

Die Blockchain – Technologiefeld und wirtschaftliche Anwendungsbereiche

Auftraggeber:

BMVIT, Bereich Innovation

**Autoren:**

Johannes Scherk B.Sc.

Mag. Gerlinde Pöchhacker-Tröscher

Datum:

Mai 2017

Bei allen Bezeichnungen, die auf Personen bezogen sind, meint die gewählte Formulierung beide Geschlechter, auch wenn aus Gründen der leichteren Lesbarkeit die männliche Form steht.

Pöchhacker Innovation Consulting GmbH

Langgasse 10

A-4020 Linz

T +43-732-890038-0

F +43-732-890038-900

E johannes.scherk@p-ic.at

W www.p-ic.at



Inhaltsverzeichnis

Inhaltsverzeichnis	3
Abbildungs- und Tabellenverzeichnis	5
Executive Summary	6
1 Einleitung	11
2 Die Blockchain	12
2.1 Distributed Ledger - Zentrale vs. dezentrale Datenbank-systeme	12
2.2 Bitcoin - Die Blockchain im Zahlungsverkehr	15
2.2.1 Traditionelles System im Zahlungsverkehr	15
2.2.2 Dezentraler Ansatz im Zahlungsverkehr	17
2.2.3 Die Double-Spending-Problematik	18
2.2.4 Neue Wege des Zahlungsverkehrs durch Bitcoin und die Blockchain	19
2.2.5 Vorteile der Blockchain gegenüber herkömmlichen Technologien	23
3 Anwendungsfelder und disruptive Potenziale der Blockchain	26
3.1 Smart Contracts	27
3.2 Cyber Security	31
3.3 Internet of Things (IoT)	33
3.4 Politik und Verwaltung	35
3.5 Eigentumsrechte	38
3.6 Sharing Economy	39
3.7 Dezentrale Energieversorgung	41
3.8 Wertschöpfungsketten	43
3.9 Verteilte Datenspeicherung	45
4 Key Players im Bereich der Blockchain	47
4.1 Key Players im Bereich der Blockchain	48



4.2	Bedeutende Blockchain-Plattformen	53
5	Herausforderungen und Risiken	56
6	Schlussfolgerungen	58
	Literatur- und Quellenverzeichnis	62



Abbildungs- und Tabellenverzeichnis

Abbildungsverzeichnis:

Abbildung 1: Ausprägungen verschiedener Ledger Systeme	13
Abbildung 2: Traditioneller internationaler Geldtransfer	16
Abbildung 3: Transaktionen in einem Trusted Third Party Netzwerk	17
Abbildung 4: Transaktionen in einem Trusted Third Party Netzwerk	18
Abbildung 5: Die Bildung von Blöcken bei Bitcoin	21
Abbildung 6: Die Entstehung der Blockchain bei Bitcoin	22
Abbildung 7: Die Funktionsweise der Blockchain im IoT	34
Abbildung 8: Aktivitäten rund um die Blockchain und Distributed Ledger Systeme (Stand 2016)	47



Executive Summary

Die Digitalisierung von Gesellschaft und Wirtschaft ist unbestreitbar einer der größten und umfassendsten Trends unserer Zeit. Fortschritte in den Informations- und Kommunikationstechnologien und des Internets haben Innovationen ermöglicht, die umfassende Teile unseres Lebens verändert haben bzw. verändern. Dabei schreitet die Digitalisierung immer schneller voran und Technologien wie Big Data, Cloud Computing, Mobile Devices und das Internet der Dinge entfalten zunehmend ihre transformativen Potenziale.

Eine relativ neue Technologie im Kontext der Digitalisierung stellt die sogenannte Blockchain dar. Das Konzept erlangte mit der Einführung der Kryptowährung Bitcoin im Jahr 2009 erstmals weltweite Aufmerksamkeit. Doch längst ist die Blockchain mehr als nur die Technologie hinter Bitcoin. Vielmehr wird die Blockchain mittlerweile als die eigentliche Innovation erachtet, die das Potenzial haben könnte, etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern.

Der Begriff „Blockchain“ ist als allgemeiner Begriff zu verstehen, der eine prinzipielle Funktionsweise beschreibt und damit auch als eine grundlegende Technologie eingestuft werden kann. Als elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die in einem verteilten Rechnernetz verwaltet werden, liegt der Blockchain das Konzept eines sogenannten „Distributed Ledger“ (verteiltes Register) zugrunde. Dabei gibt es keine zentrale Datenhaltung, alle Daten im Register werden an die Teilnehmer eines Netzwerks verteilt. Solche Ledger können dabei unterschiedlich ausgestaltet sein – als offene Netzwerke, an denen jeder teilnehmen kann oder als private Netzwerke, in denen nur bestimmte Akteure teilnehmen dürfen.

Die Blockchain stellt eine bestimmte Klasse von Distributed Ledgers dar, in denen Informationen zu Blöcken zusammengefasst im Register gespeichert werden. Ein wichtiger Teil eines jeden Blocks ist ein Verweis zum vorherigen Block, der wiederum auf den ihm vorangehenden Block verweist. Dadurch entsteht eine Kette von Blöcken – die Blockchain. In jedem Block werden sämtliche enthaltene Informationen verschlüsselt (inkl. der Informationen zum vorangehenden Block), indem ein Hashwert der zugrundeliegenden Daten gebildet wird (dabei wird eine beliebig lange Zeichenfolge in eine alphanumerische Zeichenfolge mit festgelegter Länge umgewandelt) – so werden nur definierte Bestandteile der ursprünglichen Information offen ersichtlich gemacht.

Bevor ein Datenblock der Blockchain hinzugefügt wird, wird er von den Teilnehmern des Netzwerks validiert. Nur wenn die Mehrheit des Netzwerks die Korrektheit des Blocks bestätigt, wird dieser ein Teil der Kette. Da jeder Block auf den vorangehenden Block in der Kette verweist, ist eine nachträgliche Veränderung der



Tiefendossier: Die Blockchain

Daten, sobald diese einmal in der Blockchain gespeichert sind, nicht mehr möglich. So kann gewährleistet werden, dass die in der Blockchain enthaltenen Daten korrekt sind und nicht manipuliert wurden. In der Blockchain werden dabei keine Ergebnisse von Transaktionen abgespeichert, sondern jede einzelne Aktion bleibt in seiner Form erhalten. Wenn also zB ein Kontostand in einer Bitcoin-Applikation ermittelt wird, werden dafür alle Transaktionen nachvollzogen.

Da die Blockchain als identische Kopie auf den Rechnern der Netzwerkteilnehmer hinterlegt ist, wird dadurch ein potenzieller Single-Point of Failure eliminiert und ein Ausfall einzelner Netzwerkknoten hat keine kritischen Auswirkungen auf das System. Ebenso dient die Blockchain dadurch als eine „einheitliche Version der Wahrheit“ (Single Source of Truth): Da die Teilnehmer des Netzwerks über dieselbe Kopie der Blockchain verfügen, werden Informationsungleichgewichte eliminiert und die Abstimmung von unterschiedlichen Datenbanken obsolet.

Indem die Blöcke der Blockchain eine Referenz zu dem vorherigen Block sowie einen Zeitstempel enthalten und über Hashes miteinander verbunden sind sowie Daten, sobald sie einmal in der Kette hinterlegt sind, nicht mehr im Nachhinein verändert oder gelöscht werden können, wissen die Nutzer, dass die Integrität der Daten gewährleistet ist. In Verbindung mit der dezentralen Verwaltung der Blockchain ist daher kein Vertrauen zwischen den Teilnehmern oder gegenüber zentralen Instanzen notwendig. Dadurch sind dritte Parteien (Trusted Third Parties), wie zB Banken oder andere Intermediäre, für Aktionen innerhalb des Netzwerks obsolet und Transaktionen o.ä. können direkt zwischen den Teilnehmern durchgeführt werden.

Neben dem dezentralen Aufbau und der Unveränderlichkeit der enthaltenen Daten verfügt die Blockchain über eine weitere zentrale Eigenschaft, die sie für zukünftige Anwendungen äußerst interessant macht: Sie ist programmierbar. In den Blöcken können Anweisungen und Befehle eingebettet werden, die zu entsprechenden Aktionen führen, wenn bestimmte Kriterien erfüllt sind. Die Blockchain kann damit nicht nur für Transaktionen oder als vertrauenswürdige Datenbank dienen, sondern auch komplexe konditionale Aktionen auslösen, etwa durch selbstausführende intelligente Verträge (sog. „Smart Contracts“).

Solche Smart Contracts stellen eine der vielversprechendsten Anwendungen der Blockchain dar. Sie legen fest, welche Bedingungen zu welcher Entscheidung führen und können zur automatisierten Abwicklung von Verträgen eingesetzt werden, indem sie Bedingungen in Echtzeit überwachen und Vertragsbestandteile automatisch durchsetzen. Smart Contracts ermöglichen also nicht nur die Verteilung von Daten, sondern auch von Logik innerhalb der Blockchain – und verfügen über sämtliche ihrer Vorteile: Sie sind sicher, verifizierbar, transparent und nicht manipulierbar.

Smart Contracts können für unterschiedlichste Bereiche angewendet werden, etwa



für Kaufverträge oder im Versicherungswesen. Das größte Potenzial liegt aber voraussichtlich in der Verbindung mit einer anderen disruptiven Technologie der Digitalisierung – dem Internet der Dinge (IoT). Mit dem Internet verbundene Geräte könnten sich damit selbstständig organisieren und eigenständig Transaktionen durchführen – ohne dass ein Mensch oder eine andere zentrale Instanz eingreifen muss. So könnten IoT-Netzwerke weiter dezentralisiert und den Geräten eine höhere Autonomie und schließlich sogar eine „Economy of Things“ ermöglicht werden. IBM hat in Zusammenarbeit mit Samsung bereits ein Pilotprojekt umgesetzt, in dem intelligente Geräte mittels Blockchain-Technologie autonome Handlungen durchgeführt, sich selbstständig organisiert und Transaktionen durchgeführt haben.

Die Verbindung von Blockchain und dem Internet der Dinge würde auch zur Dezentralisierung der Energiemärkte beitragen. Mittels Blockchain könnten lokale Energieproduzenten (zB Inhaber einer Photovoltaik-Anlage) und -konsumenten in einem dezentralisierten, echtzeitbasierten Energiemarkt miteinander verbunden sein und eine flexible Energieversorgung mit Bürgern und Unternehmen als aktiven Marktteilnehmern ermöglicht werden. Intelligente Geräte bzw. Computer könnten automatisch Informationen über überschüssige bzw. benötigte Energie senden und über die Blockchain eigenständig Preise verhandeln und Energiekäufe durchführen.

Auch die Sharing Economy könnte durch die Blockchain einen weiteren Schub erfahren. Die Blockchain kann dazu beitragen, das Vertrauen zwischen Anbieter und Kunden aufzubauen, etwa mittels „Reputationsmanagement“-Systemen, in denen relevante Informationen der Parteien vertrauenswürdig und transparent gespeichert sind. Mit der Blockchain wäre es sogar möglich, dass Anbieter wie Airbnb oder Uber, die Leistungen Dritter über ihre Plattformen anbieten, nicht mehr notwendig sind, sondern diese (Unternehmen und Privatpersonen) direkt mit ihren Kunden vernetzt sind und Informationsaustausch und Bezahlung direkt zwischen den beteiligten Parteien stattfinden.

Das Anwendungspotenzial der Blockchain erstreckt sich auf viele weitere Bereiche, sie kann in Politik und Verwaltung im eGovernment eingesetzt werden und die Integrität und Verfügbarkeit der Daten in allen relevanten Institutionen gewährleisten. Sie kann als Grundlage verschiedener digitaler öffentlicher Services, zur Einhebung von Steuern, für effizientere Sozialaufwendungen und sogar für neue Konzepte für Wahlen eingesetzt werden. Zudem kann sie als sicheres Register im Bereich von Eigentumsrechten, zur dezentralen Datenspeicherung, Nachverfolgung von Produkten und für effizientere Wertschöpfungsketten, als Cyber Security Instrument und vieles mehr dienen. Wie bereits erwähnt sind den vorstellbaren Möglichkeiten, die sich durch die Blockchain ergeben, kaum Grenzen gesetzt.



Tiefendossier: Die Blockchain

Dementsprechend beschäftigen sich auch zahlreiche führende Unternehmen mit der Thematik und Investoren haben zunehmend Blockchain-Start-ups im Blick. Hinter dem Technologieunternehmen R3 CEV, welches dezentrale Systeme für die Finanzbranche entwickelt, steht etwa ein Industriekonsortium von über 75 Banken und Technologieunternehmen, zu dessen Mitgliedern u.a. UBS, Deutsche Bank, J.P. Morgan, Credit Suisse, UniCredit und Barclays zählen. Im Hyperledger Projekt haben sich über 100 Unternehmen unter der Schirmherrschaft der Linux Foundation versammelt, um offene Standards für die Blockchain zu entwickeln. Zu den Projektmitgliedern gehören etwa Accenture, IBM, Daimler, Cisco, Nokia, Samsung und IBM.

Der IT-Riese IBM ist nicht nur am Hyperledger Projekt beteiligt, sondern setzt auch eigenständige Aktivitäten im Bereich der Blockchain-Technologie. Neben einer angebotenen Blockchain-Plattform für Unternehmen zur effizienteren Gestaltung von Wertschöpfungsnetzwerken erforscht IBM insbesondere die Einsatzmöglichkeiten der Blockchain im Internet der Dinge. Auch Microsoft ist längst auf die Blockchain aufmerksam geworden und bietet auf seiner Cloud-Plattform „Blockchain-as-a-Service“-Modelle für Unternehmen an. Dabei soll die Azure Plattform von Microsoft zu einem Marktplatz für zertifizierte Blockchain-Anwendungen ausgebaut werden.

Bereits heute bestehen unzählige unterschiedliche Blockchain-basierte Plattformen. Eine der einflussreichsten davon ist Ethereum, das einen universellen Ansatz der Blockchain verfolgt und die Entwicklung und Ausführung von Smart Contracts für unterschiedlichste Anwendungen erlaubt. Die Plattform Storj bietet Blockchain-basierte Cloudspeicher an, wobei im Unterschied zu konventionellen Cloud-Angeboten die Daten nicht zentral auf den Servern des Unternehmens sondern dezentral auf Rechnern der Netzwerkteilnehmer gespeichert werden. Mit der Provenance-Plattform können Unternehmen sich selbst, ihre Produkte und ihre Lieferketten transparent und nachverfolgbar darstellen und Kunden Einsicht in die Supply Chain der Unternehmen erhalten. Dabei werden Informationen zum Produkt, wie etwa Komponenten, Lieferanten, Bearbeiter etc. mit dem physischen Produkt verknüpft und die Käufer des Produkts können dessen Entstehungsgeschichte im Internet abrufen.

Die Blockchain bietet verschiedene, disruptive Potenziale und Anwendungsmöglichkeiten. Sie kann Finanzmärkte maßgeblich verändern, es intelligenten Geräten erlauben, sicher miteinander zu kommunizieren, sich zu organisieren und eigenständig Transaktionen durchzuführen und so als Enabler des Internets der Dinge werden. Die Blockchain kann zum Aufbau dezentraler Energiemärkte beitragen, das Konzept der Sharing Economy weiter vorantreiben oder als Cyber Security Instrument eingesetzt werden – den Anwendungsmöglichkeiten der Blockchain sind kaum Grenzen gesetzt.

