Timo Purkott
Barbara Scheben (Hrsg.)

KRYPTO-ASSET COMPLIANCE

Umsetzung der Regulierung und Geldwäsche-Prävention

SCHÄFFER
POESCHEL

Krypto-Asset-Compliance

Timo Purkott/Barbara Scheben (Hrsg.)

Krypto-Asset-Compliance

Umsetzung der Regulierung und Geldwäsche-Prävention

Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de/ abrufbar.

Print: ISBN 978-3-7910-6332-4 Bestell-Nr. 11605-0001
ePub: ISBN 978-3-7910-6333-1 Bestell-Nr. 11605-0100
ePDF: ISBN 978-3-7910-6334-8 Bestell-Nr. 11605-0150

Timo Purkott/Barbara Scheben (Hrsg.)
Krypto-Asset-Compliance
1. Auflage, Oktober 2025

Breitscheidstr. 10, 70174 Stuttgart
www.schaeffer-poeschel.de | service@schaeffer-poeschel.de

Bildnachweis (Cover): Starkekonzepte, Christina Peter, Wörthsee

Produktmanagement: Anna Pietras
Lektorat: Barbara Buchter, extratour, Freiburg

Schäffer-Poeschel Verlag Stuttgart
Ein Unternehmen der Haufe Group SE

Inhaltsübersicht

Inhaltsverzeichnis

Abkürzungsverzeichnis

a. A.	Andere Ansicht
Abs.	Absatz
AktG	Aktiengesetz
AO	Abgabenordnung
Art.	Artikel
ART	Asset-Referenced Token
AStG	Außensteuergesetz
AWG	Außenwirtschaftsgesetz
BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BayLDA	Bayerisches Landesamt für Datenschutzaufsicht
BayLfD	Bayerischer Landesbeauftragter für den Datenschutz
BDSG	Bundesdatenschutzgesetz
BFH	Bundesfinanzhof
Bio.	Billionen
BKA	Bundeskriminalamt
BMF	Bundesministerium der Finanzen
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drucks.	Bundestags-Drucksache
CASP	Crypto Asset Service Provider
CBDC	Central Bank Digital Currency
CCAF	Cambridge Center for Alternative Finance
CFSP-Liste	Consolidated Financial Sanctions Party List
CSDR	Central Securities Depositories Regulation
DAO	Dezentrale autonome Organisation
dAPI	Decentral Application Programming Interface
dApp	Decentralised Application (dezentrale Anwendung)
DeAI	Dezentralisierte KI
DeFi	Decentralised Finance
DePIN	Decentralised Physical Infrastructure Networks (Dezentrale physische Infrastrukturnetzwerke)
DEX	Decentralised Exchanges (dezentrale Börsen für Krypto-Assets)
DLT	*Distributed Leger Technology*
DORA	Digital Operational Resilience Act
DPoS	Delegated Proof of Stake
DSGVO	Datenschutz-Grundverordnung
EBA	European Banking Authority
EDSA	Europäischer Datenschutzausschuss
EFRAG	European Financial Reporting Advisory Group

EMT	E-Money Token
ESMA	European Securities and Markets Authority
EStG	Einkommensteuergesetz
ETO	Equity-Token-Offerings
EuGH	Europäischer Gerichtshof
EZB	Europäische Zentralbank
EU-Prospekt-VO	EU-Prospektverordnung
eWpG	Gesetz über elektronische Wertpapiere
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSB	Financial Stability Board
FVOCI	Fair Value through Other Comprehensive Income
FVTPL	Fair Value through Profit or Loss
GASP	Gemeinsame Außen- und Sicherheitspolitik
ggf.	gegebenenfalls
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GO Rh-Pf	Gemeindeordnung Rheinland-Pfalz
GRCh	Charta der Grundrechte der Europäischen Union
GTVO	Geldtransferverordnung
GwG	Geldwäschegesetz
HGB	Handelsgesetzbuch
i. d. R.	in der Regel
i. S. d.	im Sinne des
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
IASB	International Accounting Standards Board
ICO	Initial Coin Offering
ICRI	Counter Ransomware Initiative
IFRIC	IFRS Interpretations Committee
IFRS	International Financial Reporting Standards
IoT	Internet of Things
ITS	Implementing Technical Standards
KAGB	Kapitalanlagegesetzbuch
KMAG	Kryptomärkteaufsichtsgesetz
KPI	Key Performance Indicator
KryptoWTransferV	Kryptowertetransferverordnung
KWG	Kreditwesengesetz
KYC	Know your Customer
lit.	littera (Buchstabe)
m. w. N.	mit weiteren Nachweisen
MaRisk	Mindestanforderungen an das Risikomanagement
MiCA	Markets in Crypto Assets

