <https://btcdirect.eu/de-at/was-sind-token>

In der Kommunikation mit anderen Krypto-Fans und den Kryptobörsen raten wir zur korrekten Verwendung der Währungsbezeichnung, die **BTC** für Bitcoin, **BCH** für Bitcoin Cash, usw. lautet. Eine Verwechslung kann den Verlust des überwiesenen Betrags zur Folge sein, beispielsweise wenn Sie aus Versehen Bitcoin auf eine Bitcoin Cash-Wallet überweisen.

Kryptobörsen weisen fast immer Währungskürzel und Währungsname aus und informieren vor Überweisungen auf mögliche Fehler.

Beim Bitcoin haben sich als Maßeinheiten folgende Bezeichnungen eingebürgert:

- 1 BTC = 1,000 mBTC (Millibitcoin)
- 1 BTC = 1,000,000 μ BTC (Microbitcoin)
- 1 BTC = 100,000,000 Satoshis
- 1 mBTC = 100,000 Satoshis
- 1 μ BTC (Microbitcoin) = 100 Satoshis

Satoshi ist die kleinste Werteinheit beim Bitcoin.

2.4 Illegal eingesetzte Kryptowährungen

Auch wenn mancher Politiker anderes suggeriert, spielen Bitcoin und Co. für Verbrecher keine große Rolle.

Laut den Forschern von Chainanalysis⁷ machten illegale Umsätze mit Kryptowährungen im Jahr 2019 21,4 Milliarden Dollar aus. Zwar stiegen die Umsätze in 2020 auf 10 Milliarden US-Dollar, machen aber trotzdem nur 0,34 Prozent des gesamten Krypto-Transaktionsvolumens aus. Im Vergleich zu illegalen Geldern im traditionellen Finanzwesen spielen Kryptowährungen nur eine untergeordnete Rolle.

2.5 NFT

Eigentlich wollten wir NFTs in diesem Buch außen vor lassen. Weil aber viele Organisationen und Unternehmen inzwischen NFTs vermarkten, kommen wir um dieses Thema nicht herum.

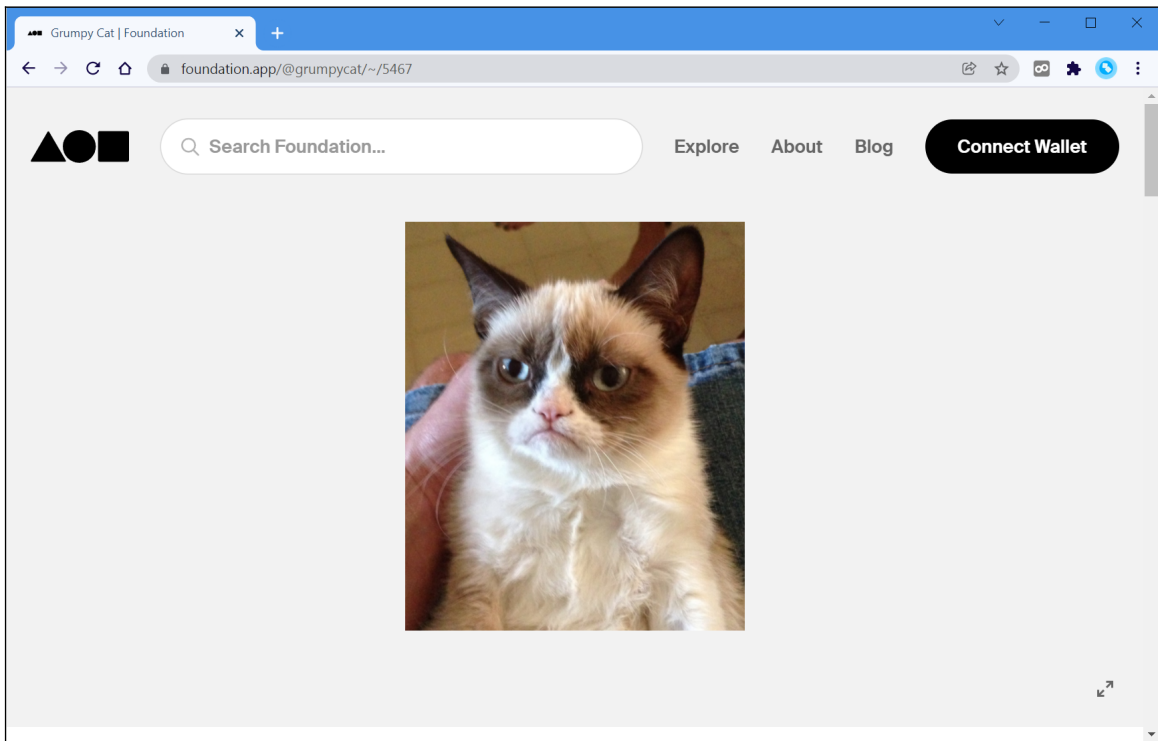
NFT steht für »non-fungible token«, auf Deutsch ungefähr mit »nicht ersetzbares Token« übersetzt. NFTs können den Besitz von digitalen und realen Objekten repräsentieren. Im Gegensatz zu Kryptowährungen, bei denen jeder Coin den gleichen Wert hat, repräsentiert jeder NFT einen anderen Vermögenswert. NFT sind im Gegensatz zu »normalen« Coins also nicht austauschbar und deshalb nicht-fungibel (nicht-ersetzbar).

