Blockchain: Hype oder Innovation

Christoph Meinel, Tatiana Gayvoronskaya,
Maxim Schnjakin

Technische Berichte Nr. 113

des Hasso-Plattner-Instituts
für Digital Engineering
an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam

Technische Berichte des Hasso-Plattner-Instituts für
Digital Engineering an der Universität Potsdam | 113

Christoph Meinel | Tatiana Gayvoronskaya | Maxim Schnjakin

Blockchain

Hype oder Innovation

Universitätsverlag Potsdam

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

Universitätsverlag Potsdam 2018
http://verlag.ub.uni-potsdam.de/

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 2533 / Fax: 2292
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Druck: docupoint GmbH Magdeburg

ISBN 978-3-86956-394-7

Zugleich online veröffentlicht auf dem Publikationsserver der Universität Potsdam:
URN urn:nbn:de:kobv:517-opus4-103141
http://nbn-resolving.de/urn:nbn:de:kobv:517-opus4-103141

The term blockchain has recently become a buzzword, but only few know what exactly lies behind this approach. According to a survey[1], issued in the first quarter of 2017, the term is only known by 35 percent of German medium-sized enterprise representatives. However, the blockchain technology is very interesting for the mass media because of its rapid development and global capturing of different markets.

For example, many see blockchain technology either as an all-purpose weapon – which only a few have access to – or as a hacker technology for secret deals in the darknet. The innovation of blockchain technology is found in its successful combination of already existing approaches: such as decentralized networks, cryptography, and consensus models. This innovative concept makes it possible to exchange values in a decentralized system. At the same time, there is no requirement for trust between its nodes (e.g. users).

With this study the Hasso Plattner Institute would like to help readers form their own opinion about blockchain technology, and to distinguish between truly innovative properties and hype.

The authors of the present study analyze the positive and negative properties of the blockchain architecture and suggest possible solutions, which can contribute to the efficient use of the technology. We recommend that every company define a clear target for the intended application, which is achievable with a reasonable cost-benefit ration, before deciding on this technology. Both the possibilities and the limitations of blockchain technology need to be considered. The relevant steps that must be taken in this respect are summarized for the reader in this study.

Furthermore, this study elaborates on urgent problems such as the scalability of the blockchain, appropriate consensus algorithm and security, including various types of possible attacks and their countermeasures. New blockchains, for example, run the risk of reducing security, as changes to existing technology can lead to lacks in the security and failures.

After discussing the innovative properties and problems of the blockchain technology, its implementation is discussed. There are a lot of implementation opportunities for companies available who are interested in the blockchain realization. The numerous applications have either their own blockchain as a basis or use existing and widespread blockchain systems. Various consortia and projects offer „blockchain-as-a-service“ and help other companies to develop, test and deploy their own applications.

This study gives a detailed overview of diverse relevant applications and projects in the field of blockchain technology. As this technology is still a relatively young and fast developing approach, it still lacks uniform standards to allow the cooperation of different systems and to which all developers can adhere. Currently, developers are orienting themselves to Bitcoin, Ethereum and Hyperledger systems, which serve as the basis for many other blockchain applications.

The goal is to give readers a clear and comprehensive overview of blockchain technology and its capabilities.

[1] Source eco, survey by YouGov, Germany, 25.01.2017 to 04.02.2017, Respondents: 266 decision-makers from medium-sized companies [104].

Der Begriff „Blockchain“ ist in letzter Zeit zu einem Schlagwort geworden, aber nur wenige wissen, was sich genau dahinter verbirgt. Laut einer Umfrage[2], die im ersten Quartal 2017 veröffentlicht wurde, ist der Begriff nur bei 35 Prozent der deutschen Mittelständler bekannt. Dabei ist die Blockchain-Technologie durch ihre rasante Entwicklung und die globale Eroberung unterschiedlicher Märkte für Massenmedien sehr interessant.

So sehen viele die Blockchain-Technologie entweder als eine Allzweckwaffe, zu der aber nur wenige einen Zugang haben, oder als eine Hacker-Technologie für geheime Geschäfte im Darknet. Dabei liegt die Innovation der Blockchain-Technologie in ihrer erfolgreichen Zusammensetzung bereits vorhandener Ansätze: dezentrale Netzwerke, Kryptographie, Konsensfindungsmodelle. Durch das innovative Konzept wird ein Werte-Austausch in einem dezentralen System möglich. Dabei wird kein Vertrauen zwischen dessen Knoten (z. B. Nutzer) vorausgesetzt.

Mit dieser Studie möchte das Hasso-Plattner-Institut den Lesern helfen, ihren eigenen Standpunkt zur Blockchain-Technologie zu finden und dabei unterscheiden zu können, welche Eigenschaften wirklich innovativ und welche nichts weiter als ein Hype sind.

Die Autoren der vorliegenden Arbeit analysieren positive und negative Eigenschaften, welche die Blockchain-Architektur prägen, und stellen mögliche Anpassungs- und Lösungsvorschläge vor, die zu einem effizienten Einsatz der Technologie beitragen können. Jedem Unternehmen, bevor es sich für diese Technologie entscheidet, wird dabei empfohlen, für den geplanten Anwendungszweck zunächst ein klares Ziel zu definieren, das mit einem angemessenen Kosten-Nutzen-Verhältnis angestrebt werden kann. Dabei sind sowohl die Möglichkeiten als auch die Grenzen der Blockchain-Technologie zu beachten. Die relevanten Schritte, die es in diesem Zusammenhang zu beachten gilt, fasst die Studie für die Leser übersichtlich zusammen.

Es wird ebenso auf akute Fragestellungen wie Skalierbarkeit der Blockchain, geeigneter Konsensalgorithmus und Sicherheit eingegangen, darunter verschiedene Arten möglicher Angriffe und die entsprechenden Gegenmaßnahmen zu deren Abwehr. Neue Blockchains etwa laufen Gefahr, geringere Sicherheit zu bieten, da Änderungen an der bereits bestehenden Technologie zu Schutzlücken und Mängeln führen können.

Nach Diskussion der innovativen Eigenschaften und Probleme der Blockchain-Technologie wird auf ihre Umsetzung eingegangen. Interessierten Unternehmen stehen viele Umsetzungsmöglichkeiten zur Verfügung. Die zahlreichen Anwendungen haben entweder eine eigene Blockchain als Grundlage oder nutzen bereits bestehende und weitverbreitete Blockchain-Systeme. Zahlreiche Konsortien und Projekte bieten „Blockchain-as-a-Service“ an und unterstützen andere Unternehmen beim Entwickeln, Testen und Bereitstellen von Anwendungen.

Die Studie gibt einen detaillierten Überblick über zahlreiche relevante Einsatzbereiche und Projekte im Bereich der Blockchain-Technologie. Dadurch, dass sie

[2] Quelle eco, Erhebung durch YouGov, Deutschland, 25.01.2017 bis 04.02.2017, Befragte: 266 Entscheider aus mittelständischen Unternehmen [104].

noch relativ jung ist und sich schnell entwickelt, fehlen ihr noch einheitliche Standards, die die Zusammenarbeit der verschiedenen Systeme erlauben und an die sich alle Entwickler halten können. Aktuell orientieren sich Entwickler an Bitcoin-, Ethereum- und Hyperledger-Systemen, diese dienen als Grundlage für viele weitere Blockchain-Anwendungen.

Ziel ist, den Lesern einen klaren und umfassenden Überblick über die Blockchain-Technologie und deren Möglichkeiten zu vermitteln.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

Der Begriff Blockchain hält sich in letzter Zeit in den Schlagzeilen. Immer mehr Artikel, aber auch Berichte und Studien versuchen, der breiten Öffentlichkeit das „Phänomen“ zu erklären. Die Technologie, das erste Blockchain-Projekt Bitcoin und neue Einsatzbereiche sollen verständlich gemacht werden. Doch trotz der zahlreichen Erklärungen fühlen sich viele Leser mit den neuen technischen Begriffen und Funktionalitäten oft alleingelassen. Die polarisierenden Schlagzeilen helfen ihnen meist nicht, einen eigenen Standpunkt zu entwickeln, sondern sie legen ihnen nahe, sich für oder gegen die Blockchain-Technologie zu entscheiden.

Handelt es sich um ein Allheilmittel für alle Probleme oder etwa nur um ein neues, unnötig kompliziertes Hirngespinst von Informatikern, das die Medien für sich entdeckt und zu einem Hype gemacht haben?

Mit dieser Studie möchten wir den Lesern helfen, sich eine eigene Meinung zur Blockchain-Technologie zu bilden und zwischen Innovation und Hype unterscheiden zu können.

1.1 Was ist eigentlich Blockchain?

Die Geschichte der Blockchain-Technologie ist noch jung und resultiert aus dem Wunsch, das Finanzwesen zu revolutionieren und ein von Dritten unabhängiges, digitales Zahlungssystem zu entwickeln.

Mit dem Begriff digitales Zahlungssystem verbinden viele zunächst das klassische Online-Banking: Transaktionen werden dabei nicht mehr in einer Bank-Filiale, sondern digital von zuhause aus oder über mobile Endgeräte getätigt. Unabhängig davon, ob sie am Bankschalter oder mittels Online-Banking ausgeführt wird, kann eine Bank-Überweisung mehrere Tage in Anspruch nehmen, da die Transaktionen in beiden Fällen anschließend von der Bank abgewickelt werden.

Aber was ist, wenn die Transaktionen direkt zwischen den Bank-Kunden selbst abgewickelt werden könnten ohne eine zentrale Instanz wie die Bank in die Transaktionsabwicklung zu involvieren? Die Idee dazu hatte der Bitcoin-„Erfinder“ Satoshi Nakamoto 2008, als er erstmals sein Konzept einer Kryptowährung namens Bitcoin skizzierte, also einer digitalen Währung mit einem dezentralen und kryptographisch abgesicherten Zahlungssystem [3].

Das Weglassen einer zentralen Instanz spart bei finanziellen Transaktionen sehr viel Zeit und Geld. Es war aber zunächst schwer vorstellbar, wie ein System eigenständig, ohne einen Administrator, funktionieren soll, der danach schaut, ob alles in Ordnung ist, bei auftretenden Problemen eingreift und Fehler behebt. Es wirkte anfangs wie eine Utopie: Ein Zahlungssystem, das sich selbst verwaltet, in dem alle Nutzer die gleichen Rechte haben und bei dem nicht Vertrauen in den Empfänger

Voraussetzung dafür ist, um an ihn Geld zu überweisen. Doch für dies alles sorgt die zugrunde liegende Blockchain-Technologie.

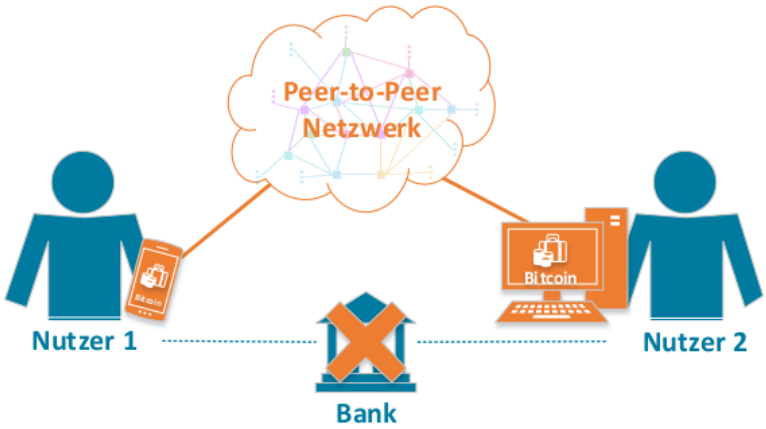


Abbildung 1.1: Bitcoin-Prinzip

Die Idee eines sicheren dezentralen Zahlungssystems, welches aus einem Netzwerk miteinander interagierender Nutzer (technisch „Knoten“ genannt) besteht und keine zentrale Verwaltungsinstanz hat, gab es bereits vor Bitcoin. Allerdings hatte sich kein bisheriger Versuch durchgesetzt, da es entweder Fehler in der Konzeption oder Probleme mit der Sicherheit (Problem der doppelten Ausgabe des gleichen Geldes[3]) gab.

Daher ist die Blockchain-Technologie eine neue und erfolgreiche Kombination bereits bekannter Technologien.

Die Begriffe Blockchain und Bitcoin werden oft als Synonyme angesehen. Dabei ist Blockchain eine Technologie und Bitcoin ein System, das die Technologie für die digitale Zahlungsabwicklung verwendet. Der gesamte Quellcode des Bitcoin-Systems ist öffentlich einsehbar (Open Source) und alle Nutzer können den Code für ihre eigenen Blockchain-Anwendungen nutzen. Die digitale Währung des Bitcoin-Systems heißt ebenfalls Bitcoin (BTC[4]). Diese ist durch eine kryptographische Prüfung abgesichert und wird deshalb als Kryptowährung bezeichnet (siehe Kapitel 2.2.1). Unter Blockchain versteht man eine Liste aller Transaktionen, die jemals in dem jeweiligen System (z. B. Bitcoin) durchgeführt wurden und die ihrerseits in Blöcke aufgeteilt sind (z. B. in Bitcoin sind es zwischen 900 und 2500 Transaktionen pro Block). Die Blöcke bilden eine Kette[5], so dass jeder folgende Block einen kryptographischen Verweis auf den vorigen Block trägt. In den Trans-

[3] Engl. double spending problem (siehe im Kapitel 2.4.3).

[4] BTC ist die Bezeichnung der Bitcoin-Währung. Bitcoin hat mehrere dezimale metrische Einheiten. Z.B. 0,1 BTC ist ein Deci-Bitcoin (dBTC), 0,01 BTC ist ein Centi-Bitcoin (cBTC), 0,001 BTC ist ein Milli-Bitcoin (mBTC), 0,000001 BTC ist ein Micro-Bitcoin (µBTC) und 0,00000001 BTC ist die kleinste Einheit und heißt Satoshi.

[5] Engl. Block Chain – Blockkette.

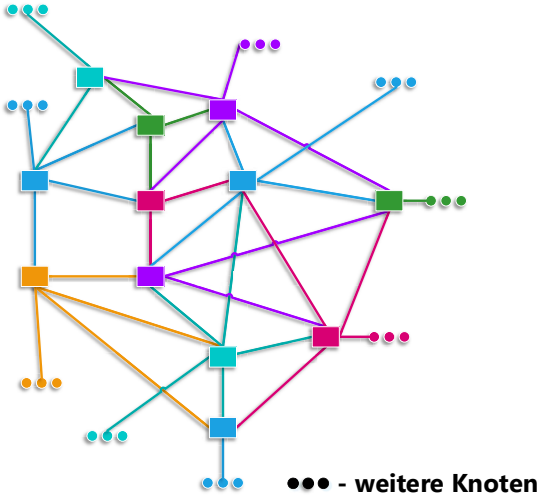


Abbildung 1.2: Ein dezentrales Netzwerk (Peer-to-Peer-Netzwerk)

aktionen werden bestimmte Werte von einer Adresse (vergleichbar mit einer Kontonummer) an eine andere übermittelt. Im Bitcoin-System zum Beispiel sind die Werte die Bitcoins, die per Transaktion übermittelt werden. Außer Kryptowährung können die Werte einen Besitz (etwa ein gemietetes Apartment, das seine Mieter wechselt) oder ein bestimmtes Ereignis (z. B. eine Berechtigung eine Büro-Tür aufzuschließen) darstellen, welche ins Blockchain-„Grundbuch“ eingetragen werden. Aus diesem Grund nennt man die Blockchain-Technologie auch das „Internet der Werte“ oder in Englisch „Internet of Value“ (siehe Abbildung 1.3).

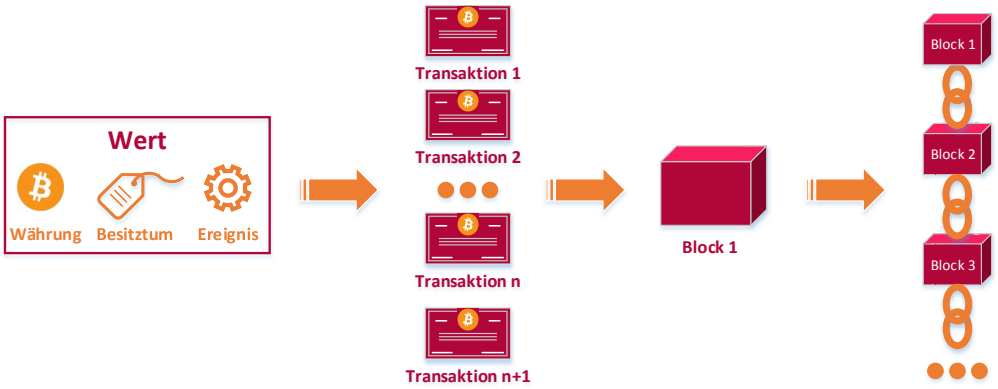


Abbildung 1.3: Blockchain-Technologie als Internet der Werte

Die Blockchain wird nicht zentral auf einem Server gespeichert, verwaltet und anschließend an alle Nutzer verteilt. Vielmehr speichert und verwaltet jeder „vollständige Nutzer“[6] die Blockchain gemäß den im System festgelegten Regeln.

Die Transaktionen werden zwischen einzelnen Teilnehmern und ohne Beteiligung von Dritten (z. B. Banken) so abgewickelt, dass die bereits ausgeführten Transaktionen nicht widerrufen werden können.

1.2 Bitcoin war erst der Anfang

2008 war das Geburtsjahr des Bitcoin-Systems. Im November publizierte Satoshi Nakamoto darüber ein White Paper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“. Bereits im Januar 2009 wurde die erste Version der Open-Source-Software veröffentlicht.

> „What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. [132]“

Da nicht bekannt ist, wer Satoshi Nakamoto ist, wird vermutet, dass der Name ein Pseudonym darstellt und für eine Gruppe von Entwicklern steht.

Um Bitcoins zu verwalten (speichern, überweisen, empfangen), benötigt der Nutzer eine Bitcoin-Geldbörse[7], diese wird auch Wallet genannt. Dafür gibt es mobile, Desktop- und Web-Anwendungen. Es gibt ebenfalls physische Bitcoin-Geldbörsen, wie Hardware- und Papier-Geldbörsen[8] (Abbildung 1.4).

Die Bitcoins können wie jede andere Währung über zahlreiche Plattformen im Internet gegen eine Gebühr gekauft und umgetauscht werden, etwa über CoinBase, BitPay oder AnycoinDirect. Da die Nachfrage nach Bitcoins sehr stark schwankt, unterliegt auch der Preis starken Änderungen. Innerhalb einer Woche hat sich der Preis in der Vergangenheit um bis zu 25 Prozent verändert. Der Bitcoin-Kurs erreicht immer wieder neue Rekordwerte. Im August 2017 kostete ein Bitcoin (BTC) 3.588,94 Euro und im Dezember desselben Jahres überschritt der Bitcoin-Kurs die 10.000 Euro-Schwelle.

Das Bitcoin-System sorgt für einen konstanten Zufluss von neuen Bitcoins. Der Prozess heißt Mining (eine detaillierte Beschreibung dazu gibt es im Kapitel 2.2.3). 2013 waren acht Millionen Bitcoins in Umlauf. Die von Satoshi Nakamoto in der Bitcoin-Architektur festgesetzte Obergrenze liegt bei 21 Millionen Bitcoins und wird 2032 zu 99 Prozent erreicht werden [54]. Durch eine definierte Obergrenze von existierenden Bitcoins kann keine unendliche Inflation auftreten [12]. Die Bitcoin-

[6] Full Node – ein Nutzer, der die komplette Blockchain (alle Block-Inhalte) mit allen Transaktionen lokal (z. B. auf seinem Computer) speichert und vollständig in ihre Verifizierung involviert ist (verifiziert alle Transaktionen und Blöcke anhand der im System festgelegten Regeln).

[7] Engl. Bitcoin wallet.

[8] Mehr zum Thema Hardware-Wallet im Kapitel 2.4.6.

Abbildung 1.4: Hardware- und Papier-Geldbörse [19] [23] [32]

Währung ist bereits von vielen Unternehmen vom IT-Dienstleister bis hin zur Gastronomie als Zahlungsmittel akzeptiert (siehe Abbildung 1.5).

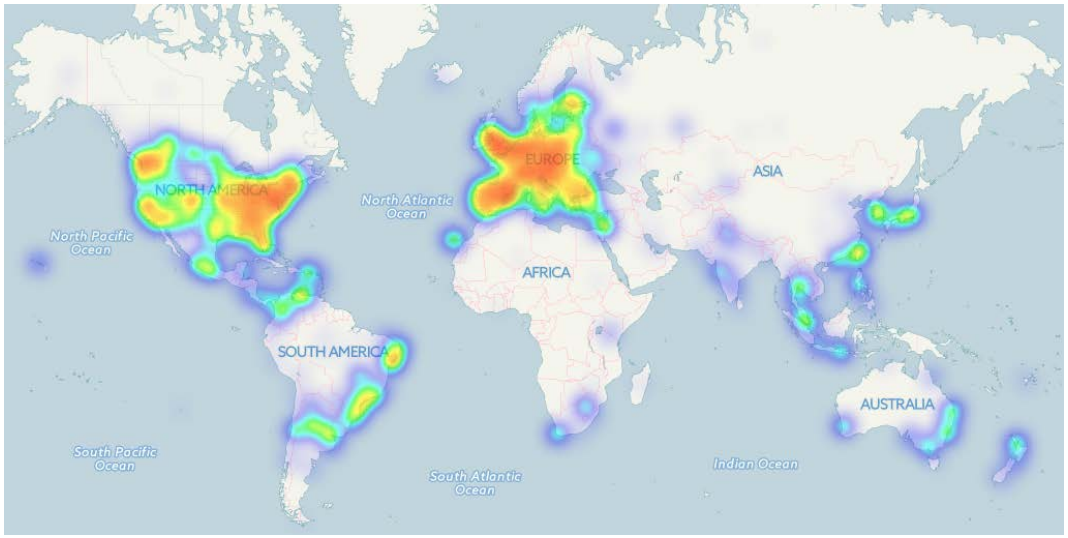


Abbildung 1.5: Verbreitung der Bitcoin-Währung weltweit (coinmap.org)

Das Finanzwesen war der allererste Einsatzbereich der Blockchain-Technologie (Bitcoin und weitere Kryptowährungs-Systeme). Mittlerweile sind zahlreiche Projekte entstanden, die auf der Blockchain-Technologie basieren und eine Vielzahl von Dienstleistungen und Produkten anbieten. Wissenschaft, Medizin, Identitätsmanagement, Cloud Computing, Internet of Things und weitere Bereiche profitieren davon.

2 Wo endet der Hype, wo beginnt die Innovation der Blockchain-Technologie?

Die Blockchain-Technologie ist zwar noch relativ jung, aber bereits vielerorts Gesprächsthema. Das Bitcoin-Projekt als erste Implementierung der Technologie und deren rasante Weiterverbreitung in vielen verschiedenen Branchen haben Blockchain zunächst einmal zu einem Hype gemacht. In den Medien wird immer wieder über neue, unglaubliche Wertsteigerungen, einen starken Absturz oder den möglichen Untergang der Bitcoins berichtet.

Auch das Beratungsunternehmen Gartner Inc.[9] weist darauf hin, dass die Blockchain-Technologie einen starken Einfluss auf die Wirtschaft haben wird. In ihrem Hype Cycle for Emerging Technologies 2016[10] positionierte das Gartner-Research Team die Blockchain-Technologie kurz vor dem „Gipfel der überzogenen Erwartungen“ (siehe Abbildung 2.1). In dieser Phase wird über die Technologie sehr viel in den Massenmedien berichtet und zahlreiche, nicht immer realistische Erwartungen werden ausgesprochen. Infolgedessen versuchen immer mehr Unternehmen, die Technologie für sich anzuwenden.

Nachdem das erste Interesse der Medien abgenommen hat, etwa weil die Technologie noch in den Kinderschuhen steckt, zumindest was die ausgearbeiteten, technologieübergreifenden Standards, einheitlichen Schnittstellen und bewährten Anwendungsfällen angeht, erlebt die Blockchain-Technologie laut Gartner Hype Cycle for Emerging Technologies 2017 einen Abstieg ins „Tal der Enttäuschungen“ (siehe Abbildung 2.2).

Nachdem die neue Technologie den zu erwartenden Abstieg überwunden hat, der viele nicht erfüllte Erwartungen und negative Berichterstattung mit sich bringen dürfte, ist damit zu rechnen, dass bestimmte Standards und einheitliche Schnittstellen festgelegt werden. Das führt in die nächste, „Pfad der Erleuchtung“ genannte Phase, um später auf die „Ebene der Produktivität“ zu gelangen, die mit breiter Anwendbarkeit im Markt verbunden ist. Solange die Blockchain-Technologie noch über keine ausgereiften einheitlichen Standards verfügt, wird sie zwischen dem Hype überzogener Erwartungen einerseits und einer Innovation, deren Lösungen hier und da immer noch mit Schwierigkeiten behaftet sind, balancieren.

[9] Gartner Inc. ist ein führendes US-amerikanisches Beratungsunternehmen, das sich mit Marktforschung und -analyse im IT-Bereich beschäftigt.

[10] Gartner Hype Cycle for Emerging Technologies dient als ein Wegweiser für die Unternehmen im Bereich neuer Technologien und hilft diesen, zwischen einem Hype und einer wirtschaftlich rentablen Technologie zu unterscheiden. Dieser besteht aus fünf Phasen.

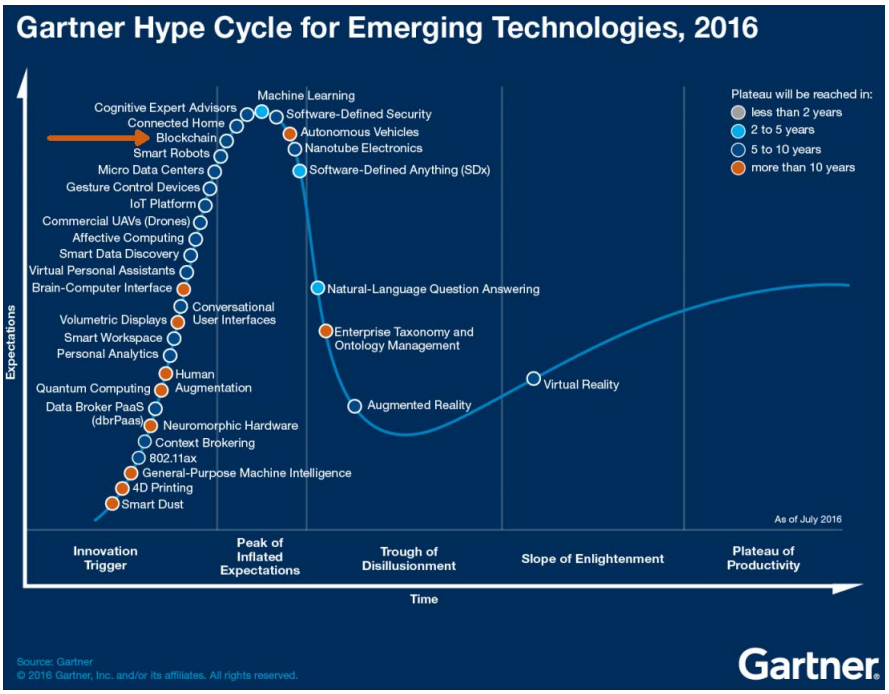


Abbildung 2.1: Hype Cycle for Emerging Technologies 2016 – Gartner Inc.

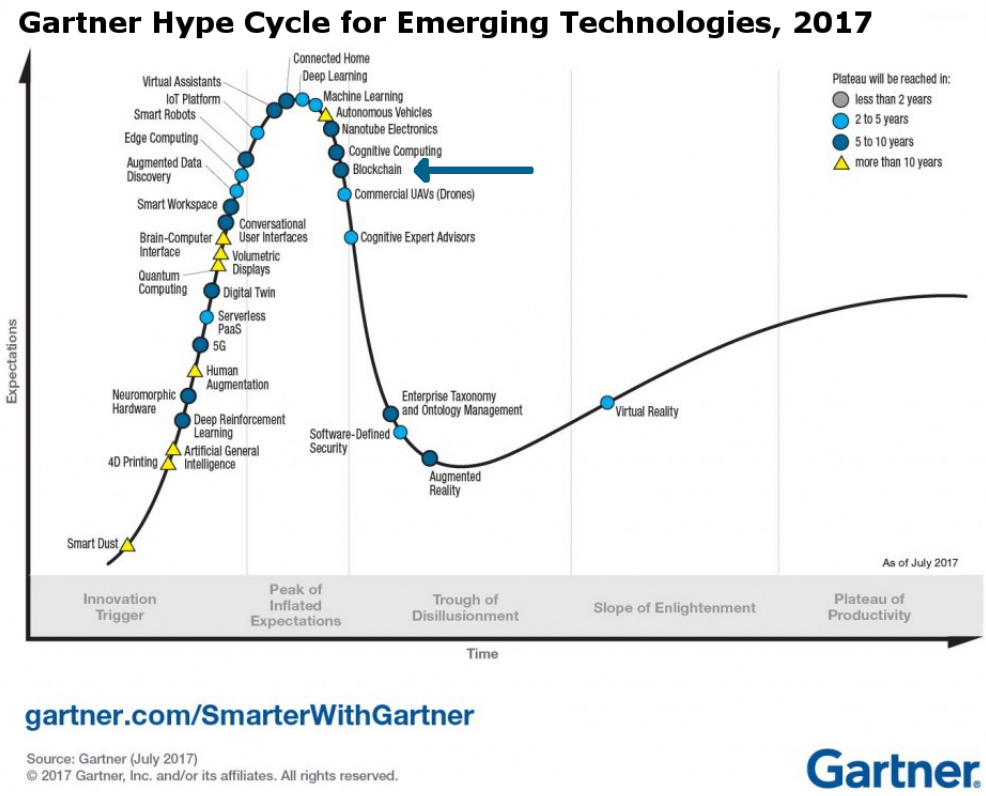


Abbildung 2.2: Hype Cycle for Emerging Technologies 2017 – Gartner Inc.

Mit diesem kompletten Kapitel wollen wir den Lesern helfen, zwischen den überzogenen Erwartungen (Hype) und den innovativen Merkmalen der Blockchain-Technologie unterscheiden zu können.

2.1 Partielle Anonymität trotz Transparenz ist möglich

Bei dem Thema Geld sind viele Menschen sehr sensibel. Kaum jemand möchte darüber in der Öffentlichkeit reden, vor allem nicht das eigene Vermögen offenlegen. Auch aus diesem Grund vertrauen wir unser „Gespartes“ einem vertrauenswürdigen Dritten, einem Finanzdienstleister an, der unseren Anlagen Anonymität verspricht.

Die Blockchain-Technologie dagegen bietet Transparenz[11] für alle Transaktionsinhalte. Somit kann jeder Nutzer alle jemals im Blockchain-System durchgeführten Transaktionen offen sehen. Im Bitcoin-System zum Beispiel bedeutet dies, dass die Informationen, wer von wem wann wie viele Bitcoins erhalten hat, öffentlich sind und der „Kontostand“ sowie alle Transaktionen einer Adresse[12] nachvollziehbar sind [59].

Um die Identität der Nutzer zu verschleiern, werden bei vielen Blockchain-Anwendungen einschließlich Bitcoin Pseudonyme (anonyme Nutzer-Adressen) verwendet, die schwierig zum Endnutzer zurückverfolgbar sind (siehe Kapitel 2.1.2 und 2.4). Zusätzlich zu den Pseudonymen werden weitere Verschleierungsmöglichkeiten angeboten, zum Beispiel auch für Bitcoin-Systeme:

- Einsatz des anonymen Netzwerks TOR für die Verschleierung der IP-Adressen,
- Anonyme Mixing Services (auch tamblers genannt) sollen die Empfänger der Transaktionen verschleiern. Die zu überweisenden Bitcoins werden dazu in mehrere Teile aufgeteilt und an mehrere vom Mixing-Service-Anbieter vorgeschlagene Adressen verschickt. Anschließend wird die gleiche Anzahl an neuen Bitcoins von diesen Adressen an den endgültigen Empfänger gesendet. Dieser Service setzt natürlich das Vertrauen des Nutzers voraus; er ist nicht in jedem Land legal.

Eine zentrale und entscheidende Rolle kommt in der Blockchain-Technologie der Kryptographie zu. Mit Hilfe der Kryptographie werden nämlich die beschriebenen Pseudonyme, Transaktionen und Blöcke generiert.

Deshalb seien hier kurz die Grundlagen der kryptographischen Methoden erläutert, die in der Blockchain-Technologie zum Einsatz kommen.

[11] Betrifft die öffentliche (Public Blockchain) und Konsortium-Blockchain (siehe Kapitel 3.1).
[12] Vergleichbar mit einer Kontonummer, mehr dazu im Kapitel 2.1.2.

2.1.1 Kryptographie

Der Begriff Kryptographie stammt aus dem Altgriechischen und bedeutet eigentlich „geheim schreiben“. Er bezeichnet aber auch eine Wissenschaft, die sich mit der Absicherung von Nachrichten (Verschlüsselung, Entschlüsselung, usw.) beschäftigt. [123] Im Laufe der langen Geschichte[13] der Kryptographie haben sich mehrere Verfahren etabliert. Darunter befindet sich das Public-Key-Verfahren, das in der Blockchain-Technologie unter anderem verwendet wird.

Die Grundidee bei der Public-Key-Kryptographie besteht darin, dass alle Teilnehmer einer verschlüsselten Kommunikation anstatt einen gemeinsamen geheimen Schlüssel für die Entschlüsselung der empfangenen Nachrichten ein unterschiedliches Paar von Schlüsseln besitzen (geheimer Schlüssel, auch Private Key genannt, und öffentlicher Schlüssel, auch Public Key genannt). Der öffentliche Schlüssel wird allen Kommunikationspartnern frei zur Verfügung gestellt. Der Private Key soll geheim bleiben und wird zum Entschlüsseln und Signieren der Nachrichten verwendet. Betrachten wir ein Beispiel mit zwei Interaktionspartnern, hier Alice und Bob genannt. Alice möchte eine Nachricht an Bob schicken. Alice verschlüsselt diese Nachricht mit dem öffentlichen Schlüssel (Public Key) von Bob, bevor sie diese abschickt. Nur Bob kann diese Nachricht mit seinem geheimen Schlüssel (Private Key) entschlüsseln (Abbildung 2.3). [119]

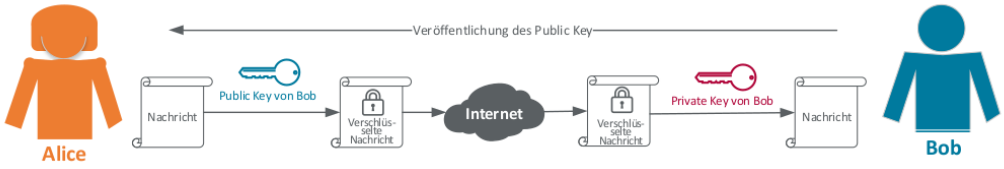


Abbildung 2.3: Public-Key-Kryptographie

Eine digitale Signatur ist eine Zahl bzw. eine Folge von Bits, die mit Hilfe des Public-Key-Kryptographieverfahrens aus einer Nachricht berechnet wird und deren Urheberschaft und Zugehörigkeit zur Nachricht durch jeden geprüft werden kann [120]. Durch das Signieren der Nachricht bestätigt Alice, dass ihre Nachricht tatsächlich von ihr kommt (dafür verwendet sie ihren geheimen Schlüssel (Private Key)). Das kann Bob durch Verifizieren nachprüfen (mit Hilfe des öffentlichen Schlüssels (Public Key) von Alice, siehe Abbildung 2.4).

Um eine digitale Signatur zu erstellen, wird eine kryptographische Hashfunktion verwendet. Hashfunktionen zählt man zu den Einwegfunktionen, d.h. die

[13] Schon 3000 Jahre vor unserer Zeitrechnung wurde Kryptografie im alten Ägypten eingesetzt [8].

