Die Blockchain-Technologie

Chance zur Transformation der Energieversorgung?

Berichtsteil Technologiebeschreibung

Die Blockchain-Technologie

Chance zur Transformation der Energieversorgung?

Berichtsteil: Technologiebeschreibung

Studie im Auftrag von:

innogy

SMA

swa
Energie Wasser Mobilität

thüga
Das große Plus für alle

TRANSNET BW

VBEW
Energie. Wasser. Leben.

Verbund

VKW
Vorarlberger Kraftwerke AG

Impressum

Bericht zum Projekt:
Die Blockchain-Technologie
Chance zur Transformation der Energieversorgung?

Veröffentlicht am:
05.06.2018

Projektpartner:
Innogy SE
SMA Solar Technology AG
Stadtwerke Augsburg Energie GmbH
Thüga AG
TransnetBW GmbH
VBEW Dienstleistungsgesellschaft mbH
Verbund AG
Vorarlberger Kraftwerke AG

Autoren:
Alexander Bogensperger
Andreas Zeiselmair
Michael Hinterstocker

ISBN:
978-3-941802-38-4

FfE-Auftragsnummer:
B10X-01

Herausgeber:

Forschungsstelle für Energiewirtschaft e.V. (FfE)

Wissenschaftlicher Leiter:
Prof. Dr.-Ing. U. Wagner
Geschäftsführer:
Prof. Dr.-Ing. W. Mauch
Projekt-Manager:
Dr.-Ing. Dipl.-Phys. R. Corradini

Kontakt:
Am Blütenanger 71
80995 München
Tel.: +49 (0) 89 158121-0
Fax: +49 (0) 89 158121-10
E-Mail: info@ffe.de
Internet: www.ffe.de

Inhalt

1 | Zusammenfassung

Die Blockchain-Technologie besteht aus einem verteilten Kassenbuch („distributed ledger“), in welches Daten in diskreten Blöcken gespeichert werden können. Aufgrund des verteilten Charakters ist die Wahrung der Datenintegrität und der Transaktionsreihenfolge durch sogenannte Konsens-Mechanismen gewährleistet. Diese basieren vor allem auf Hash-Funktionen und kryptographischen Elementen, wie sie auch in anderen Bereichen der IT-Sicherheit zum Einsatz kommen. Der zuerst angewendete Konsens-Mechanismus ist „Proof of Work“ und für die hohen Energieverbräuche der Blockchain-Technologie verantwortlich. Neue Konzepte befinden sich bereits in Erprobung oder Entwicklung. Der erste und derzeit populärste Anwendungsfall der Blockchain-Technologie sind digitale Zahlungsmittel („Kryptowährungen“). Die Technologie bietet jedoch eine Grundlage für viele Anwendungsfälle in allen Branchen – auch in der Energiewirtschaft.

Die Blockchain-Technologie ist neben der dezentralen Speicherung von Daten auch seit der Entwicklung der Ethereum-Blockchain in der Lage, Programme auszuführen und kann so z. B. Vertragsstrukturen abbilden und automatisiert abwickeln. Diese sogenannten „Smart Contracts“ sind essenziell für eine Vielzahl von Anwendungsfällen der Blockchain-Technologie – vor allem in der Energiewirtschaft. Auf ihrer Basis können verteilte Apps für Endgeräte („distributed Apps“) entwickelt werden, um Nutzern Zugang zur Blockchain zu schaffen. Abbildung 1-1 stellt die Bestandteile von Blockchain-Plattformen dar.

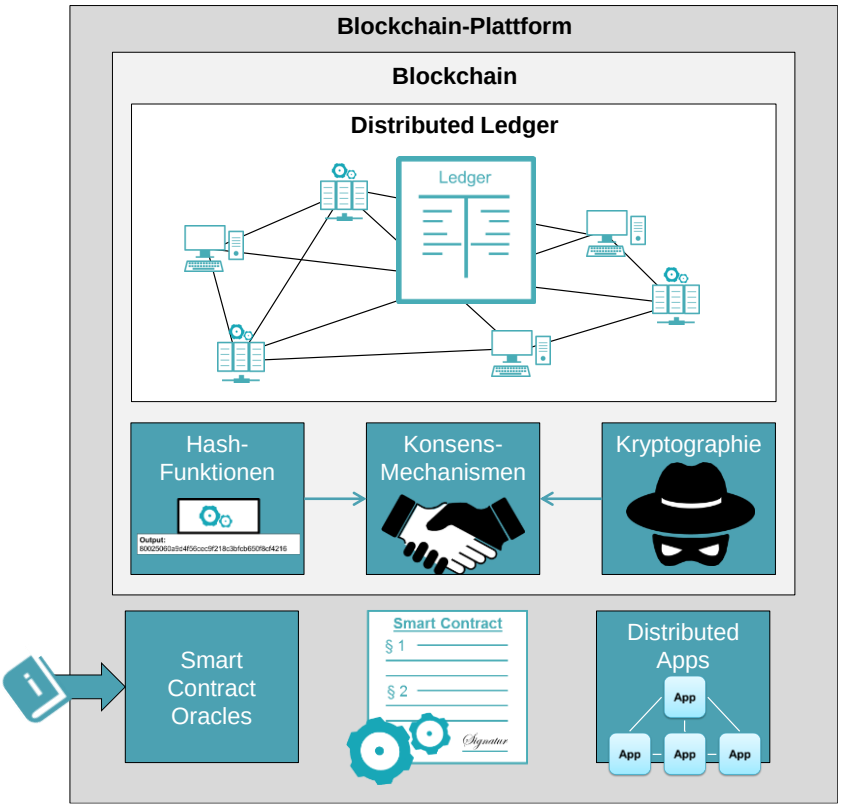

Abbildung 1-1: Grundlegende Bestandteile und Funktionen einer Blockchain-Plattform

Die vorliegende Metastudie zeigt, dass die Blockchain-Technologie grundsätzlich in verschiedenen Ausprägungsarten etabliert werden kann und z. B. so der Zugriff auf private Blockchains für externe Dritte verhindert werden kann. Doch auch hybride Modelle, beispielsweise zwischen mehreren Unternehmen, sind gegenüber der offenen Lösung – gewählt vom Gros der Kryptowährungen – möglich. Die Studie zeigt zudem die technischen Zusammenhänge der Technologie auf und hebt hervor, dass vor allem kryptographische Elemente (Hashing und Public-Key-Kryptographie) das Rückgrat der Blockchain-Technologie darstellen und für die Manipulationssicherheit essenziell sind.

Die Stärken der Technologie liegen unter anderem in der Transparenz des Transaktionsverlaufs, ihrer Manipulationssicherheit, der möglichen Pseudonymität und einem hohen Grad der Verfügbarkeit. Limitationen bestehen heute vor allem noch im Bereich der Skalierung, Transaktionskosten und -geschwindigkeit, Anonymität und Interoperabilität sowie des Energieverbrauchs. Anhand aktueller Entwicklungen zeigt sich, dass derzeit eine Vielzahl an Lösungsansätzen entwickelt werden, welche darauf abzielen, die vorhandenen Limitationen v. a. in den Bereichen Skalierung, Anonymität und Interoperabilität zu verbessern. Dazu gehören u. a. Sharding, State Channels, Sidechains, Zero Knowledge Proofs oder Ring Signaturen.

Die Einsatzmöglichkeiten der Technologie sind vielfältig und in vielen Branchen möglich. Die Blockchain-Technologie kann nicht nur als digitales Zahlungsmittel fungieren, sondern auch in einer Vielzahl digitalisierter Prozesse:

- … Vertrauen schaffen,
- … Intermediäre überflüssig machen,
- … dezentrale P2P-Interaktion ermöglichen,
- … Transparenz ermöglichen,
- … Eigentumsverhältnisse dokumentieren,
- … Anonymität oder Pseudonymität schaffen,
- … Sicherheit digitaler Transaktionen gewährleisten,
- … Mikro-Transaktionen ermöglichen,
- … Prozesse automatisieren,
- … Prozesse optimieren und
- … Datenaustausch und Abrechnung beschleunigen.

Auf Basis dieser Eigenschaften können vielfältige Anwendungsfälle entwickelt werden. So kann die Blockchain-Technologie einen Einfluss auf das Urheberrecht und geistiges Eigentum haben, Supply-Chain-Management, Sharing Economy und die dezentrale Verwaltung von digitalen Identitäten verbessern oder ermöglichen. Der Anwendungsfall der Blockchain-Technologie als Kryptowährung birgt zudem Möglichkeiten alternative Finanzierungs- und Zahlungsmöglichkeiten zu schaffen.

2 | Einleitung

Im Kontext der Blockchain-Technologie wird vielfach die Vision einer vollständig dezentralisierten und autonomen Energieversorgung skizziert, die Intermediäre wie Börsen oder Energieversorger überflüssig macht und direkten Peer-to-Peer-Handel ermöglicht (vgl. /TAP-01 17/). Über diese Vision hinaus gibt es einige weitere Anwendungsfälle, für welche die Technologie Potenziale bieten kann. Aufgrund des frühen Standes der Technologie (das Konzept stammt aus dem Jahr 2008) wird die Blockchain häufig von Dritten als „Lösung ohne Problem“ verstanden, da das tiefere Verständnis der Technologie bzw. der Bezug zu operativen Geschäftsanwendungen fehlen.

Aufgrund der schnellen technologischen Entwicklung ist es eine Herausforderung, Schritt zu halten und alle aktuell relevanten Lösungsansätze im Blick zu behalten. Eine meist sehr einseitige Darstellung der Technologie (sowohl positiv als auch negativ) polarisiert sehr stark und führt auf der einen Seite häufig zu einer überzogenen und an einen Hype grenzenden Erwartungshaltung als auch auf der anderen Seite zu einer Abwehrreaktion derer, welche die Technologie nur als „Modeerscheinung“ abtun. Es ist daher hilfreich, der Energiebranche ein neutrales und unvoreingenommenes Bild der Technologie zu vermitteln, um echtes Verständnis für die Eigenschaften, den Reifegrad und die Einsatzmöglichkeiten zu schaffen.

Bestehende Studien neigen teilweise dazu, die Technologie auf wenigen Seiten stark zu vereinfachen und weisen darauf hin, dass „um den Nutzen eines Autos oder eines Smartphones zu verstehen, (…) nicht zwingend detaillierte Kenntnisse über den Aufbau eines Getriebes für Fahrzeuge oder über Internetprotokolle für Smartphones nötig“ sind. /BDEW-101 17/ Diese Aussage ist nicht falsch, vereinfacht die Problematik jedoch sehr stark und trägt dem Gesamtbild nicht ausreichend Rechnung. Blickt man auf die erfolgreichen digitalen Unternehmen, dann basieren deren Geschäftsmodelle auf den Vorteilen der digitalen Infrastruktur. Um diese zu verstehen, ist jedoch ein tieferes Verständnis der Eigenschaften und Zusammenhänge dieser Infrastruktur nötig, das heute noch vielfach fehlt.

Die vorliegende Studie zielt darauf ab, ein detailliertes Verständnis für die Technologie zu schaffen, um im weiteren Verlauf neue Anwendungsfälle der Technologie identifizieren zu können, die häufig nicht auf den ersten Blick erschließbar sind. Ein informationstechnologischer Hintergrund ist für das Verständnis nicht notwendig. Es sollen die folgenden Fragen geklärt werden:

1) Wie ist der grundlegende Aufbau von Blockchain-Lösungen?

2) Welche Bausteine sind Bestandteil der Technologie und wie ist deren Funktionsweise?

3) Was sind Chancen und Risiken der Technologie und wie lassen sich diese begründen?

4) Welche Lösungen zur Verbesserung der Technologie werden derzeit entwickelt?

Motivation

Im Rahmen des Verbundprojekts der Forschungsstelle für Energiewirtschaft gemeinsam mit den genannten sieben Projektpartnern aus den Bereichen Energieversorgung, Netzbetrieb, Technologie und Branchenverband werden mögliche Anwendungsfälle der Blockchain-Technologie analysiert und entwickelt. Unter dem Titel „Die Blockchain – Chance zur Transformation der Energieversorgung?“ werden hierzu in einem dreistufigen Prozess (Vorstudie – Initiierungsphase – ggf. Umsetzung im Feldversuch) die wissenschaftlichen und praktischen Herausforderungen zur Umsetzung von Blockchain-Projekten evaluiert und in einen energiewirtschaftlichen Kontext eingeordnet. Zu diesem Zweck sollen Anwendungsmöglichkeiten der Blockchain ausgearbeitet, sowie deren Potenziale in der Energiewirtschaft abgeschätzt werden. Die Ergebnisse stellen wiederum die Grundlage für ein Umsetzungsprojekt, in dem die erarbeiteten Grundlagen im Feld getestet und bewertet werden sollen.

Der Fokus des Projekts liegt auf der strukturierten Analyse und Entwicklung von Anwendungsfällen der Blockchain-Technologie in der Energiewirtschaft. Ziel ist daher, am Ende aussichtsreiche Use Cases zu identifizieren, deren Potenzial zu bewerten und schließlich ein Umsetzungsprojekt zu initiieren. Um diese Aufgabe qualifiziert und auf einem einheitlichen Wissensstand umsetzen zu können, beschreibt der folgende Berichtsteil detailliert die Blockchain-Technologie als Grundlage für die sinnvolle Bewertung von Anwendungsfällen. Diesen widmet sich folglich der darauf aufbauende, zweite Projektbericht.

3 | Die Blockchain-Technologie

Dieses Kapitel beschreibt die Definition sowie die Bestandteile, den Aufbau, die Chancen und Risiken, die mit der Blockchain-Technologie verbunden sind. Das Ziel des Kapitels ist es, einen detaillierten und dennoch übersichtlichen Einblick in die einzelnen Komponenten einer Blockchain zu vermitteln. Da es viele verschiedene Blockchain-Lösungen mit unterschiedlichen Herangehensweisen und Lösungsansätzen hinsichtlich gewisser Limitationen gibt und die Entwicklung stetig voranschreitet, werden im nachfolgenden Kapitel häufig die Blockchain-Implementierungen von Bitcoin und Ethereum herangezogen. Dabei ist die Bitcoin-Blockchain die erste Blockchain überhaupt und aufgrund ihrer relativen Einfachheit ein angemessenes Anschauungsobjekt für die Grundlagen der Technologie. Die Ethereum-Blockchain bietet erweiterte Funktionalitäten (z. B. Smart Contracts) zur Bitcoin-Blockchain und ist dadurch die Grundlage für eine Vielzahl an energiewirtschaftlichen Anwendungsfällen und ein „Best-Practice-Beispiel“ für die Technologie (bzgl. ihres heutigen Standes) in diesem Bericht.

3.1 Definition, Aufbau und Abgrenzung

Der Begriff „Blockchain“ definiert sich als „dezentrale, chronologisch aktualisierte Datenbank mit einem aus dem Netzwerk hergestellten Konsens zur dauerhaften digitalen Verbriefung von Eigentumsrechten“ /GAB-10 17/. Vereinfachend bietet sich zur Illustration der Funktionalität einer Blockchain die Analogie zu einem Kassenbuch an (siehe Abbildung 3-1). Die in der Abbildung verwendeten Begrifflichkeiten werden im nachfolgenden Bericht detailliert beleuchtet.

Kassenbuch

Blockchain

Kassen**buch**	Block**Chain**
Seite mit mehreren Transaktionen	**Block** mit mehreren Transaktionen
• Transaktionen **Dokumentation von Wertaustausch**	• Transaktionen **Dokumentation von Wertaustausch**
Informationen auf der Seite: • Datum • Mehrere Transaktionen (so viele auf die Seite passen) • Seitenzahl • Stempel des Buchhalters	• Informationen im Block: • Zeitstempel • Mehrere Transaktionen in festgelegten Datenmengen • Blocknummer • Hash des Blockes
• Prüfung jeder Seite durch den Wirtschaftsprüfer	• Prüfung jedes Blocks durch das gesamte Netzwerk
• Wirtschaftsprüfer	• Jedes Mal ein anderer beteiligter Knoten im Netzwerk; überwacht durch alle Beteiligten

Abbildung 3-1: Vergleich der Blockchain-Technologie mit einem analogen Kassenbuch

Die Begriffe „Blockchain“ und „Distributed Ledger“ werden irrtümlicherweise häufig als Synonyme verwendet. Während ein „Distributed Ledger“ lediglich eine verteilte Datenbankstruktur beschreibt, ist bei einer Blockchain neben der verteilten Datenbank auch immer ein zeitdiskreter Konsens über die vergangenen Transaktionen sowie deren Reihenfolge notwendig /ECB-101 16/. Die Teilnehmer im Netzwerk sammeln und validieren Transaktionen eines gewissen Zeitraums und speichern diese mittels des zugrundeliegenden Konsens-Mechanismus in sogenannten „Blöcken“. Diese Blöcke werden wie eine Kette aneinandergereiht, um die Reihenfolge aller Transaktionen festzuschreiben und Missbrauch (sogenanntes „double spending“) zu vermeiden.

Die Blockchain-Technologie ist ein digitales, verteiltes Kassenbuch

Aufbau von Blockchain-Technologien

Blockchain-Technologien bestehen aus dezentral verteilten Datenbankstrukturen. Transaktionen werden in diskreten Zeitschritten (Blöcken) zusammengefasst und an vorangehende Blöcke angehängt. Durch den verwendeten Konsens-Mechanismus herrscht über die Validität und Reihenfolge von Transaktionen Einigkeit. Manipulationen und Missbrauch können so verhindert werden.

Die Unterscheidung von (de-)zentralen und verteilten („distributed“) Netzwerkstrukturen wird durch Abbildung 3-2 beschrieben. In einem zentralen System existiert eine entscheidende Instanz (vgl. Bank), über welche jedwede Form der Interaktion zwischen anderen Netzwerkteilnehmern abgewickelt wird. In einem dezentralen System ist keine zentrale Instanz mehr vorhanden. Eine direkte Interaktion zwischen den Teilnehmern ist jedoch noch nicht in jedem Fall möglich, da noch gewisse Hierarchieebenen existieren (vgl. Stromnetze). In einem verteilten System sind grundsätzlich alle Netzwerkteilnehmer gleichgestellt. Eine Hierarchie existiert nicht (vgl. Blockchain-Technologie).

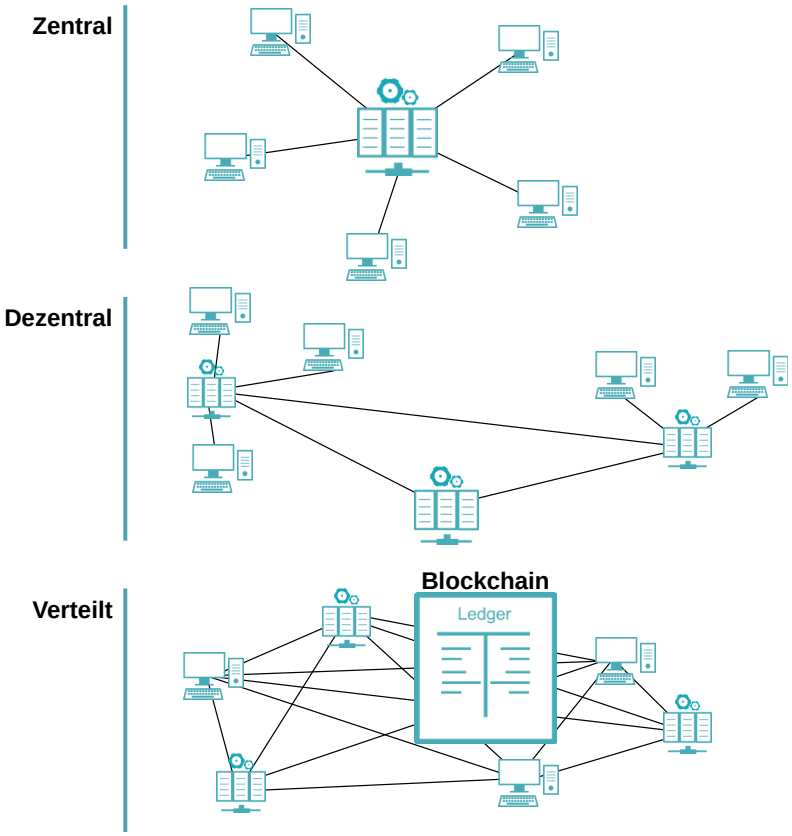

Abbildung 3-2: Zentralisation, Dezentralisation, Distribution

Standardisierung und Interoperabilität sind heute noch nicht gegeben

Im Gegensatz zum Internet kann bei der Blockchain-Technologie nicht von „der Blockchain“ gesprochen werden. Aufgrund des frühen Entwicklungsstandes, vielen parallelen Entwicklungen und mangelnder Standardisierung handelt es sich um ein Grundkonzept, welches durch viele individuelle Optimierungen und Anpassungen weiterentwickelt wird. Ob und wann sich eine Konsolidierung einstellen wird, ist zum heutigen Zeitpunkt noch nicht absehbar.

Distributed Ledger Technologien (DLT) sind ein Überbegriff

Neben der Blockchain-Technologie existieren auch weitere vergleichbare Lösungen mit unterschiedlichen Herangehensweisen, welche häufig aus der Blockchain abgeleitet wurden. Diesen Technologien ist meistens lediglich gemein, dass sie über „Distributed Ledger“, also verteilte Kassenbücher, verfügen. Daher werden sie auch als „Distributed-Ledger-Technologien“ (kurz DLT) bezeichnet. Beispiele sind auf „directed acyclic graphs“ aufbauende DLT wie das Tangle von IOTA oder Hashgraph, welche im weiteren Verlauf dieser Studie beschrieben werden (vgl. Kapitel 3.4.5).

3.1.1 Entstehungsgeschichte der Blockchain

Die Idee „Blockchain“ stammt von Satoshi Nakamoto aus dem Jahr 2008

Die Blockchain-Technologie beruht auf einer Fülle an Vorarbeiten wie z. B. der Entwicklung diverser digitaler Währungen, „distributed computing“, Hash-Algorithmen und kryptographischer Errungenschaften auf Basis wissenschaftlicher Arbeiten und technischer Entwicklungen. Der entscheidende Schritt hin zur Blockchain-Technologie ist mit dem White-Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ von Satoshi Nakamoto aus dem Jahr 2008 verbunden. In diesem wurde erstmals ein funktionierender Konsens-Mechanismus (vgl. Kapitel 3.2.3) beschrieben, der dezentralisierte Transaktionen ohne Intermediär ermöglicht /NAKA-101 08/.

Satoshi Nakamoto

Bei Satoshi Nakamoto handelt es sich um eine Person, ein Pseudonym oder eine Gruppe, welche durch das White Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ /NAKA-101 08/ im Jahr 2008 die Entstehung und frühe Entwicklung der heute als „Blockchain“ bekannten Technologie maßgeblich mitgestaltet hat.

Kryptowährungen wie Bitcoin basieren auf der Blockchain-Technologie

Auf Basis des White Papers von Satoshi Nakamoto startete am 03. Januar 2009 das Bitcoin-Netzwerk /BLO-101 14/, mit dem es möglich ist, pseudonymisiert Transaktionen durchzuführen. In den darauffolgenden Jahren gewann das Netzwerk zunehmend an Bedeutung und der Teilnehmerkreis erweiterte sich sukzessive. Die Anwendung wurde in den ersten Jahren u. a. im Darknet aufgrund des hohen Pseudonymitätsgrades für illegale Geschäfte genutzt /COIND-101 17/, /JEP-101 15/. Doch zunehmend wurde das erweiterte Potenzial hinter der Technologie erkannt und erregte nicht nur in technisch versierten Kreisen großes Interesse. Dies führte dazu, dass eine Vielzahl von weiteren Kryptowährungen auf Basis der Blockchain-Technologie mit unterschiedlichen Eigenschaften entstanden (vgl. Kapitel 4.1.1). Neben der Nutzung als Kryptowährung erkannten viele Branchen – wie auch die Energiewirtschaft – die Potenziale der Technologie, was wiederum zur Entstehung einer Vielzahl an Projekten und Start-Ups führte (siehe Kapitel 3.4).

So löste die Technologie im Jahr 2017 einen regelrechten branchenübergreifenden Hype aus, welcher die Entwicklungsgeschwindigkeit der Technologie durch weitere Akteure, Kapital und Interesse zusätzlich steigert und eine Reihe neuartiger Lösungsansätze ermöglicht. Diese Entwicklung ging auch mit einem massiven Interesse an Spekulationsgeschäften auf Basis der Kryptowährungen einher. So stieg der Preis von Bitcoin im Jahr 2017 von ca. 1 000 € auf zeitweise 20 000 €, wodurch zusätzliches öffentliches Interesse generiert wurde.

Das nachfolgende Kapitel erläutert detailliert die technischen Bestandteile der „Blockchain-Technologie“ und deren Zusammenspiel.

3.1.2 Allgemeiner Aufbau von Blockchain-Technologien

Die Blockchain-Technologie basiert auf einem Distributed Ledger

Während heute in vielen Fällen zentrale Parteien (z. B. Banken, Energieversorger) Transaktionen durchführen und die Aufzeichnungen darüber auf zentralen Servern speichern, bietet die Blockchain-Technologie (BCT) die Möglichkeit, dezentrale Transaktionen direkt zwischen gleichgestellten Nutzern („Peers“) ohne Intermediär abzuwickeln. Dabei werden die Informationen über durchgeführte Transaktionen in einem sog. „Distributed Ledger“ („verteiltes Kassenbuch“) bei einer Vielzahl teilnehmender Parteien dezentral verteilt und gespeichert, anstatt diese in zentralen Datenbanken zu sichern. In Abbildung 3-3 sind ein schematischer Aufbau der Blockchain-Technologie abgebildet.

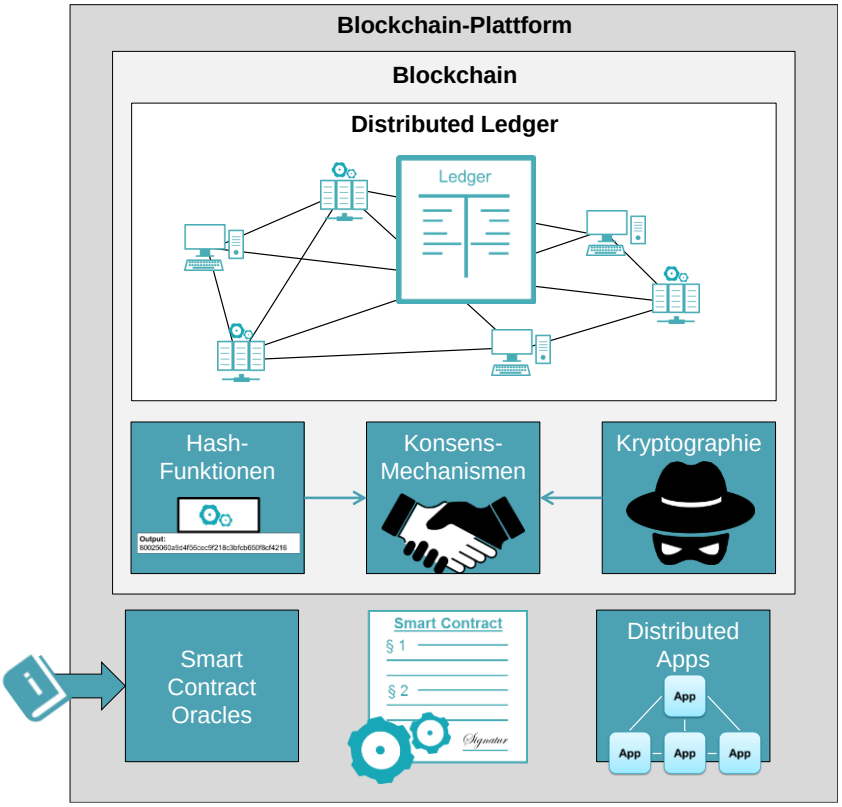

Abbildung 3-3: Grundlegende Bestandteile und Funktionen einer Blockchain-Plattform

Der Kern der Blockchain-Technologie besteht darin, in einer gewissen Zeit[1] stattgefundene Transaktionen zu sammeln und zu sogenannten **Blöcken** zusammenzufassen, die den Konsens des Netzwerks über die Korrektheit der Transaktionen sowie deren Reihenfolge abbilden.

Blöcke dienen dem Festhalten der Reihenfolge von Transaktionen

Um die Richtigkeit und Echtheit von Transaktionen in den Blöcken zu bestätigen sowie zu verhindern, dass Transaktionen desselben Transaktionsgegenstandes mehrmals stattfinden

[1] Bei Bitcoin wird beispielsweise alle ca. 10 Minuten ein neuer Block generiert.

(„double spending“), benötigt jede Blockchain einen sogenannten **Konsens-Mechanismus**. Dieser bestätigt anhand standardisierter Verfahren (dezentral) die Korrektheit der sich im Block befindlichen Transaktionsverläufe (siehe Kapitel 3.2.3) und „kettet“ den bestätigten Block an den vorherigen Block. So entsteht mit der Zeit eine ständig wachsende Kette von Blöcken („Blockchain“).

Die Blockchain bietet pseudonymisierte Transparenz

Die Block-Kette (Blockchain) ist für jeden Teilnehmer im Netzwerk zu jeder Zeit einsehbar und ermöglicht das transparente Monitoring stattfindender Interaktionen. Um trotz dieser Transparenz hinsichtlich des Transaktionsverkehrs die **Anonymität** der im System Agierenden gewährleisten zu können, sind die Nutzer mittels eines **öffentlichen Schlüssels** („public key“) pseudonymisiert. Die Tätigkeiten von Nutzern sind somit zu jeder Zeit nachvollziehbar, ohne deren Identität direkt offen zu legen. Der Zugriff auf diese öffentlichen Schlüssel erfolgt mittels individuellen **privaten Schlüsseln** („private keys“). Diese Form der asymmetrischen Verschlüsselung bietet ein hohes Maß an Sicherheit.

Smart Contracts sind „Computer-programme“ auf der Blockchain

Ein weiterer Bestandteil der Blockchain-Technologie ist die Option, Programme auf der Blockchain zu hinterlegen und diese automatisiert Tätigkeiten abwickeln zu lassen. Diese sogenannten **Smart Contracts** ermöglichen einen hohen Grad der Automatisierung da z. B. Geschäftsprozesse durch sie abgebildet werden können.

Blockchain-Technologien werden anhand des vorgestellten Aufbaus häufig mit den nachfolgenden Attributen beschrieben (s. Kapitel 3.5):

- **manipulationssicher** aufgrund des notwendigen Konsens für eine Änderung und der dezentralen Speicherung der Daten
- **vertrauensschaffend** durch die Unabänderlichkeit der Transaktionshistorie und das Fehlen eines Intermediäres
- **schnell**, da Transaktionen auf den Intermediär verzichten und direkt zwischen Peers (Peer2Peer) erfolgen

Der Quelltext von Blockchains ist in der Regel Open Source

Die meisten der derzeit renommierteren Blockchains aus der Welt der Kryptowährungen (beispielsweise Bitcoin und Ethereum) werden als Open-Source-Software zur Verfügung gestellt, um Transparenz zu schaffen und das kollektive Wissen der Community zu nutzen /CUB-101 15/. Die so verfügbaren Blockchain-Technologien sind für Anwender frei nutzbar und können für individuelle Zwecke genutzt und bis zu einem gewissen Grad angepasst werden.

Die nachfolgenden Kapitel erläutern detailliert die hier in Kürze vorgestellten Bestandteile der Technologie und gehen auf relevante Ausprägungsarten ein. Im Anschluss werden bestehende Limitationen, Chancen, Risiken und Weiterentwicklungen beschrieben, um die Technologie vollständig zu beschreiben.

3.1.3 Ausprägungsarten der Blockchain-Technologie

Die Ausgestaltungsmöglichkeiten einer Blockchain sind vielfältig und betreffen verschiedene Details. So kann eine Blockchain nicht nur allgemein und frei für jeden zugänglich sein, sondern auch alternativ gewisse Restriktionen hinsichtlich ihrer Teilnehmer und Nutzungsart haben. Das folgende Kapitel zeigt in Kürze verschiedene Ausgestaltungsmöglichkeiten auf.

Unterschieden werden kann dabei sowohl der Zugriff auf die Daten und die Nutzung des Netzwerkes („public“, „private“) als auch die Möglichkeiten zur Beteiligung an der Validierung von Blöcken im Konsens-Mechanismus („permissioned“, „permissionless“), wie Abbildung 3-4 zeigt. Neben diesen Unterscheidungen kann ein allgemeines Rollen- und Rechtemanagement individuell definiert werden. /BSI-03 18/

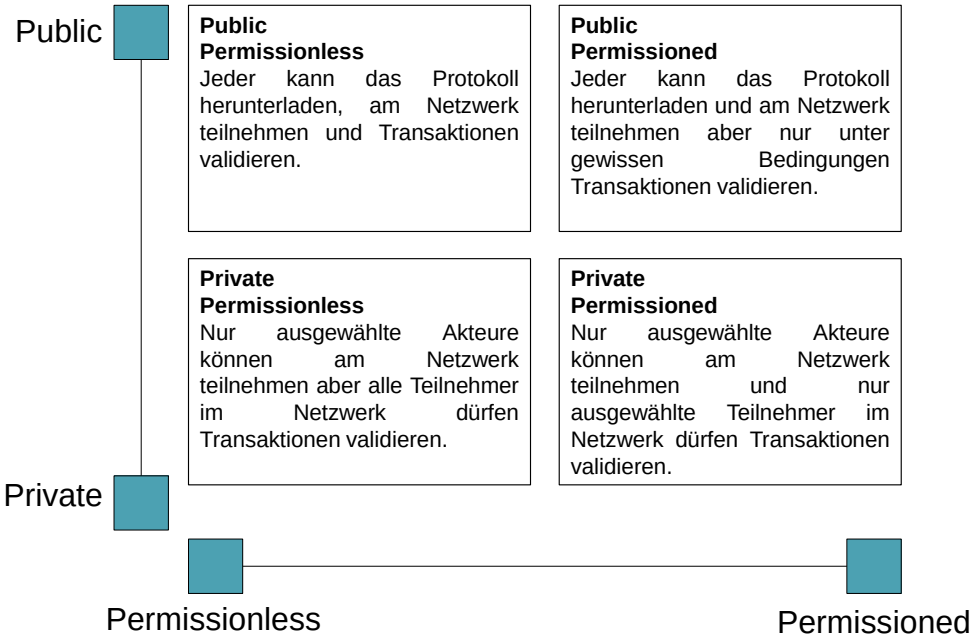

Abbildung 3-4 Abgrenzung verschiedener Ausprägungsarten nach /DIST-01 16/

Ausprägungsarten der Blockchain-Technologie

Die Begriffe „public, private“ beschreiben die Möglichkeiten zur Teilnahme am Blockchain-Netzwerk selbst. (vgl. Intranet vs. Internet)

Die Begriffe „permissioned“ und „permissionless“ beschreiben die Möglichkeiten zur Teilnahme am Konsens-Mechanismus.

