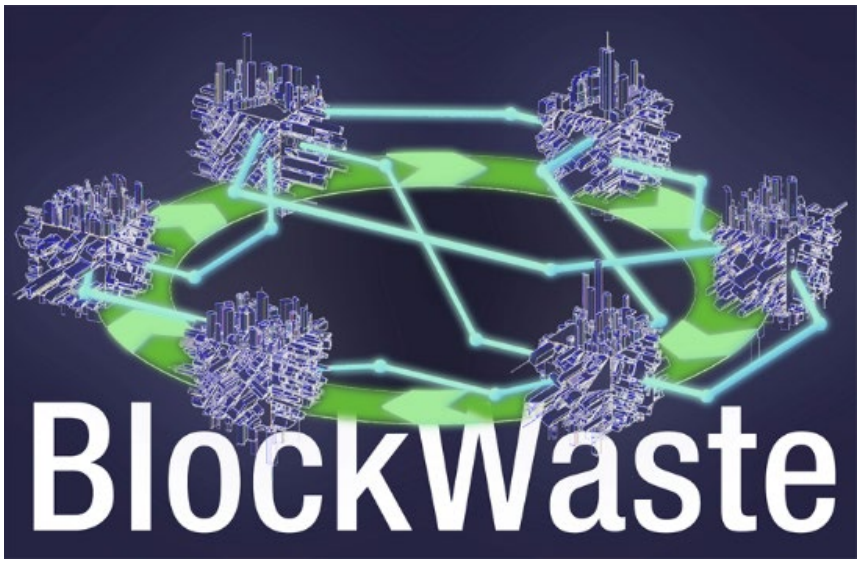
O1.A3 Handbücher zu Kreislaufwirtschaftsstrategien, die auf die kommunale Abfallwirtschaft mit Blockchain-Technologie angewendet werden

Handbuch II: Blockchain



Factsheet zur Ausgabe:

Förderprogramm	Erasmus+ Programm der Europäischen Union
Finanzierung von NA	EL01 Griechische Staatsstipendiat-Stiftung (IKY)
Vollständiger Projekttitel	Innovative Schulungen auf Basis der Blockchain-Technologie für die Abfallwirtschaft - BLOCKWASTE
Angezeigt	KA2 - Zusammenarbeit für Innovation und Austausch bewährter Praktiken KA203 - strategische Partnerschaften für die Hochschulbildung
Projektnummer	2020-1-EL01-KA203-079154
Projektdauer	24 Monate
Startdatum Des Projekts	01-10-2020
Enddatum Des Projekts:	30-09-2022

Ausgabedetails:

Ausgabetitel: O1: Lernmaterialien für interdisziplinäre Blockchain-MSW

Titel Der Aufgabe: O1/A3. Handbücher zu Kreislaufwirtschaftsstrategien, die auf die kommunale Abfallwirtschaft mit Blockchain-Technologie angewendet werden

Ausgangsleitung: NTUA

Leiter der Aufgabe: Saxion UAS

Autor(en): Christa Barkel, c.barkel@saxion.nl, Saxion UAS, Niederlande, Perry Smit, Saxion UAS, p.j.smit.01@saxion.nl, Niederlande

Geprüft von: Rainer Lenz, rlenz@fh-bielefeld.de, Fachhochschule Bielefeld, Deutschland, Paraskevas Tsangaratos, Nationale Technische Universität von Athen, ptsag@metal.ntua.gr, Griechenland

Dokumentenkontrolle

Dokumentversion	Version	Änderung
V0.1	11/03/2022	Endgültige Version - 29/04/2022

IKY Co-funded by the Erasmus+ Programme of the European Union

BlockWaste

Inhalt

Liste der Abbildungen

Liste der Abkürzungen

Abkürzung	Definition
CBDC	Digitale Währung der Zentralbank
DAO	Dezentrale Autonome Organisation
DApps	Dezentrale Anwendungen
DLT	Distributed Ledger Technology
DPOs	Delegierter Nachweis des Einsatzes
ERC-20 (Protokoll)	Ethereum Request for Comments 20 (Protokoll)
ICO	International Coin Offering
IEO	International Exchange Offering
MSW	Kommunales Abfallmanagement
NFT	Nicht fungibler Token
P2P	Peer-to-Peer
POS	Proof of Stake
POA	Proof of Authority
SPOF	Single-Point-of-Failure
STO	Angebot Für Sicherheitstoken
TTP	Vertrauenswürdige Dritte

Zusammenfassung

In diesem Handbuch wird Blockchain aus einer Vielzahl von Perspektiven angegangen. Es wird erwartet, dass dies dem Leser helfen wird, die Relevanz von Blockchain besser zu untersuchen und ein tieferes Verständnis für sein Potenzial zu gewinnen. Die ersten Grundlagen werden am Beispiel von Bitcoin erläutert. Bitcoin ist die erste Anwendung, die Blockchain verwendet. Bitcoin nutzt ein dezentrales Netzwerk, in dem alle Personen, die am Bitcoin-Entscheidungsprozess teilnehmen möchten, gemeinsam an der Entscheidungsfindung teilnehmen. Der Bitcoin-Code ist Open Source und ermöglicht es jedem, den Quellcode nach Belieben zu sehen, zu kopieren und zu bearbeiten, wodurch neue Experimente mit anderen, vielleicht besseren Formen der Kryptowährung oder anderen Anwendungen und anderen Formen des Konsenses entstehen können. Obwohl Bitcoin als Erklärungsbeispiel verwendet wird, ist es wichtig zu beachten, dass nicht nur das Finanzsystem von Blockchain betroffen ist. Die zugrunde liegende Technologie der Blockchain bietet neue Möglichkeiten, andere Branchen zu transformieren, einschließlich der kommunalen Abfallwirtschaft.

Dieses Handbuch beginnt mit einer Erklärung von Blockchain und seinen Funktionen. Es wird eine klarere Unterscheidung zwischen dem Kryptowährungs-Bitcoin und dem Bitcoin-Netzwerk gegeben und der Konsensus-Mechanismus von Bitcoin, Proof-of-Work, erläutert. Neben den grundlegenden Blockchain-Prinzipien, die in diesem Handbuch mithilfe von Bitcoin erläutert werden, verlagert sich der Fokus auf eine neuere Generation von Blockchain, die speziell entwickelt wurde, um eine Vielzahl anderer Arten dezentraler Anwendungen oder dApps zu erstellen. Eine spezielle Blockchain, auf die die Aufmerksamkeit gerichtet ist, ist Ethereum, das als erstes die Programmierung von Smart Contracts ermöglicht hat. Ein Smart Contract ist eine dezentrale Automatisierung und kann als Vertrag mit bestimmten Bedingungen definiert werden, die im Code festgelegt sind. Der Vertrag erfüllt sich selbst, da er entsprechende Maßnahmen durchführt, wenn die Bedingungen erfüllt sind.

Darüber hinaus erklärt dieses Handbuch kurz zwei Phänomene von Blockchain: Dezentrale Anwendungen (dApps) und dezentrale autonome Organisationen (DAO).

Blockchain kann aus drei Perspektiven in ihre Typen unterteilt werden: Konsensprotokoll, Governance und Arten der Zusammenarbeit zwischen Blockchain-Systemen. Konsensprotokolle sind unerlässlich, um das Vertrauen zwischen verschiedenen Teilnehmern in einem verteilten Netzwerk zu gewährleisten. Es muss Vertrauen bestehen, dass die Teilnehmer nicht beschädigt sind und dass die Daten, die unter ihnen geteilt werden, nicht beschädigt sind. Als Nächstes muss eine Blockchain wie jede Partnerschaft über eine Blockchain-Governance-Struktur verwaltet und kontrolliert werden. Die Wahl zwischen den verschiedenen Blockchains-Typen beeinflusst die Kontrolle der Organisation. Je mehr Vertrauen in die dezentrale Natur der Blockchain besteht, desto einfacher ist die Teilnahme. Je mehr Vertrauen es gibt, dass Validierer als Unbekannte am Konsensaufbau teilnehmen können, desto transparenter wird das System.

Zum Abschluss der drei Perspektiven gibt es verschiedene Arten der Zusammenarbeit zwischen Blockchain-Systemen. Blockchain, bei dem verschiedenen Unternehmen und Dritte zusammenarbeiten, ohne dass ein zentraler Nutzer diese Blockchain kontrolliert, wird als Enterprise Blockchain bezeichnet. Um eine solche Enterprise Blockchain aufzubauen, nutzen Unternehmen Blockchain-Plattformen. Diese Plattformen ermöglichen es Benutzern, Anwendungen mit bestimmten Technologien zu schreiben. Um diese Plattformen herum

wurden verschiedene Partnerschaften organisiert. Plattformen sind der dritte und letzte Weg, wie wir verschiedene Arten von Blockchains hier betrachten.

Eine der großen Erfindungen von Satoshi Nakamoto ist die Kombination von bereits vorhandenen Technologien mit einem Belohnungssystem, das ein dezentrales Netzwerk am Laufen hält: Krypto-Ökonomie. Die zentrale Idee hinter der Krypto-Ökonomie innerhalb von Blockchain ist, dass Protokolle entwickelt werden, die Menschen dazu ermutigen, sich so am Netzwerk zu beteiligen, dass der Wert des Netzwerks für die Teilnehmer maximiert wird.

Ein Krypto-Token kann auf einer Blockchain erstellt werden und stellt auch eine Handelsakquette dar. Manchmal werden Token erstellt, um ein Projekt zu finanzieren. Der Prozess der Tokenerstellung wird als Tokenisierung bezeichnet. Der Handel mit diesen Token ermöglicht die Übertragung von Eigentumsrechten an die zugrunde liegenden Vermögenswerte. In diesem Handbuch werden die verschiedenen Arten von Token und deren Verwendung erläutert.

Abschließend möchte ich sagen, dass es drei Beispiele für den Einsatz und die Anwendung von Blockchain gibt, einschließlich der Interpretation einiger entscheidender Bedingungen, die für eine erfolgreiche Implementierung von Blockchain erforderlich sind.

1 Einführung

1.1 Kurze Projektbeschreibung

Das BlockWASTE-Projekt zielt darauf ab, die Interoperabilität zwischen Abfallwirtschaft und Blockchain-Technologie anzugehen und deren ordnungsgemäße Behandlung durch Schulungen zu fördern, so dass die gesammelten Daten in einer sicheren Umgebung geteilt werden, in der es keinen Raum für Unsicherheit und Misstrauen zwischen allen Parteien gibt, die an Abfallketten oder im Recycling beteiligt sind.

Zu diesem Zweck sind die Ziele des BlockWASTE-Projekts wie folgt:

- Forschung zu Haushaltsabfällen, die in Städten entstehen und wie diese verwaltet werden, um eine Informationsbasis für bewährte Praktiken zu schaffen, um Abfälle wieder in die Wertschöpfungskette einzuführen und die Idee der intelligenten kreisförmigen Städte zu fördern.
- Die Vorteile der Blockchain-Technologie im kommunalen Abfallmanagement (MSW) zu identifizieren.
- Einen Studienplan zu erstellen, der die Ausbildung von Lehrern und Fachleuten von Organisationen und Unternehmen des Sektors ermöglicht, in der Überschneidung der Bereiche Abfallwirtschaft, Kreislaufwirtschaft und Blockchain-Technologie.
- Entwicklung eines interaktiven Tools auf Basis der Blockchain-Technologie, das es ermöglicht, das Management von Daten aus Siedlungsabfällen in die Praxis umzusetzen, so dass die Art und Weise, wie die Daten in der Blockchain implementiert werden, visualisiert und die Nutzer in die Lage versetzt werden, verschiedene Formen des Managements zu bewerten

BlockWASTE hat sich zum Ziel gesetzt, transnational neue Bildungsinhalte zu implementieren, mit dem Ziel, seine Studenten in den Partnerländern auszubilden und ihnen die notwendigen Grundkenntnisse zu vermitteln, die es ihnen ermöglichen, sich beruflich als zukünftige Arbeitnehmer in der Branche zu verhalten. Hinzufügen digitaler Kompetenzen, die von Unternehmen benötigt werden, die den Prozess der digitalen Transformation nutzen. In diesem Sinne richtet sich das Projekt an:

- Unternehmen und KMU, IT-Profis, Urbanismen und Abfallwirtschaft.
- Universitäten (Professoren, Studenten und Forscher).
- Öffentliche Einrichtungen

Das Projekt umfasst vier Intellectual Outputs wie folgt:

- O1. Lernmaterialien für interdisziplinäre Blockchain-MSW
- O2. Europäischer gemeinsamer Lehrplan über die Anwendung von Blockchain-Technologien auf Strategien der Kreislaufwirtschaft in MSW
- O3. E-Learning-Tool auf Blockchain-MSW-Basis mit Fokus auf Kreislaufwirtschaft
- O4. BlockWASTE Open Educational Resource (OER)

Dieses Dokument beschreibt und erklärt die grundlegenden Prinzipien von Blockchain. Es beschreibt, was Blockchain ist, wann Sie es verwenden können, aus welchen Komponenten eine Blockchain besteht, welche Blockchain-Technologien verwendet werden und beschreibt verschiedene erfolgreiche Blockchain-Anwendungen.

1.2 Ziele und methodischer Ansatz

Das Ziel dieses Handbuchs „Blockchain“ ist es, Fachleute aus dem Abfallwirtschaftsbereich dabei zu unterstützen, wie sie IoT- und Blockchain-Technologie als Strategien der Kreislaufwirtschaft implementieren sollten. Daher richtet sie sich an Praktiker, die über die Vorteile der Blockchain-Technologie Bescheid wissen. Die drei gemeinsamen Handbücher dieses Blockwaste-Projekts zielen darauf ab, den Lesern ausreichend Wissen über das Potenzial der Blockchain-Technologie zu vermitteln, um zu mehr Zirkularität in der kommunalen Abfallwirtschaft beizutragen. Handbuch 1 (Blockchain) und Handbuch 2 (Circular Economy) sind als Kurzkompendium zu verstehen und geben einen Überblick über die wesentlichen Inhalte des Handbook 3 (Blockchain Based Waste Management) - vgl. Abb. 1.

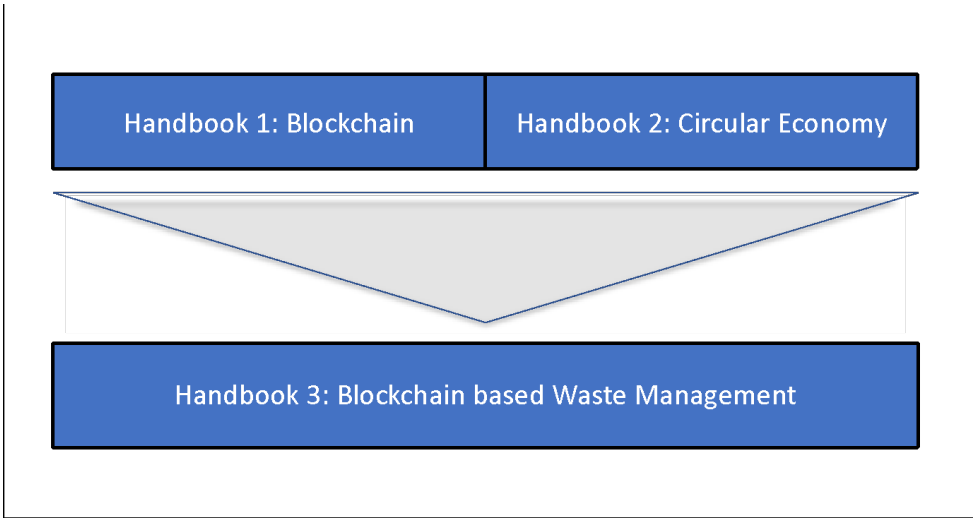


Figure 1:Handbücher BlockWASTE-Projekt (die Autoren)

Die Struktur des Handbuchs folgt einer deduktiven Logik, indem es im ersten Teil (Kapitel 1 bis 4) eine kurze Geschichte der Blockchain mittels Bitcoin und die Grundlagen der Blockchain-Technologie vorstellt. Der zweite Teil des Handbuchs (Kapitel 5) Enthält eine klare Anleitung für Anwendungen und Anwendungen der Blockchain-Technologie.

2 Blockchain-Grundlagen

Blockchain-Prinzipien durch Bitcoin verstehen

"Sorry to be a wet blanket. Writing a description for this thing for general audiences is bloody hard. There's nothing to relate it to."
- Satoshi Nakamoto (2010)

2.1 Einführung

Lernziele

- Blockchain auf der grundlegendsten Ebene, indem man Bitcoin betrachtet.
- Blockchain ist im Wesentlichen ein verteiltes Buch, in dem Sie Daten speichern können.
- Die Unterschiede zwischen einem Blockchain-Netzwerk und einem zentralisierten Netzwerk.

Einführung

Am 31. Oktober 2008 wurde eine E-Mail unter dem Namen Satoshi Nakamoto an die Cryptography Mailingliste gesendet.[1] In der E-Mail wurde auf ein **White Paper** mit dem Titel *Bitcoin: Ein Peer-to-Peer elektronisches Kassensystem*. Das Weißbuch, das er der Ankündigung angehängt hat, ist ein nur 9 Seiten langes Dokument, das die technischen Abläufe von Bitcoin umreißt. Dieses System ermöglicht es, Online-Zahlungen an andere Parteien zu senden, ohne dass ein Finanzinstitut benötigt wird.

Die wichtigsten Merkmale dieses Zahlungssystems, so Satoshi:

1. Double Spending derselben digitalen Münze wird durch ein Peer-to-Peer-Netzwerk verhindert.
2. Keine Intermediäre oder andere vertrauenswürdige Parteien.
3. Teilnehmer können anonym sein.
4. Neue Münzen werden aus HashCash-Style Proof-of-Work hergestellt.
5. Der Proof-of-Work Validierungsmechanismus befähigt das Netzwerk auch, Double Spending derselben Kryptowährung zu verhindern.

Fachbegriffe wie Double-Spending, Peer-to-Peer-Netzwerk, Proof-of-Work, HashCash, Zeitstempel, Hashing und digitale Signaturen in der E-Mail machen es der Öffentlichkeit schwer, Bitcoin oder ganz allgemein Blockchain zu verstehen. Vor allem zu der Zeit, als es für

[1]Die ursprüngliche E-Mail finden Sie unter: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.

die meisten Menschen nichts gab, mit dem es zu tun hatte. In diesem Kapitel diskutieren wir Bitcoin als das Mittel, um grundlegende Blockchain-Prinzipien zu verstehen.