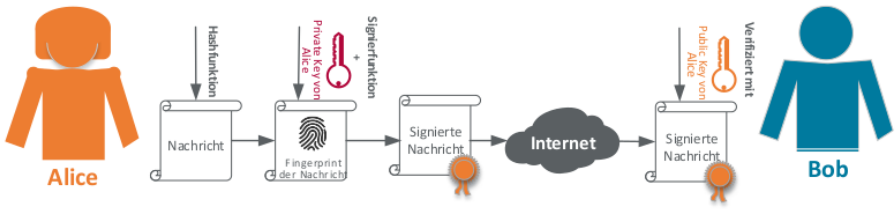


Abbildung 2.4: Digitales Signieren und Verifizieren einer Nachricht

mathematische Berechnung ist in eine Richtung[14] einfach, in die Rückrichtung[15] aber sehr schwer oder unmöglich [119]. Die Hashfunktion wandelt eine Menge von Daten unterschiedlicher Länge in einen alphanumerischen Wert fester Länge um, also eine hexadezimale Zeichenkette. Der Hashwert besteht dann aus einer Zahlen- und Buchstaben-Kombination zwischen 0 und 9 sowie A bis F (als Ersatz für die Zahlen 10 bis 15). Dieses Verfahren erlaubt es, eine Nachricht eindeutig und relativ einfach zu identifizieren, ohne den Inhalt der Nachricht zu offenbaren. Aus diesem Grund wird der Hashwert oft der Fingerprint genannt.

Die in der Blockchain-Technologie am häufigsten verwendete Hashfunktion ist SHA-256 (Secure Hash Algorithm), wobei 256 die Länge des Hashwerts in Bit angibt. Jede noch so kleine Änderung an der Nachricht ergibt einen komplett anderen Hashwert. Nachfolgendes Beispiel zeigt am Namen von Alice und mit dem SHA-256-Algorithmus, wie unterschiedlich die Hashwerte sind, wenn man nur ein einziges Zeichen ändert:

- Alice
  3bc51062973c458d5a6f2d8d64a023246354ad7e064b1e4e009ec8a0699a3043
- Alice1
  9d328d8b7ac56e1f71ce94ed3c7975d63c8b6f1a54d5186de8881cf27dd8b3a9
- alice
  2bd806c97f0e00af1a1fc3328fa763a9269723c8db8fac4f93af71db186d6e90

In der Blockchain-Technologie werden digitale Signaturen für die Bestätigung der Urheberschaft und der Zugehörigkeit zu den Werten (z. B. Bitcoins) eingesetzt.

2.1.2 Nutzeridentifizierung

Im Finanzwesen werden stets die Begriffe Bankkonto und Kontonummer verwendet. Eine Kontonummer wird für die Identifizierung eines Kontos verwendet, das ein Kreditinstitut für einen Kunden führt. Da es in der Blockchain-Technologie keine zentrale Instanz gibt, welche die Konten der Nutzer verwaltet, werden z. B. bei

[14] Aus einer Klartext-Nachricht z. B. aus dem Namen Alice, einen Hashwert zu berechnen.
[15] Nur anhand des Hashwertes und des Hash-Algorithmus die ursprüngliche Nachricht berechnen.

einer Kryptowährung alle jemals getätigten Ausgaben in der Blockchain registriert. Die Nutzer-Anwendungen, zum Beispiel Kryptowährungs-Geldbörsen (Wallets), analysieren die Blockchain und zeigen dann zum besseren Überblick des Nutzers dessen ein- und ausgehende Transaktionen und den aktuellen Geld-Bestand.

Zur Identifikation der Nutzer werden in vielen Blockchain-Anwendungen spezielle Pseudonyme verwendet. Diese nennt man Adressen (z. B. Bitcoin-Adresse). So wie man eine E-Mail an eine E-Mail-Adresse sendet, werden Bitcoins an eine Bitcoin-Adresse geschickt.

Ursprünglich gab es im Bitcoin-System die Möglichkeit, Bitcoins an IP-Adressen zu senden [68]. Dies brachte allerdings Angriffsmöglichkeiten mit sich. Aus diesem Grund nutzt man jetzt, um einem Nutzer einen Bitcoin-Wert gutzuschreiben, ausschließlich kryptographische Methoden bei der Adressen-Erstellung. Dazu wird beim Nutzer ein kryptographisches Schlüsselpaar generiert, z. B. in der Wallet. Der geheime Schlüssel (Private Key) wird für das Signieren von Transaktionen[16] verwendet, der öffentliche Schlüssel (Public Key) für die Adressen-Generierung.

Das Schlüsselpaar im Bitcoin-System und bei vielen anderen Kryptowährungen (z. B. Litecoin, Dogecoin usw. [68]) wird mit Hilfe des Elliptic Curve Digital Signature Algorithm (ECDSA) aus der Elliptischen-Kurven-Kryptographie generiert. Zuerst wird der geheime Schlüssel (Private Key) generiert, der eine Zufallszahl darstellt. Der Public Key wird von dem Private Key abgeleitet und anschließend „gehasht“[17]. Im Endeffekt ist die Adresse ein 160 Bit langer alphanumerischer Wert (z. B. 16UpLN9Risc3QfPqBMvKofHfUB7wKtjvS). Deswegen nennt man derartige Adressen auch „Pay To Public Key Hash Address“ oder P2PKH-Adresse.

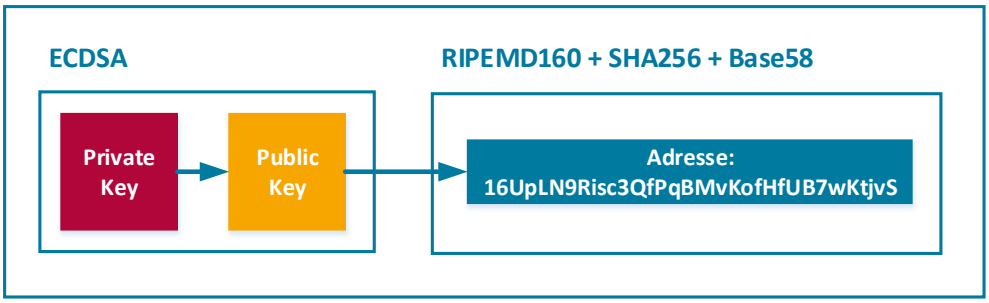


Abbildung 2.5: Adressen-Generierung im Bitcoin-System

[16] Siehe Kapitel 2.2.1.

[17] Für die Generierung der Adresse aus dem öffentlichen Schlüssel (Public Key) werden zwei kryptographische Hashfunktionen nacheinander auf den öffentlichen Schlüssel (Public Key) angewandt (RIPEMD-160 und SHA-256) und das Hash-Ergebnis wird nach Base58 Schema kodiert (ohne Zeichen 0 (Null), O (großes o), I (großes i) und l (kleines L)) (mehr dazu im Anhang 6.1).

Einige Wallets bieten so genannte Multi-Signature-Adressen. Dafür werden mehrere geheime Schlüssel (Private Keys) erstellt [28]. Das soll die Sicherheit erhöhen. Der Empfänger, dem das Guthaben gutgeschrieben wird, muss alle notwendigen geheimen Schlüssel (Private Keys) besitzen, um das erhaltene Guthaben weiter verwenden zu können. Multi-Signature-Adressen können zum Beispiel in einem Unternehmen verwendet werden, das Bitcoins akzeptiert, um Ausgaben einzelner Angestellter erst nach einer Genehmigung des Controllings zu bestätigen. In dem Fall haben der Angestellte und der Controller je einen geheimen Schlüssel (Private Key) für eine gemeinsame Bitcoin-Adresse [65].

Da alle Transaktionen in einer Blockchain[18] für alle Nutzer öffentlich sind, ist es immer möglich, den vorherigen Besitzer (die P2PKH-Adresse) sowie die ganze „Historie“ des Betrages zu verfolgen und den Kontostand (alle mit der Adresse durchgeführte Transaktionen) jedes Nutzers anzusehen. Aus diesem Grund wird Nutzern empfohlen, ihre Adressen nur einmalig zu verwenden und für jede neue Transaktion eine neue Adresse zu generieren [59].

Mit jeder Nutzer-Adresse ist also ein eigener Kontostand verbunden. Es ist zudem möglich, für unterschiedliche Zwecke mehrere Wallets zu verwenden.

Diese beinhalten grundsätzlich folgende Informationen:

- ein kryptographisches Schlüsselpaar oder mehrere,
- eine mit Hilfe des Schlüsselpaares generierte Adresse,
- eine Liste der an den Nutzer adressierten und von ihm getätigten Transaktionen,
- weitere Funktionalitäten, die vom Anbieter der Software abhängen.

Wichtig ist in erster Linie, dass die Nutzer ihren geheimen Schlüssel (Private Key) ausreichend schützen. Denn derjenige, der den geheimen Schlüssel (Private Key) einsetzt, darf das daran bzw. an die P2PKH-Adresse gebundene Guthaben ausgeben (weitere Informationen in Kapitel 2.2.1).

2.1.3 Austausch unter Gleichen

Eine der wichtigen Stärken der Blockchain-Technologie ist ihre Architektur. Sie stellt den zahlreichen Nutzern ein dezentrales, autonomes, sicheres und transparentes System zur Verfügung.

Nachfolgend stellen wir das dezentrale System hinter der Blockchain-Technologie vor und erklären, wie die mit den Transaktionen überwiesenen Werte (z. B. Bitcoins) ihrem neuen Besitzer zugeordnet werden.

Ein Blockchain-System basiert auf einem so genannten Peer-to-Peer-Netz (P2P). Die Nutzer des Systems stellen die Knoten im Netz dar. Diese sind alle gleichberechtigt und können Dienste in Anspruch nehmen sowie diese anderen Nutzern zur Verfügung stellen. Im Fall des Bitcoin-Systems sind es Nutzer, die Bitcoins

[18] Betrifft die öffentliche (Public Blockchain) und die Konsortium-Blockchain (siehe Kapitel 3.1).

an andere überweisen oder empfangen. Im Bereich des Internet of Things sind es hingegen IoT-Geräte, die in dem dezentralen Netzwerk miteinander interagieren.

Kommuniziert miteinander wird dabei über eine unverschlüsselte Internet-Verbindung (siehe Abbildung 2.6).

Da das Netzwerk über keine Authentifizierung verfügt und keine zentrale Verwaltungsstelle für die Nutzer-Konten hat, werden für das Auffinden anderer Knoten und die Informationsverbreitung Methoden aus P2P-Netzen[19] (siehe Abbildung 2.7) eingesetzt. [117]

Grundsätzlich sind im Blockchain[20]-Netzwerk alle Knoten gleichberechtigt und können zugleich Clients und Server sein. Wenn man die Größe der Bitcoin-Blockchain betrachtet (im Dezember 2017 waren es 147 GB), ist es verständlich, dass nicht jeder Nutzer über genügend Ressourcen für das Speichern und Verifizieren verfügen kann. Die Anwendung soll ja vor allem für die Verwendung durch mobile Nutzer möglichst „schlank" sein. Aus diesem Grund kann es im Blockchain-Netzwerk zwei Arten der Nutzer geben [117]:

- „Server" oder vollständige Nutzer (full node). Sie haben sowohl eingehende als auch ausgehende Verbindungen zu anderen Nutzern, speichern die komplette Blockchain und sind in deren Verifizierung involviert.
- „Clients" oder leichtgewichtige Nutzer (lightweight node, thin client oder seltener SPV[21] node) sind die am meisten verbreiteten[22] Nutzer im Bitcoin-Netzwerk. Diese verfügen nur über ausgehende Verbindungen und speichern nur einen Teil der Blockchain [121]. Sie bauen eine Verbindung zu den vollständigen Nutzern auf, um Informationen zu erhalten, die nur sie betreffen. Auch Nutzer, die nach außen[23] hin eine andere IP-Adresse haben als z. B. in ihrem Firmennetzwerk, zählen zu den Clients.

Bitcoin-Nutzer (Client und Server) unterstützen acht ausgehende Verbindungen mit anderen Nutzern. Zusätzlich unterstützt der Server bis zu 117 eingehende Verbindungen. Wenn eine der acht ausgehenden Verbindungen nicht mehr aktiv ist (z. B. weil der Nutzer offline ist), wird diese Verbindung durch eine neue ersetzt.[117] Über diese Verbindungen werden Informationen ausgetauscht, z. B. über neue Transaktionen, Blöcke und IP-Adressen[24] der vollständigen Nutzer (Server). Jeder Nutzer (Client und Server) führt eine Liste mit IP-Adressen anderer Nutzer (Server) im Netz und aktualisiert diese regelmäßig durch den Austausch mit

[19] P2P-Netz – Peer-to-Peer-Netz ist ein Rechnernetz, bei dem alle Rechner gleichberechtigt zusammenarbeiten. Das bedeutet, dass jeder Rechner anderen Rechnern Funktionen und Dienstleistungen anbieten und andererseits von anderen Rechnern angebotene Funktionen, Ressourcen, Dienstleistungen und Dateien nutzen kann. Die Daten sind auf viele Rechner verteilt. Das P2P-Konzept ist ein dezentrales Konzept, ohne zentrale Server, wie das Internet. Jeder Rechner eines solchen Netzes kann mit mehreren anderen Rechnern verbunden sein [15].

[20] Betrifft die öffentliche (Public Blockchain) und die Konsortium-Blockchain (siehe Kapitel 3.1).

[21] SPV - Simplified Payment Verification (siehe Kapitel 3.2.4).

[22] Geschätzt 13 Mal so viele Clients wie Server [117].

[23] Zum Beispiel die Nutzer hinter Firewall und NAT.

[24] Im Bitcoin-Netz: IPv4, IPv6 und OnionCat Adressen [121] [117].

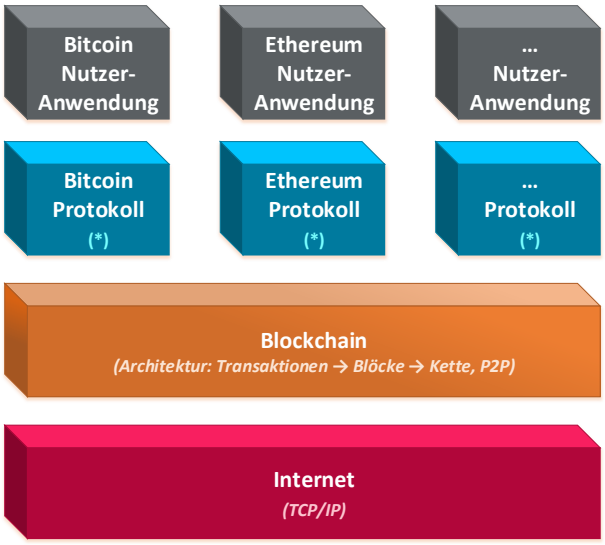


Abbildung 2.6: Abstrakte Darstellung der Blockchain-Schichtenarchitektur

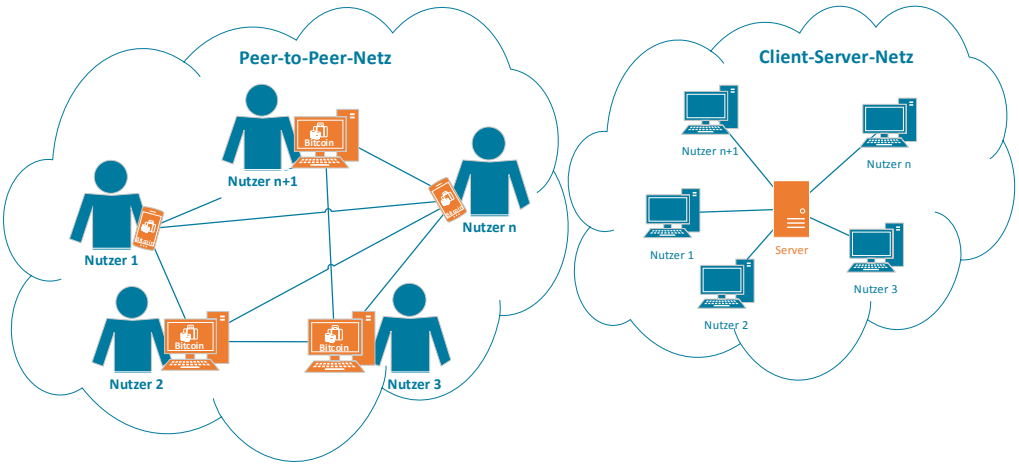


Abbildung 2.7: Vergleich des P2P- und Client-Server-Netzes

anderen Nutzern. Die IP-Adressen sind nicht mit den kryptographischen Adressen verknüpft.

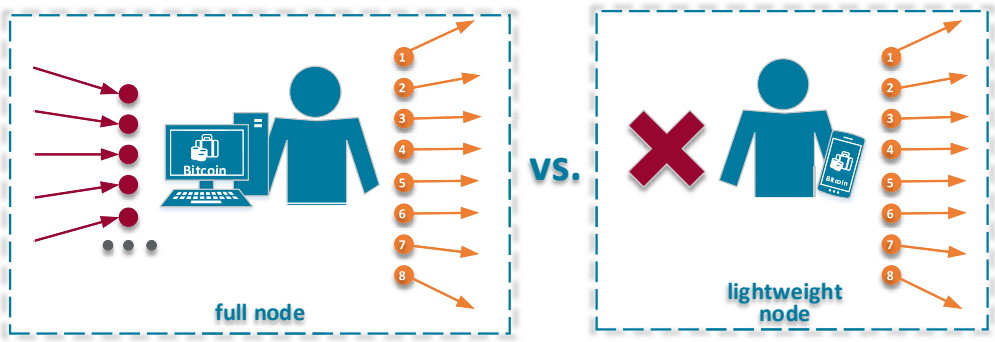


Abbildung 2.8: Vergleich der Nutzerarten (vollständiger und leichtgewichtiger Nutzer)

Zurück zum Beispiel mit Alice und Bob. Alice ist oft unterwegs und möchte das Bitcoin-System an ihrem Laptop nutzen. Wir unterstellen, dass dieser nicht über genug Speicher- und Rechenkapazität verfügt, um als ein vollständiger Nutzer (full node) laufen zu können. Außerdem ist zu berücksichtigen, dass sie sich immer wieder in unterschiedliche Netzwerke einloggt: von zuhause, der Bibliothek oder dem Büro aus. Sie installiert also die Bitcoin-Software und richtet eine Lightweight Wallet ein. Die Software enthält bereits fest programmierte DNS-Namen[25] (auch DNS seeds genannt, z. B. seed.bitcoin.sipa.be, seed.bitcoinstats.com usw.), die mehrere IP-Adressen vollständiger Nutzer (full nodes) beinhalten (siehe Abbildung 2.9).

Dann baut die Software Verbindungen mit einigen der vollständigen Nutzer (full nodes) aus der Liste auf und fragt bei diesen weitere IP-Adressen ab. Die Liste der IP-Adressen wird immer wieder aktualisiert. So kann die Software von Alice bis zu acht Verbindungen unterstützen. Das heißt: Mit acht weiteren Nutzern, in diesem Fall full nodes, kann Alice Informationen austauschen. Als erstes wird die „schlanke“ Version der aktuellen Blockchain heruntergeladen. Außerdem sendet Alice ihre Transaktionen an die Nutzer und erhält von diesen die nur für sie bestimmten Informationen. Der Nachteil eines leichtgewichtigen Nutzers (lightweight node) liegt in der geringeren Sicherheit. Alice muss dem vollständigen Nutzer (full node) Vertrauen entgegenbringen, da sie nur die „schlanke“ Version der Blockchain benutzt und somit nicht alle früheren Transaktionen nachprüfen kann.

[25] Das Domain Name System (DNS) verbindet numerische (IPv4) und alphanumerische (IPv6) IP-Adressen mit leicht zu merkenden Domain-Namen, so dass Nutzer sich keine Zahlenfolgen mehr merken müssen, sondern nur aussagekräftige Namen. Z.B. hinter dem DNS-Namen hpi.de verbirgt sich die IPv4-Adresse 141.89.225.126.

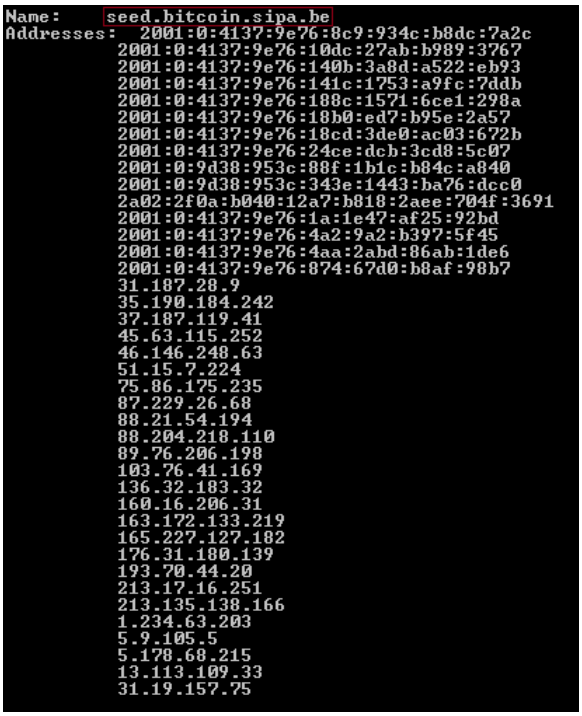


Abbildung 2.9: Auflösung vom Domainnamen eines DNS-Seed

Die Informationen im Blockchain-Netzwerk werden nach festgelegten Regeln ausgetauscht. Diese schließen zum Beispiel aus, dass eine bereits von einem Nutzer versendete Datei (Block, Transaktion, IP-Adressen) doppelt an einen anderen Nutzer versendet wird. Somit wird auch eine Überlastung des Netzes verhindert.

Nehmen wir im Gegensatz zum Beispiel mit Alice an, dass Bob einen full node betreibt. Er verfügt dann über eine vollständige Kopie der Blockchain und kann zusätzlich zu den acht ausgehenden Verbindungen zu anderen Nutzern bis zu 117 eingehende Verbindungen haben. Über die eingehenden Verbindungen empfängt er alle neuen Transaktionen und Blöcke der anderen Nutzer und verifiziert diese nach den festgelegten Regeln. Die gültigen Blöcke und Transaktionen werden in den Zwischenspeicher aufgenommen und weiter an andere full nodes verschickt. Die ungültigen werden verworfen. Die vollständigen Nutzer (full nodes) sind das Rückgrat des Bitcoin-Systems. Sie erlauben es dem System zu wachsen und weiterhin sicher und dezentralisiert zu bleiben.

Alle Dateien (neue Blöcke, Transaktionen und IP-Adressen) werden von einem Nutzer an die anderen weitergesendet (Abbildung 2.10). Eigene neue Transaktionen geben die vollständigen Nutzer (full nodes) zusammen mit neu empfangenen weiter, so dass es für die anderen Nutzer so aussieht, als wären es ihre eigenen.

Jedes Mal prüft ein Nutzer die erhaltene Datei nach den festgelegten Regeln. Wenn er die Datei bereits von einem anderen Nutzer erhalten hat, also schon in seinem Zwischenspeicher gespeichert hat, verwirft er die neu angekommene Datei.

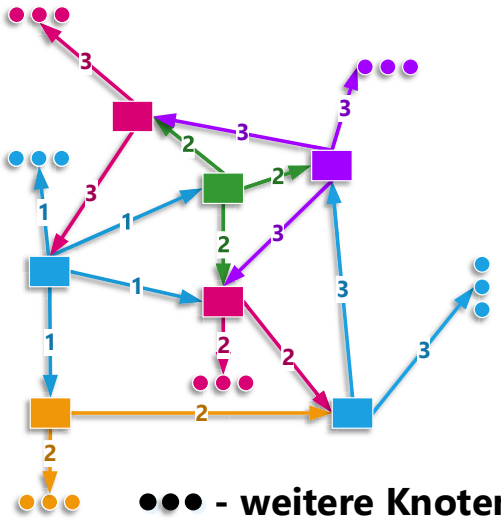


Abbildung 2.10: Verbreitung der Informationen in einem Blockchain-basierten Netz

2.1.4 Verschleierung

Wie bereits angedeutet, ist Transparenz eine der wichtigsten Eigenschaften der Blockchain-Technologie. In vielen Anwendungsbereichen würde diese Eigenschaft aber die Privatsphäre der Nutzer einschränken. Geht es jedoch zum Beispiel um die Nachvollziehbarkeit der unterschiedlichen Inhaltsstoffe[26] von Lebensmitteln oder die Nachverfolgbarkeit von Informationen über den Lagerungszustand[27] (Temperatur, Feuchtigkeit) eines Medikaments im Verlauf der Lieferkette, kommt es zentral auf Transparenz an. Bei privaten Finanzen hingegen ist sie meist nicht gewünscht.

Zu beachten ist: Die durch Pseudonyme erzeugte Anonymität der Nutzer ist nur partiell, da man anhand der IP-Adressen und des Transaktionsverlaufs den Nutzer durchaus auffinden kann (siehe Kapitel 2.4.5).

Bitcoin empfiehlt seinen Nutzern (lightweight nodes) deshalb, das anonyme Netzwerk TOR einzusetzen, um die IP-Adressen zu verschleiern [59]. Mit der Standardsoftware Bitcoin-Core[28] können die vollständigen Nutzer (full nodes) automatisch „TOR Hidden Services“ für mehr Anonymität nutzen (siehe Anhang 6.2) [66].

---

[26] Das Unternehmen ClearKarma bietet eine Lösung für eine durchgehende Nachverfolgbarkeit der Zutaten, die in der Lebensmittelindustrie eingesetzt werden. [73] Das Unternehmen plant eine Cloud-basierte Plattform mit den umfangreichen Informationen über die Nahrungsmittel, wobei die Historie über alle Informationsänderungen an der Blockchain verifiziert und gespeichert wird.

[27] Das Unternehmen Modum.io bietet eine Lösung für die durchgehende Datenintegrität in einer Lieferkette mit der Hilfe der Blockchain-Technologie [97].

[28] Seit der Version 0.12.0, veröffentlicht am 23. Februar 2016.

Das TOR-Netzwerk stellt einen Service zur Verfügung, der Verbindungsdaten anonymisiert. Die Bezeichnung TOR ist eine Abkürzung und steht für „The Onion Routing“. Das so genannte Zwiebel-Routing zeichnet sich durch die mehrfache Verschlüsselung einer Nachricht aus. Dabei sucht der TOR-Client eine Route durch das Netzwerk, das aus zahlreichen Onion-Servern (Onion Router) besteht, die jeweils einen öffentlichen Schlüssel bereitstellen (Abbildung 2.11).

In der Regel verläuft die Route über drei Server. Nachdem eine Route gefunden wurde, verschlüsselt der TOR-Client die Nachricht zunächst mit dem öffentlichen Schlüssel (Public Key) des letzten Onion-Servers (Router C) und fügt seine Adresse hinzu. Danach wird die bereits verschlüsselte Nachricht und die Adresse des Routers C mit dem öffentlichen Schlüssel des vorletzten Servers (Router B) verschlüsselt und seine Adresse wird hinzugefügt usw. Anschließend wird die Nachricht während der Übertragung durch mehrere Onion-Server schichtweise entschlüsselt.

Jeder am Routing beteiligte Server kann die für ihn bestimmte Nachricht mit dem eigenen geheimen Schlüssel (Private Key) entschlüsseln. In der Nachricht findet er eine wiederum verschlüsselte Nachricht und eine weitere Adresse. Die Nachricht wird dann weiter an die angegebene Adresse gesendet. Somit „kennt“ jeder Onion-Server nur seinen Vorgänger und Nachfolger. Nur das letzte Glied der Routing-Kette kann die Nachricht im Klartext lesen.

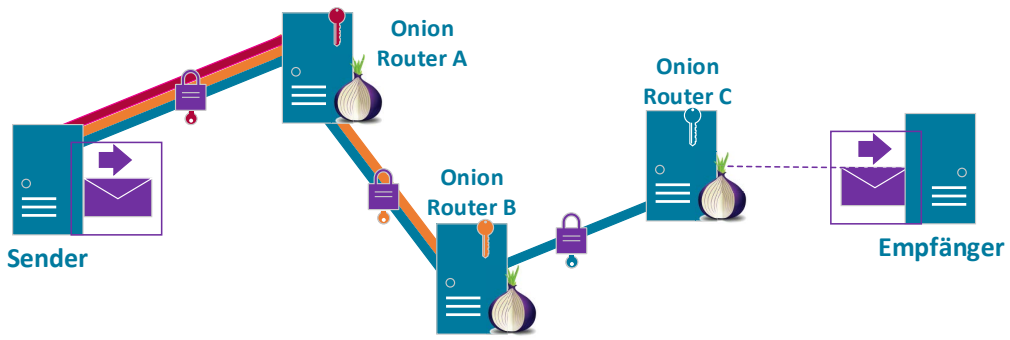


Abbildung 2.11: TOR-Netzwerk

Der Einsatz des TOR-Netzwerks ist nur für ausgehende Verbindungen möglich, also nur für leichtgewichtige Nutzer (lightweight nodes). Um durch das TOR-Netzwerk auch eingehende Verbindungen zu unterstützen, kann der Nutzer dessen so genannte versteckte Dienste[29] verwenden. In diesem Fall agiert der vollständige Nutzer (full node) als ein Service-Anbieter und vereinbart mit dem Service-Empfänger (einem anderen Nutzer) einen „Treffpunkt“ - einen sicheren

[29] TOR Hidden Services.

Onion-Server, auch als Rendezvous-Punkt bekannt. Das geschieht, um sichere und anonyme Kommunikation zu gewährleisten (Abbildung 2.12) [66].

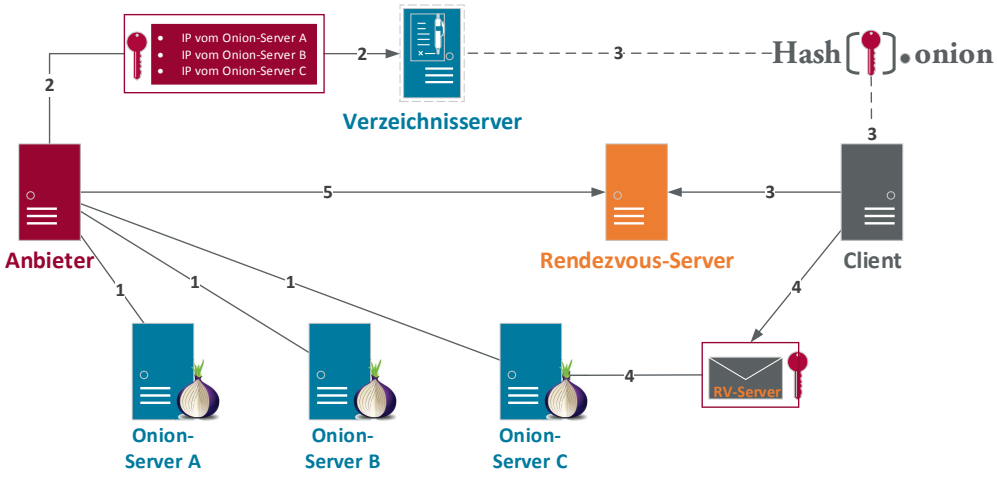


Abbildung 2.12: TOR Hidden Services (für weitere Information siehe [106])

Da es im Bitcoin-System keine Absender-Adressen[30] gibt, wird es den Nutzern zum Schutz ihrer Privatsphäre ausdrücklich empfohlen, bei jedem Empfang einer Zahlung eine neue Adresse zu nutzen. Für die weitere Verschleierung der Empfänger können bereits erwähnte Mixingservices genutzt werden. Die Legalität der Nutzung solcher Dienste kann je nach Gesetzgebung des jeweiligen Landes unterschiedlichen Regeln unterworfen sein. [59]

Die aufgelisteten Methoden bieten in dem transparenten Blockchain-System mehr Anonymität. Dennoch sollten die Nutzer mehrere Sicherheitshinweise beachten, um ihre Privatsphäre sowie die Blockchain-Endwerte (Kryptowährung wie z. B. Bitcoins, Besitz von z. B. einem gemieteten Fahrrad, Ereignis wie etwa die Berechtigung, die Tür eines Raums aufzuschließen) zu schützen.

2.1.5 Datenschutz und Haftung

Wie dargestellt, hat ein Blockchain-basiertes-System keine zentrale Instanz, agiert also dezentral und autonom und arbeitet mit einem noch nie dagewesenen Ausmaß an Transparenz [59]. Aus diesen auf den ersten Blick sehr positiven Eigenschaften ergeben sich jedoch einige datenschutzrechtliche Fragestellungen.

[30] Vereinfacht ausgedrückt enthält jede Transaktion den Bitcoin-Wert und die Empfänger-Adresse und wird anschließend von dem Absender signiert. Den erhaltenen Bitcoin-Wert kann der Nutzer nur mit seinem geheimen Schlüssel (Private Key) ausgeben, den er für die Transaktion erstellt hat (siehe Kapitel 2.2.1).

Durch die Transparenz aller Transaktionsinformationen lassen sich die geschäftlichen und damit im Prinzip auch die persönlichen Verhältnisse der Nutzer erkennen [134]. Dabei werden die vertrauenskritischen Transaktionen zwischen den Parteien ausgetauscht, ohne die Identität der Vertragspartner gegenüber einander oder der Öffentlichkeit offenlegen zu müssen. Somit treten Anonymität bzw. Pseudonymität als datenschutzrechtliche Instrumente auf. [78]

Laut Pesch und Böhme [134] können Bitcoins weder eindeutig als Rechtsgegenstand „Sache“ noch als Rechtsgegenstand „Geld“ eingeordnet werden. Aus diesem Grund können sie wegen des Verbots[31] täterbelastender Analogien im Strafrecht nicht das Objekt von Straftaten sein, deren Tatbestände sich nur auf Sachen oder Geld beziehen. [134] Ob weitere Blockchain-Werte als Rechtsgegenstand „Sache“ bezeichnet werden können, bleibt offen.

Einer der meist verbreiteten Anwendungsbereiche der Blockchain-Technologie ist der intelligente Vertrag[32]. Dieser hat Auswirkungen auf Lebensbereiche, die traditionell durch analoges Recht bzw. Institutionen reguliert werden [78]. Das Unternehmen Agrello [57] hat das Problem aufgegriffen und bereits eine Lösung in Form von rechtlich bindenden intelligenten Verträgen vorgestellt. Agrello bietet ein Produkt mit einem benutzerfreundlichen Interface (Abbildung 2.13), das den Nutzer bei der Erstellung eines rechtlich bindenden Vertrages unterstützt. Der erstellte Vertrag wird in einen intelligenten Vertrag umgewandelt und in einer Blockchain gespeichert. Parallel wird ein rechtsverbindlicher Vertrag in natürlicher Sprache erstellt und digital unterzeichnet [57]. Der Nutzer wird während der Vertragserstellung durch einen AI[33]-Agent unterstützt.

Abbildung 2.13: Agrello-App [57]

[31] *„Ein Analogieverbot besteht insbesondere im Strafrecht. Danach ist es einem Richter verboten, eine nicht strafbare Handlung zu verurteilen, auch wenn er diese als strafwürdig ansieht oder diese einer anderen Strafnorm ähnelt, jedoch nicht ganz mit dieser übereinstimmt. Dieses Verbot gilt vor allem auch für Gesetzeslücken.“* - Definition nach [7].
[32] Engl. Smart Contract. Für weitere Informationen siehe Kapitel 3.3.
[33] AI – Artificial Intelligence (auf Deutsch „künstliche Intelligenz“).

2.2 Ausfallsicherheit, Fälschungssicherheit, Nachverfolgbarkeit

Blockchain-Anwendungen unterscheiden sich von Anwendung zu Anwendung. Manche sind deutlich komplexer aufgebaut als andere. Was jedoch alle gemeinsam haben, ist die zugrunde liegende Architektur (Transaktionen, Blöcke, Kette, Konsensalgorithmus[34]). Zum Beispiel das Identitätssystem Blockstack nutzt die Vorteile der Blockchain-Technologie und protokoliert nur die Blockstack-Operationen in der Blockchain (Abbildung 2.14). Die weiteren Funktionalitäten wie Management und Speicherung von Daten werden außerhalb der Blockchain geregelt (weitere Informationen im Kapitel 4.5).