Public Blockchain

Bei „öffentlichen Blockchains“ ist der Zugang zur Blockchain für jeden Nutzer frei. Ein Identitätsnachweis ist nicht erforderlich. Public Blockchains sind in der Regel permissionless. Jeder Nutzer kann am Netzwerk teilnehmen und Transaktionen validieren. Die meisten bekannten Kryptowährungen wie Bitcoin und Ethereum setzen auf diese Konfiguration. Wird jedoch der Konsens-Mechanismus – wie in Ethereum mit dem Casper-Protokoll geplant – auf ein Proof of Stake-Modell (siehe Kapitel 0) umgestellt, ist eine gewisse Mindesteinlage

Public Blockchains sind jedem frei zugänglich und in der Regel permissionless

notwendig, um Transaktionen zu valideren. Dies stellt eine Form von Zugriffsbeschränkung auf das Validieren von Transaktionen dar (vgl. Kapitel 0).

In einer öffentlichen Blockchain besteht u. a. aufgrund des großen Datenvolumens, welches zwischen den Teilnehmern ausgetauscht werden muss, die Herausforderung der Skalierbarkeit. Eine nachträgliche Änderung der Daten ist nur durch eine Mehrheit aller beteiligten Akteure möglich /CUB-101 15/. Auch gestaltet es sich aufgrund des Mehrheitsprinzips häufig schwierig, die Blockchain technologisch zu verbessern (Governance-Problematik) und im Falle eines Missbrauchs zu verändern, wie das Beispiel des DAO-Hacks in der Ethereum-Blockchain zeigt (vgl. Kapitel 3.2.4.3) /WIRED-101 16/.

Private Blockchain

Private Blockchains sind mit Intranet-Lösungen vergleichbar

In einer privaten Blockchain ist der Ledger nicht öffentlich zugänglich. Die Zugriffsrechte bzw. Berechtigungen werden von einer oder mehreren zentralen Instanzen verwaltet. Dabei können die Lese- und Schreibrechte beliebig vergeben werden. Der Unterschied zwischen privater und öffentlicher Blockchain ist auch eine Frage des Grades der Dezentralisierung und der Gewährleistung von Anonymität /CUB-101 15/. So können private Blockchains beispielsweise für firmeninterne Zwecke genutzt werden, auf welche nur ein ausgewählter Personenkreis Zugriff hat. In der Regel sind private Blockchain-Anwendungen auch „permissioned“ d. h. nur ausgewählte Teilnehmer dürfen Transaktionen validieren.

Der Vorteil privater Blockchains ist, dass Änderungen und Updates einfacher durch die wenigen Entscheider beschlossen und durchgeführt werden können (Governance). Auch besteht die Möglichkeit, eine Kette enden zu lassen und eine Neue zu beginnen oder die beteiligten Akteure namentlich zu kennzeichnen. Private Blockchain-Lösungen kommen häufig zum Einsatz, um Anwendungsfälle in einer sicheren Umgebung zu testen, bevor sie in einer öffentlichen Blockchain zur Anwendung kommen. Auch werden sie häufig innerhalb von Unternehmen eingesetzt (vgl. Intranet).

Der Nachteil privater Blockchain-Lösungen ist, dass diese in der Regel (v. a. firmenintern) durch weniger Teilnehmer aufrechterhalten werden. Dies verringert Sicherheits- und Verfügbarkeitsaspekte, welche in Public Blockchains aufgrund der großen Anzahl an Validatoren und der vorhandenen Redundanz der Daten gewährleistet werden.

Konsortial-Blockchain

Konsortiale Blockchains sind private Blockchains mit mehreren juristischen Personen

Die Konsortial-Blockchain stellt eine Sonderform der private Blockchain dar. Während bei einer reinen private Blockchain die validierenden Knoten nur von einer juristischen Person betrieben werden, ist diese Aufgabe im Falle einer Konsortial-Blockchain auf ein Konsortium von mehreren Organisationen im Netzwerk verteilt. Typischerweise wird der Konsens bei dieser Blockchainvariante durch einen Mehrheitsentscheid der autorisierten Teilnehmer erzielt.

Der Anonymitätsgrad ist aufgrund der Zugangsbeschränkung grundsätzlich geringer als bei öffentlichen Blockchains. Auch die Governance-Problematik ist ex ante lösbar, indem feste Regeln für Updates und Änderungen an der Struktur gewählt werden (z. B. Mehrheitsprinzip im Konsortium). Konsortiale Blockchains können zum Beispiel für Transaktionen und Prozesse zwischen Unternehmen genutzt werden.

Grundsätzlich lässt sich festhalten, dass die Vorteile hinsichtlich Sicherheit und Vertrauen einer Blockchain mit steigender Zahl von sich am Konsens beteiligenden Akteuren (Validatoren) wachsen. So wird mehr Vertrauen geschaffen, Manipulationssicherheit und Dezentralisierung werden besser gewährleistet. Aufgrund des notwendigen

Mehrheitsentscheides gestaltet es sich jedoch schwierig, nachträgliche Änderungen an der Architektur durchzusetzen oder fälschlich durchgeführte Transaktionen, nutzerseitige Verluste von „Accountinformationen“ oder nutzerseitige Hacks rückgängig zu machen. Auch wird mit steigender Größe des Netzwerks die Skalierbarkeit zunehmend zur Herausforderung (Details siehe Kapitel 3.3).

Hybride Blockchain

Hierbei handelt es sich um eine Mischform von privater und öffentlicher Blockchain. Eine hybride Blockchain verfügt über eine öffentliche und eine private Ebene, wobei mit der öffentlichen Ebene mehrere private Blockchains verbunden sein können. Transaktionen können sowohl auf öffentlicher Ebene als auch auf privater Ebene durchgeführt werden, wobei sie im ersteren Fall für alle Teilnehmer im zweiten nur für die Teilnehmer an der privaten Ebene einsehbar sind. Die privat durchgeführten Transaktionen können abhängig von der Konfiguration zusätzlich über eine Transaktion auf öffentlicher Ebene abgesichert werden, die jedoch nur einen Existenznachweis der privaten Transaktion enthält und keinen Einblick in deren Inhalte gibt. Die Teilnahme am öffentlichen Netzwerk ist frei, die am privaten Teil auf bekannte Teilnehmer restringiert.

Hybride Blockchains sind Mischformen aus privaten und public Blockchains

Tabelle 3-1 zeigt die Unterschiede der drei häufigsten Ausprägungsarten tabellarisch auf.

Tabelle 3-1 Unterschiede zwischen den Ausprägungsarten der Blockchain-Technologie in Anlehnung an /BDEW-101 17/

Bewertung	Public permissionless	Konsortial permissioned	Private permissioned
Vorteile	Allgemein zugänglich, diskriminierungsfrei	Zugangsform frei wählbar	Zugang beschränkt
	Pseudonymisiert bzw. anonymisiert	Personalisierbar	Personalisierbar
	Kein single point of failure	Mehrere Teilnehmer	Nutzung für Spezialanwendungen
	Hohe Manipulationssicherheit	Höhere Transaktiongeschwindigkeit	Transparenz nur für ausgewählten Teilnehmerkreis
	Transparenz durch offene Transaktionshistorie	Transparenz nur für ausgewählten Teilnehmerkreis	Hohe Transaktionsgeschwindigkeit
	Keine zentrale Speicherung von Zugangsdaten	Account-Wiederherstellung möglich	Account-Wiederherstellung möglich
	Geringe Eintrittsbarrieren	Einfache Governance	Einfache Governance
Nachteile	Governance-Problematik	Geringere Governance-Problematik	single point of failure
	Keine klaren juristischen Verantwortlichkeiten	Klare juristische Verantwortlichkeit	Klare juristische Verantwortlichkeit
	Irreversibilität irrtümlicher/inkorrekter Transaktionen	Reversibilität irrtümlicher/inkorrekter Transaktionen ggf. durch Mehrheitsbeschluss	Reversibilität irrtümlicher/inkorrekter Transaktionen durch zentrale Instanz
	Account-Wiederherstellung nicht möglich	Größere Machtkonzentration aufgrund weniger Teilnehmer	Sehr hohe Machtkonzentration aufgrund zentraler Instanz
	Transaktionsgeschwindigkeit durch Mehrheitsprinzip limitiert		Zugangsbeschränkung (vs. Diskriminierungsfreiheit)
	Ggf. ressourcenintensiv (abh. von Konsens-Mechanismen)		
	Monetärer Anreiz für Mining nötig		

Die nachfolgenden Kapitel stellen die der Blockchain-Technologie zugrundeliegenden Sicherheits-, Kryptographie- und Hashing-Mechanismen dar, welche einen signifikanten Beitrag zu den Sicherheitsaspekten dieser Technologie beitragen.

3.2 Detaillierte Technologiebeschreibung

Das nachfolgende Kapitel beschreibt die Funktionsweisen und Bausteine der Blockchain-Technologie(n) am Beispiel der bekanntesten, aktuell vorhandenen Beispiele (v. a. Bitcoin und Ethereum). Dabei werden zudem relevante Projekte zur Lösung bestehender Herausforderungen aufgezeigt und im Anschluss Funktionalitäten und Unterscheidungsmerkmale dargestellt.

3.2.1 Kryptographie & Hashing

Die Blockchain-Technologie verbindet die transparente Abwicklung von Transaktionsprozessen, basisdemokratische Elemente mittels Konsens-Mechanismen sowie dezentralisierte und verteilte Datenbanksysteme. Um trotz dieser transparenten Eigenschaften ein hohes Maß an Manipulationssicherheit zu erreichen, kommt eine Reihe von Mechanismen zum Einsatz, welche die Sicherheit gewährleisten und im Folgenden näher beleuchtet werden.

3.2.1.1 Hashing

Hashing ist ein integraler Bestandteil jeder Blockchain-Lösung.

Hashfunktionen sind Programme, welche komplexe und umfangreiche Input-Werte – zum Beispiel eine Transaktion in der Blockchain – durch eine eindeutige Prüfsumme (Hashwert) mit fester Länge ausdrücken. Eine Änderung im Input-Wert führt zu einer anderen Prüfsumme (auch „digital fingerprint“), so dass jedem Input ein individueller Hash zugeordnet werden kann. Dabei ist entscheidend, dass es der Hashwert nicht erlaubt, die Input-Datei zurück zu errechnen. Die Funktion ist eine Einwegfunktion und somit so gut wie unumkehrbar. Bekannte Hash-Funktionen sind u. a. SHA („Secure Hash Algorithm“) /UOC-101 04/, /MERK-101 01/, welcher auch in der Bitcoin-Blockchain als SHA-256 verwendet wird /NAKA-101 08/, und KECCAK-256, wie er in Ethereum genutzt wird /ETHC-101 14/. In Abbildung 3-5 ist eine Hash-Funktion dargestellt.

Hashing

Unter **Hashing** wird die Umrechnung von Input-Werten variabler Länge in einen Hash fixer Länge bezeichnet. Von einem Hash kann nicht auf den zugrunde liegenden Input rückgeschlossen werden.

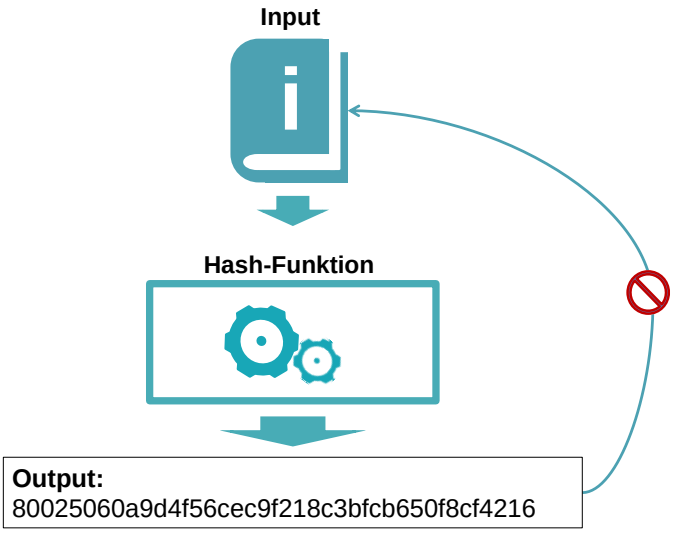

Abbildung 3-5 Schematischer Ablauf eines Hash-Vorgangs

Um als sicher zu gelten, müssen Hash-Funktionen die folgenden Bedingungen erfüllen:

Hash-Funktionen können stark und schwach Kollisions-resistent sein.

1. **Kollisionsresistenz**: Die Wahrscheinlichkeit, dass verschiedene Inputs denselben Hashwert erzeugen, geht gegen Null. Somit ist es praktisch unmöglich zwei Input-Werte zu finden, welche denselben Output erzeugen.
2. **Preimage-Resistenz**: Aus einem Hash ist es praktisch unmöglich, die bzw. eine zugrundeliegende Information (vgl. 1.) ohne erheblichen und vertretbaren Aufwand zu errechnen („one-way-function“).
3. **Second-Preimage-Resistenz**: Zu einem Hashwert soll es praktisch unmöglich sein, eine Information, welche denselben Hashwert ergibt, zu konstruieren.
4. **Deterministisch**: Derselbe Input muss immer denselben Hash generieren.
5. **Effizient und schnell**: Ein Hash muss schnell berechnet werden können, um einen effizienten Einsatz zu gewährleisten /UOC-101 04/, /MERK-101 01/, /BSI-101 15/, /TUI-101 14/.

Hashing kommt u. a. beim Vergleich großer Daten-mengen zum Einsatz.

Hashing-Mechanismen spielen eine zentrale Rolle in der Blockchain. So wird beispielsweise jeder Block und jede Transaktion in einen Hash umgewandelt. Auch die Verknüpfung zwischen den Datenblöcken erfolgt dadurch, dass der Hash des vorherigen Blockes mit in den Hash des aktuellen Blockes einbezogen wird. Dies garantiert, dass Änderungen innerhalb eines beliebigen Blocks der Kette die Hash-Werte dieses Blocks verändert und somit die Verbindung zum nächsten Block unterbricht (da die Verknüpfung nicht mehr stimmt). Alle anderen Knoten im Netzwerk können so manipulierte Ketten schnell und effizient unterscheiden.

Zum Hashing größerer Datenmengen (z. B. tausender Transaktion) kommen zudem sogenannte Merkle Trees zum Einsatz.

Merkle Trees

Bei Merkle Trees handelt es sich um eine nach Ralph C. Merkle benannte Logik, große Datenmengen überprüfbar und sicher zu speichern. Dabei werden die Hashes einzelner Transaktionen eines Blocks sukzessive zu einem einzigen Hash kombiniert. Diese Logik ermöglicht es, Rechenleistung zu sparen und die zu versendende Datenmenge so gering wie möglich zu halten /MERK-101 98/. So kann nach /NAKA-101 08/ die Blockchain beibehalten werden, obwohl nicht in jedem Knoten alle Daten aller vergangenen Transaktionen vorgehalten werden müssen. Es ist vollkommen ausreichend, den sogenannten „block header“ (bestehend aus dem Hash des vorhergehenden Blocks, dem Nonce-Value und dem Merkle Root aller Transaktionen) der längsten Kette abzuspeichern. Gerade bei dezentralen, kleinen Teilnehmern mit wenig Speicherplatz ist dies vorteilhaft, während große Teilnehmer als sogenannte „Archival Nodes“ alle Daten speichern. Mittels der Hashwerte kann jedoch jeder im Netzwerk beteiligte Akteur die Validität der Daten z. B. von archival nodes bewerten. /NAKA-101 08/

Durch Merkle-Root-Hashes muss nicht jeder Knoten alle Daten speichern.

Der Block Header beinhaltet alle wichtigen Informationen eines Blocks.

Typen von Knoten (engl. Nodes)

Bei „Full Nodes“ handelt es sich um Knoten im Blockchain-Netzwerk, welche sich an die gemeinsamen Regeln halten, Transaktionen und Blöcke validieren und so einen Beitrag zur Sicherheit und Integrität des Netzwerkes leisten. Dafür ist nicht das Vorhalten der gesamten Transaktionshistorie notwendig (vgl. Archival Node).

„Archival Nodes“ sind Knoten, welche die gesamte Transaktionshistorie des gesamten Blockchain-Netzwerkes vorhalten und die gewünschten Informationen auf Anfrage von anderen Knoten hochladen.

„Light Nodes“ oder „Lightweight Nodes“ halten nicht die gesamte Transaktionshistorie der Blockchain vor. Stattdessen werden hier lediglich die „block header“ vorgehalten. Dadurch sind sie einfach einzurichten und auch auf Geräten mit wenig Speicherplatz oder Rechenkapazität nutzbar. Light Nodes sind jedoch auf die Existenz von Full Nodes angewiesen, da sie selbst nicht aktiv am Konsens-Mechanismus teilnehmen.

Der Vorteil an Merkle Root Hashes ist, dass problemlos einzelne Transaktionen transparent im Nachgang überprüft werden können. Statt die gesamte Information (= alle Transaktionen) überprüfen zu müssen, ist es ausreichend, den Ast der zu überprüfenden Transaktion zu validieren.

Eine schematische Darstellung eines Merkle Trees ist Abbildung 3-6 zu entnehmen. Die Abbildung zeigt die baumartige Struktur auf, welcher einzelne Transaktionen (T_1 bis T_n) hashed und deren Hashes erneut so lange in neuen Hashes kombiniert, bis repräsentativ für alle Transaktionen ein einziger Hashwert entsteht (Merkle Root Hash).

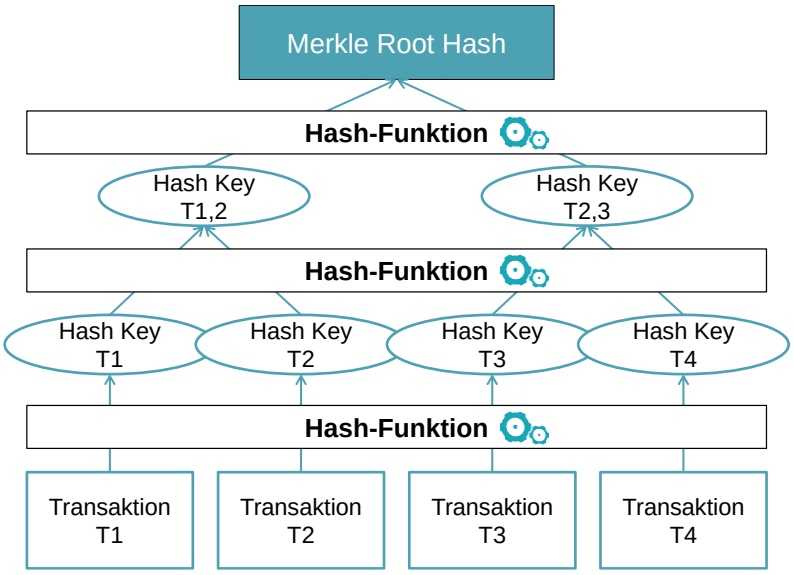

Abbildung 3-6: Merkle Tree nach /NAKA-101 08/

Durch Merkle Trees können u. a. Manipulationen schnell erkannt werden.

Erfolgt eine Manipulation innerhalb einer einzigen Transaktion (z. B. Transaktion T_2), ändern sich die Hashwerte bis hin zum Merkle Root Hash. Andere Knoten im Blockchain-Netzwerk erkennen diese Manipulation, da die Hashes nicht mehr mit den Hashes der mittels des Konsens-Mechanismus validierten Hauptkette der Mehrheit im Netzwerk übereinstimmt. Die manipulierte Kette wird vom Netzwerk ignoriert.

3.2.1.2 Kryptographie

Die Blockchain-Technologie bedient sich neben Hashing auch asymmetrischer Verschlüsselung zur Sicherung der Integrität von Daten und Identitäten.

Symmetrische Verschlüsselung beinhaltet die Problematik, dass beide an einem verschlüsselten Informationsaustausch beteiligte Akteure den zur Ver- und Entschlüsselung notwendigen Schlüssel (key) parallel zur Transaktion austauschen müssen. Dies birgt jedoch das Risiko, dass Dritte den Schlüssel abfangen können und damit Zugriff auf die Informationen erhalten. Asymmetrische Verschlüsselung hingegen ist insofern vorteilhaft, da die Schlüssel zum Ver- und Entschlüsseln unterschiedlich sind und demzufolge nicht ausgetauscht werden müssen. /SU-101 76/

Asymmetrische Verschlüsselung ist ein wichtiges Sicherheitselement.

Asymmetrische Verschlüsselung

Bei public-/private-key-Verschlüsselung werden für die Ver- und Entschlüsselung unterschiedliche Schlüssel benötigt. Damit wird in der Regel sichergestellt, dass nur die an der Transaktion beteiligten Akteure die Informationen entschlüsseln können. Diese Form der Verschlüsselung wird als „asymmetrische Verschlüsselung“ bezeichnet.

In vielen Anwendungsfällen wird eine asymmetrische Verschlüsselung nur genutzt, um einen symmetrischen Schlüssel auszutauschen (vgl. Diffie-Hellman-Schlüsselaustausch), über den in Folge die bidirektionale Kommunikation sensitiver Daten erfolgt. Da symmetrische Verschlüsselungsverfahren (z. B. AES) schneller ausführbar sind als asymmetrische Verfahren, bietet diese hybride Kombination die Vorteile aus beiden Systemen. Eine schematische Darstellung der Verschlüsselungsarten ist Abbildung 3-7 zu entnehmen.

Asymmetrische Verschlüsselung erlaubt digitale Signaturen.

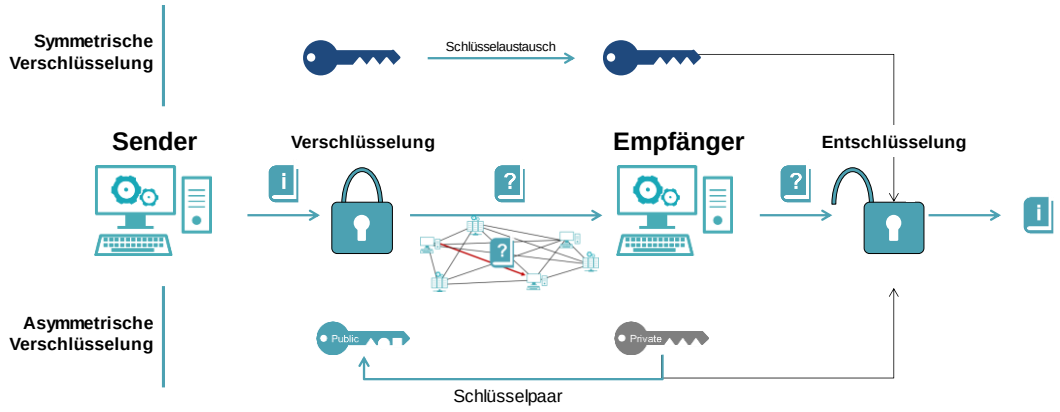

Abbildung 3-7: Symmetrische und asymmetrische Verschlüsselung im Vergleich

Weiterführendes Wissen: Mathematische Grundlagen der Verschlüsselung

Die asymmetrische Verschlüsselung basiert auf der Tatsache, dass gewisse Prozesse einfach und schnell in die eine Richtung berechenbar sind, in die andere Richtung der Zeitaufwand jedoch überproportional steigt. Für diese sogenannten Einwegfunktionen werden häufig diskrete Exponentialfunktionen verwendet. Deren Umkehrfunktion (diskreter Logarithmus) ist nur durch sehr ineffiziente Algorithmen mit viel Zeit und Ressourcenaufwand lösbar. /SUC-101 00/

Da in der Blockchain transparent alle Daten (auch der Transaktion) von allen im Netzwerk beteiligten Knoten mitgelesen werden müssen, um deren Validität zu bestätigen, wird hier auf eine Verschlüsselung der Transaktionsinhalte generell verzichtet.

Beliebte Passwörter sind heute u.a. hallo, passwort, schalke04, qwertz, passwort123.

Eine weitere Herausforderung stellt die Authentifizierung von Nutzern dar. Um Zugangsdaten stärker zu sichern und aufgrund der Dezentralität ist die Nutzung von Benutzeraccounts mit Passwörtern in einer Blockchain nicht zielführend. In einem dezentralen System müssten diese in irgendeiner Form gespeichert werden und könnten mittels Brute Force („trial and error“) lokal von jedem Teilnehmer geknackt werden. Da die von Nutzern gewählten Passwörter in der Regel nicht über die notwendige Komplexität verfügen, wären alle Konten mit gleichen Passwörtern (vgl. passwort123) unsicher.

Asymmetrische Verschlüsselung statt Passwörtern und Benutzernamen

Aus diesen Gründen wird die public-/private-key-Verschlüsselung in der Blockchain-Technologie nicht zur Verschlüsselung von Transaktionsinformationen genutzt, sondern als „Sicherung“ der Zugangsdaten und als Verifikation des Besitzes von digitalen Assets in der Blockchain mittels digitaler Signaturen. Statt einen Benutzernamen und ein Passwort durch den Nutzer festlegen zu lassen, wählt der Nutzer einen willkürlichen private key aus 2^{256} möglichen Zahlenkombinationen aus, aus welchem in Folge ein zugehöriger public key durch eine Einwegfunktion errechnet werden kann.

Der public key wird in eine Adresse (vgl. Kontonummer) umgewandelt

Dieser public key wird wiederum in eine Adresse umgewandelt („public address“) und kann ähnlich wie eine Kontonummer genutzt werden, um Transaktionen dorthin zu adressieren. Der private key ist dementsprechend die einzig nötige Zugangsinformation für Nutzer.

Die public-/private-key-Verschlüsselung wird also in der Blockchain zur Authentifizierung von Benutzern genutzt.

Weiterführendes Wissen: Verlust des private Key

Während auf klassischen Webservern das Wiederherstellen oder Zurücksetzen von verlorenen Accountinformationen in der Regel durch den zentralen Server möglich ist, ist dies in Blockchain-basierten Systemen nicht möglich. Der Verlust des private keys ist nicht rückgängig zu machen. Zum Speichern und zur Verwaltung von private keys werden verschiedene Formen von sog. „Wallets“ genutzt. Der „private key“ kann dort über einen Wallet-Anbieter meist hinter einer herkömmlichen Benutzernamen-Passwort-Wall hinterlegt werden. Somit ist der Zugang indirekt wiederherstellbar.

Zur Erstellung eines Schlüsselpaares auf einer Blockchain wird in der Regel die sogenannte „elliptic curve cryptography“ angewandt. Das Vorgehen dieses Systems ist im nachfolgenden Kapitel kurz aufgeführt.

Elliptic Curve Kryptographie (ECC)

Elliptische Kurven sind sehr sichere und schnelle Einwegfunktionen.

Public und private keys zur asymmetrischen Verschlüsselung werden mittels der „Elliptic Curve Cryptography“ erstellt, da dieses System relativ schnell und einfach durchführbar ist und sich als nicht rückrechenbar erwiesen hat. Das Verfahren soll im Folgenden vereinfacht veranschaulicht werden.

Eine elliptische Kurve errechnet sich mit Formel (1) nach /IBM-101 86/.

$$y^2 = x^3 + ax + b \ (\mathrm{mod\ p}) \qquad (1)$$

Eigenschaften dieser Kurven sind unter anderen, dass sie immer horizontal symmetrisch zur x-Achse verlaufen und eine nicht-vertikale Linie die Kurve maximal an drei Punkten schneidet. Diese Eigenschaften werden genutzt, um public und private keys zu generieren.

Viele Blockchain-Anwendungen nutzen diese Form der Verschlüsselung, welche durch ein internationales Konsortium („standards for efficient cryptography group“) stetig weiterentwickelt wird /CERT-101 09/. Dieses Konsortium stellt Informationen hinsichtlich relevanter Parameter der Kurve in /CERT-101 10/ dar.

$$T = (p, q, b, G, n, h) \quad (2)$$

p	Primzahl und Definition eines finiten Feldes F_p
a, b	Elemente des finiten Feldes und Teil der Beschreibung der elliptischen Kurve
G	Basispunkt G = (x_G, y_G) in F_p
n	Primzahl, zur Bestimmung der Ordnung von G
h	Cofaktor

Detaillierte Informationen zu Formel 2 sind /CERT-101 09/ zu entnehmen. In der ECC kommen zwei Funktionen zur Anwendung, welche als „Point Addition“ und „Point Doubling“ bezeichnet werden. Diese mathematischen Operationen sind jedoch nicht mit algebraischen Operationen (vgl. Multiplikation und Addition) zu verwechseln, sondern beschreiben spezielle mathematische Vorgänge in einer elliptischen Kurve.

Point Addition (G≠Q)

In elliptischen Kurven ist es möglich, zwei Punkte G und Q auf der Kurve miteinander zu verbinden, welche wiederum einen dritten Punkt der Kurve (-R) schneiden. Details sind **Abbildung 3-8** zu entnehmen. Der Punkt -R kann an der X-Achse gespiegelt werden und generiert den Punkt R. /CERT-101 09/

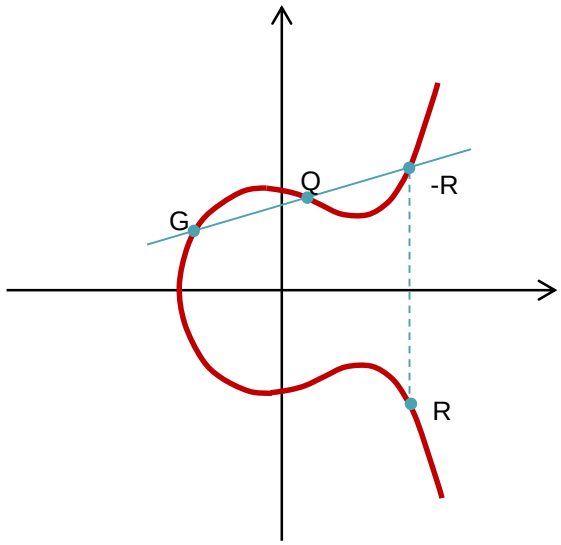

Abbildung 3-8: Beispielhafte „point addition“ in einer elliptische Kurve mit den Parametern G, Q und R

Point Doubling (P=Q)

Werden die Werte von G und Q gleichgesetzt, entsteht eine Tangente an Punkt G, welche wiederum die elliptische Kurve schneidet und erneut einen Schnittpunkt –R sowie dessen Spiegelbild (R) erzeugt. /CERT-101 09/

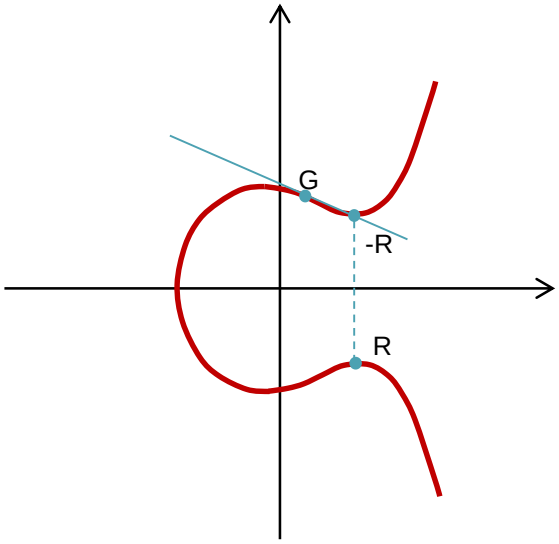

Abbildung 3-9: Beispielhafte „point doubling“ in einer elliptische Kurve mit den Parametern G, Q und R mit P=Q

Ein public key kann nun auf Basis eines private keys erzeugt werden, indem die beschriebenen Funktionen „point addition“ und „point doubling“ auf Basis des Punktes G (allgemein bekannt) und des jeweils willkürlich gewählten „private keys[2]“ wiederholt ausgeführt werden (vgl. **Formel (3)**). Dieses Verfahren ist in **Abbildung 3-10** dargestellt.

$$nG = E \tag{3}$$

G:	Generator Point (allgemein bekannt)
E	public key
n	Anzahl der Kombinationen auf Basis des private keys

Der public key ist das Ergebnis vieler Operationen auf der Elliptischen Kurve.

Der public key (hier E) beschreibt das Endergebnis dieser Operationen – jedoch sind die Anzahl und Reihenfolge bis zu diesem Punkt nicht bekannt. Daher gestaltet sich eine Rekonstruktion bis hin zum private key ausgehend vom public key als nicht durchführbar.

[2] Die Reihenfolge und Anzahl der Operationen bestimmt sich anhand der 0/1 bei binärer Schreibweise des private keys

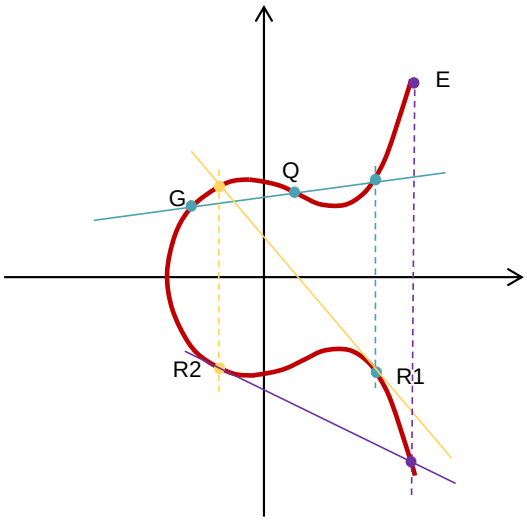

Abbildung 3-10: Kombination aus einer Point Addition und zweifachem Point Doubling (schematisch)

Dies ist eine sehr sichere und schnelle Möglichkeit, ein Schlüsselpaar zu generieren, da mit steigender Ausführungsanzahl der Rechenoperationen die Rechenzeit für die Rekonstruktion überproportional steigt, die Funktionen selbst jedoch sehr schnell und mit geringer Rechenzeit ausführbar sind.

private key

In der Regel wird für einen neuen Nutzer auf einer Blockchain ein private key zufällig generiert (z. B. auf www.bitaddress.org). Dabei ist die Zahl möglicher zufälliger private keys so hoch, dass die Wahrscheinlichkeit zweier Nutzer, den gleichen private key zu erhalten, der Wahrscheinlichkeit von $\frac{1}{Anzahl\ möglicher\ private\ keys}$ entspricht. Im Falle von Bitcoin ist die Wahrscheinlichkeit, dass zwei Nutzer die gleichen private keys erhalten bei ca. $\frac{1}{2^{256}}\ bzw.\ \frac{1}{1{,}16*10^{77}}$.

Vergleich:
Der Planet Erde besitzt ~ 10^{50} Atome, die Milchstraße ~ 10^{68} Atome

Viele Wallets bieten zudem die Möglichkeit, auf Basis des ursprünglichen private keys („seed“) für jede Transaktion über den determinierten Rechnungspfad ein neues Schlüsselpaar zu generieren, so dass die Anonymität zusätzlich gesteigert wird.

Beispiel (Bitcoin):

- Komprimiert: 13rZKpYpg4gCEzfWGxAqktUDu97gE4LLVH
- Hexadezimal: 40F6A5E198FD9D5BC91B106D49F04BF1DFB8BD821DAC036416CB3D604F32DCD9
- Base64: QPal4Zj9nVvJGxBtSfBL8d+4vYIdrANkFss9YE8y3Nk

public key

Mittels des zufällig gewählten privaten Schlüssels kann durch die Elliptic-Curve-Kryptographie ein eindeutiger public key generiert werden, der als Grundlage für die public address dient. Ankommende Transaktionen, welche mit dem public key verschlüsselt wurden, können lediglich mit dem nur dem Nutzer bekannten private key entschlüsselt werden, so dass die Informationen nicht von Dritten entschlüsselt werden können.