2.1.1 Bitcoin im Vergleich zu Bitcoin

Wir unterscheiden im Allgemeinen zwischen (Kleinbuchstaben) Bitcoin, dem digitalen Geld, das auch Kryptowährung genannt wird, und (Großbuchstaben) Bitcoin, dem zugrunde liegenden Finanznetzwerk, das das Senden und Empfangen von Bitcoins ermöglicht.

2.1.2 Peer-to-Peer-Netzwerk

Die Computer, auch Knoten genannt, die dieses Finanznetzwerk betreiben, halten und haben Zugriff auf ein Buch, auf das alle Bitcoin-Transaktionen aufgezeichnet werden. Dieses Bitcoin-Hauptbuch ist eine Aufzeichnung aller gültigen Transaktionen, die jemals an das Netzwerk übertragen wurden. Dabei handelt es sich um die zugrunde liegende Infrastruktur, die aus den Knoten besteht, die alle Bitcoin-Transaktionen verfolgen, validieren und mit einem Zeitstempel versehen. Wir nennen dieses Netzwerk ein ***Peer-2-Peer-Netzwerk (P2P)***.

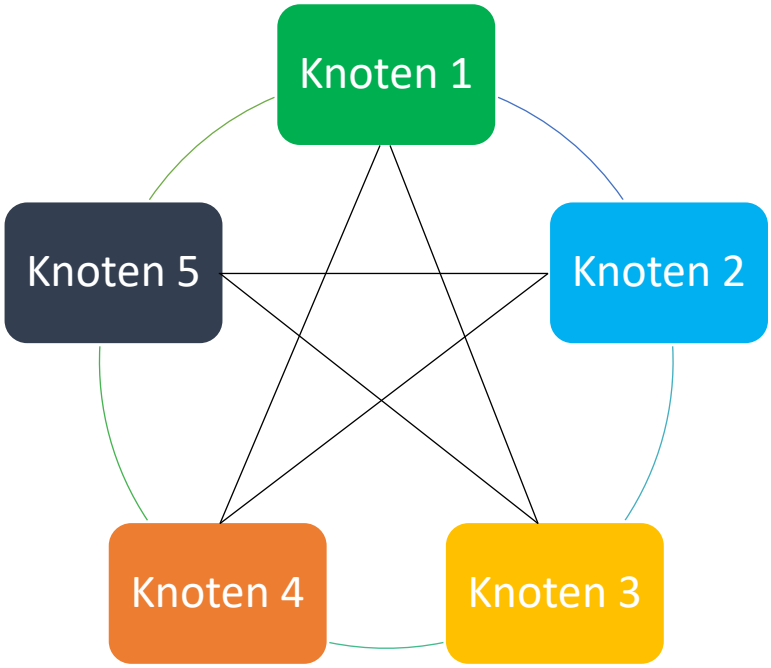


Figure 2: Eine Darstellung eines verteilten Netzwerks, in dem die Blockchain über ein Netzwerk voller Knoten verteilt ist (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 1, Seite 14).

Ein P2P-Netzwerk ist ein Netzwerk von Knoten, oft ein Computer, die gleichermaßen privilegiert sind. Jeder Knoten kann sowohl ein Dienstanbieter als auch ein Serviceverbraucher sein. Jeder hat Zugriff auf das Bitcoin-Netzwerk und kann einen Knoten im Netzwerk verwalten. Spezialisierte Knoten im Netzwerk, auch Full ***Nodes*** genannt, behalten den gesamten Transaktionsverlauf. Um das gesamte Netzwerk und die zugehörige

Transaktionshistorie zu entfernen, müsste man alle Knoten herunterfahren, was fast unmöglich ist, wenn das Netzwerk aus vielen Knoten besteht.

Jeder Teilnehmer innerhalb des Netzwerks folgt dem Bitcoin-Protokoll. Das Bitcoin-Protokoll ist die Verfahrensregeln, die das Bitcoin-Netzwerk regeln. Außerdem gibt es keinen Vermittler zwischen zwei verschiedenen Knoten. Das bedeutet auch, dass es keine zentrale Partei gibt, die Ihre Transaktionen regulieren, stoppen und einfrieren kann. Die Eliminierung solcher Vermittler ermöglicht effizientere und billigere Transaktionen.

2.1.3 Client-Server-Netzwerk

Dieses P2P-Netzwerk steht im Gegensatz zum ***Client-Server-Netzwerk*** (Workstation-Server-Netzwerk).

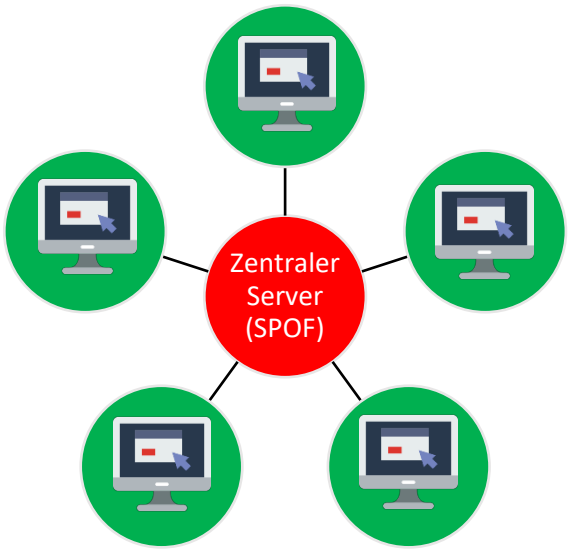


Figure 3:Vereinfachte Entscheidungsstruktur, ob Blockchain verwendet werden soll oder nicht (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 1).

Ein Client-Server-Netzwerk verwendet zentralisierte Server, die seinen Clients Dienste wie einen E-Mail-Dienst bereitstellen. Der Server enthält häufig Daten und Anwendungen. Wenn Clients Zugriff auf diese Ressourcen benötigen, können sie eine Anforderung an den Server senden. Eine Schwäche von Client-Server-Netzwerken besteht darin, dass sie einen ***Single Point of Failure (SPOF)*** enthalten. In diesem Fall ist der SPOF der zentrale Server. Nach der Deaktivierung können die Clients nicht mehr auf die Dienste des Servers zugreifen.

Die Notwendigkeit, einer zentralen Partei Ihre Daten zu vertrauen und darauf zu vertrauen, dass der SPOF nicht fehlschlägt, macht das Modell anfällig. Große namhafte Unternehmen können auch unter einem SPOF-Netzwerkdesign leiden. Im Jahr 2015 kam es beispielsweise zu einem Stromausfall in einem einzigen PayPal-Rechenzentrum. Infolgedessen konnten viele Nutzer nicht mehr auf die PayPal-Website zugreifen, Kreditkartentransaktionen konnten nicht

mehr verarbeitet werden, Personen konnten nicht mehr auf ihre persönlichen Kontodaten zugreifen oder falsche Bilanzen wurden angezeigt.[2]

2.1.4 Hybride Netzwerke: Der Fall Napster

Es gibt auch hybride Netzwerke. Ein berühmtes Beispiel ist Napster, ein Musik-Download-Service, der Ende 1990s und Anfang 2000s Bekanntheit erlangte.

1999 wurde von den Teenagern Shawn Fanning und Sean Parker ein Peer-to-Peer-File-Sharing-Dienst namens Napster gestartet. Napster ermöglichte es den Menschen, digitale Musikdateien von anderen zu teilen und herunterzuladen. Es verursachte viel Aufregung, weil zum ersten Mal Musik kostenlos miteinander geteilt wurde. Napster erlaubte es den Leuten, einzelne Songs herunterzuladen und anzuhören. Wenn man vorher einen einzigen Song haben wollte, musste man ein komplettes Album kaufen. Im Jahr 2001 wurde Napster schließlich nach einer Klage mit der Recording Industry Association of America geschlossen, weil die Verbreitung und der Download von digitalen Musikdateien als Verstoß gegen das Urheberrecht angesehen wurden. Dennoch ist Napster immer noch als revolutionärer Dienst bekannt, der die Musikindustrie gestört hat. In den Vereinigten Staaten erreichte der CD-Umsatz im Jahr 2000 seinen Höhepunkt, danach gab es einen starken Rückgang - teilweise aufgrund von Napster und nachfolgenden Diensten wie BitTorrent und Spotify.

Napster Is Told to Remain Shut

By MATT RICHTEL JULY 12, 2001

SAN FRANCISCO, July 11 _ A federal judge today ordered that the Napster music-sharing service must remain off line until it can prove that it can more effectively filter copyrighted material, signifying the first time a judge has mandated the shut down of the Internet service.

The order comes at a time when Napster had already been taken out of service, a move it made of its own accord 10 days ago to add technology that would enable it to meet an earlier court order to filter copyrighted music.

Figure 4: New York Time News item; Napster soll geschlossen bleiben, 12. Juli 2001.

Napster verwendet bekanntermaßen ein P2P-Netzwerk. Wie kam es, dass die Behörden Napster abschalten konnten, was mit Bitcoin praktisch unmöglich ist?

Napster verwendet einen zentralen Index, der nachverfolgt, welcher Computer welche Dateien für andere Benutzer hat. Wenn ein Benutzer (Computer A) nach einem Song wie Michael Jackson - Billie Jean suchen möchte, wird eine Verbindung zum Index hergestellt und

[2] https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

der Index sucht, auf welchen Computern dieser Song vorhanden ist. Wenn der Index zeigt, dass Computer B über diesen Song verfügt, wird eine direkte Peer-to-Peer-Verbindung zwischen den Computern A und B hergestellt, wodurch A die Nummer direkt vom Computer B herunterladen kann.

Napster ist ein gemischtes Modell aus Client-Server und Peer-to-Peer. Das zentrale Indexelement ist Client-Server, aber die eigentlichen Dateien werden Peer-to-Peer heruntergeladen. Der zentrale Index-Server hat sich als eine ernsthafte Achillesferse für Napster erwiesen, da er leicht geschlossen werden kann, was dazu führt, dass Napster nicht mehr funktioniert. Da Napster nur über einen zentralen Indexserver verfügt, der auflistet, welche Computer über welche gemeinsam nutzbaren Musikdateien verfügen, hat Napster selbst keine Musikdateien auf seinem Server. Es hat den Benutzern nur ermöglicht, Peer-to-Peer-Verbindungen herzustellen und Musik miteinander zu teilen.

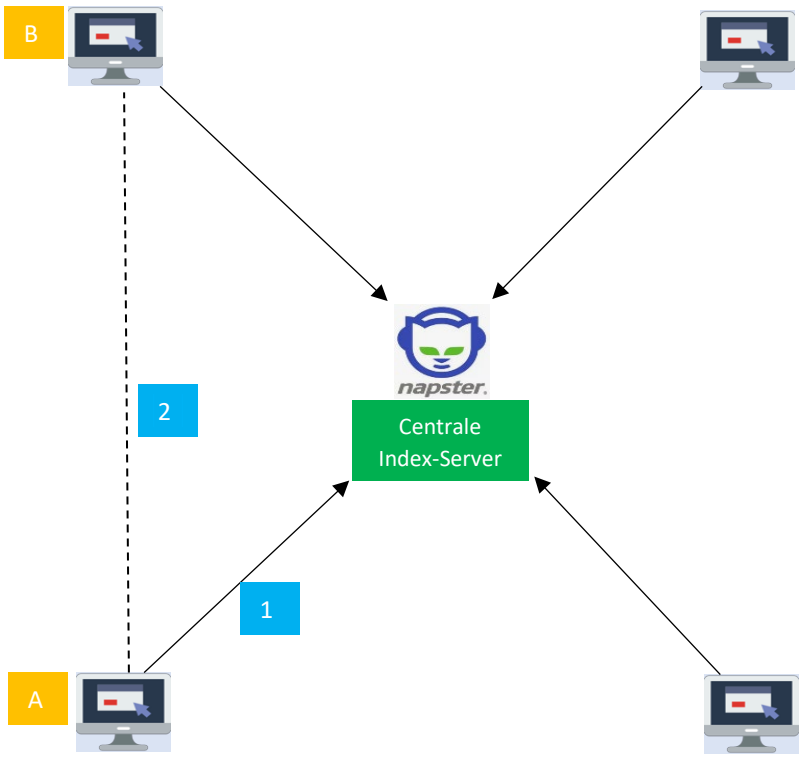


Figure 5:Napster-Netzwerk. (1) Computer A führt eine Suche auf dem zentralen Index-Server von Napster nach Michael Jackson - Billy Jean durch. Der zentrale Indexserver von Napster sucht nach Computern, die mit dem Netzwerk verbunden sind und über die Anzahl auf der Festplatte verfügen. (2) Computer B hat die Nummer. Legen von Computern A und B eine direkte Peer-to-Peer-Verbindung, nach der Computer A die Musikdatei von Computer B herunterlädt

Die gemeinsame Nutzung von Musikdateien erfolgt zwar Peer-to-Peer mit Napster, umfasst aber auch ein zentrales Server-Element, wodurch sie anfällig für Angriffe ist. In diesem Fall wurde es von der Strafverfolgung geschlossen. Mit dem Bitcoin-Netzwerk verfügen alle Knoten über eine exakte Kopie des öffentlichen Bitcoin-Ledgers. Das Bitcoin-Netzwerk besteht aus vielen Knoten, die auf der ganzen Welt verteilt sind, was es schwierig macht, sie alle zu lokalisieren und zu schließen.

2.1.5 Blockchain

Das öffentliche Bitcoin-Buch gilt als dezentral, da es auf Knoten auf der ganzen Welt verteilt ist. Das öffentliche Bitcoin-Buch wird auch als Blockkette oder Blockchain bezeichnet, die die Transaktionsdaten enthält. Wenn wir die Blockchain als eine Datenbank betrachten, die Informationen aufzeichnet, sind dies die wesentlichen inhärenten Eigenschaften einer Blockchain:

1. Die Daten sind in Datenblöcken angeordnet.
2. Die Blöcke werden schrittweise in Blocknummern aufsteigender Reihenfolge angezeigt.
3. Die Daten sind zuverlässig, da sie kryptografisch überprüfbar sind.

Die Kette ist die Transaktionsdatenbank, die von Knoten erstellt wird, die am Mining-Prozess im Bitcoin-Netzwerk teilnehmen. Die Kette wird von einem Zeitstempelserver verwaltet, der einen Nachweis über die chronologische Reihenfolge der Transaktionen liefert. Jeder Block enthält einen Hash-Verweis auf den Block, auf dem er aufbaut, was im Laufe der Zeit eine lineare Sequenz erzeugt. Blöcke können als die einzelnen Seiten eines Kassenbuches gedacht werden.

Die Miner verarbeiten ständig Transaktionen zu Blöcken, die sie am Ende der Kette hinzufügen. Der Prozess, bei dem Miner neue Blöcke zur Kette hinzufügen, wird auch Proof ***-of-Work*** genannt. Durch diesen Prozess wird das Double Spending ***derselben Kryptowährung*** verhindert.

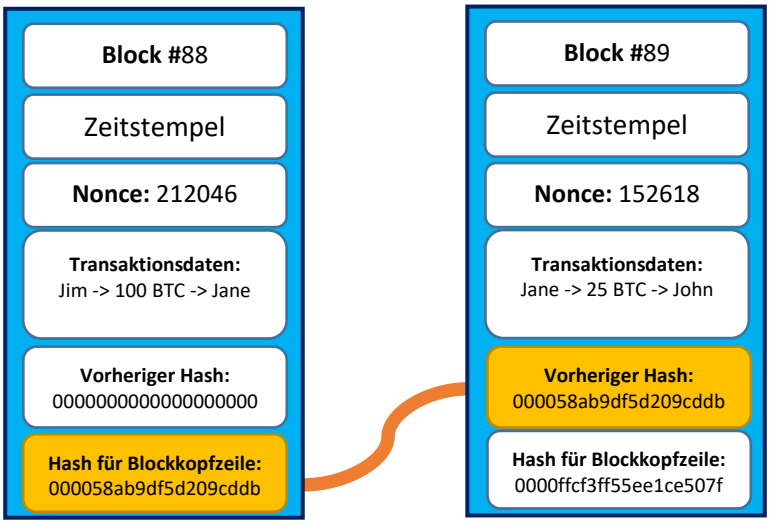


Figure 6: Vereinfachte Darstellung eines gültigen Genesis-Blocks und Blocks #2 mit beiden Blöcken, die mit dem Block-Header-Hash und dem vorherigen Hash verkettet sind. (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 3).

2.1.6 Das „Double Spending“ Problem

Ein wichtiges Thema, das ein Peer-to-Peer-elektronisches Finanzsystem lösen muss, ist das Problem des Double Spendings derselben digitalen Münze. Zum Beispiel, wenn Sie 1 Bitcoin haben und es gleichzeitig an Person A und Person B ausgeben. Innerhalb eines zentralisierten Finanznetzwerks kann das Problem der Double Spending durch einen ***vertrauenswürdigen Dritten (TTP)*** gelöst werden, der das Hauptbuch verwaltet und alle Transaktionen innerhalb des Hauptbuchs überprüft.

Innerhalb des Bitcoin-Netzwerks wird dieses Problem durch seine wirtschaftlichen Anreize und den Einsatz eines Zeitstempelservers gelöst. Miner haben einen starken Anreiz, diese Transaktionen nicht in einen Block aufzunehmen, da sie Gefahr laufen, dass ihre Sperre von anderen Minern abgelehnt wird, und darüber hinaus an der Durchführung eines Verbrechens mitbeteiligt wären.

2.1.7 Proof-of-Work

Neben der Vermeidung des Double Spendings besteht der Zweck des Proof-of-Work auch darin, das Netzwerk vor Angreifern zu schützen und einen Konsens über den Zustand des öffentlichen Hauptbuchs zu erzielen. Kurz gesagt, Proof-of-Work ist ein Mechanismus, bei dem Miner Computerleistung verwenden müssen, um die richtigen Werte für einen Block zu finden, an dem sie arbeiten. Wenn sie den richtigen Hash-Wert finden, können sie den Block der Blockchain hinzufügen und eine Belohnung in Bitcoins erhalten. Der Prozess, den richtigen Wert zu finden, wird als Mining bezeichnet.