Im ersten Halbjahr 2021 wurden weltweit NFTs in Höhe von 2,5 Milliarden US-Dollar umgesetzt⁸. Unterstützt werden NFTs von zahlreichen Blockchains, darunter Ethereum, Flow, Tron, Tezos, Cosmos, EOS, WAX und Polkadot. Am häufigsten wird dafür allerdings Ethereum verwendet. Es ist durchaus möglich, das gleiche Objekt als NFT auf verschiedenen Blockchains zu verkaufen.

Auch bei NFTs sind zahlreiche rechtliche Dinge zu beachten. Sie dürfen beispielsweise nicht einfach das (digitale) Kunstwerk eines zeitgenössischen Künstlers als NFT verkaufen – ebenso wird sich ein Musiker, der sein neues Album als NFT der breiten Öffentlichkeit anbietet, seine Wiedergabe- und Songtextrechte vorbehalten. Überhaupt sind noch zahlreiche rechtliche Fragen ungeklärt, denn viele Rechtsgeschäfte setzen eine bestimmte Form voraus, die von NFTs nicht erfüllt wird.

⁷ go.chainanalysis.com/2021-Crypto-Crime-Report-demo.html

⁸ <https://www.reuters.com/technology/nft-sales-volume-surges-25-bln-2021-first-half-2021-07-05/>



Beispiel: Grumpy Cat (engl. schlecht gelaunte Katze). Ein Foto dieses Haustiers, das für seine menschlichen Gesichtszüge weltbekannt wurde, wurde von seinen Besitzern im März 2021 als NFT für 44,20 Ethereum (140.235 US-Dollar) verkauft⁹.

Der Tokeninhalt des zugehörigen NFTs¹⁰:

```
{
  "name": "Grumpy Cat",
  "description": "We present this original remastered Grumpy Cat photographic image. This singular keepsake is available as a 1/1 authenticated edition NFT.\n\nArguably the planet's most famous feline, Grumpy Cat is a New York Times best selling author, the star of her own Lifetime Christmas movie, and the first cat in history to be honored with a Madame Tussaud's wax figure. Grumpy became a pop cultural icon on September 23, 2012, after her frowning photo was posted to Reddit.\n\n1626 x 1957 pixels.\n\nWorst NFT Ever.",
  "image": "ipfs://ipfs/QmfWtxAM2qwKrEXVoeasArDBrR12qL7HCuD2B4Tqe5R8Bs/nft.jpg"
}
```