Beispiel (Bitcoin): 03C81EABC9B6A08EF92C7C1306AADF215D474233193E1BA94D59C46C16A4271910

public address

Die public address ist mit einer IBAN bzw. Kontonummer zu vergleichen

Der public key dient als Basis für die public address. Dafür wird in der Bitcoin-Blockchain der public key mehrfach gehashed und weitere hashing Operationen[3] durchgeführt. Dafür kommt u. a. die Hashfunktion „RIPEMD“ und die „Base58[4]“ Kodierung zum Einsatz. Die public address dient als zusätzlicher Schutz des private key. Während der public key eines Nutzers erst offen gelegt wird, wenn dieser eine Transaktion aktiv anstößt, ist die public address eine zusätzliche Sicherheitsschicht. Mit dem Besitz des private keys kann über die elliptischen Kurven und diverse Hash-Funktionen auch eindeutig der Besitz der public address nachgewiesen werden. Grundsätzlich wäre diese Sicherheitsvorkehrung nicht nötig. Sollte jedoch beispielsweise die Kryptographie hinter elliptischen Kurven oder eine Hash-Funktion kompromittiert werden, sind digitale Assets weiterhin sicher, da der public key niemandem außer dem Besitzer des private key bis dahin bekannt ist und die anderen Funktionen weiterhin sicher sind.

Beispiel (Bitcoin): 192jSxCSoPSXHvJpk3vroEFk3z9GS2JDxj

Eine Abbildung aller Zusammenhänge der Schlüssel (im Bitcoin-Netzwerk) ist Abbildung 3-11 zu entnehmen:

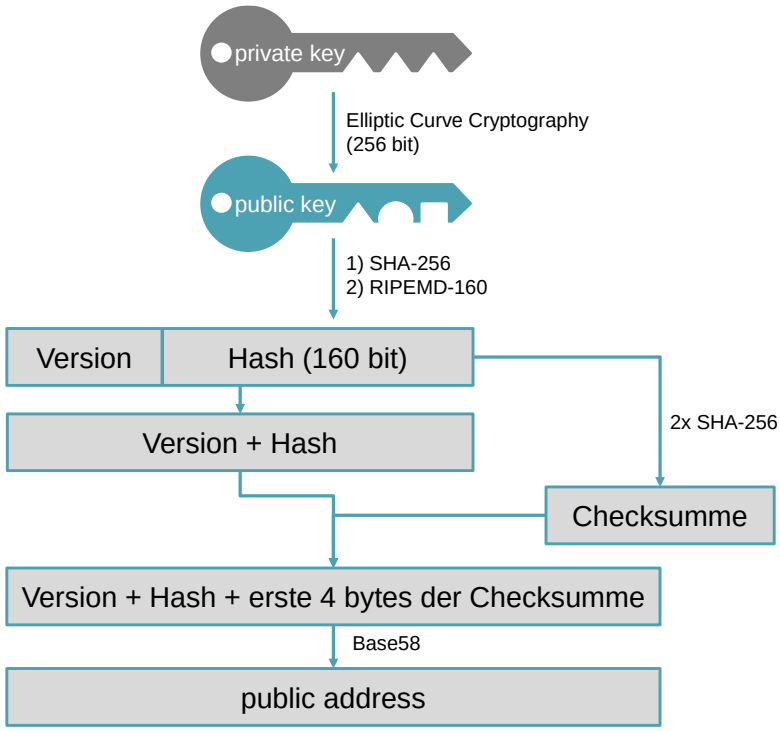

Abbildung 3-11: Zusammenhang der Schlüssel und Adressen am Beispiel des Bitcoin-Netzwerks nach /BIT-01 17/

[3] Details zu den durchgeführten Operationen im Bitcoin-Netzwerk sind im BitcoinWiki zu finden
[4] Base58 nutzt nur verwechslungsfreie alpha-numerische Zeichen und vermeidet so Verwechslungen unabhängig von der Schriftart.

Multi-Signatur-Adressen

Während in der Regel ein einzelner private key für jeden Nutzer ausreichend ist, können auch sogenannte Multi-Signature-Adressen(MultiSig) aus mehreren private keys erstellt werden. Dies ermöglicht es beispielsweise, dass eine beliebige Anzahl der ausgewählten Schlüssel (bzw. deren Signatur) für eine Transaktion erforderlich ist. Diese die Sicherheit weiter steigernde Maßnahme kann zudem genutzt werden, um Transaktionen zwischen zwei Parteien treuhänderisch durch einen neutralen Dritten überwachen und ggf. über die Abwicklung einer Zahlung entscheiden zu lassen. Auch können durch MultiSig private keys an verschiedenen Orten gespeichert werden, um das Risiko eines unbefugten Zugriffs und das Entstehen eines nutzerseitigen „single point of failure“ zu verringern oder Transaktionen nur mittels Mehrheitsentscheidung zu ermöglichen. /UB-101 14/

Beim sog. „Parity-Hack“ wurde ein Programmierfehler in MultiSig genutzt, um über 150 000 Ether zu entwenden

Es ist weiter denkbar, vertrauenswürdigen Dritten mittels MultiSig die Möglichkeit zu gewähren, Transaktionen zu prüfen und ggf. Betrug zu verhindern. Der Nutzer kann sich trotz der Verweigerung des Dritten über dessen Entscheidung hinwegsetzen, da er z. B. die notwendige Mehrheit der notwendigen private keys besitzt und die letztendliche Entscheidungshoheit nicht aus der Hand gegeben wird. /BBL-101 14/

Weiterführendes Wissen: Wallets

*Wallets sind ein PIN bzw. passwortgeschützter **Zugang zum „private key“**. Die Wallet ist kein Geldspeicher, sondern lediglich ein „pinpoint“ zum „private key“, über welche die Information des Kontostands aufgerufen und Transaktionen durchgeführt werden können. Allerdings kann der Begriff Wallet auch für eine Software stehen, die die private keys des Benutzers managt. In diesem Fall sind die „private keys“ meist auf den Servern des Softwareanbieters gespeichert.*

Digitale Signaturen

Eine digitale Signatur wird genutzt, um dem Empfänger einer Transaktion zu gewährleisten, dass die erhaltenen Informationen zwischen den partizipierenden Akteuren nicht abgeändert wurden und tatsächlich vom Sender stammen. Dies verhindert den Missbrauch durch Dritte.

Digitale Signaturen verhindern Fälschungen von Transaktionen

Eine digitale Signatur ermöglicht den zweifelsfreien Nachweis,

- dass die Transaktion von einem bestimmten Absender stammt,
- die Inhalte der Transaktion nicht nachträglich geändert wurden
- und der Absender die Transaktion zweifelsfrei abgesendet hat.

Eine digitale Signatur entsteht, wenn der Absender einer Transaktion die enthaltenen Informationen des Transaktionsobjekts an eine Hash-Funktion übergibt, und den Hash-Code im Anschluss mit dem private key verschlüsselt (vgl. **Abbildung 3-12**). Die Signatur dient demnach dem Zweck, das Vorhandensein des privaten Schlüssels durch den Absender zu beweisen, ohne diesen selbst offen zu legen. Durch die Verknüpfung des privaten Schlüssels mit der Transaktion (und ggf. einer Zufallszahl für zusätzliche Sicherheit) ist die Signatur für jede Transaktion unterschiedlich, so dass Dritte diese nicht erneut verwenden können. /NAKA-101 08/

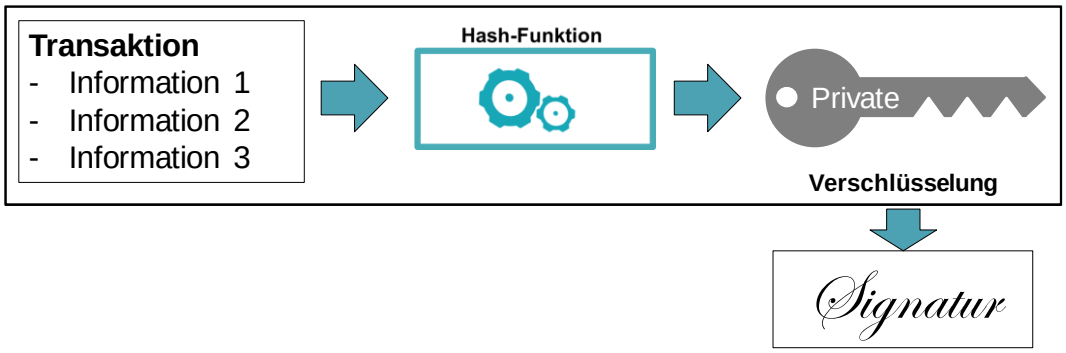

Abbildung 3-12: Schematischer Ablauf einer digitalen Signatur mit asymmetrischer Verschlüsselung

Digitale Signaturen kommen in allen Bereichen der IT-Security zum Einsatz.

Werden daraufhin die Informationen der Transaktion gemeinsam mit dem public key sowie der digitalen Signatur an den Empfänger der Transaktion via Blockchain gesendet, kann dieser mittels des public keys den verschlüsselten Hash entschlüsseln. Dies wird auch als Verifikationsalgorithmus bezeichnet. Nutzt der Empfänger die gleiche Hash-Funktion (z. B. SHA 256) wie der Sender, kann die Information in einen Hash umgewandelt und die beiden Ergebnisse verglichen werden (vgl. **Abbildung 3-13**) /CERT-101 01/.

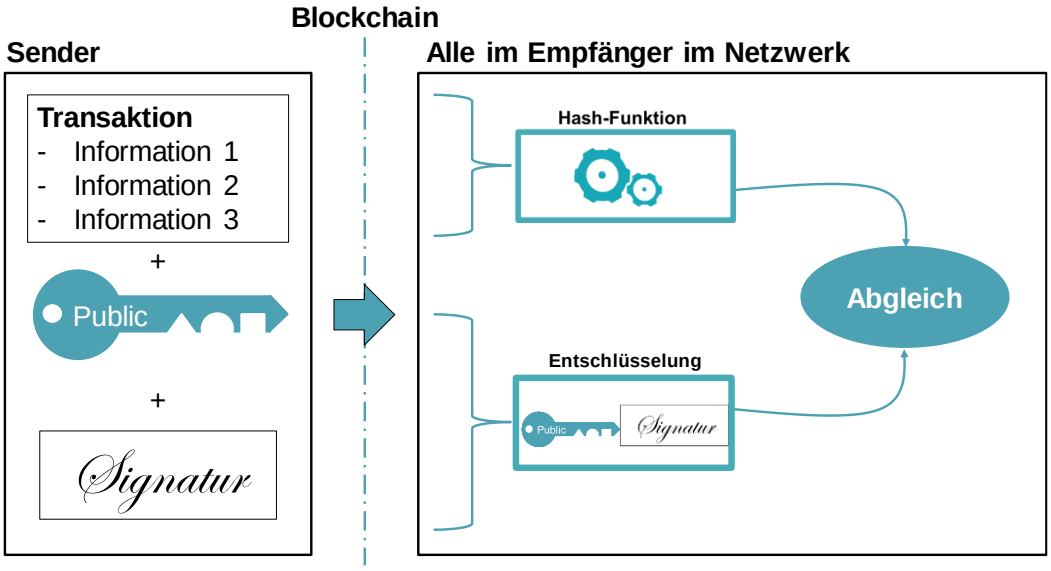

Abbildung 3-13: Schematischer Ablauf einer Transaktion mittels Signatur und asymmetrischer Verschlüsselung

Stimmen die beiden Werte überein, ist sichergestellt, dass die Informationen der Transaktion nicht manipuliert[5] wurden, während die Information selbst transparent für alle im Netzwerk einsehbar ist und jeder Teilnehmer im Netzwerk die Validität der Transaktion überprüfen kann. Diese Form der Verschlüsselung, kombiniert mit Hashing, ermöglicht es, zweifelsfrei feststellen zu können, dass der Inhalt einer Transaktion von einem bestimmten Absender stammt und gewährleistet auf diese Weise Manipulationssicherheit auf der

[5] Selbst eine geringfügig manipulierte Transaktion hätte einen anderen Hashwert zur Folge und wäre für jeden Teilnehmer im Netzwerk dadurch als solche erkennbar. Da der Manipulierende nicht im Besitz des private keys des Sendenden ist, kann die Signatur nicht gefälscht werden.

Blockchain. /CERT-101 01/ Ein Nachteil dieser digitalen Signatur ist jedoch, dass diese einen relativ großen Teil der Transaktionsvolumina und damit der Blockgröße ausmacht. /BBC-101 17/

Der in Bitcoin verwendete Algorithmus wird als ECDSA (Elliptic Curve Digital Signature Algorithm) bezeichnet. /BIT-01 17/

3.2.2 Transaktionen, Blöcke und Ketten

Während die voranstehenden Kapitel die Abläufe und Sicherheitsaspekte hinter einzelnen Transaktionen aufzeigen, ist es notwendig, die Reihenfolge der Transaktionen in der Blockchain festzuschreiben, da ansonsten die Möglichkeit des Missbrauchs besteht. Zu diesem Zweck werden alle Transaktionen innerhalb eines bestimmten Zeitraums (bei Bitcoin sind dies ca. 10 Minuten) gesammelt und durch einen sogenannten Konsens-Mechanismus an die vorherigen Blöcke angehängt.

Transaktionen

Im Bitcoin-Netzwerk existieren keinerlei Konten wie in einer herkömmlichen Bank. Stattdessen sind alle vergangenen Transaktionen öffentlich über die vergangenen Blöcke einsehbar. Ein Transaktionsobjekt (z. B. ein Bitcoin) stellt demnach nur Referenzen früherer Transaktionen dar, welche an die Hash-Werte privater Schlüssel gekettet sind. Somit erschließen sich die Kontostände/Eigentumsverhältnisse vielmehr aus der Logik aller ausgeführten Transaktionen, genannt UTXO. Nur die jeweiligen Besitzer des privaten Schlüssels sind demzufolge in der Lage, die Eigentumsverhältnisse der Transaktionsobjekte zu verändern. /JEP-101 15/

UTXO = Unspent Transaction Output

Wird eine Transaktion durch einen Sender angestoßen, enthält diese Outputs (Betrag des Transaktionsobjekts, Empfänger) sowie Inputs (Outputs früherer an den Sender referenzierter Transaktionen). Entspricht eine zu sendende Menge nicht exakt einer zuvor erhaltenen Transaktionsmenge, werden entweder mehrere Transaktionen zusammengefasst oder eine Transaktion „geteilt“ und der Rest zurück an den Absender geschickt.

Weiterführendes Wissen: UTXO

Der Begriff UTXO steht für „Unspent Transaction Output“ und ergibt sich aus der Historie aller zurückliegenden Transaktionen einer Blockchain. Nur UTXO können als Input für weitere Transaktionen genutzt werden. Die Summe aller UTXO eines Nutzers entspricht dem aktuellen „Kontostand“.

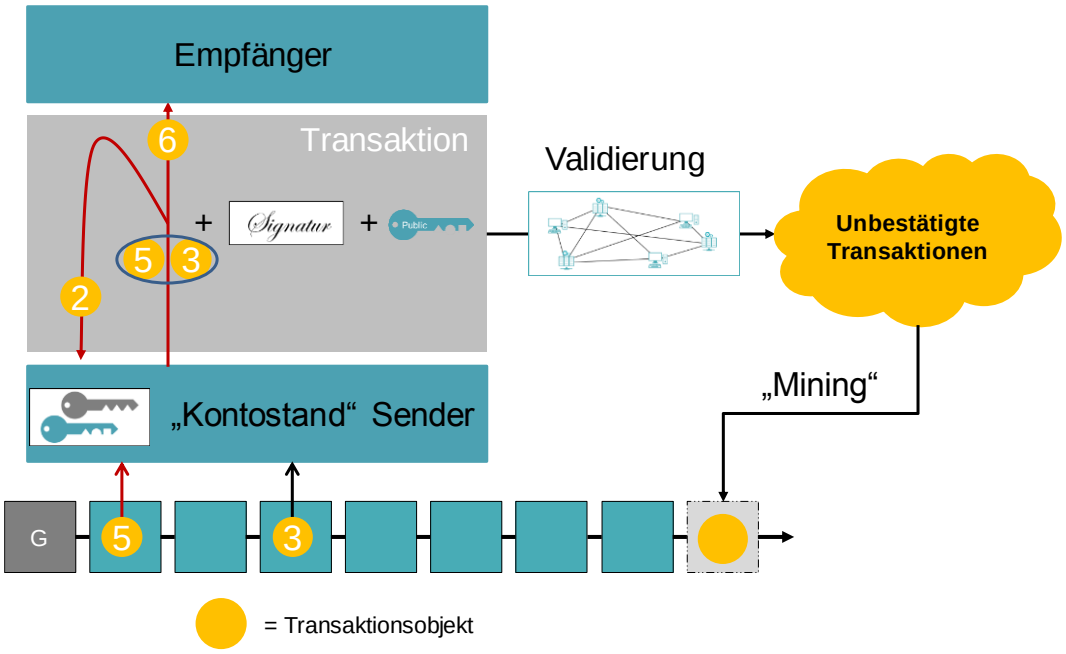

Abbildung 3-14: Schematischer Ablauf einer Transaktion

Nach /NAKA-101 08/ verläuft eine Transaktion in einer Blockchain (hier: Bitcoin) wie folgt:

1) Transaktionen innerhalb eines gewissen Zeitfensters werden an alle Knoten („Nodes“) des Bitcoin-Netzwerks gesendet[6].
2) Jeder Knoten sammelt bzw. wählt getätigte Transaktionen innerhalb des Zeitfensters, validiert diese und aggregiert sie zu einem Block.
3) Jeder Knoten führt den durch den Konsens-Mechanismus (Proof of Work bei Bitcoin) vorgegebenen Konsensalgorithmus aus.
4) Findet ein Knoten die richtige Lösung für den Block, teilt er diesen an alle Knoten mit (= “Mining“).
5) Die Knoten im Netz akzeptieren den Block, wenn alle Transaktionen darin valide sind und noch nicht zuvor ausgeführt wurden.
6) Alle Knoten akzeptieren den Block, indem sie beginnen, am nächsten Block zu arbeiten und den Hash des akzeptierten Blocks für den nächsten zu verwenden.

In einer public Blockchain kann jeder zum Node (=Knoten) werden.

Ein Knoten (engl. „node“) ist in einer Blockchain jede am Netzwerk beteiligte Recheneinheit mit gleichem Protokoll (z. B. Bitcoin). Dabei werden jedoch nicht auf jedem Knoten alle für die Blockchain essenziellen Rechenoperationen ausgeführt. Diese Knoten werden als „lightweight nodes“ bezeichnet. Knoten, welche jeden Block und jede Transaktion herunterladen und diese validieren, um den zugrundeliegenden Konsens-Mechanismus

[6] Finden innerhalb eines Zeitfensters mehr Transaktionen statt, als im Bitcoin-Netzwerk verarbeitet werden können, obliegt den Validatoren (in Bitcoin „Miner“) die Auswahl der Transaktionen für einen Block. Oft werden hier die Transaktionen gewählt, welche die höchsten Transaktionsgebühren bezahlen. Dies steht oft in der Kritik, da einerseits so die Transaktionskosten in Hochzeiten stark ansteigen und andererseits eine gewisse Form von Zensur bzw. Diskriminierung möglich ist.

anzuwenden, werden als „full nodes“ bezeichnet. Knoten, welche alle vorhandenen Daten der Blockchain speichern und anderen Teilnehmern zur Verfügung stellen, werden als „archival nodes“ bezeichnet. /BIT-01 17/

Blöcke

Ein Block in der Blockchain besteht aus verschiedenen Parametern, welche hier am Beispiel der Bitcoin-Blockchain dargestellt werden. Unter https://blockexplorer.com können alle Blöcke der Bitcoin-Blockchain eingesehen und die Transaktionshistorie bis zum ersten Block („Genesis Block“) transparent nachvollzogen werden.

Alle Blöcke öffentlicher Blockchains sind einsehbar

Tabelle 3-2: Bestandteile eines Blocks in der Bitcoin-Blockchain

Komponente	Erklärung
Number of Transactions	Anzahl der im Block enthaltenen Transaktionen
Transactions	Informationen aller Transaktionen innerhalb des Blocks
Transaction Hash	Hashes der Informationen der einzelnen Transaktionen
Block-Hash	Hash des Blocks, bestehend aus den Transaktionen des vorherigen Blocks sowie eines nonce-values
Timestamp	Zeitpunkt des Erstellens des Blocks
Difficulty	Notwendige Rechenkapazität zum Erstellen des Blocks
Previous Block	Hash des vorangehenden Blocks
Block Reward	Anzahl der Coins, die als Anreiz für das erfolgreiche Validieren an Miner ausgeschüttet werden. (Siehe Kapitel 3.2.3)
Size	Größe des Blocks in bytes
Merkle Root	Merkle Root der im Block enthaltenen Transaktionen (siehe Kapitel 3.2.1)
Nonce	Dieser Wert muss durch „Mining“ gefunden werden, um den korrekten Hash abbilden zu können.

Das folgende Kapitel erläutert die möglichen Mechanismen, nach denen die Blöcke validiert und an die Kette angehängt werden.

Ketten

Die Kette wird durch den Verweis auf den Hash des vorher-gehenden Blocks erzeugt

Wie bereits in Tabelle 3-2 aufgezeigt, sind die Blöcke einer Blockchain durch die Hashes des jeweils vorhergehenden Blockes miteinander verbunden. Wird ein einziger Wert in der Kette eines Netzwerkteilnehmers manipuliert, stimmen die Hashes des jeweiligen Blockes und damit auch aller nachfolgenden Blöcke nicht mehr mit den übrigen Teilnehmern des Blockchain-Netzwerkes überein. Dies ermöglicht es, schnell Manipulationen zu identifizieren und einen gemeinsamen Konsens über die Transaktionshistorie herzustellen.

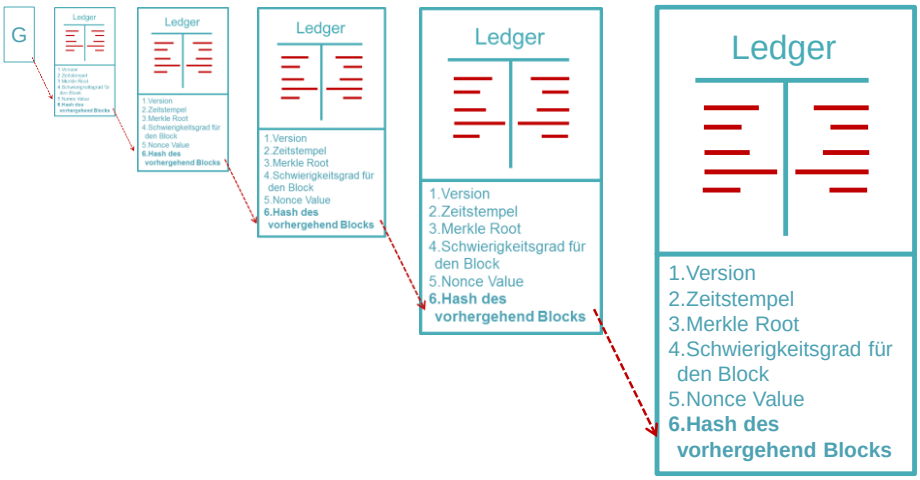

Abbildung 3-15: Verknüpfung der Blöcke zu einer Kette (Blockchain)

Weiterführendes Wissen: Forks

Der Begriff „Fork" (engl. für Gabel) beschreibt das Aufspalten einer Blockchain in verschiedene parallele Ketten i. d. R. aufgrund eines Protokoll-Updates. Nutzen nicht alle Knoten im Netz dieselbe „Software-Version" kommt es zu einem sogenannten Fork. Dabei werden die folgenden Ausprägungen unterschieden:

- ***Softfork**: unterschiedliche im Blockchain-Netzwerk verwendete Software-Versionen, die zueinander abwärts kompatibel sind und somit weiterhin miteinander kommunizieren können.*
- ***Hardfork**: die unterschiedlichen Versionen der Blockchain-Architektur können nicht mehr miteinander kommunizieren; zwei separate Stränge der Blockchain entstehen.*

Die Blöcke innerhalb eines Blockchain-Netzwerkes werden mittels sogenannter Konsens-Mechanismen gebildet. Diese Kernbestandteile der Technologie werden in den nachfolgenden Kapiteln ausführlich erläutert.

3.2.3 Konsens-Mechanismen

Der Konsens-Mechanismus einer Blockchain stellt ihren Kern und wichtigste Funktion dar. Erst durch diese Algorithmen wird letztlich sichergestellt, dass eine Transaktion ohne Intermediär zuverlässig und sicher durchgeführt wird sowie die doppelte Verwendung (double spending) von Transaktionsobjekten (z. B. digitale Währungen) unterbunden wird. Konsens-Mechanismen dienen überdies dem Zweck, Einigkeit über die Reihenfolge der getätigten Änderungen im Netzwerk zu dokumentieren und die im Protokoll festgelegten Regeln zu überwachen.

Der Konsens-Mechnismus ermöglicht erst sichere Transaktionen

Dabei sind insbesondere die folgenden beiden Herausforderungen zu bewältigen:

1) **Double Spending** bezeichnet das Problem einer möglichen doppelten Verbuchung. Dies bedeutet, dass z. B. eine Währungseinheit oder ein digitales Asset in zwei Transaktionen gleichzeitig verwendet wird. Im Blockchain-Konzept wird dieses Problem durch die zeitdiskrete Verifizierung der Transaktionen und Überprüfung durch eine Vielzahl von unabhängigen, verteilten Knoten gelöst. Dies stellt die Kerneigenschaft für den Anwendungsfall der Blockchain-Technologie als digitale Währung („Kryptowährung“) dar.
2) Als **Byzantinische Fehler** wird ein Problem bezeichnet, das beim Datenaustausch via Peer-to-Peer-Kommunikation zwischen verschiedenen Knoten auftreten kann. Dabei besteht die Möglichkeit, dass einige Knoten böswillig angegriffen werden, um die Kommunikationsinhalte zu manipulieren. Die Herausforderung für beteiligte Knoten besteht nun darin, manipulierte Informationen identifizieren zu können, um letztlich konsistente Ergebnisse mit anderen validen Knoten zu erzielen.

Die Funktion eines Konsens-Mechanismus ist es im Wesentlichen sicherzustellen, dass sich alle beteiligten Knoten auf den gleichen Block einigen und dieser als einzige valide Version akzeptiert wird. Entsprechend hängt die Sicherheit eines Blockchain-Systems grundlegend von seinem Konsensmodell ab. /PSL-01 17/, /COI-01 17/

Weiterführendes Wissen: The Byzantine Generals Problem (Byzantinischer Fehler)

Das beschriebene Problem bezieht sich auf ein Gedankenexperiment, das grundlegende Probleme in verteilten Systemen beschreibt /HAM-01 17/. Es basiert auf folgendem Konstrukt: „Mehrere Divisionen der byzantinischen Armee lagern außerhalb einer gegnerischen Stadt, jede Division wird von ihrem eigenen General kommandiert. Die Generäle können nur durch Boten miteinander kommunizieren. Sie müssen einen gemeinsamen Aktionsplan beschließen. Einige der Generäle könnten jedoch Verräter sein, die versuchen, die loyalen Generäle daran zu hindern, sich zu einigen. Die Generäle müssen einen Mechanismus haben, um sicherzustellen, dass

A. alle loyalen Generäle über denselben Aktionsplan entscheiden

Die treuen Generäle werden alle den Anweisungen des Algorithmus folgen, die Verräter aber können machen, was sie wollen. Der Algorithmus muss Bedingung A garantieren, unabhängig davon, wie die Verräter agieren. Die loyalen Generäle müssen sich ergo auf einen Plan einigen und dafür sorgen, dass

B. eine kleine Anzahl von Verrätern die treuen Generäle nicht dazu veranlassen können, einen manipulierten Plan anzunehmen.“

Die Anwendung des Problems auf Computersysteme und Lösungsansätze wurde erstmals im Jahr 1982 von Lamport, Shostack und Pease beschrieben /LAMP-01 82/.

Es besteht mittlerweile eine Reihe an unterschiedlichen Konsens-Modellen mit unterschiedlichem Entwicklungsstatus und individuellen Vor- und Nachteilen, die im Folgenden näher beschrieben werden sollen. Die aktuell wichtigsten Konzepte stellen Proof of Work (PoW), Proof of Stake (PoS) und Proof of Authority (PoA) dar (vgl. Abbildung 3-16 bzw. Kapitel 3.2.3.1, 0 und 3.2.3.3).

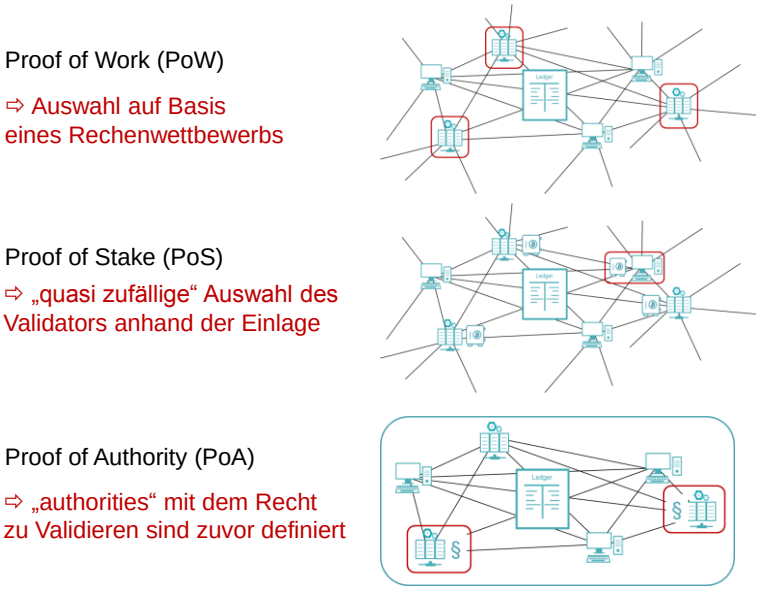

Abbildung 3-16: Vergleich der drei wichtigsten Konsensmechanismen PoW, PoS und PoA

Konsensmechanismen und Kryptowährungen

In vielen Konsensmechanismen wird die Ausschüttung von Kryptowährungen als finanzieller Anreiz zur Teilnahme eingesetzt. Grundsätzlich ist es jedoch nicht notwendig Funktionen von Kryptowährungen in eine Blockchain zu integrieren. Die Konsensmechanismen (v.a. PoW und PoA) funktionieren grundsätzlich auch ohne dieses Incentive. Vor allem in public Blockchains wird jedoch häufig ein Anreiz benötigt, um Knoten zur Teilnahme am Konsens zu bewegen. Prinzipiell kann dies aber auch auf Basis intrinsischer Motivation erfolgen. In konsortialen und privaten Blockchains ist es häufig der Fall, dass die Vorteile der Technologie für die Beteiligten gegenüber den Kosten durch den Konsens überwiegen.

3.2.3.1 Proof of Work (PoW)

Proof of Work ist der aktuell am weitesten verbreitete Konsens-Mechanismus

Proof of Work war der erste funktionierende Konsens-Mechanismus, der letztlich die Grundlage für die Umsetzung einer Blockchain geschaffen hat. Der Mechanismus wurde erstmals von „Satoshi Nakamoto“ (s. Kapitel 3.1.1) in /NAKA-101 08/ beschrieben und ist bis heute die am weitesten verbreitete Konsens-Logik. Das Grundprinzip basiert auf einem Verfahren, das den Nachweis einer Arbeit bzw. eines Aufwands durch den Teilnehmer an dem Konsensmechanismus (sog. „Miner“) nachweist. Die Kernidee ist dabei, die Verrechnungsrechte und Belohnungen durch einen Wettbewerb von Rechenleistung („Hashing-Power“) auf die Knoten zu verteilen. Im Rahmen dieses Mining-Prozesses muss ein kryptographisches Rätsel gelöst werden, das wie folgt beschrieben werden kann (vgl. Abbildung 3-17):

Aufgabe des „Miners“ ist es, die Informationen aus anstehenden Transaktionen und den vorgehenden Block mittels eines Hashing-Algorithmus (z. B. SHA-256 bei Bitcoin, s. Kapitel 3.2.1.1) in eine Zahlenkombination bestimmter Länge zu überführen. Das Ergebnis muss dabei bestimmte Vorgaben erfüllen, die wiederum die Schwierigkeit („Difficulty“) des Rätsels bestimmen. Konkret wird dies durch die Anzahl der ersten Ziffern in diesem Hash, die den Wert 0 besitzen, umgesetzt. Der „Miner“ hat hierzu lediglich die Möglichkeit, den „Nonce-Value“ als einen frei wählbaren Eingangsparameter dieses Hashing-Algorithmus zu variieren, bis sein Ergebnis die Anforderung, also die korrekte Anzahl an vorangestellten Nullen, erfüllt. Ein Zusammenhang von Eingangsparameter und Ergebnis ist dabei nicht nachzuvollziehen.

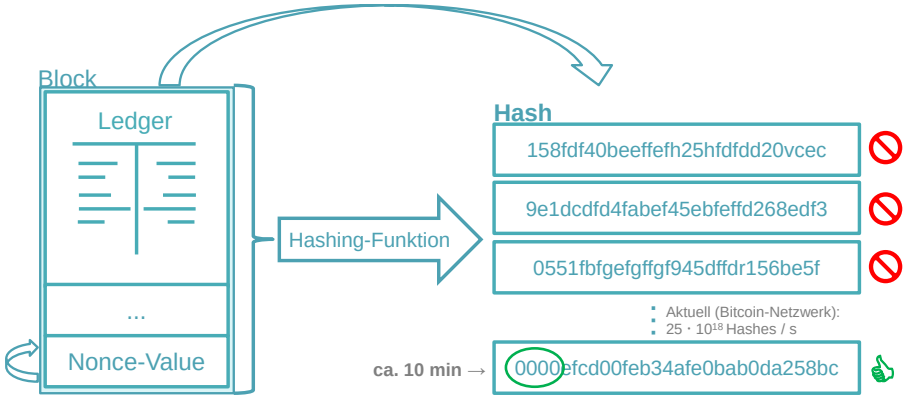

Abbildung 3-17: Proof of Work Hashing-Logik unter der beispielhaften Annahme einer sog. „Difficulty“ von vier vorangestellten „0“, die der korrekte Hash enthalten muss

Die einzelnen Berechnungsschritte erfolgen in der bei Bitcoin verwendeten Funktion namens „HashCash“ wie folgt:

1) **Abruf der Schwierigkeit**: Der Schwierigkeitswert wird (in Abhängigkeit der Hash-Rate des gesamten Netzes) durch den Bitcoin Mining Algorithmus jeweils nach der Erzeugung von 2016 Blöcken dynamisch angepasst.

2) **Sammeln der Transaktionen**: Alle offenen Transaktionen im Netzwerk werden nach der Erzeugung des letzten Blocks gesammelt. Dann wird der Merkle Root dieser Transaktionen berechnet und die Blockversionsnummer, der 256-Bit Hash-Wert des vorherigen Blocks, der aktuelle Ziel-Hash-Wert, die Nonce-Zufallszahl und andere Informationen integriert.