Transaktionen, die an das Netzwerk gesendet werden, werden weder vom Miner direkt zu einem Block hinzugefügt, noch werden sie direkt im Hauptbuch gespeichert. Sie landen zunächst in einem ***Speicherpool*** (mempool) mit anderen Transaktionen, die noch von Minern zu einem Block hinzugefügt und vom Netzwerk noch nicht bestätigt werden müssen. Sie können sich den Mempool als Wartebereich für alle eingehenden Transaktionen vorstellen, die noch vom Netzwerk bestätigt werden müssen. Jeder Miner hat seinen eigenen Mempool und es ist möglich, dass sich die einzelnen Mempools pro Miner unterscheiden. Das liegt daran, dass es in einem Computernetzwerk immer Netzwerklatenz gibt: Es dauert immer ein wenig Zeit, bis eine an das Netzwerk gesendete Transaktion alle Miner im Netzwerk erreicht.

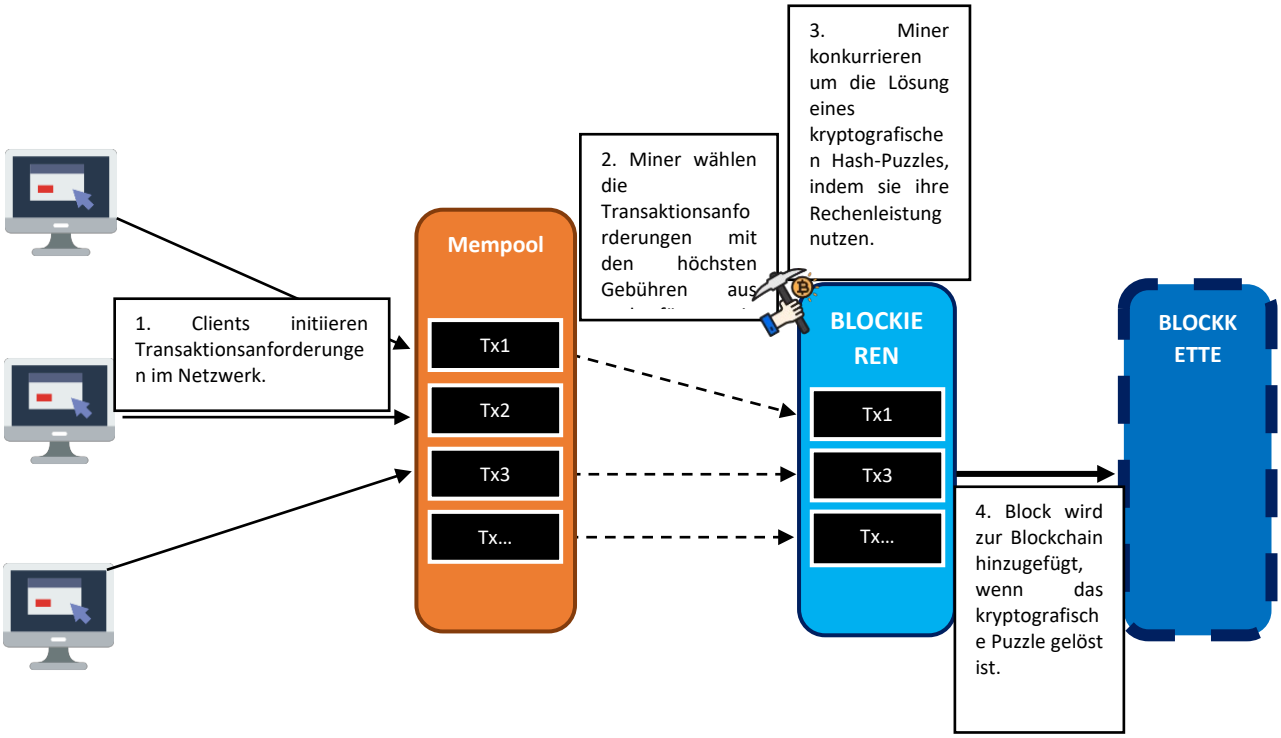


Figure 7:Schematische Darstellung, wie eine Transaktion zur Blockchain hinzugefügt wird. Im Mempool werden unbestätigte Transaktionen gespeichert. Miner wählen aus dem Mempool, welche der Transaktionen sie dem Block hinzufügen möchten. Anschließend versuchen sie, ein kryptographisches Rätsel zu lösen. Sobald sie gelöst sind, erhalten sie eine Blockprämie in Bitcoins.(Quelle: Buch: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 4).

Jede Transaktion erfordert Transaktionsgebühren. Miner werden wirtschaftlich ermutigt, die höchsten Gebührentransaktionen zu ihrem Block hinzuzufügen, weil sie diese Gebühren sammeln, wenn sie als erste einen gültigen Hash für den Block finden. Zusätzlich zu den Transaktionsgebühren erhalten Miner auch eine Blockprämie, die sich alle 210.000 Blöcke halbiert.

Das System ist sicher, solange ehrliche Knoten gemeinsam mehr Rechenleistung steuern als jede kooperierende Gruppe von Angreiferknoten.

2.1.8 Dezentralisierung

Die Begriffe ‘dezentrales Netzwerk und ‘dezentrales Netzwerk’ werden oft synonym verwendet.[3] Die Dezentralisierung stellt eine weitere wichtige Sicherheitsfunktion in Bezug auf die Zerstörung jedes einzelnen Knotens bereit, der die Daten als SPOF hostet. Die üblichen Lösungen, die Unternehmen haben, sind die mehrfache Kopie ihres gesamten Systems/ihrer

[3] Da die Blockchain eine Datenbank ist, die über verschiedene Server verteilt ist, wird diese Technologie auch als ***Distributed Ledger Technology*** (DLT) bezeichnet. Blockchain kann als DLT betrachtet werden, aber eine DLT muss nicht immer eine Blockchain sein.

gesamten Anwendung, die in Rechenzentren an mehreren Standorten gehostet wird. Dies ist eine enorme Kostenduplizierung, die für die Datensicherheit erforderlich ist, die Bitcoin allein durch sein natives Architekturdesign erreicht.

- **Eine dezentrale Blockchain erfordert Bestätigungen neuer Daten von anderen Knoten**

Mit einem zentralisierten Server ist es relativ einfach, neue Dateninjektionen in die Datenbank aufzunehmen. Die neuen Daten müssen nur von einer einzigen Partei hinzugefügt werden. Anders sieht es bei einem dezentralen Netz aus. Wenn die neuen Daten von einem Miner zu einer Blockchain hinzugefügt werden, müssen diese Daten noch von anderen vollen Nodes verifiziert und dann auch in die Blockchains, die von anderen Nodes gehostet werden, einbezogen werden.

- **Eine dezentrale Blockchain erfordert Konsens**

Wie sieht es mit neuen Aktualisierungen des Netzwerkprotokolls aus? Eine dezentrale Blockchain erfordert einen Konsens über Aktualisierungen und Vereinbarungen über den richtigen Zustand der Blockchain.

- **Eine dezentrale Blockchain ist schwer zu hacken**

Da die Blockchain auf verschiedenen Knoten gespeichert wird, die sich an verschiedenen Orten der Welt befinden, ist es schwierig, die Kontrolle über das Netzwerk zu übernehmen. Um das Netzwerk steuern zu können, muss die längste Kette erstellt werden können, die nur durch eine Mehrheitsberechnung erreicht werden kann. Sie ermöglicht es Ihnen, gültige Block-Hashes schneller zu finden als der Rest des Netzwerks zusammen. Ein Angriff, der auf Mehrheitsberechnungen basiert, wird auch als ***51%-Angriff*** bezeichnet.[4] Bei einem Angriff von 51 % könnt Ihr die Ausgaben verdoppeln.

- **Eine dezentrale Blockchain erschwert Zensur und Betrug**

Die Blockchain ist, wenn sie weit und breit genug verteilt ist, manipulationssicherer. Es ist jedoch möglich, Daten zu ändern oder zu löschen, wenn innerhalb des Netzwerks Einvernehmen darüber besteht. Wenn wir davon ausgehen, dass das Netzwerk gut dezentralisiert ist, können wir sagen, dass die Zensur der Blockchain schwierig zu erreichen ist.

2.1.9 Datenschutz

Satoshi Nakamoto erklärte bei seiner ersten Ankündigung des Bitcoin-Netzwerks, dass Bitcoin anonym sei, aber das stimmt eigentlich nicht. Bitcoin ist pseudonyme. Das bedeutet, dass es privat, aber nicht anonym ist. Es veröffentlicht alle Transaktionen in einer öffentlichen Blockchain in Klartext, damit jeder Dinge wie Algorithmen des maschinellen Lernens prüfen und ausführen kann, um Tracing-Analysen durchzuführen. Es ist jedoch privat, was bedeutet, dass, es sei denn, es besteht ein Bedarf zu wissen (wie eine gerichtliche Anordnung) und wenn

[4] Obwohl der 51%-Angriff der bekannteste ist, sind viele andere Angriffe auch möglich. Regelmäßige Angriffe, die in zentralen Netzwerken auftreten, wie Korruption von Kernentwicklern, Fehler in falsch geschriebenem Code oder Diebstahl von Schlüsseln, die Zugriff auf Server ermöglichen, treten auch mit Blockchains auf.

der Benutzer es mit der Absicht verwendet, ihre Finanztransaktion privat zu halten (indem er ihre öffentlichen Adressen nicht mehrmals wiederverwendet), da Privatsphäre integriert ist.

Die Privatsphäre wird weiterhin aufrechterhalten, indem öffentliche Schlüssel und die entsprechende Wallet-Adresse pseudonyme bleiben. Das öffentliche Hauptbuch erlaubt jedem zu sehen, welche Adresse welche Transaktion durchgeführt hat, aber solange Ihre Adressen unbekannt und nicht mit Ihren persönlichen Informationen verknüpft sind, können Sie eher 'anonym' Transaktionen durchführen.

Im Bitcoin-White Paper erwähnte Satoshi auch, dass als zusätzliche Firewall zur Wahrung der Privatsphäre für jede Transaktion ein neues Schlüsselpaar verwendet werden sollte, um zu verhindern, dass diese mit einem gemeinsamen Eigentümer verknüpft werden. Einige Verknüpfungen sind bei Transaktionen mit mehreren Eingaben immer noch unvermeidbar, was zwangsläufig zeigt, dass ihre Eingaben im Besitz desselben Eigentümers waren. Das Risiko besteht darin, dass bei der Enthüllung des Eigentümers eines Schlüssels durch die Verknüpfung andere Transaktionen aufgedeckt werden können, die demselben Eigentümer gehörten.

Die allgemeine Ansicht, dass Bitcoin eine anonyme Währung ist, ist daher faktisch falsch. Im Gegenteil, es funktioniert wie ein transparentes offenes Buch, und dies schuf einen Raum für eine ganze Reihe von Kryptowährungen, die sich darauf konzentrieren, anonym zu sein, wie Monero, Z-Cash und einige andere. Viele Länder arbeiten bereits aktiv an Rechtsvorschriften.

Das traditionelle Bankenmodell erreicht ein Maß an Privatsphäre, indem es den Zugriff auf Informationen auf die beteiligten Parteien und den vertrauenswürdigen Dritten beschränkt. Die Notwendigkeit, alle Transaktionen öffentlich bekannt zu geben, schließt diese Methode aus, aber die Privatsphäre kann weiterhin aufrechterhalten werden, indem der Informationsfluss an einem anderen Ort durchbrochen wird: Indem öffentliche Schlüssel anonym gehalten werden. Die Öffentlichkeit kann sehen, dass jemand einen Betrag an jemand anderen sendet, aber ohne Informationen, die die Transaktion mit jemandem verknüpfen. Dies entspricht dem Informationsstand der Börsen, bei denen die Zeit und die Größe einzelner Geschäfte, das „Band", öffentlich gemacht werden, ohne jedoch zu sagen, wer die Parteien waren.

2.1.10 Zusammenfassung

Obwohl es viele verschiedene Arten von Blockchains gibt und unterschiedliche Dezentralisierungsstufen aufweist, können wir daraus schließen, dass ein dezentrales Blockchain-Netzwerk im Allgemeinen die folgenden Attribute hat:

1. Es gibt keinen Single Point of Failure (SPOF).
2. Neue Daten müssen von anderen Knoten bestätigt werden.
3. Es ist eine Form des Konsenses erforderlich, um Aktualisierungen vorzunehmen und sich auf den richtigen Zustand der Blockchain zu einigen.
4. Es ist schwierig zu hacken.
5. Es erschwert die Zensur oder Änderung der Daten auf der Blockchain.
6. Es handelt sich um ein Peer-to-Peer-Netzwerk, das kein Vertrauen in eine zentrale Partei erfordert.

Abschließende Bemerkungen

- Blockchains unterscheiden sich von herkömmlichen Datenbanken.
- Napster ist deshalb gescheitert, weil es einen SPOF hatte. Eine Blockchain hingegen hat keinen SPOF und ist daher schwieriger abzuschalten.
- Eine Blockchain ist ein Peer-to-Peer-Netzwerk.

Verwendete Symbole

Computer von Prettycons aus dem Jahr www.flaticon.com

Mine von Strip aus dem Jahr www.flaticon.com

2.2 Blockchain 2,0 und Smart Contracts

„Wir wollen eine ganze Reihe von Unternehmen: Digitale Titel, digitale Medienwerte, digitale Aktien und Anleihen, digitales Crowdfunding, digitale Versicherungen. Wenn Sie Online-Vertrauen haben, wie es die Blockchain bietet, können Sie Feld für Feld neu erfinden.“
- Marc Andreessen (2014)

2.2.1 Einführung

Lernziele

- Was Blockchain 1,0 ist und warum es einen Bedarf an Blockchain 2,0 gibt.
- Ethereum ist ein Beispiel für Blockchain 2,0.
- Was Smart Contracts sind.
- Was dezentrale Anwendungen (dApps) sind.
- Was dezentrale autonome Organisationen (Daos) sind.

Einführung

Im vorherigen Kapitel wurden hauptsächlich grundlegende Blockchain-Prinzipien durch Bitcoin diskutiert. In diesem Kapitel richten wir unsere Aufmerksamkeit auf eine neuere Generation von Blockchains, die speziell dazu gedacht sind, eine Vielzahl anderer Arten dezentraler Anwendungen oder dApps zu erstellen. Eine spezielle Blockchain, auf die wir uns konzentrieren, ist Ethereum, das sich auch als dezentraler Computer der Welt wirbt.

2.2.2 Blockchain 1,0 und 2,0

Die erste Generation von Blockchains ist auch als ***Blockchain 1,0*** bekannt, die sich hauptsächlich auf digitales Geld konzentriert. Vitalik Buterin hatte die Idee, eine neue Blockchain, Ethereum, zu entwickeln, auf der neue digitale Münzen, Verträge mit Bedingungen und Anforderungen und sogar vollwertige ***dezentrale Anwendungen*** (dApps) entstehen konnten. Blockchains mit solchen Fähigkeiten werden auch als Blockchains der 2.. Generation bezeichnet: ***Blockchain 2,0***.[5]

2.2.3 Ethereum

Ethereum wurde erstmals von Vitalik Buterin im "Ethereum White Paper: A next Generation Smart Contract & Dezentrale Application Platform" (2013) vorgestellt. Im White Paper erklärt Buterin, dass Bitcoin als „First-to-File-System“ bezeichnet werden kann, bei dem die Reihenfolge der Transaktionen entscheidend ist. Technisch kann Bitcoin als ein einfaches Zustandsübergangssystem betrachtet werden, bei dem (a) der „Staat“ aus dem

[5] Dies sind Blockchains, die eine Reihe von Problemen gelöst haben, mit denen Blockchain 2,0 immer noch zu tun hat. Beispiele für solche Probleme sind Skalierbarkeit, Interoperabilität, Datenschutz sowie Nachhaltigkeit und Governance (Ackermann & Meier, S. 1). EOS, Cosmos, Cardano, Avalanche, Terra sind Beispiele für Blockchains, die als Blockchain 3,0 bezeichnet werden könnten.

Eigentumsstatus aller vorhandenen Bitcoins besteht und (b) die „Zustandsübergangsfunktion“, die einen Zustand und eine Transaktion übernimmt und einen neuen Zustand ausgibt, der das Ergebnis ist. Es ist jedoch schwierig, Verträge über die Transaktion abzuschließen, die über mehrere Staaten hinweg erfasst werden können. Es ist zum Beispiel kaum möglich, eine Logik weiterzugeben, die besagt, dass Bob sein Geld an Alice senden kann, dass Alice es aber erst dann beanspruchen kann, wenn sie etwas dafür bereitgestellt hat. (Buterin, 2013, S. 12)

Ethereum hat sich zum Ziel gesetzt, Entwicklern die Möglichkeit zu geben, Anwendungen auf der Grundlage beliebiger Bedingungen zu entwickeln. Die Programmiersprache, die speziell für Ethereum entwickelt wurde, heißt ***Solidität***.

2.2.4 Ethereum-Transaktionen und Gas

Die zugrunde liegende Kryptowährung der Ethereum Blockchain ist Äther (ETH). Eine Transaktion über das Ethereum-Netz erfordert ***Gas***. Gas wird in der Kryptowährung Ether exprimiert. Gas im Ethereum-Netz ist im Grunde das gleiche wie Transaktionskosten. Dies wird anhand der Standardkosten pro Einheit der Rechenleistung x der Anzahl der Einheiten berechnet. Sie können für jede von Ihnen durchzuführende Transaktion eine bestimmte Menge an Gas oder Transaktionskosten angeben. Der Benutzer muss eine angemessene Menge an Gas für die Transaktion bezahlen. Wenn zu wenig Gas bezahlt wird, können Miner die Transaktion nicht in den Block aufnehmen und daher wird diese Transaktion nicht ausgeführt. Zusätzlich zur Blockprämie erhält der Miner auch alle Gasgebühren, die bei den Transaktionen im Block enthalten waren.

Das Krypto-Gas aus wirtschaftlichem Grund wurde in das Ethereum-Netzwerk eingeführt, weil es wichtige Transaktionen priorisiert. Ein Block hat nur Platz für eine begrenzte Anzahl von Transaktionen. Das Gassystem stellt sicher, dass keine Energie für Spam oder Transaktionen mit geringem Wert verschwendet wird.