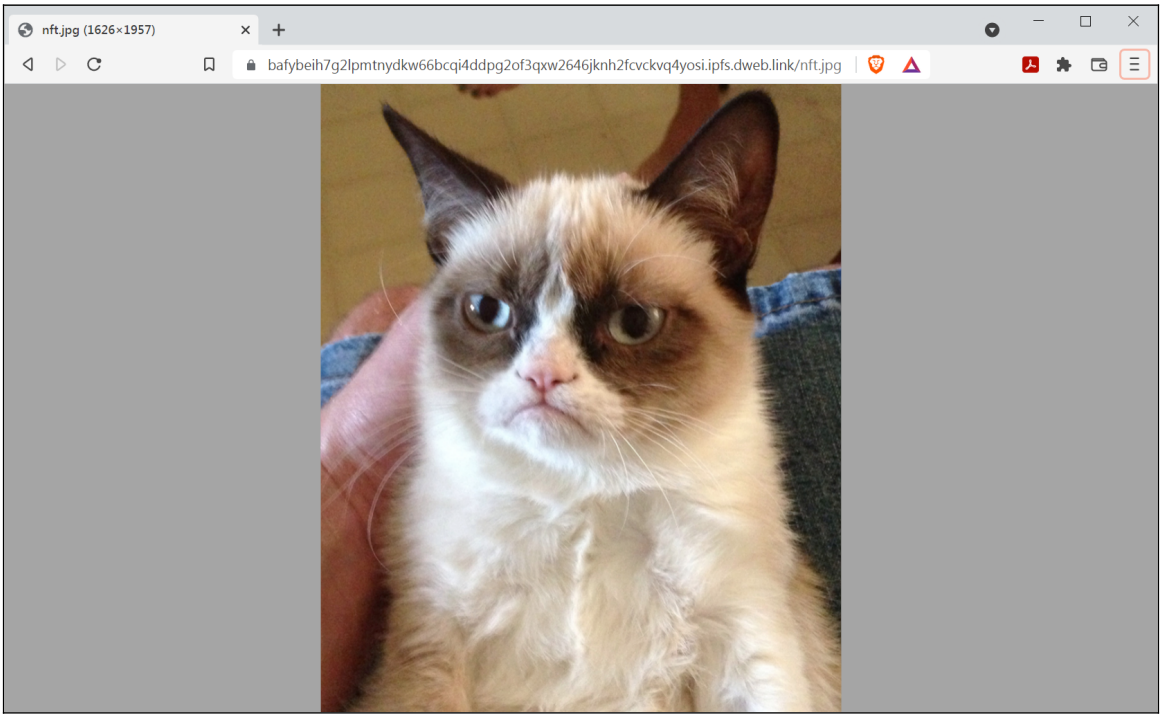
Grundsätzlich wäre es zwar möglich, auch Grafikdaten direkt in der Blockchain abzulegen, in der Praxis wird aber auf eine Webadresse verlinkt. Es kommt natürlich vor, dass Websites beziehungsweise Webadressen abgeschaltet werden und damit die in einem NFT unveränderlich abgelegte Verlinkung ungültig wird.

Im Fall der Grumpy Cat haben sich die Verkäufer mit IPFS (Interplanetarisches Dateisystem) für ein verteiltes Dateisystem entschieden, das die Grafik in einer Blockchain im Internet bereit hält – das Funktionsprinzip ähnelt also dem von Bitcoin, nur dass Dateien statt Coins vorgehalten werden. Der Zugriff auf IPFS-Dateien ist beispielsweise mit dem Brave-Webbrowser (Download unter www.brave.com) möglich¹¹.