MiCAR	Markets in Crypto-Assets Regulation
MiFID	Markets in Financial Instruments Directive (Finanzmarktrichtlinie)
MiFIR	Markets in Financial Instruments Regulation
Mio.	Million(en)
Mrd.	Milliarde(n)
MTF	Multilateral Trading Facility (Multilaterales Handelssystem)
MwStSystRL	Mehrwertsteuer-Systemrichtlinie
MwStVO	Mehrwertsteuer-Durchführungsverordnung
NFT	Non-Fungible Token
NGO	Non-governmental Organisation
Nr.	Nummer
OFAC	Office of Foreign Assets Control
OK	Organisierte Kriminalität
OSINT	Open Source Intelligence
OTF	Organised Trading Facility (Organisiertes Handelssystem)
OWiG	Gesetz über Ordnungswidrigkeiten
PoS	Proof of Stake
Rn.	Randnummer
RTS	Regulatory Technical Standard
S.	Seite
SDN-Liste	Specially Designated Nationals and Blocked Persons list
SGB	Sozialgesetzbuch
SPV	Special Purpose Vehicle (Zweckgesellschaft)
StGB	Strafgesetzbuch
STO	Security-Token-Offerings
TOM	Technischen und organisatorischen Maßnahmen
u. E.	unseres Erachtens
USD	US-Dollar
USDT	Tether (US-Dollar nachbildende Kryptowährung)
UStG	Umsatzsteuergesetz
VAG	Versicherungsaufsichtsgesetz
VASP	Virtual Asset Service Provider
VermAnlG	Vermögensanlagegesetz
VVG	Versicherungsvertragsgesetz
VwGO	Verwaltungsgerichtsordnung
WpPG	Wertpapierprospektgesetz
WpIG	Wertpapierinstitutsgesetz
ZAG	Zahlungsdienstaufsichtsgesetz

Vorwort

Liebe Leserinnen und Leser,

die Blockchain-Technologie hat das Potenzial, viele Aspekte unseres Lebens, unserer Unternehmen und unserer Wirtschaft grundlegend zu verändern. Durch Blockchain-basierte Krypto-Assets entstand die Möglichkeit, Transaktionen dezentralisiert, schnell, transparent, sicher und zuverlässig durchzuführen – und das ohne zentrale Bestätigungsinstanz, global und voll automatisierbar. Die sich daraus ergebenden Potenziale gehen weit über den ursprünglichen Zweck alternativer Zahlungssysteme hinaus, sodass sich kontinuierlich neue spannende Anwendungsfälle entwickeln.

Branchenübergreifend setzen sich Unternehmen mit den Einsatzmöglichkeiten digitaler Assets auseinander. Vor allem der Finanzsektor greift das Thema proaktiv auf, um Märkte zu vereinfachen und Prozesse effizienter zu gestalten. Gleichzeitig sehen sich Unternehmen dabei auch mit vielfältigen Herausforderungen konfrontiert. Wenn es darum geht, die Potenziale von Krypto-Assets gewinnbringend für das eigene Geschäftsmodell nutzbar zu machen, werden insbesondere die damit verbundenen rechtlichen Unsicherheiten als wesentlicher Hemmfaktor wahrgenommen. Zwar haben sich die regulatorischen Rahmenbedingungen in den letzten Jahren nach und nach konkretisiert, dennoch zeigt sich, dass die Entwicklung der diesbezüglichen rechtlichen Vorgaben – ebenso wie die Entwicklung des Kryptosektors insgesamt – von einer hohen und anhaltenden Dynamik geprägt ist.

Mit dem vorliegenden Buch wollen wir unseren Beitrag dazu leisten, die regulatorische Landschaft rund um die geschäftliche Nutzung von Krypto-Assets greifbar zu machen. Unser Ziel war es, Entscheidungsträgern[1] und Compliance-Verantwortlichen einen fundierten und anwendungsorientierten Leitfaden an die Hand zu geben, der das Thema aus den verschiedenen Compliance-Perspektiven prägnant und verständlich beleuchtet.