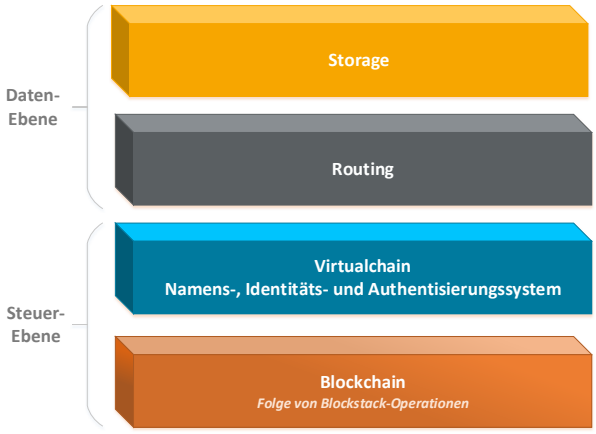


Abbildung 2.14: Blockstack-Schichtenarchitektur

Dagegen haben reine Kryptowährungen eine einfachere Architektur (siehe Abbildung 2.6):

- zugrunde liegende Blockchain,
- für die jeweilige Kryptowährung spezifische Regeln (darunter der Konsensalgorithmus) und
- eine Nutzer-Anwendung, die alles implementiert.

Durch die Art der Informationsverbreitung in einem Blockchain-System verfügt jeder Nutzer entweder über eine vollständige Kopie oder über eine „schlanke“ Version der Blockchain, die zudem regelmäßig aktualisiert wird. Die Verteilung der Blockchain auf viele voneinander unabhängige Rechner sichert gegen einen Systemausfall oder Datenverlust ab.

[34] siehe Kapitel 2.3.

Eigenschaften wie Fälschungssicherheit und Nachverfolgbarkeit der Transaktionen werden erst vollends deutlich, wenn man die Blockchain-Architektur gut versteht. In den folgenden Kapiteln geht es deshalb zunächst um die kleinste Einheit einer Blockchain (bei der Kryptowährung ist dies die digitale Münze, z. B. ein Bitcoin) und darum, wie diese in eine Transaktion eingepflegt wird. Anschließend wird erläutert, wie die Transaktionen in den Blöcken erfasst werden und wie daraus eine Kette entsteht.

2.2.1 Kleinster Baustein einer Blockchain

Ein auf der Grundlage der Blockchain-Technologie konzipiertes Netzwerk nennt man auch Internet der Werte („Internet of Value"). Anstatt beliebiger Informationen, die im Internet mal verschlüsselt und mal unverschlüsselt übertragen werden, tauschen die Endnutzer eines Blockchain-Netzwerks Werte manipulationssicher aus. Ein Wert kann in einer Kryptowährung, einem Ereignis oder einem Besitz bestehen.

Diese Werte sind die kleinsten „konzeptionellen" Bausteine einer Blockchain. Die entsprechenden Einheiten werden im Code des Blockchain-Systems nicht als extra Nachricht, Daten-Paket oder Variable definiert, sondern als ein Teil der Transaktion. Somit ist technisch gesehen eine Transaktion der kleinste Baustein einer Blockchain.

In der Blockchain wird durch eine solche Transaktion ein bestimmter Wert zwischen den Nutzern transferiert, wechselt somit seinen Besitzer. Ein neu erschaffener Endwert, entweder eine digitale Münze[35] in einer Kryptowährung oder etwa ein neues, zur Anmietung bereitgestelltes Apartment, hat keine Vorgeschichte. Im Laufe der Zeit, während der Wert von Nutzer zu Nutzer übertragen wird, speichert die Blockchain die komplette Historie, also wem er wann gehört hat. Bei dem Vorgang wird also der Wert als eine Referenz zu einer früheren Transaktion dargestellt.

Eine Transaktion hat zwei wesentliche Bestandteile: einen Eingang (Input) und einen Ausgang (Output). Beim Eingang wird ein vorhandener Wert[36] eingegeben, also die Referenz zu der früheren Transaktion, in welcher dem aktuellen Besitzer der Wert zu einem früheren Zeitpunkt überwiesen wurde. Die Referenzen zu den früheren Transaktionen sind deren Hashwerte (siehe Kapitel 2.1.1 - Kryptographie). Beim Ausgang ist die Empfänger-Adresse einzutragen, im Fall einer Kryptowährung also die Anzahl der zu überweisenden digitalen Münzen. Die Transaktion wird anschließend vom Absender signiert.

Wie erläutert, ist die Adresse vom öffentlichen Schlüssel (Public Key) abgeleitet, stellt z. B. dessen Hash dar. Somit kann der Nutzer nur dann die an ihn adressierte Transaktion weiternutzen, wenn er einen zu dem öffentlichen Schlüssel passenden geheimen Schlüssel (Private Key) hat. Die Transaktion kann dann durch Signieren mit dem passenden geheimen Schlüssel „ausgegeben"/weitergegeben werden.

Eine Transaktion kann auch mehrere Eingänge und Ausgänge umfassen. Im Bitcoin-System etwa werden alle früheren Transaktionen, die an einen Nutzer adressiert und noch nicht ausgegeben wurden, in seiner Wallet als aktueller Bitcoin-

[35] Engl. Coin.

[36] Über welchen der Nutzer bereits verfügt.

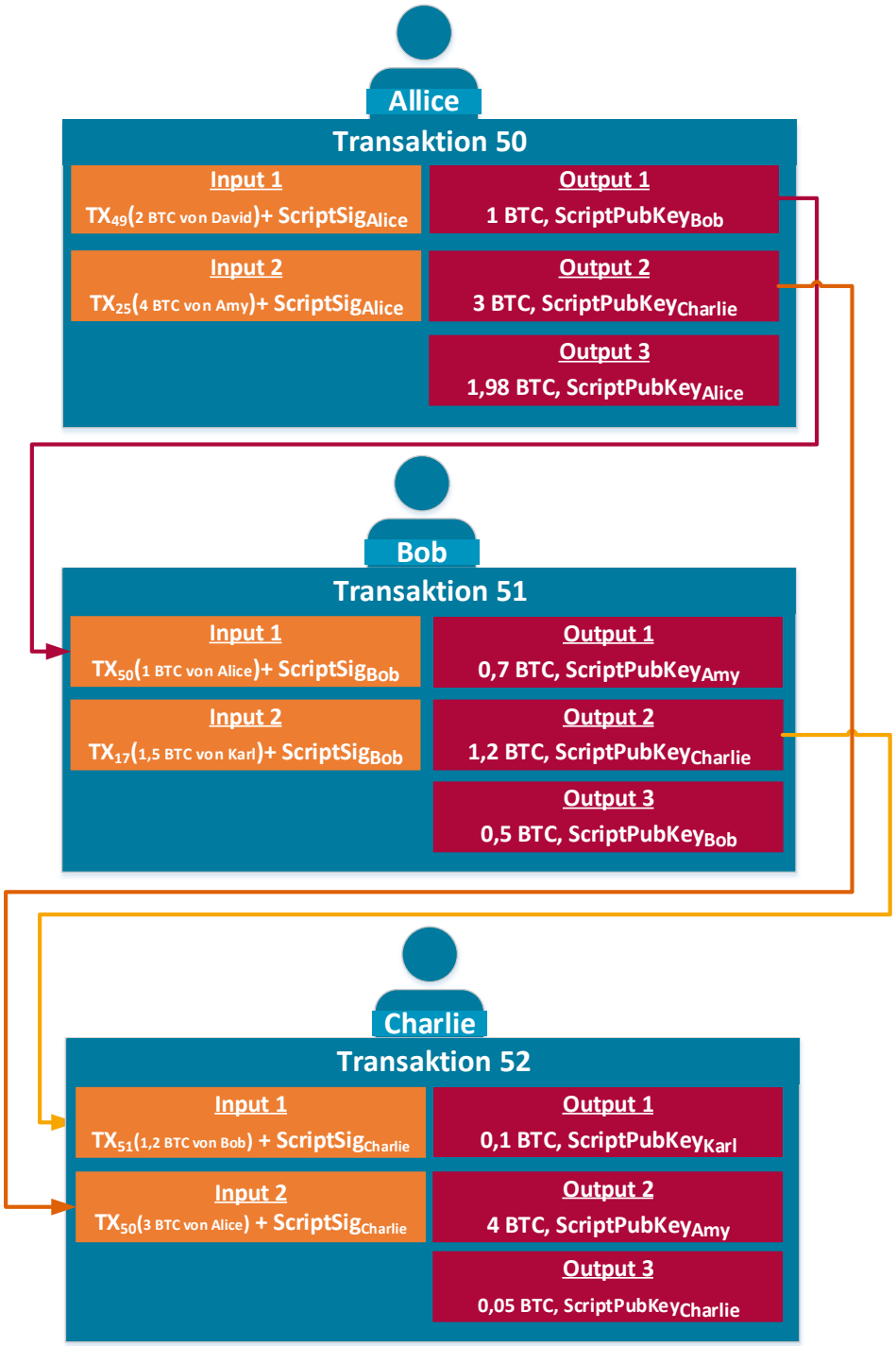


Abbildung 2.15: Transaktionen im Bitcoin-System

Bestand zusammengefasst aufgelistet. Diese früheren Transaktionen werden in neuen Transaktionen als Eingänge (Inputs) dieses Nutzers verwendet. Mehrere Ausgänge (Outputs) hat man, wenn man den zu überweisenden Wert an mehrere Empfänger aufteilt.

Wenn der Absender einen kleineren Geldbetrag als jenen überweisen möchte, der durch alle Eingänge zusammen verfügbar ist, hat er die Möglichkeit, den Restbetrag an sich selbst zu überweisen. Wenn der Absender einen Restbetrag in seiner Transaktion hat, den er nicht an sich selbst zurücküberweist, wird dieser als Transaktionsgebühr wahrgenommen (Abbildung 2.15). Transaktionen können nicht rückgängig gemacht werden.

Nachdem eine Transaktion erstellt wurde, wird diese an andere Nutzer weitergegeben, mit denen eine Verbindung besteht. Jeder vollständige Nutzer (full node) verifiziert die empfangene Transaktion nach festgelegten Regeln (siehe Anhang 6.3) und speichert diese in seinem Zwischenspeicher (memory pool), bis diese von einem so genannten Blockchain-Fortschreiber (Miner oder Minter) in einen Block aufgenommen wird. Der Prozess, in dem eine Blockchain fortgeschrieben wird, heißt Mining oder Minting (abhängig von dem Konsens-Algorithmus, siehe Kapitel 2.3). Dabei werden neue Transaktionen in Blöcken zusammengefasst und die Blöcke in einer bestimmten Reihenfolge miteinander verkettet (mehr zu dem Thema im Kapitel 2.2.3).

Hier vier Beispiele für die Verifikation von Transaktionen:

- eine Transaktion ist signiert worden,
- eine Transaktion ist nie zuvor „ausgegeben“ worden,
- wenn die Transaktion an mich gesendet wurde, fügt sie sich meiner Wallet zu,
- wenn die Transaktion einem gültigen Block hinzugefügt ist, wird diese im Zwischenspeicher gelöscht.

Eine Transaktion gilt als gültig, wenn sie in einen Block aufgenommen ist, der bereits mindestens fünf Nachfolgerblöcke hat. Diese Anzahl wurde in der Annahme festgelegt, dass potenzielle Angreifer nicht genügend Rechenleistung besitzen oder aufbringen wollen, um sechs Blöcke neu zu berechnen.

2.2.2 Block und Kette

Nachdem Transaktionen an die vollständigen Nutzer (full nodes) im Blockchain-Netzwerk verteilt sind und nach der erfolgreichen Verifizierung in deren Zwischenspeicher aufgenommen wurden, können die Nutzer sie in einer bestimmten Liste mit zusätzlichen Informationen zusammenfassen. Dafür erhalten sie eine Belohnung. Eine solche Liste wird in der Blockchain-Technologie „Block“ genannt. Der Nutzer hat nur dann eine Chance, einen gültigen Block zu erstellen und somit die Belohnung zu erhalten, wenn er die in seinem System vordefinierten Anforderungen ausführt. Im Bitcoin-System etwa soll der Nutzer eine festgelegte kryptographische Aufgabe richtig lösen (weitere Informationen dazu in Kapitel 2.2.3).

Transaktionen und Blöcke sind die wichtigsten Bausteine einer Blockchain. Zusätzliche Informationen werden im „Block-Kopf“ (im Weiteren Block-Header genannt) erfasst, gefolgt von der Liste der Transaktionen im „Block-Körper“ (Block-Body). Diese Informationen sind für den richtigen Aufbau der Blockchain und deren Verifizierung notwendig.

Im Bitcoin-System beinhaltet der Block-Header folgende Angaben:

- Nonce[37] - einen wichtigen Hinweis auf den richtigen Aufbau des Blocks, wird für das Mining verwendet (32 Bit),
- eine Referenz zum vorherigen Block: ein SHA-256 Hash des vorherigen Blocks (Block-Header + Nonce),
- einen für den Blockaufbau wichtigen Wert, der eine Zielvorgabe[38] für die kryptographische Aufgabe zeigt,
- einen Zeitstempel[39], wann der Block erstellt wurde,
- eine Referenz zu allen Transaktionen in dem Block, auch Wurzel des Merkle-Baums genannt („Merkle-Root“, 256 Bit),
- die Angabe der Software-Version der Bitcoin-Applikation, die der Nutzer, der den Block erstellt hat, verwendet und die
- Anzahl aller in dem Block erfassten Transaktionen.

Der Hash des vorherigen Blocks, die Nonce und die Zielvorgabe der kryptographischen Aufgabe sind für das Mining (Erstellung eines neuen Blockes) relevante Angaben (mehr dazu im Kapitel 2.2.3).

Wie im Kapitel Kryptographie gezeigt, erlaubt die Hash-Funktion eine eindeutige und relativ einfache Identifizierung der Daten. In der Blockchain-Technologie helfen die Hashwerte, die Reihenfolge der eingegebenen Daten zu bewahren. Sie werden als Referenzen eingesetzt. Eine Transaktion beinhaltet zum Beispiel die Hashwerte der vorherigen Transaktionen; diese sind die Eingangswerte der Transaktion, der Werte-Bestand (im Bitcoin-System der Geldbestand). Dadurch ist es möglich, die gesamte Historie der Transaktion oder des Endwertes in der Blockchain zu verfolgen.

Die Blöcke beinhalten zwei unterschiedliche Referenzen, eine zu dem vorherigen Block (Hash seines Block-Header) und eine weitere zu allen in dem Block aufgeführten Transaktionen. Diese Referenzen sind so genannte „Fingerabdrücke“ und helfen schnell nachzuweisen, ob eine Transaktion nachträglich in den Block eingeführt worden ist.

---

[37] In der Kryptographie wurde die Bezeichnung Nonce (Abkürzung für: „used only once“ oder „number used once“) aufgegriffen, um eine Zahlen- oder Buchstabenkombination zu bezeichnen, die nur ein einziges Mal in dem jeweiligen Kontext verwendet wird [110] (mehr Informationen in dem Kapitel 2.2.3).

[38] Engl. Difficulty target. Dieser Wert wird in dem Bitcoin-System zwischen allen Nutzern ausgetauscht.

[39] Engl. timestamp (in Sekunden).

Die Merkle-Root ist der letzte Hashwert im so genannten Hash-Baum. Bei dem Hash-Baum („Merkle-Tree“) geht es um eine Baum-Struktur (Graphentheorie) aus aufeinanderfolgenden Hashwerten[40]. In Abbildung 2.16 zum Beispiel ist zu sehen, dass aus Transaktion 1 (**TX1**) zuerst ein doppelter Hashwert **dh1** erstellt wird. Das ist **dh1=SHA256(SHA256(TX1))**. Das Gleiche wird mit den Transaktionen **TX0**, **TX2** und **TX3** gemacht. Dann werden aus den ersten gefundenen doppelten Hashwerten der Ursprungstransaktionen weitere Hashwerte ausgerechnet. Die Wurzel des Baums **dh0123** ist in diesem Fall die Merkle-Root.

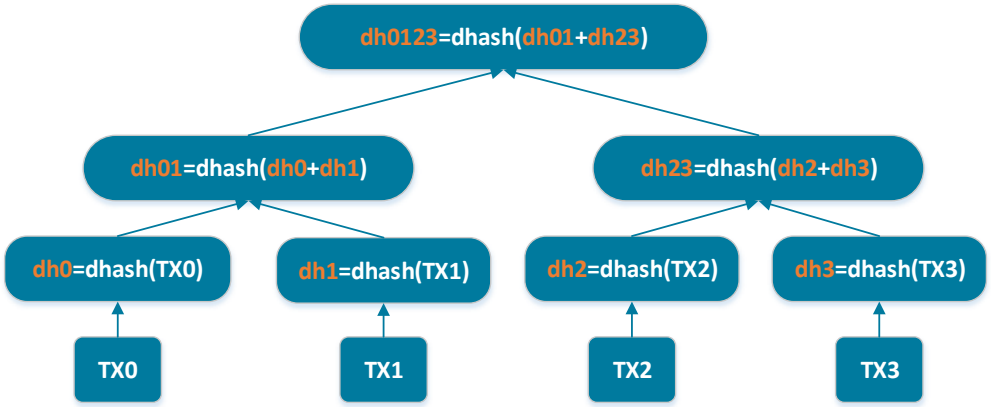


Abbildung 2.16: Hash-Baum aus Transaktionen

Die Blockgröße im Bitcoin-System ist auf 1 MB begrenzt. Somit kann ein Block ca. zwischen 900 und 2500 Transaktionen enthalten. Seit langem wird in der Bitcoin-Community darüber diskutiert, ob die Blockgröße bei 1 MB bleibt oder auf 2 MB erhöht werden soll. Am 1. August 2017 entstand durch Abspaltung vom Bitcoin-System die neue Kryptowährung Bitcoin Cash. Hier ist die Größe des Blocks auf 8 MB festgesetzt.

Eine der Vorgaben für die Block-Erstellung (Mining oder Minting, der Name hängt vom Konsens-Algorithmus ab, siehe Kapitel 2.3) ist, dass ein neuer Block in zehn Minuten erstellt werden muss.

Die erste Transaktion im Block-Body (Block-Körper) wird von demjenigen Nutzer generiert, der den Block erstellt hat – im Bitcoin-System Miner genannt – und ist an ihn selbst adressiert. Diese Transaktion ist die Belohnung für den Miner und besteht aus 12,5 neu erzeugten Bitcoins. Diese Transaktion hat keinen Input, da die Bitcoins neu geschöpfte Bitcoins sind und keine Historie haben. Nach 210.000 Blöcken wird die an Miner bezahlte Belohnung halbiert (ca. alle 4 Jahre, z. B. werden es ab 2020 nur noch 6,25 Bitcoins sein).

[40] Im Bitcoin-System wird die Hashfunktion SHA-256 doppelt angewendet.

Um sicher zu sein, ob die erstellte Transaktion gültig ist, sollten die Nutzer warten, bis die Transaktion in einen Block aufgenommen ist, der bereits mindestens fünf Nachfolgerblöcke hat. Da jeder neue Block in zehn Minuten erstellt wird, beträgt die Wartezeit zwischen einer und zwei Stunden. Je größer die Transaktionsgebühr ist, desto schneller wird die Transaktion vom Miner in einen neuen Block aufgenommen. Miner erhalten die Transaktionsgebühren aller im Block enthaltenen Transaktionen.

Nachdem ein Block erstellt ist, wird dieser an die Nutzer verteilt. Jeder vollständige Nutzer (full node) verifiziert den empfangenen Block nach festgelegten Regeln und fügt diesen zu einer Kette hinzu. Somit entsteht eine Kette aus aufeinander folgenden und durch Referenzen miteinander verketteten Blöcken. Der erste Block in der Kette wird auch Genesis-Block genannt.

Die Blockchain-Technologie listet also alle Transaktionen auf, die jemals im jeweiligen System durchgeführt wurden und ihrerseits in Blöcke aufgeteilt sind. Die aufgelisteten Blöcke bilden eine Kette, in der jeder Block eine Referenz zum vorherigen enthält. Somit entsteht eine Reihenfolge von Blöcken. Daraus entstand der Name Blockchain (Blockkette).

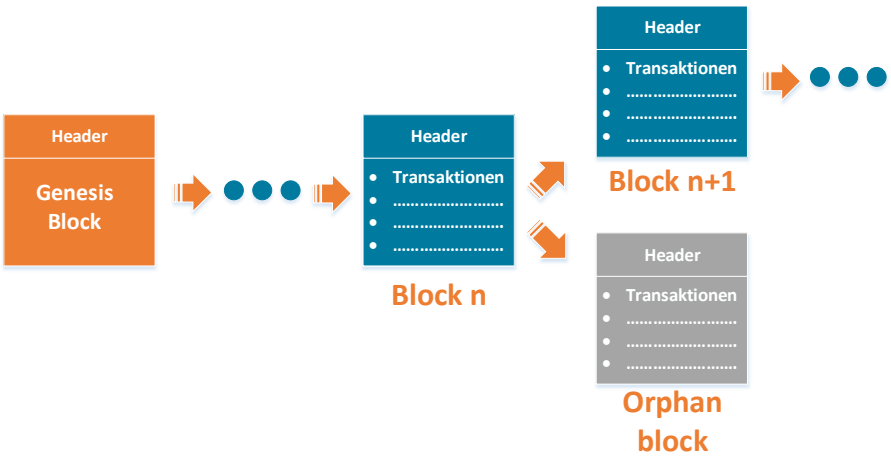


Abbildung 2.17: Blockchain

Da das Blockchain-Netz ein dezentrales ist und es zwischen den Nutzern keine Absprachen über die Priorität der erstellten Blöcke gibt, kann es dazu kommen, dass zum gleichen Zeitpunkt mehrere Miner einen neuen Block erzeugen. Wenn diese Blöcke allen Regeln entsprechen und sich auf den letzten Block beziehen, kann es zu einer Verzweigung der Kette kommen. In der Bitcoin-Terminologie wird dies „Fork“[41] genannt. Die Lösung dafür ist gleichzeitig die wichtigste Regel im Bitcoin-System: „Die längste Kette ist gültig“ (mehr dazu im Kapitel 2.2.3).

[41] Auf Deutsch - Gabel.

Die kürzeste Kette wird ignoriert; deren Blöcke nennen sich dann „orphan blocks“ (siehe Abbildung 2.17).

Die Größe der Bitcoin-Blockchain im Dezember 2017 betrug 147 GB.

2.2.3 Fortschreibung der Blockchain

Die Blockchain wird fortgeschrieben, indem neue Transaktionen in Blöcken zusammengefasst und die Blöcke in einer bestimmten Reihenfolge miteinander verkettet werden. Im Bitcoin-System heißt dieser Prozess Mining (auf Deutsch übersetzt bedeutet Mining Bergbau oder Schürfen) und die Nutzer, welche die Blockchain fortschreiben, werden Miner genannt. In der Tat liegt eine gewisse Ähnlichkeit zur Rohstoffförderung im Bergbau vor: Wer schürft, muss schwere Arbeit leisten, um an die Materie zu kommen.

In der Blockchain wird manipulationssicher protokolliert, wann zwischen wem welche Informationen ausgetauscht wurden. Neue Endwerte (Kryptowährung, Besitz, Ereignis) werden sicher ins System eingetragen und bereits vorhandene Endwerte werden nicht doppelt vergeben. Somit wird ein verlässlicher und vor Manipulationen geschützter Konsens zwischen allen Nutzern erreicht.

Die definierten Anforderungen, die ein Nutzer zu erfüllen hat, um einen gültigen Block erstellen zu können, gehören zu den zahlreichen Regeln, die für die Konsensfindung in einem dezentralen und autonomen System von ausschlaggebender Bedeutung sind.

Die Anforderungen unterscheiden sich je nach System und bestehen darin, dass der Nutzer den Nachweis erbringen muss, entweder bestimmte Ressourcen für die Blockerstellung eingesetzt zu haben oder von anderen Nutzern für die Blockerstellung auserwählt worden zu sein (mehr zu dem Thema im Kapitel 2.3).

Im Bitcoin-System ist der Nachweis einer Leistung („Proof-of-Work“) eine Anforderung für die Blockerstellung. Die beim Mining zu leistende Arbeit ist absichtlich ressourcenintensiv und schwer konzipiert, damit der Blockerstellungsprozess konstant bleibt und mögliche Angreifer davon abhält die Blöcke zu manipulieren oder das Netzwerk mit gefälschten Blöcken zu überfluten. Denn Angreifer müssen ja ebenfalls die Leistung erbringen, um neue Blöcke zu erstellen. Der Nachweis einer Leistung wird von den anderen Nutzern auf Richtigkeit überprüft und im Erfolgsfall bestätigt. Nutzer, die in die Blockerstellung einbezogen sind, werden mit neu geschöpften Bitcoins (erste Transaktion in neuem Block, siehe Kapitel 2.2.2) und Transaktionsgebühren belohnt. Somit dient die Belohnung im Bitcoin-System der Schöpfung und Verbreitung neuer Bitcoins sowie als Motivation der Nutzer, im Mining-Prozess mitzumachen und damit die Sicherheit des Systems zu wahren [64].

Nachdem getätigte Transaktionen an alle Nutzer verteilt sind, verifizieren diese die erhaltenen Transaktionen und speichern sie in ihrem jeweiligen Zwischenspeicher (memory pool), bis sie in einen Block aufgenommen werden.

Bevor ein Miner die Transaktionen in einen gültigen Block aufnehmen kann, muss er eine kryptographische Aufgabe mit einem bestimmten Schwierigkeits-

grad[42] („difficulty“) lösen. Die kryptographische Aufgabe besteht darin, einen Hashwert unterhalb der gegebenen Zielvorgabe („difficulty target“) zu finden. Der Schwierigkeitsgrad und die Zielvorgabe werden alle zwei Wochen (nach 2016 Blöcken) so angepasst, dass für die Erstellung eines Blockes zehn Minuten benötigt werden. Wenn die Rechenleistung des gesamten Netzes steigt und die 2016 Blöcke in weniger als zwei Wochen gefunden werden, dann wird der Schwierigkeitsgrad erhöht.

Der Hashwert wird durch die doppelte Hashfunktion SHA-256 aus dem Block-Header und einer Nonce[43] errechnet. Die Nonce, eine 32 Bit lange, variable hexadezimale Zeichenkette, wird immer wieder angepasst, bis der Hashwert kleiner oder gleich der Zielvorgabe ist (siehe Abbildung 2.18).

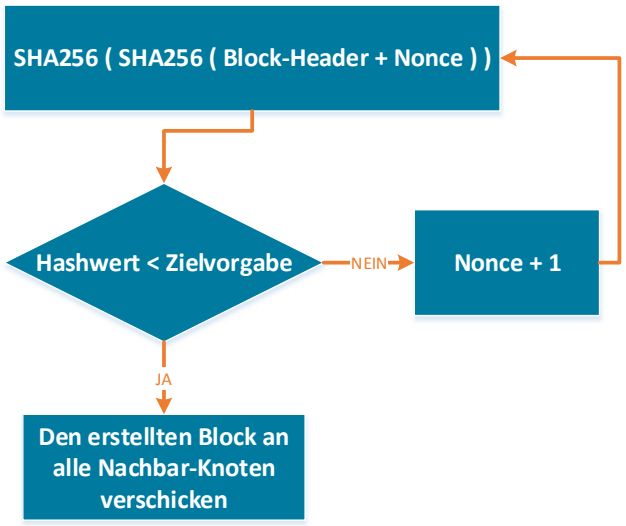


Abbildung 2.18: Mining-Prozess, Lösen der kryptographischen Aufgabe

Die Zielvorgabe ist eine 256 Bit lange hexadezimale Zeichenkette, die alle Bitcoin-Nutzer teilen. Je kleiner die Zielvorgabe ist (also mehrere Nullen am Anfang hat), desto höher ist der Schwierigkeitsgrad. Entsteht also bei der Hashberechnung eine gewisse Anzahl von Nullen am Anfang, ist die Aufgabe gelöst (Abbildung 2.19).

[42] Der Schwierigkeitsgrad gibt an, wie schwer es ist, einen Hashwert unterhalb der gegebenen Zielvorgabe zu finden.

[43] In der Kryptographie wurde die Bezeichnung Nonce (Abkürzung für: „used only once“ oder „number used once“) aufgegriffen, um eine Zahlen- oder Buchstabenkombination zu bezeichnen, die nur ein einziges Mal in dem jeweiligen Kontext verwendet wird [110].

Target for block 100,000	
Hexadecimal	000000000004864c000000000000000000000000000000000000000000000000
Decimal	186131131498380012681564362292723007636833484581425336990197350 4

Hash for block 100,000	
Hexadecimal	000000000003ba27aa200b1cecaad478d2b00432346c3f1f3986da1afd33e506
Decimal	153326787264777690215432048793065921179506558199844584874022631 0

Abbildung 2.19: Hashberechnung der Blöcke [22]

Die Wahrscheinlichkeit, dass ein Nutzer die richtige Lösung findet, ist proportional zu der von ihm eingesetzten Rechenleistung (seiner Hashrate[44]). Nachdem die passende Lösung gefunden wurde, wird der erstellte Block an alle Nutzer verteilt.

Jeder vollständige Nutzer (full node) verifiziert[45] den erhaltenen Block. Abhängig vom Verifikationsergebnis wird der Block akzeptiert (in die Hauptkette[46] oder zur Side Branch[47] hinzugefügt) oder verworfen (Orphan Block[48]). Bei Akzeptanz des Blocks wird dieser immer weiter verschickt.

Durch die Latenz des Netzwerkes verbreiten sich die Blöcke verschieden schnell. Wenn mehrere Miner die Aufgabe gleichzeitig lösen und ihre Blöcke simultan im Netz verteilen, wird sich nach einiger Zeit trotzdem nur eine einzige Kette durchsetzen. Hierfür ein Beispiel. Alice und Bob haben gleichzeitig eine Lösung für die kryptographische Aufgabe gefunden und verbreiten ihre neu geschaffenen Blöcke **a** und **b** im Netz. Jeder Nutzer speichert den zuerst erhaltenen Block nach einer erfolgreichen Verifikation als Teil der Hauptkette (Main Branch). Ein Nutzer **K** erhält den Block **b** von Bob, nachdem er den Block **a** von Alice bereits erhalten hat. Dann fügt er diesen nach einer Verifikation zur Side Branch hinzu und wartet auf den nächsten Block. Charlie ist ebenfalls ein Miner und hat zuerst den Block **b** erhalten. Er baut einen weiteren Block **b+1** und verteilt diesen an alle Nutzer. Der Nutzer **K** erhält den Block **b+1**. Nach Verifikation fügt er diesen zu seiner Side Branch (da der Block **b** von Bob gespeichert ist) hinzu und definiert diese zu einer

[44] Hashrate – oder Rechenleistung, wie viele Hashing-Operationen in einer Sekunde durchgeführt werden können.
[45] Zuerst wird geprüft, ob der Block richtig aufgebaut wurde und ob die Referenzen in dem Blockkopf (Hash) korrekt sind. Für eine detaillierte Beschreibung der Block-Verifikation siehe [13].
[46] Auch Main Branch – die längste Kette, die von allen Knoten als gültig verifiziert wurde.
[47] Side Branch entsteht bei einer Abzweigung der Kette (Fork).
[48] Orphan-Blöcke sind entweder die Blöcke, die keinen Vorgängerblock haben, oder die Blöcke aus der kürzeren Kette, die sich nicht durchgesetzt hat.

Hauptkette um, da die längste Kette am Ende zu einer Hauptkette wird. Die Blöcke aus der Side Branch werden zu Orphan-Blöcken und deren gültige Transaktionen werden wieder in den Zwischenspeicher der Nutzer verschoben. Da sich die Kette mit Bobs Block durchgesetzt hat, erhält Bob nach 100 Blöcken (Wartezeit) eine Belohnung in Form von neu geschöpften Bitcoins und Transaktionsgebühren. Alice erhält keine Belohnung für ihren Block **a**. Die Anzahl neu geschöpfter Bitcoins wird alle vier Jahre halbiert (bis 2012 waren es 50 BTC, bis Juli 2016 lag die Zahl bei 25 BTC, bis 2020 sind es 12,5 BTC, usw.).

Jeder vollständige Bitcoin-Nutzer kann Miner sein und neue Blöcke bauen. In den ersten Jahren des Bitcoin-Systems waren noch alle Teilnehmer Miner. Im Laufe der Zeit ist jedoch die Anzahl der Nutzer sowie die ins Mining eingesetzte Rechenleistung rasant gestiegen. Der Schwierigkeitsgrad der kryptographischen Aufgabe wurde daran angepasst, was eine weitere Aufrüstung der Mining-Hardware sowie steigende Stromverbrauchswerte bedeutet.

Heute müssen Miner, um am Wettlauf teilnehmen zu können, über spezielle Hard- und Software verfügen oder sich am Cloud-Mining beteiligen. Viele Miner schließen sich in so genannten Mining-Pools zusammen, um die Rechenkapazität der Nutzer zu bündeln.

Für das Mining wird entweder ein Computer mit einer leistungsstarken Grafikkarte benutzt oder für das Minen von Bitcoins speziell hergestellte Bitcoin-Miner (z. B. ASIC[49]-Mininghardware). Im Dezember 2017 waren auf dem Markt Bitcoin-Miner mit einer Energieeffizienz zwischen 0,29 J/GH[50] und 0,098 J/GH und einer Leistung zwischen 3.5 TH/s[51] und 13,5 TH/s zu finden. Diese verbrauchen ca. 1.200 Watt. Die Hashrate[52] des Bitcoin-Netzwerkes in der Zeit betrug ca. 12.337.091 TH/s [33]. Es sind also ungefähr 49 GWh, die das Bitcoin-Netzwerk in der Zeit an einem Tag verbrauchte. Zum Vergleich: Ein durchschnittlicher deutscher Haushalt mit vier Personen verbraucht 4.000 kWh an Strom im Jahr. Somit können ca. 12.250 solche Haushalte in einem Jahr genau so viel an Strom verbrauchen, wie das Bitcoin-Netzwerk an einem Tag benötigt. Die Einschätzung des Energieverbrauchs des Bitcoin-Netzwerks geht bei vielen Quellen auseinander. Zum Bespiel lagen im September 2017 Angaben bei Digiconomist bei ca. 19 TWh im Jahr und in einem wissenschaftlichen Paper von Mishra[53] (University of Texas at Dallas) bei 5 GWh.

Ein möglicher Angreifer müsste wie jeder andere Nutzer die Aufgabe mit gleichem Schwierigkeitsgrad lösen und ebenfalls die „Verluste“ in Energie-Ressourcen ertragen, um einen gültigen Block zu erstellen.

Um einen der Blöcke, der bereits in die Blockchain aufgenommen wurde, zu fälschen, müsste ein Angreifer alle weiteren Blöcke ebenfalls umrechnen. Da jede kleine Änderung in einem Block zu einem neuen Hash führt, würden die Referenzen in den Blöcken nicht mehr stimmen. Für eine erfolgreiche Manipulation

[49] Application Specific Integrated Circuits.
[50] Joule pro Gigahash.
[51] Terahashes pro Sekunde.
[52] Hashrate oder Rechenleistung – wie viele Hashing-Operationen in einer Sekunde durchgeführt werden können.
[53] Mishra, Sailendra Prasanna. Bitcoin Mining And Its Cost. 2017.

des Blockinhaltes müsste der Angreifer über 51 Prozent der Rechenleistung des kompletten Bitcoin-Netzes verfügen.

2.3 Konsensfindung in einem dezentralen Netz

Um Chaos in einem dezentralen Netz zu vermeiden, in dem jeder Teilnehmer gleichberechtigt ist und es keine vertrauenswürdige zentrale Instanz gibt, sind bestimmte Regeln und ein Entscheidungsfindungsmodell (Konsensalgorithmus[54] oder consensus algorithm) erforderlich, an die sich alle Teilnehmer halten und worauf sie sich entsprechend einstellen können.

Wie beschrieben, beinhaltet jede Nutzer-Applikation eine Reihe von Regeln – etwa wie Transaktionen und Blöcke aufgebaut, verifiziert und verbreitet werden, wie Verbindungen mit anderen Nutzern im Netzwerk aufgebaut werden und wie die richtige Reihenfolge der Blöcke in der Blockkette sichergestellt und manipulationssicher gemacht wird. Die letztgenannte Regel unterscheidet sich von System zu System und erfordert einen Konsens zwischen allen Nutzern darüber, wie der Nachweis für die Berechtigung zur Erstellung neuer Blöcke zu erbringen ist. In diesem Kapitel werden mehrere Konsensalgorithmen aufgeführt und verglichen.

Das Problem, in einem auf mehrere Rechner verteilten System, indem manche Rechner fehlerhaft sein können und somit falsche Informationen verteilen können, Einigkeit (Konsens) zu erreichen, ist auch als Problem der byzantinischen Generäle bekannt (eine Beschreibung des Problems enthält Anhang 6.4).

