Pascal Egloff und Ernesto Turnes

Blockchain in der Finanzwelt

Crypto Assets, DeFi, Tokenisierung, NFT und Metaverse

«Das Buch ermöglicht eine differenzierte und sauber strukturierte Vorstellung des Themenfelds um Blockchain, Crypto Assets und Tokens als Basis zukünftiger Ökosysteme. Die zahlreichen Exkurse ermöglichen ein flexibles Vertiefen einzelner Aspekte. Ich empfehle das Buch allen, die sich für die Trends im Bereich Finanzen und neue Technologien interessieren. Ich kenne **kein vergleichbares Werk** in deutscher Sprache, das die komplexe Welt von Blockchain und Co. so **leicht verständlich** und trotzdem **umfassend** und **systematisch** darstellt.»

Philipp Sandner, Professor und Head Blockchain Center
an der Frankfurt School of Finance & Management

«Die ausführlichen und gut verständlichen Erläuterungen, kombiniert mit zahlreichen **praktischen Beispielen,** machen das Buch zu einem super Begleiter für **Praktiker** und **Akademiker** gleichermassen.»

Thomas Moser, Stellvertretendes Mitglied des Direktoriums der
Schweizerischen Nationalbank

«Das Werk schafft wie kein zweites einen Gesamtüberblick über die Thematik. Es ist **verständlich** geschrieben, sodass man kein grosses Vorwissen benötigt: Es bringt die wichtigsten Erkenntnisse **strukturiert** auf den Punkt.»

Alexander Thoma, Head of Digital Assets bei der PostFinance

«Dieses neue **Standardwerk** eignet sich für Praktikerinnen und Praktiker, die nicht nur die technologischen Grundlagen verstehen möchten, sondern auch eine übersichtliche Einbettung in die **rechtlichen**, **buchhalterischen** und **steuerlichen** Themenfelder suchen.»

Silvan Loser, Head of DPP Swiss Accounting bei KPMG Switzerland

VERLAG:SKV
www.verlagskv.ch

1. Auflage 2023

Pascal Egloff, Ernesto Turnes: Blockchain in der Finanzwelt

ISBN 978-3-286-50306-9
Das Werk erscheint als E-Book unter der ISBN 978-3-286-11764-8 (PDF) und als ePub unter der ISBN 978-3-286-11773-0 (EPUB)

Umschlagbild: Miloš Stojanovic

Inhalt Bildquellen:
Seite 44 (Abbildung oben): Bitboy, Public domain, via Wikimedia Commons; Ethereum, gemeinfrei, via Wikimedia Commons; Ripple, CC BY-SA 4.0, via Wikimedia Commons
Seite 247: Fedor Selivanov/Shutterstock.com, Oscar Dominguez/Shutterstock.com, Iurii Motov/Shutterstock.com, GGG999/Shutterstock.com, 96cazador/Shutterstock.com, Nautiluspokal Kulturmuseum St. Gallen (Inv. Nr. G 17604), Ostschweizer Fachhochschule
Seite 256: Vector Factory
Seite 267: Colourhand/Shutterstock.com

Haben Sie Fragen, Anregungen oder Rückmeldungen?
Wir nehmen diese gerne per E-Mail an feedback@verlagskv.ch entgegen.

Die beiden Autoren haben zu gleichen Teilen das vorliegende Buch verfasst:

Ernesto Turnes ist seit 2006 Dozent und seit 2012 Professor für Banking und Finance an der Ostschweizer Fachhochschule (OST) in St. Gallen und leitete dort von 2012 bis 2023 das Kompetenzzentrum für Banking und Finance. Seit 2023 ist er Leiter des neuen Instituts für Finance und Law (IFL). Neben der Lehrtätigkeit im Bereich Aus- und Weiterbildung sowie zahlreichen Referaten und externen Seminaren leitet er diverse Forschungs- und Dienstleistungsprojekte bei Banken und Vermögensverwaltern. Er ist Co-Autor der Lehrbücher «Unternehmensbewertung und Aktienanalyse» sowie «Blockchain für die Praxis». Zu seinen Spezialgebieten zählen das Asset Management, die Bewertung von Finanzinstrumenten sowie Investments in Crypto Assets.

Ernesto Turnes amtete während zehn Jahren als Verwaltungsratspräsident einer Schweizer Asset Management Boutique und ist seit 2020 im Stiftungsrat einer grossen Schweizer Pensionskasse (Anlageausschuss). Vor seiner Tätigkeit an der FH OST arbeitete er als Aktienanalyst bei der Credit Suisse und als Kreditrisikomanager bei Raiffeisen Schweiz. Er hält zwei Masterdiplome der Universität St. Gallen (HSG): M. A. in Banking & Finance et M. A. in Volkswirtschaftslehre. Zudem ist er CFA-Charterholder (Chartered Financial Analyst) und Mitglied der Schweizerischen Gesellschaft für Finanzmarktforschung.

Pascal Egloff ist seit 2017 Dozent an der Ostschweizer Fachhochschule (OST) in St. Gallen. Seit 2023 leitet er das Kompetenzzentrum für Banking und Finance. Dabei fungiert er als Projektleiter bei Forschungs- und Dienstleistungsprojekten, unterrichtet im Rahmen von Aus- und Weiterbildungen und tritt regelmässig als Speaker sowie Panelist auf. Zu seinen Spezialgebieten zählen nebst Blockchain und Digital Assets die Bereiche Impact Finance und Innovationen im Banking. Er ist Co-Autor des Lehrbuchs «Blockchain für die Praxis» und publizierte bereits zahlreiche Artikel zum Themenfeld Blockchain und Finance. Des Weiteren leitete er das von der Innosuisse mitfinanzierte Forschungsprojekt mit dem Titel «Independent Evaluation Framework for Security Tokens», ist Präsident der Branchenvereinigung Digital Assets Switzerland (DAS) sowie Co-Leiter des Projekts «Vision of Tokenized Finance» von Swiss Fintech Innovation (SFTI).

Vor seiner Zeit als Dozent arbeitete Pascal Egloff in London bei der European Bank for Reconstruction and Development (EBRD). Im Team für Power and Energy Utilities begleitete er Finanzierungsprojekte von erneuerbaren Energien im Raum Osteuropa und Zentralasien. Er verfügt zudem über fünf Jahre Berufserfahrung im Banking bei der Credit Suisse in der Schweiz sowie in London. Er absolvierte einen Bachelor in Business Administration an der FHS St. Gallen und hält zwei Master-Abschlüsse der Universität St. Gallen (HSG) in internationalem Management (CEMS) sowie in Rechnungswesen und Finanzen (MAccFin). Zudem studierte er an der Aalto University – School of Business in Helsinki und ist zertifizierter Financial Risk Manager (FRM).

Vorwort

Die Geschichte von Blockchain und Crypto Assets begann mit der Entstehung des Bitcoins im Januar 2009. Aktuell gibt es über 22 000 Crypto Assets, die von den Befürwortern bejubelt und von den Gegnern verschmäht werden. Niemand weiss, was die Zukunft bringen wird, weshalb wir in diesem Buch bewusst darauf verzichten, unsichere Prognosen zu formulieren. Als Dozierende und Forschende einer Hochschule erachten wir es als unsere Aufgabe, die neusten Entwicklungen im Bereich Banking und Finance zu analysieren und die Vor- und Nachteile unseren Studierenden sowie der Öffentlichkeit zu vermitteln. Das Ziel dieses Buches besteht deshalb darin, eine **Brücke zwischen der Theorie und der Praxis** zu schlagen und einen Beitrag zum **besseren Verständnis der komplexen Kryptowelt** zu leisten.

Wir sind seit mehreren Jahren fasziniert von der rasanten Entwicklung und den unerwarteten Wendungen der immer noch jungen Blockchain-Technologie und ihren vielfältigen Anwendungen. Auch nach zahlreichen Forschungs- und Dienstleistungsprojekten, Referaten, Vorträgen und Panel-Diskussionen bleibt die Faszination für Blockchain und Crypto Assets erhalten. Dieses Buch soll den Leserinnen und Lesern nicht nur die Blockchain-Technologie und ihre Anwendungen näherbringen, sondern sie auch dabei unterstützen, sich ein **eigenes fundiertes Bild über das Potenzial dieser technologischen Innovationen** zu machen.