3) **Berechnung**: Der Nonce-Value wird von 0 bis 2^{32} variiert und der entsprechende Hash-Wert berechnet. Erfüllt der Hash-Wert die Anforderungen der Difficulty (Anzahl an vorangestellten Nullen), kann der Block gesendet werden.

4) **Neustart**: Wenn der Knoten den Hash-Wert zu einem bestimmten Zeitpunkt nicht berechnen kann, wiederholt er Schritt zwei. Wenn ein anderer Knoten die Berechnung abschließt, wird ab Schritt 1 neu gestartet. /NAKA-101 08/

Im Bitcoin-Netzwerk wird empfohlen, nach einer Transaktion 6 Blöcke abzuwarten.

Der neu erzeugte Block wird mit den vor ihm liegenden Blöcken verknüpft. Falls mehrere Miner gleichzeitig eine valide Lösung finden, kann es passieren, dass zeitweise mehrere Ketten parallel existieren. Welche Kette im Folgenden als valide verwendet wird, entscheidet sich demnach erst bei der Erstellung des nächsten Blocks. Die Kette, bei der dieser zuerst gefunden wird, stellt die längere Version dar. Das Netzwerk akzeptiert immer die längste valide Kette als richtig. /MIN-01 17/ Je kürzer die Block-Zeit ist, desto wahrscheinlicher sind parallele Entwicklungen. Im Bitcoin-Netzwerk wird generell empfohlen, mindestens 6 Blöcke

abzuwarten, bevor eine Transaktion als statistisch sicher durchgeführt bewertet werden kann – sich also mit an Sicherheit grenzender Wahrscheinlichkeit in der längsten Kette des Netzwerkes befindet.

Der gesamte Prozess kann letztlich nur durch enorm häufige Ausführung von Rechenoperationen erraten werden, wozu wiederum Arbeit und Ressourcen eingesetzt werden müssen (im Bitcoin-Netzwerk aktuell, Stand Juni 2018, ca. $33 \cdot 10^{18}$ Hashes/s). Dementsprechend dient bei PoW die notwendige eingesetzte Arbeit als Sicherheit keine Manipulation durchzuführen. Da die Blockerstellung zudem zeitdiskret abläuft, also eine bestimmte mittlere Zeit zwischen den Blöcken vorgegeben ist, würde die Manipulation eines Blocks in der Vergangenheit einen enormen Energieaufwand zur Lösung aller nachfolgenden Blöcke erfordern; dieser steht zudem im Wettbewerb mit allen anderen Minern. PoW dient weiter als Spamschutz, um zu verhindern das Netzwerk mit unnötigen Informationen zu überfluten. Ursprünglich wurde der Mechanismus für eben diese Aufgabe in E-Mail Programmen entwickelt und angewandt.

PoW basiert auf einem Rechenwettbewerb der beteiligten Miner

Wurde ein Ergebnis von einem Miner gefunden, kann dieses durch einmalige Ausführung der Hash-Funktion mit dem gefundenen Nonce-Value bei allen beteiligten Knoten bestätigt werden. Der Entdecker der richtigen Lösung wird mit einem festen Betrag vergütet (im Bitcoin-Netzwerk aktuell 12,5 BTC, Stand Juni 2018). Dieser Betrag wird für die Vergütung der Miner neu geschaffen. Da im Falle des Bitcoin-Netzwerks die maximale Anzahl an Bitcoins auf 21 000 000 Coins limitiert ist, wird entsprechend in regelmäßigen Abständen (alle 210 000 Blöcken) die Vergütung für einen gefundenen Block (der sog. „Block Reward“) halbiert (siehe Abbildung 3-18). Zusätzlich zum Block Reward erhält der Miner eine geringe Transaktionsgebühr, die für jede Transaktion vom Sender bezahlt wird /COI-01 17/, /PSL-01 17/.

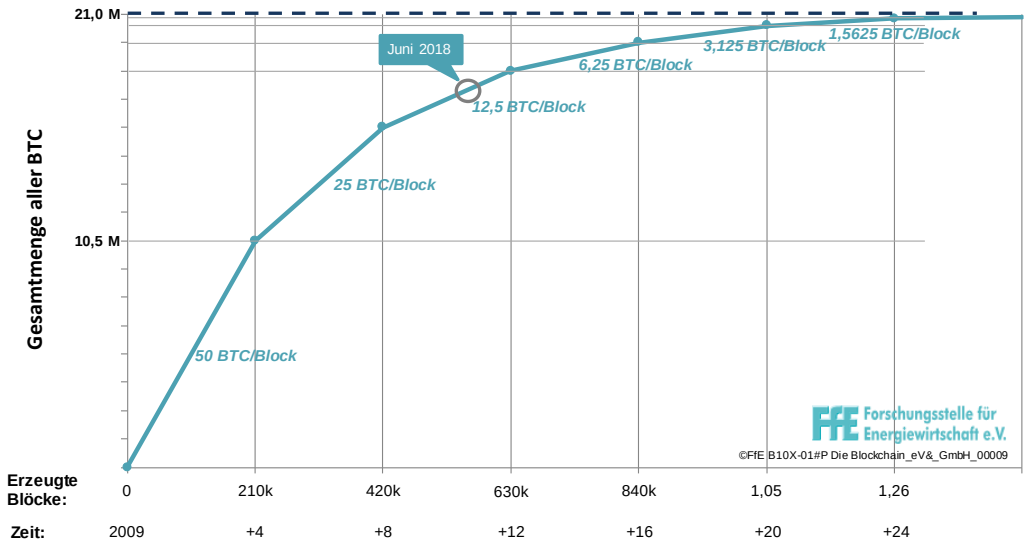

Abbildung 3-18: Zeitliche Abhängigkeit des „Block Rewards“ als Vergütung der Miner im Bitcoin Netzwerk (eigene Darstellung nach /BIT-01 17/)

Vorteile

Proof of Work ist der Konsensmechanismus, der aktuell (Stand Juni 2018) am weitesten verbreitet und somit auch in den Kryptowährungen mit der höchsten Marktkapitalisierung eingesetzt wird. Allein dieser Fakt bestätigt das große Vertrauen, das in diese Logik gesetzt wird. Insbesondere in einer offenen Umgebung, also einer „public blockchain“ (siehe Kapitel 3.1.3), in der beliebig viele Knoten am Netzwerk und auch am Mining-Prozess („permissionless“) teilnehmen können, zeigt PoW seine Vorteile. Da keinerlei Identifikation

oder Authentifizierung der Teilnehmer erforderlich ist, ist dieser Konsens-Mechanismus sehr gut skalierbar und macht die aktive Teilnahme von Tausenden von Knoten möglich. /PSL-01 17/

Um die Kette manipulieren zu können, müssten gemäß dem mehrheitlichen Konsens mehr als 50 % der weltweiten Hashing-Power von einer Instanz kontrolliert werden. Hierdurch könnte als Erster einer neuer Block erzeugt und die längste Kette bestimmt werden. Da dies mit enormem finanziellem Aufwand aufgrund der Marktkonkurrenz verbunden wäre, kann PoW somit die Sicherheit der Blockchain effektiv garantieren. Die Sicherheit ist dabei durch den finanziellen Einsatz in Form von Hardware und Ressourcen (insbesondere Energiekosten) gegeben und reduziert somit das Risiko von Manipulation. Da die Teilnahme an dem Konsensprozess dieses finanzielle Engagement verlangt, aber auch wieder vergütet, wird es von manchen Experten auch als "fairstes" Verteilungssystem für neue Währungen bezeichnet. /BUN-01 17/

Nachteile

Trotz des beschriebenen hohen Aufwands zur Manipulation ist die Möglichkeit eines Angriffs prinzipiell nicht auszuschließen, insbesondere bei einer hohen Konzentration von beteiligter Rechenleistung. Ein potenzielles Risiko bieten sogenannte „51 %-Angriffe“, bei denen ein Mining-Pool mehr als 50 % der Miningpower (Hash-Rate) kontrolliert. Somit wäre es theoretisch möglich eigene, manipulierte Blöcke in die Blockchain zu schreiben oder einen „Fork“ zu bewirken. Die Leistung der eingesetzten Hardware steigt dabei überproportional mit den Investitionskosten in Hardware, was zu einer weiteren Zentralisierung führt.

PoW ist mit erheblichem Energieaufwand verbunden

Ein häufiger Kritikpunkt sind die enormen Mengen an Rechenleistung und somit elektrischer Energie, die benötigt werden, um das Netzwerk zu betreiben. Aktuell (Stand: Juni 2018) benötigt allein die Bitcoin-Blockchain ca. 68 TWh pro Jahr, vergleichbar mit dem Energieverbrauch von Österreich und entsprechend 0,31 % des weltweiten Stromverbrauchs. Dies entspricht im Mittel einem Energieverbrauch von über 950 kWh pro Transaktion /DIG-01 18/.

Weiterführendes Wissen: Mining

Als „Mining“ oder Schürfen von Kryptowährung bezeichnet man den Vorgang, dass bei der Validierung eines Blocks der erfolgreiche Rechner (Knoten) neben den Transaktionsgebühren neu erschaffene Kryptowährung als Vergütung erhält. Diese Tatsache, kombiniert mit der dafür notwendigen „Suche“, ist somit vergleichbar mit dem Schürfen von z. B. Gold. Durch den steigenden Kurs der Kryptowährungen wurde dies zunehmend lukrativer, was zur Entstehung von sogenannten „Mining-Farmen“ führte, also Server-Zentren, deren einzige Aufgabe in der Ausführung des Proof of Work-Algorithmus besteht, mit dem Ziel, valide Blöcke zu finden und dafür vergütet zu werden. Aufgrund der hohen Ausgaben für Strom siedeln sich diese insbesondere in Regionen mit günstigen Strompreisen wie Nord-China oder Island an.

Abbildung 3-19: Mining-Anlage in Island (Genesis Mining, Marco Krohn [CC BY-SA 4.0], via Wikimedia Commons)

Die größten Mining-Kapazitäten befinden aktuell in China, Georgien, Island und den USA

Wichtige Aspekte sind auch, dass die Skalierbarkeit aufgrund des hohen Energieverbrauchs begrenzt ist und dass der Großteil des Minings in Regionen der Welt mit günstigem Strompreis zentralisiert ist. PoW hat daher relativ lange Transaktions-Bestätigungszeiten. So ist das Bitcoin-Netzwerk in der Lage, nur etwa 7 Transaktionen pro Sekunde zu bestätigen, was im Bereich des Zahlungsverkehrs als sehr langsam anzusehen ist. Insbesondere, wenn man dies mit den Transaktionsraten bei MasterCard oder VISA vergleicht, die im Mittel 4 000 (maximal 56 000) Transaktionen pro Sekunde erreichen, wird dies offensichtlich. /BIT-01 17/, /BDEW-101 17/, /PSL-01 17/ Um diese Einschränkungen zu optimieren, wird aktuell intensiv an Weiterentwicklungen und neuen Technologien wie State Channels geforscht (vgl. Kapitel 3.4.3.2).

Entwicklungsstand & Verwendung

Bitcoin als bekannteste Blockchain und Währung mit der höchsten Marktkapitalisierung (ca. 129 Mrd. US $, Stand: Juni 2018) verwendet ein auf Proof of Work basierendes Konsens-Modell namens HashCash. /COI-01 17/

Ethereum (in der aktuellen Version „Homestead“) verwendet das speziell für Ethereum entwickelte PoW Konsens-Modell Ethash. Der Unterschied zu Hashcash besteht insbesondere in deutlich schnelleren Blockzeiten von ca. 12–19 s. Ethash wurde auch entwickelt, um der Zentralisierung des Mining entgegenzuwirken. Diese ist insbesondere durch große Mining-Pools gegeben, die günstige und standardisierte ASICs (siehe Exkurs) verwenden, um Berechnungsoperationen mit sehr hohen Hash-Raten durchzuführen. EthHash ist hingegen darauf optimiert, auf Standard-Endverbraucherhardware, speziell Grafikkarten-Prozessoren (sog. GPU) durchgeführt zu werden. Somit bietet dieser durch seine höhere sogenannte „ASIC-Resistenz“ ebenfalls eine geringere Anfälligkeit gegenüber 51 %-Angriffen, da eine Konzentration von Rechenleistung aufgrund von z. B. patentierter Hardware vermieden werden kann. /PSL-01 17/

Weiterführendes Wissen: ASIC

*Als **A**pplication **S**pecific **I**ntegrated **C**ircuit, kurz ASIC, wird ein integrierter Schaltkreis (IC) bezeichnet, der nur für einen bestimmten Verwendungszweck maßgeschneidert und nicht für den allgemeinen Gebrauch bestimmt ist. Der Einsatz dieser Hardware findet sich insbesondere bei Bitcoin-Mining. So besteht mittlerweile nahezu die gesamte in der Praxis genutzte Mining-Hardware für Bitcoin aus ASICs, da diese Standard-Hardware sowohl in puncto Geschwindigkeit als auch Effizienz übertreffen. Zu beachten ist, dass diese ASIC-Chips in der Regel nur für das Mining in einem Blockchain-Netzwerk verwendet werden können.*
Da das Problem einer Konzentration von großen Mining-Kapazitäten in einzelnen Pools erkannt wurde, gibt es mittlerweile zunehmend Bestrebungen, diese Hardwareabhängigkeit mittels „ASIC-Resistenz" unter Kontrolle zu bekommen. In der Ethereum-Blockchain wurde dies im eigenen Konsens-Algorithmus EthHash verankert; für das Bitcoin-Netzwerk wird dies ebenfalls diskutiert, konnte sich bislang aber nicht durchsetzen. /BIT-01 17/

3.2.3.2 Proof of Stake (PoS)

Die am häufigsten diskutierte und am weitesten ausgearbeitete Alternative zum PoW-Algorithmus ist Proof of Stake (PoS). PoS-Algorithmen wurden entwickelt, um die Nachteile von PoW-Algorithmen in Bezug auf den hohen Stromverbrauch im Mining zu überwinden. Zum ersten Mal erwähnt wurde dieses Konsensmodells 2011 im Rahmen eines Forumsbeitrags /BITC-01 11/.

Proof of Stake soll den Energiebedarf im Vergleich zu PoW deutlich reduzieren

Grundsätzlich lässt sich bereits an der Terminologie ein Unterschied zu PoW feststellen. Während aktive Knoten eines PoW-Algorithmus' „Miner" genannt werden, sind dies im Falle von PoS lediglich „Validatoren". Die Validatoren (auch „Stakeholder" bezeichnet, da sie direkt am System beteiligt sind) werden üblicherweise ausschließlich über Transaktionsentgelte entlohnt. Letztlich kann man sich den Konsens-Prozess in PoS als eine Art „Virtualisierung" des Minings vorstellen. In diesem Prozess investieren die Stakeholder Geld statt Hardware und Ressourcen in den Konsensprozess. Im PoS-Algorithmus stellen die Validatoren ihr Geld dem System als Pfand zur Verfügung. Falls sie nicht nach den Regeln des Konsenses spielen, verlieren sie ihr Geld.

PoS ist nicht ohne gekoppelte Kryptowährung nutzbar

Die Idee dahinter ist folgende: Statt eines Miners, der 2 000 € für Mining Equipment und Strom ausgibt, um an einem PoW-Algorithmus teilzunehmen und dafür entlohnt wird, kann er bei PoS Krypto-Währung von identischem Wert (entsprechend 2 000 €) kaufen und sie als „Stake" (also Einlage) nutzen. Abhängig von der Einlage steigen proportional die Chancen, als Validator für einen Blocks ausgewählt zu werden. Der Pseudozufallsalgorithmus des PoS wählt dabei Validatoren für die Blockerstellung aus und stellt sicher, dass kein Validator vorhersagen kann, wann er an der Reihe ist. Dementsprechend würde ein Validator mit 300 Münzen (= coins) dreimal so häufig ausgewählt, wie jemand mit 100 Münzen. Wenn ein Prüfer einen „ungültigen" Block erstellt, wird seine Sicherheitskaution gelöscht und sein Privileg, Teil des Netzwerkkonsenses zu sein, erlischt.

Dabei sind die Berechnungen in PoS wesentlich einfacher zu lösen und benötigen deshalb deutlich weniger Energieressourcen. Der Validator muss lediglich beweisen, dass er einen bestimmten Betrag als Pfand hinterlegen kann. Zusammengefasst kann man PoS auch als ökonomischen Konsensmechanismus bezeichnen. Der Mechanismus basiert dabei auf einer Art Lotterie. Prinzipiell kann jeder, der eine Einlage in Form einer Anzahl an coins hinterlegen kann, als Validator agieren. Hierzu muss eine spezifische Transaktion an eine Art treuhänderischen Tresor als Pfand gesendet werden. /BITF-01 15/, /PSL-01 17/, /ETH-01 18/

Zur Auswahl der Validatoren gibt es zum Beispiel folgende Möglichkeiten /NXT-01 18/:

- **Randomisierte Auswahl**: In dem PoS-Mechanismus, wie er z. B. in den Blockchain-Varianten von „Nxt“ und „BlackCoin“ umgesetzt wurde, wird der Knoten, der den nächsten Block erzeugen darf, zufällig ausgewählt. Die Auswahl erfolgt gewichtet nach dem höchsten Einsatz. Da die Einsätze öffentlich gemacht werden, ist es prinzipiell dadurch möglich, den nächsten validierenden Knoten abzuschätzen.
- **Basieren auf dem Coin-Alter**: Im PoS-Algorithmus von z. B. „Peercoin“ wird das Konzept des Coin-Alters eingeführt. Das Alter eines Coins ist der Wert, multipliziert mit dem Zeitraum nach seiner Entstehung. Je länger ein Knoten die Münzen hält, desto mehr Rechte kann er im Netzwerk erhalten. Die Besitzer der Münzen erhalten auch eine bestimmte Belohnung in Abhängigkeit vom Münzalter. Somit werden die Knoten angeregt, die Haltedauer ihrer Coins zu erhöhen.

PoS basiert auf dem Einsatz von Kapitel anstatt Energie und Ressourcen

Vitalik Buterin, der Gründer von Ethereum, fasst den Unterschied von PoW und PoS im folgenden Satz zusammen: “The one-sentence philosophy of proof of stake is thus not ‘security comes from burning energy’, but rather ‘security comes from putting up economic value-at-loss’.” Sinngemäß bedeutet dies, dass bei PoW Glaubwürdigkeit der teilnehmenden Validatoren auf dem Wert der eingesetzten Hardware und Energie basiert. Bei PoS hingegen wird korrektes Verhalten durch hinterlegtes Kapital gewährleistet.

Vorteile

Der größte Vorteil eines PoS-Konsensmechanismus besteht wie bereits erwähnt in der Reduktion des Energiebedarfs im Vergleich zu PoW. Dementsprechend wird erwartet, dass sich die Kosten für Transaktionen und das gesamte System dadurch deutlich reduzieren.

Zudem bietet PoS Sicherheit, die sich aus den folgenden beiden ökonomischen Aspekten ableitet:

5) Würde eine manipulierende Marktmacht 51 % der Gesamtzahl der Coins kaufen müssen, um das Netzwerk zu kontrollieren, würde entsprechend der Markt mit einer schnellen Preissteigerung reagieren und die Kosten des Angriffs massiv erhöhen. /BITF-01 15/
6) Weiter reduziert sich durch diesen Fakt der Anreiz für einen Angriff: Der Angreifer würde, da er einen Großteil der Coins hält, selbst massiv von seinem Angriff betroffen sein. /BIT-01 17/

Bei PoS ist es nicht notwendig, regelmäßig neue Coins als Anreiz für die teilnehmenden Knoten auszugeben. Somit bietet sich eine flexiblere Handhabung des verfügbaren Kapitals.

PoS birgt allgemein weniger Risiken hin zu einer Zentralisierung aufgrund von „economy-of-scale“-Mechanismen, da die Rendite direkt proportional zum Einsatz ist (im Gegensatz zu PoW) und hohe Stückzahlen von spezialisierter Hardware nicht notwendig sind. Somit bietet PoS einen deutlich einfacheren Zugang als Knoten am Konsens-Mechanismus teilzunehmen und würde das „Mining“ entsprechend demokratisieren und besser über das Netzwerk verteilen. Auf technischer Seite zeigt sich eine deutlich reduzierte Größe des Clients, was es ermöglicht, mit geringem Hardware-Einsatz am Konsens-Mechanismus teilzunehmen. /ETHE-01 15/

Es gibt die Möglichkeit, ökonomische Bestrafungen einzuführen, die einen 51 % Angriff noch schwieriger machen. Der Ethereum-Entwickler Vlad Zamfir beschrieb es folgendermaßen: „It's as though your ASIC farm burned down if you participated in a 51 % attack". Schlussendlich sind mit PoS zudem deutlich kürzere Block-Zeiten und somit höhere Transaktionsraten möglich. /ETHN-01 16/, /ETH-01 18/, /ETHE-01 15/

Nachteile

Durch den Ansatz, dass die Rendite aus der Teilnahme am Konsens-Mechanismus proportional zum eingesetzten Kapital ist, führt PoS tendenziell zu einer zunehmenden Konzentration von Kapital. Letztlich ist das System jedoch mit einem festen Zinssatz zu vergleichen, der für alle Einlagehöhen gleich ist.

Sehr einfache („naive") und frühe Formen von PoS-Algorithmen leiden unter dem „Nothing-at-Stake-Problem". Diese Implementierungen sehen keine „Bestrafung" für fehlerhaftes Verhalten vor und bieten somit auch keinen Anreiz für einen Knoten, sich positiv im Sinne des Netzwerks zu verhalten. /ETH-01 18/, /PSL-01 17/

Ein weiter genanntes Problem könnten gezielte Angriffe auf Wallets mit der Einlage sein, die z. T. sehr hohe Beträge an coins als Pfand („stake") enthalten, sein, da diese immer online und bekannt sind. /BUN-01 17/

Entwicklungsstand & Verwendung

Die erste Anwendung des PoS-Algorithmus in einer Blockchain war bei PeerCoin (gefolgt von Blackcoin und NXT), welcher jedoch mit dem „Nothing-at-Stake" Problem behaftet war /MIN-01 17/. PoS wurde bereits im ersten Bitcoin-Projekt erwähnt, aber aufgrund der angeblich mangelnden Robustheit und anderer Gründe nicht verwendet.

Ethereum läuft aktuell noch mit PoW, plant jedoch einen Wechsel zu Proof of Stake. Für diesen Wechsel soll mittels des nächsten Updates („Constantinople Hard Fork"), das für 2018 erwartet wird, der Grundstein für den „Casper" PoS-Mechanismus und auch Sharding (siehe Kapitel 3.4.3.3) gelegt werden.

Aktuell arbeiten u. a. folgende coins bereits mit PoS Konsensmechanismen (in verschiedenen Ausprägungen, vgl. auch Kapitel 3.2.3.2): NEO, Lisk, Stellar Lumens, BitShares, PIVX.

Weiterführendes Wissen: Casper in Ethereum

Die aktuell vorgeschlagene Weiterentwicklung des Ethereum-Netzwerks hin zu einem PoS-Konsensmechanismus trägt den Namen „Casper". Casper verwendet eine Kombination aus Sicherheitsleistungen und Wetten, um einen Konsens zu erzielen. Dabei wurde eine minimale (1 500 ETH) und maximale Einlagehöhe (60 000 ETH) vorgeschlagen.
Mit ihrem Einsatz „wetten" die beteiligten Validatoren auf den Ausgang des Konsensprozesses. Darüber hinaus ist der Konsensprozess abhängig von der Art und Weise, wie die Validatoren wetten: ihr Ziel ist dabei genauso zu wetten, wie sie erwarten, dass auch alle anderen Validatoren wetten. Falls sie schließlich richtig liegen, bekommen sie ihren Einsatz zurück plus Transaktionsgebühren und möglicherweise zusätzlich ausgegebener Tokens. Falls sie jedoch nicht schnell genug einen gemeinsamen Konsens erlangen, bekommen sie weniger von ihrem Einsatz zurück. Durch iterierte Runden wird somit das Ziel eines Konsens angereizt und die Wetten der Validatoren konvergieren. Casper befindet sich aktuell noch in der Testphase, auch wenn bereits mehrere Versionen eines Proof of Concepts veröffentlicht wurden. Für die Einführung wurde ein Hybridsystem zwischen PoW und PoS vorgeschlagen. /ETHE-01 15/, /PSL-01 17/, /ETHN-01 16/

3.2.3.3 Proof of Authority (PoA)

Proof of Authority basiert auf der Glaubwürdigkeit ausgewählter Knoten

Blockchains mit Proof of Authority (PoA) zählen zu den „permissioned“ Blockchains, bei denen der Zugang zum Konsensmechanismus für beteiligte Validatoren erst autorisiert werden muss – im Gegensatz zu „permissionless“ Blockchains wie bei PoW oder PoS, bei denen sich prinzipiell jeder an der Konsensfindung beteiligen kann.

PoA-Algorithmen gehören zu der Familie von sogenannten „Byzantine fault-tolerant“ Konsensmechanismen, bei denen der Konsens nur unter einer begrenzten Anzahl von Validatoren gefunden werden muss. Der Grund ist, dass statt einer Vielzahl von Validatoren eine Anzahl von „authorities“ das Recht erhalten, Blöcke zu validieren, zu schreiben und somit die Blockchain sichern. Diese sind oftmals identisch mit realen, physischen Autoritäten.

Die Algorithmen funktionieren dabei rundenbasiert. In jeder Runde wird ein Knoten gewählt, der als „mining leader“ fungiert und die Aufgabe hat, neue Blöcke vorzuschlagen, für die ein verteilter Konsens erzielt wird. Dabei muss eine Mehrheit der „authorities“ den neuen Block bestätigen. Diese können hierfür folglich auch zur Rechenschaft gezogen werden. PoA kann daher insbesondere für private oder Konsortial-Blockchains eingesetzt werden. Für diese entstehen de facto keine Nachteile im Vergleich zu PoW. /PRUS-01 17/, /CINI-01 17/

Vorteile

PoA ist prinzipiell sicherer als zentralisierte Datenbankprozesse, da ein Angreifer oder eine gehackte „authority“ ein Netzwerk nicht einfach übernehmen und möglicherweise alle Transaktionen rückgängig machen kann. Im Vergleich zu PoW ist es deutlich weniger rechenintensiv und weist auch im Vergleich zu PoS eine deutlich höhere Performance auf. Bei PoA-Blockchains können die Blöcke in festen Zeitintervallen ausgegeben werden. Da kein aufwendiger Mining-Prozess notwendig ist, sind PoA-Algorithmen deutlich ressourceneffizienter als z. B. PoW.

Nachteile

PoA-Mechanismen legen das Vertrauen und die Macht über das Netzwerk in die Hände weniger, ausgewählter Knoten. Dies widerspricht insbesondere für öffentliche Blockchains dem Grundgedanken der Dezentralisierung und Demokratisierung.

Entwicklungsstand & Verwendung

Aktuell gibt es eine Vielzahl von vorgeschlagenen PoA-Protokollen, die sich in Details unterscheiden. Mit Parity und Geth stehen zwei PoA-Mechanismen zur Verfügung, die eine „permissioned“ Blockchain auf Basis von Ethereum ermöglichen. Die beiden Blockchain-Netzwerke Hyperledger und Ripple basieren ebenfalls auf PoA. /PRUS-01 17/, /CINI-01 17/

3.2.3.4 Weitere Ansätze (eine Auswahl)

Neben den beschriebenen, am meisten verbreiteten und diskutierten Mechanismen bestehen eine Vielzahl weiterer Vorschläge und Umsetzungen zu komplett neuen Algorithmen bzw. Weiterentwicklungen auf Basis von PoS oder PoA. Diese werden im Folgenden kurz beschrieben.

Konsens-Mechanismen haben sich zu einem eigenen Forschungsfeld entwickelt

Practical Byzantine Fault Tolerance (PBFT)

In „Practical Byzantine Fault Tolerance (PBFT)"-Algorithmen ist durch redundantes Abfragen eine Toleranz gegenüber fehlerhaften bzw. manipulierten Datensätzen gegeben. In jeder Runde wird ein Knoten nach bestimmten Regeln für die Durchführung der Transaktion ausgewählt. Die Entscheidung, welcher Block schließlich als rechtmäßig gesehen wird, erfolgt durch einen Mehrrundenprozess, bei dem jeder Validator eine „Stimme" für einen bestimmten Block während jeder Runde abgibt. Am Ende des Prozesses sind sich alle aktiven Validatoren darüber einig, ob ein bestimmter Block Teil der Kette ist oder nicht. PBFT setzt also voraus, dass jeder Knoten dem Netzwerk bekannt ist und ist somit sehr ähnlich zu PoA-Ansätzen. Daher sind sie insbesondere für Konsortien gedacht, bei denen die Gruppe der Teilnehmer in den Konsortien nicht nur bekannt ist, sondern deren Identität registriert und von einem zentralen Registryservice innerhalb des Systems verifiziert wird. Dies wird aktuell von Hyperledger unterstützt. /ZHE-01 17/, /MIN-01 17/, /PSL-01 17/

Das *Tendermint-Protokoll* ist ähnlich zu PBFT mit dem Unterschied, dass hierbei die Knoten Coins (entsprechend dem „Stake" bei PoS) als Einsatz hinterlegt werden müssen. Wenn ein Validator für unehrlich befunden wird, wird er bestraft.

Ein weiterer Ansatz ist *Delegated Byzantine Fault Tolerance (DBFT)*, bei dem „professionelle" Knotenpunkte durch ein delegiertes Abstimmungsverfahren von „ordinary notes" ernannt werden. /BUN-01 17/

Delegated Proof of Stake (DPoS)

DPoS-Algorithmen funktionieren ähnlich wie andere PoS-Modelle, mit dem Unterschied, dass in diesem Fall eine Repräsentation von Teilnehmern durch einen Knoten möglich ist. Diese „delegate nodes" nehmen entsprechend in Vertretung vieler kleiner Akteure mit geringerem Einsatz an dem Konsensmechanismus teil. Es ist somit vergleichbar mit repräsentativer Demokratie im Gegensatz zu direkter Demokratie bei PoS. Dies ermöglicht zum einen schnellere Bestätigungszeiten von Transaktionen und einfachere Teilhabe an dem System, zum anderen führt es allerdings auch zu größerer Zentralisierung. Eingesetzt wird das System z. B. bei BitShares. /HAM-01 17/, /ZHE-01 17/

Eine ähnliche Lösung ist das sog. *Leased Proof of Stake (LPoS)*, bei dem die Teilnehmer ihre Einlage an die validierenden Knoten verleihen und hierfür eine Vergütung erhalten.

Ripple

Das Ripple-Netzwerk verwendet einen Konsens-Algorithmus, der vertrauenswürdige Unternetze innerhalb eines größeren Netzwerks verwendet. Im Netzwerk werden zwei Knoten-Typen unterschieden: Server bzw. Gateways, die am Konsensprozess teilnehmen und Clients, die lediglich Transaktionen durchführen können. Dabei werden eigene Konsensmodelle verwendet, die eine abgeleitete Form der „Byzantine Fault Tolerance" sind. Die Blockchain-Plattformen von Ripple und auch Stellar richten sich insbesondere an Use Cases in der Finanzbranche. Sie stellen Zahlungsprotokolle zur Verfügung, mit denen grenzüberschreitende Transaktionen in Sekundenschnelle abgewickelt werden können.

Proof of Elapsed Time (PoET)

Proof of Elapsed Time (PoET) ist ein von Intel entwickelter Konsens-Algorithmus, der auf einem Lotterie-basierten Wahlmodell basiert. Die Wahl erfolgt dabei auf Basis einer vom Knoten zufällig gewählten Wartezeit. Der Knoten mit der kürzesten Wartezeit gewinnt die Lotterie und kann der Leader werden. Ziel ist dabei, einen echten Zufallsmechanismus zu schaffen, der auf sehr niedrigem Hard- und Softwarelevel implementiert ist. Die Funktionen sind dabei so konzipiert, dass sie nur auf spezialisierter Hardware („Safe Guard Extensions – Intel SGX“) ausgeführt und somit durch externe Software nicht verändert werden können. /PSL-01 17/

Neben den genannten Konsens-Mechanismen bestehen eine Vielzahl weiterer Vorschläge und Konzepte. Zu nennen sind unter anderem *Proof of Activity (PoW/PoS-hybrid), Proof of Burn (PoB), Proof of Validation (PoV), Proof of Capacity (PoC bzw. Proof of Storage), Proof of Importance (PoI), Proof of Existence (PoE)* oder *Raft*, auf die allerdings nicht näher eingegangen werden soll. Mittlerweile hat sich aus dem Themenkomplex ein komplett neues Forschungsfeld herausgebildet, das sich intensiv mit optimierten Konsens-Logiken auseinandersetzt und auf spieltheoretischer Basis testet und beweist.

3.2.3.5 Vergleich und Fazit

Abschließend soll anhand von Tabelle 3-3 ein kurzer Vergleich der wichtigsten vorgestellten Konsens-Algorithmen erfolgen.

Tabelle 3-3: Qualitativer Vergleich der vorgestellten Konsens-mechanismen

	PoW	**PoS**	**PoA**	**PBFT**	**DPOS**	**Ripple**	**POET**
Knoten Teilnahme / Identifikation	offen	offen	zugangs-beschränkt	zugangs-beschränkt	offen	offen	offen
Energie-aufwand	hoch	mittel	gering	mittel	mittel	mittel	gering
Manipulations-Toleranz	< 51 % der Rechen-leistung	< 51 % des eingesetzten Kapitals, abh. von verwen-deten Algo-rithmen	≤ 33 % der Stimm-rechte	< 33 % fehler-hafte Repliken	< 51 % der Valida-toren	< 20 % der fehler-haften Knoten in UNL	unbe-kannt
Transaktions-geschwindig-keit	gering	hoch	hoch	hoch	hoch	hoch	mittel
Skalierbarkeit des Netzwerks	hoch	hoch	gering	gering	hoch	hoch	hoch
Beispiel	Bitcoin	Peercoin	Tendermint	Hyper-ledger Fabric	Bitshares	Ripple	Hyper-ledger Sawtooth

3.2.4 Smart Contracts

Smart Contracts machen die Blockchain zur Blockchain-Plattform

Als **Smart Contract** bezeichnet man automatisiert ausführbare Programme, die dezentralisiert auf einer Blockchain Plattform laufen. Sie bilden dabei mittels Programmcode bestimmte Aktionen ab, die anhand von erfüllten Bedingungen selbständig ausgeführt werden können. Meist sind diese Aktionen mit der Ausführung von Transaktionen auf der Blockchain verbunden. Die Bedingungen können durch bestimmte Ereignisse auf der Blockchain, Anfragen von Benutzern, Transaktionen oder anderen Smart Contracts ausgelöst werden. Diese definierten Prozesse können mitunter sehr komplex sein und gesamte Geschäftsprozesse abwickeln (siehe DAO, Kap. 3.2.4.3). Der Vorteil liegt insbesondere darin, nicht von einer zentralen Instanz abhängig zu sein und somit auch anonyme Prozesse sicher durchführen zu können. Zudem ist der Code dieser Programme für alle Teilnehmer im Netzwerk transparent einsehbar und man spricht in diesem Kontext auch von „Open Execute“.