Laut Lamport [128] kann die Einigkeit zwischen den Knoten (Rechnern, Nutzern) in einem synchronen[55] System auch dann erreicht werden, wenn bis zu einem Drittel davon böswillig sind. Die Fehlertoleranz liegt somit bei rund 33 Prozent (die Einigkeit kann erzielt werden, wenn die Anzahl an fehlerhaften oder böswilligen Knoten unter 33 Prozent liegt).

In einem asynchronen[56] System ist die Fehlertoleranz entsprechend niedriger. Im FaB Paxos Protokoll[57] zum Beispiel werden bis zu einem Fünftel böswillige Knoten (oder auch byzantinische Fehler genannt) toleriert. Somit kann eine Einigung in einem asynchronen System mit 20 Prozent böswilliger Knoten erreicht werden. [141]

Es existieren mehrere Algorithmen, die es erlauben, durch das Einführen weiterer Restriktionen die Fehlertoleranz in asynchronen Systemen mit steigernder Anzahl

54 Konsens: Übereinstimmung bzgl. gemeinsamen Wertes [44].

55 Aktivitäten werden mit Synchronisation untereinander ausgeführt (durch gemeinsame Uhren oder andere Synchronisationsmechanismen gesteuert) [139].

56 Keine Synchronisation vorhanden [139].

57 Martin, J-P. and Lorenzo Alvisi. „Fast byzantine consensus.“ Dependable and Secure Computing, IEEE Transactions on 3.3 (2006): 202-215. Das Protokoll demonstriert eine Lösbarkeit des Konsensusproblems in „semi-synchronen“ Systemen und geht verschiedene Kompromisse bezüglich der Anzahl an Prozessoren, der Anzahl an Nachrichtenverzögerungen vor dem Lernen des vereinbarten Wertes, des Aktivitätslevels der einzelnen Teilnehmer, der Anzahl an versandten Nachrichten und der Fehlertypen ein [111].

der Knoten zu verbessern (z. B. Nutzen von digitalen Signaturen, Etablierung von Nutzergruppen usw.).

Zurzeit gib es eine Reihe von Blockchain-Projekten aus unterschiedlichen Branchen, die auf verschiedenen Konsensalgorithmen basieren. Folgende Algorithmen sind aktuell am weitesten verbreitet:

- Byzantine Agreement Algorithmus (BA),
- Federated Byzantine Agreement (FBA),
- Proof-of-Work (PoW),
- Proof-of-Stake (PoS),
- Proof-of-Burn (PoB).

Der Byzantine Agreement Algorithmus bietet eine Lösung für das Problem der byzantinischen Generäle und erlaubt somit eine Einigung zwischen Knoten („Generälen“) in einem synchronen System mit einem Drittel fehlerhafter oder böswilliger Knoten. Laut Lamport [128] erstellt jeder Knoten (Rechner, Nutzer) einen Vektor mit denjenigen Werten, die er von anderen Knoten erhalten hat. Nachdem die Vektoren konstruiert worden sind, werden diese ausgetauscht. Jeder Knoten prüft alle erhaltenen Werte aus jedem Vektor, trifft eine Mehrheitsentscheidung und verwendet diese als Ergebnis des Algorithmus. In seiner Arbeit nutzt Lamport zwei Restriktionen für die Lösung: Versenden von mündlichen und signierten Nachrichten. Aufgrund dessen wurden zwei Algorithmen entwickelt (siehe [143]). Für den Einsatz des Algorithmus in einem verteilten Netzwerk mit gleichberechtigten Knoten, deren Anzahl dynamisch wächst, müssen weitere Restriktionen vorgenommen werden.

Eine Weiterentwicklung des Byzantine Agreement (BA)[58] wurde im Rahmen des Stellar Consensus Protocol (SCP) vorgenommen. Stellar ist eine öffentliche Finanzplattform, mit der Geld in unterschiedlichen Währungen einfach verschickt werden kann. SCP basiert auf einem neuen Modell für Konsens, das im SCP White Paper zum ersten Mal[59] beschrieben wird. Es trägt den Namen Federated Byzantine Agreement (FBA). BA und FBA unterscheiden sich anhand mehrerer Kriterien. BA erlaubt Einigkeit trotz fehlerhafter Knoten. Dafür müssen alle Knoten im Netz einander bekannt sein und frühzeitig verifiziert werden. Im FBA benötigen die Knoten keinen kompletten Überblick über alle anderen Knoten. FBA ermöglicht jedem Knoten die freie Wahl von Mitgliedschaftsgruppen, denen vertraut wird, so genannte Quorum Slices. Ein Quorum ist eine Menge von Knoten, die ausreicht, um eine Einigung zu erzielen. Ein Quorum Slice ist die Untermenge eines Quorums, die einen bestimmten Knoten von der Einigung überzeugen kann. Jeder Knoten kann mehrere Slices haben, die er basierend auf ihrer Reputation oder finanziellem Arrangement aussuchen kann.

Die Quoren können sich überschneiden, wenn diese gemeinsame Knoten haben. Um eine Einigung zu erzielen, stimmen sich die FBA Knoten miteinander ab.

[58] Byzantinische Einigung.
[59] White Paper vom 25. Februar 2016.

Dafür nutzen diese das Federated Voting. Durch die Überschneidung der Quoren können die Slices sich gegenseitig bei der Entscheidungsfindung beeinflussen. Neue digitale Münzen (Coins) im Stellar System, auch lumens genannt, werden wöchentlich durch eine solche Abstimmung an die Knoten vergeben (ein Prozent jährliche Schöpfungsrate).

Der bereits für das Bitcoin-System vorgestellte Konsensalgorithmus Proof-of-Work (PoW) wird sowohl für die Fortschreibung der Blockchain als auch für die Erstellung neuer Bitcoins eingesetzt (Mining). Für jeden neu erzeugten Block erhält der Miner eine Belohnung in Form von neu erstellten Bitcoins und den von Nutzern (Knoten) erfassten Transaktionsgebühren. Beim Proof-of-Work-Konzept werden Energie-Ressourcen für das Lösen einer kryptographischen Aufgabe eingesetzt.

Der Vorwurf der Verschwendung von Elektrizität ist der größte Kritikpunkt am Proof-of-Work-Konzept. Im Gegensatz dazu basiert Proof-of-Stake (PoS) auf dem Anteil an digitalen Münzen einer Kryptowährung und nicht auf dem Aufwand für das Lösen der kryptographischen Aufgabe. Ein Nutzer (Knoten), der n Prozent der digitalen Münzen besitzt, darf n Prozent der Blöcke erstellen.

Im Peercoin-System[60] (nutzt PoS) etwa basiert der verwertbare Anteil an digitalen Münzen auf dem so genannten Alter der Münze (coin age). Die Anzahl an digitalen Münzen, die ein Block-Erzeuger besitzt, wird mit der Anzahl der Tage multipliziert, in denen die digitalen Münzen beim Block-Erzeuger verwahrt wurden (wenn etwa Alice 5 Münzen von Bob erhalten hat und diese in ihrer Blockchain-Wallet bereits während 10 Tage verwahrt, beträgt das Münzen-Alter also 50 Münzen-Tage). Für eine erfolgreiche Block-Erzeugung muss das Münzen-Alter zwischen 30 und 90 Tagen liegen. Diese digitalen Münzen werden bei der Blockerstellung in der ersten Transaktion vom Block-Erzeuger an sich selbst geschickt. Danach sind diese erst in 30 Münzen-Tagen wieder für Minting (Block-Erzeugung in PoS) gültig. Jeder Nutzer (Knoten) des Peercoin-Systems kann einen Block erstellen und jährlich dafür eine Belohnung im Wert von maximal einem Prozent der gehaltenen digitalen Münzen erhalten. Die Belohnung besteht aus neu erzeugten Peercoins. In diesem System werden die Transaktionsgebühren nicht an die Block-Erzeuger weitergeleitet, sondern vernichtet, um die Inflation der Peercoins und die Neigung, nur eigene Blöcke (und nicht von anderen Minters[61]) zu bestätigen, zu minimieren.

Zusätzlich zu dem Proof-of-Stake-Konzept wird im Peercoin-System auch Proof-of-Work eingesetzt (hybrid consensus).

Im Gegensatz zum Peercoin-System sind bei der NXT-Kryptowährung alle digitalen Münzen (Coins) von Beginn an (Genesis-Block) vorhanden und die Transaktionsgebühren dienen als Motivation für die Block-Erzeuger. NXT setzt einen modifizierten PoS-Algorithmus ein [125].

Für ein reines PoS Konzept gibt es das spezifische Problem „Nothing at Stake“. In dem Fall, dass es zu einer Verzweigung der Kette kommt, können die Minters parallel, auf beiden Verzweigungen, ohne wesentliche Verluste neue Blöcke bauen. Somit besteht die Möglichkeit der doppelten Ausgabe von digitalen Münzen

[60] Peercoin ist eine Peer-to-Peer Kryptowährung, welche auf dem Design von Satoshi Nakamotos Bitcoin basiert [127].

[61] Block-Erzeuger in PoS.

(double-spending problem). Da der Verlust in diesem Fall nicht so spürbar ist wie z. B. im PoW-Konzept, ist PoS stärker für Attacken anfällig.

Dieses Problem wird in einer erweiterten Art von PoS gelöst. Es nennt sich „Delegated Proof-of-Stake“. Hier gibt es Delegates (Vertrauenspersonen), nach bestimmten Regeln ausgewählte Nutzer (z. B. basierend auf der Anzahl der zu besitzenden digitalen Münzen oder der von anderen Nutzern gegebenen Wahlstimmen). Diese dürfen am Minting teilnehmen und die von anderen Delegates erstellten Blöcke verifizieren. Damit ein neuer Block akzeptiert wird, müssen mehrere Delegates diesen nach einer erfolgreichen Verifizierung signieren. Um Attacken zu vermeiden, werden die digitalen Münzen der Delegates im Falle eines bösartigen Verhaltens gesperrt.

Eine Alternative zu PoW und PoS ist das Proof-of-Burn-Konzept (PoB). Hier werden beim Mining digitale Münzen vernichtet (im übertragenen Sinne „verbrannt“). Je mehr digitale Münzen vernichtet werden, desto höher ist die Chance, dass der neu erstellte Block akzeptiert und in die Kette eingetragen wird. Die zu vernichtenden Münzen werden an eine Adresse verschickt, wo sie nicht mehr verwendbar sind.

In verteilten Netzwerken ist die dezentrale Steuerung eine essenzielle Eigenschaft. Proof-of-Work ist der bekannteste dezentrale Konsensalgorithmus, der sich durch den Einsatz physischer Ressourcen (Energieverbrauch durch Aufwendung von Rechenleistung) von anderen hier beschriebenen unterscheidet. Miner müssen sich dabei, um Verluste möglichst gering zu halten und den Wettkampf um die Belohnung zu gewinnen, an die Regeln halten (richtige Blöcke bauen) oder durch die höchste Rechenleistung (mehr als 51 Prozent) andere Knoten von der Richtigkeit der Blöcke überzeugen.

Unter diesen Umständen ist die „Strafe“ für ein bösartiges Verhalten relativ hoch. Das motiviert die Einzel-Miner zusätzlich, nach den im System festgelegten Regeln zu agieren. Die Wahrscheinlichkeit ist sehr gering, dass in einem System mit zahlreichen Knoten (wie Bitcoin) einer von diesen mehr Rechenleistung besitzt als alle anderen Knoten zusammen (über 51 Prozent der gesamten Rechenleistung).

Da die Belohnung für neu erzeugte Blöcke im Bitcoin-System aus geschöpften Bitcoins und Transaktionsgebühren besteht und sich die Anzahl der geschöpften Bitcoins alle vier Jahre halbiert, bleiben für die Miner hauptsächlich die Transaktionsgebühren als Motivation für die Blockerzeugung übrig. Der Energieverbrauch hängt von dem Schwierigkeitsgrad der kryptographischen Aufgabe ab, der seinerseits an die Rechenleistung des Bitcoin-Netzwerks angepasst wird. Wenn die Rechenleistung des Bitcoin-Netzwerks und dementsprechend der Energieverbrauch weiter steigen, müssen die Transaktionsgebühren entsprechend erhöht werden, damit es sich für die Miner weiterhin lohnt.

Konzepte wie PoS und PoB lösen das Problem des verschwenderischen Energieeinsatzes durch die Verlagerung des Schwerpunktes von physischen auf elektronische Ressourcen. Dadurch steigt allerdings die Wahrscheinlichkeit der Verzweigung der Kette und der doppelten Ausgaben, was seinerseits mit weiteren Restriktionen gelöst werden kann, z. B. mit dem Delegated Proof-of-Stake-Konzept.

Das Federated Byzantine Agreement löst das Problem des Vertrauens zwischen den Knoten ohne einen Ressourcen-Besitz vorauszusetzen, dafür wird ein Federated Voting betrieben.

Algorithmus	Dezentrale Steuerung	Geringe Latenz	Flexibles Vertrauensmodell	Asymptotic Security
Proof-of-Work	+	-	-	-
Proof-of-Stake	+	vielleicht	-	vielleicht
Byzantine Agreement	-	+	+	+
Stellar Consensus Protocol	+	+	+	+

Abbildung 2.20: Vergleich der Konsensalgorithmen und deren Eigenschaften [130]

SCP bietet laut SCP[62] White Paper gleich vier für einen Konsensalgorithmus entscheidende Eigenschaften: dezentrale Steuerung, geringe Latenz, flexibles Vertrauensmodell, Asymptotic Security (siehe Abbildung 2.20).

Im Vergleich zu Proof-of-Work und Proof-of-Stake hat SCP geringere Anforderungen an die Rechenleistung und ist offen für neue Teilnehmer.

2.4 Sicherheit

Die Blockchain-Architektur bietet ein hohes Level an Sicherheit. Die eingesetzten kryptographischen Algorithmen gehören mit zu den besten. Natürlich besteht die Gefahr, dass diese in der Zukunft durch den Einsatz von Quanten-Computern geknackt werden können [89]. Die Entwickler des Bitcoin-Systems versprechen, auf bessere Algorithmen umzuschalten, wenn die Gefahr real wird [67].

Der Quellcode des Bitcoin-Systems ist öffentlich und wird von zahlreichen IT-Experten auf Schwachstellen analysiert und kontinuierlich verbessert. In den vergangenen drei Jahren wurden keine schwerwiegenden sicherheitsrelevanten Schwachstellen mehr gefunden [67, 61]. Seitdem wurden viele Änderungen vorgenommen, um das Bitcoin-System gegen zahlreiche Angriffe sicher zu machen. Die bekanntesten werden hier aufgelistet.

2.4.1 Denial-of-Service-Angriff

Bei einer gezielten Überlastung der Netzwerkknoten, z. B. der vollständigen Nutzer (full nodes), können diese nicht mehr zur Verfügung stehen. Die Überlastung

[62] Stellar Consensus Protocol (SCP).

kann durch das Versenden unzähliger Nachrichten an das Opfer stattfinden; es verbraucht viele Ressourcen, um die empfangenen Nachrichten zu bearbeiten.

Dagegen setzt Bitcoin eine reputationsbasierte Regel ein: Jeder Nutzer, der eine fehlerhafte oder manipulierte Nachricht versendet, erhält dafür Strafpunkte. Wenn deren Anzahl 100 erreicht, wird diese IP-Adresse für 24 Stunden gesperrt [117]. Da der Angriff von mehreren IP-Adressen, z. B. von einem Botnet, ausgehen kann, stellt Bitcoin weitere Regeln gegen DoS[63]-Angriffe auf. Dazu gehören zum Beispiel diese:

- Orphan-Transaktionen und -Blöcke nicht an andere Nutzer weiterleiten,
- Transaktionen, deren Inhalt (Bitcoins) bereits aufgebraucht ist, nicht weiterleiten (double-spend transactions),
- eine bereits an einen Nutzer versendete Nachricht (Transaktion, Block, Adresse eines weiteren Nutzers) darf nicht doppelt versendet werden,
- die Blockgröße darf 1 MB nicht überschreiten.

2.4.2 Flood-Angriff – Spam-Transaktionen

Der Angreifer erstellt mehrere Transaktionen an sich selbst. Dies geschieht mit dem Ziel, dass ein neuer Block nur mit seinen eigenen Transaktionen gefüllt wird und die Aufnahme der Transaktionen von anderen Nutzern verzögert wird. Dabei setzt er keine Transaktionsgebühren ein.

Das Bitcoin-System erlaubt allerdings nur fünf Prozent gebührenfreie Transaktionen im Block. Das heißt, dass ein Angriff nur dann möglich ist, wenn der Angreifer bereit ist, seine Bitcoins dafür zu verschwenden [67].

2.4.3 51 Prozent-Angriff

Ein Miner, der über mehr Rechenkapazität verfügt (Hashrate), kann neue Blöcke schneller als andere Miner erstellen. Wenn ein Angreifer über mehr als 50 Prozent der gesamten Rechenkapazität des Netzwerkes verfügt, sind ihm folgende Manipulationen der Blockchain möglich:

- das Mining neuer Blöcke monopolisieren und die Belohnung dafür nur für sich selbst behalten,
- eine eigene Blockchain, die längste Kette, durchsetzen,
- in die Blöcke nur eigene Transaktionen aufnehmen oder die Transaktionen bestimmter Nutzer blockieren (nicht in die Blöcke aufnehmen),
- doppelte Ausgaben[64] (double spending) durchführen. Bei der Blockgenerierung soll der Miner prüfen, ob die Werte bereits vom Nutzer in früheren

[63] Denial-of-Service.

[64] Mehr zu dem Thema finden Sie im [140].

Transaktionen „ausgegeben“ wurden (also ob er der Besitzer ist). Der Angreifer kann diese Regel bei der Blockerstellung ignorieren und bereits von ihm ausgegebene Werte mehrfach nutzen.

Um frühere Blöcke zu ändern, muss der Angreifer von dem zu verändernden Block an die ganze Kette (Blockchain) neu berechnen, also alle zurückliegenden Blöcke bis zum ersten Block neu generieren. In diesem Fall kann der Angreifer nur die Reihenfolge der Transaktionen in der Kette verändern oder diese aus der Kette herausnehmen. Er kann jedoch keine neuen Werte generieren (z. B. Bitcoins, nur durch Belohnung) oder Werte aus Transaktionen anderer Nutzer auf sich umleiten (nur möglich, falls der Angreifer über geheime Schlüssel[65] der Nutzer verfügt). [116]

Leichtgewichtige Nutzer (lightweight nodes) haben keine vollständige Blockchain und können keine vollständige Verifikation der Transaktionsinhalte gewährleisten. Diese müssen also dem Miner vertrauen und sind deswegen nicht so sicher wie vollständige Nutzer (full nodes) [67]. Beide Konzepte, PoW und PoS, sind somit durch den 51 Prozent-Angriff angreifbar.

Ein derartiger Angriff kann im Bitcoin-System sehr viel Geld verschlingen. Laut BTCECHO kann eine solche Attacke rund 375,2 Millionen Euro pro Tag kosten [37]. Gewinnorientierte Angreifer bevorzugen also sicher eine günstigere Alternative.

Im Bitcoin-System haben Mining-Pools den größten Anteil an Rechenkapazität (Abbildung 2.21).

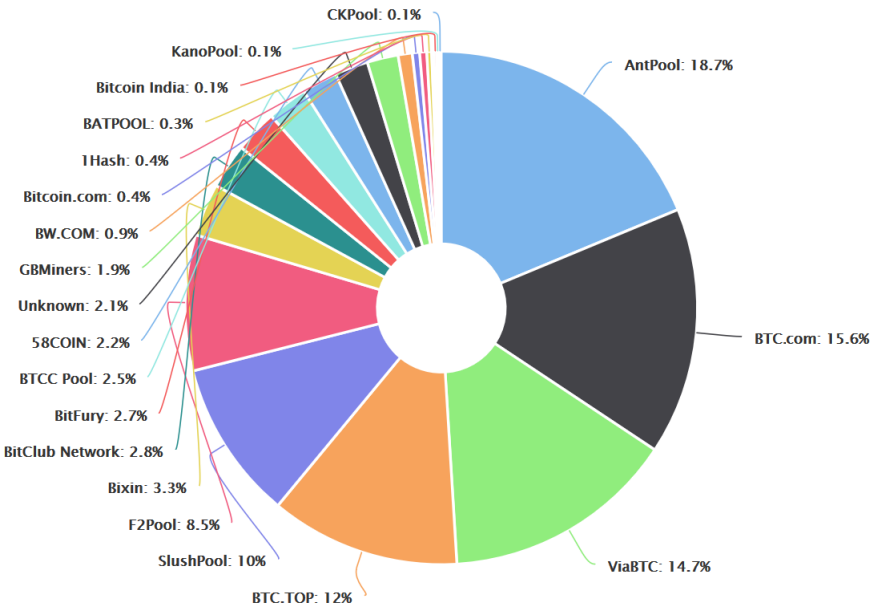


Abbildung 2.21: Marktanteil der größten Bitcoin Mining Pools, Stand 01.12.2017 [69]

[65] Private Key.

Im Juli 2014 erreichte der Mining-Pool Ghash.io mehr als 50 Prozent der Rechenkapazität des gesamten Bitcoin-Netzwerkes. Die Bitcoin-Community reagierte darauf und führte bestimmte Einschränkungen ein. Derzeit gilt eine Absprache zwischen den Mining-Pools, die Grenze von 39,99 Prozent nicht zu überschreiten. Zusätzlich wurde ein Aufsichtskomitee eingerichtet, um die Rechenkapazität der Mining-Pools zu bewachen. Es besteht aus Vertretern der Mining-Pools, Vertretern von Bitcoin-Unternehmen und weiteren Spezialisten aus diesem Bereich [109].

Trotzdem besteht durchaus die Möglichkeit, einen Angriff auch mit weniger Rechenkapazität als 50 Prozent des gesamten Netzwerks durchzuführen. Die Erfolgsrate dabei ist allerdings entsprechend gering [140].

2.4.4 Sybil-Angriff

Der Name dieser Angriffsmethode wurde nach der Hauptperson eines Buchs[66] von Flora Rheta Schreiber benannt. Beschrieben wird Sybil, eine Frau mit multipler Persönlichkeitsstörung. Ähnlich zu dem Fall im Buch erstellt der Angreifer in einem verteilten Netzwerk mehrere falsche „Identitäten“ (Knoten, Server), um die Kommunikation im Netzwerk zu manipulieren oder zu stören [17].

Im Fall eines Blockchain-Netzwerkes können solche Angreifer grundsätzlich nur ausgewählte Blöcke und Transaktionen weiterleiten und dadurch weitere Nutzer von dem Netzwerk abkapseln.

Das Bitcoin-System versucht, diesen Angriff durch die Einschränkung ausgehender Verbindungen zu umgehen (siehe Kapitel 2.1.3).

2.4.5 Verfolgung der Transaktionen

Die Verfolgung der Transaktionen zu den Absendern und Empfängern ist eins der am häufigsten auftretenden Probleme in einem Blockchain-Netzwerk. Trotz der Pseudonyme (P2PKH-Adressen[67], siehe Kapitel 2.1.2), die für jede neue Transaktion speziell generiert werden können, und trotz des Einsatzes des TOR-Netzwerkes können Transaktionen zu den Endnutzern nachverfolgt werden. In der wissenschaftlichen Arbeit von Biryukov und Pustogarov aus dem Jahr 2014 wurde eine solche Methode zur Deanonymisierung der Bitcoin-Nutzer beschrieben. Dabei wurden die Bitcoin-Adressen und die IP-Adressen der Absender verknüpft. Die Methode funktioniert auch, wenn die Nutzer eine Firewall haben oder das TOR-Netzwerk nutzen. Aufgrund dieser Informationen wurden in weiteren Bitcoin-Versionen Änderungen vorgenommen [133].

Zu beachten ist: Die IP-Adressen vieler vollständiger Nutzer (full nodes) sind öffentlich. Das erleichtert die Zuordnung von Transaktionen zu diesen IP-Adressen.

Und Mixing-Services (siehe Kapitel 2.1) bieten zwar mehr Anonymität, setzen aber Vertrauen in die Anbieter solcher Dienste voraus.

[66] „Sybil“ - Flora Rheta Schreiber, 1973.
[67] Pay To Public Key Hash Address.

2.4.6 Ausspähen der geheimen Schlüssel

Trotz der innovativen und sicheren Architektur der Blockchain-Technologie und trotz zahlreicher Schutzvorkehrungen gegen viele Angriffe bleibt der Großteil der Sicherheitsmaßnahmen letzten Endes doch dem Endnutzer überlassen. Die Werte einer Blockchain (z. B. Bitcoins) können nur dann einem neuen Nutzer übermittelt („ausgegeben“) werden, wenn der entsprechende geheime Schlüssel (Private Key) zur Verfügung steht. Angreifer können mit wenig Anstrengung und mit Standardwerkzeugen den geheimen Schlüssel eines Nutzers ausspähen, wenn dieser nicht genügend geschützt ist.

Aus diesem Grund wird z. B. den Bitcoin-Nutzern empfohlen, keine Online-Dienste zu nutzen, welche Online-Wallets anbieten. In letzter Zeit litten diese unter Sicherheitslücken, die es den Angreifern ermöglichen, die Bitcoins der Nutzer zu entwenden. [60]

Mehr Sicherheit für die Aufbewahrung der geheimen Schlüssel versprechen Anwendungen, die lokal auf dem Rechner des Nutzers installiert werden. Viele davon bieten eine Verschlüsselung der Wallet und regelmäßige Backups.

Eine Zwei-Faktor-Authentifizierung macht die Aufbewahrung der geheimen Schlüssel noch sicherer. Dabei wird die Identität des Nutzers durch den Nachweis zweier Komponenten geprüft – zum Beispiel eine Kombination aus Hardware-Wallet und PIN oder Passwort.

Dabei werden die geheimen Schlüssel auf einem externen Datenträger gespeichert, der eine PIN oder ein Passwort für die Entsperrung braucht und der immun gegen Viren ist. Der geheime Schlüssel verlässt das Speichermedium nicht. Die Transaktionen werden innerhalb des Datenträgers abgewickelt. Mittels des entsprechenden geheimen Schlüssels werden die Transaktionen signiert. Die signierten Transaktionen werden im Anschluss an die Anwendung auf dem Nutzer-Rechner übergeben. [63]

2.5 Skalierbarkeit – Problem oder Feature?

Die Skalierbarkeit gehört zu der wichtigen Eigenschaft dezentraler Netzwerke. Diese zeigt an, wie die Leistung bei der Größenveränderung des Systems variiert und ob das System verlustfrei wachsen kann.

2.5.1 Systemwachstum – neue Nutzer

Da alle jemals im System getätigten Transaktionen aufgezeichnet werden, wächst die Größe der Blockchain stetig weiter. Die Größe der Bitcoin-Blockchain im Dezember 2017 betrug 147 GB. Ein vollständiger Nutzer (full node) benötigt eine komplette Kopie der Blockchain, um eine erhaltene Transaktion verifizieren zu können.

Eine der wichtigsten Regeln in Bezug auf die Gültigkeit einer Transaktion ist, dass die darin enthaltenen Werte (z. B. Bitcoins) zuvor noch nicht vergeben wurden. Im Hinblick darauf prüft der vollständige Nutzer alle früheren Transaktionen in

der Blockchain bis hin zu der Transaktion, bei der die Werte zuletzt vergeben wurden [55].

Da es nicht im Interesse aller Nutzer ist, viel Speicherkapazität und Rechenleistung zur Verfügung zu stellen, sind im Bitcoin-System leichtgewichtige Nutzer (lightweight node) stark verbreitet. Dieser speichert die Block-Header und die Informationen, die seine Transaktionen betreffen. Anhand der in den Header enthaltenen Information (Merkle-Tree) kann der Nutzer verifizieren, ob die Transaktion in einem Block aufgenommen wurde und wie viele Blöcke bereits dem Block folgen. Da die leichtgewichtigen Nutzer keine Block-Inhalte (Transaktionen) speichern, müssen sie den vollständigen Nutzern vertrauen, dass die Blöcke und Transaktionen regelkonform erstellt sind und keine doppelten Ausgaben enthalten. Das heißt, dass die Sicherheit des Systems von den vollständigen Nutzern abhängt.

Aktuell existieren im Bitcoin-System geschätzt 13-mal so viele leichtgewichtige wie vollständige Nutzer [117]. Beide Zahlen steigen ungleichmäßig. Einige der vollständigen Nutzer betreiben Mining. Viele bündeln ihre Rechenkapazität mit der von anderen und schließen sich zu Mining-Pools zusammen. Am meisten profitieren dabei solche Mining-Pools, deren Teilnehmer aus Ländern mit günstigeren Stromkosten kommen, z. B. China. Dadurch besteht die Gefahr der Zentralisierung des Mining [43].

Für Systeme mit höherem Datenaufkommen, z. B. Cloud-Speicher und Identitätsmanagement, oder für Systeme mit geringerer Speicher- und Rechenkapazität, z. B. Internet der Dinge (IoT), besteht die Möglichkeit, die Blockchain nur zur Protokollierung der Änderungen im System (logs) einzusetzen. So hat es z. B. das Unternehmen Blockstack gelöst (siehe Abbildung 2.14). Das Unternehmen bietet ein Identitätssystem und fügt zu der Blockchain zusätzliche Komponenten für das Management und für die Speicherung von Daten hinzu.

In einer Konsortium- oder privaten Blockchain (Private Blockchain) kann die Rolle der vollständigen Nutzer vom Unternehmen übernommen werden. Die Kunden haben dann nur leichtgewichtige Nutzerapplikationen (mehr in Kapitel 3.1). Somit kann auch das Problem der Sicherheit und Skalierbarkeit gelöst werden. Allerdings bleibt das System dabei nicht mehr komplett dezentralisiert, da das Mining innerhalb des Unternehmens zentralisiert wird.

2.5.2 Systemwachstum – größeres Transaktionsaufkommen

Den Regeln entsprechend werden die Bitcoin-Transaktionen durch Miner alle zehn Minuten in 1 MB große Blöcke zusammengefasst. In der Regel sind es ca. 2.500 Transaktionen in einem Block. Da die Miner dabei möglichst viele Bitcoins verdienen möchten, priorisieren sie Transaktionen mit höheren Gebühren. Das heißt: Nutzer, die wenig oder keine Gebühren bezahlen, müssen länger warten, bis ihre Transaktion in einen Block aufgenommen wird (derzeit etwa eine Stunde). Für die Nutzer, die eher kleinere Währungsmengen austauschen möchten, ist das ungünstig.

Solche Nachteile sollen bei Off-Chain-Transaktionen behoben werden. Die Transaktionen werden hier über so genannte Micropayment-Kanäle (Micropayment channels) außerhalb des Netzwerks ausgetauscht, anschließend in eine Transaktion zusammengefasst und erst dann an das Netzwerk verschickt. Im dritten Quartal

2014 wurde die Technologie für Micropayments bereits in bitcoinj[68] Version 0.10 implementiert.

Die Idee von Micropayment-Kanälen wurde von Joseph Poon und Thaddeus Dryvja in der Bitcoin-Lightning-Network-Technologie weiter verfolgt. Die Technologie erlaubt skalierbare und sofort ausführbare Off-Chain-Transaktionen.

Zwischen den Nutzern werden befristete Micropayment-Kanäle erstellt. Die Nutzer können, solange der Kanal offen ist, Transaktionen in großen Mengen und mit hoher Geschwindigkeit austauschen und nach Ablauf der vereinbarten Zeit diese Transaktionen (oder eine Summentransaktion) für die Blockchain freigeben.

Das Lightning-Network-Konzept hat folgende Vorteile:

- Bidirectional Payment Channels. Zwei Nutzer eröffnen einen „Micropayment-Kanal“ durch Erstellung einer so genannten Finanzierungstransaktion (funding transaction). Dabei überweisen sie einen bestimmten Anteil an digitalen Münzen an eine im Rahmen des Micropayment-Kanals erstellte Adresse (2-of-2 multisignature address[69]). Zuvor haben sie sich über den zu überweisenden Betrag geeinigt (Beispiel: Bob und Charlie einigen sich auf 1.0 BTC und jeder überweist 0.5 BTC, also „finanziert die Transaktion“). In dem Fall, dass es keinen Austausch von digitalen Münzen geben soll, sondern nur einer von beiden Nutzern mehrere kleine Überweisungen tätigen möchte, werden die Münzen nur von ihm an die Adresse gesendet (z. B. Alice überweist 0.8 BTC an die 2-of-2 multisignature address, um später in mehreren Transaktionen digitale Münzen an Charlie zu senden). Nachdem die Finanzierungstransaktion erstellt ist, können nach Zustimmung beider Nutzer von der Adresse mehrere kleine Transaktionen (commitment transactions) getätigt werden. Die kleinen Transaktionen werden für die Aktualisierung des eingesetzten „Kontostandes“ beider Nutzer im Kanal verwendet. Nach dem die erste kleine Transaktion zwischen den beiden Nutzern ausgetauscht wurde, haben diese die Gewissheit, dass sie ihren Geld-Betrag zurückerhalten und sie geben die Finanzierungstransaktion an die Blockchain frei (mit dem Input, bestehend aus den Beiträgen beider Nutzer, und dem Output, bestehend aus dem 2-of-2 multisignature script). Solange die kleinen Transaktionen zwischen den Nutzern ausgetauscht werden, ist der Micropayment-Kanal offen. Um den Transaktionsaustausch zu beenden, wird die letzte kleine Transaktion an Blockchain versandt. [136]
- Möglichkeit, die Transaktionen zu wiederrufen (Revocable Sequence Maturity Contract - RSCMS).
- Jeder der beiden Nutzer kann den Kanal schließen.
- Nur die letzte aktuelle Transaktion wird an die Blockchain übertragen.
- Großes Netzwerk der Micropayment-Kanäle. Im Lightning Network ist auch ein sicherer Transaktionsaustausch zwischen zwei Nutzern möglich, die mit-

[68] Bitcoinj ist eine Java Bibliothek zum Arbeiten mit dem Bitcoin-Protokoll [31].

[69] 2-of-2 multisignature address wird ebenfalls 2-of-2 multisignature script oder 2-of-2 output genannt.

einander keinen offenen Micropayment-Kanal haben. Dabei wird ein Pfad über mehrere Netzwerk-Knoten (Nutzer) gefunden (ähnlich dem Routing im Internet, durch mehrere Hops). Die Technologie, die das erlaubt, heißt Hashed Timelock Contracts (HTLC). Beispiel: Alice hat einen offenen Kanal mit Charlie und Charlie seinerseits mit Bob. Alice und Bob wollen Off-Chain-Transaktionen austauschen. Dann fordert Alice einen Hash von Bob an und zählt die Knoten (Nutzer) zwischen den beiden. Abhängig von der Anzahl der Knoten (zwischen Alice und Bob ist nur ein Knoten - Charlie) setzt sie eine HTLC-Verfallszeit auf zwei Tage. Charlie setzt die HTLC-Verfallszeit mit Bob auf 1 Tag. Bob teilt den Hashwert mit Charlie und somit treffen die beiden eine Einigung, um kleine Transaktionen auszutauschen. Den gleichen Prozess durchlaufen Charlie und Alice (siehe Abbildung 2.22). [136]

- Reduziert die Belastung der Blockchain. Nur die Eröffnungstransaktion (Finanzierungstransaktion) und die Abschlusstransaktion (letzte kleine Transaktion) werden an die Blockchain freigegeben. Das erlaubt den Nutzern des Lightning Networks, ohne die Blockchain zu belasten schnell Transaktionen auszutauschen [29].
- Geringe Gebühren für die bidirektionalen Kanäle. Die Gebühren in Lightning Network sind sehr gering und werden zwischen den beiden im Kanal kommunizierenden Nutzern ausgezahlt.

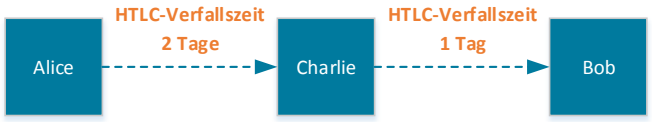


Abbildung 2.22: Netzwerk der Micropayment-Kanäle

Nach dem Whitepaper von Poon und Dryvja (Januar 2016) haben sich zwei Blockchain-Startups, The Bitfury Group und ACINQ, für die Lightning-Network-Technologie interessiert. Das Unternehmen The Bitfury Group entwickelte im Juli 2016 einen Hybrid-Routing-Algorithmus namens Flare[70], der für das Payment-Routing in Lightning Networks eingesetzt werden kann. Das französische Startup ACINQ führte im September 2016 erfolgreich Tests der Lightning-Network-Technologie und des Flare-Algorithmus durch.