Oft wird die aktuelle und künftige Entwicklung von Blockchain und Co. mit dem Siegeszug des Internets verglichen. Sollte dies zutreffen, würden wir uns aktuell erst am Anfang einer grossen Erfolgsgeschichte befinden. Den Entwicklungen rund um Blockchain, Crypto Assets, DeFi, NFTs und Metaverse wird ein **disruptiver Charakter** zugesprochen. In einer kürzlich durchgeführten Umfrage des MIT SMR Strategy Forum (2022) wurden Experten aus der akademischen Welt befragt, ob die Blockchain-Technologie eine disruptive oder eine erhaltende Innovation darstelle. Dabei hat sich unter den Befragten keine klare Meinung herauskristallisiert.

Die **Theorie über disruptive Innovationen** nach Clayton M. Christensen besagt Folgendes: Disruptive Innovationen transformieren Produkte oder Dienstleistungen, die bisher nur einem sehr beschränkten Kreis an Nutzenden zur Verfügung standen, und machen sie einem breiteren Publikum zugänglich. Meist handelt es sich dabei um Produkte oder Dienstleistungen, die bisher komplex und oder teuer waren. Die disruptive Innovation findet am unteren Ende des Marktes statt und bringt daher oftmals zu Beginn «schlechtere» Produkte als die der Marktführenden mit sich. Eine einfachere Zugänglichkeit oder ein tieferer Preis ebnen den Weg für einen breiteren Nutzerkreis der Produkte oder Dienstleistungen und schliesslich zur Disruption.

Diese sehr kurz gehaltene Definition erlaubt es nicht, ein abschliessendes Urteil über den disruptiven Charakter von Blockchains und ihren Anwendungen zu fällen. Ob sie als disruptive Innovationen einzustufen sind, wird sich erst in der Retrospektive zeigen.

Das wichtigste Indiz für eine potenziell disruptive Innovation steckt hinter dem Begriff **«einfachere Zugänglichkeit»**. Die neue Art der dezentralen oder verteilten Datenhaltung mittels Blockchain erlaubt eine gewisse Demokratisierung und lässt Grenzen (geografisch, rechtlich, kulturell) verschwimmen. Dies kann einen einfacheren Zugang zum Beispiel zu Finanzdienstleistungen ermöglichen. Ein Bitcoin beispielsweise kann problemlos und ohne Intervention von zentralen Instanzen grenzüberschreitend transferiert werden. Dies führt letzten Endes zu einem freieren Zugang zu Finanzdienstleistungen **(finanzielle Inklusion)** für einen grossen Teil der Weltbevölkerung (gemäss Weltbank hatten im Jahr 2021 über 23% der Weltbevölkerung kein Bankkonto). In der Schweiz und in vielen anderen Industrieländern wird der freie Zugang zu Finanzdienstleistungen als Normalfall betrachtet. Für Personen, die dank der Blockchain-Technologie und ihrer Anwendungen in der Finanzwelt erstmals Zugang zu Finanzdienstleistungen erhalten, stiften die Entwicklungen in der Kryptowelt einen echten Mehrwert. Dies allein macht jedoch noch keine disruptive Innovation aus. Einerseits muss sich die Blockchain-Welt zwingend weiterentwickeln (Stichworte: Skalierbarkeit und Interoperabilität), um in der Breite Erfolg zu haben. Andererseits gibt es einige Stakeholder, die künftig noch stärker miteinbezogen werden müssen. Dazu gehören insbesondere die nationalen und internationalen Regulationsbehörden. Zudem erfordert der dezentrale Charakter einer Blockchain ein weitaus grösseres Mass an Kollaboration und Zusammenarbeit unter den Stakeholdern und Nutzenden, wie dies beispielsweise auch in einer direkten Demokratie der Fall ist.

Dieses Lehrbuch beabsichtigt, das notwendige fachliche Rüstzeug zur Verfügung zu stellen, um die Entwicklungen in der Blockchain-Welt mittels handfester Informationen und praxisorientierter Hinweise voranzutreiben. Im Unterschied zum Vorgängerwerk «Blockchain für die Praxis» liegt der **Fokus auf den Anwendungen in der Finanzwelt. Klarheit, Einfachheit und Verständlichkeit** stehen bei allen Ausführungen und Visualisierungen weiterhin im Mittelpunkt.

Didaktische Aufbereitung des Buches

Das Buch umfasst insgesamt **drei Teile oder Ebenen: Technologien, Infrastrukturen und Applikationen**. Am Schluss befindet sich ein **Extrateil**, welcher die übergreifenden Themen Steuern, Rechnungslegung und Recht beinhaltet. Anhand einer **Leitgrafik** können die Lesenden stets nachvollziehen, auf welcher Ebene die jeweiligen Themen angesiedelt sind. Jedes Kapitel beginnt mit einer **Box «Ausblick»**, die darauf hinweist, welche Inhalte im jeweiligen Kapitel enthalten sind. Am Schluss des Kapitels folgt jeweils eine **Box «Rückblick und Zusammenfassung»**, die alle wesentlichen

Aspekte nochmals auflistet. In der **Marginalspalte** (am Seitenrand) wird den Lesenden angezeigt, ob im Text eine wichtige «Definition» oder ein anschauliches «Beispiel» zu finden ist. Zudem sind im Text folgende drei Arten von **Boxen** mit entsprechenden **Symbolen** integriert:

- **«Praxis»** mit Tipps und Hinweisen für **Praxisorientierte**
- **«Technik»** mit technischen Details für **Technikinteressierte**
- **«Exkurs»** mit Hintergrundinformationen für **Detailverliebte**

Diese Boxen können je nach Interesse auch übersprungen werden, ohne den roten Faden zu verlieren. Am Ende des Buches befindet sich zudem ein **Glossar** mit zahlreichen nützlichen Begriffsdefinitionen sowie ein **«Crypto Slang»-Verzeichnis** mit speziellen Begrifflichkeiten und Abkürzungen aus der Kryptoszene.

Dieses Buch richtet sich an:

- Privatpersonen und Mitarbeitende von Unternehmen aus der Finanzdienstleistungsbranche, die sich für das Potenzial und die Funktionsweise der Blockchain-Technologie interessieren. Dazu zählen zum Beispiel Angestellte von Banken, Versicherungen sowie Vermögensverwaltungsgesellschaften, aber auch des Treuhandwesens, der Wirtschaftsprüfung, der Unternehmens-, Rechts- und Steuerberatung sowie von staatlichen Institutionen. Auch Fach- und Führungskräfte von Finanzabteilungen wie beispielsweise Controller oder CFOs sind angesprochen.
- Private und institutionelle Anlegerinnen und Anleger, welche die Chancen und Risiken von Crypto Assets (Digital Assets) besser verstehen möchten.
- Studierende von Fachhochschulen und Universitäten sowie Teilnehmende von Seminaren und Weiterbildungslehrgängen.
- Blockchain- und Krypto-Interessierte, die sich mit dieser innovativen Technologie und den Anwendungsmöglichkeiten in der Finanzwelt vertieft auseinandersetzen möchten.

Danksagung der Autoren:

Folgenden Personen, die zum Gelingen dieses Buches beigetragen haben, möchten wir einen **speziellen Dank** aussprechen (in alphabetischer Reihenfolge):

- Den Fachexpertinnen und Fachexperten **Tina Balzli** (Partnerin, Rechtsanwältin bei CMS Switzerland), **Diego Benz** (Partner, Rechtsanwalt, Notar bei Kaiser Odermatt & Partner), **Marius Breier** (Managing Associate, Steuerberater bei Walder Wyss), **Christoph Burgdorfer** (Managing Director bei Asteria Corporation), **Mauro Casellini** (CEO bei Bitcoin Suisse Liechtenstein), **Jana Essebier** (Partnerin, Rechtsanwältin bei VISCHER), **Peter Fux** (Direktor vom Kulturmuseum St. Gallen), **Marco Gehrig** (Professor für Accounting, Taxation und Corporate Finance an der Ostschweizer Fachhochschule), **Janis M. Heibel** (Head of Crypto bei Synpulse Management Consulting), **Anton F. Jacober** (CEO BlockSpirit), **Philippe Kaiser** (Partner, Rechtsanwalt bei Kaiser Oder-

matt & Partner), **Valentin Kalinov** (Executive Director bei International Token Standardization Association), **Thomas Krabichler** (Dozent für Banking & Finance an der Ostschweizer Fachhochschule), **Thomas Linder** (Tax Partner bei MME), **Silvan Loser** (Head of the Department of Professional Practice [DPP] Swiss Accounting bei KPMG Switzerland), **Andra-Maria Maute** (Enterprise Architect bei Zürich Insurance Group), **Thomas Moser** (Stellvertretendes Mitglied des Direktoriums der Schweizerischen Nationalbank), **Thomas Müller** (Partner, Rechtsanwalt bei Walder Wyss), **Matthias Nimke** (Bibliothekar an der Universität St. Gallen), **Robert Ott** (Project Manager Technical Lead bei SWITCH), **Heiko Petry** (Assistant Manager bei KPMG Switzerland), **Philipp Sandner** (Professor & Head Blockchain Center an der Frankfurt School of Finance & Management), **Roman Schnider** (Präsident der Tezos Foundation), **Sven Steger** (Senior Tax Advisor bei MME), **Cornelia Stengel** (Partnerin, Rechtsanwältin bei Kellerhals Carrard), **Alexander Thoma** (Head of Digital Assets bei der PostFinance) und **Daniel Wild** (Amtsleiter-Stellvertreter des Konkursamts St. Gallen), die uns mit wertvollen Inputs und Beispielen aus der Praxis unterstützt sowie mehrere Teile unseres Buches redigiert haben.
- Allen Personen aus dem Verlag SKV, welche die professionelle Umsetzung und Publikation sicherstellten.
- Unseren Familien, die während der intensiven Schreibphase oft auf unsere ungeteilte Aufmerksamkeit verzichten mussten.