Das Konzept der Smart Contracts hängt dabei nicht unmittelbar mit der Blockchain zusammen und wurde bereits 1996 von Nick Szabo beschrieben /EXT-01 96/. Doch erst die Blockchain-Technologie ermöglicht die sichere dezentrale Abwicklung ohne Intermediär. Die Kombination wurde schließlich von Vitalik Buterin ins Gespräch gebracht und schließlich mit der Ethereum-Plattform realisiert. /ETHC-101 14/, /ETH-01 18/

Smart Contracts ermöglichen prinzipiell folgende Anwendungsfälle oder eine Kombination derselben /BER-01 17/:

- Datenspeicherung und Verwaltung,
- Erstellung von Tokens,
- Verwaltung von Vertragsbeziehungen zwischen sich unbekannten Teilnehmern ohne Intermediär,
- Interaktion und Datenbereitstellung mit anderen Smart Contracts,
- Komplexe Authentifizierungsmöglichkeiten (z. B. „M-of-N Multi-Signature Zugriff“). /BBL-101 14/

Weiterführendes Wissen: Code is law

Die Idee, dass über Programmcode, der mittels Blockchain und Smart Contract ausgeführt werden kann, rechtlich bindende Verträge ohne weitere Absprache und Definition geschlossen und ausgeführt werden können ist vielfach umstritten. Die daraus folgende Fragestellung „Is Code Law?“ wird entsprechend viel diskutiert und in juristischen Untersuchungen behandelt.
Speziell der Begriff „Smart Contract“ führt dabei oftmals zum Verständnis, dass es sich tatsächlich um eine Art Vertrag handeln könnte und wird in manchen Fällen auch so definiert. Einer Vielzahl von rechtlichen Einordnungen zu Folge ist dies, zumindest nach deutschem Recht, nicht zutreffend. Diesem Verständnis nach können Smart Contracts lediglich dem Abschluss und der Ausführung von Verträgen dienen. Mittels Blockchain und Smart Contract können folglich nur objektive Tatbestände der Willenserklärung abgebildet werden, keine subjektiven. /SCHOL-01 18/

Während die Sprache „Script“ hinter Bitcoin nicht Turing-vollständig (siehe unten) ist, ist dies für die Ethereum-Blockchain (Solidity) gegeben, wodurch diese Plattform beliebig komplexe Zusammenhänge abbilden kann.

Turing-Vollständigkeit

Turing-Vollständigkeit beschreibt (vereinfacht) die Eigenschaft eines Systems oder einer Programmiersprache, beliebige Rechenoperationen abbilden zu können. Dies beinhaltet vor allem das Berechnen von komplexen Schleifen. /PU-01 36/ Die Ethereum-Blockchain ist Turing-vollständig. Die Bitcoin-Blockchain ist dies nicht und daher nicht für komplexe Smart Contracts geeignet.

Smart Contract Oracles verbinden die Blockchain mit der Außenwelt

Smart Contract Oracles stellen eine Erweiterung des Smart-Contract-Konzepts dar. Sie ermöglichen neben den genannten Funktionen zudem die Interaktion von Smart Contracts mit Systemen außerhalb der Blockchain. So können sie auf externe Daten oder Ereignisse reagieren und diese auf der Blockchain verarbeiten. Diese externen Daten können beliebiger Natur sein: denkbar sind sowohl Inputs von digitalen Plattformen (z. B. SAP, CRM, Marktplätze) oder Webseiten-Input (über eine Web API), aber auch durch Sensoren erfasste Werte aus allen möglichen Bereichen. So können z. B. auch reale Dokumente oder Verträge hinterlegt werden und nach der (digitalen) Unterschrift automatisiert durch Smart Contracts ausgeführt werden.

Dieselbe Logik funktioniert ebenfalls in die gegengesetzte Richtung: so können Oracles auch Aktionen außerhalb der Blockchain-Umgebung ausführen. Dies bietet somit auch die Möglichkeit, verschiedene Blockchains miteinander zu verbinden; so kann z. B. durch ein Oracle in der Ethereum-Blockchain eine Transaktion auf der Bitcoin-Blockchain ausgelöst werden.

Am häufigsten wird das Konzept bislang für Markt- oder Transaktionsdaten eingesetzt, da in der Finanzbranche aktuell bereits die höchste Durchdringung der Blockchain-Technologie zu finden ist. Es ist zu erwarten, dass dieses Konzept bald aber auch auf sämtliche andere Bereiche übertragen wird (vgl. Abbildung 3-20).

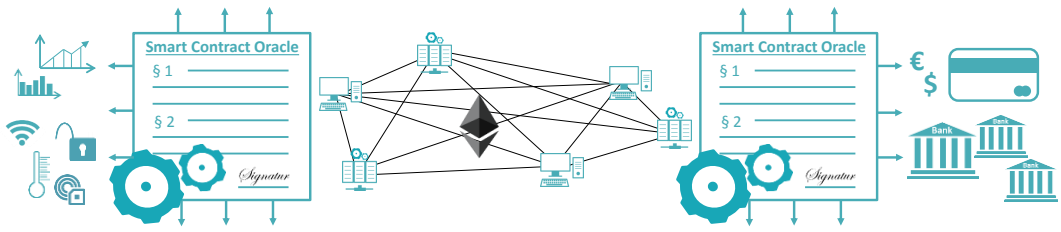

Abbildung 3-20: Funktionen von Smart Oracles als Schnittstelle der Blockchain zu externen Systemen

Es werden folgende Typen von Smart Contract Oracles unterschiedenen /BBLU-01 17/:

- **Software Oracles** verarbeiten bereits online verfügbare Daten, die z. B. auf Webseiten veröffentlicht werden. Beispiele sind Marktdaten, veröffentlichte Messreihen oder online Nutzungsdaten.
- **Hardware Oracles** verwenden Daten, die mittels Sensoren aus der physischen Welt übertragen werden. Besonders hier ist Datensicherheit und Integrität des Messsystems wichtig. Beispiele sind Umweltsensoren, aber auch RFID-Chips, die im Supply Chain Management eingesetzt werden.
- **Inbound Oracles** versorgen Smart Contracts allgemein mit externen Daten. Ein Beispiel wäre eine automatisierte Ausführung nach einem Trigger-Event, z. B. das

Ausführen einer Kauf-Order sobald ein handelbares Produkt einen bestimmten Preis erreicht.

- **Outbound Oracles** ermöglichen es Smart Contracts, Daten nach außen (in die physische Welt) zu senden. Ein Beispiel wäre die automatisierte Öffnung eines Türschlosses mittels Smart Contract, sobald eine Zahlung an deren Blockchain Adresse eintrifft.
- **Consensus-Based Oracles** ermöglichen die Berücksichtigung einer Vielzahl von Informationsquellen, was insbesondere bei sogenannten Prognose-Märkten, wie sie in den Blockchain-Projekten Augur und Gnosis umgesetzt werden, relevant ist.

Oracles sind oft Teil eines „Multi-Signature Contracts“ (siehe Kap. 3.2.1.2), wobei z. B. beteiligte Treuhänder einen Vertrag unterzeichnen, der automatisiert in Zukunft Funktionen ausführt (z. B. Transaktionen durchführt), falls eine Bedingung erfüllt ist. Bevor diese Aktion durchgeführt werden kann, muss zusätzlich ein Oracle den Smart Contract unterzeichnen und freigeben.

3.2.4.1 Technische Beschreibung

Wie beschrieben ist das Konzept der Smart Contracts auf der Blockchain historisch direkt mit Ethereum verknüpft. Ethereum bezeichnet sich deshalb explizit als Blockchain-Plattform, die Smart Contracts ausführen kann, im Gegensatz zu Bitcoin, das lediglich als Währung (inkl. der Möglichkeit, Transaktionen durchzuführen) zu verstehen ist. /ETHC-101 14/

Ethereum verwendet im Gegensatz zu Bitcoin ein Kontensystem

Zur einfacheren Umsetzung von Smart Contracts wurde bei Ethereum ein kontenbasierender Aufbau im Gegensatz zum UTXO Ansatz in Bitcoin gewählt (s. Abbildung 3-21). So wird im Bitcoin-Netzwerk das verfügbare Guthaben immer als Summe der vorhergehenden Transaktionen gebildet (vgl. Kapitel 3.2.2). Bei Ethereum wird ein Konzept, vergleichbar mit einem Bankkonto, verwendet, das neben der Adresse den Kontostand und ggf. auch Programmcode enthalten kann. Der Vorteil dieses Konzepts liegt sowohl in der Reduktion des Datenverbrauchs, als auch der intuitiveren Logik bei der Programmierung von Smart Contracts.

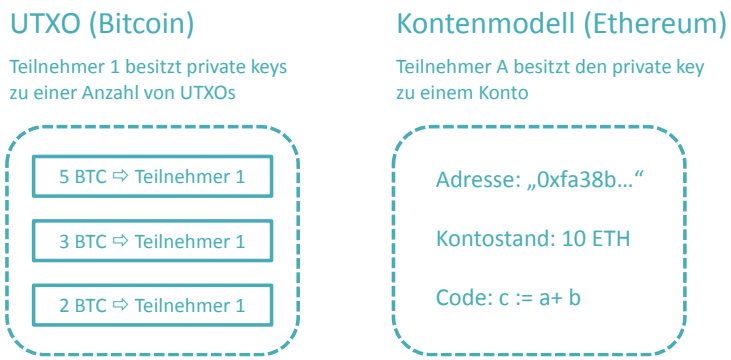

Abbildung 3-21: Vergleich des UTXO-Konzepts von Bitcoin mit dem kontenbasierenden Ansatz in Ethereum /BER-01 17/

Die Konten können in zwei Arten unterschieden werden:

- *Externally Owned Accounts (EOAs)* werden von realen Personen oder Unternehmen gehalten. Sie beinhalten lediglich den Kontostand und können Transaktionen durchführen (also Ether an andere Konten versenden oder Ausführanweisungen an Smart Contracts senden)

- *Contract Accounts (Contracts)* enthalten neben dem Kontostand einen Smart Contract Code, der durch externe Signale wie Transaktionen oder Nachrichten (sog. „function calls") aufgerufen wird. Diese function calls werden von anderen Smart Contracts oder EOAs an dieses Konto geschickt. Contract Accounts verfügen zudem über eine Möglichkeit zur dauerhaften Datenspeicherung. /BER-01 17/

Ethereum Virtual Machine

Ethereum im engeren Sinne bezeichnet eine Reihe von Protokollen, die eine Plattform für dezentrale Anwendungen schaffen. Kern der Ethereum Plattform ist die Ethereum Virtual Machine (EVM), eine Art virtueller Computer, der auf jedem Knoten parallel arbeitet und im Konsens gehalten wird. Jeder Ethereum Knoten führt die EVM und somit die hinterlegten Smart Contracts als Teil des Block-Verifikations-Prozesses aus. Die Ausführung einer Smart-Contract-Transaktion erfolgt dann, wenn der Mining-Knoten die Transaktion in einen von ihm generierten Block aufnimmt. Der Transaktions- und Smart-Contract-Code wird anschließend von jedem Knoten bei Erhalt des Blocks erneut ausgeführt. /ETHER-01 16/

Entwickler können Anwendungen, die auf EVM laufen, mit Hilfe von benutzerfreundlichen Programmiersprachen erstellen, die auf existierenden Sprachen wie JavaScript und Python basieren. Die am meisten verbreiteten Programmiersprachen in Ethereum sind Solidity, Serpent und LLL. Die Programmierumgebung von Ethereum ist „Turing complete", d. h. sie bietet alle Möglichkeiten einer modernen Programmiersprache. Die EVM kann somit Code beliebiger algorithmischer Komplexität ausführen. Diese Möglichkeiten bergen allerdings auch ein Risiko. Grundsätzlich ist es entscheidend zu verstehen, dass Ethereum nicht darauf ausgelegt oder optimiert ist, möglichst effiziente Berechnungen durchzuführen. Stattdessen sind die Berechnungen in hohem Grade redundant und somit eher ineffizient und teuer. Deshalb sollten die Berechnungen auf der Blockchain auch auf das Nötigste reduziert werden. Der entscheidende Vorteil ist jedoch, Konsens ohne eine zentrale Vertrauensperson oder Intermediär zu erzielen.

Gas

Transaktionskosten berechnen sich aus Preis und Aufwand

Um das Risiko einer massiven Überlastung der Blockchain durch zu komplexe Berechnungen oder unendliche Schleifen zu verhindern wurde bei Ethereum „gas" eingeführt. Gas dient als Vergütungseinheit für das Ausführen von Smart Contracts. Bei jeder Transaktion werden ein „gas limit" und ein „gas price" hinterlegt. Durch das „gas limit" wird die maximale Anzahl an Gas, die die Transaktion verbrauchen darf, vom Sender definiert. Es wird in der Regel automatisch auf Basis einer Schätzung berechnet. Das „gas limit" ist abhängig vom Umfang der Operationen („für 5 Zeilen Code werden 5 Einheiten gas benötigt") und bestimmt, ob die Operation durchgeführt werden kann. Der „gas price" hingegen bestimmt die Geschwindigkeit der Umsetzung. Also je höher man den „gas price" setzt, desto früher wird der Code auf der Blockchain ausgeführt. Eine detaillierte Übersetzung von „gas price" zu Geschwindigkeit inkl. Statistik findet sich auf *www.ethgasstation.info*. Die Transaktionskosten („Tx Cost" bzw. „fee") ergeben sich als:

$$Tx\ fee = gas\ limit\ \cdot gas\ price$$

Als Einheit wird dabei oft „Gwei" („Giga wei" entsprechend 10^9 wei) angegeben. „wei" bezeichnet dabei die kleinste Einheit von Ether (1 ETH = 10^{18} wei). Somit ergibt sich folglich ein Vergütungssystem zugunsten der Knoten für die Ausführung der Smart Contracts. Entsprechend würden unendliche Schleifen auch unendliche finanzielle Ressourcen benötigen. Zudem besteht ein absolutes „gas limit" pro Block an, das idealerweise in Abhängigkeit von der Netzwerkauslastung optimiert wird. Transaktionen, die dieses „block

gas limit“ übersteigen, können folglich nicht in einen Block aufgenommen werden. Das verhindert wiederum zu hohe Zeiten zur Erstellung eines Blocks.

Das Konzept der Smart Contracts wurde mittlerweile auch in anderen Blockchains adaptiert bzw. deren Umsetzung geplant. Diese kombinieren die Funktionalitäten häufig mit weiteren Eigenschaften. Beispiele hierfür sind NEO (verwendet dBFT-Konsensmechanismus und digitale Identitäten der Teilnehmer), EOS (bietet schnellere Ausführung von Smart Contract) oder Lisk (verwendet Java Script als Programmiersprache).

3.2.4.2 Decentralized Applications (dApps)

Decentralized Applications (dApps) können als Software-Anwendungen verstanden werden, die dezentral auf einem P2P-Netzwerk, also nicht nur auf einem einzelnen Computer, ausgeführt werden. Sie ermöglichen somit den Netzwerkteilnehmern, miteinander zu interagieren. dApps sind dabei nicht explizit beschränkt auf Blockchain-Anwendungen und werden bereits seit der Einführung von P2P-Netzwerken diskutiert. Bekannte Beispiele aus der Vergangenheit sind BitTorrent, Popcorn Time, BitMessage oder das Tor-Netzwerk. Fasst man den Begriff der dApp etwas weiter, kann man darunter generell die Umsetzung von Geschäftsmodellen auf Basis einer (Blockchain-) P2P-Plattform sprechen. Dabei werden Smart Contracts verwendet, um Geschäftsprozesse oder automatisierte Funktionen eines Geschäftsmodells umzusetzen. Viele dApps werden dabei Open Source lizensiert und sind somit – wie auch die Quellcodes der meisten Blockchain-Plattformen – frei verfügbar und öffentlich einsehbar. /BBLU-01 18/

dApps schaffen die Schnittstelle vom Benutzer zur Blockchain

Das Backend der Anwendung bildet der Smart Contract, der auf der Blockchain ausgeführt wird (also „on-chain“). Dies stellt auch den wesentlichen Unterschied zu klassischen Anwendungen dar, die üblicherweise zentral auf einem Server oder Endgerät laufen. Das Frontend, also die Benutzerschnittstelle, hingegen kann außerhalb der Blockchain-Umgebung ausgeführt werden und unterscheidet sich somit nicht von herkömmlichen Programmen oder Apps (vgl. Abbildung 3-22).

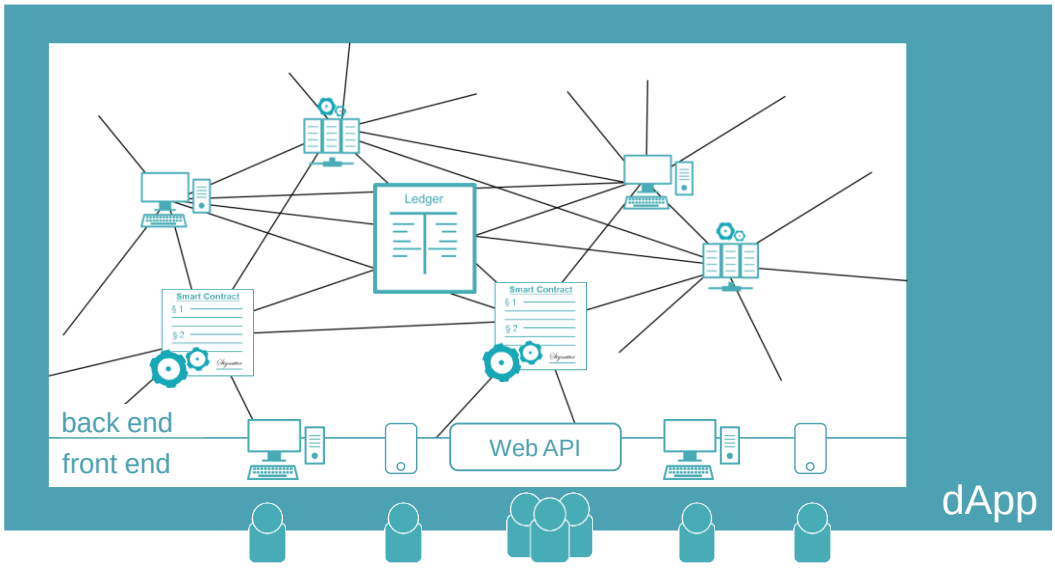

Abbildung 3-22: Aufbau von Decentralized Applications (dApps)

Eine Besonderheit kann sein, dass die Datenhaltung ebenfalls dezentralisiert geschieht. Hierfür neu entwickelte Technologien sind Swarm und IPFS. Neben der Datenhaltung kann zudem die Kommunikation unter den dApps dezentralisiert abgewickelt werden. Eine relevante Technologie dahinter nennt sich „Whisper“.

Zusammengefasst kann die Kombination der Funktionen so beschrieben werden /BBLU-01 18/:

- Smart Contracts bezeichnen die dezentralisierte Logik,
- Swarm und InterPlanetary File System (IPFS) bieten eine dezentralisierte P2P-Datenhaltung und
- Whisper ermöglicht den dezentralisierten Daten- und Nachrichtenaustausch.

Web3

Die Kombination der neuen Funktionalitäten der beschriebenen Technologie wird aktuell oft als „Web3“ bezeichnet und soll die autonome und dezentrale Struktur beschreiben. Es stellt damit die Fortentwicklung von:

- Web1 bzw. WWW im Sinne des statischen Internets, das nur zur Datenbereitstellung genutzt werden kann und
- Web2 als Weiterentwicklung hin zu einem interaktiven, programmierbaren Netz mit Social-Media-Kanälen und Sharing-Economy-Anwendungen

dar.

Web3 kombiniert als dezentralisierte Plattform die Funktionen des Computers als Endgerät mit den Funktionen des Internets. So werden Aufgaben, die bislang von Endgeräten übernommen wurden, von einem verteilten Netzwerk übernommen. Blockchain bietet dabei eine mögliche Umsetzung als Transaktionsprotokoll, das ein dezentrales Web ermöglicht. /TEC-01 16/

3.2.4.3 Beispiele für dApps

Hinsichtlich der Anzahl an aktuell entwickelten dApps liegt der Schwerpunkt im Bereich der Finanzanwendungen /FIT-01 16/. Das Spektrum erweitert sich aber zunehmend auf viele weitere Bereiche. Einige bekannte Anwendungsbeispiele werden im Folgenden diskutiert:

Token-Systeme

Token können einen virtuellen Zwilling zu einem realen Wert erschaffen

Ein Token, der auf Basis einer Blockchain abgebildet wird, kann mit einer Wertmarke verglichen werden (vgl. Kapitel 4.1.2). Er bildet Güter der realen Welt ab und bezeichnet somit virtuelle Einheiten, die von einer Instanz ausgegeben werden können und häufig einen bestimmten Gegenwert abbilden. Für Token-Systeme besteht eine Vielzahl von Anwendungen. So können mittels Tokens Vermögenswerte wie US-Dollar, Gold oder Firmenanteile abgebildet, aber auch andere Eigentumsverhältnisse nachgewiesen werden. Sie stellen dabei fälschungssichere Coupons dar, die z. B. auch als Punktesystem als Anreiz verwendet werden können.

Weiterführendes Wissen: ERC-20 Token

ERC-20 steht für „Ethereum Request for Comments 20“ und stellt einen offiziellen Standard für Smart Contracts zur Token-Implementierung und dessen Austausch auf der Ethereum Plattform dar. Dieser wurde Ende 2015 von Fabian Vogelsteller und Vitalik Buterin vorgestellt. Er beschreibt die Funktionen und Ereignisse, die in einem Ethereum-Token Smart Contract implementiert werden müssen.
So erstellte Tokens sind standardisiert auf anderen Plattformen verfügbar und können somit sehr einfach für die Erstellung von sogenannten „Initial Coin Offerings (ICO)“ verwendet werden (s. Kapitel 4.1.2). /ETH-01 18/, /ETH-02 15/, /BCP-01 18/

Zahlungsverkehr, Finanzderivate und Finanzmarkt-Anwendungen

Im Bereich der Finanzdienstleistungen besteht bereits eine Vielzahl von Anwendungsfällen. Diese reichen von mobilen Bezahlsystemen, die über die Blockchain abgewickelt werden, über Finanzderivate, die dezentral gesichert werden, bis hin zu komplexen Anwendungen, die automatisierten Handel auf verschiedenen Märkten durchführen können.

Öffentliche Verwaltung

In der Verwaltung werden zunehmend Anwendungsfälle aufgetan, die insbesondere die Manipulationssicherheit und Transparenz-Eigenschaften der Blockchain-Technologie nutzen. Beispiele hierfür sind dezentrale Katastersysteme zum Nachweis des Grundstückseigentums (entsprechend eines Grundbuchs) oder die „digitale Staatsbürgerschaft“.

Dezentralisierte Datenspeicherung

Weitere Anwendungen liegen in Cloud-Services, bei denen z. B. Speicherplatz in einem dezentralen Netzwerk angeboten wird. Dies hat den entscheidenden Vorteil, dass ein „single point of failure“ ausgeschlossen wird. Die Daten werden dabei in kleinere Teile zerlegt, verschlüsselt, mittels eines Merkle trees einander zugewiesen und über das Netzwerk verteilt.

Machine-to-Machine- (M2M) und Internet-of-Things-Anwendungen (IoT)

Neue und viel diskutierte Anwendungsbereiche sind alle Möglichkeiten rund um das Thema Maschine-zu-Maschine-Kommunikation und Anbindung von technischen Einheiten im Rahmen des Internet of Things (vgl. Abbildung 3-23). So kann über eine Blockchain sowohl der Handel von Daten und Informationen in diesen vernetzten Systemen mittels Smart Contracts autonom abgewickelt, als auch die gesamte Datenhaltung inkl. Registrierung durchgeführt werden. Letztlich können ebenso Schaltbefehle übergeben werden.

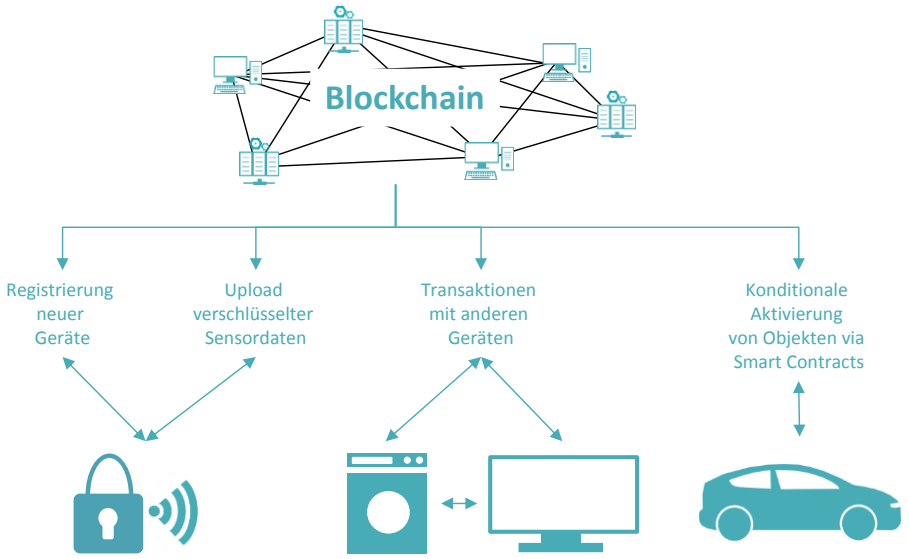

Abbildung 3-23: Möglichkeiten der Blockchain als Plattform für IoT-Anwendungen /FIT-01 16/

Distributed Autonomous Organisations (DAO)

Mittels Blockchain können Geschäftsprozesse automatisiert abgebildet werden

Distributed Autonomous Organisations (DAO) beschreiben eine neue Art der Organisation als virtuelle Einheit, die von einer Anzahl von Mitgliedern und Teilhabern gebildet wird und basisdemokratisch Entscheidungen treffen kann. Die Teilnehmer entscheiden dabei gemeinsam, wie die Organisation ihre Ressourcen verteilen soll. Die organisatorischen und operationellen Regeln werden im Vorfeld mittels Smart Contracts auf der Blockchain definiert. Diese entsprechen den Statuten (inkl. Geschäftsordnung, Gesellschaftsvertrag oder Satzung) der Organisation und agieren völlig automatisiert, sobald sie implementiert und von den Mitgliedern bestätigt wurden. DAOs haben kein zentral organisiertes Management, das die Tagesgeschäfte abwickelt. Nur außergewöhnliche Aktivitäten werden durch gewählte Teilnehmer oder externe „Agenten“ übernommen. /TEC-01 16/, /BBLU-01 18/, /ETH-02 18/

Der bislang bekannteste Versuch, eine solche Organisation zu gründen, hieß „The DAO“ und wurde 2016 in einem White Paper von Christoph Jentzsch vorgeschlagen und mit seiner Firma slock.it umgesetzt /SLO-01 16/. Das Konzept war von ihrer Funktion ähnlich eines Investmentfonds. Teilnehmer konnten DAO-Token erwerben und basisdemokratisch abstimmen, in welche Projekte, Start-Ups oder Produkte mit dem Firmenkapital investiert werden soll. Die Auswahl basierte quasi auf der „Weisheit der Vielen“ (vgl. Abbildung 3-24).

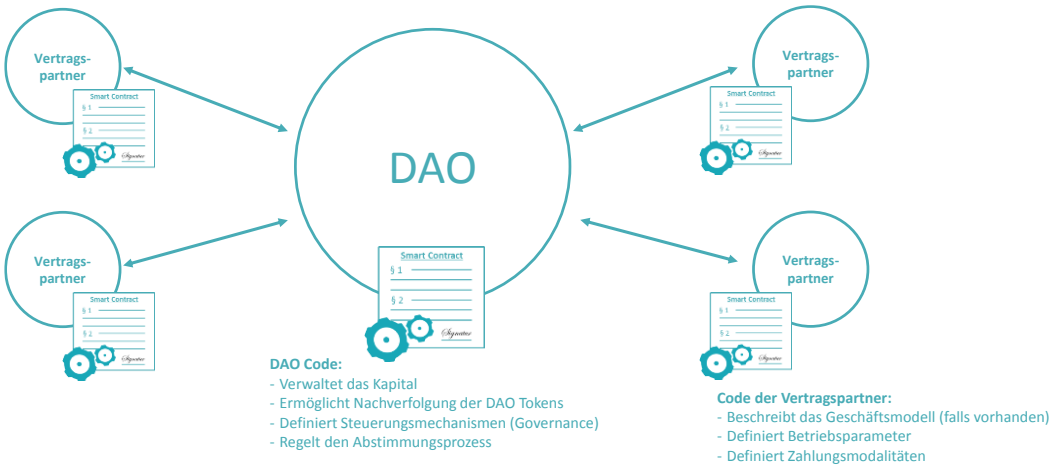

Abbildung 3-24: Beschreibung der Funktionsweise der ersten Distributed Autonomous Organisation, die 2016 von Christoph Jentzsch (slock.it) vorgestellt wurde

Die Veröffentlichung des „The DAO“ Konzepts erhielt sehr viel Aufmerksamkeit. Der damit verbundene Finanzierungsaufruf mittels eines Initial Coin Offering (ICO) Anfang 2016 brach alle Crowdfunding-Rekorde. Innerhalb kurzer Zeit wurden mehr als 160 Mio. US$ an Investmentkapital eingesammelt. Die Tatsache, dass nahezu alle Prozesse nur in Form von Code definiert werden und somit auch anfällig für Sicherheitsrisiken sind, führte schließlich auch zu einem abrupten Ende des Konzepts von „The DAO“ (vgl. „The DAO Hack“). /WIRED-101 16/

Weiterführendes Wissen: The DAO Hack

Im Juni 2016 wurde der Smart Contract von The DAO von einem unbekannten Hacker über eine fehlerhafte Sicherheits-Funktion angegriffen. Über diese Funktion wurde es möglich in einer Schleife Token in ein Unterkonto abzuziehen. Mit dieser Methode schafft es der Angreifer innerhalb kurzer Zeit DAO-Tokens im Wert von 53 Millionen US$ abzuziehen.
Es bestand allerdings eine Schutzfunktion, die den Abzug des Kapitals für eine Frist von 28 Tage sperrte. In dieser Zeit entstanden in der Ethereum-Comunity heftige Diskussionen, wie mit dem Angriff umgegangen werden sollte. Der Angreifer meldete sich über ein Bekennerschreiben und erläuterte, dass er nur nach den Regeln des Smart Contracts gehandelt hat und sich somit nicht widerrechtlich verhalten hat.
Vitalik Buterin als Vertreter der Ethereum Foundation sprach sich zunächst gegen aktive Maßnahmen aus, da die Technologie neutral agieren sollte. Nach einer Vielzahl von Lösungsvorschlägen wurde zwischenzeitlich begonnen mittels einer Gegenaktion die restlichen DAO-Tokens zu sichern. Erst kurz vor Ende der 28 Tage Frist lenkte die Ethereum Foundation ein und beschloss einen „Hard Fork“ (s. Kapitel 3.2.2), einer Abzweigung in eine neue Kette und somit der Rückstellung auf den Stand vor dem Hack und der Möglichkeit zum Rücktausch der DAO-Tokens. Die alte Kette sollte somit verschwinden, doch einige Miner verweigerten ihre Zustimmung und betreiben die alte Kette, in der der erbeutete Anteil noch existiert, unter dem Namen "Ethereum Classic" weiter. /WIRED-101 16/

Generell ist festzustellen, dass DAOs sehr komplexe Konstrukte sind, die daher auch anfällig für Systemfehler sind (vgl. Infobox „The DAO Hack“). Dennoch steht die Entwicklung erst am Anfang und bedarf noch viel Forschungs- und Entwicklungsarbeit. /TEC-01 16/

3.3 Technische Limitationen und Risiken

Eine verteilte Datenbank muss entscheidende Eigenschaften aufweisen, um Funktionalität zu garantieren. Gemäß dem sog. „CAP theorem“, können allerdings nur zwei der folgenden Eigenschaften gleichzeitig gewährleistet werden /CINI-01 17/, /HAM-01 17/:

1) **Konsistenz des gemeinsamen Zustands (Consistency)**: Das System ist im Sinne des CAP Theorems konsistent, wenn alle Knoten des verteilten Systems zu jedem Zeitpunkt die gleichen Daten sehen.
2) **Verfügbarkeit (Availability):** Das System ist verfügbar, wenn es stets auf alle Anfragen antwortet. Diese Verfügbarkeit muss im Sinne von akzeptablen Antwortzeiten gegeben sein.
3) **Partitionstoleranz (Partition tolerance):** Ein Protokoll muss auch bei Ausfall oder Manipulation eines Knotens ein korrektes Ergebnis garantieren.

Die im vorangehenden Kapitel beschriebene Technologie befindet sich noch in einem relativ frühen Stadium. Daher bestehen noch viele Herausforderungen, die derzeit Projekte in aller Welt zu lösen versuchen.

Grundlegende Herausforderungen der Blockchain-Technologie:

Herausforderungen bzgl. der Skalierung sind technisch anspruchsvoll

1. Die diskreten Blöcke und die Limitation der Blockgrößen setzen Grenzen bei der Skalierbarkeit. Es kann derzeit in bekannten Netzwerken nur eine überschaubare Anzahl an Transaktionen pro Sekunde abgewickelt werden. Die Skalierbarkeit der Technologie ist noch stark limitiert und nicht trivial lösbar:
    a. Größere Blöcke ermöglichen höhere Transaktionsraten im Netzwerk, erhöhen jedoch den Rechen- und Kommunikationsaufwand für die Konsens-Mechanismen. Dies kann v. a. im Proof of Work zu einer Zentralisierung in großen Rechenzentren und erhöhtem Energieverbrauch führen und die Hardware-Anforderungen für die Teilnahme in die Höhe treiben.
    b. Die Blockgröße kann nicht beliebig erhöht werden, da ansonsten die zu verschickenden und zu speichernden Datenmengen zu groß werden. Die Limitation stellt hier die übertragbare Datenmenge dar. Teilnehmer mit zu geringen Bandbreiten würden zunehmend vom System ausgeschlossen.
    c. Durch das ständige Vorhalten aller Informationen vergangener Transaktionen in Form der gesamten Kette steigt der Speicherbedarf der beteiligten Knoten stetig.
    d. Je aufwändiger die Möglichkeiten für Smart Contracts auf einer Blockchain sind, desto mehr Rechenzeit, -dauer und Kosten entstehen. Dies liegt an der redundanten Ausführung der Smart Contracts auf vielen dezentralen Recheneinheiten.
2. Manche Blockchain-Technologien (z. B. Bitcoin) bevorzugen das Minen mittels spezialisierter Hardware (ASIC = Application Specific Integrated Circuits). Private Nutzer können so kaum einen Beitrag zum Proof of Work liefern. Große Mining-Pools unterwandern so den dezentralen Gedanken der Technologie und aggregieren Macht.