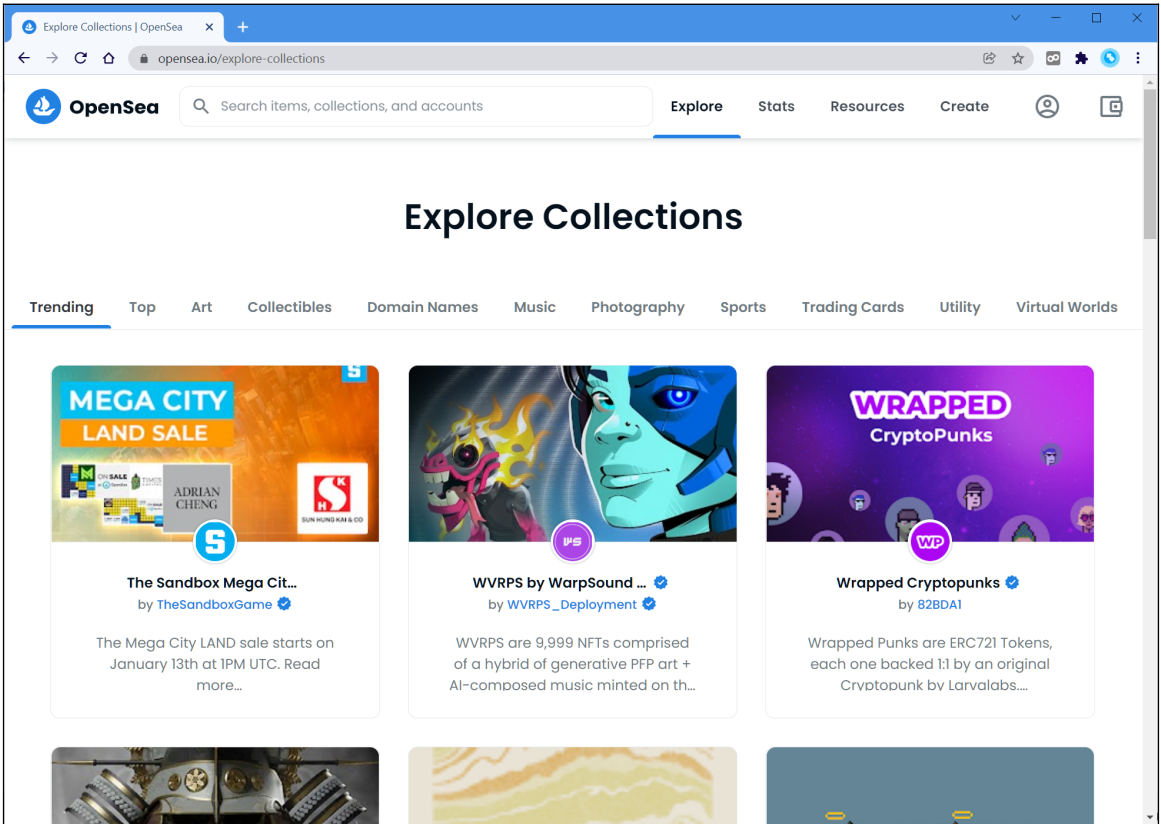
⁹ <https://foundation.app/@grumpycat/~/.5467>

¹⁰ <https://ipfs.io/ipfs/QmNNxJu36S9iq11jHAmwvC3BktTtNomSay3amoSUEhSaUF/metadata.json>

¹¹ <https://www.heise.de/news/Brave-Web-Browser-mit-eingebaitem-IPFS-Support-5031104.html>



Aufruf der im NFT-Token hinterlegten IPFS-Adresse im Brave-Webbrowser.



Die größte NFT-Plattform ist OpenSea (www.opensea.io). Dort können Sie nicht nur NFT kaufen, sondern auch selbst welche erstellen und anbieten.

2.6 DeFi

DeFi ist die englische Abkürzung für »dezentrales Finanzwesen« (Decentralized Finance).

Um DeFi zu verstehen, sollten wir erst einmal einen Blick auf den **traditionellen Finanzmarkt** werfen: Hier gibt es zahlreiche Teilnehmer, die bei jeder Finanztransaktion involviert sind und ihre Dienste in Rechnung stellen. Zudem agieren insbesondere die Banken als Türsteher, die Sie nur nach vorheriger Identitäts- und Bonitätsprüfung als Kunden akzeptieren. Wenn Sie beispielsweise an der Ladenkasse mit einer Bankkarte bezahlen, sind unter Umständen gleich vier Parteien beteiligt, der Supermarkt, ein Zahlungsabwickler, ein Kreditkartenunternehmen und Ihre Bank. Alle beteiligten Parteien stellen natürlich Gebühren in Rechnung und haben die Möglichkeit, Ihre Zahlung abzulehnen.

Bei der DeFi existieren dagegen keine Zugangsvoraussetzungen. Die Beteiligten kennen häufig nur die jeweilige Wallet-Adresse der Person, mit der sie ein Geschäft durchführen.