Wir bitten Sie, uns Ihre Kommentare und Verbesserungsvorschläge per E-Mail mitzuteilen (pascal.egloff@ost.ch und ernesto.turnes@ost.ch).

Wir wünschen allen Leserinnen und Lesern viel Spass bei der Lektüre und hoffen, mit unserem Standardwerk einen Beitrag zum besseren Verständnis der komplexen Welt von Blockchain und Crypto Assets zu leisten.

St. Gallen, im Februar 2023
Ernesto Turnes und Pascal Egloff

«Digitale Assets sind die Zukunft und ohne Blockchain-Technologie wird das Thema Finanzen nicht mehr auskommen. Das betrifft schon heute viele Bereiche: den digitalen Euro, den Bitcoin, Smart-Contract-Plattformen wie Ethereum, Decentralized Finance, Non-Fungible Tokens, Metaverse, Tokenisierung von Assets, digitale Wertpapiere. Wer mit Finanzen zu tun hat, sollte sich zügig mit dem Thema beschäftigen, etwa mit Hilfe dieses Buches.»

Philipp Sandner,
Professor & Head Blockchain Center
an der Frankfurt School of Finance & Management

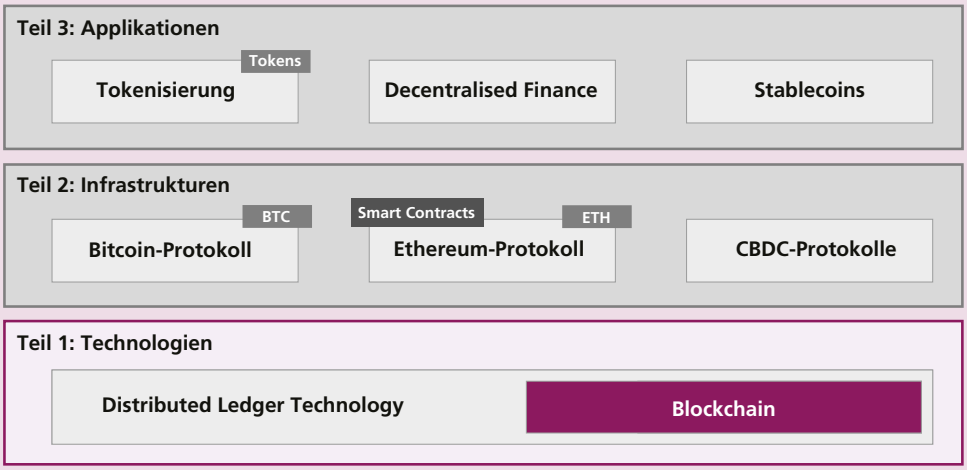
Inhalt

3 Blockchain-Technologie

Ausblick Kapitel 3

In diesem Kapitel erfahren Sie,

- wie die Blockchain-Technologie als *eine* mögliche Ausprägung von verteilten Transaktionssystemen funktioniert,
- wie die Blockchain-Technologie die fünf Anforderungen an Transaktionssysteme (Verfügbarkeit, Eigentumssicherung, Unveränderbarkeit, Überprüfbarkeit und Skalierbarkeit) erfüllt,
- welche technologischen Konzepte bei der Umsetzung von Blockchain zur Anwendung kommen und wie diese zusammenhängen sowie
- welche Herausforderungen die Entwicklerinnen und Entwickler von Blockchain-Technologien noch zu bewältigen haben.



3.1 Einleitung

Definition

Blockchain ist eine spezifische Ausprägung eines **verteilten Transaktionssystems** (DLT). Die Technologie «Blockchain» wird ermöglicht durch die **Kombination** von verschiedenen **Teilkonzepten** und **Technologien**. Diese sind isoliert betrachtet nicht revolutionär. Werden die einzelnen Konzepte jedoch verknüpft, ergibt sich eine neue Technologie mit teils bahnbrechenden Eigenschaften.

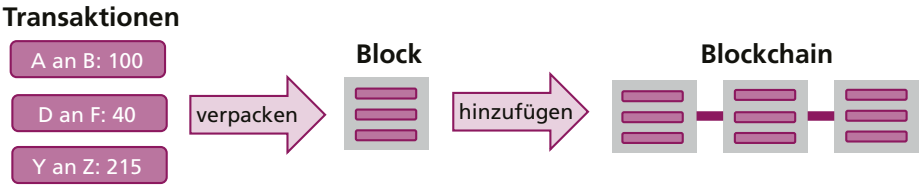
Sofern nicht anders erwähnt, behandelt dieses Buch **öffentliche Blockchains**, die keine spezifische Erlaubnis zur Teilnahme erfordern (Public Permissionless Blockchains).

Bevor in den folgenden Kapiteln im Detail darauf eingegangen wird, wie Blockchain die Anforderungen an ein **vertrauensbildendes Transaktionssystem** erfüllt, werden nachfolgend die fünf **wichtigsten Grundprinzipien** der Blockchain-Technologie erklärt:

- Die Blockchain ist eine **verteilte Transaktionsdatenbank** und ermöglicht die Speicherung und den Transfer von Daten, Werten oder Programmen.
- Die Blockchain wird laufend und **ohne zentrale Intermediäre** synchronisiert (Peer-to-Peer-Netzwerk.
- Die Blockchain garantiert eine hohe **Sicherheit durch Kryptografie** (Verschlüsselung).
- In der **Blockchain** gespeicherte Daten, Transaktionen und Applikationen sind **unveränderbar** (Fälschungssicherheit).
- Die Blockchain verwendet ein **Konsensverfahren**, um neue Blöcke zu überprüfen und diese zu der Blockchain hinzuzufügen.

Bei der Blockchain werden eine oder mehrere **Transaktionen** (z.B. Geldzahlung, Lieferung eines Gutes oder Übertragung eines Rechtes) zusammengefasst und in einen **Block verpackt**. Ein Block ist somit eine Art virtueller Sammelbehälter für Transaktionen, der jeweils zum letzten Block einer ganzen Kette von Blöcken hinzugefügt wird. Daraus entsteht die Blockchain, die es als **Ledger** (Hauptbuch, Register) erlaubt, alle historischen Transaktionen nachzuvollziehen.

Abbildung: Die Blockchain



Wie die Blockbildung genau funktioniert und welche Schritte dazu notwendig sind, wird in den nachfolgenden Kapiteln im Detail beschrieben. Zudem wird auf allfällige Fallstricke sowie mögliche Verbesserungspotenziale hingewiesen.

Von den Anforderungen zur Umsetzung mit Blockchain

Der Aufbau der folgenden Kapitel hält sich strikt an die **fünf** in Kapitel 2.2.2 definierten **Anforderungen** an verteilte Transaktionssysteme. Zuerst wird jeweils die Anforderung erklärt. Danach wird aufgezeigt, wie die Anforderung von der Blockchain-Technologie umgesetzt wird sowie welche Herausforderungen und Chancen daraus entstehen.

Die folgende Abbildung zeigt die **fünf Anforderungen** an Transaktionssysteme sowie die jeweilige **Umsetzung** im Rahmen der Blockchain-Technologie.