Da die Technologie allerdings noch in den Kinderschuhen steckt, gilt es noch eine



Reihe von Herausforderungen zu bewältigen, um die Potenziale der Blockchain vollständig zu nutzen. Ein Thema ist etwa die Skalierbarkeit von Blockchains: Je mehr Teilnehmer eine Blockchain hat und je mehr Transaktionen durchgeführt werden, desto größer wird die Blockchain, da alle Transaktionen und Informationen dauerhaft in der Blockchain hinterlegt werden. So wächst das Volumen der Blockchain bei jeder Transaktion. Da die Kette als Kopie auf den Rechnern der Netzwerkteilnehmer gespeichert wird, muss dafür genügend Speicherplatz auf diesen zur Verfügung gestellt werden, bei großen Datenbanken stoßen Blockchain-Systeme oft noch an ihre Grenzen. Dazu kommt, dass die Verifizierung der Datenintegrität hohe Rechenleistungen benötigt. Das Online Magazin „Motherboard“ hat berechnet, dass das Bitcoin-Netzwerk unter den derzeitigen Wachstumsraten bis 2020 so viel Energie benötigen würde wie ganz Dänemark.

Die Blockchain gilt generell zwar als sicherer als bestehende Systeme, jedoch ist dies nur der Fall, wenn der zugrundeliegende Programmiercode fehlerfrei ist. Fehler im Code stellen ein erhebliches Sicherheitsrisiko dar und können von Hackern ausgenutzt werden, um das System zu kompromittieren. Ein weiteres Problem der Blockchain ist die Tatsache, dass sie nur sicher ist, wenn genug Teilnehmer im Netzwerk vorhanden sind. Die Entscheidung, welche Blöcke der Kette hinzugefügt werden, wird bei der Blockchain durch ein Consensus-Modell getroffen. I.d.R. muss dafür die Mehrheit des Netzwerks die Korrektheit der Daten verifizieren – wobei es dabei meist um Rechenleistung und nicht um die Anzahl der Personen geht. Ist das Netzwerk relativ klein, ist es umso einfacher für Akteure, die Mehrheit der Rechenleistung im Netzwerk aufzubringen – wodurch eine Manipulation der Daten möglich wäre. Die Gefahr, dass eine kritische Masse an verschiedenen Netzwerkteilnehmern nicht erreicht wird, kann insb. dann bestehen, wenn eine starke Fragmentierung von Blockchain-Plattformen gegeben ist.

Auch ergeben sich durch die per Verschlüsselung und digitalen Signaturen hervorgerufene Pseudoanonymität der Blockchain – insb. bei Kryptowährungen wie Bitcoin – sowie durch ihre dezentrale Natur samt Fehlen einer Trusted Third Party oftmals Bedenken hinsichtlich der Legalität der Transaktionen. So wurde Bitcoin in der Vergangenheit mehrmals als Medium für Geldwäsche und Schwarzmarkttransaktionen in Verbindung gebracht.

Interessant ist die Blockchain-Technologie auch als Enabler anderer bedeutender Technologien und Trends: Sie könnte das Internet der Dinge, Cloud Computing, 3D-Druck, Big Data Anwendungen oder Konzepte wie die Sharing Economy vorantreiben und so weitere disruptive Potenziale zu entfalten – der endgültige Einfluss der Blockchain bleibt dennoch abzuwarten. Eines erscheint allerdings sicher: Die Blockchain wirft viele neue Fragen auf und stellt somit einen interessanten Gegenstand für Forschungsaktivitäten und die Erschließung wirtschaftlicher Anwendungspotenziale dar.



1 Einleitung

Die Blockchain stellt im Kontext der Digitalisierung eine Technologie dar, die erst vor wenigen Jahren weltweite Aufmerksamkeit erfahren hat. Im Rahmen der Kryptowährung Bitcoin wurde erstmals ihr grundlegendes Konzept beschrieben und mit der Einführung dieses digitalen Zahlungssystems eingesetzt. Seitdem hat die Blockchain in der Finanzwelt „hohe Wellen“ geschlagen, da sie grundlegende Veränderungen für das bestehende System mit sich bringen könnte.

Allerdings geht das Wirkungspotenzial der Blockchain weit über die Finanzwelt hinaus, die Einsatzmöglichkeiten sind im Zusammenhang mit digitalen Daten kaum begrenzt. Aufgrund dessen wurde Pöchhacker Innovation Consulting GmbH (P-IC) vom Bundesministerium für Verkehr, Innovation und Technologie (BMVIT), Bereich Innovation, beauftragt, eine gezielte Betrachtung der Blockchain-Technologie vorzunehmen.

Das vorliegende Dossier beschreibt das grundlegende technologische Konzept der Blockchain, gibt einen Überblick über bestehende bzw. mögliche Anwendungsfelder sowie disruptive Potenziale und stellt wesentliche Akteure und deren Tätigkeitsschwerpunkte im Bereich der Blockchain vor.

Die Darstellung des Konzepts und der Funktionsweise der Blockchain erfolgt dabei am Beispiel der Kryptowährung Bitcoin, da die Blockchain in deren Rahmen entwickelt und erstmals eingesetzt wurde. Dabei wird auch auf die Unterschiede zu traditionellen Zahlungssystemen und den neuen dezentralisierten Ansatz, der mit der Blockchain erst möglich wurde, eingegangen.

Alle potenziellen Anwendungsfelder der Blockchain zu beschreiben dürfte aufgrund ihrer zahlreichen Einsatzmöglichkeiten kaum möglich sein, daher wurden im vorliegenden Dossier neun Themengebiete beschrieben, in denen die Blockchain besonders disruptive Auswirkungen haben könnte. Dazu zählen intelligente Verträge, das Internet der Dinge, die Sharing Economy, Politik und E-Government sowie das Thema Cyber Security.

Weiters wird ein Überblick über wesentliche globale Akteure, die sich intensiv mit der Thematik Blockchain befassen gegeben. Dargestellt werden ausgewählte Technologiekonzerne, aber auch Blockchain-Unternehmen sowie wesentliche bestehende Plattformen, die auf der Blockchain basieren. Abgeschlossen wird das Dossier mit einer Übersicht über wesentliche Herausforderungen und Risiken der Blockchain sowie die daraus abgeleiteten Schlussfolgerungen.



2 Die Blockchain

2.1 Distributed Ledger - Zentrale vs. dezentrale Datenbank-systeme

1989 entwickelte Tim Berners-Lee am CERN das Konzept des World Wide Web¹ und läutete damit eine neue Ära ein. Seitdem hat das Internet unsere Gesellschaft maßgeblich beeinflusst und tiefgreifende Veränderungsprozesse eingeläutet. Eines der wichtigsten Stichworte in diesem Kontext ist die „Dezentralisierung“. Mit dem Internet wurde die Kommunikation massiv dezentralisiert, jede Person mit Zugang zum Internet konnte mit anderen Menschen rund um den Globus in Kontakt treten, Informationen und Wissen wurden frei und schnell zugänglich, die Notwendigkeiten zentraler hierarchischer Instanzen wurde geringer und Institutionen, die den freien Meinungs-austausch behinderten, konnten umgangen werden.

Durch Cloud Computing können neben der Kommunikation auch IT-Ressourcen wie Rechenleistung und Datenspeicherung dezentralisiert werden, auch das Internet der Dinge baut auf dem Prinzip der Dezentralisierung auf. Mit der Blockchain kommt nun eine Technologie hinzu, die diesen Dezentralisierungstrend weiter vorantreibt und massive Auswirkungen auf bestehende Strukturen haben könnte.

Die Blockchain ist eine sogenannte „Distributed-Ledger“-Technologie. Wörtlich lässt sich der Begriff als „verteiltes Kontobuch“ übersetzen, im Grunde beschreibt sie eine öffentliche, dezentral geführte Datenbank (bzw. Register), welche über ein Netzwerk von verschiedenen Teilnehmern geteilt wird und in dem alle Teilnehmer über ihre eigene (identische) Kopie des Ledgers verfügen (UK Government Office for Science, 2016). Solche Netzwerke, in denen jeder Teilnehmer über den gesamten Datenbestand verfügt, werden als Peer-to-Peer-Netzwerke bezeichnet (P2P-Netzwerke). Im P2P-Netzwerk haben alle Teilnehmer (oft als Knoten oder „nodes“ bezeichnet) dieselben Rechte und können auf die gleichen Informationen zugreifen sowie dem Ledger Informationen zufügen. Ein einzelner Teilnehmer kann nicht darüber entscheiden, ob und welche Einträge dem Ledger zugefügt werden, stattdessen kommt dazu ein Konsensprozess zum Einsatz, in dem die Mehrheit der Teilnehmer den Eintrag verifiziert.

Den Gegenpart zum Distributed Ledger-System stellen zentralisierte Systeme mit einer zentralen Kopie einer Datenbank dar. In einem solchen „traditionellen“ System verfügt nur der Eigentümer des Ledgers über Zugriff auf die Daten und nur er kann Informationen hinzufügen oder ändern (Credit Suisse, 2016).

¹ <https://www.ethz.ch/content/main/de/news-und-veranstaltungen/eth-news/news/2017/01/wir-brauchen-eine-dezentralisierung-des-internets.html>



Tiefendossier: Die Blockchain

Zwischen einem dezentralen System, bei dem alle Nutzer die gleichen Rechte und Informationen haben und diese für alle frei zugänglich sind, und zentralisierten Ledgers (im Folgenden auch als Traditional Ledgers bezeichnet) bestehen mehrere Abstufungen. Für deren Einstufung sind drei Kernfragen relevant: Wer verfügt über eine Kopie des Ledgers? Wer darf auf die im Ledger enthaltenen Informationen zugreifen? Und wer darf dem Ledger Informationen zufügen bzw. diese bearbeiten? (Credit Suisse, 2016).

Traditionelle zentralisierte Systeme verfügen nur über eine Kopie des Ledgers, die auch nur vom Eigentümer bearbeitet werden kann. Dabei kann das System derart gestaltet sein, dass auch nur der Eigentümer Einsicht in die Daten hat, oder dass eine Gruppe oder auch eine unbegrenzte Zahl an Personen Zugriff auf die Informationen hat. Dabei sind alle Daten auf einem zentralen Server abgespeichert und die Nutzer (Clients), die auf diese Daten zugreifen, vertrauen darauf, dass die Daten korrekt sind. Der Großteil des Internets und der derzeitigen IT-Struktur basiert auf diesem Client-Server-Modell (Brave New Coin, 2015).

Abbildung 1: Ausprägungen verschiedener Ledger Systeme

	Level	Copies	Readers	Writers
Traditional	Centralised 	One 	One 	One
Permissioned Private	De-centralised 	Multiple 	Multiple 	Multiple
Permissioned Public	De-centralised 	Multiple 	Unlimited 	Multiple
Unpermissioned Public	Distributed 	Unlimited 	Unlimited 	Unlimited

Quelle: Credit Suisse



In einem sogenannten Unpermissioned Ledger kann jeder Teilnehmer des Netzwerks Daten zufügen und verfügt über eine Kopie des Ledgers. Wird die Gruppe an Teilnehmern, die über eine Kopie des Ledgers verfügen und Einträge in den Ledger tätigen dürfen, eingeschränkt, stellt dies ein Permissioned Ledger-System dar. Hier verfügt eine definierte Gruppe an Akteuren (zB ein Industriekonsortium) über die Kopien des Ledgers, wodurch auch dieses Modell ein dezentrales System darstellt. Zu unterscheiden sind hier insb. Permissioned Private Ledgers, in dem ausgewählte Parteien über eine Kopie verfügen, Informationszugriff sowie Bearbeitungserlaubnis innehaben und Permissioned Public Ledgers, in denen Informationen öffentlich zugänglich sind (Credit Suisse, 2016).

Dezentrale Systeme verfügen über eine Reihe von Vorteilen gegenüber den zentralisierten Netzwerken bzw. eliminieren inhärente Nachteile von diesen. In zentralisierten Netzwerken kommen meist große IT-Systeme zum Einsatz, die innerhalb einer eigenständigen Institution bestehen, daran angeschlossen sind eine Reihe von Netzwerk- und Nachrichtensystemen, um mit der Außenwelt kommunizieren zu können. Solche Systeme stellen einen potenziellen Single-Point-of-Failure dar. Wird eine erfolgreiche Cyber-Attacke auf das System durchgeführt, kann der Angreifer den gesamten Ledger manipulieren. Bei Distributed Ledgers müsste der Angreifer die Mehrzahl aller Kopien des Ledgers gleichzeitig manipulieren. Da diese auf sehr vielen verschiedenen Computern hinterlegt sind, vervielfacht sich damit der Aufwand für den Angreifer, wobei er mit zunehmender Zahl an Netzwerkteilnehmern steigt (UK Government Office for Science, 2016).

Manipulationen des Ledgers können aber nicht nur von außerhalb erfolgen, sondern auch intern. Verwaltet eine zentrale Stelle den Ledger, so hat diese weitgreifende Möglichkeiten zur Manipulation, ohne dass dies direkt von Dritten geprüft werden kann: Sie könnte etwa Einträge des Ledgers löschen, verändern und fälschen oder auch Einträge blockieren bzw. zensieren. Ein weiteres Gefahrenpotenzial bei zentralisierten Ledgers stellen Störungen bzw. Ausfälle der IT-Infrastrukturen dar: Ist etwa nur eine Kopie des Ledgers auf einem Server gespeichert, ist sie bei einem Ausfall dessen nicht mehr zugänglich. Da bei dezentralen Ledgers eine große Zahl an identischen Kopien bestehen, würde der Ausfall eines einzelnen Knotens die Funktionsfähigkeit des Systems nicht wesentlich beeinflussen (Credit Suisse, 2016).

In zentralisierten Systemen sind der Aufwand, die Korrektheit des Ledgers und die Funktionalität der Systeme sicherzustellen sowie die Sicherheit gegenüber Manipulation von innen wie außen, Einbruch und Ausfall zu gewährleisten, relativ hoch. Bei dezentralen Systemen ist dies in einem deutlich geringerem Ausmaß nötig, da der Ausfall eines Knotens oder die Manipulation einer einzelnen Kopie des Ledgers keine wesentlichen Auswirkungen auf das Gesamtsystem hat.



Ein weiterer wichtiger Vorteil von dezentralen Ledgern gegenüber zentralisierten Systemen ist ihr Beitrag zur Transparenz. Da alle berechtigten Teilnehmer jederzeit über identische Kopien des Ledgers verfügen, haben auch alle denselben Informationsstand. Sobald ein neuer Eintrag in den Ledger erfolgt, findet auf allen Kopien im Netzwerk ein Update statt. Dadurch wird gewährleistet, dass die Daten synchron sind und es können Abstimmungsprozesse entfallen, welche oftmals langsam, teuer und fehleranfällig sind.