3. Gehen die Zugriffsdaten eines Nutzers in einer public Blockchain verloren oder werden gehackt, gibt es keinerlei Möglichkeiten, diese wiederherzustellen.
4. Fälschlich durchgeführte Transaktionen (z. B. bei einem Tippfehler in der Adresse des Empfängers) können nicht rückabgewickelt werden.
5. Der Ressourcen-Verbrauch der Technologie ist stark abhängig vom verwendeten Konsens-Mechanismus. Das PoW benötigt extreme Energiemengen, um Blockchains mit einer Vielzahl von Validatoren und entsprechend hohem Konkurrenzdruck (wie Bitcoin oder Ethereum) bedienen zu können.
6. Viele Komponenten der Blockchain basieren auf der Tatsache, dass verschlüsselte Daten nur durch überproportional lange und unwirtschaftliche Rechenzeiten manipuliert werden können. Mit der Entwicklung von Quantencomputern wären einige der verwendeten Sicherheitsmechanismen jedoch in relativ geringer Zeit überwindbar /IOTA-01 17/.
7. Aufgrund der Konsens-Mechanismen ist die Macht innerhalb eines Blockchain-Netzwerks ungleich verteilt. Dadurch kann Missbrauch entstehen, wenn sich zu viele Stimmanteile (z. B. durch Rechenkapazität bei PoW) in Händen weniger befinden. Kann ein Akteur mehr als 50 % der Rechenkapazität innerhalb eines Blockchain-Netzwerkes auf sich vereinigen (PoW), kann die Blockchain theoretisch manipuliert werden.
8. Zwar ist die Anonymität in Blockchain-Anwendungen durch die Pseudonymisierung mittels public key gegeben, dennoch kann jede Transaktion nachvollzogen und ggf. Transaktionsgewohnheiten durch Big-Data-Analysen abgeleitet werden. Wird irgendwann eine Schnittstelle zur Identität des Nutzers hergestellt (z. B. die Bitcoin-Bezahlung einer Bestellung mit Klarnamen), können alle vergangenen Aktivitäten nachvollzogen werden.

Vgl. SPON-Artikel: „Die Blockchain ist auch ein Trottel-Archiv“

9. Je nach Ausgestaltungsform und Anwendung der Blockchain-Technologie kann es zudem zu einer Reihe von rechtlichen Herausforderungen kommen. Das nach EU-DSGVO Art. 17 gegebene Recht auf Löschung („Recht auf Vergessenwerden“) ist in einer dezentralisierten public Blockchain nach heutigem Stand technisch nicht möglich. Es existiert auch kein „Verantwortlicher“. Auch sind rechtlich Fragen bzgl. Smart Contracs und deren Kompatibilität mit geltendem Recht weiterhin ungeklärt („Code is Law“).
10. Die Interoperabilität zwischen verschiedenen Blockchain-Technologien (z. B. zwischen Bitcoin und Ethereum) ist bisher nicht gegeben. Branchenweite oder -übergreifende Standards sind bisher nicht definiert.
11. In public Blockchains besteht die Governance-Problematik. Änderungen an der Systeminfrastruktur sind nur möglich, wenn eine ausreichende Anzahl an Teilnehmern die Änderungen akzeptiert. Ansonsten kann es zu einem Fork kommen. Grundliegende Änderungen (auch Verbesserungen) sind daher schwierig und langwierig.
12. In public Blockchains wird immer ein (monetärer) Anreiz oder Vorteil für Knoten benötigt, sodass diese aus freien Stücken am Netzwerk teilzunehmen. Eine Trennung von Kryptowährungen ist daher auch bei anderen Anwendungsfällen nicht ohne weiteres möglich.

13. Nicht alle Konsens-Mechanismen sind ohne assoziierte Kryptowährungen umsetzbar (vgl. PoS)
14. Der Code von Smart Contracts ist öffentlich einsehbar. Sind hier Schwachstellen enthalten, können diese von allen Netzwerkteilnehmern gefunden und ggf. ausgenutzt werden. Für die korrekte Implementierung ist sind ausführliche und zeitaufwändige Review-Prozesse und Qualitätskontrollen notwendig.
15. Die Innovationen für die Lösung von Problemen erfolgt häufig auf unterschiedlichen Protokollen und sind nicht direkt mit anderen Ketten kompatibel. Die Zersplitterung und mangelnde Standardisierung ist daher sowohl ein Vorteil als auch ein Nachteil, da die Konzepte und der Code zwar offen zugänglich sind und von vielen verschiedenen Akteuren mit unterschiedlichen Zielen entwickelt werden, für jede Blockchain jedoch angepasst und in die individuellen Protokolle eingefügt werden müssen (vgl. privacy-Chains vs. Smart Contract-Plattformen).
16. Blockchains benötigen eine funktionierende digitale Infrastruktur für eine Massenadaption in der jeweiligen Branche
17. „Security-by-design“ ist eine Stärke der Technologie. Die Sicherheit durch Redundanz ist jedoch grundsätzlich ineffizienter als zentrale Lösungen. („inefficiency-by-design“)

Grundsätzlich zeigen diese Limitationen auf, dass die Technologie noch an vielen Stellen weiterentwickelt werden muss, um für großangelegte Einsatzzwecke geeignet zu sein. Nichtsdestotrotz sollte beachtet werden, dass die Technologie selbst noch relativ am Anfang steht und erst seit kurzem im Fokus des öffentlichen Interesses steht. Um die genannten Herausforderungen zu lösen, ist eine Reihe von Weiterentwicklungen notwendig, die im nächsten Kapitel beschrieben werden.

Hinsichtlich der Sicherheits-Anforderungen an die führt das Bundesamt für Sicherheit in der Informationstechnik (BSI) folgende Eckpunkte auf /BSI-03 18/:

- „Blockchain allein löst keine IT-Sicherheitsprobleme.
- Die Wahl des passenden Blockchain-Modells ist wichtig.
- Bei der Konstruktion von Blockchains müssen Sicherheitsaspekte frühzeitig berücksichtigt werden.
- Sensible Daten mit langfristigem Schutzbedarf müssen in einer Blockchain besonders geschützt werden.
- Einheitliche Sicherheitsniveaus für Blockchains müssen definiert und durchgesetzt werden.“

3.4 Weiterentwicklungen

Es findet derzeit ein rasanter Entwicklungsprozess der Technologie statt

Die Blockchain-Technologie ist noch in einem relativ frühen Entwicklungsstadium. Durch die vermehrte Nutzung, steigendes öffentliches und kommerzielles Interesse sowie hohe Marktkapitalisierungen der Kryptowährungen steigt die Anzahl der Start-Ups, Projekte und Unternehmen, welche sich mit dem Thema beschäftigen, seit dem Jahr 2015 sprunghaft an. Das wachsende Know-How und die bereitgestellten Finanzmittel, welche zur Weiterentwicklung herangezogen werden, führen zu einer starken Verbesserung der Technologie und der aufgeführten Schwachstellen. So ist durch den nicht unerheblichen

Hype, welcher die Blockchain-Technologie umgibt, zu erwarten, dass viele der aufgeführten Schwächen in den nächsten Jahren gelöst sein werden. Auch die vorhandenen Kryptowährungen unterliegen weiterhin großen Anpassungen, da die Entwickler regelmäßig bekannte Schwachstellen überarbeiten und die Technologie sukzessive verbessern.

Die heutigen Blockchain-Technologien, wie sie z. B. im Bitcoin-Netzwerk eingesetzt werden, weisen aufgrund ihrer Blockgrößen und ihrer grundlegenden Architektur Limitationen hinsichtlich der Skalierbarkeit und Anonymität auf. Das nachfolgende Kapitel beschreibt übersichtlich ausgewählte Lösungsansätze, um bestehende Restriktionen der bisher vorgestellten Blockchain-Technologien zu optimieren.

3.4.1 Programmierung und Sicherheit von Smart Contracts

Die erste und prominenteste Plattform für Smart Contracts stellt die Ethereum Blockchain dar. Smart Contracts werden hier u. a. mittels der Turing-vollständigen Programmiersprache „Solidity“ entwickelt, welche entfernt an JavaScript erinnert. Dies ermöglicht auch komplexere Logiken mit Schleifen („Loops“). Im Gegensatz dazu kommt in der Bitcoin Blockchain eine einfache nicht-Turing-vollständige Programmiersprache („Script“) zum Einsatz, welche lediglich simple Prozesse ohne Schleifen ausführen kann /BIT-01 17/. Während dies einerseits die Einsatzmöglichkeiten der Blockchain-Technologie stark reduziert, wird andererseits auch eine Überlastung des Netzwerks vermieden. Durch Endlosschleifen ist es rein theoretisch möglich, Smart Contracts und somit das Netzwerk grundsätzlich lahm zu legen. Die Ethereum-Blockchain bedient sich daher einer Gebühr für Rechenleistung (vgl. Kap. 3.2.4).

Neben dieser technologischen Restriktion unterliegen Smart Contracts einem weiteren Risiko. Ihr Code ist öffentlich einsehbar, grundsätzlich kann jeder mit ihnen interagieren und in Verknüpfung mit Kryptowährungen ist oft ein großer Wert mit ihnen verbunden. Daher haben viele ein Interesse, Schwachstellen in ihrer Programmierung zu identifizieren und diese für sich auszunutzen. Der DAO-Hack (s. Kap. 3.2.4.3 /WIRED-101 16/) oder die Parity Hacks /BID-01 17/ zeigen eindrucksvoll, dass dort Millionensummen erbeutet werden können. Eine Studie von Wissenschaftlern der National University Singapore gelang es, aus 970.898 untersuchten Smart Contracts der Ethereum-Blockchain insgesamt 34.200 Smart Contracts mit Sicherheitslücken zu identifizieren. Die Forscher wären nach eigenen Angaben dazu in der Lage gewesen 4.905 Ether zu stehlen. Dies entsprach zum Zeitpunkt der Studie (Juni 2018) einem Wert von ca. 2,9 Mio. US$. /NUS-01 18/ Dies zeigt, dass die Blockchain-Technologie zwar sicher ist, die darauf ausgeführten Smart Contracts aber oft nicht den benötigten Sicherheitsstandards gerecht werden.

Smart Contracts müssen sehr sicher programmiert werden

Diese Sicherheitslücken entstehen durch mehrerlei Gründe. Eine Überprüfung bei imperativer Programmierung ist z. B. durch Peer Reviews, Emulation, Testen oder Simulation möglich, was jedoch sehr zeitintensiv ist und oft nicht ausreichend sorgfältig durchgeführt wird. Im Gegensatz dazu ist es bei sogenannten funktionalen Programmiersprachen möglich, mathematisch zu begründen, ob ein Code Einfallstore bietet oder nicht /UPMC-01 07/. Dies verbessert die grundlegende Sicherheit von Smart Contracts. Neue Blockchain-Ansätze wie z. B. die Cardano-Blockchain setzen hier an, auch funktionale Plattformen für Smart Contracts anzubieten, um deren Sicherheit und Qualität quantifizierbar zu machen. Dabei wird (im Fall der Cardano-Blockchain) die funktionale Programmiersprache „Haskell“ für das Blockchain-Protokoll eingesetzt, während „Plutus“ für Smart Contracts als Pendant zu Solidity zum Einsatz kommt. /IOHK-01 17/ Diese Verbesserungen der Programmierschnittstellen ermöglicht es, die Sicherheit der Smart Contracts zu verbessern.

Programmier-schnittstellen (API) = application pro-gramming interface

3.4.2 Interoperabilität & Normung

Prinzipiell sind verschiedene Blockchain-Technologien (z. B. Ethereum und Bitcoin) nach heutigem Stand nicht miteinander kompatibel. Eine direkte Transaktion zwischen diesen Technologien ist derzeit nicht möglich. Nichtsdestotrotz versuchen manche Unternehmen und Projekte ähnlich wie bei Sidechains eine Verbindung zwischen diesen Technologien zu schaffen (vgl. Cosmos, Plasma, Qtum, MultiChain).

Es gibt erste Normungs-bestrebungen in der ISO/TC 307

Mittlerweile beschäftigt sich auch die internationale Organisation für Normung (ISO) im Komitee „ISO/TC 307 - Blockchain and distributed ledger technologies“ mit der Thematik Normung und Interoperabilität /ISO-01 17/. Die DIN ist an diesem Prozess beteiligt und zielt darauf ab, frühzeitig deutsche Interessen in die internationale Normung einfließen zu lassen. /DIN-03 16/

Das Thema Interoperabilität ist essenziell, um langfristig verschiedene Blockchain-Ökosysteme miteinander zu verbinden. Vitalik Buterin beschreibt in /ETH-02 16/ die folgenden Anwendungsfälle für Interoperabilität:

Interoperabilität ist in vielen Ausprägungen möglich

1. „**Portable assets**“ beschreibt die Möglichkeit, Transaktionsobjekte sicher von einer auf eine andere Blockchain und zurück zu verschieben und dort normal weiter zu verwenden.

2. “**Payment-versus-payment or payment-versus-delivery**” wird häufig unter dem Begriff “atomic swap” verwendet und beschreibt den sicheren Tausch zweier Transaktionsobjekte auf verschiedenen Ketten. Dabei können die Transaktionen nur im Paar auftreten und nur dann erfolgen, wenn die jeweils andere auf der anderen Blockchain auch ausgeführt wurde.

3. „**Cross-chain oracles**“ ermöglichen es, Ereignisse auf der einen Blockchain (A) als Auslöser für Ereignisse in Smart Contracts auf einer anderen Blockchain (B) zu nutzen. Dabei wird nicht direkt in die Blockchain (A) eingegriffen und diese beeinflusst.

4. „**Asset encumbrance**“ ermöglicht es, Transaktionsobjekte auf einer Kette zu sperren und nur durch Aktivitäten auf einer anderen Kette (bzw. Kanal) zu entsperren.

5. „**General cross-chain contracts**“ sind Smart Contracts, welche plattformübergreifend agieren und so auf verschiedenen Blockchains Aufgaben verrichten können.

3.4.3 Transaktionsgeschwindigkeit / Skalierbarkeit

Eine der Kernherausforderungen von Blockchain-Technologien stellt die Skalierbarkeit und die Transaktionsgeschwindigkeit dar. Die Lösungsansätze dafür sind vielfältig.

3.4.3.1 Sidechains

Der Begriff Sidechains ist irreführend

Der Begriff Sidechains („Nebenketten“) ist im Allgemeinen etwas irreführend, da damit implizit eine Form der Unterordnung der Nebenkette einhergeht. Es können jedoch auch zwei „Hauptketten“ (z. B. Bitcoin und Ethereum) über ähnliche Mechanismen miteinander verknüpft werden. /ETH-02 16/

Eine einheitliche Definition des Begriffes „Sidechain“ liegt bisher nicht vor. In dieser Studie wird unter Sidechains der in Kapitel 3.4.2 beschriebene Fall der „portable assets“ zwischen

zwei Ketten aufgefasst, der es ermöglicht, digitale Assets von einer Kette auf eine andere (nicht zwangsläufig untergeordnete) Kette und wieder zurück zu transferieren.

Sidechains

„Sidechains“ ist ein Sammelbegriff für interoperable Blockchains, die den Austausch von Transaktionsobjekten zwischen einander ermöglichen. So kann einerseits die Skalierbarkeit und die Funktionalität verbessert werden, andererseits steigen Komplexität und Sicherheitsrisiken.

Sidechains ermöglichen mehr Funktionalität und Komplexität

Sidechains sind parallel zur Hauptkette der Blockchain betriebene Blockchains, auf welche ein Übertrag von Transaktionsobjekten aus der Hauptkette und ggf. zurück möglich ist. Sie sind somit als kompatible, zusätzliche Parallel-Infrastruktur zu vorhandenen Blockchains zu verstehen, welche Funktionalitäten auslagern und somit die vorhandene Infrastruktur gezielt ergänzen können. Im Gegensatz zu „Altchains“ (alternativen Blockchains), welche aufgrund ihrer Inkompatibilität zu vorhandenen Lösungen zu einer Fragmentierung der Blockchain-Infrastruktur führen, sind Sidechain-Lösungen kompatibel zu einer oder mehreren vorhandenen BC-Technologien. Sie ermöglichen so die Bewegung von Transaktionsobjekten zwischen verschiedenen BCT. Ist auch wieder eine Transaktion von der Sidechain auf die Hauptkette möglich, spricht man von two-way pegged Blockchain („two-way peg“).

Die Verknüpfung zweier „two-way pegged Blockchains“ kann vereinfacht wie folgt dargestellt werden (vgl. Abbildung 3-25):

1. Der sogenannte „simplified payment verification proof“ (SPV proof) sperrt die zu transferierenden Assets auf der Hauptkette („parent chain“) für die weitere Verwendung und verhindert so die Vervielfältigung von Transaktionsobjekten zwischen den Ketten.
2. Die Sidechain erhält die Bestätigung, dass die Transaktionsobjekte auf der Hauptkette valide transferiert und gesperrt wurden sowie die Informationen über das zu transferierende Asset.
3. Auf der Sidechain wird das Asset erschaffen (z. B. die Menge an Kryptowährung, die in der Hauptkette gesperrt wurde) und für die Nutzung (z. B. für Smart-Contracts) freigegeben, bis es erneut zurück auf die Hauptkette überführt werden soll.
4. Die Rückführung erfolgt durch die Sperrung des Assets auf der Sidechain und den Übertrag der Informationen auf die Hauptkette. /BLO-101 14/

Während die meisten Blockchain-Technologien in der Lage sind, als Hauptkette zu fungieren und ihre Transaktionsobjekte auf Sidechains zu übertragen, ist ein „Erschaffen“ (Punkt 3) von Assets aus Sicherheitsgründen bisher auf ihnen nicht direkt möglich, d. h. es ist nur möglich, dieselbe Menge (oder weniger) an Transaktionsobjekten wie zuvor auf der Hauptkette zu entsperren und ggf. anderen Akteuren zuzuweisen. Hier besteht stattdessen auch die Möglichkeit eines Tausches mit einer Transaktion in die entgegengesetzte Richtung (vgl. Payment-versus-payment or payment-versus-delivery in Kapitel 3.4.2).

Sidechains sind v. a. eine Lösung für die Skalierung

Während Sidechains eine Fülle an Lösungsmöglichkeiten u. a. zu bekannten Skalierungsproblemen beitragen können, sind auch hier gewisse Nachteile zu erkennen. So wird durch Seitenketten vor allem die Komplexität gesteigert und es entstehen potenzielle Einfallstore, sollte eine der Ketten kompromittiert werden können.

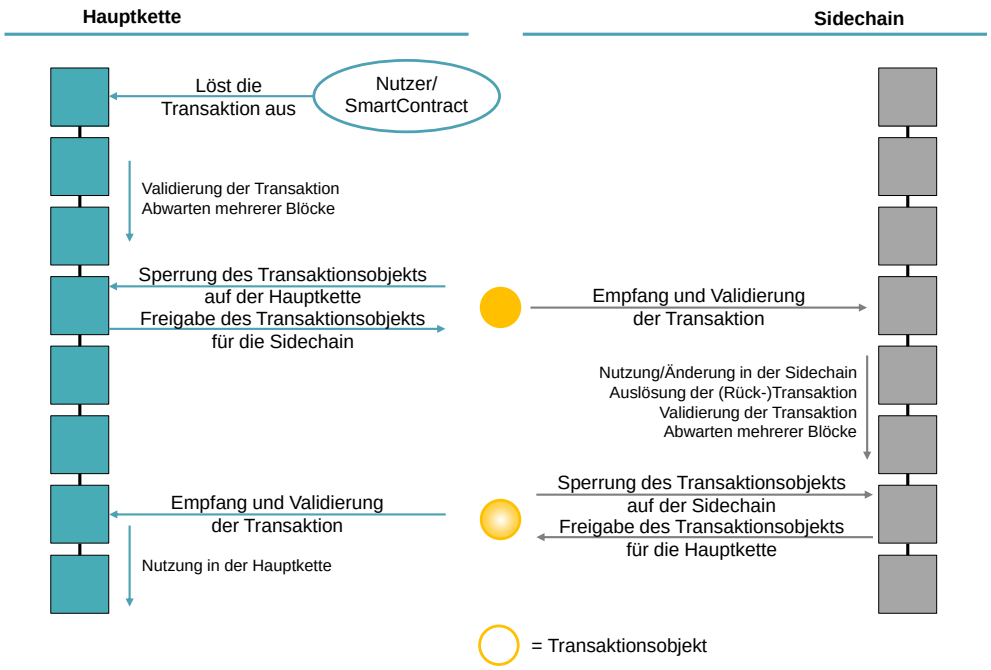

Abbildung 3-25: Schematischer Ablauf einer Transaktion auf eine Sidechain

Das Polkadot-Projekt beschäftigt sich mit den Herausforderungen, mehrere Sidechains (hier: „parachains“ genannt) mit unterschiedlichen Charakteristika (durch sogenannte „bridges“) miteinander zu verbinden und Transaktionen verschiedenster Art zwischen verschiedenen Blockchain-Technologien durchzuführen. /ETHC-01 16/

Durch Sidechain-Lösungen werden sogenannte Multi-Layer-Blockchains möglich – also mehrere parallele und hierarchisch aufgebaute Ketten (vgl. Abbildung 3-26).

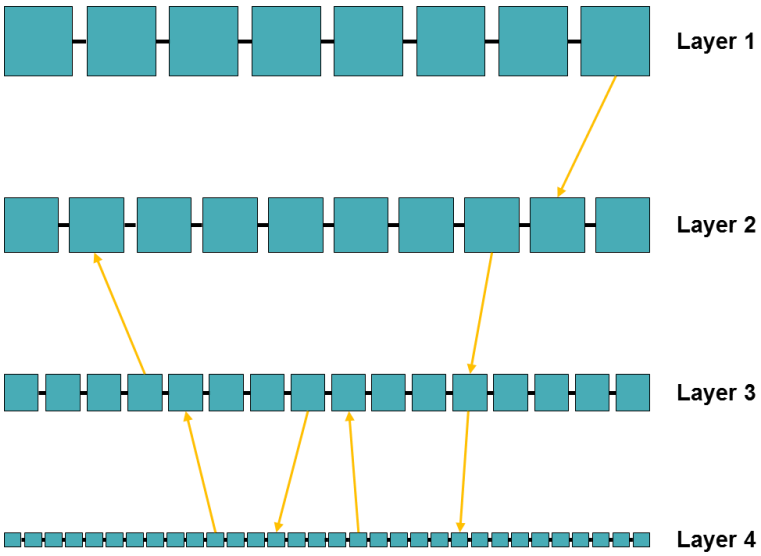

Abbildung 3-26: Schematische Darstellung von Multi-Layer-Blockchains

Rootstock ermöglicht Smart Contracts auf der Bitcoin-Blockchain

Eine weitere Möglichkeit wird durch Sidechains ersichtlich. So ist z. B. die Bitcoin-Blockchain nicht in der Lage, selbst Smart Contracts auszuführen. Durch angehängte Sidechains ist es jedoch möglich, eine parallele Kette für die Automatisierung zu nutzen. Die Rootstock-Plattform versucht, Bitcoin um diese Funktionalität zu erweitern /RSK-01 15/. Auch Plasma dient dem Zweck, durch Smart Contracts eine hierarchische Blockchain-Struktur mit Sidechains in das Ethereum-Netzwerk zu integrieren /LIG-01 17/.

3.4.3.2 State Channels

Neben Sidechains gibt es das Konzept sogenannter „state channels“ (Ethereum) oder „payment channels“ (Bitcoin) welche parallel zur Hauptkette vor allem für Mikrotransaktionen oder Transaktionen mit hohen Anforderungen an die Privatsphäre geeignet sind. Dabei wird eine Reihe von Transaktionen z. B. zwischen untereinander handelnden Parteien außerhalb der Blockchain Hauptkette durchgeführt und nur der letzte Stand, auf welchen sich die Parteien einigen können (also die letzte valide Transaktion) zurück an die Hauptkette geschickt. So kann eine Reihe von Mikro-Transaktionen eine Zeit lang außerhalb der Blockchain „gesammelt“ werden, bevor das Endergebnis an die Hauptkette weitergegeben wird. /LIG-01 16/ Eine Eigenschaft dieser State Channels ist, dass diese nach außen hin intransparent sein können und so auch Transaktionen mit höheren Datenschutzanforderungen getätigt werden können.

Das Lightning-Network ist ein funktionsfähiger „payment channel“ für Bitcoin

State Channels

State Channels dienen dem Zweck, Mikrotransaktionen außerhalb der Hauptkette auszuführen und nur das von allen Teilnehmern validierte Endergebnis auf die Blockchain zu schreiben. So müssen nicht mehr alle Transaktionen direkt auf der Blockchain geschrieben werden, wodurch mehr Transaktionen pro Sekunde möglich werden. Dadurch wird die Skalierbarkeit gesteigert und Transaktionskosten gesenkt, andererseits steigt die Intransparenz. Dies kann jedoch positive Implikationen auf den Datenschutz aufweisen.

Eine schematische Darstellung dieses Vorgangs ist **Abbildung 3-27** zu entnehmen.

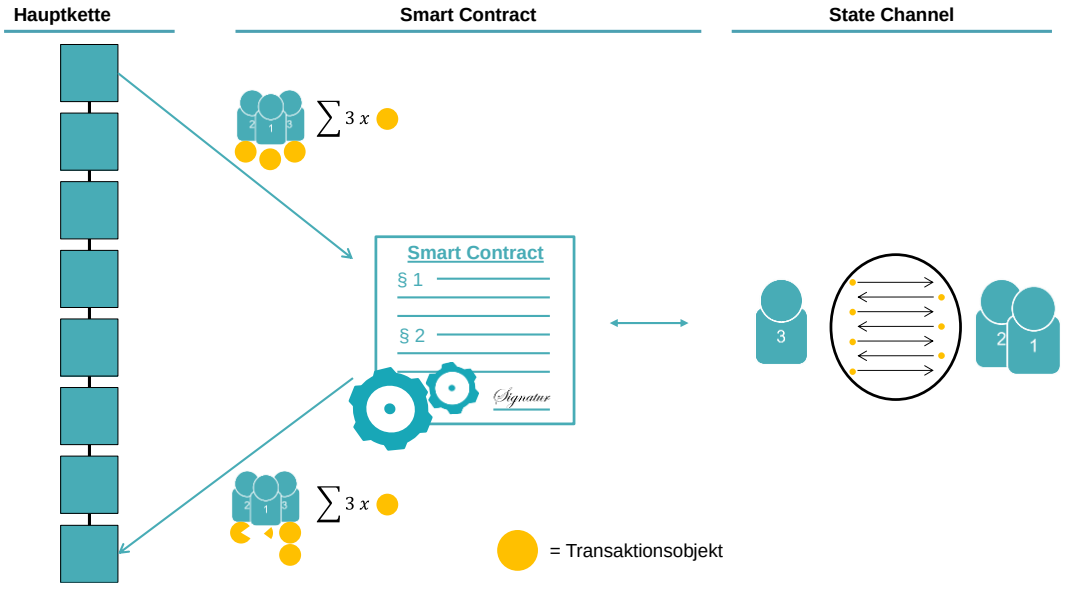

Abbildung 3-27: Schematischer Ablauf vieler Mikro-Transaktionen mittels „state channel“

Der Vorteil dieser Lösung ist, dass nur die beteiligten Parteien den Ablauf der Zwischentransaktionen sehen können, während die Hauptkette nur den Endpunkt, nicht jedoch die Zwischentransaktionen erhält und validiert. Dadurch kann das Skalierungsproblem einiger Konsens-Mechanismen teilweise verzögert werden und es müssen zur Bestätigung nicht die teilweise langen Blockzeiten abgewartet werden. So ist es möglich, Transaktionen sehr schnell und in hoher Zahl durchzuführen sowie Transaktionskosten zu sparen. Nach /RMI-01 17/ soll es mittels State Channels möglich sein, die Transaktionsgeschwindigkeit auf bis zu 10^6 Transaktionen pro Sekunde zu steigern. /LIG-01 16/

State Channels sind v. a. für unzählige und kostengünstige Microtransaktionen geeignet

Derzeit befindet sich eine Reihe von Lösungen in der Entwicklung. Unter anderem kann dieses Konzept eingesetzt werden, um die Mikro-Transaktionen zwischen Elektrofahrzeugen und induktiven Ladestationen an Ampeln in State Channels zu bündeln und beispielsweise nach einer gewissen Zeit oder Mindestsumme über die Blockchain abzurechnen.

Lightning Network /LIG-01 16/ und Raiden Network /ETH-01 17/ zielen u. a. darauf ab, für verschiedene Blockchains State-Channel-Lösungen zu implementieren. Der Austausch zwischen verschiedenen Blockchain-Lösungen (auch mit unterschiedlichen Konsens-Mechanismen) soll möglich sein, solange diese dieselbe Hash-Funktion verwenden.

3.4.3.3 Sharding

Sharding führt zu einer Aufteilung der Daten einer Block-chain in kleinere Stücke (Shards)

Wie beschrieben werden bei konventionellen Blockchain-Implementierungen die durchgeführten Transaktionen von allen teilnehmenden Nodes validiert und gespeichert. Dies führt zu stark ansteigendem Rechen- (PoW) bzw. Kommunikationsaufwand bei einer hohen Anzahl von Transaktionen und begrenzt deshalb die möglichen Transaktionen pro Zeiteinheit. Eine Möglichkeit, dieses Problem zu umgehen, ist das so genannte Sharding. Der Begriff Sharding bezieht sich ursprünglich auf die verteilte Speicherung von Datenbanken, welche eingesetzt wird, um große Datenmengen zu verwalten. Dabei wird sowohl die benötigte Speicherkapazität als auch die Rechenleistung mehrerer Server kombiniert, um die notwendigen Kapazitäten bereitstellen zu können.

Sharding ist bisher ein theoretisches Konstrukt und noch nicht implementiert

Im Blockchain-Kontext bezeichnet Sharding das Konzept, eine Transaktion nicht von allen Nodes verarbeiten zu lassen, sondern nur von einer kleinen Auswahl der Nodes im Netzwerk. /ETH-01 17/ Bisherige Ansätze zeigen, dass nur verteilte Validierung oder nur verteilte Speicherung nicht ausreichend zur Lösung des Problems beitragen, es müssen also beide Schritte entsprechend nur ausgewählten Nodes zugeordnet werden. Dies kann mittels einer Aufteilung des zu speichernden Zustands in so genannte Shards umgesetzt werden (vgl. Abbildung 3-28). Diese Shards speichern jeweils einen Teil des aktuellen Zustands sowie die zugeordneten Transaktionen und werden dementsprechend auch nur vom jeweils zugeordneten Teil der verfügbaren Nodes im Netzwerk verarbeitet. Analog zum Merkle-Tree (s. Kap. 3.2.1.1) können diese Shards übergeordnet konsolidiert und transparent gemacht werden. Die Kommunikation zwischen verschiedenen Shards erfolgt mittels spezieller Protokolle. Dies erhöht den Aufwand für Transaktionen zwischen verschiedenen Shards, weshalb die konkrete Implementierung Gegenstand aktueller Forschung ist. /ETH-01 17/

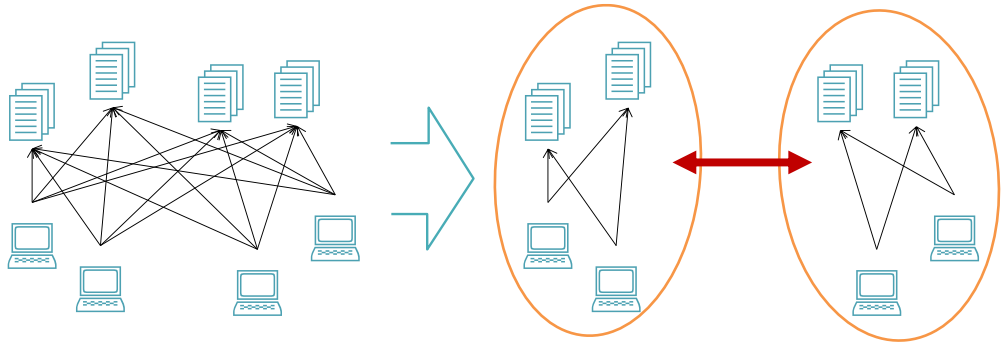

Abbildung 3-28: Sharding Konzept mittels Aufteilung des Netzwerks in sog. „Shards“

3.4.4 Anonymität

3.4.4.1 Zero-Knowledge-Proofs

Zero-Knowledge-Proofs sind ein relativ neues Verfahren in der Kryptographie, welches es ermöglicht, einem Dritten zu beweisen, dass eine gewisse Information bekannt ist oder ein Computerprogramm ordnungsgemäß berechnet wurde, ohne Informationen über Inputs, Vorgänge oder Outputs preisgeben zu müssen. Dies ist theoretisch für viele Anwendungen von großem Nutzen, wurde aber bisher in der Praxis aufgrund des hohen Aufwands wenig eingesetzt.

Zero-Knowledge-Proofs spielen v.a. für den Datenschutz eine große Rolle

Die erste Anwendung im Blockchain-Umfeld war die Kryptowährung „Zcash“, welche vollständige Anonymität der Transaktionen gewährleistet. Zero-Knowledge-Beweise werden in diesem Fall dafür eingesetzt, eine Validierung von Transaktionen durch die Blockchain zu ermöglichen, ohne die Details dieser Transaktion zu übertragen. Die technische Umsetzung basiert dabei auf zk-SNARK (**z**ero-**k**nowledge **S**uccinct **N**on-interactive **AR**gument of **K**nowledge), wodurch der Aufwand im Vergleich zu klassischen Zero-Knowledge-Protokollen deutlich verringert werden kann. Dadurch wird die Nutzung für anonymisierte Kryptowährungen praktikabel. /ZER-01 14/

zk-SNARKs sind eindeutige nicht-interaktive Argumente in ZCash

Zero-Knowledge-Proofs

Zero-Knowledge-Proofs sind kryptographische Verfahren, die Korrektheit und Validität einer Handlung (hier: in einer Blockchain) zu bestätigen, ohne Inhalte der Handlung offen legen zu müssen. Dadurch wird die Integrität und Manipulationssicherheit der Technologie bei gleichzeitig hohem Datenschutz gewährleistet. Die Lösungen sind heute jedoch noch ressourcenintensiv und haben noch einen negativen Effekt auf die Skalierbarkeit.