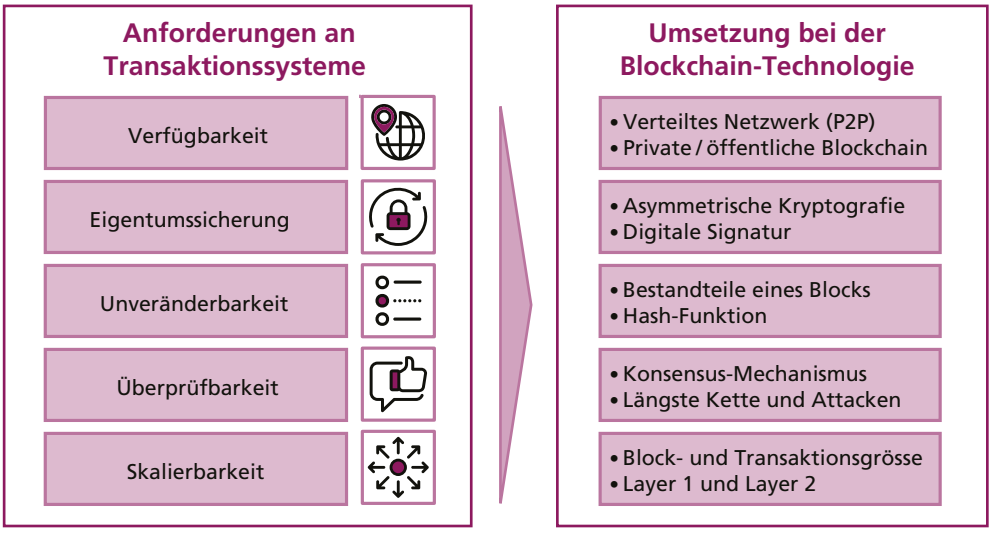
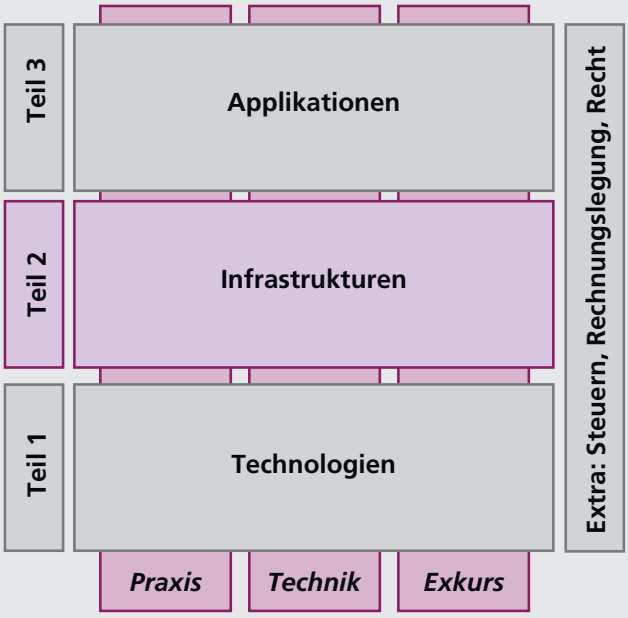


Abbildung: Umsetzung von Blockchain

Obschon alle fünf Anforderungen für die Umsetzung einer DLT wichtig sind, stehen in der **Praxis** die drei Anforderungen **«Eigentumssicherung»**, **«Unveränderbarkeit»** und **«Überprüfbarkeit» im Mittelpunkt**. Anhand dieser drei Eigenschaften, die eng miteinander verbunden sind, lässt sich die Blockchain-Technologie beschreiben. Nichtsdestotrotz dürfen die Anforderungen **«Verfügbarkeit»** und **«Skalierbarkeit»** nicht vernachlässigt werden. Die Verfügbarkeit eines Transaktionssystems ist eine Grundvoraussetzung. Sie wird in der Regel als gegeben betrachtet. Die Skalierbarkeit ist dagegen ein entscheidendes Kriterium für eine weiterführende Verbreitung der Blockchain-Technologie. Dieses Kriterium mit seinen Konsequenzen wie den Kosten pro Transaktion bis hin zum Energiekonsum ganzer Infrastrukturen wird in der Fachwelt heiss diskutiert. Kapitel 3.6 zeigt die wichtigsten Ansätze, wie die Skalierungsproblematik aktuell in der Branche angegangen wird.

Die folgenden Ausführungen in den Kapiteln 3.2 bis 3.6 beziehen sich grundsätzlich auf die **Blockchain-Technologie**. Die **Protokolle** (Regeln) erlauben eine individuelle Umsetzung einzelner Teilbereiche der Blockchain-Technologie (vgl. z.B. Unterscheidung zwischen Proof of Work und Proof of Stake in Kapitel 3.5). Zur Vereinfachung wird im Buch an mehreren Stellen die Funktionsweise basierend auf dem **Bitcoin-Protokoll** erläutert. Dieses stellt immer noch die bekannteste Ausprägung einer Blockchain dar und ist beim Interpretieren von alternativen Ausprägungen hilfreich.



Teil II

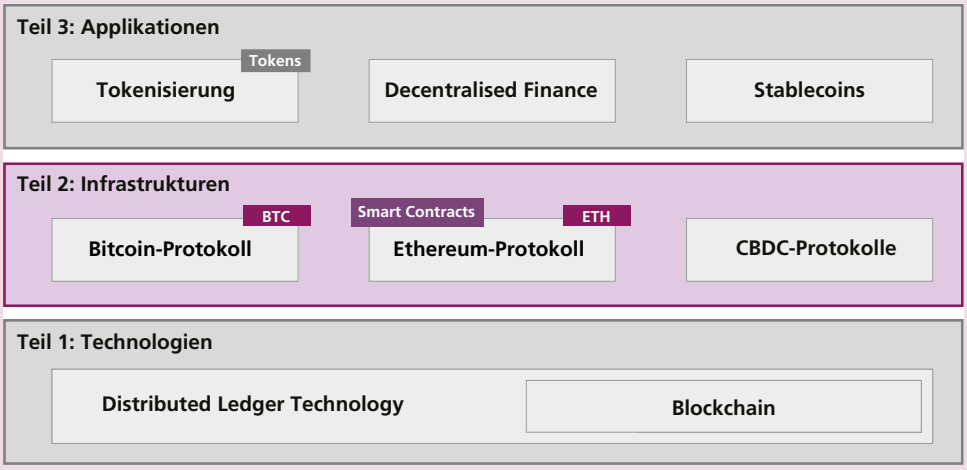
Infrastrukturen

5 Einführung Infrastrukturen

Ausblick Kapitel 5

In diesem Kapitel erfahren Sie,

- was unter einem Protokoll zu verstehen ist und welche Bestandteile ein Protokoll beinhaltet,
- was eine Plattformfunktion eines Protokolls ist,
- wie Smart Contracts und Oracles funktionieren sowie
- wie sich Protokollanpassungen im Rahmen von Soft und Hard Forks differenzieren.



5.1 Infrastrukturen und Protokolle

Die Technologien, die im ersten Teil des Buches vorgestellt werden, legen die Basis für die Ausführungen des zweiten Teils. Diese zweite Ebene, die mit dem Titel **Infrastrukturen** zusammengefasst wird, beschreibt die effektiven Umsetzungen von Blockchains in der Praxis. Nicht alle dieser Umsetzungen in der Form von sogenannten **Protokollen** sind jedoch als Endnutzer erkenn- oder direkt und unmittelbar nutzbar.

Beispiel

Protokolle stellen also eine Art Infrastruktur dar. Als Analogie für eine Infrastruktur im Alltag dient das Strassennetz. Es ermöglicht verschiedenen Verkehrsteilnehmern, von A nach B zu gelangen. Die Einschränkungen sind dabei relativ gering. Auf der gleichen Strasse verkehren beispielsweise Lastwagen, Autos und Fahrräder. Ganz ähnlich verhält es sich im Blockchain-Umfeld. Einige Protokolle erlauben das Verwenden der Infrastruktur für die verschiedensten Arten von Applikationen und stellen diesen dazu die

Grundfunktionen und Vorteile eines dezentralen Transaktionssystems (in der Regel für ein Entgelt) zur Verfügung. Der Schlüssel dazu sind **plattformfähige Protokolle** wie Ethereum. Ähnlich wie im Strassenverkehr ist die Nutzungsgebühr von Ethereum abhängig von der Nutzungsintensität (vgl. Kapitel 7.2.2). Grosse beziehungsweise komplexe Applikationen (Lastwagen) erfordern höhere Strassenverkehrssteuern (Transaktionsgebühren) als kleinere beziehungsweise einfachere Applikationen (Personenwagen).

Was ist ein Protokoll?