2.2 Bitcoin - Die Blockchain im Zahlungsverkehr

Was genau eine Blockchain ist, wie sie funktioniert und welche Vorteile sie gegenüber bestehenden Technologien hat, soll im Folgenden am Beispiel der Kryptowährung Bitcoin erklärt werden, da das technische Modell der Blockchain im Rahmen von Bitcoin entwickelt wurde. Bitcoin ist eine rein digitale Währung, die 2009 begründet wurde und auf einem dezentralen Bezahlnetzwerk basiert, dessen Rückgrat die Blockchain ist.²

2.2.1 Traditionelles System im Zahlungsverkehr

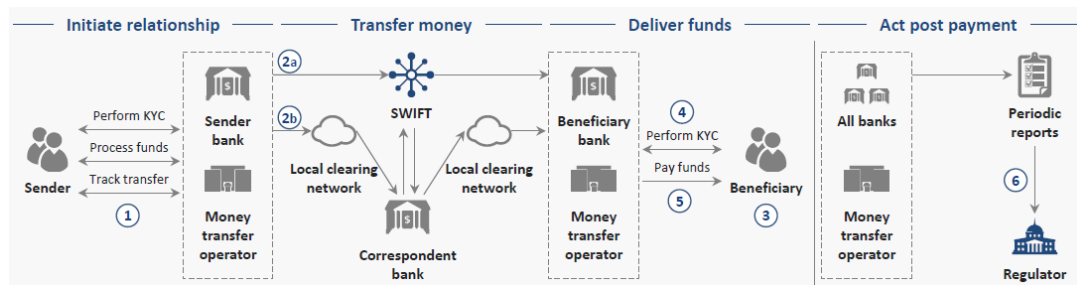
Heute laufen Finanzprozesse meist über einen oder mehrere Intermediäre, bevor ein Zahlungs- oder Wertpapierhandelsvorgang abgeschlossen werden kann. Besonders trifft dies auf den internationalen Zahlungsverkehr zu. Dabei haben Länder oft eigene Zahlungssysteme, mit denen das Clearing und Settlement der Transaktionen der Banken abgewickelt wird.

Will eine Person Geld an eine andere Person im Ausland überweisen, muss deren Bank das Geld an die Bank des Empfängers überweisen, die diesem das Geld auf das Konto überweist. Somit sind bereits zwei Intermediäre im Zahlungsprozess involviert, soweit sie im SWIFT-Netzwerk vertreten sind. Sind die Banken das nicht, muss die Kundenbank des Absenders das Geld erst an eine inländische Bank transferieren, die ein Korrespondenzverhältnis zu einer Bank innerhalb des Zahlungssystems der Bank des Empfängers unterhält. Zudem müssen die Banken periodisch Berichte an Regulierungsbehörden über ihre Transaktionen übermitteln. Damit wären für die Transaktion zwischen zwei Personen bereits sechs verschiedene Akteure involviert (World Economic Forum, 2016).

² <http://www.computerwoche.de/a/blockchain-was-ist-das,3227284>



Abbildung 2: Traditioneller internationaler Geldtransfer



Quelle: WEF (2016)

Ein derartiger Prozess ist langsam, teuer und fehleranfällig, da alle im Prozess beteiligten Akteure bzw. Intermediäre eigene Systeme betreiben und der Prozess von System zu System wandern muss. Dabei sind die einzelnen Systeme meist in einem zentralisierten Ansatz aufgebaut, es handelt sich dabei also um geschlossene Systeme, welche die Verwaltung der Abwicklung der Transaktionen vornehmen. Jedes System hat dabei einen eigenen Ledger, in dem die Konten- und Transaktionsinformationen gespeichert werden (Roßbach, 2016).

Solche zentralisierten Systeme, in denen die Akteure über eigene, geschlossene Ledger verfügen und Intermediäre die Zahlungen abwickeln, finden sich bei weitem nicht nur im internationalen Zahlungsverkehr – bei einem Großteil finanzieller Transaktionen kommt dieses Modell zum Einsatz, dass auf sog. Trusted Third Parties basiert. Trusted Third Parties (TTP, „vertrauensvolle Dritte“) sind Institutionen, die diese Interaktionen kontrollieren und verifizieren.

Bei Überweisungen übernimmt etwa die Geschäftsbank die Rolle der TTP und identifiziert den Sender und den Empfänger der Transaktion, führt diese durch und registriert die neuen Kontobilanzen. Sie dient damit als Vermittler und Vertrauensinstanz der beteiligten Parteien. Dafür verlangt sie Gebühren, wodurch Kosten für ihre Nutzer entstehen.³

Solche Trusted Third Parties sind notwendig, da die an der Transaktion beteiligten Akteure eigene, geschlossen Bücher führen in denen die Informationen abgelegt werden. Es gibt damit keine „Single Source of Truth“, d.h. die Ledger der Akteure können unterschiedliche Informationen zur Transaktion enthalten. Um die Korrektheit der Transaktion zu gewährleisten, wird eine TTP einbezogen, die alle relevanten Transaktionsdaten in ihrem Ledger hinterlegt.

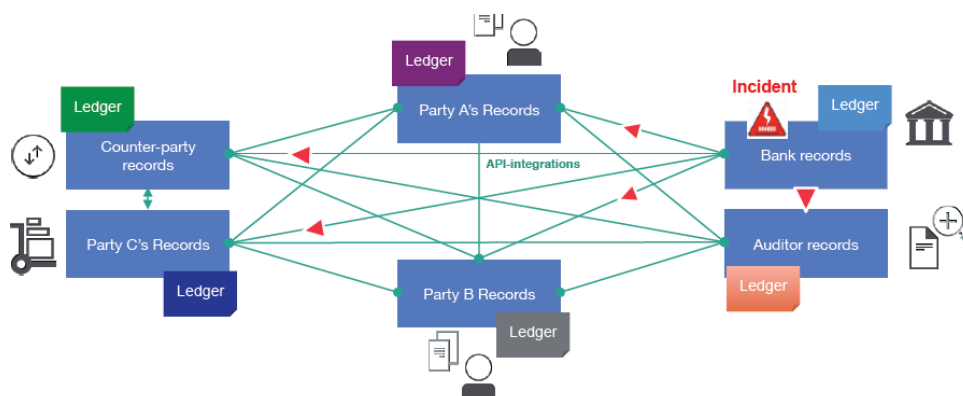
³ <http://www.think-ordo.de/2015/10/digitale-dezentralisierung-die-schleichende-revolution/>



Da nur die TTP, also etwa eine Bank, über einen vollständigen Ledger der Transaktionen verfügt, stellt sie in einem solchen zentralisierten System einen potenziellen Single Point of Failure dar. Wird der Ledger der TTP manipuliert oder ist er durch andere Gründe fehlerhaft, wirkt sich dies auf alle beteiligten Akteure aus.

Solche TTP-Netzwerke sind damit oft ineffizient – da für Transaktionen und damit der Feststellung des Eigentumsübergangs – zusätzliche Intermediäre eingebunden werden müssen, was zu erhöhtem Zeitaufwand und Komplexität führt. Dazu verursachen sie Kosten, da die TTPs Gebühren für ihre Dienste verlangen und sie sind fehleranfällig, da aufgrund der geschlossenen Systeme Single Point of Failures drohen.

Abbildung 3: Transaktionen in einem Trusted Third Party Netzwerk



Quelle: IBM (2016)

2.2.2 Dezentraler Ansatz im Zahlungsverkehr

Als Alternative zum Trusted Third Party-Modell bietet sich der dezentrale Ansatz durch Shared Ledgers an. In diesem Netz aus unterschiedlichen Teilnehmern (Knoten), die Länder, Banken, Unternehmen, Privatpersonen etc. sein können, hat im Sinne eines Distributed Ledgers jeder Teilnehmer dieselben Rechte (P2P-Netz) und verfügt über eine eigene Kopie des Ledgers.

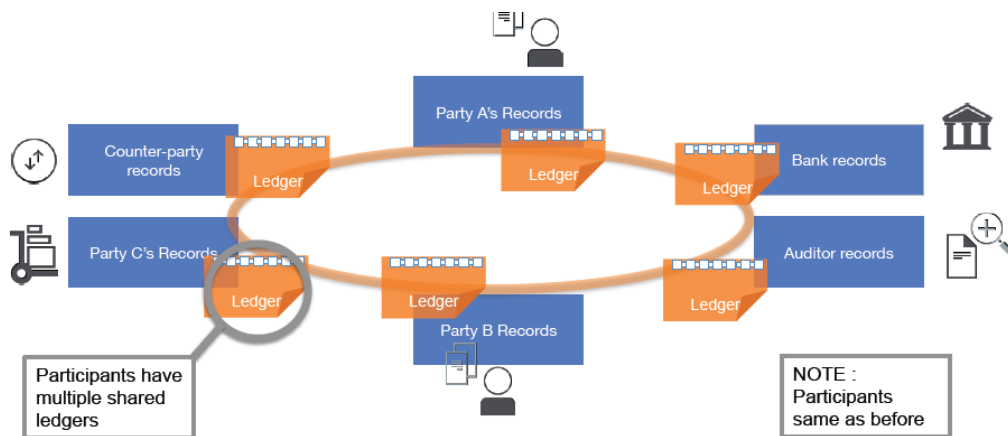
Im Vergleich zum traditionellen, zentralisierten TTP-Modell würde dies einen Basischutz des Netzes vor Manipulationen bedeuten, da diese an der Mehrzahl der Knoten durchgeführt werden müssten – das Risiko des Single Point of Failures würde eliminiert werden. Die Funktionsfähigkeit des Netzes würde auch bestehen bleiben, wenn ein Knoten ausfällt. Die durch die Verteilung des Ledgers bewirkte vollständige Redundanz ist somit ein Mittel gegen einseitige Macht, Manipulation und Ausfall (Roßbach, 2016).

In einem solchen Ansatz wäre das Vorhandensein einer Trusted Third Party nicht mehr notwendig. Da neue Einträge in den Ledger auf allen Knotenpunkten erfol-



gen und verifiziert werden, hat keine einzelne Instanz die Kontrolle über das Verzeichnis und die Nutzer müssen ihr Vertrauen nicht in eine zentrale Institution setzen. Da alle Teilnehmer über eine identische Kopie des gesamten Ledgers verfügen, stellt der Ledger eine sog. „Single Source of Truth“ dar. Dadurch würde im Vergleich zum zentralisierten Modell die Effizienz durch das Wegfallen der Abstimmung durch die TTP steigen sowie durch die TTP entstehende Kosten wegfallen. Weiters würde die Transparenz zwischen den Teilnehmern des Netzwerks aufgrund der identischen Informationslage deutlich steigen.

Abbildung 4: Transaktionen in einem Trusted Third Party Netzwerk



Quelle: IBM (2016)

2.2.3 Die Double-Spending-Problematik

Vor der Einführung von Bitcoin scheiterten derartige dezentrale Ansätze im Finanzbereich an der Double-Spending-Problematik. Diese besagt, dass man sein Geld nicht mehrfach ausgeben oder Wertpapiere mehrfach verkaufen kann. Traditionell wird dies durch die Intermediäre, also etwa Banken, erkannt und verhindert. In einem dezentralen Netzwerk ohne einen derartigen Intermediär besteht dieser Schutzmechanismus jedoch nicht.

Die Problematik ergibt sich dabei in erster Linie dadurch, dass in einem verteilten P2P-Netzwerk neu auftretende Informationen nicht zum exakt selben Zeitpunkt auf allen Knoten zur Verfügung stehen, sondern sich erst im Netz verteilen müssen. Sie werden an einer Stelle, genauer gesagt an einem Knoten, dem Netzwerk zugefügt und verbreiten sich von dort aus auf das gesamte Netz, was Zeit in Anspruch nimmt. Schickt nun ein Knoten eine Transaktion mit einem Asset in eine Richtung des Netzwerks und eine zweite Transaktion mit demselben Asset in eine andere, würde dies das Netz in einen inkonsistenten Zustand bringen, da die Teilnehmer über unterschiedliche Informationen verfügen (Roßbach, 2016).



Die Problematik des Double-Spendings betrifft nicht nur Transaktionen sondern alle digitalen Informationseinheiten, da digitale Güter unbegrenzt vervielfältigt werden können. Ohne eine Lösung der Double-Spending-Problematik ist das Konzept eines Distributed Ledgers damit kaum umzusetzen.

2.2.4 Neue Wege des Zahlungsverkehrs durch Bitcoin und die Blockchain

Die Problematik des Double-Spendings wurde erstmals im Rahmen der Kryptowährung Bitcoin gelöst. 2008 wurde unter dem Namen Satoshi Nakamoto (es wird davon ausgegangen, dass der Name ein Pseudonym eines oder einer Gruppe von Autoren ist) das technische Konzept „Bitcoin: A Peer-to-Peer Electronic Cash System“ (Nakamoto, 2008) veröffentlicht, in dem die Blockchain als zugrundeliegende Technologie erstmalig beschrieben wurde. 2009 ging Bitcoin online – und setzte zum ersten Mal das Konzept der Blockchain in der Realität um.

Bitcoin ist ein elektronisches Peer-to-Peer Zahlungssystem, das den Nutzern erlaubt, Transaktionen online und ohne die Einbindung eines Intermediärs von einem Teilnehmer zum anderen vorzunehmen. Um die Transaktionen zu schützen, werden die Daten dabei verschlüsselt, daher werden Bitcoin und ähnliche Zahlungssysteme auch als Kryptowährungen bezeichnet (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015). Bitcoin ist dabei „open source“, d.h. bestehende Urheberrechte wurden an die Allgemeinheit abgetreten und das System wird nicht von einer einzelnen Institution sondern von den Teilnehmern des Netzwerks aufrechterhalten.

Bei Bitcoin stellt die Blockchain ein Transaktionsverzeichnis dar, in dem alle Transaktionen, die jemals über Bitcoin getätigt wurden, verzeichnet sind. Die Bitcoin-Blockchain ist ein Distributed Ledger, also eine kollektive, öffentliche Datenbank und steht allen Teilnehmern zur Einsicht zur Verfügung und wird gleichzeitig von niemandem zentral kontrolliert. Die Speicherung des Ledgers erfolgt nicht zentral sondern als lokale Kopie bei den Teilnehmern des Bitcoin-Systems, sie ist also eine replizierte, geteilte Datenbank.

Alle Netzwerkteilnehmer von Bitcoin können Transaktionen lokal validieren, ohne sich auf eine externe Aufsichtsinstanz verlassen zu müssen. Im Rahmen des Validierungsverfahrens für Transaktionen werden diese in Blöcken zusammengefasst, wobei jeder Block auf den vorangegangenen Block verweist, wodurch eine Kette von Blöcken verschiedener Transaktionen entsteht – die Blockchain. Im Folgenden wird das System von Bitcoin und damit zusammenhängend die Technologie der Blockchain beschrieben.



Bei Bitcoin finden sämtliche Transaktionen verschlüsselt statt. Dazu kommen Hashing-Funktionen zum Einsatz – mathematische Prozesse, die einen Dateninput unterschiedlicher Größe und Form in einen Output mit festgelegter und immer gleicher Länge umwandeln (bei Bitcoin kommt eine Hash-Funktion mit 256 bits zum Einsatz). Der Vorteil solcher Hash-Funktionen ist, dass es äußerst schwierig ist, aus einem gegebenen Output den ursprünglichen Dateninput zu rekonstruieren. Das zweite wichtige Merkmal von Hash-Funktionen ist, dass bereits bei einer kleinen Änderung der Inputdaten ein vollkommen anderer Output entsteht (Kaye Scholer, 2016).