2.2.5 Smart Contracts

Ein Smart Contract ist eine dezentrale Automatisierung und kann als Vertrag mit bestimmten Bedingungen definiert werden, die im Code festgelegt sind. Der Vertrag erfüllt sich selbst, da er entsprechende Maßnahmen durchführt, wenn die Bedingungen erfüllt sind.

Ein Smart Contract könnte beispielsweise ein Arbeitsvertrag sein, bei dem Alice Bob €500 bezahlen will, um eine Website zu entwickeln. Der Vertrag könnte wie folgt funktionieren:

1. Alice setzt €500 in den Vertrag und die Mittel sind gesperrt.
2. Wenn Bob die Website entwickelt hat, sendet Bob eine Nachricht an den Vertrag, um die Gelder an ihn freizugeben.
3. Der Fonds wird freigegeben, wenn Alice zustimmt.
4. Wenn Bob sich entschließt, die Website nicht abzuschließen, kann Bob seinen Job kündigen, indem er eine Nachricht an den Vertrag sendet, wonach der Fonds automatisch an Alice zurückgegeben wird.

5. Wenn Bob behauptet, dass er die Website fertiggestellt hat, Alice aber nicht damit einverstanden ist, könnte nach einer 7-tägigen Wartezeit ein Richter angerufen werden, um ein Urteil zugunsten von Alice oder Bob abzugeben. (Buterin, 2014)

Vorteile von Smart Contracts

Smart Contracts bieten viele Vorteile. Chaintrade (2017) hat die folgenden elf gelistet:

1. *Genauigkeit:* Alle Geschäftsbedingungen sind in einem Smart-Vertrag detailliert zu erfassen. Werden bestimmte Bedingungen weggelassen, kann dies zu einem unerwünschten Verhalten des Smart-Vertrags führen.
2. *Transparenz:* Alle Geschäftsbedingungen sind vollständig sichtbar und für alle Beteiligten zugänglich. Sobald der Vertrag abgeschlossen ist, können Sie ihn nicht mehr bestreiten.
3. *Klare Kommunikation:* Die Notwendigkeit sorgfältig definierter Smart Contracts stellt sicher, dass die Kommunikation im Vertrag klar geregelt ist, sodass kein Raum für Fehlkommunikation und Fehlinterpretation besteht.
4. *Geschwindigkeit:* Smart Contracts können herkömmliche Geschäftsprozesse automatisieren und erheblich beschleunigen. Es müssen keine Anträge zur Genehmigung eingereicht und keine Dokumente von Einzelpersonen bearbeitet oder genehmigt werden.
5. *Sicherheit:* Smart Contracts laufen auf Blockchain-Plattformen und nutzen Datenverschlüsselung.
6. *Effizienz:* Aufgrund der Genauigkeit und Geschwindigkeit führen Smart Contracts Geschäftsprozesse effizienter aus oder eliminieren sie sogar vollständig.
7. *Papierfrei:* Für die Durchführung von Smart Contracts ist kein Papierkram erforderlich.
8. *Storage und Backup:* Smart Contracts und ihre Details werden dauerhaft in der Blockchain gespeichert. Daher können sie nicht verloren gehen und sind leicht zu finden.
9. *Kosteneinsparungen:* Smart Contracts können eine Menge Kosten einsparen, da es weniger nötig ist, dass Vermittler wie Rechtsanwälte, Zeugen und Banken die Verträge auslegen und durchsetzen.
10. *Vertrauen:* Die beteiligten Parteien können darauf vertrauen, dass Smart Contracts – wenn sie ordnungsgemäß eingerichtet sind - fair ausgeführt werden, ohne die Möglichkeit von Datenmanipulation und Vorurteilen.
11. *Garantierte Ergebnisse:* Durch den Einsatz von selbstausführenden Verträgen werden die Parteien die Regeln des Smart-Vertrags einhalten und es wird weniger Rechtsstreitigkeiten geben.

2.2.6 Dezentrale Anwendungen

Wir definieren eine ***dezentrale Anwendung*** (Dapp) als eine Anwendung, die den dezentralen Datenspeicher einer Blockchain nutzt. Die Applikation wird nicht über einen zentralen Server ausgeführt, sondern über ein dezentrales Knotennetzwerk. Wie eine normale Anwendung verfügt sie häufig über ein Front-End und eine Benutzeroberfläche. Das Interface bietet dem Nutzer eine einfachere Interaktion mit Smart Contracts und der Blockchain. Durch die dezentrale Speicherung und Ausführung der Smart Contracts, aus denen der Kerncode eines

Dapps besteht, gibt es keinen Single Point of Failure. Der Betrieb der Anwendung und die Daten der Anwendung können nicht einfach zensiert oder entfernt werden.

2.2.7 Dezentrale autonome Organisation (DAO)

Dezentrale autonome Organisationen (Daos) können als eine nicht hierarchische Organisation definiert werden, die Routineaufgaben in einer Blockchain ausführt und registriert. Die Regeln, die das DAO befolgt, werden auch auf der Blockchain aufgezeichnet. Darüber hinaus ist die DAO auf freiwillige Beiträge interner Akteure angewiesen, um die Organisation durch einen demokratischen Konsultationsprozess zu leiten. (Hsieh et al., 2018, S. 2)

Was ein DAO grundlegend von einer zentralisierten Organisation unterscheidet, ist, dass es kein Top-Management-Team oder einen CEO hat. Es gibt auch keine Niederlassungen, Mitarbeiter oder Tochtergesellschaften. Stattdessen existiert ein DAO in einem dezentralen Netzwerk von Benutzern und Knoten, die Transaktionen auf einer Blockchain sammeln, verifizieren und aktualisieren. Entscheidungen über Änderungen des Kodex werden durch demokratische Abstimmungsprozesse getroffen. Es ist eine völlig andere Art, eine Geschäftsorganisation zu gegründet. Aufgrund seiner autonomen Natur - immerhin handelt es sich um ein autarkes und selbstorganisierendes System - kann Bitcoin als DAO bezeichnet werden, weil es (a) ein Zahlungssystem betreibt, (b) Subunternehmer beschäftigt, die als Miner arbeiten und (c) diese Subunternehmer mit neu verteilten Bitcoins bezahlt (Vigna & Casey, 2015, S. 229). Darüber hinaus können Miner über ihre Rechenleistung für Vorschläge zur Verbesserung des Protokolls stimmen. Daos werden durch einen kollektiven Entscheidungsprozess von Stakeholdern über ein dezentrales Protokoll gesteuert und werden nicht von einem zentralen Leitungsgremium beeinflusst.

Abschließende Bemerkungen

- Mit Blockchain 2,0 können eine Vielzahl neuer Anwendungsarten entwickelt werden.
- Sie können Smart Contracts auf Ethereum entwickeln, wenn die Geschäftsbedingungen so klar festgelegt sind, dass im Falle einer Vertragsverletzung eine Auslegung Dritter nicht mehr erforderlich ist.
- Bitcoin ist ein First-to-File-System.
- Bitcoin ist die erste dezentrale autonome Organisation (DAO).

3 Arten von Blockchain

In diesem Kapitel werden wir Blockchain aus drei Perspektiven in seine Typen aufteilen: Konsensprotokoll, Governance und Arten der Zusammenarbeit zwischen Blockchain-Systemen.

3.1 Arten von Blockchain nach Konsensus-Protokoll

Konsensprotokolle sind unerlässlich, um das Vertrauen zwischen verschiedenen Teilnehmern in einem verteilten Netzwerk zu gewährleisten. Es muss Vertrauen bestehen, dass die Teilnehmer nicht beschädigt sind und dass die Daten, die unter ihnen geteilt werden, nicht beschädigt sind. Um dieses Vertrauen zu gewährleisten, müssen teilnehmende Knoten Nachrichten oder Transaktionen auf Richtigkeit überprüfen und andere Teilnehmer neutralisieren, die korrupt und irreführend sind: Die Lösung des Problems der byzantinischen Generäle, wie im vorherigen Kapitel besprochen.

Da ein Konsensprotokoll daher das Wesen eines Blockchain-Systems berührt, wird es hier als eine Möglichkeit zur Unterscheidung von Blockchain-Typen verwendet.
Im vorherigen Kapitel wurde am Beispiel des Bitcoin das erste Konsensprotokoll, Proof **-of-Work**, eingeführt. Nach diesem Protokoll darf ein Datenblock nur dann zur Blockchain hinzugefügt werden, wenn ein gültiger Hash des Blocks gefunden wurde. Als sich die Minenarbeiter von Bitcoin in einen harten Wettbewerb in der Rechenleistung einmissten, um die Vorteile zu erhalten, zuerst einen gültigen Hash zu finden, hat der Stromverbrauch des Bitcoin-Netzwerks zu Sorgen über die negativen Auswirkungen von Blockchain auf die Umwelt geführt. Die daraus resultierende Suche nach nachhaltigeren Lösungen für das Problem der byzantinischen Generäle hat zu alternativen Konsensprotokollen geführt.
Eine der wichtigsten Alternativen zum Proof-of-Work ist der Proof-of-Stake, der jetzt in verschiedenen Blockchain-Projekten umgesetzt wurde, mit dem bemerkenswerten Beispiel von Ethereum, das 2022 auf Proof-of-Stake übergeht.

Während Miner bei Proof-of-Work neue Blöcke produzieren dürfen, wenn sie einen gültigen Hash finden können, wird ein Blockproduzent bei Proof-of-Stake auf der Grundlage von (a) einem zufallsbasierten Auswahlverfahren und (b) einem **„Stake“** d.h. nach der Anzahl der digitalen Münzen, die er besitzt, ausgewählt. Daher benötigen Sie für die Teilnahme keine Rechenleistung. Es braucht nur einen Standardcomputer, eine Internetverbindung und eine digitale Münze. Der Blockproduzent beim Proof-of-Stake wird daher nicht als Miner, sondern als ***Forger*** bezeichnet. Da der Forger auch eine Belohnung erhält, wenn er einen neuen Block produziert, können Sie auch **den** Nachweis des Einsatzes als eine Methode sehen, bei der Sie ein passives Einkommen auf Ihren Münzen verdienen. Je mehr Einsatz Sie haben, desto höher ist die Chance, dass Sie den nächsten Block produzieren können. Neben der Produktion von Blöcken validieren Forger auch Transaktionen und tragen so zur Sicherung des Netzwerks bei.

Neben der Energieeffizienz liegen die Vorteile des Proof-of-Stake-Beweises darin, dass das einfache Stacking eine bessere Verteilung der Blockchain ermöglicht und dass die Durchführung eines 51%-Angriffs weniger attraktiv ist.

Es gibt verschiedene Varianten innerhalb des Proof-of-Stake, die ihre eigenen einzigartigen Eigenschaften haben. Erstens kann jeder, der eine digitale Münze besitzt, im **delegierten**

Proof-of-Stake seine Stimme delegieren. Als Ergebnis kann der delegierter Proof-of-Stake mehr Transaktionen pro Sekunde verarbeiten als Blockchains, die dezentraler sind.
Zweitens kann jeder in einem **geleasten Proof-of-Stake** seine Münzen an Stake-Knoten leasen, wodurch die Chance für Stake-Knoten erhöht wird, einen Block zu produzieren. Die Stake-Knoten verteilen ihre Belohnung proportional zwischen sich selbst und den Leasingnehmern. Daher ermutigt dieses Protokoll seine Nutzer, sich am Abstimmungsprozess (Staking) zu beteiligen.

Drittens werden Velocity-Nutzer mit **einem Proof-of-Stake** für (a) die Anzahl der Münzen, die sie besitzen, und (b) die aktive Verwendung ihrer Münzen belohnt. Die Gemeinschaft wird daher ermutigt, die Münzen nicht nur aufzubewahren, sondern sie auch tatsächlich für Transaktionen zu verwenden.

Viertens werden Blockhersteller (Autoritätsknoten) mit **Proof-of-Authority** auf der Grundlage ihrer Identität und ihres Rufs authentifiziert und genehmigt. Durch die Verknüpfung von Reputation und Identität werden Autoritätsknoten zusätzlich dazu angeregt, gutes Verhalten zu zeigen und keine böswilligen Transaktionen in die Blockchain aufzunehmen. Wenn sie dies tun, wird dies zu Rufschäden führen. Proof-of-Authority ist ein Beispiel für die Erstellung einer Proof-of-Stake-Variante, bei der die Chance, einen neuen Block zu erstellen, nicht vollständig von der Anzahl der Münzen abhängt, die Sie setzen.
Bedenken Sie, dass es zweifelhaft ist, ob der Nachweis der Autorität unter den Nachweis der Beteiligung fällt. Es wird manchmal als eine Form des delegierten „Proof-of-Stake“ gedacht und häufiger in geschlossenen, genehmigtem Blockchains verwendet.

Ein Vorteil der Typisierung der Blockchain mithilfe von Konsensus-Protokollen ist, dass sie die Unterschiede in der **Skalierbarkeit von Blockchain** erklären hilft. Dies, da die Skalierbarkeit im Allgemeinen vom Einfluss der Konsensprotokolle auf die Blockzeit, die Blockgröße, die Verteilungs- oder Dezentralisierungsebene der Blockchain und die Art und Weise der Blockproduktion abhängt, Transaktionen an die Blockchain gesendet und Transaktionen verifiziert werden. Um diese Skalierung zu verbessern, werden verschiedene Lösungen getestet, wie z. B. die Übernahme von Transaktionen außerhalb der Kette. Bekannte Beispiele hierfür sind das Lightning Network, Plasma (beides sogenannte ‘Layer 2’-Lösungen) und Sharding.

3.2 Blockchain-Governance und wer mit welcher Rolle teilnehmen kann

Eine Blockchain muss, wie jede Partnerschaft, verwaltet und kontrolliert werden. Die daraus resultierende Blockchain-Governance-Struktur bietet eine zweite Möglichkeit, Blockchain-Typen zu unterscheiden, die hier diskutiert werden.

Zu den bemerkenswerten Governance-Elementen gehören:

1. **Rechte** zur Einreichung, Ausführung und Überwachung **von Entscheidungsvorschlägen** durch eine Gruppe oder an alle.
2. **Verantwortlichkeit** und das Recht, Entscheidungen und Verhaltensweisen zu überwachen und für Ihre Verantwortung verantwortlich gemacht zu werden.
3. **Anreize** und Anreize für die Teilnehmer zur Aufrechterhaltung der Blockchain.

Die Art und Weise, wie diese Elemente interpretiert werden, hängt von den Zielen der Partnerschaft und damit von der Art der Governance ab, die sie benötigt.

Einer der Governance-Bedürfnisse kann sein, dass eine zentrale Gruppe von Menschen Kontrolle übt und Begriffe diktiert (**zentrale** Kontrollmentalität**)**, im Gegensatz zu den Bedürfnissen einer größeren Gruppe, auf gleicher Basis ohne Hierarchie oder zentrale Kontrolle (**dezentrale** Kontrollmentalität) zusammenzuarbeiten.

Die Art der Kontrolle, die ausgeübt wird, wird verwendet, um zu entscheiden, wer die Erlaubnis zur Teilnahme an einer Blockchain erhält oder nicht. Wenn zentrale Behörden den Zugang gewähren, ist die Blockchain der **private** Blockchain-Typ. Wenn der Zugang für alle organisiert ist, wird die Blockchain als **öffentliche** Blockchain bezeichnet. Die öffentlichen und privaten Blockchain-Typen finden sich in dem Konsortium Blockchain-Typ zusammen, einer Zwischenform, die stärker zentralisiert ist als eine öffentliche Blockchain und dezentraler ist als eine private Blockchain.

In einem Konsortium arbeiten mehrere Organisationen zusammen, um eine Blockchain zu erstellen, und der Konsens wird von einer Auswahl von Knoten verwaltet. Das Konsortium entscheidet für das gesamte Netzwerk, wer mit welcher Rolle mitwirken kann, welche Transaktionen offen gesehen oder vor anderen Teilnehmern abgeschirmt werden können und wie die Governance strukturiert werden soll.

Sie verwenden hauptsächlich eine **öffentliche Blockchain**, bei der jeder gleich behandelt wird, wenn Sie eine Gruppe gleichgesinnter Menschen zusammen arbeiten wollen. Die Zusammenarbeit wird hier durch den Konsensmechanismus garantiert, der als 'Vertrauensmaschine' fungiert. 'Zugang zu allen' führt zu einer größeren Anzahl von Knoten, die Vertrauen in das Blockchain-System aufbauen. Eine öffentliche Blockchain zeigt ein geringeres Vertrauen in Behörden, die die Blockchain im Namen anderer regieren. Diese Einstellung zu Vertrauen und Vertrauen begünstigt die Entscheidung für Konsensungsprotokolle mit dezentralerem Charakter, das Vertrauen in den Open Source-Charakter seiner Blockchain sowie den Wunsch nach vollständiger Transparenz der Entscheidungsfindung. Diese Haltung führt daher zu einem größeren Vertrauen in die Aufnahme und Teilnahme fremder Personen an der Partnerschaft. Schließlich liegt das Vertrauen im System und nicht im Benutzer.

Im Allgemeinen wird ein Unternehmen, das zu einer **privaten Blockchain** neigt, wissen wollen, wer im Blockchain-System ist. Denken Sie an ein Intranet, in dem Sie die Knoten, Daten und den Quellcode überprüfen. Sie wissen, dass jeder und alle Transaktionen angezeigt werden können, wenn dies erforderlich ist, aber Sie schützen Menschen auch vor der Überprüfung oder Anzeige bestimmter Transaktionen. Dies ist nützlich, wenn die Daten unternehmensempfindlich sind. In einem öffentlichen System ist es auch möglich, dies technisch einzubauen, aber in der Praxis erweist sich dies vorerst als Herausforderung.

Daher ist es in einer privaten Blockchain wichtig, alle Rollen zu kennen, die Sie den Teilnehmern zuweisen, auf die Sie Zugriff gewährt haben. Eine wichtige Rolle ist die Möglichkeit, **den Konsensmechanismus** beizubehalten. Soll diese Möglichkeit allen Teilnehmern der Blockchain oder nur einer ausgewählten Gruppe gegeben werden?

Die Antwort auf diese Frage führt zu den **permissionless** und **permissioned** Blockchain-Typen.

Wenn jedem Teilnehmer der Blockchain erlaubt wird, den Konsensmechanismus beizubehalten, handelt es sich um einen „**permissionless"** Blockchain-Typ. Wenn die Rolle zur Aufrechterhaltung des Konsensmechanismus einer ausgewählten Gruppe vorbehalten ist, sprechen wir über „**permissioned"** Blockchain.