Definition

Das **Protokoll** bestimmt die **Regeln** für die **Operationen** sowie die **Kommunikation** zwischen den Netzwerkknoten (Nodes). Ein Protokoll ist somit nichts anderes als ein **Regelwerk**, das in der Form eines Codes die **Spielregeln** einer Software vorgibt. Insofern unterscheidet sich der Begriff kaum von dessen Bedeutung im allgemeinen Sprachgebrauch. In einem Netzwerkprotokoll wird einerseits die Kommunikation zwischen den Netzwerkteilnehmenden definiert, und andererseits wird festgelegt, wie die Daten ausgetauscht werden und ein Konsens im Netzwerk geschaffen wird. Die bekannten

Beispiel

Protokolle TCP/IP, SMTP, HTTP und HTTPS regeln beispielsweise die effiziente Kommunikation zwischen den Computern im Internet. Auf der Basis dieser Protokolle können im nächsten Schritt **Programme und Applikationen** entwickelt werden.

Die **DLT-Technologien** Blockchain und DAG werden durch **Protokolle** umgesetzt. Sie definieren als Softwarecodes die **Netzwerknutzung** sowie allenfalls die Bildung von Applikationen. Im Unterschied zum Internet-Beispiel müssen dabei keine Daten an eine zentrale Instanz geliefert werden, weshalb die Nutzenden grundsätzlich im Besitz ihrer eigenen Daten bleiben.

Beispiel

Ein **Blockchain-Protokoll** wie zum Beispiel das **Bitcoin-Protokoll** definiert die Spielregeln und beantwortet dabei unter anderem folgende Fragen:

- Wie interagieren die Netzwerkteilnehmenden (volle Knoten) miteinander?
- Wie werden digitale Signaturen überprüft?
- Wie funktioniert die Überprüfung von Transaktionen und Blöcken?
- Wie wird ein Konsens zwischen den Netzwerkteilnehmenden gebildet?
- Aus welchen Bestandteilen setzt sich ein Block zusammen?
- Wer darf einen neuen Block zur Blockchain hinzufügen?
- Wie werden neue Crypto Assets und Tokens geschaffen?
- Welche ökonomischen Anreize sind mit der Teilnahme am Netzwerk verbunden?
- Inwiefern werden Smart Contracts unterstützt?

Ein **DAG-Protokoll** wie zum Beispiel das **Tangle-Protokoll** definiert die Spielregeln und beantwortet dabei unter anderem folgende Fragen: Beispiel

- Wie interagieren die Netzwerkteilnehmenden (volle Knoten) miteinander?
- Wie werden digitale Signaturen überprüft?
- Wie funktioniert die Validierung von Transaktionen?
- Wie werden die zwei früheren Transaktionen (Eltern) von den neuen Transaktionen (Kinder) ausgewählt?
- Inwiefern werden Smart Contracts unterstützt?

Arten von Protokollen

Grundsätzlich kann zwischen zwei Hauptarten von Blockchain-Protokollen unterschieden werden. Einerseits bestehen Protokolle, die sich auf die **Durchführung von Transaktionen** (des zugrunde liegenden Native Tokens) fokussieren. Das bekannteste Beispiel dafür ist Bitcoin. Das Bitcoin-Protokoll erlaubt in erster Linie die Durchführung von Bitcoin-Transaktionen. Beispiel

Andererseits gibt es auch Blockchain-Protokolle, die zusätzlich eine **Plattformfunktion** enthalten. Sie stellen eine Art Infrastruktur dar. Diese Infrastruktur kann für eine breite Palette von Applikationen genutzt werden. Das bekannteste Beispiel für ein Protokoll mit Plattformfunktion ist das Ethereum-Protokoll. Plattformen wie Ethereum können nicht nur für das Ausführen von Transaktionen des zugrunde liegenden Native Tokens (in diesem Fall Ether) genutzt werden. Sie dienen zudem als Fundament für diverse **Applikationen wie zum Beispiel Applikations-Tokens oder dezentrale Applikationen (DApps)**. Diese Applikationen werden im dritten Teil des Buches genauer vorgestellt. Zahlreiche Plattformen wollen der am meisten genutzten **Ethereum-Plattform** die Vormachtstellung streitig machen. Dazu zählen zum Beispiel Algorand, Avalanche, BNB Chain, Cardano, Cosmos, Polygon, Solana und Tezos. Beispiel

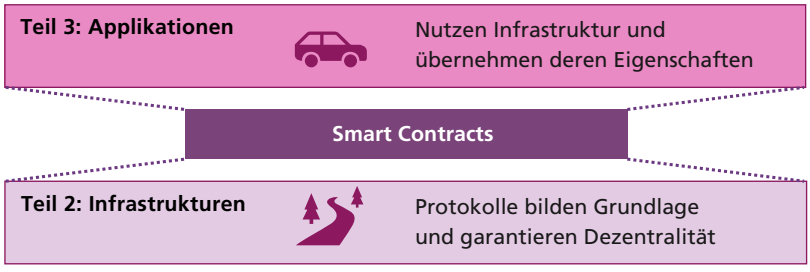


Abbildung: Smart Contracts als Verbindungselement

Was alle Blockchain-Protokolle mit Plattformfunktion gemeinsam haben, ist die Möglichkeit, Smart Contracts dezentral abzuspeichern und laufen zu lassen. **Smart Contracts** dienen als **Grundlage für alle Applikationen** und bilden eine Art Verbindungselement zwischen der Infrastrukturebene und der Applikationsebene.

Technik

Die virtuelle Maschine oder der Welt-Computer

Die Plattformfunktion eines Blockchain-Protokolls baut auf der Idee einer Art **virtuellen Maschine** auf. Die virtuelle Maschine wird von den Nodes des Netzwerks bzw. der Blockchain dezentral betrieben. Sie führt die eigens dafür geschaffenen **Programme (Smart Contracts)** aus.

Das bekannteste Beispiel ist die **Ethereum Virtual Machine (EVM)** des Ethereum-Protokolls. Sie ist nicht nur die bekannteste, sondern auch die erste Umsetzung und wurde deshalb auch schon öfters als «Welt-Computer» bezeichnet. Weitere Informationen zu EVM werden in Kapitel 7.2.1 aufgezeigt.

5.2 Protokollanpassungen (Soft und Hard Forks)

Wie bei allen Softwares müssen auch **Protokolle** für verteilte Transaktionssysteme hin und wieder **auf den neuesten Stand gebracht** oder **Anpassungen** vorgenommen werden. In einem verteilten System kann jedoch **nicht einfach ein Softwareupdate** installiert werden, zumal das System von unzähligen Nodes verteilt geführt wird. Deshalb braucht es auch bei Updates einen **Konsens zwischen den Nodes**, das heisst, die Systemteilnehmenden müssen mit der Änderung einverstanden sein und die **neue Software** anwenden. Die folgenden Ausführungen beziehen sich nur auf **Blockchain-Protokolle.**

Wenn ein Update des Protokolls von einem oder mehreren Nodes vorgeschlagen wird, kann es zu einer **Gabelung** (Fork) der Blockchain kommen. Die Nodes des Systems können sich dann entscheiden, ob sie diesen **Vorschlag akzeptieren** (und die neue Software anwenden) **oder nicht** (und mit der alten Version weiterarbeiten). Damit sich ein **Update** durchsetzt, müssen möglichst viele Nodes beziehungsweise Systemteilnehmende die neue Software anwenden. Es wird zwischen folgenden **zwei Arten von Forks** unterschieden:

Definition
- **Soft Fork:** Eine Soft Fork wird als **abwärtskompatibel** bezeichnet (die Nodes mit der alten Software akzeptieren auch die Meinung der Nodes mit der neuen Software). Die **beiden Versionen** sind **kompatibel**. Die Änderungen im Rahmen einer Soft Fork passen ins Regelwerk des **bestehenden Protokolls**. Demzufolge entsteht **kein neues Protokoll** aus einer Soft Fork. Ein Beispiel für eine Soft Fork wäre die Einführung von SegWit beim Bitcoin-Protokoll (vgl. Kapitel 3.6.5, 7.1.2 und 7.1.3). Bei der Renovation eines Hauses wäre eine Soft Fork als Analogie das Streichen der Wände in einer anderen Farbe.

Definition
- **Hard Fork:** Die **Hard Fork** ist eine Art der Gabelung, die **nicht abwärtskompatibel** ist (bestehende Nodes müssen die Software **zwingend** aktualisieren, um die neuen

Blöcke berücksichtigen zu können). Die Anpassungen am Protokoll sind somit weitreichend und **nicht** mit dem **bisherigen Protokoll kompatibel**. Dies hat zur Folge, dass bei einer Hard Fork eine **Abspaltung** von der bestehenden Blockchain resultiert und ein **neues, eigenständiges Protokoll** entsteht. Ein Beispiel für eine Hard Fork wäre die Gabelung im Jahr 2016, die in den beiden Blockchain-Protokollen Ethereum und Classic mündete (vgl. Kapitel 7.2.3). Bei der Renovation eines Hauses wäre eine Hard Fork als Analogie das Herausreissen einer Wand, um einen Raum zu vergrössern.