Ob es dabei um die Akzeptanz von Kryptowährungen als Zahlungsmittel, das Anbieten von Krypto-Dienstleistungen oder die Ausgabe eigener Krypto-Token geht – die damit verbundenen Compliance-Fragen sind so vielfältig wie die Arten und Verwendungsmöglichkeiten von Krypto-Assets selbst. Daher werfen wir in diesem Buch gemeinsam mit unseren renommierten Expertinnen und Experten aus den verschiedenen Fachbereichen der Prüfungs- und Beratungspraxis einen umfassenden Blick auf den Themenkomplex Krypto-Asset Compliance, stellen die unterschiedlichen regulatorischen Anforderungen dar und geben Hinweise zu deren praktischer Handhabung.

1 Aus Gründen der besseren Lesbarkeit verwenden wir in diesem Buch bei Personenbezeichnungen und personenbezogenen Substantiven das generische Maskulinum. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Neben kapitalmarkt- und bankaufsichtsrechtlichen Fragen widmen wir uns dabei unter anderem den Bereichen Datenschutz, Tax- und Accounting-Compliance sowie der Verhinderung von Geldwäsche, Terrorismusfinanzierung und Verstößen gegen Finanzsanktionen. Eine Einführung sowohl in die technischen Aspekte von Krypto-Transaktionen und Blockchain-Technologie als auch in die wesentlichen Entwicklungen des Krypto-Marktes trägt darüber hinaus zum ganzheitlichen Verständnis bei.

Dieses Sammelwerk wäre ohne die engagierte Arbeit und Expertise unserer Autoren nicht möglich gewesen. Wir danken allen, die ihre Zeit und ihr Wissen eingebracht haben, um dieses Werk zu einem wertvollen Beitrag für die Krypto-Asset Compliance zu machen. Ein besonderer Dank gilt *Anna Pietras* und *Claudia Knapp* vom Schäffer-Poeschel Verlag, die uns bei der Veröffentlichung unterstützt haben, sowie unserer Lektorin *Barbara Buchter*, die mit ihrer sorgfältigen Arbeit zur Qualität des Werkes beigetragen hat. Ebenso möchten wir die redaktionelle Unterstützung von *Christine Sittner* und *Alexandra Knöfel* hervorheben, die mit ihrem Einsatz und ihrer Expertise maßgeblich zum Gelingen dieses Projekts beigetragen haben.

Wir hoffen, dass Sie durch die Lektüre inspiriert werden, die Chancen dieser vielversprechenden Technologie zu nutzen und gleichzeitig die notwendigen Schritte zur Einhaltung von Compliance-Vorgaben zu unternehmen.

Mit besten Grüßen
Die Herausgeber

A Einführung

1 Technische Grundlagen von Krypto-Assets

Dirk Siegel

Key Facts

- Krypto-Assets sind digitale Einheiten, die auf einer Blockchain verwaltet werden.
- Blockchains beschreiben eine Art dezentral bzw. verteilt geführte Datenstruktur, die redundant und unveränderlich bei den Teilnehmenden des jeweiligen Netzwerks gespeichert und daher nicht auf zentrale Instanzen angewiesen ist.
- Neben der ersten und nach wie vor bedeutendsten Bitcoin-Blockchain existieren inzwischen zahlreiche weitere Blockchains mit unterschiedlichen technischen Spezifikationen und Eigenschaften, wie etwa die Ethereum-Blockchain, auf der auch kleine Programme (Smart Contracts) abgelegt und ausgeführt werden können.
- Smart Contracts bieten die Möglichkeit, Prozesse innerhalb einer Blockchain-Umgebung zu automatisieren, was zur Etablierung Blockchain-basierter Finanzinstrumente und -dienstleistungen (Decentralized Finance – DeFi) geführt hat.

1.1 Überblick

Krypto-Assets sind Werte oder Rechte, die dezentral organisiert durch Blockchains abgebildet werden.[1]

Krypto-Assets werden also durch die ihr zugrunde liegende Technologie (und nicht etwa durch die Natur des Wertes bzw. die Asset-Klasse) definiert. Die Blockchain-Technologie erlaubt sichere Transaktionen und ein hohes Maß an Automatisierung, ohne dass zentrale, als integer vorausgesetzte Institutionen (Banken, Zentralbanken, Börsen etc.) nötig sind.

Das Erzeugen von Transaktionssicherheit in einem Netzwerk von Akteuren, die sich nicht vertrauen (und sich in der Regel nicht einmal kennen), ist die einzigartige Leistung der Blockchain-Technologie. In diesem Kapitel erläutern wir die Technologie, die dies alles ermöglicht und die somit die Basis für alle Krypto-Assets darstellt.