Neben der Wahrung des Konsenses gibt es Rollen, die es Ihnen ermöglichen, Transaktionen in der Blockchain auszuführen, anzuzeigen und anzupassen, die Blockchain technisch zu pflegen oder an der Abstimmung über Ideen teilzunehmen. Diese Rollen sind nicht relevant für die Wahl zwischen einem „permissionless“ oder „permissioned“ System. Diese Rollen sind jedoch für die Art der Partnerschaften relevant. Dies ist relevant, denn wenn es den Behörden nichts ausmacht, wer auf das System zugreift, und sie Vertrauen in das System selbst setzen, wird es wahrscheinlicher sein, den Teilnehmern Anonymität zu gewähren. Unternehmen, die derzeit klassische Managementkontrollsysteme verwenden, würden sich jedoch dafür entscheiden, die Personen zu kennen, zu denen sie Zugang gewähren, sowie zu wissen, welche Rollen vorhanden sind und welchen Teilnehmern sie welche Rolle zuweisen können.

Durch die Trennung der Rollen können diese Unternehmen ihre zugrunde liegende Organisationsstruktur weiterhin nutzen. So können sie ihre Unternehmensidentität innerhalb ihrer Blockchain durchsetzen, indem sie das Profil der Personen sowie ihre Rollen kontrollieren. Darüber hinaus können sie nicht nur teilweise Vertrauen in das System übertragen, sondern auch ihre Organisation, ihr eigenes Management-Kontrollsystem, wie z. B. das spezifische Personalmanagement, verwalten.

Dies hilft zu erklären, warum in einem zugangslosen System Krypto-Token zur Förderung der Zusammenarbeit zur Verfügung gestellt werden.

Die verschiedenen Blockchain-Typen werden in Kombination in den heutigen Blockchain-Modellen eingesetzt:

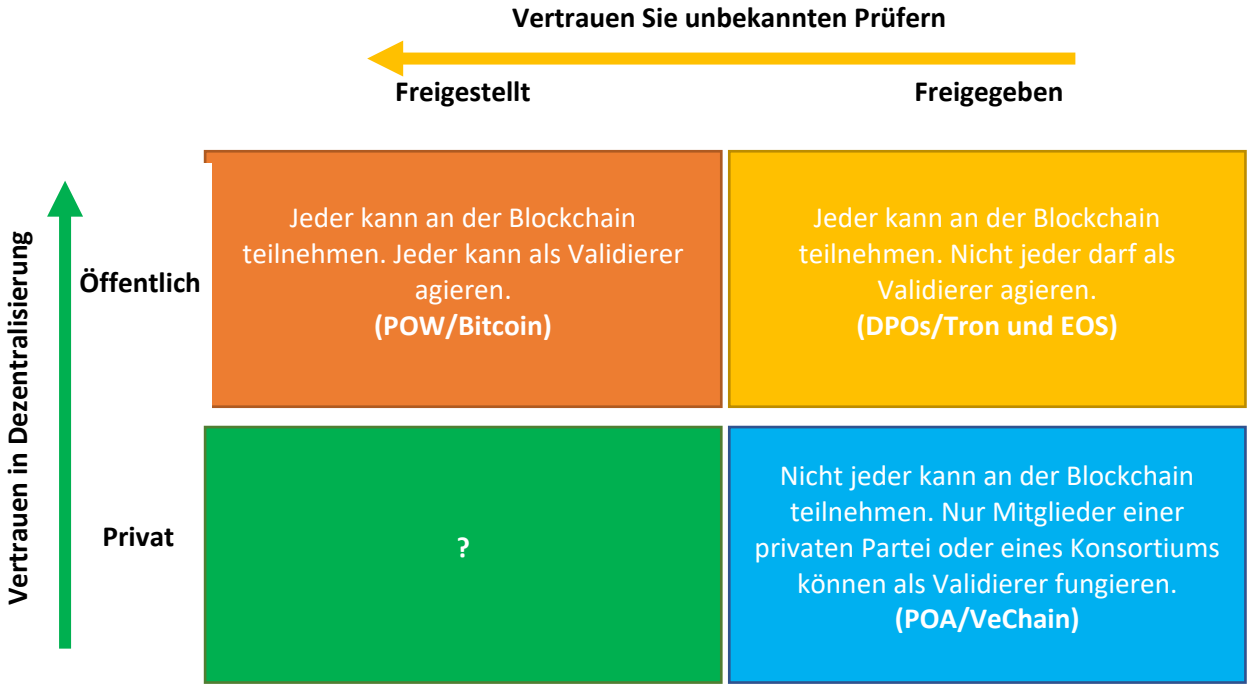


Figure 8:Ein Überblick über verschiedene Blockchain-Typen, ausgedrückt in „Permissionless“, „Permissioned“, „Private“ und „Public“ (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 9).

Da das Vertrauen in das System mit öffentlichen Blockchains liegt, wird der ‘Wer Daten in die Blockchain schreibt’, ‘wer Daten aus der Blockchain liest’ und ‘wer die Blockchain aufrechterhalten darf’ als von geringerer Bedeutung angesehen. Dies wiederum führt

dazu, dass die meisten öffentlichen Blockchains nicht mehr zugangslos sind. Aufgrund der geringen Hürde, dem Netzwerk beizutreten, sind solche Blockchains am dezentralsten.

Die Teilnehmer bestimmen die Funktionsweise der Blockchain entsprechend den Gruppenmotiven wie Offenheit, Neutralität und Freiheit. Innerhalb der öffentlichen Blockchain kann jeder auch an der Entscheidungsfindung zu allen Governance-Fragen teilnehmen.

Eine **öffentliche** Blockchain ist für Unternehmen nicht immer wünschenswert, vor allem in einem stärker regulierten Umfeld, in dem unter anderem erwartet wird, dass sie die Identität aller Parteien kennen, die Daten an die Blockchain schreiben.

Diese zentrale Partei hat oft eine Reihe von Knoten eingerichtet, die sich selbst verwalten und die Blockchain am Laufen halten. Im extremen Fall hat die Partei einen einzigen Knoten, auf dem die Blockchain läuft. Gegenüber einem zentralen Netzwerk, das ebenfalls ein SPOF ist, bietet dies jedoch keine Vorteile.

Die Wahl zwischen den verschiedenen Blockchains-Typen beeinflusst die Kontrolle der Organisation. Je mehr Vertrauen in die dezentrale Natur der Blockchain besteht, desto einfacher ist die Teilnahme. Je mehr Vertrauen es gibt, dass Validatoren als Unbekannte am Konsensaufbau teilnehmen können, desto transparenter wird das System. Schließlich kann jeder einen vollständigen Node ausführen und dabei helfen, alle Daten zu validieren. Aufgrund der dezentralen Natur verfügen solche Systeme oft über viele Validatoren und haben zum Teil auch deshalb noch Skalierbarkeitsprobleme. Auch solche Blockchains sind relativ teurer als die weniger dezentralen und genehmigungsfreien Varianten.

Langfristig wird jedoch erwartet, dass öffentliche Blockchains zunehmend effizienter werden, so dass sich mehr professionelle Parteien für solche Blockchain entscheiden werden. Diese Blockchains müssen dann so angeordnet werden, dass die Rollen, die die Teilnehmer für Geschäftsanwendungen übernehmen können, gut definiert sind und den Geschäftsanforderungen entsprechen. So können Unternehmen, die auf „permissionless“ öffentlichen Blockchains arbeiten, Daten durch Zero-Knowledge-Proofs anonymisieren und Teilnehmer auf Anwendungsebene aufgefordert werden, ihre Identität zu zeigen.

3.3 Plattformen und Konsortien

Eine Blockchain, in der verschiedene Unternehmen und Dritte zusammenarbeiten, ohne dass ein zentraler Nutzer diese Blockchain kontrolliert, wird als Enterprise Blockchain bezeichnet. Um eine solche Enterprise Blockchain aufzubauen, nutzen Unternehmen Blockchain-Plattformen. Diese **Plattformen** ermöglichen es Ihnen, Anwendungen mit bestimmten Technologien zu schreiben. Um diese Plattformen herum wurden verschiedene Partnerschaften organisiert. Plattformen sind der dritte und letzte Weg, wie wir verschiedene Arten von Blockchains hier betrachten.

Blockchain **-Plattformen** ermöglichen es ihrer Anwendung, mit anderen Anwendungen zusammenzuarbeiten, beispielsweise in ihrer eigenen oder gemeinsam genutzten Programmiersprache, Dokumente werden gespeichert oder gemeinsam genutzt, und der Zugriff auf ein bestimmtes Netzwerk wird erlangt. Die beiden prominentesten Plattformen sind derzeit Ethereum und Hyperledger, wobei Corda die drittprominenteste ist.

Jede Plattform hat ihre eigenen einzigartigen Funktionen. Ethereum ist im Allgemeinen eine öffentliche Blockchain, Hyperledger bietet Plug-and-Play-Module mit verschiedenen Technologien und Corda ist dezentrale Ledger-Technologie, die sich mehr auf Finanzdienstleistungen spezialisiert hat. Mitglieder, die einer Partnerschaft auf einer Plattform beigetreten sind, sind oft auch Mitglieder von Partnerschaften auf anderen Plattformen. Die Plattformen selbst sind Open Source. Ethereum und Hyperledger streben in den letzten Jahren eine stärkere Integration zwischen den beiden an, um Blockchain-Systeme überall in Unternehmen zu implementieren.

Wenn es sich bei Partnerschaften um eine Form der Zusammenarbeit von Blockchains handelt, in der die neuen Marktteilnehmer bekannt sind und ihnen bestimmte Rollen zugewiesen werden, arbeiten sie in Strukturen, die verwirrend auch Konsortien genannt werden (siehe oben Absatz 3,2), aber aus einer anderen Perspektive, die dann nur Merkmale öffentlicher und privater Blockchains vermischt. Die kooperierenden Parteien können von staatlichen Stellen, Interessengruppen und Unbekannten bis hin zu Lieferanten, Kunden und direkten Wettbewerbern variieren.

Darüber hinaus helfen Konsortien hier Parteien dabei, vier Hauptherausforderungen zu meistern, die Unternehmen bei der Implementierung von Blockchain bewältigen müssen. Erstens teilen Konsortien Wissen über (supra) nationale Aufsichtsgremien und pflegen einen aktiven Kontakt zu diesen. Konsortien helfen dann unter anderem dabei, die Gesetze und Vorschriften zu klären.

Zweitens helfen Konsortien Organisationen, die Risiken auf verschiedene Parteien zu verteilen, indem sie Ressourcen teilen, um Blockchain-Systeme zu entwickeln.

Drittens liefern Konsortien durch Zusammenarbeit eine kritische Masse, um ein stabiles Performing-System einzuführen.

Und viertens bieten Konsortien die Möglichkeit, neue dezentralisierte Partnerschaften mit vertrauenswürdigen und nicht vertrauenswürdigen Parteien aufzubauen, ohne dass teilnehmende Organisationen zu viel von ihrer Autonomie verlieren. Dies bietet Wettbewerbern beispielsweise Standardverfahren zum Erstellen und Austauschen von Daten untereinander oder zur Zusammenarbeit mit Kunden und Lieferanten des jeweils anderen Anbieters. Da sich die beteiligten Parteien jedoch gegenseitig vertrauen müssen, um zusammenarbeiten zu können, setzen sie ihr Vertrauen in der Regel durch Verträge über gemeinsame Ressourcen, Entscheidungsfindung, Sanktionen, vertrauliche Informationen und den gegenseitigen Datenaustausch durch. Diese Verträge neigen dazu, die Hürde für den Beitritt zu einem Konsortium zu erhöhen, ebenso wie die Hürde für den Austritt aus einem Konsortium. Es ist wahrscheinlich, dass verschiedene Konsortien nebeneinander existieren. Dabei spielt die Interoperabilität innerhalb und zwischen Konsortien eine wichtige Rolle.

4 Kryptowährungen und Token

Eine der großen Erfindungen von Satoshi Nakamoto ist die Kombination von bereits vorhandenen Technologien mit einem Belohnungssystem, das ein dezentrales Netzwerk am Laufen hält. Wie bereits erwähnt, wird die Belohnung in Bitcoins an den Miner gezahlt, der einen Block produziert.

Token in unserer heutigen Gesellschaft sind als Gutscheine und Münzen bekannt - zum Beispiel Treuepunkte, Casino-Münzen und Geschenkkarten. Wir kennen auch Token in der IT, die Zugriffsrechte für ein Netzwerk zur Ausführung einer Aufgabe oder als Darstellung von Rechten für zugrunde liegende Ressourcen bereitstellen. Ein Bitcoin, den man auch als kryptographisches Token sehen könnte, unterscheidet sich von den oben genannten Token in dem Sinne, dass es Wert darstellt. Kryptografische Token können aus vielen Gründen verwendet werden. In der Blockchain-Landschaft dienen sie vor allem einem **Internet of Value** , in dem Werte über ein dezentrales Internet vertrauensvoll ausgetauscht werden können.

Mit kryptografischen Token wie Bitcoin können Sie bezahlen oder sparen, aber Sie können auch noch einen Schritt weiter gehen. Bitcoin kann beispielsweise durch die Bereitstellung von Computerleistung zur Herstellung neuer Blöcke verdient werden. Dadurch entsteht eine Wirtschaft, in der mehrere Teilnehmer ermutigt werden, im Austausch gegen Krypto zur Sicherung des Netzwerks beizutragen. Die Verwendung von kryptografischen Token, um bestimmte Verhaltensweisen der Teilnehmer zu stimulieren und falsches Verhalten durch ein Konsensprotokoll zu bestrafen, ist Teil der **Krypto-Ökonomie**.

In diesem Kapitel beschreibt 4.1 zunächst die **Krypto-Ökonomie** als das Basiskonzept, bei dem Token eine nützliche Rolle spielen. Anschließend beschreibt Kapitel 4.2 **was Token** sind und wie sie **klassifiziert** werden. Diese Klassifizierung umfasst Dapp-Token und Kryptowährung, aber auch den Unterschied zwischen fungiblen und nicht fungiblen Token und wie sie die Kryptoökonomie unterstützen. Das Kapitel wird in Abschnitt 4.3 mit einem Überblick darüber fortgesetzt, wie Token für das Fundraising durch ein Initial Coin Offering, ein Security Token Offering und ein Initial Exchange Offering verwendet werden können.

4.1 Kryptoökonomie

Kryptografische Token dienen unterschiedlichen Zwecken, wie dem Zugriff auf ein System oder der Darstellung von Informationen aus einem physischen Objekt. Dadurch erhalten die Token einen **Wert**, der zwischen verschiedenen Parteien innerhalb einer Blockchain ausgetauscht werden kann. Diese neue Disziplin, die den Transfer von Reichtum durch Computernetzwerke, Kryptographie, Spieltheorie und Softwareentwicklung sowie die Schaffung und den Konsum von Reichtum untersucht, wird **Krypto -Ökonomie** genannt.

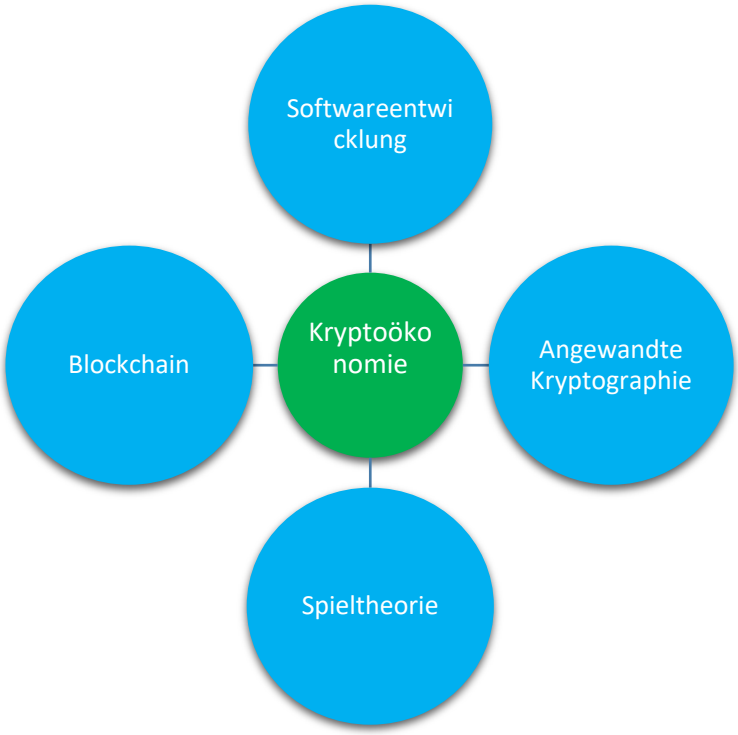


Figure 9:Multidisziplinäre Aspekte der Kryptoökonomie. (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 10).

Computernetzwerke sind mit bestimmten Regeln gestaltet, die als eine Art Gesetz für jeden, der daran teilnimmt, dienen. Diese Gesetze werden jedoch von privaten Parteien/Gemeinschaften entworfen und teilweise durch Software und nicht durch Regierungen durchgesetzt. Innerhalb dieser Gesetze werden dann Annahmen darüber getroffen, wie sich Teilnehmer im Netzwerk verhalten und sich nicht verhalten können.

Die zentrale Idee hinter der Krypto-Ökonomie innerhalb **von Blockchain** ist, dass Protokolle entwickelt werden, die Menschen dazu ermutigen, sich so am Netzwerk zu beteiligen, dass der **Wert** des Netzwerks **für die Teilnehmer maximiert** wird. Der Netzwerkwert kann nur maximiert werden, wenn das Netzwerk und die darin gespeicherte Transaktionen ebenfalls **gesichert** sind. Um dies zu erreichen, wird **Kryptographie** verwendet, um Transaktionen innerhalb des Netzwerks über Software wie z. B. Hash-Funktionen und digitale Signaturen zu sichern. Zusätzlich werden Prämien an Teilnehmer gezahlt, die zum Schutz des Netzwerks beitragen, z. B. durch Mining oder Abstecken. Die Kombination dieses Denkens wird beispielhaft in der Rolle von Bitcoin als Token dargestellt, der Menschen zur Zusammenarbeit anregt und so dazu beiträgt, ein selbstorganisierendes Krypto-Wirtschaftssystem zu erhalten. Die Krypto-Wirtschaft ist eine wichtige Voraussetzung, um die Idee eines nachhaltigen und vorzugsweise selbstorganisierenden Systems zu unterstützen, ohne dass die zentralen Parteien die Menschen dazu drängen, in einer bestimmten Weise zu handeln. Wichtig für diese Prämisse ist die **Spieltheorie,** eine Studie darüber, wie optimale Bedingungen in einem wettbewerbsorientierten Umfeld geschaffen werden, um die Teilnehmer immer dazu zu bringen, bei ihren Entscheidungen gutes Verhalten zu zeigen, da dies zu mehr Gewinn führt als schlechtes Verhalten. Eine Möglichkeit, Teilnehmer zu gutem Verhalten zu ermutigen, ist die Belohnung von Krypto-Token.