5.3 Smart Contracts

Smart Contracts («intelligente Verträge») werden in diesem Buch auf der **Infrastrukturebene** behandelt, obschon sie auch als Applikationen bezeichnet werden können. Smart Contracts und die auf ihnen basierenden Applikationen machen die Blockchain-Technologie und andere verteilte Transaktionssysteme interessant für Wirtschaft und Gesellschaft.

Der Begriff beziehungsweise die Idee von «Smart Contracts» ist schon bedeutend älter als die relativ junge Blockchain-Bewegung. Meist wird der Computerwissenschaftler Nick Szabo mit dem Begriff «Smart Contracts» in Verbindung gebracht. Er prägte diesen bereits in den 1990er-Jahren und spielte mit ähnlichen Ideen, wie sie heute vermehrt in der Praxis zur Anwendung kommen.

Was sind Smart Contracts?

Definition

Ein Smart Contract ist eine in **Computercode** verfasste **Vereinbarung** (im Falle von Ethereum heisst die verwendete Sprache «Solidity»). Diese Vereinbarung wird auf einer Blockchain gespeichert und kann aufgrund der Unveränderbarkeit der Blockchain im Nachhinein nicht mehr geändert werden.

Aus einem technischen Blickwinkel betrachtet, ist ein Smart Contract ein **Computerprogramm**, das **automatisch ausgeführt** wird. Mit automatischer Ausführung ist gemeint, dass **keine zentrale Partei** in die Ausführung involviert ist. Dies funktioniert, indem der Smart Contract auf einem Blockchain-Protokoll mit Plattformfunktion oder einem anderen verteilten Transaktionssystem gespeichert wird. Der Smart Contract übernimmt somit die Prozessabwicklung von Intermediären.

Beispiel

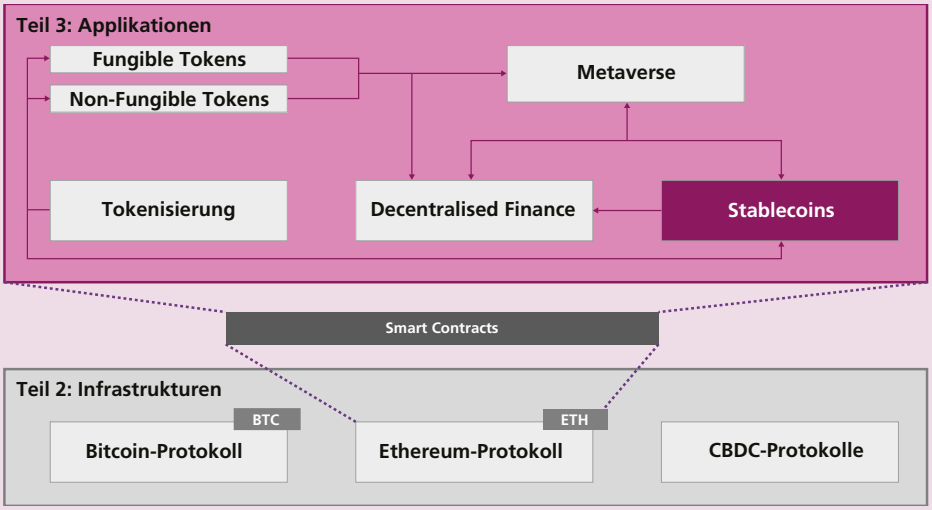
Beim Aufsetzen (Codieren) eines Smart Contracts werden **Inputs und Outputs** definiert. Oft wird auch von einer **Wenn-dann-Beziehung** gesprochen. Dabei wird zum Beispiel definiert, dass, wenn die Bedingung X eintrifft **(Input)**, der Smart Contract automatisch die Aktion Y **(Output)** ausführt. Der Programmcode, der diese Logik beinhaltet, ist auf einem verteilten Transaktionssystem (z.B. Blockchain) hinterlegt und **erbt dessen Eigenschaften** (z.B. Dezentralität und Unveränderbarkeit). Smart Con-

9.3 Stablecoins

Ausblick Kapitel 9.3

In diesem Kapitel erfahren Sie,

- wie sich der Markt für (private) Stablecoins entwickelt hat,
- welche Arten von Stablecoins unterschieden werden sowie
- welche Anwendungsfelder und Praxisbeispiele für Stablecoins existieren.



Da **private Stablecoins** mittels Smart Contracts auf einer **Blockchain mit Plattformfunktion** ausgegeben werden, handelt es sich um Applikations-Tokens oder Non-Native Tokens. Aus diesem Grund befinden sie sich in unserer Leitgrafik auf der Ebene der Applikationen. Im Gegensatz dazu sind die **CBDC-Protokolle** auf der Infrastrukturebene angesiedelt, obschon sie grundsätzlich über die **gleichen Anwendungsfelder** wie Stablecoins verfügen. Da digitale Zentralbankwährungen (CBDCs, vgl. Kapitel 7.3) eher auf privaten Blockchains beruhen, können sie im Gegensatz zu Stablecoins, die auf öffentlichen Blockchains basieren (z.B. Ethereum), die **Privatsphäre** der Token Holders nicht in gleichem Ausmass gewährleisten. Auf der anderen Seite ist das Vertrauen in die Nationalbanken, zumindest in Industrieländern, wohl immer noch grösser als das **Vertrauen** in die **Banken** oder die Programmcodes, die hinter den Stablecoins stehen.

Die folgenden Kapitel gehen auf die Entstehung, die Arten, die Anwendungsfelder sowie die bekanntesten Praxisbeispiele von Stablecoins ein.

9.3.1 Entstehung von Stablecoins

Definition

Stablecoins oder Stabletokens sind **privat ausgegebene** Non-Fungible Tokens, deren **Wertentwicklung** an eine **Referenzeinheit** gekoppelt ist. Die **relative Wertstabilität** von Stablecoins wird meist über die **Besicherung** mit Vermögenswerten wie Fiatwährungen, Gold oder Crypto Assets sichergestellt. Es gibt aber auch Stablecoins, welche die Wertstabilität über einen **Algorithmus** herzustellen versuchen. Im Unterschied zur hohen **Volatilität** von Zahlungs-Tokens wie Bitcoin überzeugen Stablecoins durch die **relative Wertstabilität zur Referenzeinheit** (meist USD). In dieser Hinsicht erfüllen Stablecoins die Anforderungen an ein **Zahlungsmittel** besser als Zahlungs-Tokens wie beispielsweise Bitcoin.

Beispiel

Die Erfolgsgeschichte der Stablecoins hat im Jahr 2014 mit dem ersten **USD-Stablecoin von Tether (USDT)** begonnen. Im Jahr 2018 ist der zweite USD-Stablecoin **(USDC)** auf den Markt gekommen, gefolgt von zwei weiteren USD-Stablecoins **(BUSD und DAI)** im Jahr 2019.[1] Die folgende Grafik zeigt die Entwicklung der **Marktkapitalisierung** dieser vier grössten Stablecoins, die allesamt an die **Referenzeinheit US-Dollar** gekoppelt sind.

Abbildung: Marktkapitalisierung der grössten Stablecoins

Quelle: https://www.theblock.co/data/decentralized-finance/stablecoins (Stand: 27.02.2023)

Beispiel

Im Jahr 2019 hat ein **Konsortium** rund um **Facebook** seine Absicht veröffentlicht, mehrere Stablecoins unter dem Namen **«Libra»** (später **Diem**) lancieren zu wollen.[2] Die damit verbundenen, potenziellen Auswirkungen und Gefahren für die Geldpolitik hat die Notenbanken und die Regulatoren weltweit wachgerüttelt. Fortan haben sich die Notenbanken intensiv mit den Vor- und Nachteilen von Stablecoins und digitalen Zentralbankwährungen (Central Bank Digital Currencies, CBDCs) befasst (vgl. Kapitel 7.3).