Weiters kommen bei Bitcoin digitale Signaturen zum Einsatz. Es wird ein privater Schlüssel zur Signatur der Transaktion sowie ein damit verbundener öffentlicher Schlüssel zur Verifikation generiert. Dabei kann mit dem öffentlichen Schlüssel nachgewiesen werden, dass die digitale Signatur mit dem privaten Schlüssel durchgeführt wird, ohne den eigentlichen privaten Schlüssel kennen zu müssen (Kaye Scholer, 2016).

Will eine Person eine andere Bitcoins überweisen, generiert sie mit ihrer „Bitcoin-Wallet“ (Gegenstücke einer echten Geldbörse im Bitcoin-Netzwerk, die die privaten Schlüssel einer Person enthält) einen privaten Schlüssel sowie den zugehörigen öffentlichen Schlüssel. Der Sender schickt eine digital signierte Nachricht der Transaktion an die Adresse des Empfängers und teilt diesem den öffentlichen Schlüssel mit, womit dieser die digitale Signatur verifizieren kann (Credit Suisse, 2016).

Ist die Transaktion durch den Empfänger validiert, wird sie an alle Knoten (Teilnehmer) im Netzwerk gesendet, mit denen die Wallet des Empfängers verbunden ist. Jeder Knoten, der die Transaktion empfangen hat, führt eine Reihe von insg. 20 verschiedenen Überprüfungen der Transaktion durch, insb. ob die digitale Signatur des Senders korrekt ist und er der tatsächliche Eigentümer der Bitcoins ist und ob er über ausreichend Bitcoins verfügt, um die Transaktion durchführen zu können. Dazu werden alle Transaktionen, die der Sender jemals durchgeführt hat und die im Ledger gespeichert sind, geprüft (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015). Wird die Transaktion als gültig eingestuft, senden die Knoten die Transaktion an weitere Teilnehmer im Netz mit denen sie verbunden sind. Dieser Prozess wird als „Flooding“ bezeichnet (Credit Suisse, 2016).

Damit ist zwar die Korrektheit der Transaktion sichergestellt, die Double-Spending-Problematik ist dadurch allerdings noch nicht gelöst. Dafür muss sichergestellt werden, dass alle Knoten über die gleichen Informationen verfügen und es keine unterschiedlichen bzw. widersprüchlichen Informationsstände gibt. Dazu müssen sich die Teilnehmer des Netzwerks darauf einigen, welche Transaktionen in den Ledger aufgenommen werden (dieser Prozess wird gemeinhin als „Consensus“



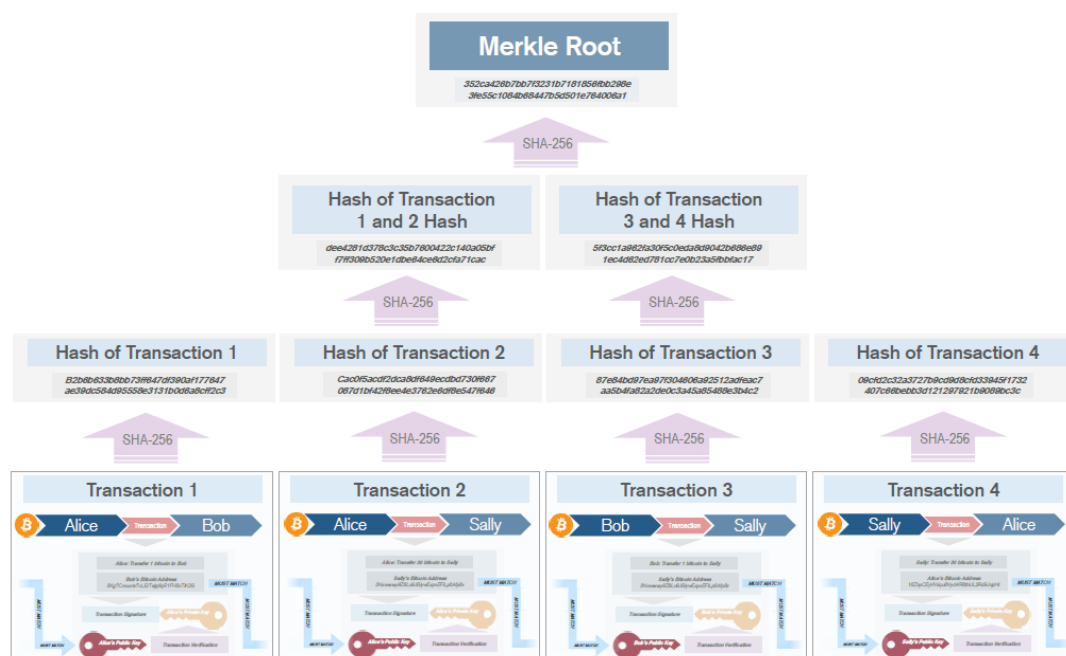
Tiefendossier: Die Blockchain

bezeichnet). Dabei muss gelten, dass die erste Transaktion, die im Ledger aufgenommen wird, die einzig gültige ist und nicht im Nachhinein verändert oder aus dem Ledger entfernt werden kann (Roßbach, 2016).

Diese Problemstellung löste Bitcoin mit der Blockchain. Bei dieser werden ausstehende und als korrekt eingestufte Transaktionen in Blöcken gesammelt und als Gruppe in den Einigungsprozess eingebracht und dem Ledger sequentiell angehängt – diese Kette von Blöcken ist die Blockchain.

Der Bau der Blockchain findet wie folgt statt: Nach dem Flooding der als korrekt eingestuften Transaktion werden diese von sogenannten „Minern“ mit anderen noch ausstehenden Transaktionen zu einem Block zusammengefasst. Miner sind Teilnehmer, die dem Netzwerk Rechenleistung zur Verfügung stellen und mit spezieller Soft- und Hardware Transaktionen verarbeiten, bestätigen und versuchen, gültige Blöcke zu „finden“, wofür sie mit Bitcoins entlohnt werden. Der finale Block wird dabei mit Hilfe eines Hash-Baums (englisch: merkle tree) erzeugt: Aus den Hashwerten zweier Transaktionen wird ein neuer Hashwert erzeugt, der für beide Transaktionen gilt. Dieser wird wiederum mit einem zweiten aus zwei Transaktionen erzeugten Hashwert gepaart und ein neuer Hashwert ermittelt. Dies wird solange fortgesetzt, bis für alle ausstehenden Transaktionen ein einzelner Hashwert gefunden ist (Credit Suisse, 2016).

Abbildung 5: Die Bildung von Blöcken bei Bitcoin



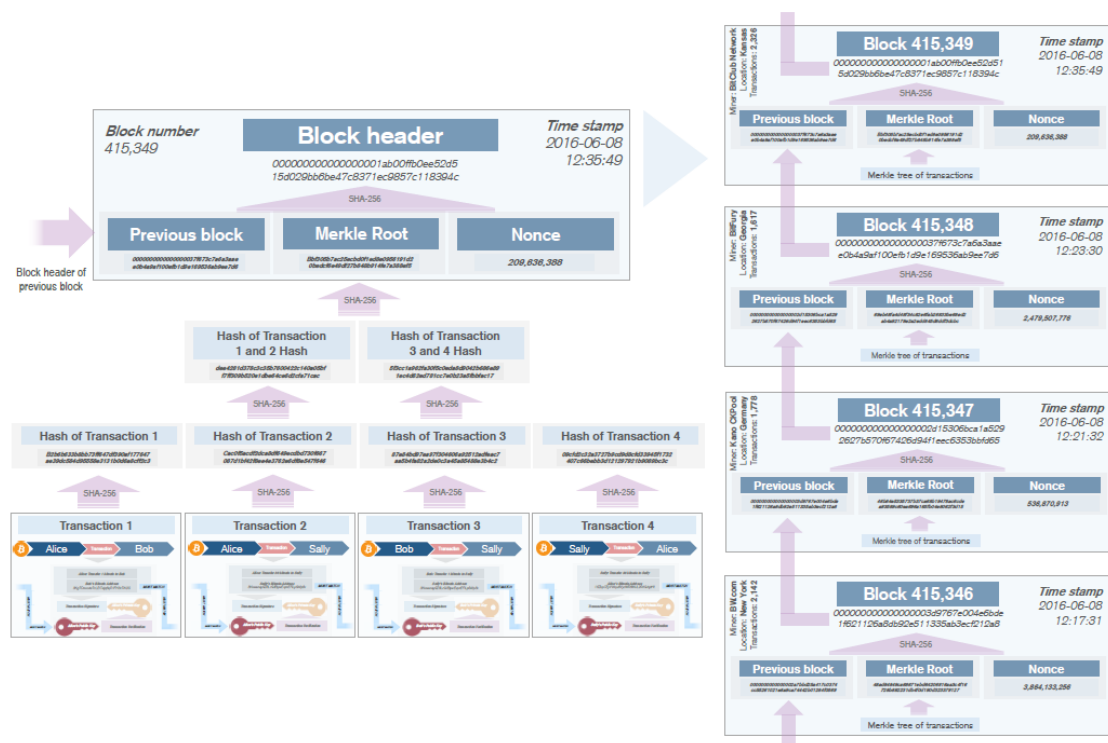
Quelle: Credit Suisse, 2016



Neben den gesammelten Transaktionen enthält jeder Block zudem ein Abbild des vorangehenden Blocks (ebenfalls als Hash), so dass in jedem Block als digitaler Fingerabdruck ein kryptografisches Abbild des vorhergehenden Blocks eingebaut ist. Auf diese Weise werden die Blöcke in Form einer Kette verbunden, da das Abbild eines Blocks von dem des vorhergehenden und damit auch von allen anderen vorhergehenden Blöcken im Ledger abhängt. Eine Manipulation eines Blocks würde dadurch zu einem anderen kryptografischen Abbild führen. D.h. für eine Manipulation müssten auch alle nachfolgenden Blöcke manipuliert werden – und zwar bevor der nächste Block entsteht und ebenso auf der Mehrzahl aller Knoten im Netzwerk (Roßbach, 2016).

Eine solche Manipulation wird umso schwieriger, je aufwändiger die Herstellung eines Blockes ist. Daher müssen die Miner, welche die Blöcke erstellen, bei Bitcoin einen „Proof-of-Work“ (POW) erbringen. Im Grunde ist dies ein mathematisches Puzzle, zu dessen Lösung ein hoher Rechenaufwand nötig ist. Bei Bitcoin ist dieses so gestaltet, dass die Lösung und damit die Erstellung eines neuen Blocks im Schnitt rund zehn Minuten dauert (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015).

Abbildung 6: Die Entstehung der Blockchain bei Bitcoin



Quelle: Credit Suisse, 2016

Sobald ein Miner den Proof-of-Work erbracht und einen neuen Block erstellt hat, wird dieser an die anderen Teilnehmer im Netz gesendet. Diese verifizieren den Block und fügen ihn der Blockchain hinzu. Werden mehrere Blöcke gleichzeitig



erstellt, entscheidet eine „Longest-Chain-Rule“ darüber, welcher Block an die Blockchain angefügt wird (derjenige Block wird angefügt, auf den die längste Kette an nachfolgenden Blöcken verweist) (Brave New Coin, 2015). Da die Blockchain umso sicherer ist, je tiefer eine Transaktion in ihr liegt, d.h. je mehr Blöcke dem Block der Transaktion folgen, wird bei Bitcoin die finale Transaktion erst nach sechs nachfolgenden Blöcken in der Blockchain freigegeben (Credit Suisse, 2016).

2.2.5 Vorteile der Blockchain gegenüber herkömmlichen Technologien

In den vorangegangenen Ausführungen wurde die Blockchain anhand der Kryptowährung Bitcoin erklärt, bei der sie als Transaktionsverzeichnis eingesetzt wird. Zwar können andere Blockchain-Plattformen im Vergleich zu Bitcoin sehr wohl anders ausgestaltet sein, etwa hinsichtlich des Netzwerktyps (zB öffentlicher Ledger vs. privater Ledger) oder des verwendeten Konsensmechanismus und der Verschlüsselung von Daten. Die dargestellte Funktionsweise der Blockchain bleibt im Kern allerdings immer dieselbe: Daten und Informationen werden verschlüsselt, zu Blöcken zusammengefasst, validiert und dem Ledger hinzugefügt. Dabei verweist jeder Datenblock auf den ihm vorangehenden Block, wodurch eine Blockkette entsteht. Weitere wesentliche Merkmale, die eine Blockchain i.d.R. aufweist sind (Deloitte, 2016a):

- ✱ Digitale Verteilung der Blockchain auf mehreren Rechnern: In einem dezentralen System werden digitale Kopien der gesamten Blockchain auf den Rechnern der Netzwerkteilnehmer abgespeichert.
- ✱ Consensus-Modelle: Die Blockchain nutzt viele Teilnehmer in Netzwerk, um die Integrität der Daten zu validieren und einen Konsens darüber zu erreichen, welche Daten der Kette hinzugefügt werden.
- ✱ Blockchains nutzen Kryptografie und digitale Signaturen, um Identitäten zu bestimmen, Transaktionen nachzuverfolgen und diese gleichzeitig sicher und nicht für jeden einsehbar zu gestalten.
- ✱ Blockchains verfügen über Mechanismen, um es Angreifern möglichst schwierig zu machen, bestehende Daten zu manipulieren (zB Proof-of-Work-Konzepte).
- ✱ Blockchains verfügen über einen Zeitstempel: Durch die singuläre Aneinanderreihung der Daten in Blöcken ist jederzeit ersichtlich und belegbar, wann welche Daten in der Blockchain registriert wurden – eine nachträgliche Änderung des Zeitstempels ist nicht möglich.
- ✱ Blockchains sind programmierbar: In den Blöcken können Anweisungen eingebettet sein, die zu entsprechende Aktionen führen, falls bestimmte Kriterien erfüllt werden, sowie weiterführende Daten zu Transaktionen o.ä. enthalten.



Gerade die Programmierbarkeit der Blockchain macht diese interessant: D.h. die Blockchain kann nicht nur für Transaktionen verwendet werden, sondern für alle denkbaren Anwendungen, die auf digitalen Daten basieren. Die Blockchain kann damit als sichere und transparente Datenbank für Informationen aller Art, zur Kommunikation zwischen den Teilnehmern im Netzwerk und oder als Instrument zur Nachverfolgung von Daten und Aktionen verwendet werden. Das größte Potenzial der Blockchain könnte jedoch darin liegen, selbstausführende Verpflichtungen – sog. „Smart Contracts“ – zu ermöglichen, die eine automatische Ausführung von Handlungen bei der Erfüllung festgelegter Kriterien erlauben. Solche Smart Contracts könnten insb. im Kontext des Internets der Dinge für die Kommunikation, den Austausch von Daten sowie die Selbstorganisation intelligenter, vernetzter Geräte eingesetzt werden. Eine Reihe von möglichen Anwendungsfeldern der Blockchain wird im nachfolgenden Kapitel vorgestellt.