4.2 Klassifizierung von Blockchain-Token

Das Internet wurde zunächst eingerichtet, um Informationen miteinander auszutauschen. Dies ist auch als **Internet der Informationen** bekannt. Innerhalb dieser ist es schwierig, Werte ohne einen vertrauenswürdigen Vermittler zu speichern und zu bewegen (Tappscott, 2016), der hauptsächlich prüft, ob derselbe Wert wie der Euro nicht zweimal ausgegeben wird (Satoshi, 2008, S. 2). Mit dem Aufkommen von Blockchain können Sie die Notwendigkeit von Vermittlern umgehen und Peer-to-Peer-Werte direkt handeln. Dies wird auch als **Internet of Value** bezeichnet. Krypto-Token spielen eine entscheidende Rolle bei der Entwicklung dieses Krypto-Wirtschaftssystems. Ein Krypto-Token kann auf einer Blockchain erstellt werden und stellt auch einen handelbaren digitalen Vermögenswert dar. Manchmal werden Token in einem ICO oder einem STO erstellt, um ein Projekt zu finanzieren. Der Prozess der Tokenerstellung wird Tokenisierung genannt. Durch den Handel mit diesen Token können Sie das Eigentum an den zugrunde liegenden Vermögenswerten übertragen.

Es gibt verschiedene Perspektiven, wie man Krypto-Token betrachtet. Das folgende Format umfasst alle verschiedenen Token mit dem zusätzlichen Vorteil, dass die zukünftige Rolle von Token in einem Internet of Value adressiert wird:

Anwendung	Token zum Vorteil der Anwendung	Token als Assets
Fungible Token	Netzwerk: Ether dApp: Augur	Vorteil: Gold Wertpapier: Teil Shell Kryptowährung: Bitcoin
Nicht fungible Token		Asset: Geburtsurkunde Wertpapier: Privatkredit

Figure 10: Token im doppelten Format. Zum einen, um Token zu unterscheiden, die im Blockchain-Netzwerk verwendet werden, um vs zu halten, um Eigentum zu demonstrieren und zu übertragen. Auf der anderen Seite, um Token zu unterscheiden, die austauschbar vs nicht austauschbar sind. (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, 2021, Kapitel 10).

Beachten Sie, dass Token eine duale Tokenstruktur haben können, in der sie mehrere Zwecke gleichzeitig erfüllen. Bitcoin wird beispielsweise als Netzwerk- oder Anwendungstoken und als Asset verwendet.

Token zum Vorteil der Anwendung werden auf der grundlegendsten Ebene verwendet, um Menschen zu ermutigen, an einer Blockchain-Anwendung teilzunehmen und dieses Netzwerk in Gang zu halten. Dieses Netzwerk kann als Plattform dienen, auf der dezentrale Anwendungen, dApps, ausgeführt werden. Hier **werden Netzwerk-Token** verwendet, um

Teilnehmer für die Arbeit zu belohnen, die sie zur Aufrechterhaltung des Netzwerks leisten. Diese Token nehmen einen zentralen Platz innerhalb einer Blockchain ein, weil sie als organisatorische Idee ein verteiltes vertrauenswürdiges Netzwerk unterstützen und so das kryptoökonomische System einer Blockchain prägen. Neben einer Anwendung kann ein Netzwerk auch eine **Plattform** sein, auf der Anwendungen wie Ethereum oder Cardano mit ihren ETH- und ADA-Token ausgeführt werden, um einen Konsens zu erzielen und das Transaktionssystem zu belohnen. Wenn Sie das Denken einen Schritt weiter gehen, können Sie sehen, dass es innerhalb einer Blockchain die Wahl gibt, ein Token zu verwenden oder die Verwendung von Token alle zusammen zu ignorieren.

DApp-Token oder **Utility-Token** sind nur innerhalb ihrer eigenen Anwendung nützlich und werden für den Zugriff auf dieses Dienstprogramm verwendet. Sie sind außerhalb dieser Anwendung nicht von Nutzen. Sie können sie auch außerhalb der Anwendung tauschen. Sie sind jedoch nicht immer als Währung oder Share in einem Netzwerk programmiert. Zum Beispiel Siacoin (SC), wo Menschen SC verdienen können, wenn sie ihren freien Speicherplatz anderen im Netzwerk zur Verfügung stellen.

DApp-Token auf Ethereum werden gemäß dem **Ethereum Request for Comments 20** (ERC-20)-Protokoll erstellt. Das Protokoll definiert bestimmte Regeln und Standards im Zusammenhang mit der Ausgabe von Token im Ethereum-Netzwerk. Alle gemäß ERC-20 hergestellten DApp-Token sind einzigartig in ihrer Anwendung und können innerhalb des Ethereum-Netzwerks gehandelt werden.

Token zum Nutzen von Anwendungen unterscheiden sich von Token, die sich um die Erfassung und den Austausch von Werten innerhalb der Blockchain-Anwendungen drehen, mit denen sie den Besitz dieses Werts nachweisen und die Übertragung des Rechts auf diesen Wert ermöglichen, Token **als Vermögenswerte**. Dies können in Asset-Token, Security-Token und Krypto-Währungen unterteilt werden.

Asset Tokens stellen Aufzeichnungen über Rechte und Pflichten an dem zugrunde liegenden Vermögenswert wie Gold oder Öl, aber auch an ein Haus, eine Büroklammer oder Krypto-Sammlerstücke wie Game Avatare oder digitale Kunstwerke dar. Diese Tokens können vernachlässigbare bis sehr große zugrundeliegende Werte darstellen. Eine wichtige Voraussetzung für Asset-Token ist, dass die Identität des Eigentümers festgelegt werden kann. Asset-Krypto-Token bieten möglicherweise Vorteile, da sie programmiert werden können (**Smart-Token**) und mit geringen Transaktionskosten und hoher Sicherheit gehandelt werden können:

1. Sie können die Vermögensbestände leicht aufteilen und in kleinen Einheiten zur Verfügung stellen. Ein Beispiel für diese **Aufteilung** ist die Eigentumsrechte an der Mona Lisa in 1.000 Token zu verkaufen / leasen. Stichwort „Fractional Ownership“.
2. Sie können Rechte an dem kryptografischen Token programmieren und diese über Smart Contracts durchsetzen. Stellen Sie zum Beispiel Ihren Mona Lisa Token so ein, dass er nur an gemeinnützige Organisationen verkauft wird, oder programmieren Sie, dass ein Wiederverkauf automatisch eine 2 %-Provision an den ursprünglichen Verkäufer beinhaltet.
3. Sie reduzieren die Transaktionskosten beim Kauf und Verkauf, teilweise aufgrund der schnellen und billigen Mikrotransaktionen. Ein intelligenter Kühlschrank scannt beispielsweise für bestimmte Zeitintervalle den günstigsten Strom.

4. Sie können alle relevanten Informationen für die zugrunde liegenden Assets im Token aufzeichnen. Sie überprüfen zum Beispiel die früheren Besitzer der Gebrauchtmaschine, um die Sharing Economy zu verbessern.
5. Sie können ganz einfach selbst ein Asset erstellen, z. B. eine Eintrittskarte für ein Heimkonzert.

Kurz gesagt: Smart Tokens übertragen problemlos Wert, Informationen, Ideen, Rechte und Pflichten durch Smart Contracts.

Security-Token (Wertpapier-Token) stellen Anleihen, Aktien, Kredite, Futures, Optionen und andere verhandelbare finanzielle Vermögenswerte dar. Obwohl sie zu den Asset-Token gehören, werden sie separat erwähnt. Es können alle Arten von Rechten an Wertpapiertoken vergeben werden. Zum Beispiel das Recht, das Wertpapier nicht an jeden weiterzuverkaufen oder jemandem vorübergehend Stimmrechte im Unternehmen zu verleihen.

Kryptowährungstoken gehören ebenfalls zu Asset Tokens und werden aufgrund ihrer großen erwarteten finanziellen und wirtschaftlichen Auswirkungen separat behandelt. Bitcoin ist das bekannteste Beispiel einer Kryptowährung. In diesem Fall soll der Token als Geld fungieren. Langsam, aber sicher **erregen Stable Coins** Aufmerksamkeit, da sie mögliche Wege aufzeigen, den Wert von Krypto-Token zu stabilisieren und damit unter anderem als dezentrale Alternative oder Repräsentationsmöglichkeiten von fiat-Währungen dienen können. Stable Coins können mit mehreren Vermögenswerten wie fiat-Währung oder Gold oder Krypto-Münzen besichert oder gar nicht besichert werden.

Eine Reihe von Zentralbanken testet Stable Coins als eine so genannten **Zentralbank-Digitalwährung** (CBDC). Obwohl das CBDC Elemente von Blockchain verwenden kann, ist es nicht unbedingt eine Blockchain-Anwendung. Die CBDC stehen im diametralen Gegensatz zu den dezentralen Ursprüngen von Bitcoin, da ein CDBC eine zentral regulierte Währung ist.

Es stellt sich die Frage, wie Krypto-Token in einem Wirtschaftssystem, in dem der Austausch stattfindet, angewendet werden können. Eine Möglichkeit, dies zu tun ist, um Token Fungibility zu betrachten. Einige Token können leichter gegen eine andere ausgetauscht werden. Zum Beispiel kann eine 1 kg schwere Packung Mehl gegen eine weitere 1 kg schwere Packung Mehl ausgetauscht werden. Eine €10-Banknote kann auch gegen zwei €5-Banknoten eingetauscht werden. Gleiches gilt für **fungible Token**: die einzelnen Einheiten sind voneinander nicht zu unterscheiden und können untereinander ausgetauscht werden. Ein Beispiel ist Polkadot: 1 Polkadot-Token können gegen einen anderen und zwei halbe Polkadot-Token gegen 1 ganze Polkadot getauscht werden.

Im Gegensatz dazu sind **nicht-fungible Token (NFTs)** Token, die für sich einzigartig und daher knapp sind. Denken Sie beispielsweise an Personen, Länder- und Geburtsurkunden, die nicht gegen andere Personen, Länder- und Geburtsurkunden ausgetauscht werden können.

Insbesondere die Blockchain eignet sich gut, um diese Art von Token effizient zu erfassen und zu handeln, auch wenn die Token nur einen winzigen Wert darstellen und/oder in ihrer Art einzigartig sind. Dies ist wichtig, da es in einer digitalen Welt einfach ist, eine Kopie eines digitalen Gutes zu erstellen. Wenn man also eine Marke als Repräsentation hat, gibt es nicht nur die Möglichkeit, Waren aus der realen Welt zu handeln. Es gibt Ihnen auch die Möglichkeit, jedem physischen gut eine authentische digitale Darstellung zu geben, so klein es auch sein mag, und sie zu handeln. Außerdem ist die Schaffung eines knappen Tokens wirtschaftlich

interessant, wenn Sie den Preis angesichts des adagio: 'Je geringer das Angebot an Token, desto größer die Knappheit und damit die Chance auf einen höheren Preis".
Eine Reihe der Vorteile, die bereits für Asset-Krypto-Token wie die Fraktionierung von Eigentumsrechten und die Erstellung von Smart-Token erwähnt wurden, unterstützen den Anwenderfall für nicht fungible Token, da sie zu höchst individuellen Darstellungen jedes (zu digitalisierenden) Objekts werden können, das zu niedrigen Transaktionskosten erstellt und gehandelt wird (alle können eingeben, alle können teilnehmen) sicheres Netzwerk, das Internet of Value. Ein Internet, mit dem sich die Auswirkungen des individuellen Handelns auf die Umwelt transparent messen und jedes Individuum dazu bringen könnte, die Ziele einer größeren Gemeinschaft zu unterstützen.

In der Zukunft könnten theoretisch alle Vermögenswerte, die jemand besitzt oder verwendet „tokenisiert" werden und diese Token können Bruchteile des Ganzen abbilden und zudem anderweitig als Zahlungsmittel oder Finanzierungsmittel dienen.

4.3 Token für den Erwerb von Fonds

All diese separaten Token können dann auf verschiedene Weise verwendet werden, um Gelder zu erwerben: Von Initial Coin Offerings (ICO) über Security Token Offerings (STO) und Initial Exchange Offerings (IEO) bis hin zu Initial DEX Offerings (IDO).

Das **Initial Coin Offering** (ICO) wurde in der Vergangenheit hauptsächlich dazu verwendet, im Internet Mittel für Blockchain-Projekte zu sammeln. Insbesondere Ethereum war die primäre Blockchain, um Token zu erstellen und zu verkaufen. Zu Beginn des ICO-Trends kam es zu einer erheblichen Anzahl von Missbrauchsfällen, auch weil die ICO-Verfahren außerhalb des Schutzes nationaler Gesetze und Vorschriften stattfanden.

Das Token Offering (STO) wurde für den gleichen Zweck konzipiert wie ein ICO, jedoch jetzt mit der Berücksichtigung eines Tokens als Sicherheit mit Standardprotokollen, Stimmrechten und mehr im Einklang, wenn auch nicht vollständig, mit mehreren nationalen Wertpapieren und Börsengesetzen und -Vorschriften. Der STO hat sich im öffentlichen Raum bisher nicht besonders erfolgreich erwiesen. Außerdem wurden neue, stärker regulierte, aber immer noch 'offene" Alternativen wie das **Initial Exchange Offering** (IEO) und **das Initial DEX Offering** (IDO) konzipiert. Hier bieten zentralisierten oder dezentralen Austausch wie Binance oder Uniswap Start-ups die Möglichkeit, Crowdfunding über ihre Zwischenplattform zu erhalten, die in der Regel KYC- und AML-Checks übernimmt.

Der Trend zur Gestaltung eines dezentralen Internet of Value durch die Gemeinschaft scheint sich in einem Wirbelwind von aufeinanderprallenden Idealen, Ideen, technischen Möglichkeiten, Fehlern, wunderbaren Unfällen und Ausdauer fortzusetzen.

5 Nutzen und Anwendungen von Blockchain

In diesem Kapitel werden drei Beispiele für den Einsatz und die Anwendungen von Blockchain aufgeführt. Vorangestellt wird eine Einführung, wie Unternehmen strategisch über relevante Elemente ihres Geschäftsmodells und die Chancen,die die Blockchain bietet, nachdenken können. Das Kapitel endet mit bestimmten Punkten, auf die ein Unternehmen achten sollte, sobald es Blockchain implementiert hat.

5.1 Geschäftsmodelle

Blockchain bietet in der Regel einen Mehrwert innerhalb von Geschäftsmodellen und Geschäftsökosystemen, in denen digitale Daten und Technologien erstellt und zwischen Partnern geteilt werden können. Blockchain ist eine digitale Technologie, die zu diesen digitalen datengetriebenen Geschäftsmodellen passt und Partnern die Zusammenarbeit ermöglicht, wo sie es vorher nicht konnten. Diese Partner können nun ihr Vertrauen 'in das System' setzen, wo sie sich vor Blockchain nicht von Anfang an gegenseitig zur Zusammenarbeit vertrauten. In diesem Sinne ist Blockchain vor allem eine Chance, Ökosysteme zu wachsen und zu digitalisieren, die digitale **datengetriebene Geschäftsmodelle** nutzen.

Für Geschäftsmodelle ist das **dezentrale Geschäftsmodell Canvas**[6][7] relevant sowie Dezentralisierung zentral für die freistellungslosen Blockchain-Anpassungen der Öffentlichkeit. In diesem speziellen Bildschirm haben Token-Inhaber eine zentrale Position, da sie über mehrere Rollen verfügen, z. B. Benutzer, Prüfer, Mitarbeiter und/oder Eigentümer. Diese Art 'neuen' Denkens gibt eine Vorstellung von den potenziellen neuen Möglichkeiten, die die öffentlich zugängliche Blockchain mit sich bringt, da Parteien, die sich nicht kennen, alternativ eine kostengünstiges System einrichten und nutzen können, um Daten auszutauschen und zu verifizieren, während sie sich nicht kennen.

Die Governance wird dann dezentral von der Öffentlichkeit eingerichtet, die Daten dezentral gespeichert und die Kommunikation zwischen den verschiedenen Parteien erfolgt Peer-to-Peer. Dies ist die offenste Form einer Blockchain. Es steht einem Unternehmen frei, die Bausteine von Blockchain selbst anzupassen. Mit einem zentralisierten System trifft eine zentrale Organisation die Entscheidungen.

In einem dezentralen Geschäftsmodell werden die Umsätze häufig unter denjenigen aufgeteilt, die am meisten zum Netzwerk beitragen und die Kosten für die Nutzung der Plattform sind sehr gering – zum Beispiel mit der Social Blogging Blockchain-Plattform Steemmit.

5.2 Blockchain-Anwendungen für Unternehmen

In diesem Absatz werden drei Anwendungen in vier verschiedenen Branchen vorgestellt und anhand der komparativen Vorteile verglichen, die Blockchain in diesen Anwendungen bietet. Die vier Anwendungen sind:

[6] https://canvanizer.com/new/decentralized-business-model-canvas
[7] https://medium.com/mvp-workshop/decentralized-business-model-canvas-1-9daf6e4bc9fe

1. Regierung und öffentliche Güter von Lantmäteriet.
2. Herstellung durch BMW.
3. Digitale Geldbörse von Singapore Airlines.

Eine hilfreiche Übersicht, die helfen soll, zu verstehen, wo viele Blockchain-Sektoren Blockchain implementiert wurde, stammt aus der unten stehenden Forschung unter 67 Blockchain-Unternehmensnetzwerken und den Sektoren, in die diese Implementierungen fallen (Rauchs, Blandin, Bear, McKeon, 2019).