1 Weitere Ausführungen zu den vier erwähnten Stablecoins (USDT, USDC, BUSD und DAI) folgen in Kapitel 9.3.4.

2 In der Zwischenzeit hat sich das Konsortium aufgelöst und die Idee von eigenen Stablecoins fallengelassen.

9.3.2 Arten von Stablecoins

Die **relative Wertstabilität** von Stablecoins wird entweder über die **Besicherung** mit Vermögenwerten (Collaterals) oder mit dem Einsatz eines **Algorithmus** (ohne Hinterlegung von Sicherheiten) gewährleistet. Bei der Besicherung mit Vermögenswerten (Asset-backed) wird zwischen **Fiatwährungen** (Fiat-backed), **Gold** (Commodity-backed) und **Crypto Assets** (Crypto-backed) unterschieden.[1]

Die Art der hinterlegten Vermögenswerte spielt auch für den **Grad an Dezentralität** eine wichtige Rolle. Fiatwährungen und Gold werden **ausserhalb der Blockchain** (off-chain) bei einer zentralen Instanz hinterlegt, wohingegen Crypto Assets in Smart Contracts auf der Blockchain aufbewahrt werden (on-chain).

Bei **algorithmischen Stablecoins** wird die relative Wertstabilität über die automatische Steuerung von Angebot und Nachfrage sichergestellt. Die folgende Grafik veranschaulicht die unterschiedlichen Arten von Stablecoins im Hinblick auf die Besicherung[2]:

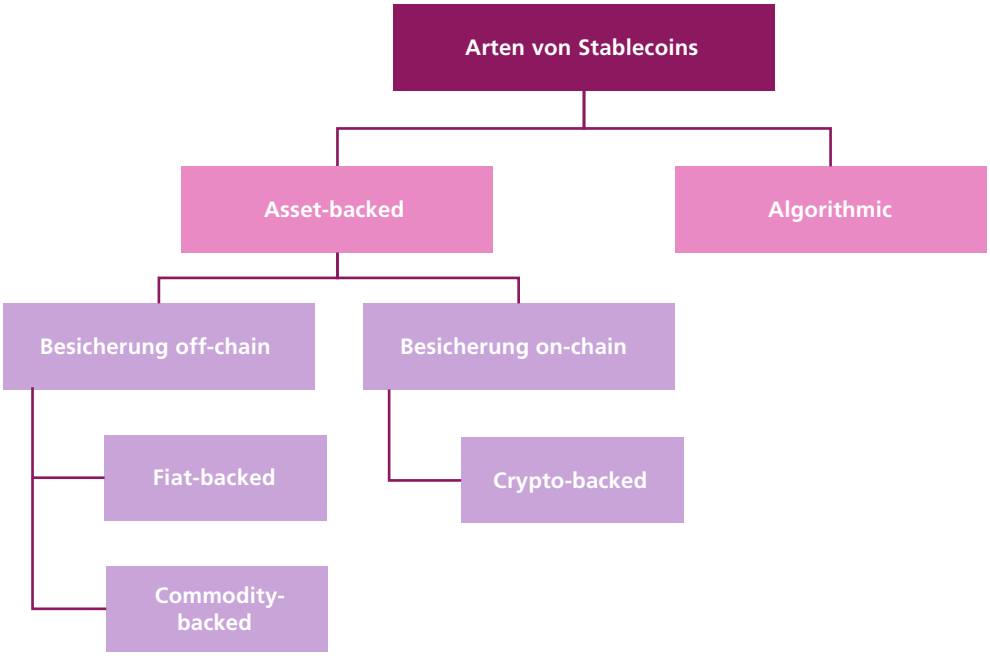


Abbildung: Arten von Stablecoins

1 Es gibt auch hybride Varianten von Stablecoins. Der Stablecoin uUSD der dezentralen Plattform «youves» ist eine Mischung aus Crypto-backed und Algorithmic Stablecoin. Er bietet eine relative Wertstabilität zum US-Dollar und ist auf der Tezos-Blockchain umgesetzt.

2 Im September 2019 hat die FINMA ihre ICO-Wegleitung vom Februar 2018 mit der aufsichtsrechtlichen Einordnung von Stablecoins ergänzt. Die konkrete Ausgestaltung von Stablecoins unterscheidet sich im Einzelfall in rechtlicher, technischer, funktionaler und ökonomischer Hinsicht sehr stark. Eine allgemein gültige Kategorisierung ist daher nicht möglich. Neben dem Geldwäschereigesetz sind jeweils auch Berührungspunkte mit dem Bankengesetz und/oder dem Kollektivanlagengesetz zu prüfen.

ziell. Auch die Eigenschaften der Einzigartigkeit und klaren Identifizierbarkeit beschränkt sich in der Regel auf das verwendete Blockchain-Protokoll. Ein NFT kann problemlos auf einer anderen Plattform nochmals ausgegeben werden. Theoretisch ist es sogar möglich, den genau gleichen NFT auf demselben Protokoll ein zweites Mal auszugeben. Damit das originale Gut oder Werk jeweils identifiziert werden kann, braucht es aktuell meist immer noch einen Intermediär wie ein Auktionshaus. Zudem ist **relativ viel Vorwissen** nötig, um die entsprechenden Überprüfungen überhaupt selbständig durchführen zu können.

Dies führt auch gleich zum nächsten Punkt: der immer noch **unzureichenden Benutzerfreundlichkeit**. Für NFT-Neulinge ist es nahezu unmöglich, sich in angemessener Frist zurechtzufinden, um mit Überzeugung einen NFT auszugeben oder zu handeln. Auch die rechtliche Situation von NFTs ist noch sehr unübersichtlich. Eine grössere Investition sollte daher wohlüberlegt und nur nach ausführlicher Recherche und allfälligem Beizug von Experten durchgeführt werden. Hinzu kommen die für alle Digital Assets geltenden Grundregeln und Vorsichtsmassnahmen wie zum Beispiel die Wahl einer vertrauenswürdigen und sicheren Verwahrungslösung. Zusammenfassend kann auch für NFTs der allgemein gültige Leitspruch der DLT-Welt verwendet werden: **DYOR** (Do Your Own Research).

9.4.3 Anwendungsmöglichkeiten und Praxisbeispiele

Auch bei NFTs ist eine Kategorisierung nicht ganz einfach. Wir haben uns deshalb entschieden, einzig zwischen **NFTs mit und NFTs ohne physischen Zwilling (Abbild)** zu unterscheiden. Andere Dimensionen könnten sich auch auf die **rechtliche Einordnung** (z.B. Eigentum- oder Nutzungsrecht), die betreffende **Branche** (z.B. Fashion, Sport oder Gaming), die **Art der zugrundeliegenden Datei** (falls digital: Text, Audio oder Video), den **potenziellen Kreis der Nutzenden** (alle oder nur eingeschränkter Personenkreis) oder die **technologische Umsetzung** (Layer-1 oder Layer-2-Lösung) beziehen.

Beispiel

Um dennoch einen Überblick über das enorm breite Anwendungsgebiet von NFTs zu geben, werden in den folgenden Abschnitten einige bekannte Anwendungsmöglichkeiten mitsamt Praxisbeispielen vorgestellt. Diese Aufzählungen sind jedoch nicht abschliessend.

Die Vorteile von NFTs, wie zum Beispiel die Möglichkeit zur Partizipation an Sekundärmarkttransaktionen (vgl. Kapitel 9.4.1), werden nicht explizit für alle Anwendungsfälle wiederholt. Gleiches gilt für die Nachteile.

Profilbilder / Avatare

NFTs wie die je 10 000 Charaktere von **CryptoPunks** oder die (gelangweilten) Affen von **Bored Ape Yacht Club** (BAYC) werden oft von ihren Token Holders als Profilbilder für ihre Social-Media-Konten eingesetzt. Seit Anfang 2022 bietet zum Beispiel Twitter auch eine spezifische Funktion für eine standardisierte Integration von NFTs als Profilbild an.

Beispiel

Sammlerstücke (Collectibles)

Oft werden NFTs auch als Sammlerstücke (Collectibles) beschrieben. Auch bei dieser Kategorie von NFTs ist die Nachfrage entscheidend für die Wertentwicklung. Collectibles sind insbesondere dann interessant, wenn es einen grossen Kreis an Sammlern gibt.

Beispiel Bekannte NFT-Sammlerobjekte sind zum Beispiel die NFTs von **NBA Top Shot**. Dabei handelt es sich um kurze Videos von speziellen Spielsituationen der Spiele der National Basketball Association (NBA) der USA.

Beispiel Ein anderes bekanntes Beispiel sind die neuen **NFT-Briefmarken der Post**. Verschiedene nationale Postanbieter (z.B. die Österreichische Post oder die Schweizer Post) haben bereits solche NFT-Briefmarken ausgegeben. Die NFTs werden als Paper Wallet (der private Schlüssel ist hinter einem Rubbelfeld verborgen) verkauft und sind in ihrer physischen Gestalt auch tatsächlich als Briefmarke einsetzbar. Sie können aber auch in ein digitales Wallet übertragen werden und sind somit **digital handelbar**.