Die wichtigsten DeFi-Anwendungen sind:

- **Handel:** Tauschen oder handeln Sie Coins mit anderen Kryptonutzern. Siehe Kapitel 11.8 *Kryptowährungen handeln ohne KYC*.
- **Staking:** Beim Staking werden Blockchain-Transaktionen durchgeführt, für die es eine Bezahlung gibt. Dazu schließen sich mehrere Teilnehmer zu sogenannten Pools zusammen. Siehe Kapitel 3.3 *Staking*.
- **Lending**¹²: Das Lending (engl. Verleih) erfolgt nach ähnlichen Regeln wie in der traditionellen Finanzwelt. Man stellt seine Coins dazu einem Liquiditätspool zur Verfügung, der diese wiederum gegen Zinsen an Dritte verleiht. Gegen mögliche Wertverluste – immerhin schwanken Kryptokurse permanent – kann man sich absichern, indem man nur Stablecoins verleiht. Stablecoins sind fest an eine Währung gebunden und schwanken daher nie (siehe Kapitel 8.6.1 *Stablecoins*).
- Für gemeinsame Ziele gibt es **DAOs**. DAO steht für Decentralized Autonomous Organization (dezentrale selbstständige Organisation). Die Regeln des DAO werden durch die Organisationsmitglieder festgelegt und in einem Computerprogramm (**dApp**) beispielsweise auf der Ethereum-Blockchain abgelegt. Die Kryptowährungen Dash und Uniswap sind Beispiele für von einem DAO gelenkte Projekte.

In diesem Buch gehen wir – bis auf den Kryptohandel – nicht weiter auf DeFi-Anwendungen ein, da sie zum einen nur für erfahrene Nutzer interessant sind, zum anderen steuerliche Nachteile mit sich bringen. Siehe für Letzteres auch Kapitel 5 *Besteuerung von Kryptowährungen*. Falls Sie sich dennoch DeFi einsetzen möchten, empfehlen wir auch einen Blick auf die DeFi-Angebote der Kryptohandelsplattformen. Zwar kommen Sie dadurch nicht in den Genuss völliger Unabhängigkeit, dem ursprünglichen DeFi-Ziel, sind aber vor Betrugereien geschützt, auf die nächstes Kapitel eingeht.

2.6.1 Gefahren beim DeFi

Es gibt unzählige DeFi-Plattformen und jeden Tag entstehen neue, mit teilweise irrwitzigen Renditeversprechen. Betrüger nutzen dabei den Umstand der systemimmanenten Anonymität und des geringen Aufwands für das Aufsetzen einer DeFi-Plattform.

Beim sogenannte **Rug Pull** (engl. Teppich wegziehen) erstellen die DeFi-Betreiber eine eigene Kryptowährung und verlassen das eigene Projekt, sobald genügend Leute eingezahlt haben.

Flash Loan (engl. schneller Kredit)-Angriffe nutzen die prinzipbedingte zeitverzögerte

¹² <https://de.beincrypto.com/lernen/defi-lending-erklart-was-sind-defi-loans>

Verarbeitung auf den Blockchains aus.

Vereinfachtes Beispiel für einen Flash Loan mit Betrugsabsicht:

- Der Angreifer erschafft sich einen sogenannten Fake Coin, was heutzutage keinen Aufwand darstellt. Der Fake Coin-Wert wird sehr niedrig angesetzt.
- Nun leiht sich der Angreifer große Ethereum-Beträge und tauscht diese gegen den Fake Coin.
- Anschließend wird der Kurswert des Fake Coin künstlich nach oben getrieben und wieder gegen Ethereum getauscht.
- Der DeFi-Kredit wird zurückgezahlt.

Beispiele für Flash Loan-Angriffe in den letzten Monaten:

- Wormhole: Verlust von 325 Millionen US-Dollar (02/2022)
- Qubit Decentralized Finance: Verlust von 80 Millionen US-Dollar (01/2022)
- Poly Network: Verlust von 600 Millionen US-Dollar (10/2021)
- Cream Finance: Verlust von 37,5 Millionen US-Dollar (02/2021) und 130 Millionen US-Dollar (10/2021)
- Pancake Bunny: Verlust von 200 Millionen US-Dollar (05/2021)
- Warp Finance: Verlust von 7 Millionen US-Dollar (12/2020)

Es ist anzumerken, dass nicht alle Flash Loan-Angriffe erfolgreich sind und die DeFi-Betreiber manchmal noch Teile der »Beute« zurückholen können. Beim Wormhole-Hack wurde sogar einige Tage später das komplette Diebesgut in Höhe von 325 Millionen US-Dollar sichergestellt¹³. Teilweise entschädigen die Betreiber die Betroffenen aus Eigenmitteln.

¹³ <https://www.newsbtc.com/news/solana/solana-price-soars-10-as-325-million-reinstated-on-wormhole>