[70] Whitepaper [137].

Die Blockchain-Giganten Bitcoin und Ethereum sind ebenfalls dabei, Lightning Networks zu implementieren.[71] Plasma heißt das Framework, das Lightning-Networks-Technologie in Ethereum erlauben wird [135].

2.6 Richtiger Einsatzbereich verspricht den Erfolg

Der Einsatz einer neuen Technologie in einem bestehenden System muss bestimmte Vorteile bringen, also z. B. die Effizienz steigern oder die Kosten senken. Das Kosten-Nutzen-Verhältnis sollte klar sein, bevor man sich für die Blockchain-Technologie entscheidet. Das Ziel, welches dadurch letztlich erreicht werden soll, muss deutlich definiert werden. Dabei sind sowohl die Möglichkeiten als auch die Grenzen der Blockchain-Technologie zu beachten.

Die Blockchain-Technologie erlaubt den Werte-Austausch in einem dezentralen System, ohne dass Vertrauen zwischen dessen Nutzern vorausgesetzt ist. Die Intelligenz liegt bei den Nutzern und nicht bei einer zentralen Instanz. Die Werte werden unveränderbar und unwiderruflich in die Blockchain-Historie aufgenommen. Diese ist transparent und erlaubt den Nachweis, wann ein Wert bei wem in Besitz war.

Ein Unternehmen kann sich, wenn z. B. die Verantwortung für die Konsensfindung im Hause bleiben muss, für eine Konsortium-Blockchain entscheiden oder für eine Private Blockchain, wenn dem Nutzer nur bestimmte Berechtigungen zugeteilt werden sollen (mehr dazu im Kapitel 3.1.).

Die Blockchain-Technologie erlaubt ebenfalls einen Werte-Austausch mit Wenn-Dann-Bedingungen. Dies ist mittels so genannter Smart Contracts möglich (siehe Kapitel 3.3.).

Dadurch, dass die Blockchain-Technologie noch relativ jung ist und sich schnell entwickelt, fehlen ihr noch einheitliche Standards, an die sich alle Entwickler halten können. Aktuell orientieren sich Entwickler an Bitcoin-, Ethereum- und Hyperledger-Systemen; diese dienen als Grundlage für viele weitere Blockchain-Anwendungen.

Ein deutlicher Hinweis auf Schwierigkeiten beim praktischen Einsatz kommt vom Beratungsunternehmen Gartner. Wie die Experten ermittelt haben, scheitern die meisten Blockchain-Projekte bereits in den ersten 18 bis 24 Monaten [83].

Durch fehlende einheitliche Standards kann auch keine Interoperabilität[72] zwischen den unterschiedlichen Blockchain-Anwendungen gewährleistet werden [83]. Aktuell versuchen viele Forscher und Entwickler, eine Balance zwischen Skalierbarkeit und Sicherheit herzustellen und zu gewährleisten.

Wenn sich nach einer kritischen Analyse herausstellt, dass die Blockchain-Technologie für die Umsetzung der Projekt-Ziele von Vorteil ist, sind deren Umsetzungsmöglichkeiten und Anwendungs-Beispiele zu beachten (siehe Kapitel 3 und 4).

[71] Mehr zu dem Thema in [58, 71, 105, 74].
[72] Plattformübergreifende Kompatibilität.

3 Wie setzt man eine Blockchain um?

Sobald klar definiert ist, was man durch die Implementierung der Blockchain-Technologie erreichen möchte, und dies mit den Möglichkeiten und Grenzen der Technologie übereinstimmt, ist zu entscheiden, wie man die Technologie möglichst effizient umsetzt.

Unabhängig davon, mit welchem Ziel oder in welchem Ausmaß die Blockchain-Technologie eingeführt wird, ist es entscheidend, deren Struktur und Funktionsweise genau zu verstehen. Dabei sind folgende Aspekte zu beachten:

- Es müssen die Werte definiert werden, die im neuen System zwischen den Knoten (z. B. Nutzer oder IoT-Geräte) ausgetauscht werden sollen. Diese lassen sich im Normalfall von dem vordefinierten Use-Case[73] ableiten (siehe Kapitel 4).
- Es sind die Berechtigungen der Nutzer festzulegen: Sollen alle Nutzer gleiche Rechte haben und somit ein dezentrales System bilden, oder darf nur ein Teil der Nutzer, der vom Unternehmen festgelegt ist, die Historie der Blockchain ansehen sowie im Konsensfindungsprozess (z. B. die Blockchain fortschreiben) mitwirken? Zu unterscheiden ist dabei zwischen einer öffentlichen[74], Konsortium- und privaten Blockchain[75] (siehe Kapitel 3.1).
- Davon ausgehend wird entschieden, ob eine bereits existierende Blockchain (z. B. Bitcoin oder Ethereum) als Basis für ein neues System verwendet oder eine neue Blockchain entwickelt wird (siehe Kapitel 3.2).

Da Bitcoin und viele weitere Blockchain-Projekte Open-Source-Projekte sind, stehen Systeme mit unterschiedlichen Konsensalgorithmen für die Duplizierung und Modifikation zur Verfügung. In diesem Fall ist der Begriff „Fork“ von Bedeutung. Denn jegliche Modifikation einer bestehenden Blockchain-Software, die zu Änderungen in festgelegten Regeln führt (consensus protocol), wird als Forking bezeichnet (z. B. Bitcoin Fork). Die Blockchain verzweigt sich dann; die daraus entstehenden beiden Zweige haben bis zur Verzweigungsstelle den gleichen ersten Block (Genesis-Block) und die gleichen Vorgänger-Blöcke.

Blockchain-Forking kennt zwei Arten: die Hard und Soft Fork. Bei der Hard Fork müssen die Änderungen in der Software von allen Knoten akzeptiert werden (etwa eine Änderung in der Architektur der Blockchain: Blockgröße von 1 MB auf 2 MB erhöhen). Es sind bereits mehrere Hard Forks an der Ethereum-Blockchain

[73] Kryptowährung, Aufzeichnung des Besitzes oder komplexere Systeme mit Smart Contracts.
[74] Public Blockchain.
[75] Private Blockchain.

durchgeführt worden. Die erste fand am 20. Juli 2016 statt, da einen Monat zuvor durch einen Angreifer, der einen Fehler im The DAO[76]-Framework gefunden hatte, 3,6 Millionen Ether[77] (65 Millionen Euro) entwendet wurden. Die Ethereum-Entwickler spürten den Fehler auf und entschieden sich für ein Hard Fork Update, um die entwendeten Ether wiederzubekommen.

Soft Fork betrifft Änderungen in Blockchain, etwa neue oder aktualisierte Funktionalitäten, die nur von den Minern sowie von den Nutzern, die sie verwenden möchten, angenommen werden müssen. Eine Soft Fork ist im Gegensatz zur Hard Fork rückwärtskompatibel. So entstehen viele neue Applikationen, die z. B. Bitcoin-Blockchain verwenden. Dabei werden manche Funktionalitäten geändert oder hinzugefügt.

3.1 Private und Public Blockchain

Das große Interesse vieler Unternehmen an der Blockchain und deren Implementierung für unterschiedliche Anwendungszwecke hat zahlreiche Versuche zur Folge, die Technologie an eigene Bedürfnisse anzupassen. So wird, wie bereits angerissen, mittlerweile zwischen der öffentlichen[78], privaten[79] und Konsortium-Blockchain unterschieden.

In einer öffentlichen Blockchain (Public Blockchain) können alle Nutzer Transaktionen senden und empfangen, die Historie sehen sowie an der Blockchain-Fortschreibung (Mining, Minting usw.) teilnehmen. Soweit weitere Einschränkungen in den Nutzer-Berechtigungen vorgenommen werden, spricht man über Konsortium- oder Private Blockchain. Dadurch bleibt das Blockchain-System nicht mehr komplett dezentral.

In einer Konsortium-Blockchain (Consortium Blockchain) werden die Berechtigungen für die Teilnahme am Konsensfindungsprozess auf eine Gruppe von Nutzern eingeschränkt. Die Möglichkeit, die Blockchain-Historie einzusehen, kann dabei entweder allen Nutzern oder nur einer bestimmten Gruppe gegeben werden [20].

Die private Blockchain (Private Blockchain) führt zu weiteren Einschränkungen in den Nutzer-Berechtigungen. Es besteht keine Transparenz der Historie mehr, diese ist nur für vordefinierte Nutzer gegeben (z. B. im Bereich eines Unternehmens oder auf mehrere Unternehmen verteilt). Die Berechtigung, die Blockchain fortzuschreiben und Transaktionen zu erstellen, ist auf eine Gruppe von Nutzern eingeschränkt.

In den privaten Blockchains sind Änderungen an der Software einfacher und schneller durchzuführen. Die Nutzer, welche die Blockchain fortschreiben und verifizieren können, sind bekannt. Das Risiko eines 51 Prozent-Angriffes besteht, wenn

[76] The DAO – auf Ethereum-Blockchain realisierte dezentrale autonome Organisation (Decentralized Autonomous Organization). Mehr dazu im Kapitel 4.2.
[77] Ether – Kryptowährung von Ethereum.
[78] Public Blockchain.
[79] Private Blockchain.

auch modifiziert, trotzdem weiter. Denn die Nutzer, die für die Fortschreibung der Blockchain und die Teilnahme an dem Konsensfindungsprozess vorausgewählt wurden, können von möglichen Angreifern manipuliert werden [107].

Jede Art der Blockchain hat eigene Vorteile und Nachteile, die sich in bestimmten Einsatzbereichen stärker oder schwächer ausprägen.

3.2 Einsatzarten der Blockchain

Gewünschter Einsatzbereich der Blockchain, zu übertragende Werte, Nutzerberechtigungen, mögliche/geplante Ausgaben – anhand solcher Fakten sollte man sich für die Art entscheiden, wie die Blockchain-Technologie umgesetzt werden soll. Es gibt zahlreiche Projekte und Anbieter auf dem Markt, die Unternehmen bei der Blockchain-Einführung unterstützen. Letztlich muss sich ein Unternehmen entscheiden, ob es eine eigene Entwicklung anstrebt oder ob eine bestehende Blockchain (z. B. Bitcoin oder Ethereum) verwendet werden kann.

Es besteht grundsätzlich die Möglichkeit, entweder eigene Miner zu haben oder ein Merged Mining zu betreiben. Im Rahmen des Merged Mining wird der Prozess vom Miner einer Blockchain für mehrere Systeme gleichzeitig betrieben [76]. Das heißt: Miner einer Blockchain erstellen Blöcke für mehrere andere Blockchains. Zum Beispiel werden die Blöcke der Namecoin-Blockchain von den Bitcoin-Miner gebaut. Dabei hat jede Blockchain ihren eigenen Schwierigkeitsgrad.

Nachfolgend sind die bekanntesten Methoden aufgelistet.

3.2.1 Colored Coins

Die „Colored-Coins"-Methode (gefärbte Münzen) ist die einfachste Art, die Blockchain-Technologie zu nutzen. Das Prinzip baut auf einer bereits bestehenden Blockchain[80] auf und fügt zu den bereits vorhandenen Werten (genauer gesagt zu UTXO[81]) zusätzliche Informationen (Metadaten) hinzu. Die originalen digitalen Münzen, z. B. Bitcoins, werden also mit anderen Informationen verknüpft, „gefärbt" und bekommen somit eine andere Semantik/Verwendung. Z. B. nach dem Hinzufügen von zusätzlichen Informationen zu den Bitcoins, können diese einen neuen Wert repräsentieren: ein Zertifikat, eine Aktie, ein Kinoticket, ein gemietetes Apartment oder einen digitalen Schlüssel für ein Haus oder ein Auto [85].

Die Knoten (Nutzer), welche die gefärbten Münzen austauschen, nutzen eine Colored-Coins-Applikation und wissen, welchen Wert oder welche Eigenschaft die Münzen besitzen. Die Miner oder Minter der Blockchain können jedoch die „Farbe" der digitalen Münzen nicht erkennen und sehen alle eingehenden Transaktionen als Standard-Transaktionen. Aus diesem Grund sollen die zugefügten Informationen (Metadaten) von den Nutzern, die Colored Coins verwenden, verifiziert werden.

[80] Die meist benutzten Blockchains für die Colored-Coin-Methode sind Bitcoin-Blockchain und Ethereum-Blockchain.

[81] Unspent Transaction Output (UTXO).

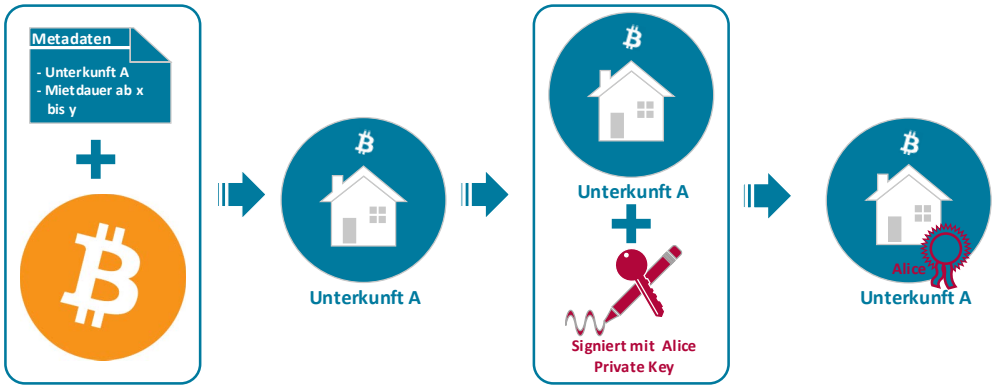


Abbildung 3.1: Colored-Coins-Methode auf Basis der Bitcoin-Blockchain mit einem neuen Wert (Apartment zur Miete)

Ein bekannter Anbieter von „Colored-Coins"-Geldbörsen (Colored coin wallet) ist Coinprism.

Die größte US-amerikanische Börsen-Plattform NASDAQ[82] setzt seit Dezember 2015 Colored Coins in ihrer neuen Plattform namens LINQ ein. LINQ bietet einen Service für sichere private Transaktionen und erlaubt durch die Blockchain-Technologie einen Überblick über alle Vorbesitzer. Die Colored Coins werden zwischen privaten Investoren und/oder Banken ausgetauscht und mit Wertpapieren gekoppelt.

Ein israelischer Provider von Blockchain-basierten-Technologien, Colu, setzt auf Colored Coins in Verbindung mit Lightning-Networks. Das erlaubt einen dezentralen Werte-Transfer mit minimaler Verifikationszeit, einer hohen Rate an Transaktionen pro Sekunde und geringen Gebühren. [48]

3.2.2 Meta Coins

Da die Miner der Bitcoin-Blockchain keine „Farbe" der Colored Coins erkennen und alle eingehenden Transaktionen als Standard-Transaktionen sehen, sollen die zugefügten Informationen (Metadaten) von den Colored-Coins-Nutzern verifiziert werden. Eine Verbesserung des Colored-Coins-Protokolls liefern die Meta Coins. So wie Colored Coins können die Meta Coins beliebige Werte darstellen und werden in einer bestehenden Blockchain erstellt. Der Unterschied zwischen diesen zwei Methoden liegt in einer Middleware[83]-Schicht in Form von dedizierten Servern (diese verifizieren die Colored-Coin-Transaktionen) [126]. Diese wird auf die bestehende

[82] NASDAQ - National Association of Securities Dealers Automated Quotations.

[83] Laut Duden ist Middleware eine Software für den Datenaustausch zwischen Anwendungsprogrammen, die unter verschiedenen Betriebssystemen oder in heterogenen Netzen arbeiten.

Blockchain gesetzt. Diese Methode erlaubt mehr Funktionalitäten im Vergleich zu Colored Coins.

3.2.3 Alternative Chain

Alternative Chain, auch Altchain genannt, ist eine separate und eigenständige Blockchain, die nicht auf eine bereits existierende (z. B. Bitcoin) aufgesetzt wird. Da Bitcoin und viele weitere Blockchain-Projekte Open-Source-Projekte sind, steht der Quellcode der Blockchain mit unterschiedlichen Konsensalgorithmen zur Duplizierung und Modifikation zur Verfügung.

In einer Altchain können die Blockchain-Einheiten[84] beliebige Werte aus unterschiedlichen Einsatzgebieten einnehmen, z. B. kann es sich um digitale Münzen (Altcoins) handeln. Die Blockchain-Regeln können angepasst werden, z. B. können mehr Daten übertragen, die Blockgrößen geändert, die Geschwindigkeit der Blockerstellung erhöht und ein passender Konsensalgorithmus ausgewählt werden.

Durch die Änderungen an der Blockchain können Vorteile erzielt werden wie eine höhere Anzahl an Transaktionen pro Sekunde, aber zugleich können Schwachstellen in der Sicherheit auftreten.

3.2.4 Sidechain

Die Intention, neue Blockchain-Systeme zu entwickeln und diese für neuartige Einsätze zu konzipieren, führt zu immer weiteren Änderungen und Anpassungen in dem ursprünglichen Bitcoin-Code und lässt viele Altchain-Projekte entstehen. Außer Sicherheitsproblemen treffen Altchain-Entwickler beim Aspekt „Interaktion zwischen den Blockchains“ auf weitere Komplikationen wie Interoperabilität (jede Altchain implementiert die Technologie auf ihre eigene Art) oder schwankender Wechselkurs einer neue Kryptowährung (Altcoin) [115].

Die Autoren der wissenschaftlichen Arbeit „Enabling Blockchain Innovations with Pegged Sidechains“ [115] beschreiben deshalb einen neuen Mechanismus, um eine interoperable Altchain einfach entwickeln und nutzen zu können. Mit Hilfe dieses Mechanismus können die Einheiten einer Blockchain an eine andere Blockchain, die Sidechain, übertragen werden. Sidechain nennt man eine Blockchain, die Daten anderer Blockchains erkennen und prüfen kann [115].

Die Idee einer Blockchain-übergreifenden[85] Übertragung bestand bereits vor dieser wissenschaftlichen Arbeit[115]. Das Verfahren[86], als Atomic Swap oder Atomic Exchange bekannt, wurde bereits im Jahr 2012 zwischen Blockchain-Entwicklern diskutiert und 2013 von Tier Nolan weiterentwickelt (siehe Anhang 6.5).

Im Jahr 2014 wurde die Sidechain-Technologie von Adam Back [115] vorgestellt. Die Kernidee sind so genannte Pegged Sidechains. Im Unterschied zur Sidechain kann eine Pegged Sidechain die von einer anderen Blockchain erhaltenen Daten

[84] auch scarce tokens oder ledger assets genannt.
[85] In Englisch: cross-chain oder inter-chain.
[86] Dafür wurden Contracts verwendet, mit einem Secret-Austausch und Lock-Time-Parameter.

zurückübertragen. Der Mechanismus wird Two-Way-Peg genannt und ermöglicht eine Übertragung von Blockchain-Einheiten zwischen Sidechains in beide Richtungen – zu einem festen Umrechnungskurs. Somit kann der Nutzer, ohne neue Blockchain-Werteinheiten direkt zu erwerben, eine neue Blockchain durch die „Umwandlung" vorhandener Werteinheiten testen.

Der Two-Way-Peg-Mechanismus wird in zwei Arten eingeteilt:

- symmetrischer und
- asymmetrischer.

Der Unterschied liegt in der Transaktionsverifizierung. Symmetrischer Two-Way-Peg-Mechanismus unterstützt SPV[87]-Verifizierung auf beiden Blockchains – Parent[88]- und Sidechain – das heißt: Die beiden Blockchains „kennen" sich. Bei dem asymmetrischen Verfahren wird SPV-Verifizierung nur auf der Parentchain gemacht. Das bedeutet: Die Parentchain „kennt" die Sidechain nicht und muss eine SPV-Verifizierung der Sidechain-Daten machen, wobei die Nutzer der Sidechain vollständige Prüfer der Parentchain sind und keinen SPV-Nachweis für die Daten der Parentchain benötigen.

Ein Beispiel: Alice verfügt über Bitcoins und möchte eine andere Kryptowährung oder bestimmte Werte aus einer anderen Blockchain (in unserem Fall Sidechain) haben. Sie nutzt dafür das symmetrische Verfahren. Sie erstellt eine Transaktion, derer Output eine bestimmte Adresse in ihrer Parentchain hat (in dem Fall Bitcoin-Blockchain), wo ihre Bitcoins vorerst für eine Bestätigungsperiode[89] gesperrt werden. Nachdem die Bestätigungsperiode abgelaufen ist, wird eine Transaktion auf der Sidechain erstellt, die sich auf den Output aus der Bitcoin-Blockchain bezieht und einen SPV-Nachweis unterstützt. Die Bitcoins werden anhand eines festen Umrechnungskurses in Sidechain-Werteinheiten umgerechnet. Dann werden die Werteinheiten für weitere ein bis zwei Tage in der Sidechain für eine Wettbewerbsperiode[90] gesperrt. Dies soll die doppelte Ausgabe von Werteinheiten (double-spending) verhindern. Nach der Wettbewerbsperiode stehen Alice die Sidechain-Werteinheiten zur Verfügung (siehe Abbildung 3.2). Sie enthalten Informationen über ihre Parentchain (Bitcoin) und können somit auf die gleiche Weise zurück übertragen werden (ebenfalls mit gesperrtem Output, Bestätigungs- und Wettbewerbsperiode sowie SPV-Nachweis).

Ein wichtiger Faktor bei der Übertragung von Blockchain-Werteinheiten zwischen den Sidechains ist die Sicherheit: Die Empfänger-Chain muss erkennen können, dass die Werteinheiten an der Sender-Chain richtig gesperrt sind.

[87] SPV – Simplified Payment Verification Proof oder in Deutsch - vereinfachter Zahlungsüberprüfungsnachweis, gibt Nutzern eine Möglichkeit Transaktionen zu verifizieren, ohne ganze Blockchain herunterzuladen (z. B. anhand von Block-Header). Bevor eine Transaktion zur Wallet hinzugefügt wird, prüft der Nutzer, ob die Transaktion in dem Block ist und ob der Block in der Hauptkette ist.

[88] Elternblockchain.

[89] Confirmation Period: 1-2 Tage.

[90] Contest Period.

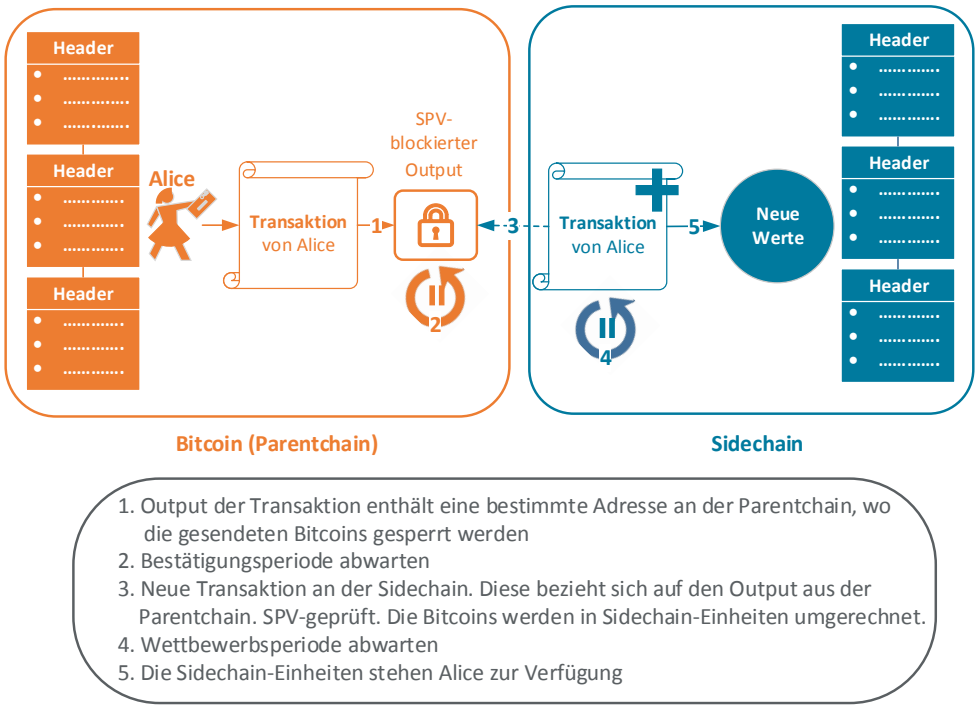


Abbildung 3.2: Konvertierung der Bitcoins in Sidechain-Einheiten

Grundsätzlich kann jede Blockchain angepasst werden, um mit Sidechains interagieren zu können. Die Blockchain-Einheiten können zwischen mehreren Sidechains und zurück zur Parentchain übertragen werden. Um Bitcoin als Parentchain zu nutzen, muss eine Erweiterung (Soft Fork) im Bitcoin-System implementiert werden, um SPV-Nachweise erkennen und validieren zu können.

Die Nachteile der Sidechain-Technologie wurden bereits von deren Entwicklern klar beschrieben:

- Komplexität,
- Risiko der betrügerischen Übertragung,
- Risiko der Zentralisierung von Mining und
- Risiko der Soft Fork (jede Änderung an einem bestehenden System kann Sicherheitsprobleme mit sich bringen) [115].

Die Autoren des Sidechain-Papers gründeten im Jahr der Veröffentlichung das Unternehmen Blockstream, um die Technologie voranzutreiben und Sidechains für unterschiedliche Projekte zu entwickeln.

Ein im Jahr 2015 gestartetes Projekt Rootstock[91] nutzt die Sidechain-Technologie und bietet damit eine Plattform für Smart Contracts an. Die Rootstock-Sidechain hat eine Two-Way-Peg-Verbindung zur Bitcoin-Parentchain, besitzt keine eigene Kryptowährung und gibt die Transaktionsgebühren fürs Merged Mining an Bitcoin-Miner weiter. Die Blöcke auf der Rootstock-Sidechain werden alle zehn Sekunden erstellt.

3.3 Smart Contracts

Zu den Blockchain-Entwicklungen der jüngsten Zeit gehört die Smart-Contracts-Technologie. Dabei wird der Einsatz nicht nur auf den Bereich Kryptowährungen begrenzt, sondern die Technologie mehr als eine programmierbare dezentrale Vertrauensinfrastruktur[92] genutzt.

Ethereum gehört zu solchen Blockchain 2.0-Applikationen und hat nach Bitcoin die am meisten verbreitete und stärkste Blockchain. Sie verfügt über eine Programmiersprache[93] zur Erstellung der so genannten Smart Contracts (intelligente Verträge) und dezentraler Applikationen (kurz „Dapps“ genannt). Dabei lassen sich beliebige Regeln, Transaktionsformate und Funktionalitäten implementieren [81].

Smart Contracts werden von den Ethereum-Entwicklern mit kryptographischen „Kisten“ verglichen, die bestimmte Werte enthalten. Diese Werte können nur entsperrt werden, wenn gewisse Bedingungen erfüllt sind.

Smart Contracts sind komplexe autonome Applikationen,[94] die entsprechend den Anweisungen[95] bestimmte Stücke des Quellcodes mit Wenn-Dann-Bedingungen ausführen. Ein Beispiel: Wenn ein potenzieller Mieter das Geld für das anzumietende Apartment eingezahlt hat und der Tag des Mietbeginns gekommen ist, dann wird ein digitaler Schlüssel für das Aufschließen des Apartments an den Mieter verschickt [34].

Die Smart Contracts haben Kontrolle über ihre Inhalte und Bestandteile, z. B. über die enthaltenen Werte, Bedingungen sowie die Kryptowährung, die für systemabhängige Gebühren benutzt werden kann. Die Smart Contracts werden in einer höheren Programmiersprache geschrieben und anschließend in einen Bytecode übersetzt [103]. Das Ergebnis wird einer Transaktion hinzugefügt. Smart Contracts haben wie Nutzer eigene Adressen, so genannte Accounts, und können sowohl von anderen Contracts durch spezielle Nachrichten[96] oder von Nutzern durch Transaktionen kontaktiert werden. Das bedeutet also: Sowohl die Nutzer-Adresse als auch die Smart-Contract-Adresse kann als Ziel einer Transaktion angegeben werden.

---

91 White Paper [129].
92 Blockchain as a programmable distributed trust infrastructure [27].
93 Höhere Programmiersprachen Solidity, Serpent, LLL usw. [42].
94 Smart-Contract-Applikationen beinhalten Script-Anweisungen wie Contracts und Time-Locks.
95 Erhaltene Nachrichten von anderen Contracts oder Transaktionen von anderen Nutzern [81].
96 Engl. Messages.

Auf dem Rechner jedes Ethereum-Nutzers wird eine virtuelle Maschine (EVM) ausgeführt, die das Lesen und Schreiben von Daten und Code aus und in der Blockchain sowie die Verifizierung der digitalen Signaturen erlaubt. Die EVM führt den Code aus dem Smart Contract nur dann aus, wenn sie eine signierte Nachricht erhält und die Informationen aus der Blockchain-Historie die Ausführung bestätigen [77].

Das Konzept von Smart Contracts gab es längst vor Entwicklung der Blockchain-Technologie. Bereits 1997 hat Nick Szabo in seiner Arbeit „Formalizing and Securing Relationships on Public Networks“ [142] den Begriff Smart Contracts definiert. Dabei beschreibt er die Smart Contracts als eine Kombination aus Protokollen und Benutzerschnittstellen für die Sicherstellung der rechtlich gestützten und kryptographisch gesicherten Beziehungen zwischen den Knoten in einem Rechnernetz. Laut Szabo sollen die von Computern automatisch ausführbaren Verträge im Vergleich zu deren papierbasierten Vorfahren die Kosten für die Bearbeitung reduzieren.

Ein bekanntes Beispiel für den Einsatz von Smart Contracts ist die Vermietung von Autos oder deren Kauf auf Kredit. Anhand der Rahmenbedingungen, die im Smart Contract beschrieben sind, kann das Auto dem Mieter oder Käufer zur Verfügung gestellt werden. Wenn der Käufer eine Kreditrate nicht rechtzeitig bezahlt oder die Mietzeit des Autos abgelaufen ist, kann das Auto für den Nutzer blockiert werden.

Ein Vorteil im Vergleich zu Bitcoin ist bei Ethereum die Multi-Signature-Methode („multisig“). Sie bietet mehr Flexibilität. Im Bitcoin-System können die Nutzer zum Beispiel mit drei von fünf geheimen Schlüsseln ein Guthaben entsperren. Dagegen hat der Ethereum-Nutzer mittels Smart Contracts die Möglichkeit, mit vier von fünf geheimen Schlüsseln das gesamte Guthaben, mit drei von fünf Schlüsseln zehn Prozent pro Tag oder mit zwei von fünf Schlüsseln 0,5 Prozent pro Tag auszugeben. Die Ethereum-Nutzer können unabhängig voneinander eine Transaktion signieren. Somit wird die Transaktion automatisch nach der letzten Signatur abgeschickt [81].

Zu beachten ist: Wenn nur ein geheimer Schlüssel verwendet wird, dann hat man auch nur eine Schwachstelle [94]. Am 19. Juli 2017 wurde ein Fehler in Ethereums Multi-Signature-Wallet gefunden und von Angreifern ausgenutzt. Um weitere betroffene Wallets zu schützen, wurden diese durch eine Gruppe von White-Hat-Hackern gesichert [80].

Für höhere Flexibilität in Smart Contracts sorgen so genannte Oracles. Diese fungieren als eine Brücke zur realen Welt, indem Informationen aus dieser den Smart Contracts zur Verfügung gestellt werden [70]. Zum Beispiel wird für den Umtausch von US-Dollar in BTC ein Oracle für die genaue Umrechnung mit dem jeweils aktuellen Wechselkurs in den Smart Contract eingefügt [81]. Das Londoner Startup Oraclize bietet einen solchen Service für die Verbindung von Blockchain-Daten mit externen Informationen aus dem Internet (Abbildung 3.3) an. Eins der Projekte von Oraclize ist Proof-of-Identity [98]. Dabei wird eine Ethereum-Adresse mit einer estnischen digitalen Identifikationsnummer (Digi-ID) verbunden.

Zusammenfassend gesagt, können die Smart Contracts als spezielle Programme beschrieben werden, die dezentral von jedem Nutzer mit Hilfe einer zur Verfügung stehenden Software erstellt und verifiziert werden. Die wichtigsten Herausforderungen von Smart Contracts liegen in ihrer Rechtsverbindlichkeit sowie in Haftung und Datenschutz. Wer trägt die Verantwortung, wenn sich in den Code des Smart

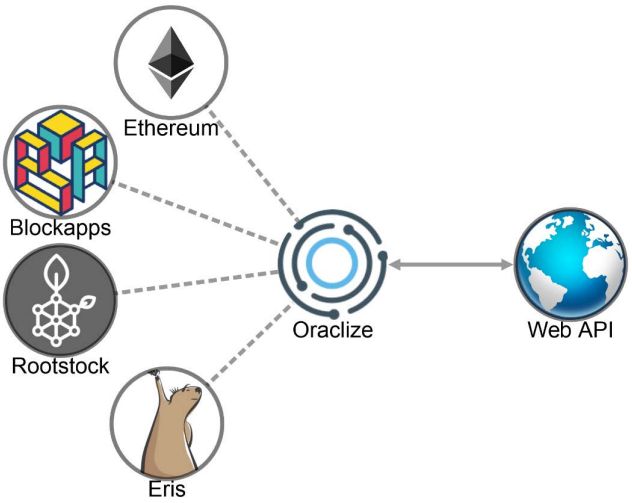


Abbildung 3.3: Oraclize – Datenbote für dezentrale Applikationen

Contracts ein Fehler eingeschlichen hat? Oder wie kann die Rechtsverbindlichkeit eines Smart Contracts in der realen Welt nachgewiesen werden?

Eine Lösung für das Problem der Rechtsverbindlichkeit von Smart Contracts bietet, wie in Kapitel 2.1.5 erwähnt, das Unternehmen Agrello [57]. Sein Produkt unterstützt mit einem benutzerfreundlichen Interface (Abbildung 2.13) bei der Erstellung eines rechtlich bindenden Vertrages. Der mit Hilfe dieser Lösung erstellte Vertrag wird in einen Smart Contract umgewandelt und in einer Blockchain gespeichert. Parallel wird ein rechtsverbindlicher Vertrag in natürlicher Sprache erstellt und digital unterzeichnet [57]. Der Nutzer wird während der Vertragserstellung durch einen AI[97]-Agent unterstützt.

Smart Contracts bieten ein breites Feld an Anwendungsmöglichkeiten, angefangen bei Token[98]-Systemen bis hin zu dezentralen autonomen Organisationen (DAOs). Die Token können unterschiedliche Werte repräsentieren: Währung, Besitz, Ereignis, Eigenschaft [81].

„The DAO“ ist der Name einer Applikation, die als Smart Contract auf der Ethereum-Blockchain realisiert wurde [52]. Diese hatte keine zentrale Managementinstitution und basierte auf den im Code festgeschriebenen Regeln, also gewissermaßen ein Unternehmen ohne eigene Mitarbeiter. „The DAO“ war sozusagen eine Investment-Firma, die allein durch einen Abstimmungsprozess Crowdfunding betrieb. Nach dem Angriff im Juli 2016, der einen entdeckten Fehler im Code ausnutzte, wurde „The DAO“ eingestellt.

Das Unternehmen Ripple plant neuerdings, eine eigene dezentralisierte Applikation auf Basis von Smart Contracts und so genannten Oracles anzubieten [16].

---

97 AI – Artificial Intelligence (auf Deutsch – künstliche Intelligenz).

98 Ein Token (engl. für Zeichen, Marke) ist ein Hilfsmittel zur Synchronisation paralleler Prozesse – wer das Token hat, darf auf die Ressource zugreifen. Wenn z. B. ein Nutzer das Token freigegeben hat, darf ein anderer Nutzer die Ressource benutzen [113].