Eine Weiterentwicklung der zk-SNARKs sind die 2018 vorgestellten zk-STARKs (**z**ero-**k**nowledge **S**uccinct **T**ransparent **AR**guments of **K**nowledge). Während erstere aus technischer Sicht nicht vollständig transparent sind, da sie auf einem geheimen public-/private-Schlüsselpaar[7] aufbauen, ist dies bei zk-STARKS nicht mehr notwendig. zk-STARKs sind ca. 1.000 mal länger und verbrauchen dadurch mehr Speicherplatz/Datenvolumen als zk-SNARKs, sind aber nach Angaben der Entwickler quantensicher und transparenter als ihre Vorgänger. Die Entwicklung dieser Technologie befindet sich jedoch noch in einem sehr frühen Stadium. /ZER-01 18/

zk-STARKs sind die Weiterentwicklung von zk-SNARKs

3.4.4.2 Ring-Signaturen

Die Kryptowährung „Monero“ setzt statt einer vollständig transparent einsehbaren Transaktionshistorie auf sogenannte „Ring Signatures“. Anstatt wie in **Kapitel 3.2.1.2** im Kontext der Digitalen Signaturen erläutert, signiert hier nicht jeder Sendende einer Transaktion mittels seines eigenen private keys, sondern mehrere Akteure zusammen. Dies macht es für Außenstehende unmöglich, zurückzuverfolgen, woher Transaktionsobjekte stammen, da alle im Ring ausgewählten Akteure als Sender in Frage kommen. Zudem werden Transaktionsobjekte nicht direkt an die öffentliche Adresse („public address“) eines Nutzers gesendet, sondern an eine für die Transaktion generierte einmalig nutzbare Adresse („stealth address“). Um dennoch die Integrität der Daten sowie das Vermeiden von „double

Ring-Signaturen werden v. a. in der Kryptowährung Monero eingesetzt

[7] Die Zeremonie zur Schaffung dieses Schlüsselpaar in der Kryptowährung Zcash ist unter https://www.youtube.com/watch?v=D6dY-3x3teM zu sehen.

spending“ zu gewährleisten, werden zusätzlich sogenannte „key images“ verwendet, um zu erkennen, ob Transaktionsobjekte doppelt versandt wurden oder nicht. /MRL-01 15/

Ring-Signaturen

Durch Ring-Signaturen können Absender und Empfänger von Transaktionen im Netzwerk verschleiert werden. So ist es möglich mehr Anonymität und Datenschutz zu gewährleisten und dennoch die Manipulationssicherheit zu wahren. Die Lösungen sind heute jedoch noch ressourcenintensiv und haben noch einen negativen Effekt auf die Skalierbarkeit.

Ring-Signaturen gewährleisten Anonymität und Datenschutz

Die von Monero gewählte Lösung, die Transaktionshistorie zu verschleiern, führt im Gegensatz zu Bitcoin nicht nur zur Pseudonymität der Nutzer, sondern zu einer vollständigen Anonymität. Während bei klassischen Blockchain-Lösungen die gesamte Transaktionshistorie eines bekannten Nutzers überprüft werden kann, ist dies hier nicht mehr möglich. Weitere Details sind u. a. *https://getmonero.org/resources/research-lab/* sowie diversen White Papers der Entwickler (vgl. /MRL-01 15/) zu entnehmen.

Ring Confidential Transactions

Neben Ringsignaturen kommen in der Kryptowährung „Monero“ auch Ring Confidential Transactions zum Einsatz. Diese Innovation ermöglicht es, nicht nur den Absender (Ring-Signaturen) sondern auch die Anzahl der versendeten Transaktionsobjekte zu verschleiern. Dabei kommen “Multilayered Linkable Spontaneous Anonymous Group signatures (MLSAG)” zum Einsatz. /MRL-01 15/ Dadurch wird es möglich, vollkommen anonymisierte Transaktionen durchzuführen.

3.4.5 Alternative Distributed-Ledger-Technologien

3.4.5.1 Tangle (IOTA)

Die IOTA-Foundation hat ihren Hauptsitz in Berlin

Eine neue Entwicklung im Bereich der Kryptowährungen ist die sogenannte Tangle-Technologie, welche durch den Verzicht auf diskrete „Blöcke“ den Rechenaufwand pro Transaktion deutlich reduziert und so gebührenfreie Zahlungen kleinster Beträge zulässt. Dies wird auch als Kryptowährung dritter Generation bezeichnet. Die erste praktische Umsetzung ist die Währung „IOTA“, welche im August 2016 gestartet ist. Geplante Anwendungen finden sich im Bereich IoT (Internet of Things), in dem zukünftig eine sehr hohe Anzahl von Geräten interagiert und damit auch die Anzahl an Transaktionen das Maß übersteigen wird, das mit einer Blockchain-basierten Währung sinnvoll abgewickelt werden kann.

Tangle (IOTA)

Das „Tangle“ basiert auf Directed Acyclic Graphs (DAG) und ist eine Weiterentwicklung der Blockchain-Technologie, die auf Blöcke vollständig verzichtet. Dadurch wird einerseits die Skalierbarkeit verbessert, andererseits die Möglichkeiten für Smart Contracts stark eingeschränkt. Die Technologie befindet sich noch in einem sehr frühen Stadium. Ihr wird großes Potenzial für die Kommunikation und den Datenaustausch zwischen Internet-of-Things-Geräten zugeschrieben.

Das Tangle ist der spezielle Directed Acyclic Graph (DAG) in IOTA

Die technische Umsetzung des Distributed Ledger basiert auf einem „Tangle“ (deutsch: Knäuel) genannten Directed Acyclic Graph (DAG) im Gegensatz zur klassischen Chain (siehe **Abbildung 3-29**). Bei der Durchführung einer neuen Transaktion werden jeweils zwei vorangehende Transaktionen validiert und die Transaktion an der entsprechenden Stelle im

Tangle eingefügt. Aufgrund dieser kontinuierlichen Validierung findet kein „Mining“ statt wie beispielsweise bei Bitcoin, es werden also auch keine neuen Geldeinheiten generiert. Da kein Bedarf für die Zusammenfassung in Blöcke besteht, können Transaktionen sofort ausgeführt werden ohne Einschränkungen durch die notwendige Blockgröße. /IOTA-01 17/

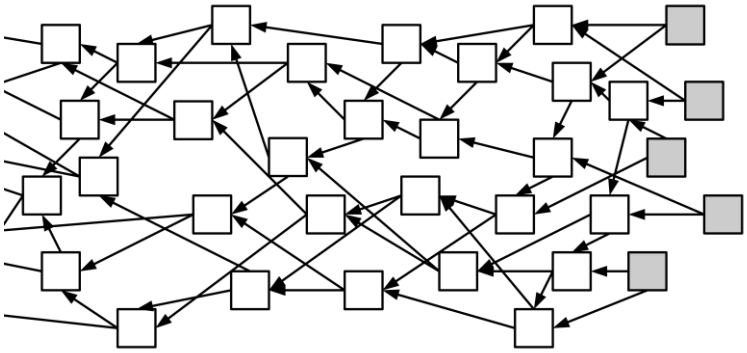

Abbildung 3-29: Schematische Abbildung eines Tangles (vgl. /IOTA-01 17/)

Neben der prominentesten Anwendung des DAG durch die IOTA-Foundation (Berlin) gibt es ähnliche Projekte wie Byteball und DAGCoin. Auch Hashgraph setzt auf DAG. Dabei ist die Systemarchitektur jedoch unterschiedlich. Grundsätzlich ist die größte Stärke und gleichzeitig Schwäche dieser Technologien das Fehlen diskreter Blöcke und die draus resultierenden Limitationen bzgl. Smart Contracts. Diese werden bei einer Blockchain während der Berechnung der Blöcke (vgl. Konsens-Mechanismen) ausgeführt. Dies ist hier nicht äquivalent abbildbar. Auch fehlt eine exakte zeitdiskrete Reihenfolge von Transaktionen, weswegen eine Vielzahl von Smart Contracts in DAG-basierten Technologien nicht abgebildet werden können.

3.4.5.2 Hashgraph

Die grundlegende Herausforderung der Blockchain-Technologie ist die Schaffung von Konsens, welcher nach derzeitigem Entwicklungsstand zu Skalierungsproblemen führt. Das sogenannte „Tangle“ (DAG) ist hier bereits eine alternative Lösung, welche statt Blöcken eine alternative Architektur mit referenzierten Transaktionen nutzt. Eine weitere Lösung stellt „Hashgraph“ dar, welches im Folgenden dargestellt wird.

Ein vollständiger Datenaustausch zwischen allen Knoten benötigt zu viel Bandbreite

Eine sehr gute Lösung zur Klärung der Validität von Transaktionen und der Konsensfindung stellt ein basisdemokratisches Governance-System auf Basis von Abstimmungen dar. Statt wie im Fall von Blockchain-Technologien dies in diskreten Zeitschritten für eine limitierte Anzahl an Transaktionen durchzuführen, wäre alternativ auch eine Abstimmung aller Knoten im Netzwerk zu jeder Transaktion eine sichere Lösung („Voting Algorithm“). Da dies jedoch aufgrund von Skalierung und Limitationen wegen der Netzwerkbandbreite nicht möglich ist, wurde mit Hashgraph eine Lösung entwickelt, welche ein vergleichbares Ergebnis erzielt, jedoch skalierbar bleibt. Dabei kommt ein sogenanntes „Gossip Protocol“ zum Einsatz. Hier wird nicht jede Transaktion zwischen allen im Netzwerk beteiligten Knoten gleichzeitig kommuniziert. Stattdessen sucht sich jeder Knoten im Netzwerk zufällige andere Knoten und teilt diesen den aktuellen Stand seines Wissens in signierter Form (siehe digitale Signaturen) mit (=“Event“) – respektive nur die jeweiligen Unterschiede der Wissensstände. Dieser Prozess nennt sich „syncing“. Dies beinhaltet u. a. die Informationen über die Transaktionspartner aller bisher stattgefundenen Transaktionen sowie Zeitpunkt und Transaktionsobjekt einer Transaktion. Zusätzlich wird auch die Information weitergegeben, woher diese Information stammt. Da der empfangene Knoten dies seinerseits an weitere zufällige Knoten kommuniziert, entsteht so über die Zeit ein gemeinsamer Konsens hinsichtlich der Transaktionshistorie. Mit einer gewissen Zeitverzögerung bildet sich so das gleiche Ergebnis wie in einem Voting Protocol, jedoch mit einer strukturellen Anordnung in

Das „Gossip Protocol“ ist ein patentierter Konsens-Mechanismus

Form eines „directed acyclic graphs“ im Gegensatz zu einer Blockchain. Im Vergleich zu einer Blockchain werden jedoch auch hier alle Events durch Hashes der vorhergehenden Events miteinander verbunden.

Im Gegensatz zu den meisten anderen Distributed-Ledger-Technologien ist die Entwicklung von Hashgraph jedoch nicht „Open-Source“ sondern patentiert. /SWI-01 16/

Hashgraph

Hashgraph ist eine spezielle Distributed Ledger Technologie basierend auf Directed Acyclic Graphs (DAG) und ist ebenfalls eine Weiterentwicklung der Blockchain-Technologie, die auf Blöcke vollständig verzichtet. Im Gegensatz zu IOTA (Tangle) wird hier jedoch eine neue Form des Konsens-Mechanismus („Gossip Protocol“) eingesetzt.

3.4.6 Wertstabile Kryptowährungen

Kryptowährungen wie Bitcoin, Ethereum, Ripple, Cardano, EOS, IOTA, Dash, Monero u. v. m. weisen heute sehr starke Wertfluktuationen auf, da sie vor allem als Spekulationsobjekte genutzt werden. Diese Eigenschaft macht sie für beständige, auf Kryptowährungen basierende Geschäftsmodelle z. B. in der Energiewirtschaft, vorerst unbrauchbar. Langfristig muss eine gewisse Wertbeständigkeit sichergestellt sein, so dass das Risiko für Anbieter und Nutzer von Dienstleistungen auf Basis von Kryptowährungen minimal ist.

Um Wertstabilität von Kryptowährungen zu gewährleisten, können Devisen wie Dollar oder Euro bzw. Ressourcen wie Öl oder Gold eingesetzt werden. Alternativ ist es auch möglich, die Verknüpfung von Coins und Tokens auf Smart-Contract-fähigen Blockchain-Netzwerken zu nutzen, um automatisch, transparent und unabhängig von Einlagen Wertstabilität zu schaffen.

Eine dieser Lösungen ist der sog. DAI-Stablecoin. Dabei kann eine Kryptowährung, wie z. B. Ethereum, durch einen Smart Contract (Collateralized Debt Position) zu „Dai“ umgetauscht werden. Durch ein ausgeklügeltes Governance-System, Sicherheitssysteme, Risikoparameter und Verknüpfungen an die Kursverläufe von FIAT-Währungen (vgl. SDR des IWF) bleibt der Kurs von DAI zu FIAT-Währungen relativ wertstabil (Target Rate Feedback Mechanism). DAI kann wie andere Kryptowährungen genutzt und u. a. für die Ausführung von komplexen Smart Contracts verwendet werden. /DAI-01 17/

Venezuela setzt mit dem „Petro“ eine durch Öl gedeckte Krypto-währung gegen Inflation ein

Stabile Kryptowährungen

Durch komplexe Smart Contracts und Mechanismen zur Stabilisierung von Kryptowährungen im Verhältnis zu Fiat-Währungen ist es möglich (relativ) wertstabile und dennoch dezentrale und unabhängige Kryptowährungen zu schaffen. Dies Verbessert deren Eigenschaften für Geschäftsanwendungen.

3.5 Technologische Möglichkeiten und Chancen

Der Economist nannte die Blockchain auf seinem Cover (2015) „The trust machine“

Die Kapitel über die Funktionsweise der Blockchain zeigen, dass Blockchain-Technologien sehr hohe Sicherheitsstandards erfüllen können, sobald die Anzahl der Akteure und die Art des Konsens-Mechanismus auf den jeweiligen Anwendungsfall angepasst sind. Die Vorteile der Blockchain umfassen nach heutigem Stand:

- Datenintegrität und Manipulationssicherheit aufgrund des Konsens-Mechanismus schaffen Vertrauen,
- Zuverlässigkeit aufgrund des Fehlens eines „single point of failure“ sowie hohe Verfügbarkeit aufgrund der vielen partizipierenden Akteure über Ländergrenzen hinweg,
- Transparenz durch den manipulationssichere und öffentlich einsehbare Distributed Ledger,
- Pseudonymität durch das eingesetzte public-/private-Schlüsselpaar statt Benutzernamen,
- hoher Grad der Automatisierung durch Smart Contracts und die Einbindung externer Events mittels Smart Contract Oracles,
- Möglichkeiten zur Individualisierung der Blockchain durch ihre Eigenschaft als Open-Source-Software (z. B. public/private/hybrid),
- dApps als Benutzerschnittstelle zu Smart Contracts, um Programme und Funktionen einer breiten Öffentlichkeit zugänglich zu machen,
- allgemein und einfach zugänglich,
- Funktionen als (volatiles) digitales und sicheres Zahlungsmittel („Kryptowährung“).

Die Blockchain-Technologie muss noch weiter-entwickelt werden

Durch die in Kapitel 3.4 dargestellten Weiterentwicklungen der Technologie lassen sich zusätzlich die folgenden Eigenschaften perspektivisch erkennen:

- Hohe **Transaktionsgeschwindigkeit** und **niedrige Transaktionskosten** u. a. durch alternative Konsens-Mechanismen, State Channels, Sharding oder alternativen DLT,
- **verbesserte Sicherheit** bei Smart Contracts durch funktionale Programmiersprachen,
- **Anonymität** und **Datenschutz** aufgrund von Weiterentwicklungen rund um Zero-Knowledge-Proofs und Ring-Signaturen bzw. Ring-Confidential-Transactions,
- **Interoperabilität** zwischen verschiedenen Blockchain-Protokollen durch zunehmende Standardisierung (vgl. ISO/TC 307 /ISO-01 17/) und technologische Fortschritte wie Sidechains und Atomic Swaps (siehe Kapitel 3.4.2),
- **verringerter Energieverbrauch** durch alternative Konsens-Mechanismen,
- **Skalierbarkeit** durch DAG-Lösungen (vgl. Tangle, Hashgraph),
- **wertstabile Kryptowährungen** durch Stablecoin-Mechanismen.
- **Verbesserte Nutzerfreundlichkeit** durch neue Systemarchitekturen und Programmierschnittstellen (API)

Abschließend lässt sich konstatieren, dass die Technologie heute noch viele Limitationen aufweist, Lösungsmöglichkeiten jedoch bereits an vielen Stellen entwickelt werden. Es ist erst in ein paar Jahren mit skalierbaren, interoperablen, nutzerfreundlichen, ggf. anonymen Blockchain-Lösungen für großflächige Geschäftsmodelle zu rechnen. Nichtsdestotrotz können bereits heute Geschäftsmodelle entwickelt, analysiert und erprobt werden, die mittelfristig eingesetzt werden können.

Die Blockchain ist noch nicht bereit für einen kommerziellen Einsatz

Weiterführendes Wissen: Analogie mit dem Internet der 90er Jahre

Parallelen zur Blockchain-Technologie (Stand 2017/2018) können zum Internet der 90er Jahre gezogen werden. Die Technologie steckt noch in den Anfängen, Skeptiker, Realisten und Optimisten versuchen gleichermaßen Vor- und Nachteile sowie aktuellen Stand hervorzuheben und die Öffentlichkeit von ihrem Standpunkt zu überzeugen. Die genauen Potenziale und Möglichkeiten der Technologie lassen sich kaum erahnen – tragfähige Geschäftsmodelle existieren nur vereinzelt. Auch Experten geben (nachträglich betrachtet) falsche Prognosen. Die Nutzerfreundlichkeit ist noch gering; eine Verwendung ist umständlich, teuer und langsam. Mit dem Fortschreiten der Technologie werden zunehmend mehr Start-Ups gegründet und die Spekulation an Aktienmärkten nimmt überhand. Ein Hype entsteht um das Thema und wird teilweise auch ausgenutzt (vgl. „Dotcom-Blase"). Diese Entwicklungen lassen sich auch im Bereich der Blockchain erkennen.
Ob die Blockchain-Technologie ähnlich disruptiv sein kann wie das Internet ist heute noch nicht objektiv zu beantworten – das Thema nüchtern zu analysieren und die Entwicklungen zu verfolgen ist jedoch grundsätzlich empfehlenswert.

Das nachfolgende Kapitel zeigt die Einsatzmöglichkeiten der Blockchain-Technologie in verschiedenen Branchen auf.

4 | Einsatzmöglichkeiten

4.1 Aktuelle Anwendungen (in verschiedenen Branchen)

In nahezu allen Branchen wird bereits mit Blockchain experimentiert

Die Blockchain-Technologie findet, über die Nutzung von Kryptowährungen hinaus, in vielen Branchen und in verschiedensten Bereichen Anwendung. In Tabelle 4-1 ist eine Auswahl von Branchen und Bereichen, in denen Blockchain-Anwendungen intensiv diskutiert werden, dargestellt.

Tabelle 4-1: Einsatzmöglichkeiten für die Blockchain-Technologie nach /CDC-01 16/, /BID-02 17/

Einsatzbereich	Beschreibung
Bankwesen und Zahlungsverkehr	Mittels Blockchain (und Kryptowährungen) wird Millionen von Menschen der Zugang zu grenzüberschreitenden Finanzdienstleistungen zugänglich gemacht. Auch sind Kryptowährungen eine sichere (wenngleich noch volatile) Alternative zu Fiat-Währungen.
Cyber Security	Die Blockchain liefert durch Verschlüsselung und die Konsens-Mechanismen ein sehr hohes Maß an Sicherheit. Dies sichert Computersysteme und Netzwerke und macht viele Bereiche der Cyber Security deutlich einfacher.
Identifikation & Identität	Heute noch analoge und zentral ausgegebenen Pässe und Identifikationsdokumente können über eine Blockchain dezentral abgewickelt werden.
Supply Chain Management	Durch eine transparente und fälschungssichere Rückverfolgung einzelner Transaktionen können alle Vorgänge entlang einer Lieferkette kostengünstig und sicher überwacht werden. Auch können mittels Blockchain Produkte bis zum Endkunden überwacht werden und so z. B. in der Pharma-Industrie Medikamentenfälschungen eingedämmt oder Kühlketten überwacht werden.
Eigentums-nachweise	Mittels der Blockchain-Technologie können Wertgegenstände jeder Art bis zum Ursprung zurückverfolgt werden und somit Eigentumsverhältnisse klar rekonstruiert werden. Beim Handel mit Diamanten findet dies bereits Anwendung (Everledger).
Urheber- & Patentrecht	Mittels der Blockchain können Patente und deren Besitzer einwandfrei identifiziert werden. Durch eine internationale Blockchain ist es auch möglich, den Besitz eines Patents oder Urheberrechts über die Ländergrenzen hinaus zu beweisen.
Beweismittel-sicherung	Mittels der Blockchain-Technologie können digitale Beweismittel (z. B. Videomaterial aus Dashcams, Dateien und Chatverläufe) direkt oder indirekt durch Hashes fälschungssicher gespeichert werden und ggf. vor Gericht als Beweismittel zugelassen werden.
Internet of Things	Die Blockchain ermöglicht dezentrale Machine2Machine Interaktion bei gleichzeitig hohen Sicherheitsstandards.

Versicherung	Durch die Blockchain-Technologie können auch kleinere Objekte direkt versichert werden bzw. wird Vertrauen geschaffen, z. B. durch den Besitznachweis oder Identitätsnachweise. Auch können durch externe Events (z. B. Naturereignisse) direkt gewisse Zahlungen automatisiert werden oder Versicherungsbetrug z. B. durch Mehrfachversicherungen vermieden werden.
Sharing Economy	Die Peer2Peer-Interaktionen der Sharing Economy basieren auf vergleichbaren Prämissen wie die Blockchain-Technologie. Statt Unternehmen wie Uber und AirBnB kann die Blockchain die Aufgabe der Vermittlung übernehmen.
Datenspeicherung	Daten können statt wie bisher zentral, dezentral und sicher auf der Blockchain gespeichert werden. Auch ist das automatisierte Verwalten/Löschen von Daten möglich.
Spenden & Gemeinnützige Organisationen	Die Blockchain-Technologie ermöglicht es, den Zahlungsverkehr transparent nachzuvollziehen und den häufig kritisierten Verwaltungsapparat, Ineffizienzen und Korruption weitestgehend zu vermeiden.
Verwaltung	Durch den hohen Automatisierungsgrad auf Basis der Smart Contracts können viele Verwaltungsaufgaben über eine Blockchain abgebildet werden und dadurch Bürokratie und Korruption vermieden werden. (Beispiele: Katastersysteme, Wahlen)
Gesundheitswesen	Das sichere Speichern von Patientendaten kann mittels Blockchain gelöst werden.
Kunst & Musik	Das Urheberrecht kann mittels Blockchain nachweislich verbessert werden. Auch können Transaktionen direkt zwischen Künstler und Nutzer abgewickelt werden.
Medien	Mittels der Blockchain-Technologie können jegliche produzierte Inhalte (Filme, Videos, Bilder, Artikel etc.) direkt verteilt und über Kryptowährungen sofort bezahlt werden.

Neben dieser Übersicht über mögliche Branchen, welche durch die Blockchain Veränderungen erfahren können, sind in Tabelle 4-2 ausgewählte Projekte aufgeführt, die die Blockchain für gezielte Anwendungen nutzen.

Tabelle 4-2: Beispielhafte Anwendungen der Blockchain-Technologie

Projekt	Beschreibung
Chronicled	Überwachung von Kühlketten im Supply-Chain-Management (Temperatur-Logger wird dafür z. B. in die Verpackung integriert)
Everledger	Identifikation und Nachverfolgung von Diamanten (z. B. durch Einschlüsse und Reinheitsgrad). Die Besitzverhältnisse dieser Diamanten werden in der Bitcoin-Blockchain hinterlegt.
Storj	Open-Source-Cloud-Speicher auf Blockchain-Basis
Spell of Genesis	Mobiles Trading-Card-Game auf Basis der Blockchain-Technologie
OriginStamp	Speicherung von Hashes von Beweismaterial (z. B. Body- oder Dashcams) zur Absicherung vor Manipulation. Dadurch könnten Dashcam-Aufnahmen vor Gericht verwertbar werden.
Augur	Dezentrale Plattform für Vorhersagen zukünftiger Ereignisse auf Basis der „Weisheit der Vielen“
Follow my Vote	Sichere und transparente Online-Plattform für Wahlen
ShoCard	Digitale Identität
Dtube	Dezentrale Plattform für Videos (vgl. Youtube) auf der Blockchain ohne Zensur und mit Bezahlung über die Kryptowährung Steem.
Steemit	Blogging und Social-Media-Plattform auf Basis der Steem-Blockchain.
Kryptokitties	Plattform zum Sammeln, Tauschen und Vermehren von bunten Kätzchen auf Basis der Ethereum Blockchain.
Neufund	Plattform zum Handeln von Unternehmensanteilen

4.1.1 Kryptowährungen

Kryptowährungen waren der erste Blockchain-Anwendungsfall

Kryptowährungen sind Blockchain-Systeme mit einer i. d. R. fest vorgegebenen Anzahl an einzigartigen Transaktionsobjekten (hier sog. „Coins“). Diese „Coins“ sind aufgrund des Aufbaus der Blockchain nicht fälschbar, manipulierbar oder beliebig reproduzierbar. Sie selbst verfügen jedoch über keinerlei intrinsischen Wert. Ein realer Gegenwert entsteht erst, wenn Personen bereit sind, auf sogenannten Exchanges (= Handelsplattformen) Fiat-Währungen in Kryptowährungen zu tauschen. Analog zu vielen Fiat-Währungen, welche heute nicht mehr durch ausreichende Goldreserven gedeckt sind, entsteht ein Wert von Geldsystemen häufig erst durch den Nutzen des Geldes selbst, Anwendungsmöglichkeiten, staatliche Regulierung und Vertrauen in die Währung. Die in Tabelle 4-3 dargestellten Eigenschaften sind Geld grundsätzlich zu Eigen.

Tabelle 4-3: Eigenschaften von Währungen nach /LUCI-01 10/, /OVM-01 07/

Eigenschaft	Bedeutung	Gewährleistung durch DLT
Knappheit	Erst durch die Knappheit eines Gutes kann diesem ein ausreichend hoher Wert zugemessen werden. So wird u. a. dessen Transport einfacher.	Im Blockchain-Protokoll ist eine feste Inflation und Anzahl der Kryptowährung vorgegeben. So wird bei PoW als Belohnung für das erfolgreiche Mining eines Blockes eine fest vorgegebene und degressive Anzahl von Coins an Miner ausgeschüttet.
Transportfähigkeit	Geld sollte einfach und schnell transportiert werden können, um als Zahlungsmittel immer und überall zum Einsatz kommen zu können.	Digitale Währungen sind grundsätzlich überall einsetzbar. Es ist jedoch immer eine digitale Infrastruktur notwendig, um sie nutzen zu können.
Teilbarkeit	Durch Teilbarkeit wird gewährleistet, dass Güter mit unterschiedlichsten Preisen damit bezahlt werden können.	Kryptowährungen sind in der Regel in sehr kleine Mengen teilbar. So entspricht 1 Satoshi 0,00000001 Bitcoin oder 1 Ether 10^{18} Wei.
Wert und Nützlichkeit	Geld ist erst ein sinnvolles System, wenn damit Waren erworben werden können.	Hier besteht derzeit noch eine große Schwäche von Kryptowährungen. Die Möglichkeiten, reale Gegenwerte käuflich zu erwerben, sind derzeit noch relativ begrenzt.
Unzerstörbarkeit & Wertstabilität	Grundsätzlich sollten Geldsysteme die Zeit möglichst unbeschadet sowohl in ihrem Wert als auch in Ihrer Substanz überdauern, so dass sie langfristig genutzt werden können.	Während Kryptowährungen zwar grundsätzlich fälschungssicher existieren, solange Knoten an der Blockchain teilnehmen, ist deren Wert derzeit noch hoch volatil.
Homogenität	Alle Münzen einer Währung sollten über denselben Wert verfügen.	Dies ist im Falle von Kryptowährungen gegeben. Alle „Coins“ verfügen über denselben Wert.

Marktkapitalisierung, Kursverlauf

Aufgrund der Volatilität der Kryptowährungen ist eine Übersicht über deren Kurse in dieser Studie nicht zielführend. Aktuelle Kurse und Börsen, auf welchen Kryptowährungen gehandelt werden können, können u. a. www.coinmarketcap.com entnommen werden.

Weiterführendes Wissen: HODL

Der Begriff „HODL" stammt aus einem Reddit-Post aus dem Jahr 2013. Ein offensichtlich betrunkener Nutzer lamentiert im Zuge eines Kursabsturzes von Bitcoin darin über seine nicht vorhandenen Fähigkeiten, hinsichtlich des Marktverhaltens die richtigen Rückschlüsse auf sein Investitionsverhalten ziehen zu können. Quintessenz seines Beitrags ist dabei, dass er seine Bitcoin trotz Kursabsturz halten wird („I am holding") wobei ihm ein Rechtschreibfehler unterläuft („I AM HODLING"). Dieser Begriff wurde schnell viral und wird bis heute verwendet.
Ausprägungsformen sind u. a.: WE OL SHAL HODL! HODLING hard! Keep HODLING.

Funktionalitäten ausgewählter Währungen

Tabelle Tabelle 4-4 zeigt ausgewählte Kryptowährungen sowie deren „unique selling propositions" (USP) auf:

Tabelle 4-4: Ausgewählte Kryptowährungen und deren Eigenschaften

Logo	Name	Kurzbeschreibung
	Bitcoin	Erste funktionsfähige Kryptowährung
	Ethereum	Erste Kryptowährung mit Smart Contracts. Blockchain-Plattform u. a. für ICO
ripple	Ripple	Blockchain für den Austausch v. a. zwischen Banken
	IOTA	Distributed Ledger auf Basis eines DAG (Tangle) für IoT-Interaktion
	Monero, ZCash, Dash	Kryptowährungen mit starkem Fokus auf Anonymität
CARDANO	Cardano	Erstellung und Ausführung von dezentralen Anwendungen und Verträgen auf Basis funktionaler Programmierung
nem	NEM, NEO	Digitale Anwendungsplattform mit Smart Contracts
	Stellar	Blockchain für Wertaustauschgeschäfte unterschiedlicher Art

Unterschiede Coins/Token

Eine Unterscheidung zwischen den beiden Begriffen „Coin" und „Token" basiert lediglich auf der zugrundeliegenden Blockchain. Coins werden explizit einer speziellen Blockchain mit deren spezifischen technischen Eigenschaften zugeordnet, wie beispielsweise der Bitcoin der Bitcoin-Blockchain und der Ether-Coin der Ethereum Blockchain. Token hingegen basieren auf einer Blockchain, die nur die Infrastruktur für sie bereitstellt. Token nutzen dementsprechend lediglich die technischen Eigenschaften einer bestimmten Blockchain, ohne diese direkt zu vertreten. So gibt es beispielsweise auf der Ethereum-Blockchain eine Vielzahl von Tokens. Beispiele hierfür sind OmiseGO (OMG), EOS (EOS), Tron (TRX), VeChain (VEN), ICON (ICX), Augur (REP), 0x (ZRX) u. v.m. (Stand: Juni 2018)

Die Erstellung eines Tokens, z. B. auf Basis von Ethereum, ist dabei relativ einfach umzusetzen, vgl. Kapitel 3.2.4.3 (ERC-20 Standard).

4.1.2 Initial Coin Offering (ICO)

2017 wurden über ICOs 3,8 Mrd. US$ eingesammelt; davon 28 Mio US$ im Bereich Energie

Initial Coin Offering (ICO) bezeichnet eine neue Art von Kapitalbeschaffung im Kontext der Blockchain-Technologie und speziell für Start-Ups und Projekte, die in diesem Bereich aktiv sind. Der Begriff bedient sich dabei einer Analogie zum Begriff Initial Public Offering (IPO), womit der Börsengang eines Unternehmens bezeichnet wird. Eine direkte Analogie des Vorgangs zu Aktienemissionen ist jedoch „weder technisch noch rechtlich der Fall“ /BFRF-01 17/.

De facto ist damit eine Art Crowdfunding verbunden, wobei eine eigene Kryptowährung für ein bestimmtes Projekt oder Unternehmen erschaffen wird. Die Einheiten dieser Währung, also Coins bzw. Tokens, können von Investoren gegen Risikokapital erworben werden. Der Zeitraum dieser ICOs ist meist im Vorfeld zeitlich begrenzt. Die handelbaren Coins oder Tokens sind in ihrer Zahl begrenzt und am Ende des ICOs größtenteils ausgeschüttet. Nach Ablauf der Frist können diese jedoch an Sekundärmärkten, sogenannten Kryptobörsen gehandelt werden. Der dort zugrundeliegende Preis bestimmt sich folglich rein aus Angebot und Nachfrage.

Initial Coin Offerings

Initial Coin Offerings (ICOs) bieten ein neues Mittel der Kapitalaufnahme zur Finanzierung von unternehmerischen Vorhaben. Es wird somit das Einsammeln von Venture-Kapital von verschiedensten privaten und institutionellen Investoren ermöglicht. Die geförderten Projekte bewegen sich meist im Kontext der Blockchain-Technologie.

46 % der ICOs im Jahr 2017 waren nicht erfolgreich

ICOs können auf verschiedene Arten durchgeführt werden, durch die neue Token bzw. Coins erstellt werden (Token Generating Event). Diese werden meist in einem „unregulierten öffentlichen Bieterverfahren an interessierte Anleger verkauft“ (Token Sale). Aktuell bestehen folgende beiden Varianten eines ICOs:

- Mittels Erstellung von Token über einen Smart Contract auf einer bestehenden Blockchain-Plattform, z. B. über einen ERC-20 Token auf Basis der Ethereum Blockchain (vgl. 3.2.4.3). Manche Blockchains, wie die „Waves-Plattform“, bieten diesen Service bereits sehr benutzerfreundlich und ohne jegliche Programmierkenntnisse an.
- Durch Schaffung einer neuen Blockchain mit eigenständigen Coins als neuer Kryptowährung. Technisch bietet es somit auch eine Lösung des Verteilungsproblems von ursprünglich erzeugten Coins einer neu aufgesetzten Blockchain. /BFRF-01 17/

Die technische Beschreibung der zu erwerbenden Token wird meist im Vorfeld in einem sogenannten Whitepaper, das von dem Emittenten veröffentlicht wird, beschrieben. Generell können die Modelle nach /CMS-01 18/ folgendermaßen charakterisiert werden:

- Intrinsic Token, bei denen der Erwerb der Token mit keinerlei expliziten Rechten verbunden ist, z. B. bei reinen Kryptowährungen.
- Der Token kann gegen eine künftige Leistung in der Zukunft eingetauscht werden

- Der Token gewährt eine zukünftige, regelmäßige Dividende, die mittels Smart Contracts definiert ist
- Der Token steht für ein Stimmrecht in einem Unternehmen (Distributed Autonomous Organization (DAO), s. Kapitel 3.2.4.3)
- Der Token bildet Unternehmensanteile ab und soll somit ein Recht am Unternehmen verkörpern, das bei Weiterverkauf auch übertragen werden kann.

Die Umsetzung eines ICOs weist typischerweise folgenden Prozess auf /BBLU-01 18/:

1. **Whitepaper**: Üblicherweise wird zu Beginn eine ausführliche Vorhabenbeschreibung veröffentlicht, in der die Idee, der konkrete Anwendungsfall und die Funktionalitäten der geplanten Anwendung bzw. des Projekts erläutert und ggf. zur Diskussion gestellt werden.
2. **Prototyp**: Die Vorstellung geht häufig mit der Präsentation eines ersten Prototyps einher.
3. **Pre-Sale**: Ein Vorab-Verkauf von Tokens wird angeboten
4. **Initial Coin Offering (ICO)**: Anteile an der geplanten Anwendung bzw. des Start-Ups werden – im Sinne eines Crowd-Investments – öffentlich angeboten.
5. **Implementierung & Markteinführung**: Die geplante Anwendung wird (mit Hilfe der eingesammelten finanziellen Mittel) umgesetzt und vertrieben.