In Kapitel 1.2 werden wir zunächst die grundsätzlichen technischen Merkmale einer Blockchain anhand der Bitcoin-Blockchain, der ersten und wertmäßig nach wie vor relevantesten Blockchain, beschreiben und erklären.

In Kapitel 1.3 erläutern wir die zusätzlichen Features von Blockchain-Netzwerken, die Smart Contracts und damit – technisch gesehen – eine zweite Variante von Krypto-Assets unterstüt-

1 Vgl. Art. 3 Abs. 1 Nr. 5 MiCA Verordnung (2023/1114); Bülow (2019).

zen. Das wird an einem Beispiel verdeutlicht, nämlich am Beispiel Ethereum, der derzeit wichtigsten Plattform für diesen Blockchain-Typ.

Smart Contracts verwalten nicht nur Krypto-Assets, sie ermöglichen auch das Abbilden zahlreicher Finanzdienstleistungen ohne die Vermittlung traditioneller Banken. Das Zusammenwirken von auf Smart Contracts basierenden Komponenten hat das Feld Decentralized Finance bzw. »DeFi« entstehen lassen, das wir in Kapitel 1.4 behandeln. Die technische Basis von Krypto-Assets verändert sich fortlaufend. Wir zeigen daher im abschließenden Kapitel 1.5 Risiken, deren Mitigationen und einige generelle Trends der Weiterentwicklung der Blockchain-Technologie auf.

1.2 Das Bitcoin-Blockchain-Netzwerk

Die technische Basis für das Verwalten von Krypto-Assets ist in der Regel ein Blockchain- beziehungsweise ein DLT-Netzwerk. DLT steht für *Distributed Leger Technology* und stellt eine Verallgemeinerung der Blockchain-Technologie dar, wobei die Unterschiede für unsere Zwecke nicht wesentlich sind.

Da die Blockchain-Technologie auf mannigfaltige Weise kryptografische Verfahren nutzt, hat sich für die mit ihrer Hilfe abgebildeten Assets der Name »Krypto-Assets« etabliert.

Die Initialzündung der Blockchain-Technologie erfolgte am 9. Januar 2009 mit dem Start des Bitcoin-Blockchain-Netzwerks. Noch heute ist die Bitcoin-Blockchain – gemessen am Wert der auf ihr abgebildeten Assets (den »Bitcoins«) – die bedeutendste Blockchain, obwohl es mittlerweile tausende andere, auf technologischen Varianten basierende Blockchain-Netzwerke gibt.

Wir werden daher die Erläuterung der technischen Grundlangen und der Funktionsweise einer Blockchain am Beispiel der Bitcoin-Blockchain durchführen und an den entsprechenden Stellen auf wesentliche Varianten bei anderen Blockchain-Netzwerken verweisen.

Das Bitcoin-Blockchain-Netzwerk funktioniert als digitales Register (als »Ledger«) für Bitcoins: Es bildet alle Bitcoins (und ihre Untereinheiten) ab und führt Buch über alle in Bitcoin getätigten Transaktionen.

Grundsätzlich ließe sich ein solches Register sehr einfach mit den Werkzeugen klassischer Datenbank-Technologien erstellen. Satoshi Nakamoto[2], das Mastermind hinter der Bitcoin-Blockchain, wollte allerdings drei wesentliche Zusatzanforderungen erfüllen:

1. Nicht eine zentrale Stelle sollte den Ledger führen, stattdessen sollten die am Blockchain-Netzwerk Beteiligten die Führung und Sicherung des Ledgers gemeinschaftlich übernehmen.

2 Nakamoto (2008).

2. Anonyme Zahlungen sollten – wie beim Bargeld – möglich sein.
3. Das digitale Register sollte ein Höchstmaß an Sicherheit bieten, damit sich auch signifikante Werte abbilden lassen.

> **Hintergrund**
> Das Ziel der Dezentralität, das Abrücken von zentralen Instanzen wie Banken und staatlichen Institutionen, war wohl motiviert von der Weltfinanzkrise 2007–2008, die auch als eine Krise dieser zentralen Institutionen wahrgenommen wurde.

Alle im Folgenden erläuterten Designkriterien und ihre Umsetzungen in der Bitcoin-Blockchain dienen dazu, die genannten Anforderungen im Kontext eines dezentralen Netzwerks umzusetzen.