4 Projekte und Einsatzbereiche der Blockchain-Technologie

Es ist erstaunlich, mit welcher Geschwindigkeit sich die Blockchain-Technologie verbreitet. Durch zahlreiche Tests und viele Projekte dürfte es derzeit wohl keinen Einsatzbereich mit dezentraler Infrastruktur geben, in dem noch keine Blockchain-Einführung versucht wird. Wissenschaft, Medizin, Identitätsmanagement, Cloud Computing, Internet of Things, Banken, Versicherungen, Logistik, Einzelhandel, Energieversorgung – diese und weitere Sektoren sind Nutznießer. Zahlreiche Start-ups werden gegründet, die Blockchain als Gesamtlösung oder Teil einer Lösung anbieten und dabei entweder eine bestehende Blockchain nutzen (z. B. Bitcoin oder Ethereum) oder eine eigene Blockchain entwickeln. Aber auch Unternehmen mit entwickelten Infrastrukturen und eingeführten Produkten und Services wie IBM, Microsoft, Samsung, SAP, Intel und andere experimentieren längst mit dieser Technologie und starten neue Projekte.

Beispielweise nutzt OpenBazaar die Blockchain-Technologie für den P2P-Online-Handel. Jeder Knoten kann als Käufer oder Verkäufer agieren und die erworbene Ware in Bitcoins bezahlen. Die Vorgehensweise, durch Signieren von Transaktionen den Besitz von Objekten oder Daten zu bestätigen und Smart Contracts einzusetzen, ist auch für weitere Einsatzbereiche geeignet:

- Bildende Kunst: Beispielweise beim Kauf und Verkauf von Gemälden auf Auktionen lassen sich Herkunft, Vorbesitzer und gegenwärtiger Besitz einfach nachweisen (Wann wo von wem gekauft?).
- Buchung und Vermietung von privaten Unterkünften sowie Vermietung von Autos und Fahrrädern: Anbieter wie etwa Airbnb und Uber können durch den Einsatz der Blockchain-Technologie besonders profitieren.
- Voting-Systeme: FollowMyVote bietet in Zusammenarbeit mit BitShares eine auf der Blockchain basierende Abstimmungs-Plattform. Das System bietet die Sicherheit, dass abgegebene Stimmen nicht von Dritten geändert werden können, sowie Transparenz und Flexibilität. Ein Voting-Prozess kann nun auf mobilen Geräten von überall aus stattfinden.
- Medizin: Der Einsatz der Blockchain-Technologie im medizinischen Bereich bietet mehr als bloß eine digitalisierte Patientenakte. Da durch neue Technologien, zum Beispiel tragbare Geräte wie Fitness-Armbänder oder Smart Watches, immer mehr neue Gesundheitsdaten generiert werden, ist der Vorteil nicht zu unterschätzen, dass Patientendaten sicher und digital gespeichert werden können – mit beschränkten Zugriffsrechten für bestimmte Daten. Ein smartes Profil kann Patienten zudem die Möglichkeit geben, über die Freigabe eigener Daten selbst zu entscheiden. Darüber hinaus ist es zum Beispiel

möglich, über die Blockchain die anonymisierten Daten mit Forschern (Public Research Repository) zu teilen, mehr über die eigene Erkrankung zu erfahren, mit anderen Erkrankten zu kommunizieren, Spendenakquisition bzw. Crowdfunding zu betreiben und Verschreibungen und Rechnungen digital im Überblick zu behalten [18]. Im Mai 2017, beim Blockchain-Technologie-Treffen „Consensus 2017" in New York, hat das in Los Angeles ansässige Startup-Unternehmen Gem das erste Blockchain-Produkt für das Management von Gesundheitsdaten vorgestellt (Abbildung 4.1) [84].

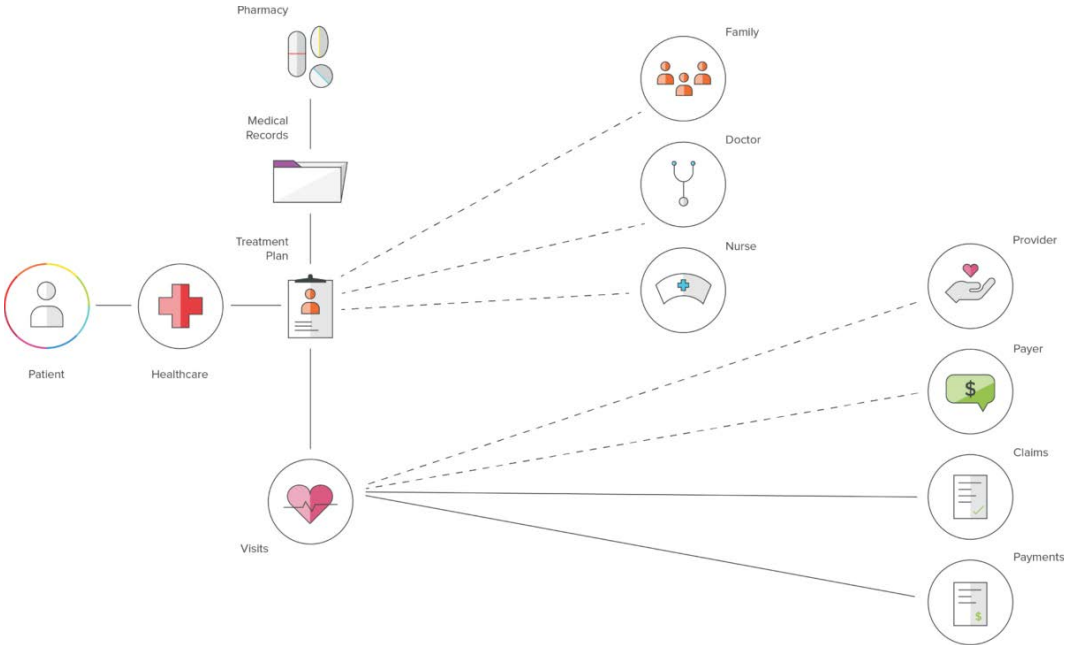


Abbildung 4.1: Gem – Blockchain für Gesundheitsdaten [84]

Für einen sicheren Zugang zu anonymisierten Genom-Daten will zudem das Unternehmen Encrypgen mit der Gene-Chain sorgen.

Soziale Netzwerke und freie Presse profitieren ebenfalls von der Blockchain-Technologie. Steemit ist eine Blockchain-basierte Social-Media-Plattform. Die Nutzer der Plattform publizieren dort ihre Inhalte (z. B. Nachrichten) und werden von anderen Nutzern dafür in der eigenen Kryptowährung belohnt. Steemit gab auch den Impuls für ein weiteres Projekt namens Publicism. Dieses hat das Ziel, freie Meinungsäußerung zu ermöglichen und Journalisten eine Plattform für anonyme und sichere Veröffentlichungen zur Verfügung zu stellen. Die Journalisten werden durch Micro-Payments belohnt, die durch Spenden und Crowdfunding zusammenkommen. Dank Blockchain-Technologie ist Zensur durch eine zentrale Instanz ausgeschlossen [99]. Eine der Herausforderungen im Projekt ist die absolute Anonymität der Nutzer (z. B. Journalisten).

Eine weitere Blockchain-Lösung richtet sich nicht nur auf eine bestimmte Zielgruppe, sondern sieht sich als eine Personen-Schicht in einem dezentralen Pro-

tokollstapel. Das Unternehmen Colony bietet in diesem Zusammenhang eine Infrastruktur für die Entwicklung offener Organisationen. Das Colony-Protokoll ist ein Ehtereum Smart Contract und ermöglicht Entwicklern, in ihre Anwendungen dezentrale und selbstregulierende Arbeitseinteilung, Entscheidungsfindung und Finanzmanagement zu integrieren. Das bedeutet: Dank der Colony-Lösung können anonyme und dezentrale Organisationen entstehen, deren Mitarbeiter aus der ganzen Welt kommen, sich für ein oder mehrere Projekte digital zusammenschließen und nach ihrem Einsatz belohnt werden [75].

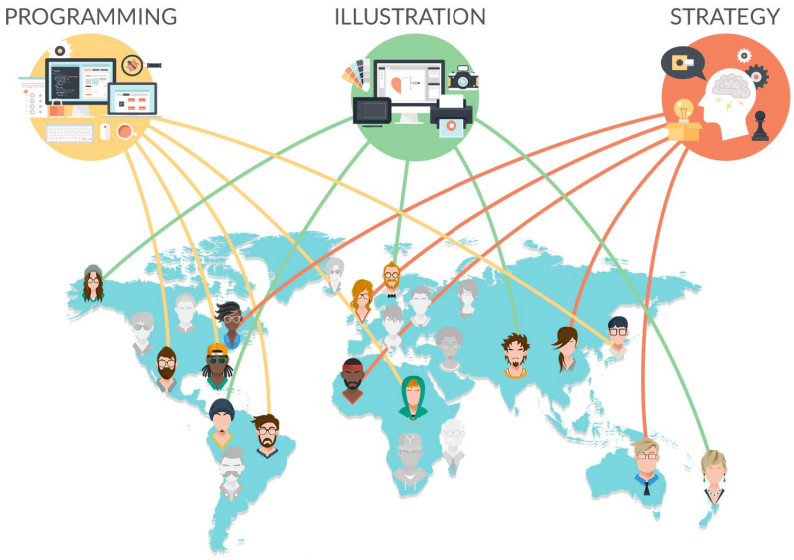


Abbildung 4.2: Colony-Vorgehensweise [1]

Das Unternehmen Peerism wiederum orientiert sich auf Kompetenzen und Fertigkeiten einzelner Personen, fügt diese so genannten Kompetenz-Tokens[99] hinzu und hat als Ziel, die Personen mit bezahlten Jobs zusammenzubringen. Die Beta-Version der Peerism-Lösung soll in der ersten Jahreshälfte 2018 vorgestellt werden. Sie basiert auf einem Ethereum-Smart-Contract [95]. Diese Lösung würde Business-Netzwerken wie LinkdIn oder Xing den Rang ablaufen.

Mit neuen Blockchain-Lösungen haben die Entwickler stets vor, bestehende Prozesse effizienter zu gestalten. Dank der rasanten Entwicklung der Technologie werden bereits existierende Blockchain-Projekte weiterentwickelt.

Ein Beispiel dafür ist Gridcoin [86], dessen Entwickler am größten Kritikpunkt des Bitcoin-Systems ansetzen, dem hohen Energieverbrauch. Die Entwickler nutzen ihre Kryptowährung für einen guten Zweck. Der Konsensalgorithmus von Gridcoin ist ursprünglich für die Unterstützung wissenschaftlicher Projekte aus

[99] Engl. Skill-Tokens.

dem BOINC[100]-Framework konzipiert worden. Der Algorithmus DPoR (Distributed Proof-of-Research) verbindet die Proof-of-BOINC (PoB) und Proof-of-Stake (POSv2) Algorithmen. PoB ist dem Proof-of-Work-Algorithmus ähnlich. Statt bloß einen Hash zu berechnen und damit große Mengen an Energie umsonst zu verbrauchen, wird die Rechenkapazität für wissenschaftliche Zwecke zur Verfügung gestellt. Die Miner werden im Rahmen des PoB Researchers genannt und setzen ihre Rechenkapazitäten (CPU, GPU, etc.) für das Lösen der Aufgaben aus BOINC-Projekten unterschiedlicher Bereiche (Physik, Mathematik, Medizin, etc.) ein.

Größte Hotspots der Blockchain-Startup-Szene sind im internationalen Vergleich die USA und Großbritannien, gefolgt von Kanada, den Niederlanden und China [122] (siehe Abbildung 4.3). Das US-Unternehmen Ripple zum Beispiel ist seit 2013 im Finanzbereich aktiv, bietet Banken einen Blockchain-basierten Echtzeit-Überweisungsservice und unterstützt unterschiedliche Fiat[101]- und Kryptowährungen (Dollar, Euro, Yen, Bitcoin etc.). Ein weiteres US-Startup aus dem Finanzbereich ist Chain, gegründet im Jahr 2014. Es bietet eine Blockchain-Plattform für Finanzdienstleistungen.

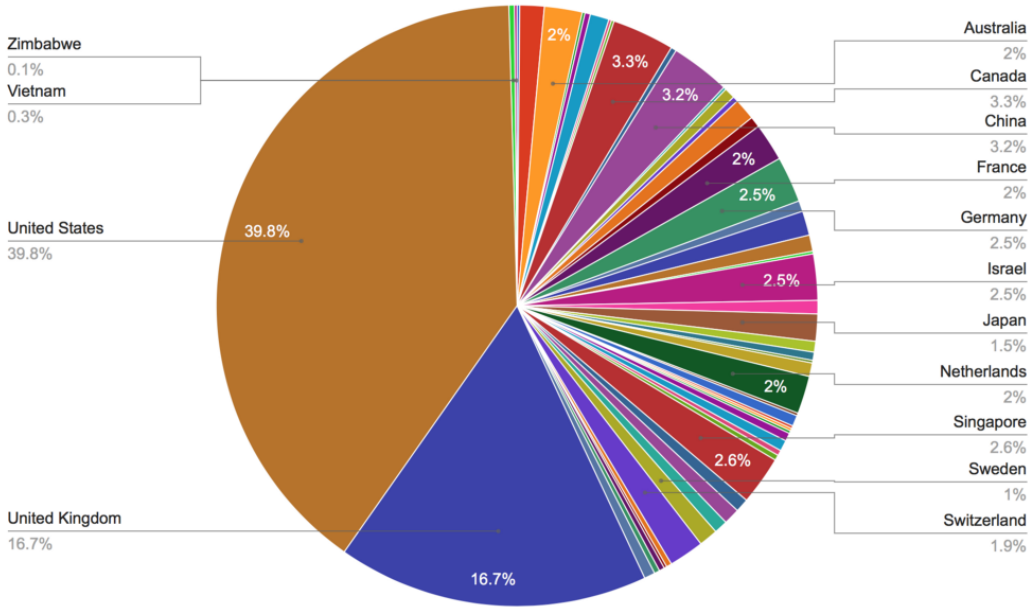


Abbildung 4.3: Aufteilung der Blockchain-Startups nach Ländern [49]

[100] BOINC (Berkeley Open Infrastructure for Network Computing) ist ein von der Universität Berkeley entwickeltes Opensource-Framework für verschiedene Distributed-Computing-Projekte [50].

[101] Fiatwährung oder Fiatgeld ist Geld, das durch keine Vermögenswerte gedeckt wird. Das Geld wird als Tauschmittel verwendet, hat aber keinen inneren Wert. Heutige Währungssysteme werden meist mit keinem Rohstoff gedeckt. Zum Beispiel wird von einer Zentralbank ausgestelltes Geld wie Euro oder Dollar als Fiat-Geld bezeichnet.

Ein bekanntes Startup, das in Großbritannien startete, ist Eris Industries (ab Oktober 2016 Monax Industries mit Hauptsitz in den USA). Eris stellt eine Plattform für das Entwickeln, Testen und Betreiben von Blockchain-basierten Applikationen zur Verfügung.

Die zahlreichen Anwendungen haben entweder eine eigene Blockchain als Grundlage oder nutzen bereits bestehende und weitverbreitete Blockchain-Ketten wie zum Beispiel von Bitcoin oder Ethereum.

Das Thema Blockchain wird nicht nur von einzelnen Unternehmen verfolgt, sondern mehrere Länder widmen sich dem Thema auf nationaler Ebene. In dem Bericht „Backing Australian FinTech" begrüßte Australiens Regierung 2016 eine Initiative der Australian Securities Exchange (ASX[102]), die Blockchain-Technologie für deren Clearing- und Abwicklungsprozesse einzuführen.

> „The Government welcomes the announcement by the ASX that it is exploring Blockchain technology for a new post-trade solution for the Australian equity market. While it is in the early stages of development, the technology has the potential to radically simplify the way our market operates end-to-end, with significant benefits to investors, participants, regulators and government agencies." [124]

Außerdem will die International Organization for Standardization (ISO) Australien bei der Entwicklung neuer internationaler Standards für die Blockchain-Technologie unterstützen. Australiens Finanzminister Scott Morrison sagte dazu: „Establishing standards around this emerging technology will provide a common language for industry, policy makers, regulators and technology developers. This will provide a basis for ensuring interoperability as this technology becomes more widely used." [131]

In Europa gehört Estland zu den Vorreitern und nennt sich verdient „e-Estonia". Bereits seit 1999 arbeitet das estnische Kabinett papierlos [56] (siehe Abbildung 4.4). Seit Entstehung der Technologie im Jahr 2008 experimentiert die estnische Regierung mit der Blockchain. Seit 2012 ist die Blockchain bereits in vielen Registern Estlands, so im Gesundheitswesen, im parlamentarischen Raum, in der Justiz und im Bereich der Sicherheits-Behörden, eingeführt. Estland nutzt eine eigene Blockchain namens KSI-Blockchain (siehe Anhang 6.6). Diese Technologie wird ebenfalls von der NATO, dem US-Verteidigungsministerium und den EU-Informationssystemen für Cyber-Sicherheit genutzt. [79]

„In fact, blockchain has the power to transform almost every aspect of our lives – improving democracy and providing greater opportunities – but it may only be possible to unleash this full potential with the support and co-operation of governments." So äußerte sich der Geschäftsführer des digitalen estnischen Registers e-Residency, Kaspar Korjus, in einem Artikel mit der Überschrift „Welcome to the blockchain nation". Darin erklärte er, wie die Regierung dazu beitragen kann, das volle Potenzial der Blockchain-Technologie auszuschöpfen [96].

In Deutschland wurde am 29. Juni 2017 ein Blockchain-Bundesverband mit Sitz in Berlin gegründet. Er hat mehr als 20 Arbeitsgruppen und veröffentlichte im

[102] ASX ist die australische Wertpapierbörse mit Sitz in Sydney.

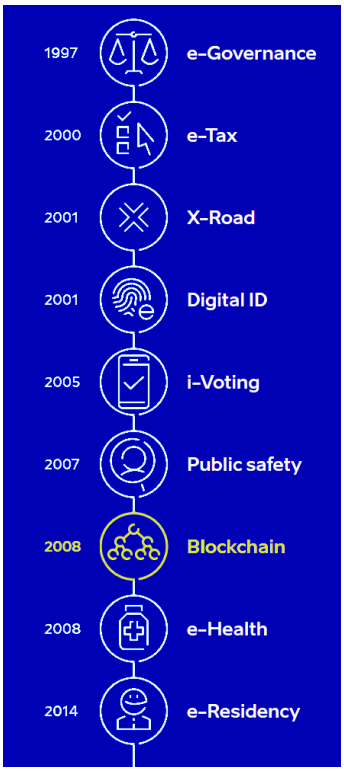


Abbildung 4.4: Estlands Digitalisierungsweg [79]

Oktober ein Positionspapier mit Handlungsempfehlungen, um Deutschland zu einem Global Player im weltweiten Blockchain-Ökosystem zu machen [72].

Interesse an der Technologie zeigt unter anderem auch Schweden. Die Regierung in Stockholm plant, ein Blockchain-basiertes Grundbuch einzuführen. In den Niederlanden nennt sich Arnhem bereits Bitcoin-Stadt; sie erlaubt in mehreren Läden, Cafés und Bars das Bezahlen mit Bitcoins.

Im Folgenden sollen diejenige Einsatzbereiche und Projekte detailliert erläutert werden, in denen die Blockchain-Technologie bereits am stärksten verbreitet ist.

4.1 Finanzwesen

Der allererste und immer bedeutendste Einsatzbereich der Blockchain-Technologie ist das Finanzwesen. Eine Vielzahl an Kryptowährungen ist seit der Bitcoin-Einführung entstanden, jedoch konnten sich nicht alle durchsetzen. Die am meisten bekannten und verbreiteten Kryptowährungen sind:

- Litecoin (2011, PoW),
- Namecoin (2011, PoW),
- Peercoin (2012, PoW und PoS),

- Primecoin (2013, PoW),
- XRP von Ripple (2013, RPCA[103]),
- Nxt (gegründet 2013, PoS),
- BlackCoin (2014, PoS).

Neben den Börsenunternehmen NASDAQ[104] in den USA und ASX[105] in Australien setzen bereits zahlreiche Finanzunternehmen auf die Blockchain-Technologie. Es sind mehrere so genannte Blockchain-Konsortien entstanden, deren Teilnehmer Finanzunternehmen sind. Das japanische Blockchain-Konsortium BCCC hat bereits über 100 Mitglieder [36]. Das Blockchain-Konsortium R3 mit dem Hauptsitz in New York zählt bereits über 70 Mitglieder. In Taiwan wird ebenfalls ein Konsortium gestartet, dieses wird von Microsoft unterstützt [47]. Zurzeit experimentiert eine Vielzahl von Banken (z. B. Deutsche Bank, Santander, UBS, Barclays Bank, usw.) mit der Technologie [46].

Der Großteil dieser Finanzdienstleistungs-Unternehmen interessiert sich wegen des Transaktionsaustauschs untereinander für den Einsatz der Blockchain-Technologie. Einige von ihnen setzen die Blockchain-Technologie aber auch in Lösungen ein, die sie ihren Kunden anbieten.

Blockchain-Lösungen im Finanzbereich sind vorwiegend Applikationen, die intelligente Verträge (Smart Contracts) einsetzen. Unternehmen wie Starbase und WeiFund betreiben ein Blockchain-basiertes Crowdfunding für Startups und Projekte. 2016 hat BNP Paribas Securities Services ein auf Blockchain-Technologie basierendes Pilotprojekt mit dem in Frankreich führenden Crowdfunding-Plattform-Anbieter SmartAngels gestartet [35].

Das Unternehmen Circle ermöglicht einen auf der Blockchain-Technologie basierenden P2P-Geldtransfer und bietet somit einen einfachen Weg an, Transaktionen in aktuellen Währungen (Fiatgeld) zu tätigen. Eine neue, auf der Blockchain-Technologie beruhende Clearing-Plattform für die OTC-Aktienmärkte (Märkte im außerbörslichen Handel) bietet das Unternehmen Clearmatics [39]. Finanzunternehmen offeriert das Startup Chain Blockchain-basierte Lösungen, die das Erstellen, Signieren und Validieren von Transaktionen in Millisekunden erlauben [38].

Eris vom Unternehmen Monax ist eine weitere Plattform, die die Entwicklung sowie das Betreiben von Blockchain-basierten Applikationen für Geschäftsökosysteme anbietet.

Zugleich entstehen rund um das Bitcoin-System zahlreiche Unternehmen und bieten Leistungen für den Handel und den Einsatz dieser Kryptowährung, z. B itBit und XAPO, an.

[103] Ripple Protocol Consensus Algorithm.
[104] NASDAQ - National Association of Securities Dealers Automated Quotations.
[105] ASX ist die australische Wertpapierbörse mit Sitz in Sydney.

4.2 Dezentrale Autonome Organisation

Wie bereits skizziert, sind durch die Blockchain-Technologie so genannte dezentrale autonome Organisationen (DAO) möglich. Das heißt: Die Organisation hat weder einen Geschäftsführer, noch eine andere zentrale Führungsinstanz oder einen Firmensitz, sondern besitzt stattdessen eine dezentrale Struktur mit automatisierter Entscheidungsfindung nach festgelegten Regeln. Diese werden durch Mehrheitsentscheidungen der involvierten Teilnehmer aufgestellt und stetig weiterentwickelt [41]. DAO wird durch eine Open-Source-Software realisiert (der Code ist frei einsehbar). Das Konsensprotokoll basiert auf einer Reihe von Regeln, die es erlauben, Einigkeit zwischen den Teilnehmern zu erreichen (z. B. im Fall der Verzweigung der Kette), Sicherheit gegen Attacken zu gewährleisten sowie die Blockchain zu betreiben und weiterzuentwickeln (neue Blöcke erzeugen, Software erweitern).

DAOs kaufen gemäß ihren Smart Contracts Produkte und Dienstleistungen bei dritten Parteien ein, den so genannten Contractors. Bezahlt wird in der Kryptowährung. Die Contractors produzieren in Anlehnung an die Spezifikation ihre Produkte und Dienstleistungen, die wiederum von der DAO benutzt oder vermarktet werden. Mit der Vermarktung dieser Produkte und Dienstleistungen verdient die DAO wiederum Geld, das re-investiert oder an ihre Anteilseigner aufgeteilt werden kann [9].

Die erste dezentrale autonome Organisation hieß „The DAO“ und hat nur weniger als ein Jahr existiert. Sie war durch einen Fehler im Code manipulierbar. Nach mehreren Software-Updates, die den Fehler und die Folgen des Angriffs beheben sollten, wurde „The DAO“ eingestellt.

4.3 Hyperledger

Hyperledger ist ein Open-Source-Konsortium, das im Dezember 2015 von der Linux Foundation gegründet wurde, um branchenübergreifende Blockchain-Anwendungen voranzubringen. Im Jahr 2017 zählte es ca. 170 Mitglieder. Es handelt sich um eine weltweite Zusammenarbeit führender Unternehmen aus den Bereichen Finanzen, Banken, Internet der Dinge, Lieferketten, Fertigung und Technologie mit über 400 Programmierern. Das Konsortium Hyperledger zählt zu den am schnellsten wachsenden Kooperationsprojekten der Linux Foundation. Hyperledger unterstützt mehrere Projekte in unterschiedlichen Einsatzbereichen, um Interoperabilität der zahlreichen Blockchain-Businesslösungen zu gewährleisten. Zurzeit stellt das Konsortium fünf Open Source Blockchain Frameworks[106] und vier Open Source Blockchain Tools mit Smart Contracts, Client-Bibliotheken, grafischen Schnittstellen und Beispielanwendungen zur Verfügung. Mithilfe dieser Frameworks und Tools können Unternehmen auf der Blockchain-Technologie basierende Applikationen und Services für Ihre Geschäftsfelder implementieren [90].

[106] Ein Framework ist noch kein fertiges Programm, sondern stellt nur den Rahmen zur Verfügung, innerhalb dessen der Programmierer eine Anwendung erstellt, wobei u.a. durch die in dem Framework verwendeten Entwurfsmuster auch die Struktur der individuellen Anwendung beeinflusst wird [108].

4.4 Cloud

In manchen Quellen wird die Blockchain-Technologie auch als verteilte Datenbank bezeichnet. Das spielt auf die Eigenschaft an, Daten verteilt auf mehreren Rechnern aufzubewahren. Da die Blockchain-Technologie eine zentrale Instanz für die Datenaufbewahrung und das Datenmanagement nicht braucht, hat jeder der vollständigen Nutzer die komplette und identische Kopie der Blockchain auf seinem Rechner. Die Manipulationssicherheit der darin enthaltenen Daten macht die Technologie für verteilte Cloud-Lösungen attraktiv. Es stellt sich dabei allerdings die Frage des Schutzes von Daten und Privatsphäre, da die Blockchain-Technologie für die Transparenz der Inhalte sorgt.

Das Unternehmen Storj bietet eine Lösung für dieses Problem. Storj ist ein Anbieter von P2P-Cloud-Speicher mit einer clientseitigen Verschlüsselung. Die Nutzer, die ihren Speicherplatz zur Verfügung stellen, werden Farmer genannt und werden dafür mit den Storj-Coins (Storj-eigene Kryptowährung) belohnt. Die aufzubewahrende Datei wird zuerst verschlüsselt und dann in mehrere Teile, so genannte Shards, zerlegt, bevor sie in der Storj-Cloud gespeichert wird. Zu jedem Shard wird ein Salt[107] hinzugefügt und daraus ein Hashwert erstellt. Dieser wird als Vor-Blatt (pre-leaf) in einem Merkle-Baum[108] bezeichnet. Anschließend werden aus Vor-Blättern (pre-leaves) erneut Hashwerte erstellt, die man Blätter (leaves) des Merkle-Baumes nennt. Aus den Blättern werden erst Zweige (branches) und dann eine „Wurzel“ des Merkle-Baumes (Merkle-Root) errechnet (siehe Abbildung 4.5).

Die „Wurzel“, die Salts und die „Tiefe des Merkle-Baumes“ werden bei dem Besitzer der zu versendenden Datei gespeichert. Die Blätter des Merkle-Baumes (leaves) werden zusammen mit den Shards dann an die Farmer gesendet. Der Besitzer der zu übersendenden Datei kann entscheiden, wie sie in Shards aufgeteilt wird und wo die Shards im Netzwerk gespeichert werden. Dabei sollen die Nutzer die Redundanz[109] beachten [144].

Microsoft Azure[110] bietet im Rahmen seines Blockchain-as-a-Service-Konzepts mehrere Blockchain-basierte Lösungen. IBM verfügt ebenfalls über einen Blockchain-Cloud-Service, dieser Service ist über die Blumix-Plattform verfügbar.

Acronis, ein Anbieter von Hybrid Cloud Data Protection- und Storage-Lösungen, setzt ebenfalls auf die Blockchain-Technologie. Am 20. Oktober 2016 kündigte das Unternehmen ein neues Produkt „Acronis Storage“ an. Die Lösung ist für heterogene Standardhardware konzipiert und umfasst Acronis CloudRAID und Acronis Notary mit Blockchain, um regelbare Redundanzen und sicheren Nachweis zu garantieren, dass gespeicherte Objekte nicht modifiziert wurden [26].

[107] Salt wird eine zufällig gewählte Zeichenfolge genannt, die an einen gegebenen Klartext vor der Verwendung einer Hashfunktion angehängt wird [112].
[108] Engl. Merkle-Tree.
[109] Es kann z. B. einfache Spiegelung oder „K-of-M Erasure Coding“ benutzt werden. Es ist geplant, in Zukunft „Reed-Solomon Erasure Coding“ einzusetzen [144].
[110] Sammlung integrierter Cloud-Dienste.

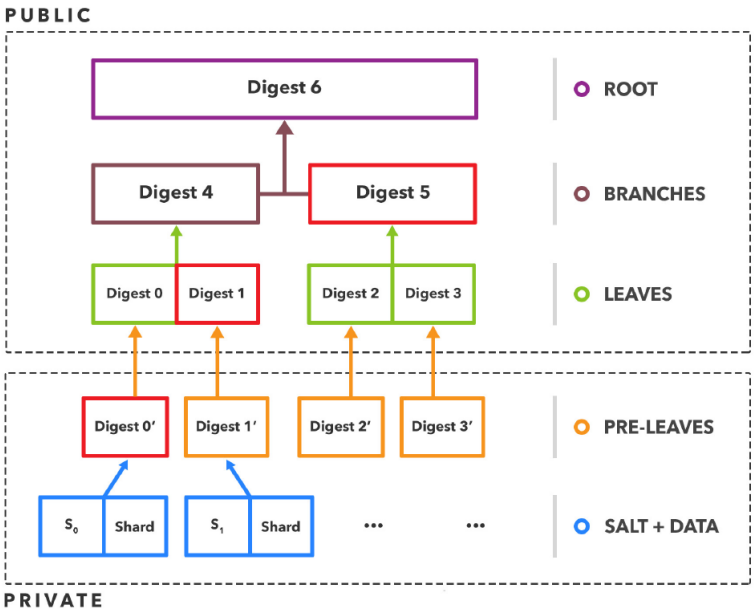


Abbildung 4.5: Storj Merkle-Tree [144]

4.5 Identitätsmanagement

Durch die stets wachsende Anzahl digitaler Dienste im Internet und die damit verbundene Menge an Anmeldedaten gewinnt das Management digitaler Identitäten permanent an Bedeutung. Dieses muss trotz Nutzerfreundlichkeit eine sichere Infrastruktur gewährleisten können. Digitale Identitäten können und sollen in der Zukunft sogar physische Ausweise ersetzen.

Die größten Schwächen des gegenwärtigen Identitätsmanagements sind folgende:

- Sicherheitsmängel,
- Für jeden Web-Dienst wird eine eigene digitale Identität benötigt. Es ist aber viel einfacher, unterschiedlichen Diensten partielle Berechtigungen für bestimmte Daten einer digitalen Identität zuzuweisen, als für jeden neuen Dienst eine neue Identität zu erstellen,
- Management der Passwörter.

Laut Zookos Dreieck[111] kann ein Namensraum[112] in einem Rechnernetz gleichzeitig nur zwei der folgenden drei Eigenschaften erfüllen:

- dezentralisiert – es gibt keine zentrale vertrauenswürdige Instanz, die die Namen verwaltet,
- sicher – Authentizität muss gewährleistet werden (möglich mit einem kryptographischen Schlüsselpaar),
- aussagekräftig - für Menschen lesbare Namen, die von Menschen ausgewählt werden können und nicht automatisch generierte, zufällige Zeichenfolgen [114].

Ein Großteil der aktuellen Namenssysteme unterstützt tatsächlich nur zwei der drei Eigenschaften. Das Blockchain-basierte Namecoin-System hingegen ist das erste Namenssystem, das alle drei Eigenschaften anbieten kann. Der ursprüngliche Anwendungsfall von Namecoin war ein Blockchain-basiertes Domain Name System. Bei Registrierung der Namen im Namecoin-System wird eine Zwei-Stufen-Bestätigungsmethode eingesetzt. Zuerst wird ein Hash des Namens angefragt und anschließend werden die Nutzerdaten registriert. Namecoin erlaubt eine Aktualisierung der Nutzerdaten [114].

2013 wurde das Projekt NameID ins Leben gerufen. Es verbindet die beiden Konzepte Namecoin und OpenID. Die Namecoin-Identität wird mit einem OpenID-Provider verknüpft. Die Nutzer, welche die Namecoin-Identität haben, können sich bei jeder Webseite, die den OpenID-Dienst unterstützt, ohne Problem mit gleichen Anmeldedaten anmelden.

Namecoin war außerdem die Grundlage für ein weiteres Blockchain-basiertes Identitätssystem: Blockstack ID. Dieses hatte den zweitgrößten Namensraum auf Namecoin. Nachdem die Gründer des Blockstack ID feststellten, dass ein einziger Mining-Pool über mehr als 51 Prozent der Rechenleistung des ganzen Namecoin-Systems verfügt, wurde Blockstack von Namecoin auf Bitcoin umgestellt.

Zurzeit ist das Blockstack-System die größte Applikation, die auf der Bitcoin-Blockchain aufgebaut ist (an der Zahl der Transaktionen gemessen) und nicht aus dem Finanzwesen kommt. Blockstack zählt bereits über 68.465 registrierte Identitäten aus allen Ländern der Welt.

Die Entwickler des Blockstack-Systems haben versucht, durch eine neue, komplexe Architektur Nachteile der Blockchain-Technologie zu umgehen wie begrenzte Kapazitäten für die Datenspeicherung, die Blockgröße und die geringe Geschwindigkeit, mit der Transkationen bestätigt werden, sowie die immer weiter wachsende Blockchain-Größe. Die Blockchain muss ja von jedem neuen Nutzer heruntergeladen und validiert werden, was bis zu drei Tage in Anspruch nehmen kann. Die

[111] Das Zookos Dreieck ist ein Trilemma dreier Eigenschaften, die für die Namensgebung in einem Netzwerk gewünscht sind.

[112] Der Begriff Namensraum kommt aus der Programmierung. In einem Namensraum wird jedes Objekt, z. B. eine Adresse oder ein anderer Wert, eindeutig mit einem Namen verknüpft. Ein Name kann in mehreren Namensräumen unterschiedlichen Objekten zugeordnet werden.

Blockstack-Architektur besteht deshalb aus vier Schichten (Layer). Die ersten beiden (Blockchain-Layer und Virtualchain-Layer) befinden sich in der Steuer-Ebene und die übrigen zwei (Routing-Layer und Speicher-Layer) in der Datenebene (siehe Abbildung 4.6).

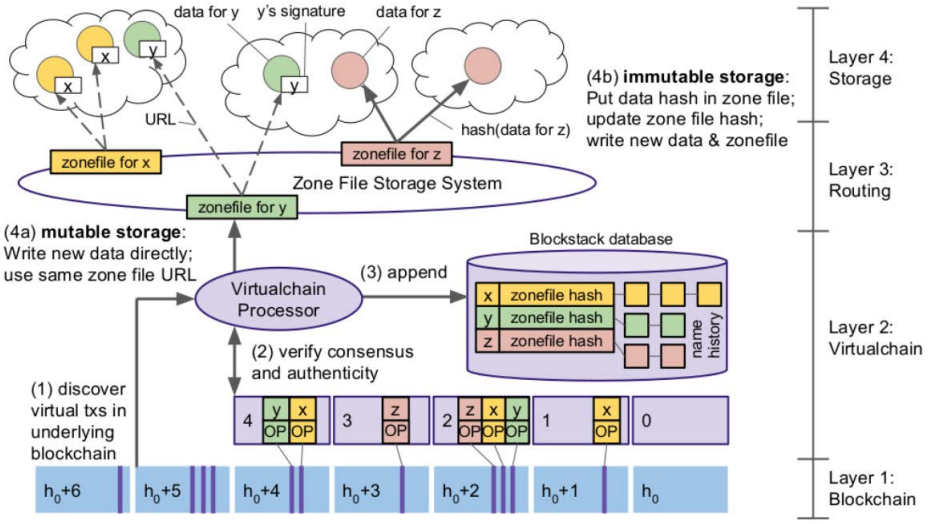


Abbildung 4.6: Architektur des Blockstack-Systems [114]

Die zugrunde liegende Blockchain wird als ein Kommunikationskanal für die Ankündigung von Zustandsänderungen eingesetzt (wenn die Nutzerdaten geändert werden). In der Steuer-Ebene werden die für Menschen lesbaren Namen registriert, die Name-Hash-Verbindungen sowie die Verbindungen zu den kryptographischen Schlüsselpaaren erstellt. Die Datenebene ist für die Datenspeicherung sowie Datenverfügbarkeit zuständig [114].