Verbreitung und Ausblick

Weltweit finden ICOs in verschiedensten Ausprägungen großen Anklang und verzeichnen regelmäßig neue Rekorde bzgl. ihres Emissionsvolumens. Insgesamt wurden nach Schätzungen bis Ende 2017 bereits Token im Wert von über 3,8 Mrd. US$ über ICOs ausgegeben. /CMS-01 17/, /COIN-01 18/

Nichtsdestotrotz bieten ICOs keine Erfolgsgarantie; nach Hochrechnungen sind 46 % der gestarteten ICOs im Jahr 2017 gescheitert /BNS-01 18/.[8]

„Mastercoin“ bezeichnete den ersten ICO, der im Jahr 2013 Bitcoins im Wert von rund 5 Mio. US$ einsammelte. Seitdem steigern sich die Emissionswerte auf immer höhere Werte. So konnte der ICO von Bancor in nur drei Stunden ca. 150 Mio. US$ generieren. Ein weiteres populäres Beispiel ist der ICO von „The DAO“, der ebenfalls ca. 150 Mio. US$ einsammelte (vgl. Kapitel 3.2.4.3). /CMS-01 18/

Rechtliche Implikationen

Von Seiten der Regulatoren zieht das Thema entsprechend zunehmend größer werdende Aufmerksamkeit auf sich. So haben die ursprünglich größten Märkte für ICOs, China und Südkorea, diese mittlerweile verboten. Auch in Deutschland bezieht die zuständige BaFin bereits klar Stellung.

[8] Eine aktuelle Liste von anstehenden ICOs findet sich beispielsweise unter www.icowatchlist.com oder www.smithandcrown.com/icos/.

ICOs bieten ein großes Missbrauchspotenzial und unterliegen selbstverständlich rechtlichen und steuerlichen Regularien. Abbildung 4-1 zeigt eine vereinfachte rechtliche Entscheidungskette, die relevante Fragen vor der Emission eines ICOs aufwirft. /BFRF-01 17/

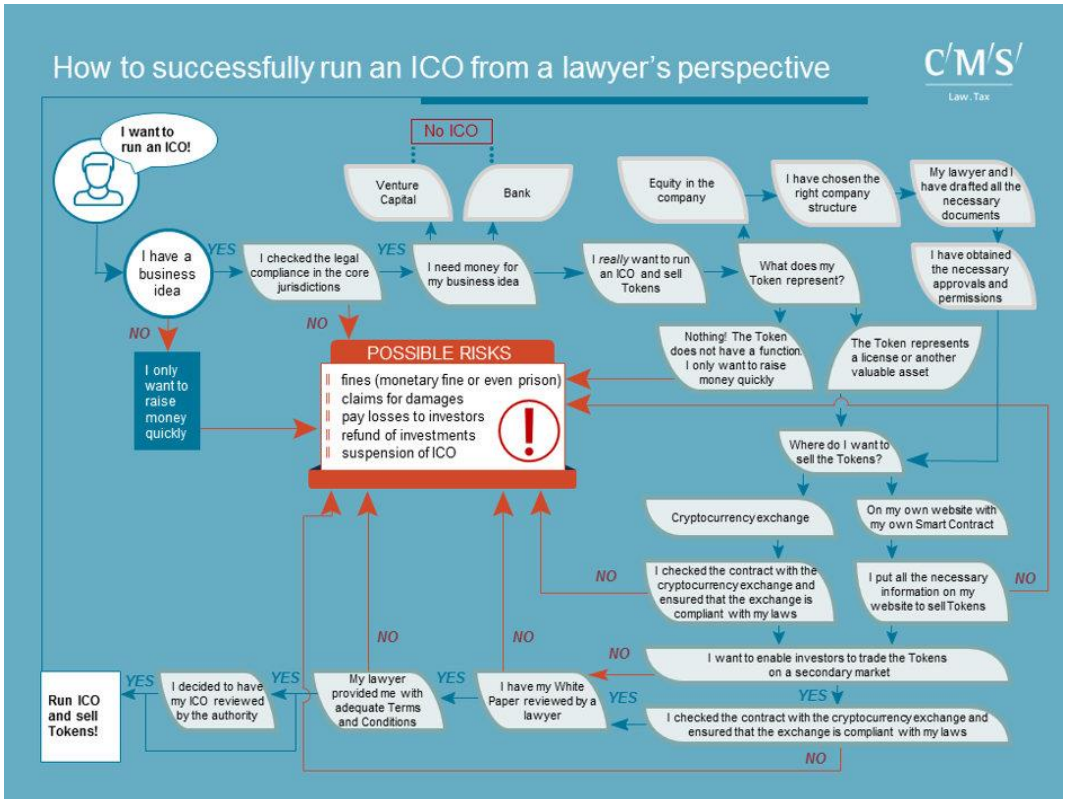

Abbildung 4-1: Entscheidungsbaum zu möglichen rechtlichen und steuerlichen Risiken eines Initial Coin Offerings /VMG-01 18/

4.2 Aktuelle Projekte in der Energiewirtschaft

Der Blockchain-Technologie wird großes Potenzial in der Energiewirtschaft zugeschrieben. Nichtsdestotrotz sind die meisten Startups zurzeit in der IKT-, Finanz- und Versicherungsbranche zu finden. Die Energiewirtschaft ist nur zu einem relativ geringen Teil vertreten. /OUT-01 17/

Tabelle 4-5 zeigt eine Übersicht über bestehende Umsetzungsprojekte aus der Energiewirtschaft (weltweit) mit dem Fokus auf Energie.

Tabelle 4-5: Aktuelle Projekte aus der Energiewirtschaft nach /BDEW-101 17/, /IAG-01 17/ und den jeweiligen Internetauftritten

Peer-to-Peer Energiehandel

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
	Conjoule	Deutschland	Conjoule Gmbh, Innogy Innovation Hub	Pilot mit privaten PV-Anlagen und Haushaltsabnehmern im Ruhrgebiet über Conjoule Plattform
	WePower	Gibraltar	WePower	P2P Handelsplattform für Energie, sowie Investmentplattform für Green Energy Projects
	Power Ledger	Australien	Power Ledger, Vector, westernpower	P2P Handel im Fokus, weitere Anwendungen wie Carbon Trading, Micro-Grid Management, Neo-Retailer
	Pylon Network	Spanien	Klenergy	Dezentrale Energiehandelsplattform
	Energimine	Großbritannien	energimine	Dezentraler globaler Energiemarkt zur Belohnung von Energieeffizienz
	Greeneum	Israel	Greeneum	Tokenisierung von Energie für den Handel auf einer dezentralen Handelsplattform
	SunContract	Slowenien	SunContract	P2P Handelsplattform für Energie
	Brooklyn Microgrid	USA	LO3, Siemens	P2P Stromhandel in einem Microgrid (Aussicht auf Blockchain ebenfalls als Steuerungselement)
	Enerchain	Deutschland	Ponton	Blockchain als Plattform für bilaterale OTC-Handelsprozesse im Strom und Gas Großhandel
	Mieterstrom	Österreich	Verbund, Salzburg AG, (FH Salzburg, Grid Singularity)	Mieterstrom (Vernetzung im Mehrfamilienhaus)

Asset Handelsplattform

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
	Green Asset Management Platform	International	IBM, Hyperledger Fabric	Handel von Carbon Assets (zunächst in China)
	Veridium	Hong Kong	Veridium Labs, ConsenSys AG, EnVision Corporation	Dezentraler Markt für Handel von Carbon Credits (Token), Natural Capital
	Poseidon	Schweiz	Poseidon	Plattform für die Erstellung, Verwaltung und Löschung von Carbon Credits / CO_2-Zertifikaten

Labeling und Zertifizierung

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
	GrünStromJeton	Deutschland	SolarDAO	Geprüfter Nachweis des tatsächlich bezogenen Strommixes für den Kunden
	ENGIE	Frankreich	ENGIE	Rückverfolgbarkeit von Wasser-, Erdgas- und Elektrizitätsflüssen
	Volt Markets	USA	Volt Markets	Monitoring und Verfolgung von Zertifikaten erneuerbarer Energien auf Basis der Ethereum Blockchain

Elektromobilität

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
SHARE & CHARGE	Share&Charge	Deutschland	Innogy Innovation Hub, slock.it	Autom. Transaktion zwischen Ladesäule und Auto via Ethereum Blockchain

Finanzierung

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
theSunExchange	the SunExchange	Südafrika	SunExchange	Marktplatz für projektbezogenes Leasing von PV Anlagen, größtenteils für Afrika
	MITO (Mitigation Token)	Russland	MITO	Plattform für „grüne“ Investitionen zur Reduktion des Klimawandels auf Basis des „DAO IPCI“
	ImpactPPA (USA)	USA	ImpactPPA	Plattform für „grüne“ Energielösungen für Entwicklungsländer auf Basis der Ethereum Blockchain

Netze

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung
enerchain	Gridchain	Deutschland	Ponton	Prozessoptimierung im Stromnetz mit Fokus auf Systemdienstleistungen (Teil des Projektes Enerchain)
sonnen	Vernetzte Stromspeicher	Deutschland	TenneT, sonnen, IBM	Einsatz von vernetzten dezentralen Heimspeichern zur Netzstabilisierung
ENERES	SmartGrid und Blockchain	Japan	Eneres	SmartGrid Vernetzung auf Blockchain-Basis zur netzdienlichen Steuerung; Pilot mit 1.000 Haushalten
vandebron	Net-balancing and e-mobility	Niederlande	Vandebron, TenneT, IBM	Netzdienstleistungen mit Elektrofahrzeugen, gesteuert mittels Blockchain
FILAMENT	Filament	USA	Transpower, Vector, Powerco	Mesh-Network zur Kommunikation von IoT-Devices u. a. auf Strommasten zur besseren Integrität von Sensordaten

Weitere

Logo	Projektname	Team	Beteiligte Firmen	Beschreibung	Tags
ENERGY WEB FOUNDATION	Tobalaba	Schweiz	Energy Web Foundation	Blockchain Testnetzwerk als öffentliche Plattform für Entwickler	Entwicklungs-umgebung
GRID+	Grid+	USA	ConsenSys	„Smart Agent“ Einheit für Haushalt zum automatisieren Stromhandel	Handel, IOT
	Farad Cryptoken	Vereinigte Arabische Emirate	Farad	Token/Währung, hinterlegt/verknüpft mit der Produktion von „ultra-capacitor cells“ zur Energiespeicherung (ERC-20 Token)	Währung
bankymoon	bankymoon	Südafrika	bankymoon	Lösung zur Zahlung von Energielieferungen auf Haushaltsebene mittels Bitcoin (von überall aus)	Währung
M-PAYG	M-PAYG	Dänemark	M-PAYG	Prepaid Lösungen für Energielieferungen in Entwicklungsländern	Währung, Finanzierung

5 | Fazit und Ausblick

Die vorliegende Metastudie zeigt, dass die Blockchain-Technologie auf einer Vielzahl von bereits existierenden technologischen Bausteinen – wie digitalen Signaturen, asymmetrischer Kryptografie und Hashing – aufbaut, um eine verteilte Datenbankstruktur zu schaffen. Dabei ist die Kerninnovation der Blockchain der sogenannte Konsensmechanismus, mit dessen Hilfe Einigkeit über vergangene Änderungen in der Datenbank (also Transaktionen) geschaffen werden kann. Dies ermöglicht es, dezentral und ohne Intermediär Vertrauen zu schaffen und gewährleistet dabei ein sehr hohes Maß an Sicherheit.

Um sogenannte Smart Contracts erweitert, wird die Blockchain zu einer Blockchain-Plattform, auf der Programme automatisiert ausgeführt und z. B. Geschäftsprozesse abgebildet, optimiert und automatisiert werden können. Diese Eigenschaften ermöglichen einen Einsatz in vielen Bereichen und Branchen – so auch der Energiewirtschaft.

Die Ausgestaltung einer Blockchain (-Plattform) ist prinzipiell frei wählbar und kann sowohl was den Datenzugriff (public / private) als auch was die Teilnahme am Konsens (permissioned / permissionless) betrifft individuell konfiguriert werden.

Eine Analyse von Stärken und Schwächen der Technologie zeigt, dass sie – unter anderem aufgrund ihres relativ kurzen Bestehens – noch vor großen technischen Herausforderungen steht und zum heutigen Stand (Q2/2018) für einen großflächigen Einsatz im Rahmen eines tragfähigen Geschäftsmodells kaum geeignet ist. Gerade Limitationen hinsichtlich der Skalierbarkeit, dem Ressourcenverbrauch durch den heute vornehmlich eingesetzten Konsensmechanismus Proof of Work sowie die fehlende Nutzerfreundlichkeit und mangelnde Interoperabilität erschweren einen Einsatz. Haftungsfragen, wie auch viele weitere rechtliche Fragen, z. B. im Bereich des Verbraucherschutzes, des Steuerrechts oder des Datenschutzes, sind bisher nicht vollständig geklärt und müssen anwendungsfallspezifisch und individuell je nach Blockchain-Konfiguration bewertet werden.

Die Betrachtung von aktuellen Weiterentwicklungen zeigt, dass die Technologie einem enormen Innovationsschub unterliegt, dabei aber stark zersplittert ist und viele verschiedene Blockchain-Protokolle existieren. Der Fokus vieler Entwicklungen liegt dabei auf unterschiedlichen Zielen, wodurch eine große Diversität entsteht. Diese sind mitunter vielschichtig und zielen vor allem auf die großen Limitationen hinsichtlich Skalierbarkeit, Interoperabilität und Anonymität ab. Die Blockchain-Technologie ist heute bereits in der Lage, Datenintegrität, Manipulationssicherheit, Zuverlässigkeit, hohe Verfügbarkeit, Transparenz und Anonymität bei digitalen Prozessen zu gewährleisten. Perspektivisch ist zu erwarten, dass durch neue Entwicklungen die Nutzerfreundlichkeit verbessert wird, Transaktionsgeschwindigkeiten- und -kosten verringert, Anonymität und Datenschutz verbessert werden, Interoperabilität geschaffen und der Energieverbrauch durch alternative Konsensmechanismen drastisch reduziert wird. Auch wenn die Konzepte grundsätzlich in andere Protokolle übertragen werden könnten, mangelt es noch an Standardisierung. Dies hat zur Folge, dass viele Innovationen auf anderen Blockchains nur zum Einsatz kommen können, wenn sie individuell angepasst werden. Eine technologische Konsolidierung hat diesbezüglich noch nicht stattgefunden.

Grundsätzlich lässt sich konstatieren, dass die Eigenschaften der Blockchain-Technologie einen vielfältigen Einsatz möglich machen. Die Einsatzmöglichkeiten umfassen u. a. das

Bankwesen, Urheber- und Patentrecht, Internet of Things, das Versicherungswesen, Sharing Economy und viele Weitere. Auch in der Energiewirtschaft ist eine Zunahme an Projekten erkennbar. So beschäftigen sich die meisten Umsetzungsprojekte mit den Themen: Peer-to-Peer Energiehandel, Asset Handelsplattformen, Labeling und Zertifizierung, Elektromobilität, Finanzierung und Netzdienstleistungen.

Ausblick

Mit der detaillierten Beschreibung wurde der Grundstein für die weitere Identifikation und Bewertung sinnvoller Anwendungsfälle der Blockchain-Technologie in der Energiewirtschaft gelegt. Im nächsten Schritt werden auf Grundlage von gemeinsamen Workshops mit den Projektpartnern des Projektes [B10X] der Forschungsstelle für Energiewirtschaft Use Cases systematisch erfasst, entwickelt und beschrieben. Darauf aufbauend wird eine Analyse- und Bewertungsmethodik entwickelt und auf die identifizierten Anwendungsfälle angewandt. Ziel ist dabei, aussichtsreiche Use Cases zu identifizieren, deren Sinnhaftigkeit und Potenzial zu bewerten und schließlich alle Voraussetzung für die Umsetzung eines Pilotprojekts zu schaffen. Eben hierzu ist ein genaues Verständnis der Blockchain-Technologie entscheidend. Die Vorstellung der Methodik, eine detaillierte Beschreibung und schließlich Bewertung der identifizierten Anwendungsfälle werden im zweiten Teilbericht vorgestellt.

6 | Abbildungsverzeichnis

7 | Tabellenverzeichnis

8 | Literaturverzeichnis

BBC-101 17 Baraniuk, Chris: Bitcoin splits as new currency takes off . In: http://www.bbc.com/news/technology-40800270. (Abruf am 2017-10-16); (Archived by WebCite® at http://www.webcitation.org/6vWn2FMmC); London: BBC, 2017.

BBL-101 14 Buterin, Vitalik: Multisig: The Future of Bitcoin. Lake Success, NY: Bob Bonomo, LLC, 2014.

BBLU-01 17 Voshmgir, Shermin: Blockchain Oracles . In: https://blockchainhub.net/blockchain-oracles/. (Abruf am 2018-01-29); Berlin: BlockchainHub by Lilon UG, 2017.

BBLU-01 18 Voshmgir, Shermin: Decentralized Applications – dApps . In: https://blockchainhub.net/decentralized-applications-dapps/. (Abruf am 2018-01-31); (Archived by WebCite® at http://www.webcitation.org/6wsQX4L8x); Berlin: Lilon UG, 2018.

BCP-01 18 Ethereum Community: The Ethereum Wiki . In: https://theethereum.wiki. (Abruf am 2018-02-22); Sydney, Australien: Bok Consulting Pty Ltd., 2018.

BDEW-101 17 Strüker, Jens et al.: Blockchain in der Energiewirtschaft - Potenziale für Energieversorger. Berlin: Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW), 2017.

BER-01 17 Fang, Max: Ethereum and Smart Contracts - Enabling a decentralized future. In: Blockchain at Berkeley; Berkeley, USA: Berkeley University of California, 2017.

BFRF-01 17 BaFin: Initial Coin Offerings - Hohe Risiken für Verbraucher. In: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2017/fa_bj_1711_ICO.html. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xQDERaAs); Bonn: Bundesanstalt für Finanzdienstleistungsaufsicht, 2017.

BID-01 17 Keogh, Eddie: The amount of ether frozen in digital wallets is worth $162 million — which is less than initially feared . In: http://www.businessinsider.de/ethereum-price-parity-hack-bug-fork-2017-11?r=US&IR=T. (Abruf am 2017-12-04); (Archived by WebCite® at http://www.webcitation.org/6wu8Clk2i); Karlsruhe: Business Insider Deutschland, 2017.

BID-02 17 Meola, Andrew: The growing list of applications and use cases of blockchain technology in business & life . In: http://www.businessinsider.de/blockchain-technology-applications-use-cases-2017-9?r=US&IR=T. (Abruf am 2017-11-08); (Archived by WebCite® at http://www.webcitation.org/6xMpKfn3h); Karlsruhe: Business Insider Deutschland, 2017.

BIT-01 17 Bitcoin community: Bitcoin Wiki . In: https://en.bitcoin.it. (Abruf am 2018-01-23); weltweit: Bitcoin community, 2017.

BITC-01 11 QuantumMechanic: Proof of stake instead of proof of work . In: https://bitcointalk.org/index.php?topic=27787.0. (Abruf am 2018-01-24); (Archived by WebCite® at http://www.webcitation.org/6whmsKOSK); Las Vegas, USA: BitcoinTalk.org, 2011.

BITF-01 15 Vavilov, Valery et al.: Proof of Stake versus Proof of Work - White Paper. Amsterdam, Niederlande: BitFury Group, 2015.

BLO-101 14 Back, Adam et al.: Enabling Blockchain Innovations with Pegged Sidechains in: https://www.blockstream.com/sidechains.pdf. Blockstream, 2014.

BNS-01 18 Sedgwick, Kai: 46% of Last Year's ICOs Have Failed Already . In: https://news.bitcoin.com/46-last-years-icos-failed-already/. (Abruf am 2018-03-05); (Archived by WebCite® at http://www.webcitation.org/6xjgZCp7P); St. Kitts: Bitcoin News, Saint Bitts LLC, 2018.

BSI-101 15 Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 1: Telematikinfrastruktur (BSI TR-03116-1). Ausgefertigt am 2015-12-03; Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015.

BSI-03 18 Blockchain sicher gestalten - Eckpunkte des BSI. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018.

BUN-01 17 Buntinx, JP: What is Delegated Byzantine Fault Tolerance? . In: https://themerkle.com/what-is-delegated-byzantine-fault-tolerance/. (Abruf am 2018-01-23); (Archived by WebCite® at http://www.webcitation.org/6wghtOz1P); Soquel, USA: The Merkle, 2017.

CDC-01 16 Szabo, Nick et al.: Smart Contracts: 12 Use Cases for Business & Beyond - A Technology, Legal & Regulatory Introduction. Washington, D.C.: Chamber of Digital Commerce, 2016.

CERT-101 01 Johnson, Don et al.: International Journal of Information Security - The Elliptic Curve Digital Signature Algorithm (ECDSA). Mississauga, Canada: Certicom Corp., 2001.

CERT-101 09 Brown, Daniel R. L: Standards for Efficient Cryptography - SEC 1: Elliptic Curve Cryptography. Mississauga, Canada: Certicom Corp., 2009.

CERT-101 10 Brown, Daniel R. L.: Standards for Efficient Cryptography - SEC 2: Recommended Elliptic Curve Domain Parameters. Mississauga, Canada: Certicom Corp., 2010.

CINI-01 17 De Angelis, Stefano et al.: PBFT vs Proof-of-Authority - Applying the CAP Theorem to Permissioned Blockchain. In: Italian Conference on Cybersecurity; Venedig, Italien: CINI Cyber Security National Laboratory, 2017.

CMS-01 17 Kaulartz, Markus et al.: BaFin: rechtmäßige ICOs sind in Deutschland möglich, aber… . In: https://www.cmshs-bloggt.de/banking-finance/bafin-rechtmaessige-initial-coin-offering-icos-in-deutschland-moeglich/. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xQDoWK0o); Köln: CMS Hasche Sigle, 2017.

CMS-01 18 Kaulartz, Markus: ICO – Initial Coin Offering . In: https://www.cmshs-bloggt.de/banking-finance/ico-initial-coin-offering/. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xQDVImG4); Köln: CMS Hasche Sigle, 2018.

COI-01 17 Castor, Amy: A (Short) Guide to Blockchain Consensus Protocols . In: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/. (Abruf am 2018-01-23); (Archived by WebCite® at http://www.webcitation.org/6wgfJxwXJ); New York: Coindesk, 2017.

COIN-01 18 Coinschedule: Cryptocurrency ICO Stats 2017 . In: https://www.coinschedule.com/stats.html?year=2017. (Abruf am 2018-03-05); (Archived by WebCite® at http://www.webcitation.org/6xjgMjvho); Hertfordshire, GB: Coinschedule Ltd., 2018.

COIND-101 17 Santori, Marco: Silk Road Goes Dark: Bitcoin Survives Its Biggest Market's Demise . In: https://www.coindesk.com/bitcoin-milestones-silk-road-goes-dark-bitcoin-survives-its-biggest-markets-demise/. (Abruf am 2017-10-14); (Archived by WebCite® at http://www.webcitation.org/6vWltqnjt); New York: Coindesk, 2017.

CUB-101 15 Pilkington, Marc: Blockchain Technology: Principles and Applications - Research Handbook on Digital Transformations. Bourgogne: COMUE Université Bourgogne Franche-Comté, 2015.

DAI-01 17 Christensen, Rune et al.: The Dai Stablecoin System - Whitepaper. Kopenhagen, Dänemark: Dai Foundation, 2017.

DIG-01 18 de Vries, Alex: Bitcoin Energy Consumption Index . In: https://digiconomist.net/bitcoin-energy-consumption. (Abruf am 2018-01-23); (Archived by WebCite® at http://www.webcitation.org/6wgiFKRvQ); Diemen, Niederlande: Digiconomist, 2018.

DIN-03 16 Jacumeit, Volker: Blockchain and Electronic Distributed Ledger Technologies - Frühzeitig dabei sein ist alles. In: https://www.din.de/de/mitwirken/normenausschuesse/nia/blockchain-and-electronic-distributed-ledger-technologies-208242. (Abruf am 2017-11-11); Berlin: DIN e. V., 2016.

DIST-01 16 Kravchenko, Pavel: Ok, I need a blockchain, but which one? In: https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xPxe2kO3); Kharkiv, Ukraine: Distributed Lab, 2016.

ECB-101 16 Pinna, Andrea et al.: Distributed Ledger Technologies in Securities Post-Trading Revolution or Evolution?. Frankfurt am Main: European Central Bank (ECB), 2016.

ETH-02 15 Vogelsteller, Fabian et al.: ERC-20 Token Standard - EIP 20. In: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xQBoFXiu); Ethereum Foundation, 2015.

ETH-02 16 Buterin, Vitalik: Chain Interoperability. Zug, Switzerland: Ethereum Foundation, 2016.

ETH-01 17 Zamyatin, Alexei: On sharding blockchains. In: https://github.com/ethereum/wiki/wiki/Sharding-FAQ. (Abruf am 2018-01-01); Zug, Switzerland: Ethereum Foundation, 2017.

ETH-01 18 Ethereum Community: Ethereum Wiki. In: https://github.com/ethereum/wiki/wiki. (Abruf am 2018-01-24); Zug, Schweiz: Ethereum Foundation, 2018.

ETH-02 18 Ethereum Foundation: Decentralized Autonomous Organization - How to build a Democracy on the blockchain. In: https://ethereum.org/dao. (Abruf am 2018-02-22); (Archived by WebCite® at http://www.webcitation.org/6xQC7JtHq); Zug, Schweiz: Ethereum Foundation, 2018.

ETHC-101 14 Wood, Gavin: Ethereum: a secure decentralised generalised transaction ledger (EIP-150 REVISION). Zug, Switzerland: ETHCORE, 2014.

ETHC-01 16 Wood, Gavin: Polkadot: Vision for a heterogeneous multi-chain framework. Zug, Switzerland: ETHCORE, 2016.

ETHE-01 15 Zamfir, Vlad: Introducing Casper “the Friendly Ghost” . In: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/. (Abruf am 2018-01-24); (Archived by WebCite® at http://www.webcitation.org/6whtGyOkR); Zug, Schweiz: Ethereum Foundation, 2015.

ETHER-01 16 Community, Ethereum: Ethereum Homestead Documentation . In: http://www.ethdocs.org/en/latest/. (Abruf am 2018-01-31); Ethereum Community, 2016.

ETHN-01 16 Manning, Jim: Proof-of-Work Vs. Proof-of-Stake Explained. In: https://www.ethnews.com/proof-of-work-vs-proof-of-stake-explained. (Abruf am 2018-01-29); (Archived by WebCite® at http://www.webcitation.org/6wpR55B4M); Los Angeles, USA: ETHNews, 2016.

EXT-01 96 Szabo, Nick: Smart Contracts: Building Blocks for Digital Markets. Los Angeles, USA: Extropy, 1996.

FIT-01 16 Schlatt, Vincent et al.: Blockchain: Grundlagen, Anwendungen und Potenziale. Bayreuth: Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, 2016.

GAB-10 17 Mitschele, Andreas: Stichwort: Blockchain . In: http://wirtschaftslexikon.gabler.de/Archiv/-2046105401/blockchain-v5.html. (Abruf am 2018-02-03); Wiesbaden: Springer Gabler Verlag, 2017.

HAM-01 17 Hammerschmidt, Chris: Consensus in Blockchain Systems. In Short. . In: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe. (Abruf am 2018-01-23); (Archived by WebCite® at http://www.webcitation.org/6wgfrMUbk); San Francisco, USA: Medium, 2017.

IAG-01 17 Blockchain in energy and utilities - Use Cases | Vendor Activity | Market Analysis. In: https://www.indigoadvisorygroup.com/blockchain. (Abruf am 2018-02-21); New York: Indigo Advisory Group, 2017.

IBM-101 86 Miller, Victor S.: Use of Elliptic Curves in Cryptography. Yorktown Heights, NY: Exploratory Computer Science, IBM Research, 1986.

IOHK-01 17 Hoskinson, Charles: Cardano Settlement Layer Documentation. In: https://cardanodocs.com/introduction/. (Abruf am 2018-01-03); (Archived by WebCite® at http://www.webcitation.org/6wu96VIQl); Hong Kong: IOHK, 2017.

IOTA-01 17 Popov, Serguei: The Tangle. Berlin: IOTA Foundation, 2017.

ISO-01 17 Dunn, Craig: ISO/TC 307 - Blockchain and distributed ledger technologies. In: https://www.iso.org/committee/6266604.html. (Abruf am 2018-01-05); Sydney, Australien: International Organization for Standardization, 2017.

JEP-101 15 Böhme, Rainer et al.: Bitcoin: Economics, Technology, and Governance. In: Journal of Economic Perspectives Volume 29, Number 2. Nashville, Tennessee: Journal of Economic Perspectives, 2015.

LAMP-01 82 Lamport, Leslie et al.: The Byzantine Generals Problem. In: ACM Transactions on Programming Languages and Systems (TOPLAS) Volume 4 Issue 3, Juli/1982. New York, USA: ACM, 1982.

LIG-01 16 Poon, Joseph et al.: The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. San Francisco: Lightning Network, 2016.

LIG-01 17 Poon, Joseph et al.: Plasma: Scalable Autonomous Smart Contracts. San Francisco, USA: Lightning Network, 2017.

LUCI-01 10 Jarchow, Hans-Joachim: Grundriss der Geldtheorie (12. Auflage). Greven: Lucius & Lucius, 2010.

MERK-101 01 Merkle, Ralph C.: One Way Hash Functions and DES. Palo Alto: Xerox PARC, 2001.

MERK-101 98 Merkle, Ralph C.: A Digital Signature based on a conventional encryption function. San Jose: Elxsi, 1998.

MIN-01 17 Mingxiao, Du et al.: A Review on Consensus Algorithm of Blockchain. In: International Conference on Systems, Man, and Cybernetics (SMC); Banff, Canada: IEEE, 2017.

MRL-01 15 Noether, Shen: Ring Confidential Transactions. Monero Research Labs, 2015.

NAKA-101 08 Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. Unbekannt: Satoshi Nakamoto, 2008.

NUS-01 18 Ivica, Nikolic et al.: Finding The Greedy, Prodigal, and Suicidal Contracts at Scale. Singapur: National University Singapore, 2018.

NXT-01 18 Whitepaper:Nxt - Nxt Wiki. In: http://nxtwiki.org/wiki/Whitepaper:Nxt. (Abruf am 2018-02-07); (Archived by WebCite® at http://www.webcitation.org/6x3JueExk): Nxt, 2018.

OUT-01 17 Burke, Jamie et al.: Startup Tracker . In: https://outlierventures.io/startups/charts/. (Abruf am 2018-02-21); Berlin: Outlier Ventures, 2017.

OVM-01 07 Hardes, Heinz-Dieter et al.: Grundzüge der Volkswirtschaftslehre. München: Oldenbourg Verlag München Wien, 2007.

PRUS-01 17 Prusty, Narayan: Building Blockchain Projects - Building decentralized Blockchain applications with Ethereum and Solidity. Birmingham, UK: Packt Publishing, 2017.

PSL-01 17 Baliga, Arati: Understanding Blockchain Consensus Models . In: https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf. (Abruf am 2018-01-23); Santa Clara: Persistent Systems Ltd., 2017.

PU-01 36 Turing, Alan: On computable numbers, with an application to the Entscheidungsproblem. New Jersey, USA: Princeton University, 1936.

RMI-01 17 Zeranski, Todd: Energy companies join forces with Rocky Mountain Institute and Grid Singularity to launch global blockchain initiative for energy . In: https://www.rmi.org/about/news-and-press/press-release-energy-web-foundation-launch/. (Abruf am 2018-01-03); (Archived by WebCite® at http://www.webcitation.org/6wuIH4Jn8); Basalt, Colorado/Vienna, Austria: Rocky Mountain Institute (RMI), 2017.

RSK-01 15 Lerner, Sergio Demian: RSK Rootstock Plattform - Bitcoin powered Smart Contracts (White paper). Buenos Aires, Argentinien: Rootstock (RSK), 2015.

SCHOL-01 18 Scholtka, Boris et al.: Blockchain in der Energiewirtschaft - Rechtsfragen bei Blockchain und Smart Contracts. In: EWeRK Fachseminar; Berlin: PwC Legal, 2018.

SLO-01 16 Jentzsch, Christoph: Decentralized Autonomous Organizations to automate governance - White Paper. Mittweida: slock.it, 2016.

SU-101 76 Diffie, Whitfield et al.: New Directions in Cryptography in IEEE Transactions on Information Theory archive Volume 22 Issue 6, November 1976. Stanford: Stanford University, 1976.

SUC-101 00 López, Julio et al.: An Overview of Elliptic Curve Cryptography. Sao Paulo, Brazil: State University of Campinas (Institute of Computing), 2000.

SWI-01 16 Baird, Leemon: The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. College Station TX (USA): Swirlds, Inc, 2016.

TAP-01 17 Tapscott, Don et al.: Blockchain Revolution - How the technology behind Bitcoin is changing money, business and the world. New York: Penguin Random House LLC, 2017.

TEC-01 16 Voshmgir, Shermin: Blockchains, Smart Contracts und das Dezentrale Web. Berlin: Technologiestiftung Berlin, 2016.

TUI-101 14 Schäfer, Günter et al.: Netzsicherheit - Grundlagen & Protokolle, Mobile & drahtlose Kommunikation, Schutz von Kommunikationsinfrastrukturen. Ilmenau: Technische Universität Ilmenau, 2014.

UB-101 14 Mann, Christopher et al.: Two-factor Authentication for the Bitcoin Protocol. Bonn: Universität Bonn, 2014.

UOC-101 04 Rogaway, Phillip et al.: Cryptographic Hash-Function Basics: Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance, and Collision Resistance. Davis, CA: Dept. of Computer Science, University of California, 2004.

UPMC-01 07 Manoury, Pascal: Functional programming, inductive data types and proofs. Paris: Université Pierre et Marie Curie, 2007.

VMG-01 18 Kaulartz, Markus: 10 Dinge, an denen ein ICO scheitern kann - How to successfully run an ICO from a lawyer's perspective. In: https://www.gruenderszene.de/allgemein/rechtskonform-ico-regulierung-bafin-finanzierung-recht. (Abruf am 2018-03-01); (Archived by WebCite® at http://www.webcitation.org/6xaZaOWxQ); Berlin: Vertical Media GmbH, 2018.

WIRED-101 16 Biederbeck, Max: Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen . In: https://www.wired.de/collection/business/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde. (Abruf am 2017-10-13); (Archived by WebCite® at http://www.webcitation.org/6vWmiy8ld); Berlin: Condé Nast Verlag GmbH, 2016.

ZER-01 14 Ben-Sasson, Eli et al.: Zerocash: Decentralized Anonymous Payments from Bitcoin. Haifa, Israel: Zerocash, 2014.

ZER-01 18 Ben-Sasson, Eli et al.: Scalable, transparent, and post-quantum secure computational integrity. Haifa, Israel: Zerocash, 2018.

ZHE-01 17 Zheng, Zibin et al.: An Overview of Blockchain Technology - Architecture, Consensus, and Future Trends. In: 6th International Congress on Big Data; Honolulu, Hawaii, USA: IEEE, 2017.