Redundanz
Ein hohes Maß an Sicherheit ergibt sich daraus, dass der digitale Ledger nicht an einer Stelle, sondern identisch auf jedem Knoten der Bitcoin-Blockchain geführt wird: Derzeit besteht das Bitcoin-Netzwerk aus mehreren Tausend (ca. 20.000 per Juni 2025) Knoten, die alle eine identische Version des Bitcoin-Ledgers speichern.

Unveränderlichkeit
Die Redundanz der Bitcoin-Knoten schützt zwar vor Datenverlust und Manipulation, schafft aber auch folgendes Problem: Wie kann die Gleichheit und Integrität einer großen Anzahl von Ledger-Instanzen garantiert werden?

Der Lösungsansatz besteht darin, den Datenbestand als Verkettung von Blöcken (daher auch der Name) darzustellen, und zwar so, dass im Netzwerk eine Übereinstimmung nur hinsichtlich des jeweils neuen Blocks (bestehend aus den jeweils neu zu speichernden Transaktionen) erzielt werden muss, während alle vorausgehenden Blöcke als unveränderlich angesehen werden.

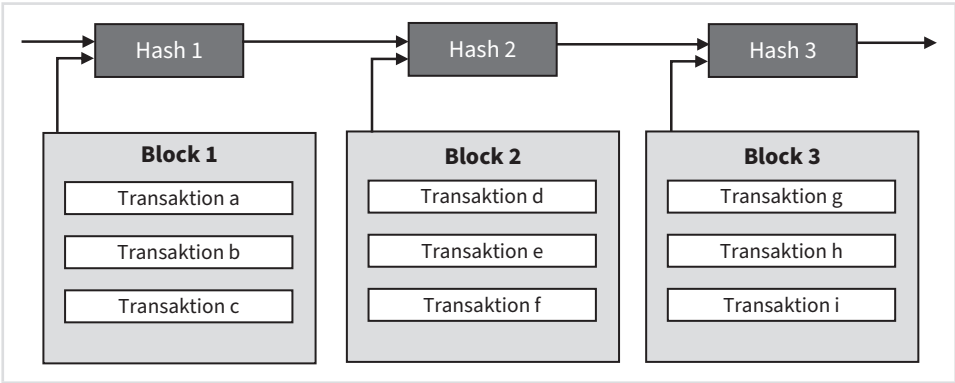

Abb. 1: Vereinfachte Darstellung der Blockchain-Struktur (in Anlehnung an Wilkens/Falk, 2019, S. 6)

Blöcke fassen die Transaktionen zusammen, die innerhalb der sogenannten Blockzeit (bei Bitcoin: 10 Minuten) auftreten. Naturgemäß ist es viel einfacher, im Netzwerk Einigkeit über einen Block (der derzeit[3] ca. 2 Megabyte Daten umfasst) zu erzielen als über den vollständigen Datenbestand der ganzen Blockchain (dieser beträgt derzeit ca. 660 Gigabyte).

Um die Unveränderlichkeit bestehender Blöcke zu garantieren, enthält jeder Block als Teil seines Datenbestands im sogenannten Header einen Fingerabdruck (technisch: den Hash, siehe Abb. 1 und im Kasten »Vertiefung« unten). Ändert man einen Block, dann würde dies sogleich zu einem Mismatch mit seinem im Nachfolgeblock gespeicherten Fingerabdruck führen: Ein solcher Datenbestand wird sofort als nicht integer erkannt und aussortiert.

> **Vertiefung**
> Das Konzept der Hash-Funktion ist in der Kryptografie von höchster Bedeutung. Vereinfacht zeichnet sich eine Hash-Funktion durch zwei Eigenschaften aus:
> - Sie bildet beliebig große Datenmengen auf einer Zahl mit vorgegebener Bitzahl ab (z. B. mappt der verbreitete SHA256-Algorithmus einen beliebigen Input immer auf eine Zahl mit 256 Bits).
> - Selbst kleinste Abweichungen im Input führen zu komplett anderen Ergebnissen. Dieses Streuen der Ergebnisse erklärt den englischen Namen (Hash = Hackfleisch) und macht das Invertieren (das Finden eines Inputs, der zu einem gegebenem Output führt) äußerst aufwendig – oder bei gegebener Rechnerleistung faktisch unmöglich.

Digitale Signaturen
Bitcoin nutzt – so wie alle anderen wichtigen Kryptowährungen auch – das kryptografische Verfahren der **Digitalen Signatur**, um Transaktionen zu sichern. Digitale Signaturen kommen in verwandter Form auch bei einer Vielzahl anderer Anwendungsfälle zum Einsatz.