Im Vergleich zu traditionellen, zentralisierten Systemen bietet die Blockchain eine Reihe von Vorteilen und Chancen, die im Folgenden kurz zusammengefasst werden:

- ✱ **Immutability of record:** Da die Blöcke der Blockchain eine Referenz zu dem vorherigen Block sowie einen Zeitstempel enthalten und über Hashes miteinander verbunden sind, können Daten, sobald sie einmal in der Kette hinterlegt sind, nicht mehr im Nachhinein verändert oder gelöscht werden.
- ✱ **Disintermediation of trust:** In einem Blockchain-System ist kein Vertrauen zwischen den Teilnehmern oder gegenüber zentralen Instanzen notwendig, dadurch sind dritte Parteien (Trusted Third Parties) für Aktionen innerhalb des Netzwerks und die Verwaltung der Blockchain obsolet.
- ✱ **Datenintegrität:** Durch Consensus-Modelle wird sichergestellt, dass nur korrekte Daten in die Blockchain aufgenommen werden. Da die in der Blockchain hinterlegten Daten zudem nicht manipulierbar sind, wissen die Nutzer, dass die Integrität der Daten gewährleistet ist. Zugleich wird das Problem des Double Spendings gelöst.
- ✱ **Netzausfallsicherheit:** Als Distributed Ledger wird die Blockchain als identische Kopie auf den Rechnern der Netzwerkteilnehmer hinterlegt, dadurch wird ein potenzieller Single-Point of Failure eliminiert und der Ausfall einzelner Netzwerkknoten hat keine kritischen Auswirkungen auf das System.
- ✱ **Single Source of Truth:** Die Teilnehmer des Netzwerks verfügen alle über dieselbe Kopie der Blockchain, wodurch Informationsungleichgewichte eliminiert und die Abstimmung von Datenbanken obsolet werden. Zudem sind alle historischen Informationen in der Blockchain hinterlegt und können eingesehen werden, sodass die Transparenz unter den Teilnehmern des Netzwerks steigt.



Tiefendossier: Die Blockchain

- * **Programmierbarkeit:** Durch die Programmierbarkeit lassen sich komplexe, konditionale Transaktionen und Aktionen in Blockchain-Systemen gestalten, etwa durch selbstausführende Smart Contracts. Dadurch eröffnen sich zahlreiche Anwendungsfelder für die Blockchain-Technologie.
- * **Zugangskontrolle:** Die Verwendung der Blockchain ist nur mit einem privaten Schlüssel möglich, wodurch eine detaillierte Zugangskontrolle ermöglicht wird. Privaten Schlüsseln können spezifische Erlaubnisse zugeteilt werden.
- * **Prozessintegrität:** Da die Prozesse im Netzwerk nach einem entsprechend spezifizierten Programmcode ablaufen, besteht eine hohe Prozessintegrität.

Der Einsatz einer Blockchain stellt in einem dezentralisierten System damit sicher, dass sämtliche Daten korrekt sind und alle Teilnehmer des Systems über die exakt gleichen Informationen verfügen – das Problem des Double Spendings und unterschiedlicher Informationen in den Kopien der Daten bei den einzelnen Teilnehmern werden damit behoben. Dadurch, dass Manipulationen bestehender Daten so gut wie ausgeschlossen sind, stellt Blockchain eine einheitliche, historische Quelle für alle eingespeisten Daten dar. Dadurch ist zwischen den Teilnehmern eines Blockchain-basierten Systems kein Vertrauen notwendig – der vielleicht größte Vorteil der Blockchain.

Für den Einsatz dezentraler Datenbanksysteme muss sichergestellt werden, dass alle Teilnehmer über die gleichen Informationen verfügen und es keine unterschiedlichen bzw. widersprüchlichen Informationsstände gibt. Dazu müssen sich die Teilnehmer des Netzwerks darauf einigen, welche Informationen in das System aufgenommen werden. Dabei muss gelten, dass die erste Transaktion, die im aufgenommen wird, die einzig gültige ist und nicht im Nachhinein verändert oder aus dem System entfernt werden kann. Diese Problemstellung kann mit der Blockchain gelöst und damit eine essentielle Bedingung für die Nutzung dezentraler Datensysteme in zahlreichen Bereichen erfüllt werden.



3 Anwendungsfelder und disruptive Potenziale der Blockchain

Ihren Ursprung fand die Blockchain mit der Kryptowährung Bitcoin im digitalen Zahlungswesen, seitdem haben sich zahlreiche alternative Blockchain-basierte Zahlungsplattformen, oft mit großer Ähnlichkeit zu Bitcoin, entwickelt. Die Finanzbranche war dementsprechend eine der ersten, die sich mit der Blockchain auseinandersetzte. Durch den dezentralen Netzwerkaufbau, die Gewährleistung der Datenintegrität und die Transparenz von Blockchains können Transaktionen sicher und direkt zwischen den Teilnehmern des Netzwerks durchgeführt werden – ohne dass dabei eine zentrale Instanz nötig ist. In der Finanzbranche könnte die Blockchain damit zu disruptiven Veränderungen führen. Banken können mit der Blockchain etwa neue Geschäftsmodelle entwickeln und den Zahlungsverkehr und dessen Abläufe vereinfachen. Da ein Blockchain-basiertes Währungssystem im Grunde aber ohne zentrale Instanz auskommt, stellt die Blockchain aber auch eine Gefahr für die Institute dar und könnte diese zumindest in manchen Bereichen obsolet machen.

Blockchain-basierte Anwendungen sind jedoch nicht auf die Finanzbranche beschränkt. Durch die Programmierbarkeit von Blockchains, ergeben sich zahlreiche mögliche Anwendungsfelder, in denen die Blockchain in Zukunft eingesetzt werden könnte. Eine Reihe von wesentlichen Anwendungsmöglichkeiten der Blockchain wird in diesem Kapitel vorgestellt:

- * Smart Contracts
- * Cyber Security
- * Internet of Things (IoT)
- * Politik und Verwaltung
- * Eigentumsrechte
- * Sharing Economy
- * Dezentrale Energieversorgung
- * Wertschöpfungsketten
- * Verteilte Datenspeicherung



3.1 Smart Contracts

Eine der vielversprechendsten Anwendungen für die Blockchain stellen Smart Contracts dar. Diese sind eine neue, intelligente Form von Verträgen. Im Grunde handelt es sich dabei um webbasierte Computerprotokolle, die Verträge abbilden und deren Abwicklung technisch unterstützen. Smart Contracts legen fest, welche Bedingungen zu welcher Entscheidung führen und können zur automatisierten Abwicklung von Verträgen eingesetzt werden, indem sie die Bedingungen permanent und in Echtzeit überwachen und die Rechte der Vertragspartner automatisch durchsetzen.

Kontrolle und Einhaltung der Verträge erfolgen dabei durch die in den Smart Contracts zur Verfügung gestellten Daten(banken). So können mehrere Parteien in die Verträge eingebunden werden, die sich nicht hundertprozentig vertrauen, ohne dass die Einhaltung der Verträge und deren Klauseln durch Dritte (etwa Anwälte) überwacht werden muss – was wiederum zu massiven Kosteneinsparungen führen könnte.⁴ Die Vorteile solcher „smarten“ Verträge bestehen darin, dass Gegenleistungsrisiken und Transaktionskosten gesenkt werden. Grund ist, dass die Gegenleistung beim Erbringen der Leistung bereits feststeht und damit garantiert ist.

Smart Contracts ermöglichen also nicht nur die Verteilung von Daten und Informationen über die Blockchain sondern auch von Logik. So können zB Transaktionen durch Smart Contracts automatisch durchgeführt werden, sobald die dafür festgelegten Bedingungen erfüllt sind – im Grunde folgen Smart Contracts also einem „Wenn – Dann“-Prinzip“. Da sie auf einer Blockchain gespeichert sind, verfügen sie auch über deren Vorteile: Smart Contracts sind sicher, verifizierbar, transparent und unveränderlich. Zudem können vorgefertigte Smart Contracts leicht vervielfältigt und standardisiert werden und so insbesondere in Bereichen, in denen viele inhaltlich ähnliche oder idente Verträge benötigt werden, eingesetzt werden (Credit Suisse, 2016).

Für die Umsetzung von Smart Contracts ist die Integrität und Verlässlichkeit der zugrundeliegenden Daten von höchster Bedeutung. Diese können durch die Blockchain sichergestellt werden, die die Verifizierung der Daten und Vorgänge ermöglicht. Die Ausführung von Smart Contracts hängt vom Eintreffen der Variablen in die Blockchain ab, die in den Bedingungen für die Ausführung festgelegt sind. Das kann zB das Eintreffen einer Zahlung oder das Erreichen eines Fälligkeitsdatums sein. Meist handelt es sich um eines oder mehrere externe Ereignisse. Die Verbindung zur Außenwelt erfolgt über sogenannte "Oracles". Mittels eines Oracle für eingehende Daten können Datenfeeds über außerhalb der Blockchain anfallende

⁴ <http://www.computerwoche.de/a/blockchain-im-einsatz,3316539>



Ereignisse abgerufen und berücksichtigt werden. Durch eine Oracle für ausgehende Daten können wiederum Anweisungen an Systeme gegeben werden, die sich außerhalb der Blockchain befinden. Oracles speichern und filtern diese Daten vor der Weitergabe an den Smart Contract.

Smart Contracts können beispielsweise im Handel eingesetzt werden: Der Verkäufer veröffentlicht auf einer Blockchain einen Smart Contract, der eine Beschreibung des Produkts, Preise, Verfügbarkeit sowie verschiedene Bedingungen etwa bezüglich Lieferung und Zahlung enthält. Ein Käufer kann auf der Blockchain den Vertrag einsehen, wenn weiterführende Daten hinterlegt sind, die Reputation des Verkäufers beurteilen und anschließend die Bestellung aufgeben. Der Verkäufer wiederum kann über einen Smart Contract ein Unternehmen mit der Lieferung beauftragen, sobald diese erfolgt ist, erhält der Lieferant automatisch seine Bezahlung und genauso wird die Zahlung des Kunden freigegeben, ohne dass ein Intermediär eingreifen müsste.

Die Vorteile dieses Ansatzes sind u.a. niedrige Eintrittsbarrieren für Verkäufer und Käufer bei der Durchführung der Transaktion. Die Reputation der Teilnehmer wird auf der Blockchain durch Smart Contracts aus der Vergangenheit ersichtlich und intelligente Geräte können für einige Transaktionen menschliches Contracting ersetzen und über das IoT Überblick über den Status und Zustand von Smart-Verträge geben (Cognizant, 2016).

Auf Anwaltskanzleien und das Notariatswesen könnten Smart Contracts eine disruptive Wirkung entfalten, teilweise wird davon ausgegangen, dass sie diese auch (in manchen Bereichen) ersetzen könnten. Bisher enthalten traditionelle Verträge Bedingungen und Angaben, die nicht deterministisch sind und von Menschen beurteilt werden. Oft sind sie in ihrer Formulierung sehr komplex, verlangen abstraktes Denken und menschliche Aktionen – was zu möglichen Fehlerquellen führt (Think Consortium, 2016).

Smart Contracts können für unterschiedlichste Bereiche angewendet werden, auch etwa im Versicherungswesen. Versicherungsverträge sind meistens sehr komplex und für Kunden schwierig zu verstehen. Zudem können bei der Inanspruchnahme ebenso komplexe Prüfungsprozesse durch den Versicherer erfolgen. Auf der Gegenseite besteht für den Versicherer immer die Gefahr des Versicherungsbetruges. Durch Smart Contracts können Verträge und Ansprüche auf der Blockchain hinterlegt und durch das Netzwerk validiert werden und sicherstellen, dass nur berechtigte Ansprüche ausgezahlt werden (Deloitte, 2016a). Es können zB Daten von anderen Institutionen unkompliziert eingebunden und validiert werden sowie Auszahlungen automatisch erfolgen, wenn festgelegte Bedingungen eintreten, ohne dass der Versicherte überhaupt einen formellen Anspruch erheben muss.



Use Case – Allianz

Die Allianz Risk Transfer AG (ART) und Nephila Capital Limited (Nephila) haben gemeinsam in einem Pilotprojekt erfolgreich die Nutzung von Smart Contracts mittels Blockchain bei der Durchführung eines Naturkatastrophen-Swaps getestet.

Katastrophen- oder „Cat“-Swaps und -Anleihen sind Finanzinstrumente, die bestimmte Risiken – typischerweise Naturkatastrophen wie Orkane oder Taifune – von einem Versicherer auf Investoren oder andere Versicherer übertragen. Allianz und Nephila testeten dabei den Einsatz von Smart Contracts für das Vertragsmanagement: Mit festgelegten Parametern wird ein Trigger-Ereignis definiert, tritt das festgelegte Trigger-Ereignis ein, werden die vordefinierten Datenquellen aller Teilnehmer erfasst und dann über Smart Contracts automatisch alle Zahlungen zu oder von Vertragspartnern ausgeführt.

Der Testlauf demonstrierte, dass sich durch digitale, automatisierte Blockchain-Verträge die Abwicklung von Transaktions- und Zahlungsprozessen zwischen Versicherern und Investoren deutlich beschleunigen und vereinfachen lässt. Auch die Handelbarkeit von Katastrophenanleihen verbesserte sich.⁵

Auch das IoT, also die Anbindung von Gegenständen an das Internet, stellt ein zukunftssträchtiges Anwendungsfeld für Smart Contracts dar. Durch diese können eine „intelligente Umgebung“ verrechtlicht und die Geräte dazu befähigt werden, selbstständig bestehende Verträge zu vollziehen. Geräte könnten so etwa eigenständig Lieferungen bestellen (zB eine Maschine ein Ersatzteil, wenn sie eine fehlerhafte Komponente feststellt), ohne dass der Eingriff eines Menschen notwendig wäre.

Auch durch ein weiteres Beispiel aus der Versicherungsbranche lässt sich der Einsatz von Smart Contracts im IoT veranschaulichen. Möglich wäre etwa ein Smart Contract für eine KFZ-Versicherung. Wird vom Fahrzeug durch Sensoren festgestellt, dass der Fahrer ein besonders riskantes Fahrverhalten an den Tag legt, kann es diese Verhaltensdaten weitergeben und durch einen Smart Contract erhöht sich automatisch der Versicherungsbeitrag des Fahrers.

Denkbar ist auch, dass etwa im Falle ausstehender Zahlungen (zB Leasingraten) für ein Gerät – oder wie im obigen Beispiel für ein Fahrzeug – dieser Tatbestand durch Smart Contracts automatisch erkannt wird und Handlungen auslöst. Dies

⁵ <https://www.allianz.com/de/presse/news/engagement/sponsoring/160615-erfolgreiches-pilotprojekt-mit-blockchain-technologie/>



könnte dazu führen, dass die betreffende Person von der Nutzung des Geräts bzw. Fahrzeugs ausgeschlossen wird (etwa indem Zugangsdaten gesperrt werden).⁶

Die wohl bekannteste bestehende Plattform für Smart Contracts ist Ethereum. Das Konzept von Ethereum wurde erstmals 2013 von Vitalik Buterin allgemein beschrieben, 2015 wurde der Betrieb der Plattform gestartet. Ethereum zielt darauf ab, eine Blockchain anzubieten, die über eine Turing-vollständige Programmiersprache verfügt – d.h. universell programmierbar ist – und dazu genutzt werden kann, Smart Contracts für beliebige Anwendungen zu kreieren. Als verteiltes System mit einer eigenen öffentlichen, konsensbasierten Blockchain verwendet Ethereum die Kryptowährung Ether als Zahlungsmittel für Rechenleistung, die die Teilnehmer des Systems zur Verfügung stellen. Neben Smart Contracts soll Ethereum die Bildung von sog. „dezentralen autonomen Organisationen“ (Decentralized Autonomous Organizations, abgekürzt DAOs) ermöglichen (Buterin, 2013). DAOs stellen im Grunde digitale Unternehmen dar, deren Geschäftsordnungen unveränderlich in einem eigenen Code festgelegt sind und in denen sämtliche Entscheidungen über einen dezentral erarbeiteten Konsens über die Blockchain getroffen werden. Ein Vorstand, eine Geschäftsführung oder ähnliche Gremien bestehen in einem solchen System nicht.