Blockstack bietet mehrere Optionen für das Identitätsmanagement. Eine von diesen ist Onename (gegründet im März 2014, ab 16. Mai 2016 Blockstack Inc.). Sie ist auf der Blockstack-Grundlage aufgebaut und bietet einen einfachen Service für die Registrierung und das Management digitaler Identitäten an. Die Identitäten werden Blockchain ID genannt. Im Mai 2015 wurden die Möglichkeiten der Blockchain ID erweitert.

Der Grundgedanke von Blockchain ID ist, eine digitale Form der Identitäts- und Zugangskontrolle anzubieten, die zunächst Passwörter und künftig dann physische Ausweise wie Pässe und Führerscheine sowie Haus- und Büro-Schlüssel ersetzen soll [24]. Blockchain IDs nutzen Blockchain Auth für ein dezentralisiertes Single-Sign-On-System, um die Passwörter und Drittanbieter aus dem Benutzerauthentifizierungsprozess herauszunehmen [21]. Die Blockchain-ID-Profile enthalten folgende Informationsfelder:

- Name – Nutzername,
- Bio – eine kurze Beschreibung des Nutzers,

- Location – Standort des Nutzers,
- Website – die Webseite des Nutzers,
- Bitcoin – Bitcoin-Adresse,
- Avatar – ein Foto des Nutzers,
- Cover – Hintergrundbild, das dem Profil persönliches Flair verleiht,
- PGP – Informationen zum öffentlichen PGP-Schlüssel des Nutzers,
- E-mail – E-Mail-Adresse des Nutzers,
- Twitter – Twitter-Account-Information,
- Facebook – Facebook-Account-Information,
- Github – Github-Account-Information [21].

Die Nutzer können ihre Blockchain ID auf ihren Webseiten oder Blogs einbetten oder auch als digitale Visitenkarten nutzen.

Laut Gartner Inc. können digitale Identitäten auf Basis der Blockchain-Technologie portabel und flexibel werden. Ziel eines erfolgreichen Identitätsmanagements ist es, nur einen Zugang für alle Services zu haben und dabei Sicherheit und Nutzerfreundlichkeit zu bewahren. Somit kann das lästige Anlegen von Benutzerkonten für jeden einzelnen Dienst wie zum Beispiel Facebook, Amazon, Spotify usw. entfallen [40].

Eine Blockchain-Anwendung von SAP namens TrueRec bietet eine Lösung für das Management hoheitlicher Dokumente, die Identitätsattribute einer realen Person nachweisen. Die Dokumente selbst werden nicht in der Blockchain gespeichert, sondern nur der digitale Fingerabdruck (Hash) der Daten wird in die Blockchain geschrieben. Wenn ein neues Dokument über TrueRec erstellt wird, erhält der Nutzer das Dokument als eine spezielle TRU-Datei, die er in seiner TrueRec-App ansehen und von dort aus mit anderen Institutionen oder Personen teilen kann. Die Gültigkeit der Dokumente kann mit der Blockchain sofort geprüft werden [100].

Eins der Projekte von Hyperledger namens Iroha stellt für mehrere Unternehmen die Möglichkeit des gemeinsamen Managements der KYC-Daten (Know Your Customer) vor [90].

4.6 Internet of Things

Trotz rasanter Entwicklung und Verbreitung hat das Internet der Dinge noch einige Herausforderungen zu bewältigen. Laut einer IoT-Studie von IBM sind das:

- hohe Kosten (hohe Infrastruktur- und Wartungskosten durch Cloud-Systeme, Server-Farmen und Service-Kosten der Zwischenhändler),
- Sicherheit (Sicherheitsmodelle müssen transparent und dürfen nicht verschleiert sein, deswegen ist Open Source die richtige Lösung),

- mangelnde Zukunftssicherheit (z. B. im Bereich Smart Home erwartet der Nutzer eine lange Lebensdauer der Geräte: Das intelligente Gerät soll über mehrere Jahre hinweg mit Updates versehen werden können und im Gegensatz zu einem Smartphone eher seltener getauscht werden),
- Mangel an Smartness (nicht genug sinnvolle Wertschöpfung, es reicht nicht, die Geräte zu vernetzen, ohne ihnen sinnvolle Funktionalität zu verleihen),
- Mangel an nachhaltigen und profitablen Geschäftsmodellen.

Hinzu kommt, dass die IoT-Systeme unterschiedliche Cloud-Infrastrukturen nutzen und es keine gemeinsame Plattform gibt, über die sich alle smarten Geräte verbinden, was eine flächendeckende P2P-Kommunikation erschwert [53].

Um die Herausforderungen zu meistern, muss jede dezentrale IoT-Lösung einen sicheren P2P-Datentransfer und eine robuste und skalierbare Form des Gerätemanagements unterstützen [138]. Der IBM-Studie zufolge liefert die Blockchain-Technologie eine elegante Lösung dafür (siehe Abbildung 4.7).

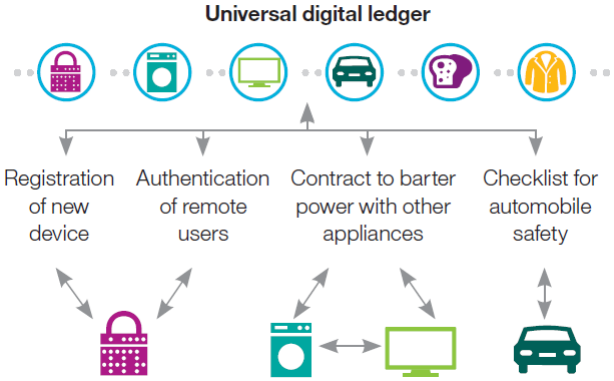


Abbildung 4.7: Blockchain-Technologie ermöglicht verschiedene Arten von IoT-Transaktionen zwischen den Geräten [138]

Blockchain-Lösungen für den IoT-Bereich bietet zum Beispiel bereits das deutsche Startup Slock.it an. Es nutzt Smart Contracts und setzt dafür die Ethereum-Blockchain ein. Das erste Produkt des Unternehmens war ein intelligentes Türschloss, das sich durch eine Smartphone-App öffnen lässt. Unternehmen wie Airbnb können in Zukunft von einer solchen Lösung profitieren. Zusammen mit Siemens und Canonical plant Slock.it einen Ethereum-Computer zu bauen, der als ein Smart Hub[113] funktioniert und mit dem man die smarten Geräte kontrollieren

[113] In der Datenkommunikation ist ein Hub ein Kopplungselement, an dem Daten aus einer oder mehreren Richtungen zusammentreffen und von dort in mehrere Richtungen weitergeleitet werden [25]. Ein Hub nimmt ein Datenpaket entgegen und sendet es an alle anderen Ports weiter [2].

kann [30]. In einem Projekt mit RWE namens Blockcharge wird sich das Startup um einfaches und sicheres Bezahlen für das Laden von Elektroautos kümmern. In der Zukunft sollen diese nach den Vorstellungen von Slock.it und RWE per Induktion an roten Ampeln aufgeladen werden können. Ähnlich soll es bei Drohnen an bestimmten Ladestationen sein [51]. Die Bezahlung läuft dabei automatisch.

Das Unternehmen Filament setzt ebenfalls die Blockchain-Technologie in IoT-Lösungen ein. Schwerpunkt sind die industriellen Anwendungen von IoT [45]. Dafür wird eigene sichere Hardware entwickelt, die erweiterte kryptographische Funktionen unterstützt und physisch geschützt ist. Dabei werden die kryptographischen Schlüssel auf den Geräten sicher verwaltet. Die Kommunikation verläuft komplett verschlüsselt. Dafür wird das Telehash-Protokoll verwendet [82]. Solche Filament-Lösungen können z. B. für die Optimierung der Wertschöpfungs- und Lieferkette eingesetzt werden (Abbildung 4.8).

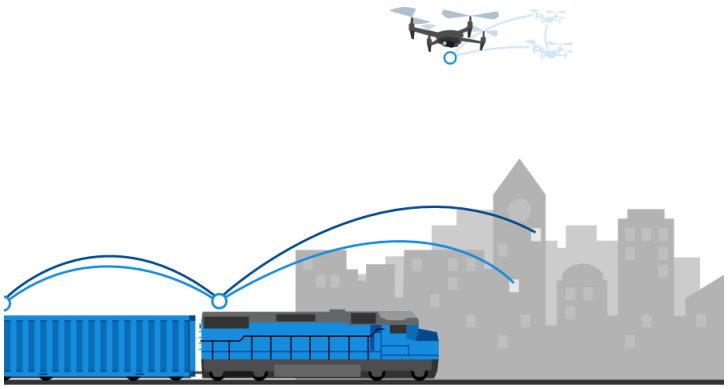


Abbildung 4.8: Filament – Optimierung der Wertschöpfungs- und Lieferkette

Die IBM-Lösung für diesen Anwendungsbereich heißt Watson IoT Platform und ermöglicht es, die von den IoT-Geräten gesendeten Daten in eine private Blockchain (Private Blockchain) zu übertragen, also die Daten an Blockchain-Token zu adressieren (siehe Abbildung 4.9) [92].

Trotz der Vorteile, welche die Blockchain-Technologie für das Internet der Dinge bietet, sind noch einige Herausforderungen zu bewältigen. Das sind z. B. die notwendige Rechenleistung für die Validierung der Transaktionen sowie die notwendige Speicherkapazität der Knoten. Diese und weitere Herausforderungen können durch unterschiedliche Konzepte gelöst werden (weitere Informationen bei [118]).

Nach einem Blockchain- und IoT-Summit im Dezember 2016 schlossen sich mehrere bekannte Großunternehmen und Blockchain-Startups zusammen[114]. Gemeinsam wollen sie die Grundlagen dafür legen, dass IoT-Anbietern Kernfunktionen

[114] Bosch, Cisco, Gemalto, Foxconn, Ambisafe, BitSE, Chronicled, ConsenSys, Distributed, Filament, Hashed Health, Ledger, Skuchain und Slock.it.

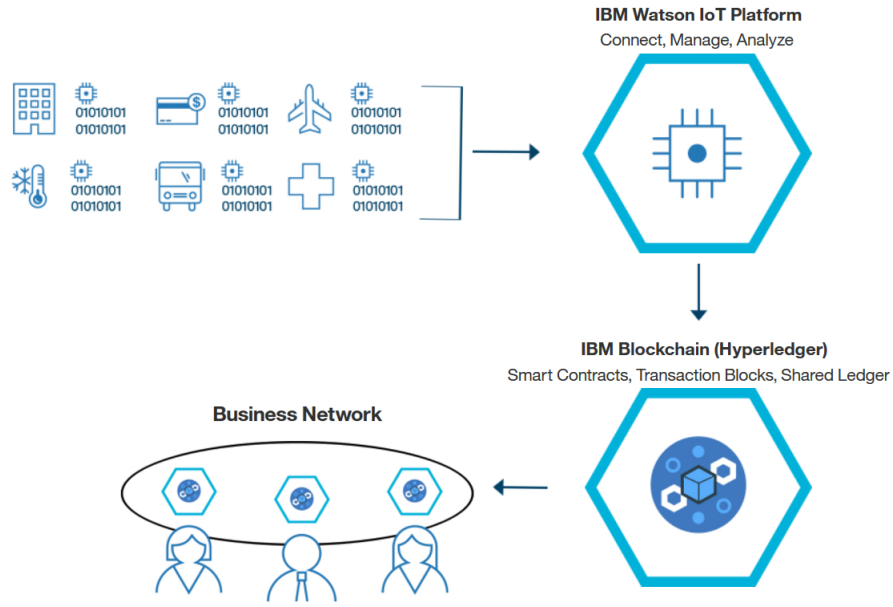


Abbildung 4.9: Watson IoT mit Blockchain [92]

zur Verfügung stehen, die sie mit unterschiedlichen Blockchains nutzen können [102].

Ein Konsortium namens „Chain of Things“ unterstützt die kollaborative Entwicklung von Open-Source-Standards für die Blockchain-Technologie im IoT-Bereich. Auf dieser Basis sind bereits drei Projekte entstanden:

- Chain of Security (sichere IoT-Anwendungen),
- Chain of Solar (ElectriCChain Solar Project: verbindet IoT- und Blockchain-Technologie für den Einsatz im Solar-Energie-Sektor),
- Chain of Shipping (IoT- und Blockchain-Technologie im Kontext von Handel, Schifffahrt und Transport).

4.7 Energie

Ein viel versprechender Anwendungsfall der Blockchain-Technologie ist der Energie-Sektor. Hier kann ein Blockchain-Wert z. B. mit einer Energie-Einheit gekoppelt werden.

In einem Projekt namens „Blockcharge“ haben der Energiekonzern RWE und das deutsche Blockchain-Startup Slock.it vor, das Aufladen von Elektroautos durch die Blockchain-Technologie zu modernisieren. Dadurch sollen die Besitzer der Elektroautos einfach per App für das Aufladen bezahlen können. Möglich wird dies mit Ethereum Smart Contracts. In Zukunft soll das Auto bereits über eine integrierte Kryptowährungs-Wallet (Geldbörse) verfügen und den Bezahlvorgang für das Aufladen automatisch mit der Ladestation organisieren [30].

Unternehmen aus dem Konsortium „Chain of Things“ haben 2016 das Projekt ElectriCChain ins Leben gerufen. Ziel des Projekts ist es, die gegenwärtig sieben Millionen Solaranlagen in der ganzen Welt zu verbinden und die Echtzeit-Daten an die Blockchain zu schicken. Das soll zum Beispiel Wissenschaftlern die Möglichkeit geben, die Solarstromerzeugungsdaten zu überblicken und zu analysieren. Im Rahmen des Projekts wird die Entwicklung offener Standards und Tools für das Schreiben und Lesen der Stromerzeugungsdaten in und durch die Blockchain unterstützt.

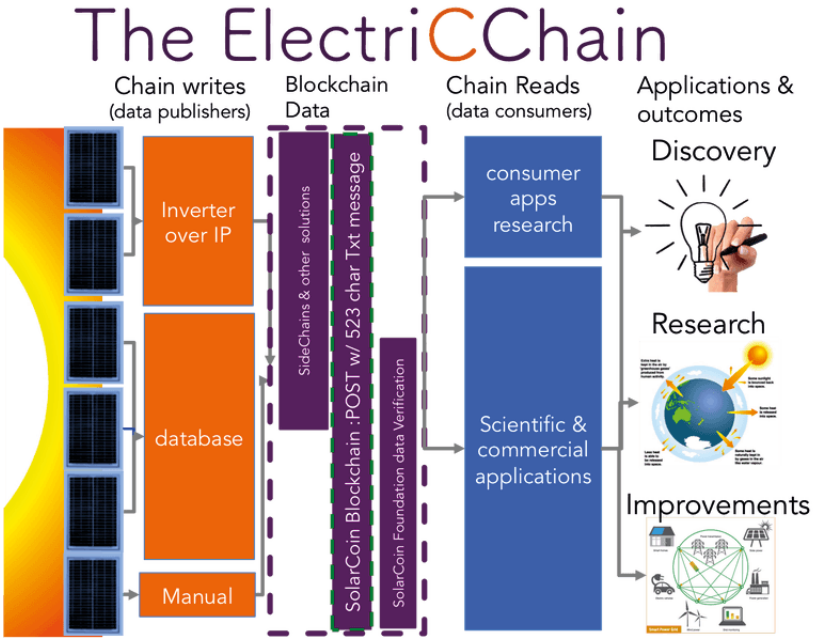


Abbildung 4.10: ElectriCChain-Projekt

Die Daten werden von Solarzellen an die Datenlogger übertragen. Dort werden diese geprüft und weiter an die Blockchain-Knoten der SolarCoin-Blockchain kommuniziert, wobei sie mit den SolarCoins verknüpft werden (Abbildung 4.11).

SolarCoin repräsentiert 1 MWh Solarstromerzeugung. Verifizierte Solarstromproduzenten können SolarCoins kostenlos erhalten. Dafür müssen sie eine passende Wallet auswählen (für Windows, Mac OS, usw.) und die Solaranlage registrieren.

Da lokale Erzeuger erneuerbarer Energie ebenfalls betroffen sind, sobald herkömmliche Netzwerke versagen [88], werden Microgrids[115] notwendig, um lokalen Energiehandel betreiben zu können. Ein Joint Venture[116] zwischen „LO3 Energy“

[115] Microgrid ist ein Stromnetz, das Stromerzeuger und Stromverbraucher in einem Netz oder Teilnetz vereinigt, welches autark betrieben werden kann [11].
[116] Als Joint-Venture wird ein Tochterunternehmen bezeichnet, das von zwei voneinander unabhängigen Unternehmen gegründet und geführt wird [6].

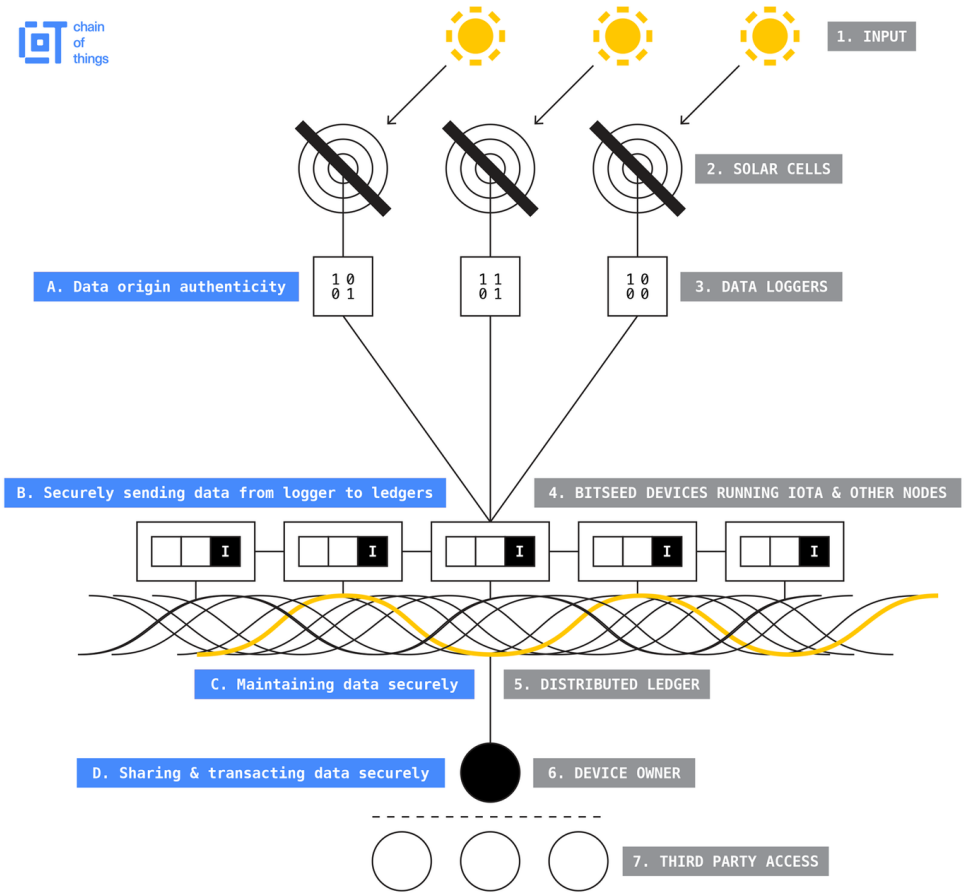


Abbildung 4.11: Chain of Things – ElectriCChain-Projekt – Umwandlung der Sonnenenergie in die Blockchain-Werte

und „Consensys“ namens „Transactive Grid“ hat es sich als Ziel gesetzt, ein Microgrid in Verbindung mit der Blockchain- und IoT-Technologie zu bringen und das System zunächst einmal für mehrere Haushalte im New Yorker Stadtteil Brooklyn aufzubauen. Dadurch werden überschüssig produzierte Stromerzeugnisse in der Blockchain registriert (Energieeinheit wird zu einem Blockchain-Wert) und zwischen den Nachbarn anhand von Smart Contracts gehandelt (Abbildung 4.12).

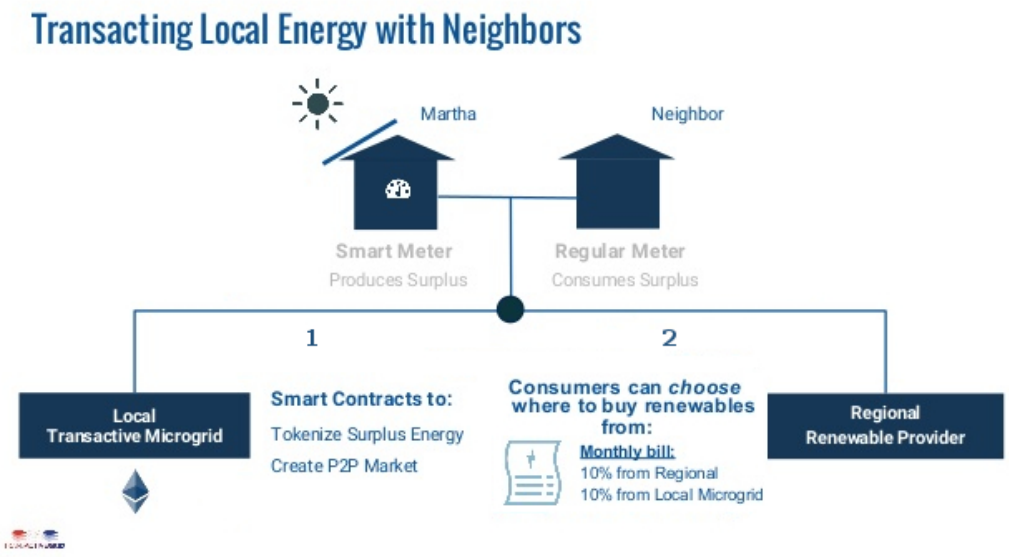


Abbildung 4.12: Transactive Grid

Das Brooklyn-Projekt hat Impulse für ein weiteres Projekt in Deutschland geliefert. Das Landau Microgrid Project (LAMP) ist ein Pilot- und Forschungsvorhaben des Karlsruher Instituts für Technologie (KIT) in Zusammenarbeit mit dem Energieversorger Energie Südwest AG und der Hard- und Softwarefirma LO3 Energy. Im Rahmen des Projekts wird ebenfalls die Blockchain-Technologie für einen lokalen Handel der Stromerzeugnisse eingesetzt. 20 Haushalten wird eine Blockchain-basierte Handelsplattform zur Verfügung gestellt. Auf dieser kann der lokal erzeugte „grüne“ Strom zwischen den Haushalten gehandelt werden. Über eine App erhalten die Teilnehmer Zugang zu ihren eigenen Stromverbrauchs- und -erzeugungsdaten und können ihre Preisvorstellungen für die lokal erzeugte Energie aus erneuerbaren Quellen angeben. [93]

4.8 Logistik

Die Logistik berührt mehrere Geschäftsfelder eines Unternehmens und erzeugt riesige Mengen an Informationen, die zwischen den in die Warenflüsse involvierten Parteien ausgetauscht werden. Ziel ist es, die Verfügbarkeit des richtigen Gutes

in der richtigen Menge im richtigen Zustand am richtigen Ort zur richtigen Zeit für den richtigen Kunden zu den richtigen Kosten zu gewährleisten [4]. Neben den physischen Aktivitäten sind auch die begleitenden Auftragsabwicklungs- und Geldflussprozesse wichtig.

Supply Chain Management baut integrierte Logistikketten (Material- und Informationsflüsse) über den gesamten Wertschöpfungsprozess auf und verwaltet sie, von der Rohstoffgewinnung bis hin zum Endverbraucher. Durch erfolgreiches Management und papierlosen Datenaustausch können die Beschaffungs-, Produktions- und Vertriebsplanungen auf den verschiedenen Stufen aufeinander abgestimmt werden. Die Unternehmen können mit Planänderungen unmittelbar auf Störungen reagieren [5].

Ins Supply Chain Management involvierte Teilnehmer haben unterschiedliche Zugangsberechtigungen zu den Informationen und Aufgaben. Heutzutage sind Supply Chains (Lieferkette) sehr komplex und umfassen viele Teilnehmer aus der ganzen Welt. Umso wichtiger ist es, Kosten, Effizienz und Qualität im Auge zu behalten.

Ein Blockchain-basiertes Supply Chain Management kann einem Unternehmen erhebliche betriebswirtschaftliche Vorteile bringen (Abbildung 4.13). Dabei sind folgende Merkmale der Blockchain-Technologie von großer Bedeutung:

- Ein kryptographischer Nachweis ersetzt Vertrauen – ein einfaches Zugangsberechtigungs- und Benutzermanagement wird möglich.
- Durch eine sichere Protokollierung der Daten sowie die Transparenz der Inhalte sind Ausfallsicherheit, Fälschungssicherheit und Nachverfolgbarkeit der Daten garantiert.
- Ein dezentrales Teilnehmernetzwerk, Smart Contracts sowie Oracles können viele Zwischenhändler ablösen. Beim Passieren bestimmter Zielorte der Supply Chain können die in den Smart Contracts hinterlegten Konditionen geprüft und nach Notwendigkeit weitere Aufgaben/Funktionen aktiviert werden (z. B.: Wenn alle Konditionen erfüllt sind, soll die Dienstleistung bezahlt werden).

In Verbindung mit der IoT-Technologie gibt es mehrere Anwendungsmöglichkeiten in der Logistik. Besonders sensible Güter können etwa mit IoT-Geräten ausgestattet werden, die über notwendige Sensoren verfügen und gesammelte Informationen weiter an die Blockchain senden. Das Unternehmen Modum.io bietet eine Lösung für die Nachverfolgbarkeit von Informationen über den Lagerungszustand (Temperatur, Feuchtigkeit) von Medikamenten während der gesamten Lieferkette (Supply Chain).

IBM und Maersk[117] entwickeln ihrerseits eine auf dem Hyperledger Framework „Fabric“ basierende Lösung für die Schifffahrts- und Logistikindustrie. Diese ermöglicht einen Austausch von Ereignissen und Dokumenten in Echtzeit entlang der ganzen Supply Chain mit Hilfe einer digitalen Infrastruktur. Durch eine klare

[117] Die weltweit größte Containerschiff-Reederei.

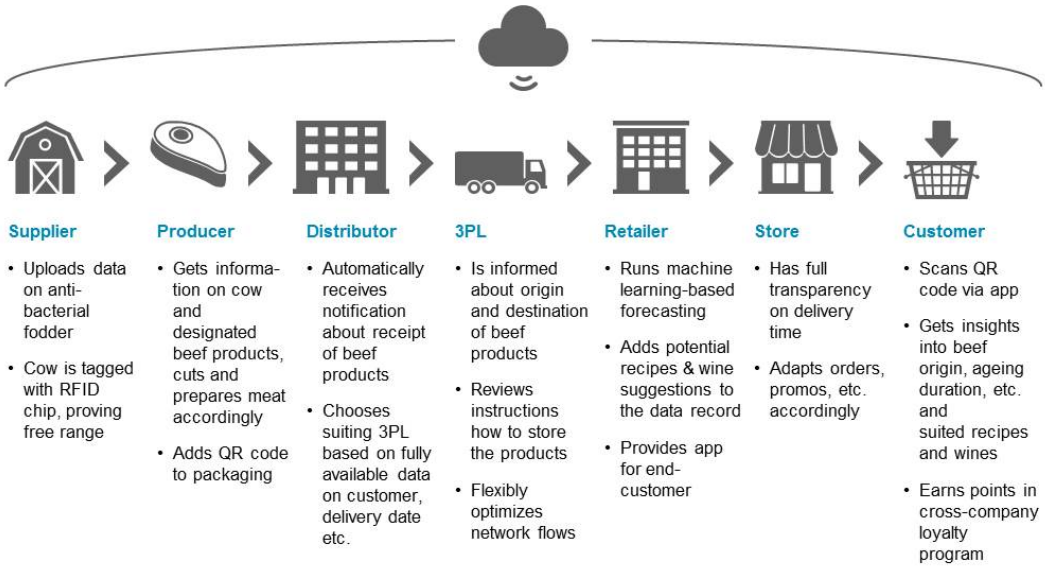


Abbildung 4.13: End-To-End Blockchain-basiertes Supply-Chain [10]

Übersicht über alle einbezogenen Prozesse sowie einen sicheren Zugriff auf bestimmte Daten für bestimmte Nutzer wird ein nachhaltiger Transport gefördert [91].

Foxconn, einer der weltweit größten Hersteller von Elektronik- und Computerteilen, plant zusammen mit dem chinesischen Online-Kreditgeber Dianrong eine Blockchain-basierte Supply-Chain-Finanzplattform. Das Projekt wird sich zunächst auf die Automobil-, Elektronik- und Bekleidungsindustrie konzentrieren. Dadurch sollen die Zahlungen und Transaktionen in der Supply Chain transparenter, überschaubar und einfacher authentifiziert werden. Mithilfe der Blockchain-Technologie soll die Effizienz in der gesamten Supply Chain erhöht sowie durch Einsparung von Drittanbietern Kosten gesenkt werden. Die gesamte Supply Chain und nicht nur ihrer Finanzflüsse sollen auf Basis der Blockchain-Technologie abgewickelt werden. Wenn alle Transaktionen der Supply Chain einfacher zu valideren sein werden, soll die Effizienz des gesamten Ökosystems zunehmen [101].

5 Ängste und Risiken oder Erfolg und Effizienzsteigerung?

Einer neuen Technologie, die gleichzeitig hohe Erträge, Kosteneinsparungen und Effizienzsteigerung verspricht, ist immer mit einer gewissen Vorsicht zu begegnen. Der von vielen Akteuren um die Blockchain-Technologie gelegte Mantel eines Hypes lässt sie als eine Allzweckwaffe erscheinen, die jedoch nur ausgewählten Unternehmensgiganten mit ihren Innovation Labs zugänglich ist.

Sieht man von dem Hype einmal ab, steht eine zwar noch nicht ausgereifte aber aufsteigende Technologie vor Augen, die mit einer richtigen Einsatz- und Implementierungs-Strategie tatsächlich Geschäftsprozesse schlanker und effizienter gestalten kann. Wie bei jeder Innovation geht man dabei Risiken ein, da es an Standards und Interoperabilität zwischen den Systemen noch mangelt.

Die Innovation der Blockchain-Technologie liegt in ihrer erfolgreichen Zusammensetzung bereits vorhandener Ansätze: dezentrale Netzwerke, Kryptographie, Konsensfindungsmodelle. Durch das innovative Konzept wird ein Werte-Austausch in einem dezentralen System möglich. Dabei wird kein Vertrauen zwischen dessen Knoten (z. B. Nutzer) vorausgesetzt. Die Intelligenz liegt bei den Knoten und nicht bei einer zentralen Instanz. Die Werte werden unveränderbar und unwiderruflich in die Blockchain-Historie aufgenommen. Diese ist transparent und erlaubt den Nachweis, wann ein Wert bei wem in Besitz war. Dabei ist ein Werte-Austausch mit komplexen Wenn-Dann-Bedingungen möglich (Smart Contracts).

Ein dezentrales und sicheres System, bei dem verschiedene Subsysteme miteinander interagieren (z. B. Identitätsmanagement, Internet der Dinge, Cloud-Speicher) kann durch die Blockchain-Technologie gewährleistet werden. Nur mit einer Blockchain-Wallet einkaufen zu gehen, das Türschloss im Büro oder zu Hause zu öffnen, sich für eine Abstimmung anzumelden und an einer Wahl teilzunehmen, dem Arzt bestimmte Informationen der persönlichen Krankenakte zur Verfügung zu stellen oder das Auto ohne physischen Schlüssel zu öffnen und zu starten – das sind Anwendungsfälle, die durch den Einsatz einer einheitlichen Technologie, welche sichere P2P-Kommunikation unterstützt, bald möglich sein werden.

Interessierten Unternehmen stehen viele Umsetzungsmöglichkeiten zur Verfügung. In den vergangenen drei Jahren sind zahlreiche Konsortien und Projekte entstanden, die „Blockchain-as-a-Service“ anbieten und andere Unternehmen beim Entwickeln, Testen und Bereitstellen von Anwendungen unterstützen. Zahlreiche Einsatzgebiete sind bereits von der Blockchain-Technologie erobert und immer mehr Unternehmen bieten fertige, für spezielle Bereiche angepasste Lösungen an.

Jedes Unternehmen, das auf den Blockchain-Zug aufspringen möchte, sollte sich intensiv mit dem Kosten-Nutzen-Verhältnis auseinandersetzen, bevor es sich für die Implementierung entscheidet. Das Ziel, welches man durch den Einsatz der Technologie erreichen möchte, muss gleich am Anfang klar definiert werden.

Dabei sind die Möglichkeiten und Grenzen der Blockchain-Technologie im Auge zu behalten.

Bitcoin-, Ethereum- und Hyperledger-Frameworks haben sich in der Blockchain-Szene gewissermaßen als Standards behauptet und dienen gegenwärtig als Grundlage für viele weitere Anwendungen. Bitcoin gilt dabei immer noch als stärkstes und sicherstes Blockchain-System. Trotzt der hohen Volatilität der Kryptowährung und sinkender Miner-Belohnung wächst das System rasant. Es wird vor allem wegen seiner Nutzung bei anonymen Geschäften sowie für seinen hohen Verbrauch an Elektrizität stark kritisiert. Um die Kosten des hohen Energieverbrauchs weiterhin decken zu können, müssen die Transaktionsgebühren entsprechend erhöht werden, damit es sich für die Miner weiterhin lohnt tätig zu sein.

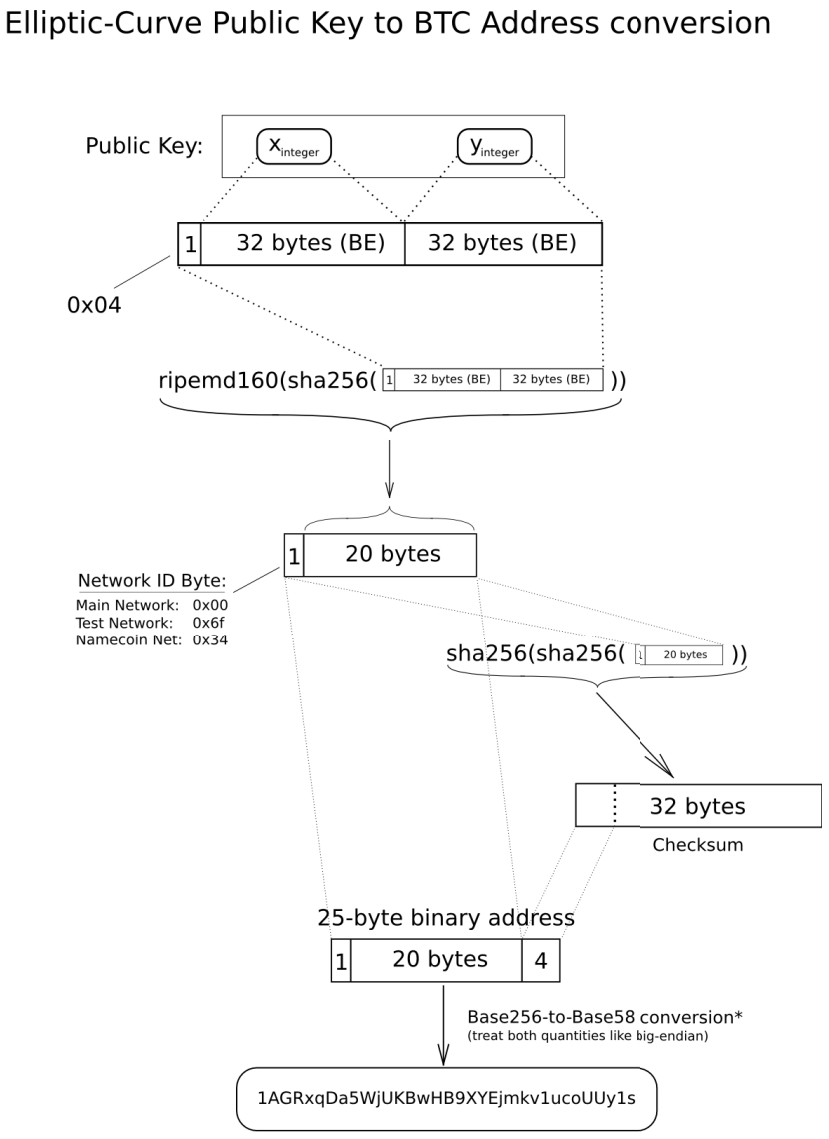
Neue Blockchains laufen Gefahr, geringere Sicherheit zu bieten, da Änderungen an der bereits bestehenden Technologie zu Schutzlücken und Mängeln führen können. Ausgenutzt werden können diese zum Beispiel bei den so genannten 51 Prozent-Attacken, bei denen ein Miner oder ein Miningpool über mehr als die Hälfte der gesamten Rechenkapazität (Hashrate) im Netzwerk verfügt und somit neue Blöcke erstellen und diese manipulieren kann. Wie eine Schwachstelle im Code ausgenutzt werden kann, zeigt zudem die Attacke auf das dezentrale autonome Netzwerk „The DAO“, das mittlerweile nicht mehr existiert.