Ein sogenannter **Private Key** (mit 256 Byte Länge) ist vom Nutzenden selbst zu wählen und geheim zu halten.[4]

Der sogenannte **Public Key** wird aus dem Private Key durch Anwenden einer Hash-Funktion errechnet. Der Falltürcharakter der Hash-Funktion stellt sicher, dass der Private Key aus dem Public Key nicht zurückgerechnet werden kann.

Will ein Nutzender über die an seine Adresse gesendeten Bitcoins verfügen, erstellt er aus seinem Private Key und den Transaktionsdaten eine **Digitale Signatur**. Mittels Public Key kann

3 »Derzeit« bezieht sich, wenn wir Schätzzahlen angeben, immer auf die Mitte des Jahres 2025.
4 Da der Verlust des Private Keys unwiederbringlich dazu führt, dass man nicht mehr über empfangene Bitcoins verfügen kann, hat sich ein ganzer Dienstleistungsbereich (die sogenannten Wallet Provider) etabliert, der Endnutzenden hilft, ihre Private Keys sicher zu speichern – wir gehen weiter unten auf diesen Sachverhalt ein.

nun jeder im Netzwerk die Gültigkeit der Digitalen Signatur verifizieren (ohne dafür den Private Key kennen zu müssen).

Konsensmechanismus
Das Netzwerk muss Konsens hinsichtlich des neuen Blocks (und nur in Hinblick auf diesen) erzielen (vgl. Abschnitt »Unveränderlichkeit«). Dazu muss zunächst geprüft werden, ob die Transaktionen, die in den nächsten Block Eingang finden sollen, echte und erlaubte Transaktionen sind, die den Regeln des Protokolls entsprechen. Diese Überprüfung übernimmt die Knotensoftware, indem sie u. a. die oben erwähnten Signaturen der Transaktionen verifiziert.

Des Weiteren muss verhindert werden, dass einzelne Knoten das Netzwerk mit neuen Blöcken überschwemmen (spammen) oder versuchen, alternative Versionen der Blockchain (sogenannte »Forks«/Abzweigungen) zu erzeugen.

Das in der Bitcoin-Blockchain implementierte Verfahren zur Vermeidung solcher Aktionen ist das sogenannte Proof-of-Work.[5] Es stellt sicher, dass beim Festschreiben eines neuen Blocks eine signifikante Rechenarbeit geleistet werden muss. Im Detail funktioniert das Verfahren bei der Bitcoin-Blockchain wie folgt:

Das Bitcoin-Regelwerk (das sogenannte Bitcoin Protocol) stellt die Knoten untereinander in einen Wettbewerb, welcher von ihnen den nächsten Block für verbindlich erklären und der Blockchain hinzufügen kann. Als Incentivierung erhält der Knoten, der den Wettbewerb gewinnt, neu geschöpfte Bitcoins – derzeit 3,125 Bitcoins (ca. 300.000 US-Dollar) pro Block. Die Aufgabe, die im Wettbewerb gelöst werden soll, besteht darin, den Datenbestand des neu zu erzeugenden Blocks durch Hinzufügen weiterer frei wählbarer Bytes (der sogenannten Nonce) so zu ergänzen, dass der Hash-Wert des sich so ergebenden Datensatzes kleiner als eine vorgegebene Zahl ist.

Aufgrund der Irreversibilität des Hash-Algorithmus kann diese Aufgabe nur durch Ausprobieren gelöst werden. Im Durchschnitt müssen derzeit ca. 1,25 * 1014 (125.000.000.000.000) Möglichkeiten ausprobiert werden, um eine Lösung zu finden. Die Schwierigkeit (Difficulty) der Wettbewerbsaufgabe wird laufend der im Bitcoin-Netzwerk zur Verfügung stehenden Rechenperformance (der »Hash Power«) angepasst: Steigt die Hash Power des Netzwerks und sinkt so die Blockzeit unter 10 Minuten, wird die Schwierigkeit erhöht. Das System kalibriert sich somit selbst.

Eine weitere wesentliche Konsequenz des Proof-of-Work ist, dass aus dem Wettbewerb zufällig verteilt immer andere Knoten als Sieger hervorgehen. Dieses Zufallselement bei der Auswahl

5 Spamming ist bekanntermaßen u. a. auch im Bereich E-Mail ein Problem. Auch dort kommen Proof-of-Work-artige Verfahren als Gegenmaßnahme zum Einsatz.