Wenngleich Ethereum enorme Potenziale eingeräumt werden, so gab es in der Vergangenheit wie auch heute noch Probleme, die zeigen, dass die Entwicklung von Plattformen für Smart Contracts noch nicht vollständig ausgereift ist. Beispielsweise wurden Angriffe auf das System durchgeführt, die Clients zum Absturz brachten und das Netzwerk verlangsamten, etwa indem das System mit massenhaften Spam-Transaktionen geflutet wurde. Der schwerste Angriff auf Ethereum war ein Hack einer DAO, bei der die Angreifer große Teile des Kapitals der DAO abziehen konnten. Ethereum reagierte darauf mit einem sog. Hard Fork – einer Änderung im Blockchain-Protokoll, die neue Regeln in die Clientsoftware einführt, wobei alle nicht updatenden Nutzer ausgesperrt werden. Dadurch wurde quasi eine vollkommen neue Blockchain geschaffen, das Kapital konnte der Kontrolle der Angreifer wieder entzogen und auf eine neue Adresse transferiert werden. Geldgeber der DAO konnte darüber ihre Einlage wieder zurückfordern. In der Geschichte von Ethereum war dies nicht das erste und letzte Mal, dass ein solcher Hard Fork durchgeführt wurde und somit quasi neue Blockchains geschaffen wurden.⁷ Ein weiteres Problem stellt wie bei allen Blockchains die Skalierbarkeit dar, da die auf den Rechnern der Teilnehmer gespeicherten Kopien mit jedem neuen Smart Contract zusätzlichen Speicherplatz benötigen.

⁶ <https://www.datenschutzbeauftragter-info.de/smart-contracts-vertragsabwicklung-durch-computer/>

⁷ <https://www.heise.de/newsticker/meldung/Kryptowaehrung-Ethereum-Crowdfunding-Projekt-DAO-um-Millionen-beraubt-3240675.html>



Es bestehen weitere Problemstellungen bei Smart Contracts, die es zu lösen gilt. Eine davon betrifft die Eigenschaft der Unveränderlichkeit in der Blockchain: Da ein Smart Contract, sobald er in der Blockchain hinterlegt ist, nicht verändert werden kann, können Spezifikations- und Programmierfehler schwere Folgen haben. Hat der Entwickler eines Smart Contracts keine Funktion implementiert, die es ermöglicht, einen Smart Contract im Notfall anzuhalten oder zu deaktivieren, kann zudem bei Zweckentfremdung des Smart Contracts ohne aufwändige Eingriffe in das Verhalten der Blockchain keine schützende Maßnahme ergriffen werden.

Ein Smart Contract kann in verschiedenen Programmiersprachen implementiert werden. Unter anderem ist es möglich, diese in Serpant, LLC, Mutan oder Solidity zu schreiben. Allen Programmiersprachen ist gemein, dass der Quellcode zu einem Kompilat übersetzt werden muss und nicht wie bei Skriptsprachen interpretiert wird. Um einen Smart Contract ausführbar zu machen, wird zuerst der Sourcecode mittels eines Compilers in Bytecode umgewandelt, welcher in einer Laufzeitumgebung ausgeführt werden kann.

Weiters müssen sich die Parteien auf einen Provider für externe Daten einigen (der diese in die Blockchain einspeist) und auch darauf, was passiert, falls dieser ausfällt. Der Provider – ein sogenannter „Oracle“ - muss in diesem Sinne wieder eine Trusted Third Party darstellen.

Generell erscheint eine Entwicklung und Implementierung von Smart Contracts schwierig, wenn Situationen die Umkehrung von Transaktionen oder eine subjektive Analyse verlangen, die Umwandlung in Code von sehr komplexen oder unklaren bzw. nicht eindeutigen Grundsätzen (zB interpretierbare Standards) nötig ist oder sehr umfangreiche externe Daten aus vielen verschiedenen Quellen für die Durchsetzung des Vertrags benötigt werden (Chamber of Digital Commerce, 2016).

3.2 Cyber Security

Aufgrund ihrer grundlegenden Eigenschaften eignet sich die Blockchain-Technologie für den Einsatz als Cyber Security-Tool. Dabei sind insb. zwei Merkmale der Blockchain von Bedeutung: Der dezentrale Ansatz des Systems und die Unveränderlichkeit der Daten, sobald diese in der Blockchain enthalten sind.

Der dezentrale Aufbau einer Blockchain, bei dem mehrere identische Kopien der Daten auf verschiedenen Knoten des Netzwerks bestehen, führt dazu, dass in einem auf der Blockchain basierten System kein „Single Point of Failure“ besteht. Bei einem zentralen System kann ein Angreifer bei einer erfolgreichen Attacke dieses manipulieren und Kontrolle über wesentliche Systembestandteile erhalten. Illegale Eingriffe in das System können zudem auch von innen heraus erfolgen und Daten gestohlen, gelöscht oder verändert werden. Dazu kommt das Risiko von System-



störungen, zB durch Serverausfälle, Softwarefehler etc.

Bei einem Blockchain-basierten System würden diese Risiken minimiert: Da die Datenkopien auf vielen verschiedenen Knoten des Netzwerks gespeichert sind, müsste ein Eingriff auf der Mehrzahl dieser Knoten gleichzeitig erfolgen – was einen vielfach höheren Aufwand verlangen würde als ein Eingriff auf eine zentrale Stelle. Auch der Ausfall einzelner Knoten oder der Verlust einzelner Kopien würde das System nicht wesentlich beeinträchtigen (UK Government Office for Science, 2016).

In zentralisierten Systemen ist der Aufwand, die Korrektheit der Daten und die Sicherheit gegenüber Manipulation von innen wie außen zu gewährleisten hoch. Vor der Implementierung eines Sicherheitssystems müssen zuerst detaillierte Gefahrenmodelle entwickelt und Sicherheitsanforderungen identifiziert werden. Meist basieren Anti-Virus-, Anti-Malware-Programme und Angreiferkennungssysteme auf der Suche nach Schwachstellen im System und reagieren auf Angriffe bekannter Viren- bzw. Malware-Typen. Bei einem Sicherheitssystem, das auf der Blockchain basiert, kann dagegen ein direkter Ansatz der Sicherung der Daten verfolgt werden – indem deren Korrektheit jederzeit bestätigt werden kann.

Dies wird durch die zweite zentrale Eigenschaft der Blockchain ermöglicht – der Unveränderlichkeit der Daten. Da jeder einzelne Datenblock in der Blockchain ein kryptografisches Abbild des vorherigen Blocks enthält (und damit Abbilder aller vorangehenden Blöcke in der Kette), können vorangehende Datenblöcke nicht manipuliert werden: Würde ein Angreifer dies versuchen und einen bestehenden Datenblock in der Kette verändern, würden sich auch alle nachfolgenden Datenblöcke ändern. Der Eingriff würde sofort sichtbar werden, da die kompromittierte Datenkette nicht zu den Kopien der restlichen Knoten des Netzwerks passt und in weiterer Folge vom System abgelehnt wird (Goldman Sachs, 2016).

Use Case - Guardtime

Ein Vorreiter, der die Blockchain nutzt, um die Datenintegrität von Organisationen sicherzustellen, ist das Unternehmen Guardtime. Auf einer digitalen Plattform werden dabei alle relevanten digitalen Informationen in Form eines verschlüsselten Hash-Wertes einer Blockchain registriert, dadurch wird ein mathematisch überprüfbares Abbild des Netzwerks geschaffen – ein sog. „Clean State of Proof“. Danach können die Daten des tatsächlichen Netzwerks permanent mit dem in der Blockchain gespeicherten, nicht manipulierbaren Abbild verglichen, die Integrität



des Netzwerks überprüft und Eingriffe in bzw. Manipulationen des Netzwerks identifiziert werden.⁸

Ein mögliches Einsatzfeld der Blockchain als Cyber-Security-Instrument (unter vielen) stellt der Schutz von kritischen Infrastrukturen dar. Da digitale Technologien zunehmend in diese integriert werden, sind viele davon auch an das Internet angebunden und stellen daher ein potenzielles Angriffsziel für Cyber-Attacken dar, die zu erheblichen Schäden führen können. Durch den Einsatz von Blockchain Technologie kann sichergestellt werden, dass das Betriebssystem und die Firmware der Infrastrukturen hinsichtlich unerlaubter Änderungen überwacht werden, intakt sind und nicht manipuliert wurden und übertragende Daten (auch von IoT-Systemen) nicht geändert wurden (UK Government Office for Science, 2016).

3.3 Internet of Things (IoT)

Der dezentrale und autonome Aufbau der Blockchain, bei der keine Trusted Third Parties zur Überwachung der Korrektheit der Daten nötig sind und die Teilnehmer des Netzwerks sich nicht zwangsläufig vertrauen müssen, verleiht ihr das Potenzial, ein elementarer Bestandteil des Internets der Dinge (Internet of Things – IoT) zu werden. In einem IoT-Netzwerk kann die Blockchain ein selbstständiges Agieren von vernetzten, intelligenten Geräten (Smart Devices) ermöglichen, ohne dass dabei eine zentrale Instanz benötigt wird.⁹

Das Internet der Dinge verbreitet sich mit zunehmender Geschwindigkeit, damit einher gehen aber auch einige Herausforderungen, die mit den aktuellen Ansätzen nur schwer lösbar sind. So stellen etwa derzeitige, zentralisierte und cloud-basierte IoT-Plattformen einen Kapazitätsengpass für die Kommunikation bei einer hohen Zahl an verbundenen Geräten dar – und gleichzeitig auch einen möglichen Single Point of Failure, der das ganze Netzwerk und die darin verbundenen Geräte beeinträchtigen kann. Ebenso stellt die enorme Menge an Daten, die von den vernetzten Geräten gesammelt wird, ein Sicherheitsrisiko für Nutzer, Unternehmen und auch Regierungen dar. Dazu kommen Fragen bezüglich Kosten der Kommunikation der Geräte, Datenspeicherung und des Serverbetriebs, ebenso wie unterschiedliche Plattformen und Protokolle für die Vernetzung der Geräte.

Durch den Einsatz der Blockchain im IoT wären viele solcher bestehenden Probleme lösbar. Etwa könnten verbundene Geräte direkt über die Blockchain miteinander kommunizieren und über Smart Contracts miteinander interagieren – ohne

⁸ <https://guardtime.com/solutions>

⁹ <http://www.cio.com/article/3027522/internet-of-things/beyond-bitcoin-can-the-blockchain-power-industrial-iot.html>

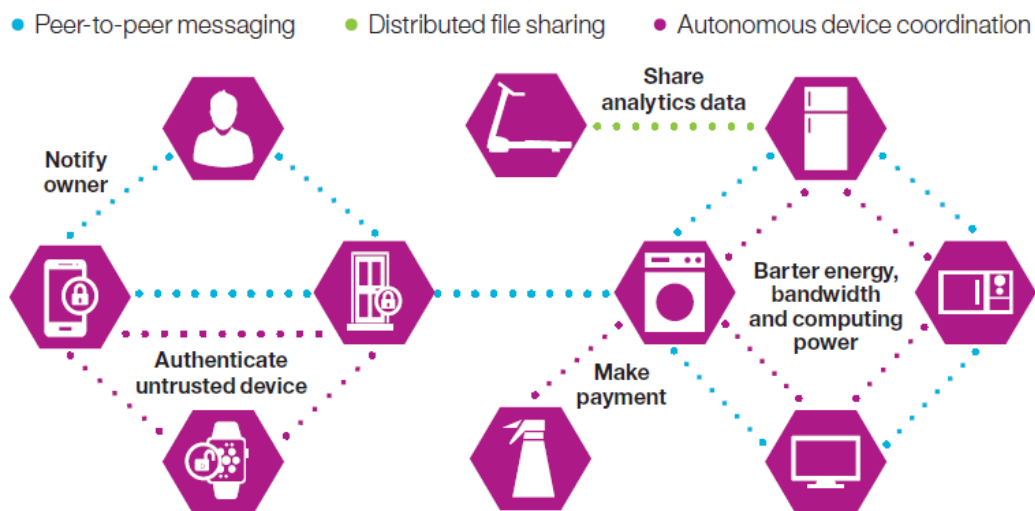


dass ein menschliches Überwachen oder Eingreifen notwendig ist. Durch Smart Contracts und spezifische Konsensmechanismen könnten auch kompromittierte Geräte aus dem Netzwerk ausgeschlossen werden.¹⁰

Durch die Blockchain kann ein IoT-Netzwerk weiter dezentralisiert und den verbundenen Geräten ein höherer Grad an Autonomie verliehen werden. Diese wäre in der Lage selbstständig auf Märkten zu agieren und Transaktionen durchzuführen und so eine „Economy of Things“ zu schaffen. Diese Möglichkeit stellt insb. auch in der Sharing Economy und im Bereich dezentraler Energiesysteme ganz neue Möglichkeiten dar (IBM, 2015).

Die Blockchain unterstützt drei zentrale Funktionen im Internet der Dinge: Die Kommunikation zwischen Geräten (Peer-to-Peer Messaging), einen dezentralen Datenaustausch zwischen den Geräten sowie eine autonome Koordination der Geräte untereinander.

Abbildung 7: Die Funktionsweise der Blockchain im IoT



Quelle: (IBM, 2015)

Ein Einsatz der Blockchain im IoT ließe sich etwa folgendermaßen gestalten: Sobald die Produktion eines Geräts abgeschlossen ist, wird dieses vom Hersteller in der Blockchain angemeldet. Einmal angemeldet, bleibt das Produkt über seine gesamte Lebensdauer eine individuelle Einheit innerhalb der Blockchain. Die Blockchain dient dabei als vertrauenswürdige Produktdatenbank, in der Produktinformationen, Historie und Änderungen am Produkt, Garantiedetails etc. festgehalten werden.

¹⁰ <https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html>



Tiefendossier: Die Blockchain

Durch die Blockchain kann das vernetzte Gerät zudem nicht nur mit anderen Geräten kommunizieren und Daten austauschen sondern sich über Smart Contracts auch mit diesen koordinieren und sogar finanzielle Transaktionen durchführen. Vernetzte Maschinen könnten so zB selbstständig Produktionsmaterialien, Ersatzteile, Reparatur- und Wartungsarbeiten etc. anfordern.

Durch die Blockchain könnten also IoT-Komponenten nicht nur Daten sondern beispielsweise auch Bandbreite, Rechenleistung oder Energie teilen und zuverlässige und verteilte Handelsplätze bilden, in denen Objekte, die sich nicht notwendigerweise vertrauen müssen, handeln und kooperieren können. Es könnten durch diesen Handel in Echtzeit liquide Märkte entstehen, in denen Angebot und Nachfrage mit erhöhter Transparenz und Autonomie koordiniert werden.