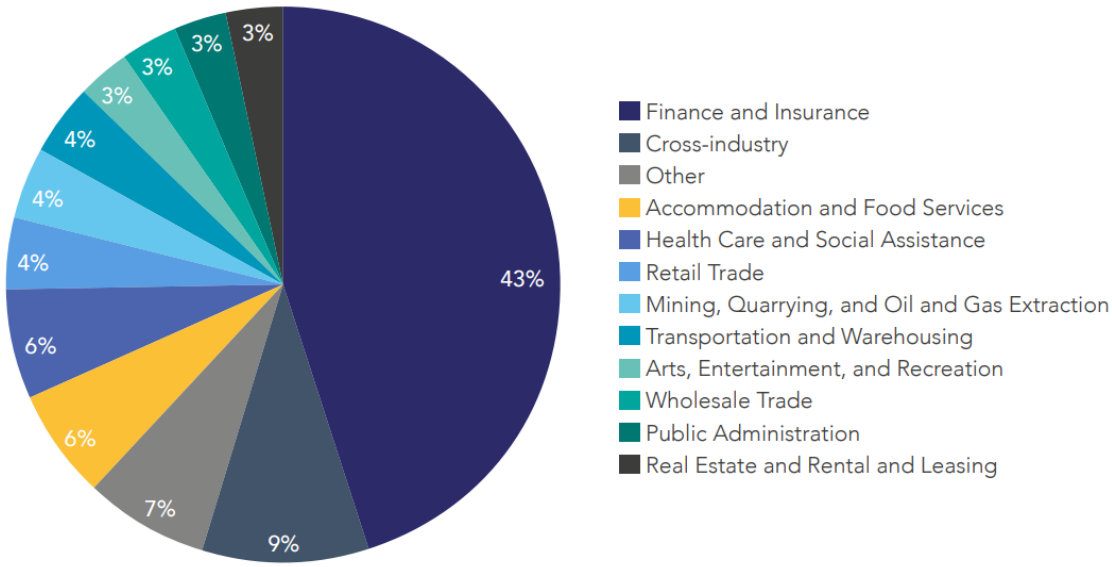


Figure 11: Überblick über 67 Blockchain-Netzwerke in Unternehmen und in welche Sektoren sie fallen (Quelle: Rauchs, Blandin, Bear, McKeon, 2019).

Das erste Beispiel betrifft den **Sektor der Regierung und der öffentlichen Güter**. Die schwedische **Lantmäteriet** hat die Aufgabe, das Katastersystem zu erhalten, Geodaten bereitzustellen und die Landregistrierung durchzuführen. Es besteht Bedarf an mehr Transparenz und Effizienz des Projekts, da verschiedene Partner zusammenarbeiten und manuelle Prozesse verwenden, die ineffizient und fehleranfällig erscheinen.

Lantmäteriet testete daher eine Lösung, um zu sehen, wie Akteure wie Immobilienkäufer, Verkäufer, Makler, Finanzdienstleistungen, Rechtsanwälte, Pensionskassen und das Lantmäteriet können auf einer effizienten Online-Plattform zusammenarbeiten, die über digitale Geräte sofortige Transparenz einer Anfrage bietet. Das Projekt wurde als inkrementelles Projekt (2015-2019) in einer kontrollierten Box-Situation mit vertrauenswürdigen Partnern eingerichtet, ohne jedoch kurzfristig ehrgeizig Dezentralisierung zu betreiben. Es wurde ein klarer Fokus daraufgelegt, mit dem Register der Landtitel niedrig hängende Früchte zu pflücken und gleichzeitig eine Grundlage für zukünftige Dienstleistungen zu schaffen.

Während des Projekts kamen rechtliche Fragen auf, die überwunden werden mussten. Zum einen musste Lantmäteriet überlegen, wie mit dem Recht von Einzelpersonen auf Kontrolle ihrer eigenen Daten umzugehen ist (EU-Datenschutzgrundverordnung - DSGVO),

einschließlich der Möglichkeit, diese zu schützen und zu löschen, wo dies gewünscht und möglich ist. Sowie darüber, wie digitale Signaturen als rechtsverbindliche Signaturen innerhalb der EU (eIDAS-Richtlinie) oder der Status digital signierter (e-)Verträge auf Basis von Blockchain verwendet werden können.

Der Verkauf von Landtiteln war ehrgeizig, da verschiedene Parteien einen neuen Prozess und ein neues Spiel mit einer neuen technologischen Lösung schufen. Die Blockchain-Lösungen umfassten sowohl private, geschlossene, genehmigte Blockchain-Systeme als auch ein verteiltes öffentliches Netzwerk. Die private Blockchain befindet sich im Staatsbesitz, wird von einer begrenzten Anzahl von Knoten von vertrauenswürdigen Vermittlern betrieben und steht unter der Aufsicht der schwedischen öffentlichen Regierung. Dieses System arbeitet mit ChromaWay und dem privaten Netzwerk der Interessengruppen zusammen. Es nutzt Smart Contracts, die praktische byzantinische Fehlertoleranz und Proof-of-Work-Konsensmechanismen, abschaltbare und abschaltbare digitale Identitäten über eine Handy-App und keine Token.

Die Urkunde bleibt bei Lantmäteriet registriert und wird aufgrund der früheren Probleme mit der DSGVO nicht an eine öffentliche Blockchain übertragen. Verträge werden manuell unterzeichnet und über Hashes auf die Blockchain gesetzt. Die ursprünglichen Verträge befinden sich auf dem Server mit anderen Parteien, diese Informationen haben Backups. Telia bietet eine mobile App-ID-Lösung an, mit der sich Personen registrieren können, ohne ihre schwedische Dienstnummer zu veröffentlichen. Diese Registrierungen werden über einen Hash auf der Bitcoin Blockchain gespeichert und verifiziert. Digitale personenbezogene Daten können entfernt werden, wenn eine Person dies wünscht und es gesetzlich nicht erforderlich ist, öffentliche Informationen zu sein.

Die wichtigsten Vorteile waren die Sicherheit der Verwendung der Blockchain-Technologie sowie die betriebliche. Was Letzteres betrifft, da sich der Zeitrahmen für die Registrierung eines Grundstücks von 4-6 Monaten auf wenige Tage bewegte. Außerdem waren Einsparungen von €100 Millionen pro Jahr durch weniger Fehler und Wartung geplant (Kairos Future, 2017). Dies reduziert dann die Risiken eines Vertrags mit unklaren Eigenschaften, betrügerischen Daten oder Chancen, Eigentum zu stehlen. Der Audit-Trail für den Kunden, den Wirtschaftsprüfer als Gesetzgeber, wurde ebenfalls transparent. Zudem stärkte das Ökosystem seine gegenseitigen Prozesse und den Datenaustausch, ohne sein zentrales Service- und Geschäftsmodell zu stark zu umgestalten. Und nicht zuletzt erhöhte die öffentliche Zugänglichkeit das Vertrauen in den Prozess und die Parteien. Nach dem Test könnte das System auf Parteien wie Versicherer, Notare und andere lokale Behörden ausgeweitet werden.

Das Projekt wurde im Jahr 2019 abgeschlossen und zeigte, dass die Plattform-Architektur funktioniert hat. Mats Snäll, Chief Innovation Officer bei Lantmäteriet, erklärte jedoch: „Es wurde nie in das Produktionssystem des Grundbuchs integriert“, da eine Gesetzesänderung erforderlich wäre, bevor das System in Zukunft erweitert werden könnte. (Baraniuk, 2020). Wahrscheinlich deutet dies auf die Herausforderung hin, Benutzeridentitätsdaten in der öffentlichen Blockchain zu veröffentlichen.

Andere Forschungen weisen auch auf die Richtung einer ‘fundamentalen Veränderung der Governance-Struktur hin, wie die Rolle des Lantmäteriiet’, die speziell für die Immobilienökosysteme ein zugrundeliegendes Motiv geschaffen haben könnte, um weitere Fortschritte des Projekts einzufrieren (Schnuer, 2020).

Währenddessen nutzt Lantmäteriet seine Lehren, um mit Bockchain weiter zu experimentieren. Zum Beispiel die gemeinsame Regierungsaufgabe mit DIGG, wo es darum geht, ‘eine Modell- oder konzeptionelle Lösung zu finden, wie man Vertrauen in die Automatisierung mit KI und anderen neuen Technologien wie der Blockchain-Technologie schafft“ (AI Sweden, Lantmäteriet, 2020).

Das zweite Anwendungsbeispiel Blockchain betrifft BMW im **Fertigungssektor. Die Geschäftsmodelle der Automobilindustrie müssen sich unter** immer umweltbewussten Bedingungen mit Technologien der 4. Industriellen Revolution wie Elektrifizierung und autonomen Systemen auseinandersetzen.

BMW versucht in diesem Beispiel zu verstehen, wie eine digitale Identität für Autos genutzt werden kann, um die Nutzung anderer Technologien und Konzepte der 4. Industrial Revolution zu ermöglichen. Insbesondere die Datenschutz-/Sicherheitsprobleme einer konstanten Internetverbindung von Auto und Benutzer sowie die Notwendigkeit, diese Daten sicher zu speichern. Dieser sichere Datenaustausch zwischen Geräten, der sichere digitale Identitäten garantiert, ist das, was Blockchain potenziell auf den Tisch bringt und BMW damit einen Einstieg in den Car-Sharing-Economy-Markt bietet.

BMW hat eine Reihe von Carsharing-Apps wie Share Now getestet, bei denen die digitale Identität beider Fahrzeuge als Nutzer einbezogen werden kann. Diese kombinierten digitalen Identitäten im Automobilbereich können beispielsweise registrieren, wann Benzin getankt wird oder wo das Auto geparkt wird. Diese Art von Informationen kann dann in Geschäftsmodellen verwendet werden, in denen die Automobilhersteller zusammen mit oder ohne Vermittler personalisierte Dienstleistungen wie Schadenversicherung, autonome Autofahrten anbieten oder ihr Autoerlebnis im Allgemeinen verbessern.

In diesem speziellen Beispiel experimentierte BMW jedoch mit einem einfacheren Projekt, bei dem der Fokus ausschließlich auf die ID des Fahrzeugs und seine gespeicherten Daten lag, also nicht auf den Nutzer. Die Idee ist, dass mögliche Käufer von gebrauchten BMW wäre in vertrauenswürdigen Daten über die Kilometerstand, Unfallhistorie, Service-Geschichte und andere Informationen des Autos interessiert. Ein potenzieller Verkäufer könnte diese Daten mit einem potenziellen Verkäufer oder seinem Versicherer teilen, BMW könnte die Informationen nutzen, um sein Geschäftsmodell zu verbessern, wie es zum besseren Service für seine Kunden zu nutzen.

Um diese Lösung zu schaffen, arbeitete die BMW Startup Garage mit Blockchain-Start-ups, in diesem Fall mit VeChain, zusammen. Zudem nutzt BMW die Ergebnisse zur Entwicklung eines Fahrzeugausweises, einem ersten Schritt zu einer Fahrzeugidentität (VID), die die Mitglieder der Mobility Open Blockchain Initiative (MOBI) gemeinsam nutzen können. MOBI ist ein Blockchain-Konsortium, das gemeinsam Blockchain-Standards entwickelt.

Aus der Zusammenarbeit mit VeChain entstand die **VerifyCar App** . VeChain ist eine dezentrale autonome Organisation mit einem zentralen Leitungsgremium, das die Proof-of-Authority-Konsensus-Methode und verschiedene Token auf seiner öffentlichen VeChain Blockchain verwendet.

Die VID hat eine eindeutige ID auf dieser Blockchain. Die App erfasst in regelmäßigen Abständen Daten (über SIM-Karten im Auto und Machine-to-Machine-Kommunikation), die auf der VeChain Blockchain verifiziert werden: VeChain speichert nur den Verweis auf die

Daten, die Daten verbleiben auf dem Fahrzeug selbst. Die erfassten Fahrzeugdaten enthalten sowohl statische Informationen wie Typ und Produktionsdatum des Fahrzeugs als auch dynamische Informationen wie die Anzahl der gefahrenvollen Kilometer. Wenn ein Autobesitzer Daten mit einer anderen Partei teilen möchte, nutzt er die VerifyCar App, um die Daten einschließlich der Referenzen auf der Blockchain anzuzeigen, um zu zeigen, dass es sich um die tatsächlichen Daten handelt, die auf dem Fahrzeug gespeichert sind.

Die Absicht von BMW, keine Kontrolle über die VeChain Governance oder den Code zu haben. Ab 2022 wurde die App nicht mehr produziert.

Mit der Pilotphase dieser Lösung macht BMW einen kontrollierten ersten Schritt zur schrittweisen Integration der dezentralen Blockchain-Technologie. Wenn VerifyCar auch für Autos verwendet werden kann, warum dann nicht über einen VID-ähnlichen digitalen Personalausweis verfügen, um sicherzustellen, dass Autoteile nicht gefälscht werden, an welchem Standort gekaufte Rohstoffe in der Produktionslinie zu finden sind oder die Herstellungs- oder Transportbedingungen bestimmter von Ihnen bestellter Produktionsmaschinen verstehen? Entsprechend dieser Denkweise experimentiert BMW mit Blockchain, um auch eine **transparente Lieferkette** zu nutzen.

Im Jahr 2019 wurde beispielsweise das **PartChain** -Pilotprojekt für den Kauf von Front Lights mit Amazon Web Services, Microsoft Azure und Hyperledger Fabric Blockchain (Ledger Insights (2020, 31. März) auf andere Anbieter ausgeweitet. Dies ermöglichte es BWM, seine Komponenten und langfristig kritischen Rohstoffe ‘von der Mine bis zur Schmelze’ nachzuverfolgen. (BMW PressClub Global, 2020). Und zusätzlich ‘einfachere Zertifizierung und kürzere Zollverfahren’ zu gewährleisten (BMW, 2019).

Ein **letztes Beispiel ist die digitale Brieftasche von Singapore Airlines, KrisPay**. Singapore Airlines wollte die Loyalität seiner Kunden durch den Einsatz von Blockchain weiter steigern. Dies führte 2018 zur Stärkung des Vielfliegerprogramms KrisFlyer mit der digitalen Blockchain-Geldbörse von KrisPay.

Mit KrisPay können Kunden ihre KrisFlyer Flugmeilen gegen KrisPay-Meilen, Kryptowährungs-Token, eintauschen. Diese KrisPay-Token können bei verschiedenen Händlern wie Banken, Tankstellen und Geschäften eingespart/ausgegeben werden. Außerdem kann der Kunde andere Prämien sparen und eintauschen, z. B. mit der Kreditkarte der DBS (Development Bank of Singapore Limited), oder Meilen von Singapore Airlines sammeln, kaufen oder einlösen, z. B. für Upgrades von Flügen. Der Geldwert des KrisPay-Tokens selbst wird von Singapore Airlines diktiert. Die Lösung, die KrisPay hier anbietet, besteht darin, Kunden eine einfache Möglichkeit zu geben, ihre Prämien einzulösen, um zu verhindern, dass Meilen neben dem Speichern dieser Token im Händlernetzwerk verschwendet werden. Auf eine Art und Weise erhalten Kunden eine digitale Ergänzung/Alternative zu fiat-gestützten Währungen.

Die Funktionalität von KrisPay ist über eine App auf Ihrem Mobilgerät und sofortige POS-Transaktionen einfach zu bedienen. Um die Benutzerfreundlichkeit zu erhöhen, können die KrisFlyer Meilen innerhalb der Familie oder von autorisierten Nominierten übertragen werden.

Durch die Kombination von Blockchain-Geldbörsen und Kryptowährungen nutzt KrisPay Blockchain-Stärken wie Sicherheit für alle Nutzer, da die Registrierung der Transaktionen

manipulationssicher ist. Händler lassen ihre Transaktionen sofort genehmigen und aufschlussreich machen, ohne dass ein langsamer, teurerer Händler eingesetzt werden muss. Dies unterstützt den Abgleich von Token-Zahlungen zwischen den Händlern (und ihren Finanzverwaltungen) und gibt ihnen aktuelle Kundeninformationen.

KrisPay wurde mit KPMG Digital Village und Microsoft entwickelt. KrisPay ist ein privates Unternehmen von Singapore Airlines, das an einer Kombination von Microsoft Azure (ursprünglich basierend auf dem Ethereum-Protokoll) mit Azure-App- und Datenbankfunktionen arbeitet. Verschiedene Partner pflegen und verifizieren die Blockchain-Datenbank, so dass jeder die Kunden-/Transaktionsinformationen gleichzeitig zur Verfügung hat.

Microsoft kündigte an, seine Azure Blockchain 2021 außer Betrieb zu nehmen und Kunden bei der Migration zum Quorum Blockchain Service, einer weiteren Variante des Ethereum-Protokolls, zu unterstützen (Microsoft, 2021).

Die KrisPay-Token und das Portemonnaie wurden 2020 in einer neuen App, Kris+, kombiniert. Diese App nutzt außerdem Kundendaten, damit Singapore Airlines seinen Kunden einen besseren Service bieten und personalisierte Angebote anbieten kann, sogar basierend auf der geografischen Lage vom Mobiltelefon aus.

Möglicherweise kann das KrisPay-Guthaben für die Ticketausstellung, die Überprüfung Ihrer digitalen Identität oder als weiteres generisches Token verwendet werden, das gegen fiat-Währungen oder andere Treuepunkte getauscht werden kann.

Alle **diese Anwendungen** sind handhabbare, gut definierte Blockchain-Fälle, die im Rahmen einer größeren Vision in einer Umgebung, der die Initiatoren vertrauen und die sie kontrollieren, sorgfältig implementiert werden. Die Fälle zeigen Klarheit über die Elemente, die sie als Chance oder keine Chance ansehen, und verwenden einen schrittweisen Änderungsprozess, in dem sie den Aufwand von vorsichtigen ersten Schritten bis zur vollständigen Implementierung intensivieren.

Ihre Umgebung besteht aus stabilen Prozessen, einem bekannten Geschäftsmodell und vertrauenswürdigen Partnern, um mit den erprobten Aspekten der Technologie und ihren dezentralen geschäftlichen Auswirkungen zu experimentieren.