Große Unternehmen sowie Startups schließen sich seit einiger Zeit zu Gemeinschaften zusammen, um für die Verbesserung der Blockchain-Technologie und die Weiterentwicklung der Standards zu sorgen. Durch diese Unterstützung sowie Bemühungen auf nationaler Ebene besteht die Chance, dass die Blockchain kein Hype bleibt, sondern eine übergreifende und nachhaltige Technologie wird.

6 Anhang

6.1 Conversion from ECDSA public key to bitcoin address

Bildquelle [62].



*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'

6.2 Automatically use TOR Hidden Services

Quelle: `https://bitcoin.org/en/release/v0.12.0`

Starting with Tor version 0.2.7.1 it is possible, through Tor's control socket API, to create and destroy 'ephemeral' hidden services programmatically. Bitcoin Core has been updated to make use of this. This means that if Tor is running (and proper authorization is available), Bitcoin Core automatically creates a hidden service to listen on, without manual configuration. Bitcoin Core will also use Tor automatically to connect to other .onion nodes if the control socket can be successfully opened. This will positively affect the number of available .onion nodes and their usage.

This new feature is enabled by default if Bitcoin Core is listening, and a connection to Tor can be made. It can be configured with the `-listenonion`, `-torcontrol` and `-torpassword` settings. To show verbose debugging information, pass `-debug=tor`.

6.3 Verifizieren der Transaktion im Bitcoin-System

Quelle: [13]

1. Check syntactic correctness.
2. Make sure neither in or out lists are empty.
3. Size in bytes $<$ MAX_BLOCK_SIZE.
4. Each output value, as well as the total, must be in legal money range.
5. Make sure none of the inputs have hash $= 0$, $n = -1$ (coinbase transactions).
6. Check that nLockTime $<= INT\_MAX$, size in bytes $>= 100$, and sig opcount $<= 2$.
7. Reject 'nonstandard' transactions: scriptSig doing anything other than pushing numbers on the stack, or scriptPubkey not matching the two usual forms.
8. Reject if we already have matching tx in the pool, or in a block in the main branch.
9. For each input, if the referenced output exists in any other tx in the pool, reject this transaction.
10. For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions, if a matching transaction is not in there already.
11. For each input, if the referenced output transaction is coinbase (i.e. only 1 input, with hash $= 0$, $n = -1$), it must have at least COINBASE_MATURITY (100) confirmations; else reject this transaction.

12. For each input, if the referenced output does not exist (e.g. never existed or has already been spent), reject this transaction.
13. Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in legal money range.
14. Reject if the sum of input values $<$ sum of output values.
15. Reject if transaction fee (defined as sum of input values minus sum of output values) would be too low to get into an empty block.
16. Verify the scriptPubKey accepts for each input; reject if any are bad.
17. Add to transaction pool.
18. Add to wallet if mine.
19. Relay transaction to peers.
20. For each orphan transaction that uses this one as one of its inputs, run all these steps (including this one) recursively on that orphan.

6.4 The Byzantine Generals Problem

Quelle: Leslie Lamport, Robert Shostak and Marshall Pease - The Byzantine Generals Problem, July 1982

We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general. The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have an algorithm to guarantee that

1. all loyal generals decide upon the same plan of action. The loyal generals will all do what the algorithm says they should, but the traitors may do anything they wish. The algorithm must guarantee condition A regardless of what the traitors do. The loyal generals should not only reach agreement, but should agree upon a reasonable plan. We therefore also want to insure that
2. a small number of traitors cannot cause the loyal generals to adopt a bad plan.

6.5 Atomic cross-chain trading

Quelle: [14]

A and B are two Nodes, that hold Units (coins) on different blockchains.

A picks a random number x

A creates TX1: "Pay w BTC to <B's public key> if (x for H(x) known and signed by B) or (signed by A & B)"
A creates TX2: "Pay w BTC from TX1 to <A's public key>, locked 48 hours in the future"
A sends TX2 to B
B signs TX2 and returns to A

1. A submits TX1 to the network

   B creates TX3: "Pay v alt-coins to <A-public-key> if (x for H(x) known and signed by A) or (signed by A & B)"

   B creates TX4: "Pay v alt-coins from TX3 to <B's public key>, locked 24 hours in the future"

   B sends TX4 to A

   A signs TX4 and sends back to B

2. B submits TX3 to the network

3. A spends TX3 giving x

4. B spends TX1 using x

This is atomic (with timeout). If the process is halted, it can be reversed no matter when it is stopped.
Before 1: Nothing public has been broadcast, so nothing happens
Between 1 & 2: A can use refund transaction after 48 hours to get his money back
Between 2 & 3: B can get refund after 24 hours. A has 24 more hours to get his refund
After 3: Transaction is completed by 2

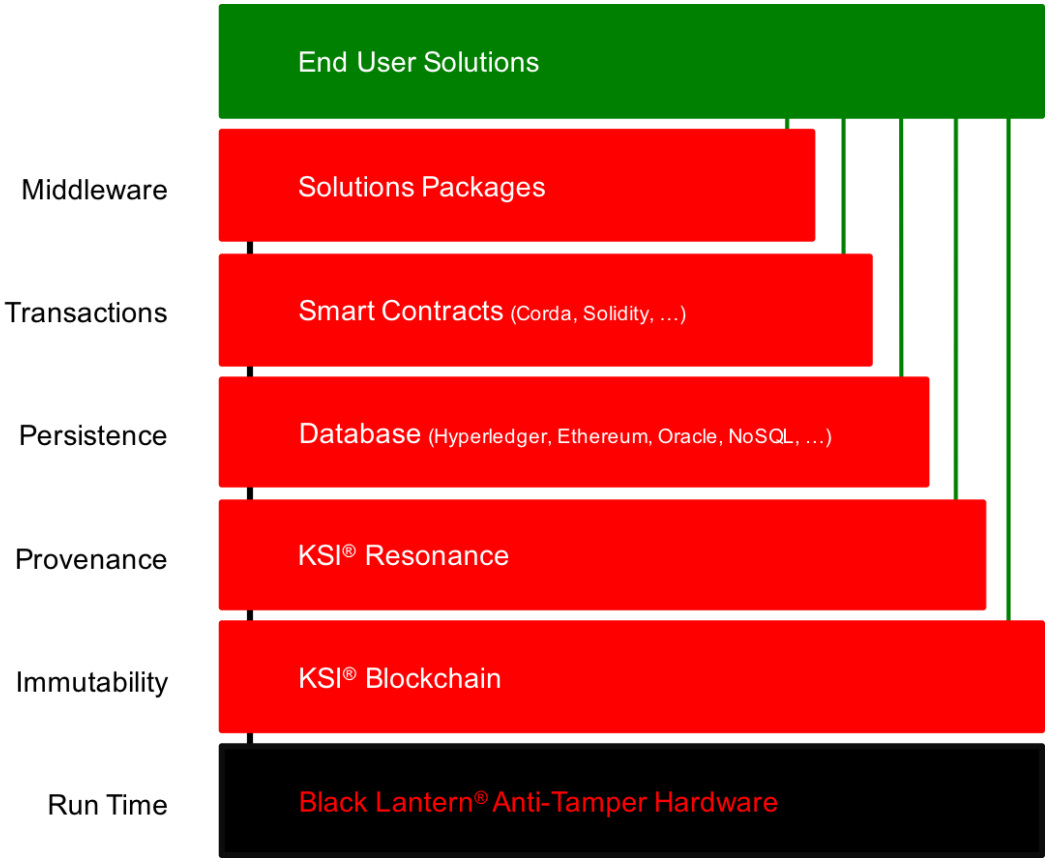
- A must spend his new coin within 24 hours or B can claim the refund and keep his coins

- B must spend his new coin within 48 hours or A can claim the refund and keep his coins

For safety, both should complete the process with lots of time until the deadlines.

6.6 Technologie Stack von Guardtime

Guardtime's KSI® Technology Stack [87]



Literatur

[1] Colony-Picture. https://wallscover.com/images/colony-7.jpg. Besucht am 11.10.2017.

[2] Elektronik Kompendium – Hub. https://www.elektronik-kompendium.de/sites/net/1405161.htm. Besucht am 23.10.2017.

[3] Gabler Wirtschaftslexikon – Kryptowährung. http://wirtschaftslexikon.gabler.de/Definition/kryptowaehrung.html. Besucht am 08.11.2017.

[4] Gabler Wirtschaftslexikon – Logistik. http://wirtschaftslexikon.gabler.de/Definition/logistik.html. Besucht am 08.11.2017.

[5] Gabler Wirtschaftslexikon – Supply Chain Management (SCM). http://wirtschaftslexikon.gabler.de/Definition/supply-chain-management-scm.html. Besucht am 08.11.2017.

[6] Gründer Szene Lexikon – Joint-Venture. https://www.gruenderszene.de/lexikon/begriffe/joint-venture. Besucht am 09.11.2017.

[7] JuraForum – Analogieverbot. https://www.juraforum.de/lexikon/analogieverbot. Besucht am 12.09.2017.

[8] Kryptografie.de. http://kryptografie.de/kryptografie/index.htm. Besucht am 15.06.2017.

[9] LEADVISE Reply – DAO – Dezentrale Autonome Organisationen. http://www.leadvise.de/latest-thinking/blockchain/dao-dezentrale-autonome-organisationen/. Besucht am 20.10.2017.

[10] Oliver Wyman – Blockchain: The Backbone Of Digital Supply Chains. http://www.oliverwyman.com/our-expertise/insights/2017/jun/blockchain-the-backbone-of-digital-supply-chains.html. Besucht am 08.11.2017.

[11] Zhaw – Was ist der Unterschied zwischen Microgrids und Smart Grids? https://www.zhaw.ch/de/lsfm/institute-zentren/iunr/ecological-engineering/erneuerbare-energien/microgrids/unterscheidung/. Besucht am 06.11.2017.

[12] Bitcoin Wiki – Hauptseite. https://de.bitcoin.it/wiki/Hauptseite, 2011. Besucht am 13.04.2016.

[13] Bitcoin Wiki – Protocol rules. https://en.bitcoin.it/wiki/Protocol_rules, 2011. Besucht am 21.06.2016.

[14] Bitcointalk.org. https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949, 2013. Besucht am 02.12.2016.

[15] ITWissen.info – Peer-to-Peer-Netz. http://www.itwissen.info/Peer-to-Peer-Netz-peer-to-peer-network-P2P.html, 2014. Besucht am 06.09.2017.

[16] Bitcoin Magazin – Ripple Discontinues Smart Contract Platform Codius, Citing Small Market. https://bitcoinmagazine.com/articles/ripple-discontinues-smart-contract-platform-codius-citing-small-market-1435182153, 2015. Besucht am 23.12.2016.

[17] BitcoinBlog.de – Ein Startup, Sybils Angriff und die Privatsphäre. https://bitcoinblog.de/2015/03/19/ein-startup-sybils-angriff-und-die-privatsphare/, 2015. Besucht am 06.10.2017.

[18] CoinDesk – How Bitcoin's Technology Could Reshape Our Medical Experiences. http://www.coindesk.com/bitcoin-technology-could-reshape-medical-experiences/, 2015. Besucht am 17.11.2016.

[19] Coinwelt – Hardware-Wallet Trezor. http://coinwelt.de/wp-content/uploads/2015/09/trezor_transparent.png, 2015. Besucht am 14.04.2017.

[20] Ethereum Blog – On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, 2015. Besucht am 22.10.2017.

[21] Github.com – blockstack. https://github.com/blockstack/blockchain-id/wiki, 2015. Besucht am 15.01.2017.

[22] Learn me a bitcoin – Difficulty. http://learnmeabitcoin.com/guide/difficulty, 2015. Besucht am 12.07.2017.

[23] Ledgerwallet – Hardware-Wallet Ledger. https://www.ledgerwallet.com/images/products/lwn/ledger-nano-solo-large.png, 2015. Besucht am 14.04.2017.

[24] Onename.com – Introducing a Blockchain-based Digital Identity. http://blog.onename.com/blockchain-id/, 2015. Besucht am 15.01.2017.

[25] TechTarget – Hub. http://www.searchnetworking.de/definition/Hub, 2015. Besucht am 23.10.2017.

[26] Acronis – Acronis integriert Acronis Notary mit Blockchain und CloudRAID in seine Software-Defined Storage Lösung Acronis Storage. https://www.acronis.com/de-de/pr/2016/10/20-09-39.html, 2016. Besucht am 17.10.2017.

[27] Bird&Bird – Blockchain 2.0, smart contracts and challenges. https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges, 2016. Besucht am 28.10.2017.

[28] Bitcoin Wiki – Address. https://en.bitcoin.it/wiki/Address, 2016. Besucht am 18.04.2017.

[29] Bitcoin Wiki – Lightning Network. https://en.bitcoin.it/wiki/Lightning_Network, 2016. Besucht am 24.02.2017.

[30] BitcoinBlog.de – RWE und slock.it wollen Ethereum für Elektroautos nutzen. https://bitcoinblog.de/2016/02/26/rwe-und-slock-it-wollen-ethereum-fuer-elektroautos-nutzen/, 2016. Besucht am 03.01.2017.

[31] Bitcoinj – What is bitcoinj? https://bitcoinj.github.io/, 2016. Besucht am 14.12.2016.

[32] Bitcoinpaperwallet – Paper-Wallet. https://bitcoinpaperwallet.com/images/front-back-sample-big.jpg, 2016. Besucht am 14.04.2017.

[33] Blockchain.info – Hashwert. https://blockchain.info/de/charts/hash-rate, 2016. Besucht am 11.08.2016.

[34] Blockgeeks – Smart Contracts: The Blockchain Technology That Will Replace Lawyers. https://blockgeeks.com/guides/smart-contracts/, 2016. Besucht am 26.10.2017.

[35] Brave Newcoin – BNP Paribas and SmartAngels blockchain pilot targets Europe's growing crowdfunding sector. https://bravenewcoin.com/news/bnp-paribas-and-smartangels-blockchain-pilot-targets-europes-growing-crowdfunding-sector/, 2016. Besucht am 20.12.2016.

[36] BTC-ECHO – Ein auf Blockchain ausgerichtetes Consortium in Japan berichtet jetzt von einer wachsenden Mitgliederzahl von über 100 Unternehmen. https://www.btc-echo.de/japanisches-blockchain-consortium-zaehlt-nun-ueber-100-mitglieder/, 2016. Besucht am 19.12.2016.

[37] BTC-ECHO – So viel Geld benötigst du für eine Bitcoin 51 Prozent Attacke. https://www.btc-echo.de/so-viel-geld-benoetigst-du-fuer-eine-bitcoin-51-attacke/, 2016. Besucht am 20.12.2016.

[38] Chain Core. https://chain.com/technology/, 2016. Besucht am 20.12.2016.

[39] Clearmatics. http://www.clearmatics.com/, 2016. Besucht am 20.12.2016.

[40] Computerwoche – Identitäten verwalten mit Blockchain. https://www.computerwoche.de/a/identitaeten-verwalten-mit-blockchain,3316591, 2016. Besucht am 01.11.2017.

[41] Datarella – Eine Dezentrale Autonome Organisation DAO – Was ist das? http://datarella.de/dezentrale-autonome-organisation-dao-was-ist-das/, 2016. Besucht am 20.10.2017.

[42] Ethereum Homestead Documentation – Contracts. http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html, 2016. Besucht am 30.10.2017.

[43] Gartner – The CIO's Guide to Blockchain. https://www.gartner.com/smarterwithgartner/the-cios-guide-to-blockchain/, 2016. Besucht am 11.10.2017.

[44] Hochschule Niederrhein, Fachbereich Elektrotechnik und Informatik – Verteilte Algorithmen. https://lionel.kr.hs-niederrhein.de/~rethmann/shs06/shs05.pdf, 2016. Besucht am 12.07.2017.

[45] International Business Times – Filament evolving entire IoT space using Bitcoin blockchain. http://www.ibtimes.co.uk/filament-evolving-entire-iot-space-underwhelming-use-blockchain-1579096, 2016. Besucht am 03.01.2017.

[46] Let's Talk Payments – Know more about Blockchain: Overview, Technology, Application Areas and Use Cases. https://letstalkpayments.com/an-overview-of-blockchain-technology/, 2016. Besucht am 20.12.2016.

[47] Microsoft News – Microsoft and AMIS announce Asia's first blockchain consortium. https://news.microsoft.com/apac/2016/12/12/microsoft-and-amis-announce-asias-first-blockchain-consortium/, 2016. Besucht am 19.12.2016.

[48] Nasdaq – Colu Announces Colored Coins and Lightning Network Integration. http://www.nasdaq.com/article/colu-announces-colored-coins-and-lightning-network-integration-cm710111, 2016. Besucht am 23.10.2017.

[49] Outlier Ventures – 5 Things We Learned From Analysing the Location of 950+ Blockchain Startups. https://medium.com/outlier-ventures-io/5-things-we-learned-from-analysing-the-location-of-950-blockchain-startups-96daa788560c#.78ofyxve8, 2016. Besucht am 21.11.2016.

[50] Rechenkraft.net – BOINC. https://www.rechenkraft.net/wiki/BOINC, 2016. Besucht am 21.11.2016.

[51] Slock.it – Solutions. https://slock.it/solutions.html, 2016. Besucht am 03.01.2017.

[52] StackExchange. http://ethereum.stackexchange.com/questions/3336/what-is-the-difference-between-a-smart-contract-and-a-dao/4240, 2016. Besucht am 21.12.2016.

[53] TechCrunch – Decentralizing IoT networks through blockchain. https://techcrunch.com/2016/06/28/decentralizing-iot-networks-through-blockchain/, 2016. Besucht am 04.01.2017.

[54] 3sat – Bitcoin, der Wert der digitalen Währung schwankt extrem. http://www.3sat.de/page/?source=/nano/glossar/bitcoin.html, 2017. Besucht am 14.09.2017.

[55] Academic library – Full vs. Simplified Payment Verification. https://academlib.com/7951/education/full_simplified_payment_verification, 2017. Besucht am 12.10.2017.

[56] Adobe Blog – Wie Estland zum Digital Government-Vorreiter in Europa wurde. https://blogs.adobe.com/digitaleurope/de/governmental-

affairs/wie-estland-zum-digital-government-vorreiter-in-europa-wurde/, 2017. Besucht am 14.10.2017.

[57] Agrello. https://www.agrello.org/how-it-works, 2017. Besucht am 12.09.2017.

[58] Altcointoday – Ethereum Lightning Network Moves into Test Phase. http://www.altcointoday.com/ethereum-lightning-network-moves-into-test-phase/, 2017. Besucht am 12.10.2017.

[59] Bitcoin – Schützen Sie ihre Privatsphäre. https://bitcoin.org/de/schuetzen-sie-ihre-privatsphaere, 2017. Besucht am 17.04.2017.

[60] Bitcoin – Sichern Sie Ihre Wallet. https://bitcoin.org/de/sichern-sie-ihre-wallet, 2017. Besucht am 10.10.2017.

[61] Bitcoin Wiki – Common Vulnerabilities and Exposures. https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures, 2017. Besucht am 17.09.2017.

[62] Bitcoin Wiki – Elliptic-Curve Public Key to BTC Address conversion. https://en.bitcoin.it/w/images/en/9/9b/PubKeyToAddr.png, 2017. Besucht am 11.05.2016.

[63] Bitcoin Wiki – Hardware wallet. https://en.bitcoin.it/wiki/Hardware_wallet, 2017. Besucht am 11.10.2017.

[64] Bitcoin Wiki – Mining. https://en.bitcoin.it/wiki/Mining, 2017. Besucht am 15.09.2017.

[65] Bitcoin Wiki – Multisignature. https://en.bitcoin.it/wiki/Multisignature, 2017. Besucht am 18.04.2017.

[66] Bitcoin Wiki – Setting up a Tor hidden service. https://en.bitcoin.it/wiki/Setting_up_a_Tor_hidden_service, 2017. Besucht am 10.09.2017.

[67] Bitcoin Wiki – Weaknesses. https://en.bitcoin.it/wiki/Weaknesses, 2017. Besucht am 15.09.2017.

[68] BitcoinBlog.de – Adressen bei Kryptowährungen: eine Einführung. https://bitcoinblog.de/2017/06/12/adressen-bei-kryptowaehrungen-eine-einfuehrung/, 2017. Besucht am 17.04.2017.

[69] Blockchain.info – Mining Pools. https://blockchain.info/de/pools?timespan=4days, 2017. Besucht am 01.12.2017.

[70] Blockgeeks – Blockchain Glossary: From A-Z. https://blockgeeks.com/guides/blockchain-glossary-from-a-z/, 2017. Besucht am 26.10.2017.

[71] Brave Newcoin – Ethereum scaling solution, Plasma, could facilitate "billions of transactions per second". https://bravenewcoin.com/news/ethereum-scaling-solution-plasma-could-facilitate-billions-of-transactions-per-second/, 2017. Besucht am 14.10.2017.

[72] Bundesblock – Blockchain Bundesverband. http://bundesblock.de/2017/10/17/bundesverband-veroeffentlicht-positionspapier/, 2017. Besucht am 25.10.2017.

[73] ClearKarma. http://www.clearkarma.com/, 2017. Besucht am 09.09.2017.

[74] CoinDesk – Bitcoin's Lightning Network Moves Closer to Compatibility. https://www.coindesk.com/bitcoins-lightning-network-moves-closer-compatibility-standard/, 2017. Besucht am 21.10.2017.

[75] Colony. https://colony.io/, 2017. Besucht am 11.10.2017.

[76] CryptoCompare – What is merged mining – Bitcoin & Namecoin – Litecoin & Dogecoin? https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/, 2017. Besucht am 24.10.2017.

[77] Dapps for beginners – Introduction to development on Ethereum. https://dappsforbeginners.wordpress.com/tutorials/introduction-to-development-on-ethereum/, 2017. Besucht am 11.10.2017.

[78] Deloitte – Die Blockchain aus Sicht des Datenschutzrechts. https://www2.deloitte.com/dl/de/pages/legal/articles/blockchain-datenschutzrecht.html, 2017. Besucht am 12.09.2017.

[79] E-Estonia. https://e-estonia.com/, 2017. Besucht am 14.10.2017.

[80] Ethcore Blog – The Multi-sig Hack: A Postmortem. https://blog.ethcore.io/the-multi-sig-hack-a-postmortem/, 2017. Besucht am 11.10.2017.

[81] Ethereum White Paper – A Next-Generation Smart Contract and Decentralized Application Platform. https://github.com/ethereum/wiki/wiki/White-Paper, 2017. Besucht am 28.10.2017.

[82] Filament – Security Overview. https://filament.com/assets/downloads/Filament%20Security.pdf, 2017. Besucht am 14.10.2017.

[83] Gartner – Top 10 Mistakes in Enterprise Blockchain Projects. https://www.gartner.com/smarterwithgartner/top-10-mistakes-in-enterprise-blockchain-projects/, 2017. Besucht am 11.10.2017.

[84] Gem – Health. https://gem.co/health/, 2017. Besucht am 11.10.2017.

[85] Github – Colored Coins Protocol Specification. https://github.com/Colored-Coins/Colored-Coins-Protocol-Specification/wiki/Introduction, 2017. Besucht am 23.10.2017.

[86] Gridcoin. http://gridcoin.us/, 2017. Besucht am 23.06.2017.

[87] Guardtime – Our Technology. https://guardtime.com/technology, 2017. Besucht am 14.10.2017.

[88] Handelsblatt – Strom aus der Nachbarschaft. http://www.handelsblatt.com/technik/energie-umwelt/circular-economy/transactive-grid-

mikronetzwerk-fuer-zehn-haeuserblocks/14793648-2.html, 2017. Besucht am 06.11.2017.

[89] Heise Security – Sicherheit der Verschlüsselung. https://m.heise.de/security/artikel/Kryptographie-in-der-IT-Empfehlungen-zu-Verschluesselung-und-Verfahren-3221002.html?artikelseite=all, 2017. Besucht am 17.09.2017.

[90] Hyperledger – Frameworks. https://www.hyperledger.org/, 2017. Besucht am 31.10.2017.

[91] IBM – Maersk and IBM Unveil First Industry-Wide Cross-Border Supply Chain Solution on Blockchain. http://www-03.ibm.com/press/us/en/pressrelease/51712.wss, 2017. Besucht am 09.11.2017.

[92] IBM – Watson Internet of Things. http://www.ibm.com/internet-of-things/iot-news/announcements/private-blockchain/, 2017. Besucht am 04.01.2017.

[93] Landau Microgrid Project. https://im.iism.kit.edu/1093_2058.php, 2017. Besucht am 06.11.2017.

[94] Medium – Exploring Simpler Ethereum Multisig Contracts. https://medium.com/@ChrisLundkvist/exploring-simpler-ethereum-multisig-contracts-b71020c19037, 2017. Besucht am 11.10.2017.

[95] Medium – Introducing Peerism: the Skill Token Economy for Post-Capitalism. https://medium.com/peerism/introducing-peerism-the-skill-token-economy-for-post-capitalism-6d3a8a893ccc, 2017. Besucht am 14.10.2017.

[96] Medium – Welcome to the blockchain nation. https://medium.com/e-residency-blog/welcome-to-the-blockchain-nation-5d9b46c06fd4, 2017. Besucht am 14.10.2017.

[97] Modum.io. https://modum.io/, 2017. Besucht am 09.09.2017.

[98] Oraclize.it – Ethereum Proof of Identity. http://dapps.oraclize.it/proof-of-identity/, 2017. Besucht am 14.10.2017.

[99] Publicism – Could Blockchain Technology help free press? https://medium.com/publicism/could-blockchain-technology-help-photographers-free-press-129a7fec4f9, 2017. Besucht am 11.10.2017.

[100] SAP – Die SAP stellt TrueRec vor: Basierend auf der Blockchain-Technologie lassen sich mit der Lösung zuverlässig digitale Zeugnisse und Zertifikate verwalten. https://news.sap.com/germany/truerec-blockchain/?source=email-de-newscenter-newsletter-20170920&lf1=2531622534d194024351450e79609376, 2017. Besucht am 01.11.2017.

[101] SCF Briefing – Foxconn uses blockchain for new SCF platform after 6,5 million dollar pilot. http://www.scfbriefing.com/foxconn-launches-scf-blockchain-platform/, 2017. Besucht am 10.11.2017.

[102] Silicon – Neue Initiative will IoT mit Blockchain sicherer machen. http://www.silicon.de/41639843/neue-initiative-will-iot-mit-blockchain-sicherer-machen/?inf_by=59799667671db810758b4634, 2017. Besucht am 15.10.2017.

[103] Stackoverflow – Where do smart contracts reside in blockchain (Ethereum or Hyperledger). https://stackoverflow.com/questions/42081194/where-do-smart-contracts-reside-in-blockchain-ethereum-or-hyperledger, 2017. Besucht am 31.10.2017.

[104] Statista – Inwiefern ist Ihnen Blockchain ein Begriff? https://de.statista.com/statistik/daten/studie/683611/umfrage/umfrage-zur-bekanntheit-der-blockchain-technologie-im-mittelstand-in-deutschland/, 2017. Besucht am 09.01.2018.

[105] The Cointelegraph – Lightning Network Will Come to Bitcoin "From Tomorrow": Reports. https://cointelegraph.com/news/lightning-network-will-come-to-bitcoin-from-tomorrow-reports, 2017. Besucht am 14.10.2017.

[106] Tor Project – Tor: Hidden Service Protocol. https://www.torproject.org/docs/hidden-services.html.en, 2017. Besucht am 11.09.2017.

[107] Wikipedia – Blockchain. https://en.wikipedia.org/wiki/Blockchain, 2017. Besucht am 22.10.2017.

[108] Wikipedia – Framework. https://de.wikipedia.org/wiki/Framework, 2017. Besucht am 31.10.2017.

[109] Wikipedia – Ghash.io. https://en.wikipedia.org/wiki/Ghash.io, 2017. Besucht am 20.09.2016.

[110] Wikipedia – Nonce. https://de.wikipedia.org/wiki/Nonce, 2017. Besucht am 13.09.2016.

[111] Wikipedia – Paxos (Informatik). https://de.wikipedia.org/wiki/Paxos_(Informatik), 2017. Besucht am 19.12.2016.

[112] Wikipedia – Salt (Kryptologie). https://de.wikipedia.org/wiki/Salt_(Kryptologie), 2017. Besucht am 04.01.2017.

[113] Wikipedia – Token, Rechnernetz. https://de.wikipedia.org/wiki/Token_(Rechnernetz), 2017. Besucht am 31.10.2017.

[114] Muneeb Ali, Jude Nelson, Ryan Shea, and Michael J. Freedman. Blockstack: A global naming and storage system secured by blockchains. In *2016 USENIX Annual Technical Conference (USENIX ATC 16)*, pages 181–194. USENIX Association, 2016.

[115] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter

Wuille. Enabling blockchain innovations with pegged sidechains. *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, 2014.

[116] Martijn Bastiaan. Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin. In *Availab le at http://referaat. cs. utwente. nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-of-two-phase-proof-of-work-in-bitcoin. pdf, year=2015*.

[117] Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in Bitcoin P2P network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, pages=15–29, year=2014, organization=ACM*.

[118] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

[119] Bernd Eylert and Dorothee Eylert. Ausgewählte Verschlüsselungsverfahren. In *Sicherheit in der Informationstechnik, pages=67–83, year=2012, organization=News & Media*.

[120] Bernd Eylert and Janett Mohnke. Signaturverfahren. In *Sicherheit in der Informationstechnik, pages=84–90, year=2012, organization=News & Media, Berlin*.

[121] Pedro Franco. *Understanding Bitcoin: Cryptography, engineering and economics*. John Wiley & Sons, 2014.

[122] Maximilian Friedlmaier, Andranik Tumasjan, and Isabell M Welpe. Disrupting Industries With Blockchain: The Industry, Venture Capital Funding, and Regional Distribution of Blockchain Ventures. 2016.

[123] Tatiana Gayvoronskaya and Bernd Eylert. Smartcard-Einsatz für sicheren, personaliesierten Dateitransfer im Automotive Bereich. In *Wildau, TH, Masterarbeit, A2013/0201, pages=109, year=2012, organization=Wildau, TH*.

[124] The Australian Government. Backing Australian FinTech, 2016.

[125] BitFury Group. Proof of Stake versus Proof of Work. In *White Paper, Sep 13, 2015 (Version 1.0), pages=1–26, year=2015, organization=BitFury Group*.

[126] BitFury Group. Digital Assets on Public Blockchains. *White paper*, 2016.

[127] Sunny King and Scott Nadal. PPCoin: Peer-to-Peer Kryptowährung mit Proof-of-Stake. *peercoin.net*, 2012.

[128] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[129] Sergio Demian Lerner. Rootstock – Bitcoin powered Smart Contracts. *theblockchain.com*, 2015.

[130] David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.

[131] Scott Morrison. Australia leading international blockchain standards. `http://sjm.ministers.treasury.gov.au/media-release/097-2016/`, 2016. Besucht am 23.11.2016.

[132] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[133] Giuseppe Pappalardo, Tiziana Di Matteo, Guido Caldarelli, and Tomaso Aste. Blockchain Inefficiency in the Bitcoin Peers Network. *arXiv preprint arXiv:1704.01414*, 2017.

[134] Paulina Pesch and Rainer Böhme. Datenschutz trotz öffentlicher Blockchain? *Datenschutz und Datensicherheit-DuD*, 41(2):93–98, 2017.

[135] Joseph Poon and Vitalik Buterin. Plasma: Scalable Autonomous Smart Contracts. *White paper*, 2017.

[136] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2015.

[137] Pavel Prihodko, Slava Zhigulin, Mykola Sahno, Aleksei Ostrovskiy, and Olaoluwa Osuntokun. Flare: An Approach to Routing in Lightning Network. *bitfury.com*, 2016.

[138] Veena Pureswaran and Paul Brody. Device democracy: Saving the future of the Internet of Things. *IBM Corporation*, 2015.

[139] Hans P. Reiser and Rüdiger Kapitza. Verteilte Algorithmen. In *Verteilte Algorithmen, pages=1–16, year=2003, organization=Universität Erlangen-Nürnberg*.

[140] Meni Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[141] David Schwartz, Noah Youngs, and Arthur Britto. The Ripple protocol consensus algorithm. *Ripple Labs Inc White Paper*, 5, 2014.

[142] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[143] David M. Toth. *The Byzantine Agreement Protocol Applied to Security*. PhD thesis, WORCESTER POLYTECHNIC INSTITUTE, 2004.

[144] Shawn Wilkinson, Tome Boshevski, Josh Brandoff, and Vitalik Buterin. Storj a peer-to-peer cloud storage network. 2014.

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren / Redaktion
112	978-3-86956-391-6	**Automatic verification of behavior preservation at the transformation level for relational model transformation**	Johannes Dyck, Holger Giese, Leen Lambers
111	978-3-86956-390-9	**Proceedings of the 10th Ph.D. retreat of the HPI research school on service-oriented systems engineering**	Christoph Meinel, Hasso Plattner, Mathias Weske, Andreas Polze, Robert Hirschfeld, Felix Naumann, Holger Giese, Patrick Baudisch, Tobias Friedrich, Emmanuel Müller
110	978-3-86956-387-9	**Transmorphic : mapping direct manipulation to source code transformations**	Robin Schreiber, Robert Krahn, Daniel H. H. Ingalls, Robert Hirschfeld
109	978-3-86956-386-2	**Software-Fehlerinjektion**	Lena Feinbube, Daniel Richter, Sebastian Gerstenberg, Patrick Siegler, Angelo Haller, Andreas Polze
108	978-3-86956-377-0	**Improving Hosted Continuous Integration Services**	Christopher Weyand, Jonas Chromik, Lennard Wolf, Steffen Kötte, Konstantin Haase, Tim Felgentreff, Jens Lincke, Robert Hirschfeld
107	978-3-86956-373-2	**Extending a dynamic programming language and runtime environment with access control**	Philipp Tessenow, Tim Felgentreff, Gilad Bracha, Robert Hirschfeld
106	978-3-86956-372-5	**On the Operationalization of Graph Queries with Generalized Discrimination Networks**	Thomas Beyhl, Dominique Blouin, Holger Giese, Leen Lambers
105	978-3-86956-360-2	**Proceedings of the Third HPI Cloud Symposium "Operating the Cloud" 2015**	Estee van der Walt, Jan Lindemann, Max Plauth, David Bartok (Hrsg.)
104	978-3-86956-355-8	**Tracing Algorithmic Primitives in RSqueak/VM**	Lars Wassermann, Tim Felgentreff, Tobias Pape, Carl Friedrich Bolz, Robert Hirschfeld
103	978-3-86956-348-0	**Babelsberg/RML : executable semantics and language testing with RML**	Tim Felgentreff, Robert Hirschfeld, Todd Millstein, Alan Borning
102	978-3-86956-347-3	**Proceedings of the Master Seminar on Event Processing Systems for Business Process Management Systems**	Anne Baumgraß, Andreas Meyer, Mathias Weske (Hrsg.)

ISBN 978-3-86956-394-7
ISSN 1613-5652