Use Case – ADEPT

IBM hat in Zusammenarbeit mit Samsung bereits ein Pilotprojekt durchgeführt, indem eine Waschmaschine mittels Blockchain eigenständige Handlungen durchgeführt hat. U.a. konnte sie durch Smart Contracts selbstständig Waschmittel bestellen und bezahlen, wenn es zur Neige ging. Im Falle eines Schadens konnte sie ihren Garantiestatus überprüfen und einen geeigneten Handwerker bestellen. Darüber hinaus wurde im Rahmen des Prototyps ein Handelsplatz für Energieversorgung geschaffen, in dem die Waschmaschine mit dem Micro-Grid einer Gemeinde kommunizieren und im Gegenzug für Energie mittels eines Vertrages zwischen dem Besitzer und der Gemeinde eine bestimmte Anzahl an Waschgängen für Gemeindemitglieder anbieten konnte (Fraunhofer FIT, 2016).

3.4 Politik und Verwaltung

Der Einsatz der Blockchain in Politik und Verwaltung würde die E-Government-Aktivitäten von Regierungen erheblich unterstützen. Informationen und Datensätze könnten mit geringem Aufwand und gesichert zwischen verschiedenen öffentlichen Einrichtungen und Verwaltungsbereichen ausgetauscht und auf dem neuesten Stand gehalten werden. Daneben könnte eine Vielzahl an innovativen Services für Bürger und Unternehmen durch den Einsatz der Blockchain angeboten werden.



Use Case – Estlands Einsatz der Blockchain im E-Government

Estland ist eines der ersten Länder, dessen Verwaltungsapparat im Bereich E-Government auf die Blockchain setzt – seit 2013 nutzt das Land die Blockchain, um die Informationen in seinen Datenbanken zu authentifizieren. Die Einführung der Blockchain im E-Government von Estland wurde von zwei vorangegangenen Maßnahmen maßgeblich begünstigt: Bereits 2001 führte Estland „X-Road“ ein, ein dezentrales Datenbanksystem, bei dem sämtliche Informationen allen Verwaltungseinheiten zur Verfügung stehen. 2002 führte Estland offiziell die digitale Signatur ein, mit der sich Bürger und Unternehmen elektronisch ausweisen können. Der dezentrale Aufbau des Systems verbunden mit digitalen Signaturen legte den Grundstein für die Implementierung der Blockchain in das E-Government von Estland.

Die estländische Regierung nutzt das Blockchain-basierte Keyless Signature Infrastructure (KSI)-System von Guardtime, um die Daten in den elektronischen Verwaltungsregistern zu authentifizieren. Durch die Blockchain werden neue Informationen in ein verteiltes und transparentes Register gespeichert und die Integrität der Daten gewährleistet.

Mit Unterstützung der Blockchain bietet Estland seinen Bürgern eine Reihe von innovativen elektronischen Services an: Einwohner können mit einer elektronischen ID-Card online wählen, Steuererklärungen abgeben, Testamente hochladen, staatliche Beihilfen beantragen, Einsicht in Schulakten ihrer Kinder erhalten, Online-Banking nutzen, medizinische Rezepte verwalten etc. – insgesamt werden hunderte verschiedene e-Services von der Regierung angeboten.

Unternehmen können online Jahresberichte einreichen, Shareholder-Dokumente veröffentlichen, Lizenzen beantragen und innerhalb von nur wenigen Minuten online gegründet (bzw. registriert) werden.¹ Verwaltungsmitglieder nutzen das System, um Dokumente zu verschlüsseln und sicher zu kommunizieren oder Genehmigungen zu unterzeichnen – sogar im Kabinett wird eine dezentrale Datenbank zur Organisation von Sitzungen verwendet (UK Government Office for Science, 2016).

Neben Estland überlegen zahlreiche weitere Regierungen auf die Blockchain umzusteigen. 2016 kündigte Dubai etwa an, bis 2020 sämtliche Regierungsprozesse auf die Blockchain umzustellen, etwa Gehaltsabrechnungen für öffentlich Bedienstete, Dokumente oder Eigentumstitel. Ebenso hat das Department of Defense in den USA begonnen, in die Blockchain-Technologie zu investieren und will sie für eine sichere Datenübertragung und Cyber-Sicherheitsüberwachung in Datenbanken und anderen Computersysteme einsetzen (Think Consortium, 2016).



Hohes Potenzial für die Blockchain wäre im Bereich der staatlichen Ausgaben denkbar, da diese transparenter und effizienter durchgeführt werden könnten. So könnten etwa die Identitäten von potenziellen Empfängern staatlicher Beihilfen und deren Anspruchsberechtigungen sowie erfolgte Zahlungen in einer Blockchain hinterlegt und in Echtzeit aktualisiert werden, um Sozialbetrug und Überzahlungen zu verhindern. Ebenso könnten – sofern Transaktionen elektronisch über die Blockchain erfolgen würden – die ausbezahlten Mittel hinsichtlich ihres Verwendungszwecks spezifiziert werden (UK Government Office for Science, 2016). Ähnlich ließe sich etwa auch im Steuerwesen vorgehen, sodass auch kost- und zeitintensive Nachbearbeitungen entfallen würden.

Das Department of Work and Pensions der Regierung Großbritanniens hat bereits ein Experiment mit einem Blockchain System zur Verteilung von Sozialhilfegeldern durchgeführt. Dabei hat das Department u.a. mit Barclays, dem Fin-Tech Startuop GovCoin sowie dem University College London zusammengearbeitet. Das System umfasste eine mobile App sowie ein Blockchain-System zur Aufzeichnung von Zahlungen die von Sozialhilfeempfängern getätigt oder empfangen wurden.¹¹

Eine höhere Transparenz und mögliche Zweckbindung von Zahlungen könnten überdies beispielsweise auch im Bereich der Entwicklungshilfe Fortschritte bringen. Betrug und Korruption in Entwicklungsländern führen oft dazu, dass Hilfgelder aus dem Ausland versickern und nur wenig Wirkung zeigen. Durch die Nachverfolgbarkeit der Geldflüsse und eine eventuelle Zweckbindung der Mittel (zB zum Bau von Schulen) könnte sichergestellt werden, dass die Mittel in den dafür vorgesehenen Bereichen landen (UK Government Office for Science, 2016).

Die Blockchain könnte auch die Buchhaltung und Steuerzahlungen revolutionieren. Steuerzahlungen könnten langfristig deutlich effizienter durch Smart Contracts auf der Blockchain am Tag der Bezahlung von Rechnungen direkt an den Staat transferiert werden. Der aufwendige Erfassungsprozess durch Buchhaltungsabteilungen der betroffenen Firmen sowie deren Steuerberater, könnte langfristig somit abgeschafft werden. Korruption und Steuerhinterziehung werden von vornherein vermieden (Technologiestiftung Berlin, 2016).

Eine ebenfalls diskutierte Möglichkeit, die Blockchain in der Politik zu verwenden, stellen Wahlen dar. Hier könnten den Bürgern weitere Wahlrechte eingeräumt werden und Wahlen mittels der Blockchain abgehalten werden. Vorstellbar wäre es etwa, dass statt periodischen Wahlperioden im Papierformat eine Art „Dauerwahl-system“ implementiert wird, bei dem Wähler in kürzeren Wahlperioden ihre Stimme online abgeben können. Über die Blockchain könnte sichergestellt werden, dass die Stimmen ordnungsgemäß in die Wahlauswertung einfließen und kein

¹¹ <http://www.coindesk.com/uk-government-trials-blockchain-welfare-payments-system/>



Wahlbetrug vorliegt. Ebenfalls ließen sich mittels Blockchain Volksabstimmungen schnell, flexibel und kostengünstig durchführen.¹²

3.5 Eigentumsrechte

Ein weiteres potenzielles Anwendungsfeld der Blockchain ist der Schutz von Eigentumsrechten. Diese können in der Blockchain mit einem Zeitstempel und der digitalen Signatur des Eigentümers registriert werden und dadurch transparent und mit relativ wenig Aufwand deren Eigentümer zweifelsfrei bestimmt werden. Durch die Registrierung der geistigen Eigentumsrechte (IPR) von Unternehmen in einer Blockchain statt traditionell über Patentanmeldungen könnten etwa aufwändige und kostenintensive Patentprozesse vermieden werden (UK Government Office for Science, 2016).

Use Case – Die Blockchain in der Musikindustrie

In der Musikindustrie hat das Start-up Mycelia intelligente Songs entwickelt, in welche Smart Contracts eingebaut sind, wodurch Tantiemen und Lizenzvereinbarungen automatisch durchgesetzt werden und die Künstler dadurch direkt bezahlt werden. So können sie ihre Songs über das Internet direkt an Hörer verkaufen, ohne dass ein zwischengeschaltetes Label dafür notwendig ist, welches einen Großteil der Einnahmen einstreichen würde. Ein weiteres Beispiel ist Ascribe, ein Start-up, über dessen Blockchain Künstler ihre Werke uploaden, mit einem Wasserzeichen als einzig gültige Version kennzeichnen und über das Netzwerk teilen können – ähnlich den Transaktionsvorgängen von Bitcoin.¹

Die Blockchain kann wie in obigen Beispiel nicht nur in der Kreativwirtschaft sondern in allen Industriezweigen zum Schutz vor Nachahmung eingesetzt werden. Beispiele dafür sind die Pharmaindustrie, in der damit die Verbreitung von gefälschten Arzneimitteln verhindert werden kann, gleiches gilt zB auch für die Luxusgüter- und Elektronikindustrie. Die Plattform BlockVerify bietet solche Lösungen zum Schutz vor Nachahmungen: Das Produkt wird mit einer Kennzeichnung versehen, seine Echtheit validiert und in der Blockchain registriert. Danach können Händler und Konsumenten die Echtheit und die Herkunft des Produkts über eine Smartphone-App überprüfen (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015).

¹² <http://www.computerwoche.de/a/blockchain-im-einsatz,3316539>



Der Schutz von geistigen Eigentumsrechten wird voraussichtlich durch die zunehmende Individualisierung der Produktion in den kommenden Jahren noch deutlich stärker an Bedeutung gewinnen. Durch 3D-Druck-Verfahren soll in Zukunft etwa eine kundenindividuelle Massenproduktion ermöglicht werden. Allerdings stellt der Schutz der IPR dabei eine große Herausforderung dar. Durch die Blockchain könnten Hersteller Metadaten zu ihren Produkten, wie etwa die verwendeten Substanzen, registrieren und ihr Produkt vor Nachahmung schützen.

3.6 Sharing Economy

Die Sharing Economy – die „Ökonomie des Teilens“ gilt als einer der größten globalen Wirtschaftstrends und soll zu einer effizienteren Nutzung von Ressourcen führen. In diesem Konzept besitzen Kunden keine Produkte sondern nutzen diese vorübergehend und bezahlen dafür eine Nutzungsgebühr. In der kommerziell orientierten Sharing Economy ermöglicht es durch die massenhafte Verbreitung von Internet und Smartphone Anbieter sowie Nutzer in Sekundenschnelle zu verbinden – und das global. Zu den bekanntesten Beispielen der Sharing Economy zählen die Beherbergungsplattform Airbnb und der Fahrdienstvermittler Uber.

Die Blockchain kann dazu beitragen, Vertrauen zwischen Anbietern und Kunden in der Sharing Economy aufzubauen und diese weiter voranzutreiben. Sie ermöglicht eine eindeutige Identifizierung von Anbietern und Kunden sowie die Entwicklung von „Reputationsmanagement“-Systemen, wodurch sowohl Anbieter und Kunde leichter die „Qualität“ der Gegenseite beurteilen können, da über diese umfangreiche und authentifizierte Informationen vorliegen. In solch einem System könnte die Blockchain als Register für Anmeldedaten und den Verlauf geschäftlicher Interaktionen dienen, welches plattformübergreifend genutzt werden kann. So können etwa Personendaten (zB Ausweisdaten) sicher in der Blockchain gespeichert, authentifiziert und mit vergangenen Zahlungsinformationen verknüpft werden, um die Verlässlichkeit von potenziellen Kunden feststellen zu können. Dazu können eine weitere Reihe von Daten angehängt werden, zB Reviews. Da die Sharing Economy maßgeblich vom Vertrauen zwischen Anbieter und Kunde abhängig ist und Verträge umso schneller zustande kommen, je höher das Vertrauen zwischen den Parteien ist, könnte die Blockchain als „Vertrauensinstrument“ erheblich zur Verbreitung des Konzepts der Sharing Economy beitragen (Goldman Sachs, 2016).

Airbnb hat mit der Übernahme des Start-ups ChangeCoin im Jahr 2016 bereits den ersten Schritt zur Implementierung der Blockchain in das Geschäftssystem unternommen, um das Reputationsmanagement auf der Plattform zu erleichtern. Analysten von Goldman Sachs gehen davon aus, dass sich das wirtschaftliche Potenzial der Blockchain in der Beherbergung in einen Umsatzwachstum von \$ 3-9 Mrd. niederschlagen könnte (Goldman Sachs, 2016).



Für Plattformen wie Airbnb und Uber kann die Blockchain aber nicht nur ein effizientes Hilfsmittel darstellen sondern auch eine ernstzunehmende Bedrohung. Denn auch wenn die beiden Plattformen auf den ersten Blick wie dezentralisierte P2P-Netzwerke wirken, so sind im Grunde doch beide zentralisierte Systeme, bei denen Transaktionen über die Infrastrukturen und Software der Unternehmen laufen. Diese verlangen nicht nur Gebühren, sondern haben auch die Kontrolle über die Plattformen und können Konditionen jederzeit ändern.¹³

Durch die Blockchain ist es allerdings möglich, dass zentrale Autoritäten innerhalb der Sharing Economy wie Airbnb und Uber nicht mehr nötig und Anbieter und Kunden direkt miteinander vernetzt sind. Kommunikation und Informationsaustausch, Bezahlung und Inanspruchnahme der Leistung könnten direkt zwischen den Parteien stattfinden und Kosten für die zentralen Vermittler entfallen.¹⁴ Solch ein System wird mitunter als „echte Sharing Economy“ oder „Sharing Economy 2.0“ bezeichnet.

Use Case – Arcade City

Arcade City ist eine App, die ein Blockchain-basiertes System für Fahrdienstleistungen anbietet, und damit Uber Konkurrenz machen will. Über die Ethereum-Blockchain verbindet sie Fahrer mit Kunden in einem P2P-Netzwerk, die Fahrpreise werden nur zwischen Fahrer und Fahrgast verhandelt. Der Fahrer wird so selbst zum Unternehmer und kann durch das Wegfallen eines zentralen Vermittlers wie Uber mehr vom Fahrgeld behalten und dies in Form von günstigeren Preisen an den Kunden weitergeben.¹

Generell kann die Blockchain dazu führen, dass in Zukunft vermehrt nutzungs-basierte Preismodelle anstatt der bisherigen Kaufmodelle angewendet werden. Produkte würden dann nicht einmalig zu einem bestimmten Preis verkauft werden, sondern die Bezahlung nach dem Ausmaß der Nutzung der Produkte erfolgen. Vorstellbar wäre dies zB auch bei Computerprozessoren, wo die Hersteller Zahlungen von ihren Kunden abhängig von der Häufigkeit und vom Ausmaß der Kapazitätsnutzung verlangen könnten. Hersteller von Fahrzeugen würden diese nicht einmalig verkaufen, sondern durch intelligente Fahrzeuge und Smart Contracts automatisch nach jeder Fahrt bezahlt werden. So würden relativ langfristige und gleichmäßige Cashflows entstehen, bei denen der Nutzer auch wirklich nur jene Leistung bezahlt, die er in Anspruch nimmt (Ernst & Young, 2016).