Es gab keinen Platz, um die Anwendung eines vollständigen dezentralen Geschäftsmodells zu zeigen. Wenn Sie ein Beispiel wünschen, lesen Sie unbedingt das Marktbeispiel für Augur-Prädikationen in Kapitel 16,5. (Lin Lim, Janse, 2021).

5.3 Wann ist die Blockchain-Implementierung sinnvoll?

Aus den vorherigen Beispielen ist klar, dass es bestimmte Bedingungen geben muss, um Blockchain erfolgreich umzusetzen.

Es gibt eine Reihe von Kriterien, die zu prüfen sind, um zu entscheiden, ob die Blockchain eine sinnvolle Anwendung für das Unternehmen ist. Diese Kriterien zielen darauf ab, Transaktionskosten mit Daten- oder Datenverkehr zu beseitigen oder Chancen mit Daten- und Datenverkehr zwischen Parteien zu schaffen. Als Faustregel können die Kriterien wie folgt zusammengefasst werden:

1. **Digitale Innovation** ist Teil der Strategie.
2. Verschiedene Parteien **teilen Daten**.
3. Diese Daten und ihre Transaktionen betreffen **den monetären Wert**.
4. Die Daten sind **vertraulich**.
5. Verschiedene Parteien bearbeiten Daten.
6. Die Daten müssen überprüft werden.
7. Es gibt eine **klare und ausreichende Kapitalrendite**, die berechnet werden muss.
8. Die Verifizierung ist **komplex, kostet und dauert immer** mehr.
9. Die Lösung für Blockchain ist die **einfachste Lösung**, um das Problem zu lösen.
10. Die Lösung beeinflusst die bestehende Organisationsstruktur.
11. Die Lösung wirkt sich auf den vorhandenen Workflow aus.
12. Die Lösung wirkt sich auf das bestehende Ökosystem aus.
13. Die technische Lösung ist in der Nähe von bestehenden Systemen oder kann in bestehende Systeme integriert werden.
14. Die Lösung ist datenintensiv, aber skalierbar. Denkbar sind Unterschiede von 1k, 10k, 100k, 1 Millionen oder> 10 Millionen Transaktionen pro Stunde.

Sobald die Möglichkeit besteht, Blockchain auf der Grundlage dieser Kriterien zu implementieren, kann man mit dem Verständnis der zugrunde liegenden Benutzerdienstprogramme fortfahren, die benötigt werden, sowie der Bausteine, aus denen diese Dienstprogramme bestehen. Der Baustein „Payment Token“ wirkt sich beispielsweise auf die Leichtigkeit, Geschwindigkeit und Transparenz von Zahlungstransaktionen aus. Weitere Beispiele für Bausteine sind Geldbörsen, Smart Contracts, dApps, Tokentypen, Orakel, und so weiter.

Derzeit konzentrieren sich die Auswirkungen von Blockchain in Unternehmen hauptsächlich auf Effizienz, Disintermediation und Registrierung. Am stärksten wirkt sich das auf die Zusammenarbeit aus, wenn neue Daten freigesetzt und erstellt werden. In Zukunft werden jedoch komplexe Blockchain-Implementierungen, die die Dezentralisierung und Integration von Ökosystemen vorantreiben, die größten Vorteile von Blockchain erwarten.

Der nachfolgende vereinfachte Entscheidungsbaum kann helfen, um die Nutzung eines Blockchain-Projekts einzuschätzen:

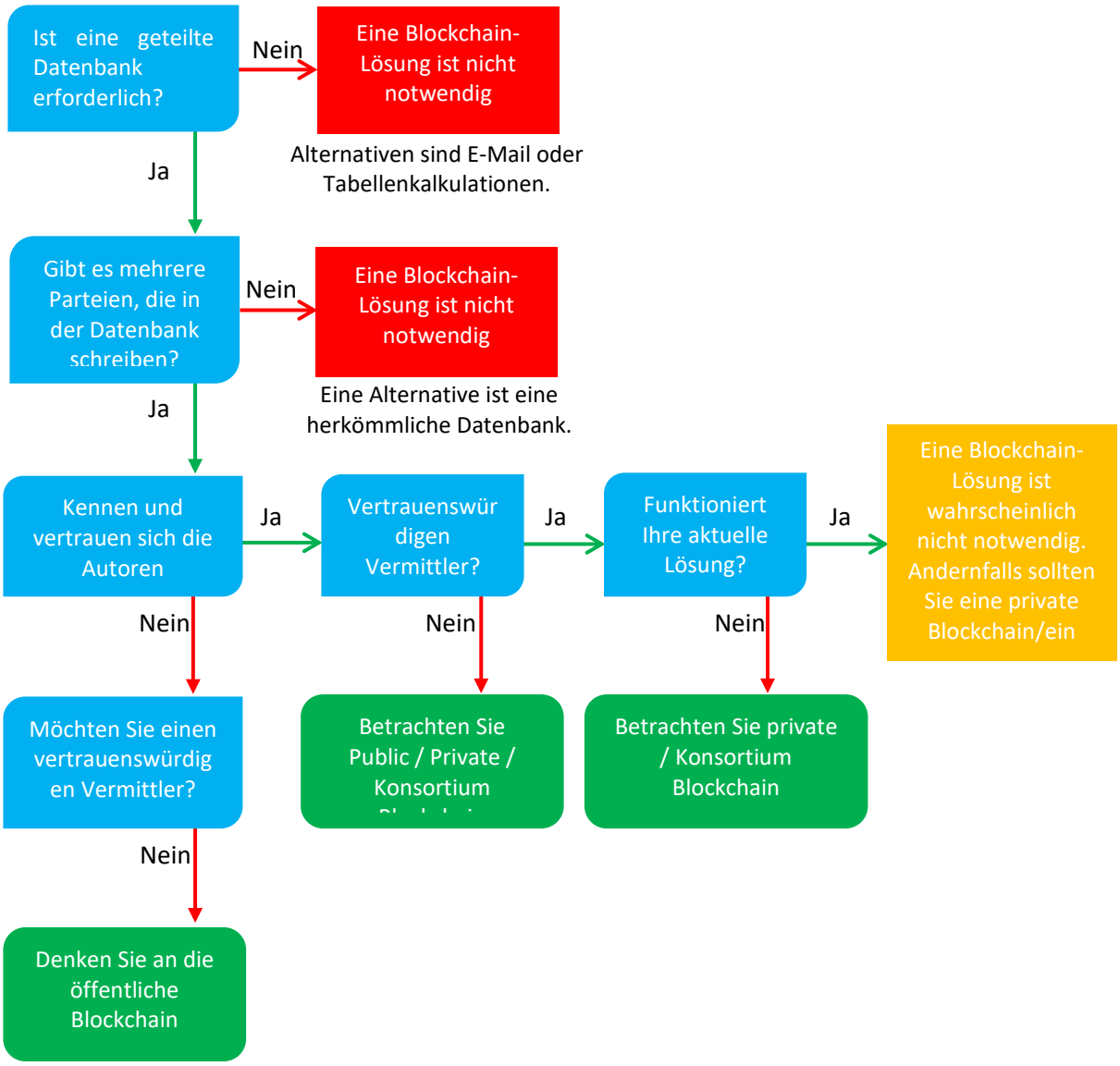


Figure 12: Vereinfachte Entscheidungsstruktur, ob Blockchain verwendet werden soll oder nicht (Quelle: Lin Lim, C., Janse, A., Blockchain Basics, L 2021, S.

6 Referenzen und Quellen für weitere Lektüre

Ackermann, J. & Meier, M. (2018). *Blockchain 3,0: Die nächste Generation von Blockchain-Systemen.*

Advanced Seminar Blockchain Technologies, Sommersemester 2018, Technische Universität Munch.

AI Sweden, Lantmäteriet (2020, November). *Aufbau eines KI-Vertrauensmodells für den öffentlichen Sektor,* konsultiert von https://www.ai.se/en/node/85154

Antonopoulos, A. M. (2016). *Das Internet des Geldes: Gespräche von*. Merkle Bloom Llc.

Augur. (n. d.). *Übersicht*. Konsultiert am 23. Dezember 2019, ab https://docs.augur.net/#overview

Augur. (2018, Juli 9). *Forecast Foundation OU Datenschutzrichtlinie*. Konsultiert am 23. Dezember 2019, von Augur.net Website: https://www.augur.net/privacy-policy/

Baraniuk, C. (2020, Februar 11). *Blockchain: Die Revolution, die nicht ganz stattgefunden*hat. Konsultiert von https://www.bbc.com/news/business-51281233

Bitcoin Block Reward Halbierung Countdown. (2019). Wurde am 23. Dezember 2019 von konsultiert

Bitcoinblockhalf.com Website: http://www.bitcoinblockhalf.com

BMW, (2019, Oktober 14). Wie Blockchain-Lösungen Treiber unterstützen können. Konsultiert von https://www.bmw.com/en/innovation/blockchain-automotive.html

BMW PressClub Global (2020, 31. März). *Die BMW Group setzt Blockchain ein, um die Transparenz der Lieferkette zu fördern.* Konsultiert von https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency.

Buterin, V. (2013). *Ethereum White Paper: Eine Smart Contracts- und dezentrale Anwendungsplattform der nächsten Generation* [White Paper]. Am 27. Dezember 2019 von Blockchainlab konsultiert: http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

Buterin, V. (2014, Mai 6). *Daos, DACs, das und mehr: Ein Unvollständiger Terminologieleitfaden.* Konsultiert am 27. Dezember 2019, von Ethereum.org Website: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Kettenhandel. (2017, Dezember 27*). 10 Vorteile der Verwendung von Smart Contracts*. Konsultiert am 27. Dezember 2019, von Medium Website: https://medium.com/@ChainTrade/10-Vorteile-der-Verwendung-smart-Contracts-bc29c508691a

Hsieh, Y.-Y., Vergne, J.-P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). Bitcoin und der Aufstieg

Der dezentralen autonomen Organisationen. Journal of Organization Design, 7(1). https://doi.org/10.1186/s41469-018-0038-1

Kaoris Zukunft. (2017) *das Grundbuch in der Blockchain – testbed*. Konsultiert von https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

Lantmäteriet, Telia, ChromaWay & Kairos Future. (2016). *Das Grundbuch in der Blockchain.* Konsultiert von http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf

Ledger Insights (2020, 31. März). *BMW erweitert Supply Chain Blockchain für die Rückverfolgbarkeit von Teilen.* Konsultiert von https://www.ledgerinsights.com/bmw-blockchain-supply-chain-parts-traceability/

Ledger Insights (2020, Oktober 15), *Singapore Airlines erweitert ihre digitale Geldbörse auf Blockchain-Basis*. Konsultiert am https://www.ledgerinsights.com/singapore-airlines-extends-its-blockchain-based-reward-digital-wallet/

Lin Lim, C., Janse, A., *Blockchain Handbook*, September 2021, Kapitel 10. Herausgeber: De boekdrukker Amsterdam. NUR: 781 ISBN: 978-90-80866140 https://www.saxion.nl/binaries/content/assets/onderzoek/meer-onderzoek/blockchain/chhay-lin-lim-en-arthur-janse---blockchain-basisboek-digitale-versie-2.pdf

Microsoft, 2021, Mai 14). *Aktion Erforderlich: Migrieren Sie Ihre Azure Blockchain Service-Daten bis zum 10. September 2021*. Konsultiert am https://azure.microsoft.com/en-us/updates/action-required-migrate-your-azure-blockchain-service-data-by-10-september-2021/

Microsoft (2019, Mai 2), *Singapore Airlines transformiert die Kundenbindung mit Blockchain auf Azure*. Konsultiert am 4

MOBI. (2019). *Fahrzeugidentitätsstandard*. Konsultiert von https://dlt.mobi/wp-content/uploads/2019/07/MOBI-Vehicle-Identity-Standard-v1.0-Preview.pdf

Nakamoto, S. (2008). *Bitcoin P2P E-Cash-Papier.* Wurde am 23. Dezember 2019 von konsultiert Metzdowd.com Website: http://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html

Nakamoto, S. (2010, September 30). *Re: Ich habe meine Brieftasche gebrochen, sendet nie bestätigen jetzt.* [Online kommentar im forum]. Nachricht veröffentlicht am https://bitcointalk.org/index.php?topic=1306.msg14714#msg14714

Parker, L. (2015, November 1). *Der jüngste Stromausfall von PayPal treibt die Annahme von Bitcoin*voran. Am 23. Dezember 2019 auf der Website Bravenewcoin.com abrufbar: https://bravenewcoin.com/insights/paypals-recent-power-outage-drives-bitcoin-adoption

Rauchs M., Blandin, A., Bear, K., McKeon, S. (2019). 2. *Global Enterprise Blockchain Benchmarking-Studie*. Konsultiert von https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-10-ccaf-second-global-enterprise-blockchain-report.pdf

Schnuer, C. (2020, Dezember 7). *Veränderung des Immobilienmarktes durch Blockchain*. Konsultiert von https://delano.lu/article/delano_changing-property-market-through-blockchain

Strategyzer. (n. d.) *Business Model Canvas*. Wurde am 23. Dezember 2019 von https://www.strategyzer.com/canvas/business-model-canvas konsultiert https://www.strategyzer.com/canvas/business-model-canvas

Sultan, K., Ruhi, U. und Lakhani, R. (2018). *Konzeption Von Blockchains: Merkmale Und*

Anwendungen. 11. IADIS International Conference Information Systems 2018, 49–57

Vigna, P., & Casey, M. (2015). *Das Zeitalter der Kryptowährung: Wie Bitcoin und die Blockchain sind Herausforderung der Weltwirtschaftsordnung*. New York, New York: Picador/St. Martins Presse.

Young, S. (2018). *Durchsetzung Verfassungsrechtlicher Rechte Durch Computerkodex.* Von konsultiert Website DES CUA Law Scholarship Repository: https://scholarship.law.edu/jlt/vol26/iss1/5/

Anhang I – Glossar der Begriffe

51 % Angriff: Ein Angriff auf die Blockchain, der durch die Gewinnung von mehr als 51 % der gesamten Rechenleistung des Netzwerks erreicht wird.

Client-Server-Modell: Das Modell, bei dem Clients (Benutzer) mit einem Server verbunden sind. Der Server enthält Daten, die für die Clients relevant sind. Die Clients stellen eine Verbindung zum Server her, um auf diese Daten zuzugreifen. Dadurch sind die Clients vom Server abhängig.

Distributed Ledger Technology (DLT): Distributed-Ledger-Technologie.

Double Spending: Zweimal denselben Bitcoin ausgeben. Zum Beispiel, dass Sie 1 Bitcoin haben, aber damit senden Sie 1 Bitcoin an Person A und 1 Bitcoin an Person B.

Vollständiger Knoten: Ein Knoten, der eine vollständige Kopie der Blockchain enthält.

Miner: Ein Computer, der Rechenleistung bereitstellt, um einen gültigen Block zu erzeugen. Ein Block ist nur gültig, wenn er einen nonce findet, der zu einem gültigen Hash-Wert führt.

Knoten: Gerät, das mit einem Computernetzwerk verbunden ist.

P2P: Siehe Peer-to-Peer.

Peer-to-Peer: Ein Computernetzwerk, in dem Computer einander gleich sind und sich gegenseitig Dienste anbieten können.

Nachweise: Ein Konsensmechanismus, bei dem Miner Computerleistung verwenden müssen, um den richtigen Hash-Wert für einen neuen Block zu finden. Wenn sie den richtigen Hash-Wert finden, können sie den Block zur Blockchain hinzufügen und eine Belohnung erhalten.

Single Point of Failure (SPOF): Der Teil eines Netzwerks, der den Betrieb des gesamten Netzwerks im Falle eines Ausfalls stoppt.

SPOF: Siehe Single Point of Failure.

Vertrauenswürdiger Dritter (TTP): Vertrauenswürdiger Vermittler.

TTP: Siehe Vertrauenswürdige Drittpartei.

Whitepaper: Ein Dokument, das beschreibt, wie ein bestimmtes Problem gelöst wird. Satoshi Nakamoto hat im Bitcoin-Whitepaper geschrieben, wie Bitcoin das Problem des Double Spendings in einem verteilten Netzwerk löst.

Blockchain 1,0: Die erste Generation von Blockchains, die hauptsächlich zur Erleichterung der Speicherung und Übertragung von Kryptowährungen eingesetzt wurden.

Blockchain 2,0: Die zweite Generation von Blockchains, die sich mehr auf die Schaffung von Smart Contracts, dApps und Daos konzentrieren.

Blockchain 3,0: Die dritte Generation von Blockchains, die eine Reihe von Problemen gelöst haben, mit denen Blockchain 2,0 noch zu tun hat. Beispiele für solche Probleme sind Skalierbarkeit, Interoperabilität, Datenschutz, Nachhaltigkeit und Governance.

Gas: Transaktionskosten für die Durchführung einer Transaktion auf der Ethereum Blockchain.

Dezentrale Anwendung (Dapp): Eine Anwendung, die die dezentrale Datenspeicherung einer Blockchain nutzt. Die Applikation wird nicht über einen zentralen Server ausgeführt, sondern

über ein dezentrales Knotennetzwerk. Wie eine normale Anwendung verfügt sie häufig über ein Front-End und eine Benutzeroberfläche.

Dezentrale autonome Organisation (DAO): Eine autonome Einheit, die auch auf die Einstellung von Personen angewiesen ist. Diese Personen können bestimmte notwendige Aufgaben ausführen, die das Unternehmen nicht ausführen kann. Der DAO steht zu diesem Zweck internes Kapital zur Verfügung, mit dem bestimmte Aktivitäten dieser Individuen belohnt werden können. Was ein DAO grundlegend von einer zentralisierten Organisation unterscheidet, ist, dass es kein Top-Management-Team oder einen CEO hat. Es handelt sich um eine nicht hierarchische Organisation.

Smart Contract: Ein Vertrag mit bestimmten Bedingungen, die im Code festgelegt sind. Der Vertrag erfüllt sich selbst, da er bei Erfüllung der Bedingungen entsprechende Maßnahmen selbst durchführt. Der Vertrag muss jedoch ausreichende Informationen von jeder Partei enthalten, die an dem Vertrag beteiligt ist, um den Parteien ihre Kündigungsfähigkeit zu entziehen. Es gibt zwei Arten von Smart Contracts: Deterministische und nicht-deterministische.

Solidität: Die Programmiersprache, die speziell für Ethereum entwickelt wurde, um Smart Contracts zu schreiben.