Gaming

Ein grosses Potenzial wird den NFTs speziell auch im Gaming-Bereich zugesprochen. Gemäss Juniper Research (2021) wurden im Jahr 2020 weltweit In-Game-Käufe im Wert von circa USD 54 Milliarden getätigt (für 2025 wird der Markt auf über USD 74 Milliarden prognostiziert). Viele dieser sogenannten In-Game Items[1] haben das Potenzial, künftig als NFTs abgebildet zu werden. Die Einsatzgebiete sind sehr breit gestreut.

Beispiel Bekannte Beispiele, die heute schon NFTs in Applikationen mit Gaming-Charakter einsetzen, sind **Zed.run** oder **Axie Infinity** (beide sind auf Ethereum implementiert). Auf Zed.run werden virtuelle Pferderennen (die Pferde sind als NFTs dokumentiert) durchgeführt. Die Spieler können auch eine virtuelle Pferdezucht betreiben und sich so einen ganzen Stall mit Rennpferden aufbauen. Bei Axie Infinity werden virtuelle Charaktere (sogenannte «Axies», ähnlich wie Pokémons) aufgezogen und gehandelt. Die Axies können dann im Spiel auch gegeneinander antreten und kämpfen.

Beispiel Weitere bekannte sogenannte **Massively Multiplayer Online Role-Playing Games (MMORPGs)**, die auf Blockchain basieren, sind: Ember Sword (auf Polygon), Klaymeta (auf Klaytn), Treeverse (auf Ethereum) oder Outer Ring (auf BNB Chain). In der Regel können diese Spiele auch als **Play-to-Earn Games** bezeichnet werden, da die Spieler eine Möglichkeit haben, ihre Fähigkeiten im Spiel zu monetarisieren.

Mode / Fashion

Die Mode- und Fashion-Industrie ist eine weitere Branche, die sich dem Trend von NFTs angenommen hat. Sie bieten digitalisierte Mode beziehungsweise digitale Abbilder von

1 Das könnten z.B. digitale Schwerter, Schilde oder Kleidungsstücke für den eigenen Avatar sein.

Glossar

Die folgenden **188 Begriffe** werden allesamt im Buch thematisiert und im Detail erklärt. Das Glossar dient als Nachschlagemöglichkeit beziehungsweise dazu, sich einen kurzen Überblick zu verschaffen. Zur Zitierung und Referenzierung wird empfohlen, die entsprechende ausführliche Textpassage im Buch zu verwenden.

51-%-Attacke	Bekannter «Angriffspunkt» von Blockchain-Protokollen, bei welchem mindestens 51% der Rechenkapazität (bei Konsensverfahren PoW) oder 51% der gestakten Tokens (bei Konsensverfahren PoS) des Systems nötig sind. Eine solche 51-%-Attacke ist bei grossen Netzwerken eher unwahrscheinlich.
Airdrops	Bei einem Airdrop werden kostenlose Tokens oder NFTs an die Nutzenden eines Blockchain-Projekts versendet. Das Ziel besteht darin, die Bekanntheit eines Projekts zu erhöhen.
Algorithmus	Eine Ansammlung von Anweisungen, die nach der Eingabe eines Inputs immer zu einem Output (Ergebnis) führen. Der Begriff Algorithmus stammt vom persischen Mathematiker Muhammad al-Khwarizmi, der um die Jahrhundertwende vom 8. zum 9. Jahrhundert gelebt hat.
Altcoins	Alternative Coins. Damit sind alle Crypto Assets mit Ausnahme des Bitcoins gemeint.
Anlage-Tokens	Auch «Asset Tokens». Anlage-Tokens reflektieren Vermögenswerte wie Aktien oder Obligationen.
Append-Only-Regel	«Nur-Anfügen»-Regel. Regel, die besagt, dass Transaktionen immer nur in der Form von neuen Blöcken an die Blockchain angefügt werden dürfen.
Applikationen	Programme, die auf einem plattformfähigen Blockchain- oder DLT-Protokoll aufbauen. Sie besitzen die dezentralen bzw. verteilten Eigenschaften der Protokolle und verwenden Smart Contracts als wichtigste Bestandteile.
Asset Tokens	Vgl. Anlage-Tokens
Atomic Swaps	Werden eingesetzt, um Crypto Assets von verschiedenen Blockchains bzw. Blockchain-Protokollen gegeneinander auszutauschen. Alternativ können intermediäre Parteien wie eine Kryptobörse benutzt werden.
Aussonderungsrechte im Konkursfall	Als Teil des Schweizer DLT-Gesetzes wurden die Aussonderungsrechte von Crypto Assets im Konkursfall eines Drittverwahrers (Custodians) geregelt.
Automated Market Maker (AMM)	AMMs sind Protokolle von dezentralen Börsen (Decentralised Exchanges, DEX), die der Preisfindung und somit dem Handel von Tokenpaaren an einer DEX dienen.
Avatare	Digitaler Körper oder Zwilling, der eine Identität im Metaverse (virtuelle Welt) abbildet.
Backend	Gegenstück zum «Frontend» einer Computersoftware. Bleibt im Hintergrund («Backend») und ist für die Benutzenden nicht direkt ersichtlich.

Bitcoin	Native Token des Bitcoin-Protokolls (Protokoll-Token). Erste, grösste und bekannteste Kryptowährung (Zahlungs-Token).
Bitcoin Improvement Proposals (BIP)	Verbesserungsvorschläge von Entwicklerinnen und Entwicklern innerhalb der Bitcoin-Community.
Bits	Binärzahlen 0 oder 1.
Blockchain	Beispiel eines verteilten Transaktionssystems (DLT). Die Technologie Blockchain wird ermöglicht durch die Kombination von verschiedenen Teilkonzepten.
Blockexplorer	Werkzeug in der Form einer Internetseite, welche Informationen zu den Blöcken, Transaktionen und Entwicklungen eines Blockchain-Protokolls dokumentiert und der Öffentlichkeit zur Verfügung stellt. Blockexplorer vereinfachen die Überprüfung von Informationen auf einer Blockchain. Alternativ müssten die Nutzenden einen eigenen Node betreiben.
Blockintervall	Zeitlicher Abstand zwischen zwei Blöcken einer Blockchain. Wird im Fall vom Konsensmechanismus PoW durch die Difficulty beeinflusst.
Body	Auf Deutsch «Körper». Bezeichnet den Teil eines Blocks, der die Transaktionen beinhaltet. Der Body wird über den Transaktionsverweis (Merkle Root) mit dem Header des Blocks verbunden.
Bounty	Tokens, die für das Entdecken von Fehlern oder das Verfassen von Social-Media-Beiträgen an die jeweiligen Personen ausgeschüttet werden.
Broadcasting	«Übertragung» oder «Bekanntmachung» des erfolgreichen Anfügens eines neuen Blocks an die vollen Knoten im Netzwerk. Teil des Konsensverfahrens.
BTC	Abkürzung für den «Bitcoin».
Burning	Auf Deutsch «verbrennen». Wird eingesetzt, um Tokens aus dem Verkehr zu ziehen. Burning kann auch bewusst angewendet werden, um eine deflationäre Wirkung auf bestimmte Tokens zu erwirken.
Central Bank Digital Currencies (CBDCs)	Auf Deutsch «digitale Zentralbankwährungen». CBDCs werden von Zentralbanken ausgegeben und basieren meist auf privaten Blockchains. Es ist zwischen Retail CBDCs (für private Haushalte, Unternehmen und Staat) und Wholesale CBDCs (für Finanzintermediäre) zu unterscheiden.
Centralised Exchanges (CEX)	Auf Deutsch «zentrale Kryptobörsen». Als zentrale Instanzen (z.B. Binance, Coinbase) bieten sie den Handel von Crypto Assets an. Die Kundschaft muss sich registrieren, um einen Zugang (teilweise auch mit Fiatwährungen) zu erhalten. Die Preisfindung basiert auf Auftragsbüchern.
Centralised Finance (CeFi)	Auf Deutsch «zentrale Finanzwelt». Überbegriff für alle zentralen Finanzintermediäre, die Finanzdienstleistungen in der dezentralen Kryptowelt anbieten (z.B. zentrale Kryptobörsen).
Channels	Channels stellen eine Form von Off-Chain-Skalierung (Layer 2) von Blockchain-Protokollen dar. Sie können in State und Payment Channels unterschieden werden.