¹³ <http://www.nasdaq.com/article/move-over-uber-blockchain-technology-can-enable-real-sustainable-sharing-economy-cm716709#ixzz4ZV2HtvFG>

¹⁴ <https://www.ibm.com/developerworks/library/iot-blockchain-sharing-economy/>



3.7 Dezentrale Energieversorgung

Die Energiewirtschaft ist ein weiterer Sektor, in dem die Blockchain in Zukunft ihr disruptives Potenzial entfalten könnte, indem sie zur Dezentralisierung der Energieversorgung eingesetzt wird. Mittels Blockchain könnten lokale Energieproduzenten und -konsumenten in einem dezentralisierten echtzeitbasierten Energiemarkt miteinander verbunden werden und damit eine flexible Energieversorgung mit Bürgern und Unternehmen als aktive Marktteilnehmer ermöglichen.

Derzeit erfolgt die Bereitstellung von Energie bzw. Strom durch relativ wenige, große Energieversorger. Diesem System inhärent sind einige bedeutende Schwachstellen: Durch lange Wege vom Energieerzeuger zum Verbraucher gehen signifikante Energiemengen verloren. Die relativ zentralisierte Infrastruktur führt zu hohen Ausfallrisiken, Stromausfälle durch einen Kraftwerks- oder Leitungsausfall führen zu massiven Kosten in der Wirtschaft. Und insb. kurzzeitige Angebots- und Nachfrageschwankungen sind nur schwer auszugleichen, i.d.R. sind Anbieter dazu gezwungen, mehr Energie bereitzustellen als tatsächlich verbraucht wird (Goldman Sachs, 2016).

In einem dezentralisierten Energiemarkt, in dem Einzelpersonen und Unternehmen nicht nur als Energieverbraucher sondern auch als eigenständige Energieversorger agieren, können diese Probleme deutlich eingeschränkt werden. Die Verbreitung von Anlagen zur Erzeugung regenerativer Energien wie etwa Photovoltaik-Anlagen, Smart Meters und Fortschritte bei der Energiespeicherung stellen die Basis für einen dezentralisierten Energiemarkt dar. Die dezentral organisierte Blockchain könnte dabei eingesetzt werden, um sichere und schnelle Transaktionen zwischen einer hohen Anzahl an Parteien zu ermöglichen und ein Peer-to-Peer-Verkaufsnetz zu fördern. Potenzial bietet sich dabei v.a. bei kleinen und lokalen Mikronetzen. Je mehr Teilnehmer aber in einem solchen Netz vorhanden sind, desto höher wären dessen Verlässlichkeit und Effizienz hinsichtlich des Matchings zwischen Angebot und Nachfrage.

In Verbindung mit dem Internet der Dinge könnte die Blockchain zudem eine automatische Festlegung von Energiepreisen ermöglichen: Anbieter könnten automatisch Informationen über ihre überschüssige Energie senden (und wie lange diese zur Verfügung steht) und Nutzer automatisch ihren Energiebedarf. Basierend auf einer Blockchain können Computer bzw. Smart Devices automatisch Preise verhandeln und Transaktionen durchführen. Dies könnte in Form von Smart Contracts geschehen, in denen eine „if-then“-Bedingung festlegt, wann eine Transaktion zustande kommt.



Use Case – Brooklyn Micro Grid

In New York baut das Start-up LO3 Energy bereits einen Prototypen für ein Blockchain-basiertes Peer-to-Peer Energienetzwerk auf, in dem Bewohner in den Vierteln Gowanus und Park Slope in Brooklyn mit Solaranlagen erzeugten Strom verkaufen können.

Das Microgrid in Brooklyn, das als Pilotprojekt von LO3 Energy startete, wird derzeit mit Hilfe der Siemens-Geschäftseinheit Digital Grid in den USA weiterentwickelt. Hierbei wird erstmals eine Microgrid-Control-Lösung von Siemens mit der TransActive Grid genannten auf der Blockchain-basierten Peer-to-peer-Handelsplattform von LO3 Energy vereint.¹

Der Einsatz der Blockchain im Bereich der Energieversorgung könnte durch den Anreiz für Einzelpersonen und Unternehmen, eigenständige Energieversorger zu werden, auch dazu führen, dass Technologien, die für ein verteiltes Energienetz nötig sind, weitere Verbreitung erfahren. Dies betrifft etwa Anlagen zur Erzeugung erneuerbarer Energien wie PV-Anlagen, IoT-Applikationen und auch Elektrofahrzeuge. Insgesamt schätzt Goldman Sachs das Potenzial der Blockchain bei Smart Grids auf \$ 2,5-7 Mrd. pro Jahr – nur für die USA (Goldman Sachs, 2016).

In Österreich beteiligt sich die Wien Energie gemeinsam mit anderen internationalen Energieunternehmen an einem von BTL GROUP LTD, einem kanadischen Blockchain startup, durchgeführten Blockchain Pilotprojekt. Im Rahmen des Pilotprojekts testet Wien Energie die Tauglichkeit der neuen Blockchain-Technologie für eine Tradingplattform im internationalen Gashandel.¹⁵

Die Blockchain kann nicht nur in Smart Grids sondern auch im Bereich der E-Mobilität eingesetzt werden. Der deutsche Energieanbieter RWE ging etwa eine Kooperation mit dem Unternehmen Slock.it ein, um die Blockchain für die Bezahlung an Ladestationen von Elektroautos einzusetzen. Damit soll ein einheitliches und kostengünstiges Bezahlssystem geschaffen werden, das ohne physische Bezahlstationen auskommt. In Zukunft sollen dann etwa Elektroautos während Stehzeiten an Ampeln mittels Induktion geladen werden, die Bezahlung der dabei relativ geringen Geldbeträge soll kostengünstig und automatisch über die Blockchain erfolgen. Das stationäre Laden im Stadtverkehr würde dabei überflüssig werden.¹⁶

¹⁵ http://www.ots.at/presseaussendung/OTS_20170214_OTS0055/wien-energie-testet-blockchain-technologie

¹⁶ <http://www.computerwoche.de/a/blockchain-im-einsatz,3316539>



Use Case – Blockchain Car eWallet

Der Automobilzulieferer ZF Friedrichshafen AG hat gemeinsam mit UBS und innogy Innovation Hub das Car eWallet entwickelt, das mehrere komfortable Zahl- und Abrechnungsfunktionen bietet. Das Car eWallet erlaubt Nutzern die „on-the-go“-Bezahlung von Autobahnmaut sowie Park- und Ladegebühren. Gleichzeitig kann es Zahlungen entgegennehmen: etwa aus dem Car-Sharing, der Bereitstellung von Energie für das Stromnetz oder für Liefer-Services. Das innogy Innovation Hub hat Anforderungen aus der Lade-Infrastruktur in das System integriert – dadurch kann das Car eWallet den Bezahlvorgang automatisch und sicher nach dem Laden der Batterie abschließen.

Nutzer können die Wallet entweder vom heimischen PC oder mittels einer speziellen App durchführen. Damit wird das Auto vom Besitzer des Car eWallet autorisiert, eigenständig Zahlungen bis zu einem bestimmten Limit durchzuführen. Wird beispielsweise auf der morgendlichen Fahrt ins Büro eine Maut fällig, zahlt das Auto automatisch die Gebühren und erspart zeitraubendes Stehen in der Warteschlange. Der Fahrer wird erfasst während er im Auto bleibt, gleichzeitig erhält der Nutzer online einen Update über alle Transaktionen des Car eWallet.¹⁷

3.8 Wertschöpfungsketten

Die Wertschöpfungsketten der modernen Wirtschaft werden stetig komplexer und an der Herstellung eines Produkts sind zahlreiche Akteure beteiligt. Die Blockchain kann ein geeignetes Instrument darstellen, um die Transparenz innerhalb von Wertschöpfungsketten bzw. -netzwerken zu erhöhen. Mittels Blockchain kann eine ordnungsgemäße Zugangskontrolle für Daten, die zwischen den Teilnehmern der Wertschöpfungskette geteilt werden, ermöglicht werden. Durch den kontinuierlichen Echtzeitzugriff auf zuverlässige, geteilte Daten in der Blockchain kann die Wertschöpfungskette effizienter gestaltet werden als in traditionellen Systemen.

Use Case – Blockchain in der Bergbauindustrie

BHP Billiton, eines der größten Bergbauunternehmen der Welt, hat Ende 2016 begonnen, die Ethereum Blockchain zu nutzen, um damit die Supply-Chain-Prozesse neu zu organisieren. Das Unternehmen will die Blockchain nutzen, um Bewegungen von Gesteins- und Flüssigkeitsproben zu erfassen, die von verschiedenen Lieferanten bezogen werden, sowie Echtzeit-Daten, die während der Lieferung entstehen zu sichern. Dabei arbeitet BHP mit den Blockchain-Startups Block-

¹⁷ http://www.zf.com/corporate/de_de/press/list/release/release_29127.html



Apps und Consensus zusammen.

BHP ist laut eigener Aussage in nahezu allen Prozessbereichen stark von externen Anbietern abhängig, mit Geologen und Lieferunternehmen werden Verträge über die Sammlung und Analyse der Proben geschlossen, daneben sind weitere zahlreichen Parteien rund um den Globus in die Geschäftsprozesse involviert. Durch die Blockchain verspricht sich das Unternehmen, dass die Datenerfassung, Speicherung und Analyse deutlich erleichtert wird, und man jederzeit einen Überblick darüber hat, wo sich die Materialien gerade befinden.¹⁸

Konsumenten verlangen mehr und mehr nach Transparenz von Produkten, etwa bezüglich deren Herkunft, des Herstellungsverfahrens, der Produktinhalte und mehr, zudem steigen auch regulatorische Anforderungen an die Hersteller. Die Blockchain ermöglicht einen sicheren digitalen Transfer von Eigentum über die komplette Wertschöpfungskette hinweg, und die im Laufe des Prozesses erbrachten Leistungen der einzelnen Akteure sind für alle Teilnehmer der Wertschöpfungskette sichtbar. Durch die Rückverfolgbarkeit aller Prozessschritte wird nicht nur die Wertschöpfungskette für deren Teilnehmer transparenter und dadurch effizienter, auch für Verbraucher und Verwaltung verbessert sich die Informationslage (IBM, 2016b). Der US-Handelsriese Walmart hat diesbezüglich eine Zusammenarbeit mit IBM und der Tsinghua Universität in Peking gestartet, um die Bewegungen von chinesischem Schweinefleisch digital über die Blockchain nachzuverfolgen und will so die Lebensmittelsicherheit erhöhen.¹⁹

Insbesondere bei komplexen Produkten wie Fahrzeugen, Flugzeugen, Produktionsanlagen etc. ist die Herkunft der einzelnen Produktkomponenten oft schwer nachzuverfolgen. In einer Blockchain können alle Herkunftsinformationen wie zB Angaben zu Hersteller, Produktionsdatum, Charge, Maschinenprogramm bei der Produktion etc. für sämtliche Produktkomponenten gespeichert werden. Der Zugang zu den Informationen kann für den OEM, sämtliche Zulieferer, Inhaber der Produkte, Wartungs- und Reparaturdienstleister und Regulatoren o.ä. bestehen. Der Vorteil darin läge in einem höheren Vertrauen unter den Teilnehmern der Wertschöpfungskette, da diese Informationen nicht nur in der Hand eines Teilnehmers (etwa dem OEM) liegen, auch könnten Wartungsarbeiten an Geräten und Produktfehlern leichter durchgeführt werden. Produktrückrufe könnten zudem etwa deutlich spezifischer und in geringerem Ausmaß durchgeführt werden (IBM, 2016b). Der japanische Automobilkonzern Toyota hat bereits begonnen, mit der Blockchain die Tausenden Teile zu verfolgen, die durch verschiedene Länder, Fabriken und Lieferan-

¹⁸ <http://www.coindesk.com/bhp-billiton-blockchain-mining-company-supply-chain/>

¹⁹ <http://fortune.com/2016/10/19/walmart-ibm-blockchain-china-pork/>



ten transportiert werden, um ein einzelnes Auto herzustellen.²⁰

Use Case – Die Blockchain in der Diamantenindustrie

Eine Branche, die die Blockchain bereits zur Rückverfolgung ihrer Produkte einsetzt, ist die Diamantenindustrie. Diese ist besonders anfällig für kriminelle Aktivitäten: Transaktionen werden oft vertraulich durchgeführt, Diamanten können leicht geschmuggelt werden und werden oft zur Geldwäsche oder zur Finanzierung krimineller oder terroristischer Aktivitäten verwendet. Die Nachverfolgung der Diamanten gestaltet sich dabei schwierig, da diesbezügliche Dokumente (im Papierformat) vielfach gefälscht werden. Aus diesem Grund hat die Diamantenindustrie damit begonnen, die Blockchain für die Nachverfolgung einzusetzen.

Das Everledger System stellt für jeden einzelnen Diamanten einen eigenen digitalen „Reisepass“ aus: Zuerst werden eine elektronische Identität für jeden Diamanten, die spezifischen Eigenschaften des Diamanten und eine eingravierte Seriennummer digitalisiert und in die Blockchain eingefügt. Anschließend wird für den Diamanten ein digitaler „Reisepass“ erstellt, der die Transaktionshistorie, Herkunft und Bewegungen des Diamanten aufzeichnet. Jede Veränderung im „Reisepass“ wird in die Blockchain eingefügt. Dadurch können bei jeder neuen Transaktion der Ursprung des Diamanten, bisherige Transaktionen und Eigentumswechsel und eventuelle Veränderungsprozesse am Stein geprüft werden. Das System beinhaltet auch Smart Contracts, in denen die Geschäftsbedingungen für den Verkauf und Transport der Diamanten festgelegt werden können (UK Government Office for Science, 2016).

3.9 Verteilte Datenspeicherung

Cloud Computing gilt als eine der zentralen Technologien der Digitalisierung, jedoch könnte die Blockchain schon bald ebenfalls zur verteilten Speicherung von Daten und Rechenleistung genutzt werden. Im derzeitigen Cloud-System dienen die Cloud-Anbieter als Trusted Third Party, durch eine meist relativ zentrale Speicherung von Daten (gemäß Standard müssen in der Regel drei Kopien der Daten angelegt werden) bestehen aber Sicherheitsrisiken. Per Blockchain können die Daten verteilt auf vielen Rechnern und mit End-to-End-Verschlüsselung sicher gespeichert werden, ohne dass eine Trusted Third Party mit einbezogen werden muss (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015).

²⁰ <https://www.ibm.com/developerworks/cloud/library/cl-blockchain-for-cognitive-iot-apps-trs/index.html>



Use Case – Storj

Eine Plattform, die eine „verteilte Cloud-Speicherung“ von Daten anbietet, ist das Storj Netzwerk. In diesem können Nutzer ihre Daten mit einem Private Key verschlüsseln und in einem Peer-to-Peer-Netzwerk speichern. Jeder Teilnehmer des Netzwerks kann dabei seinen freien Festplattenspeicherplatz vermieten. Will ein Nutzer seine Daten im Netzwerk speichern, wird die Datei zuerst in mehrere kleinere Dateien bzw. Stücke aufgeteilt, die dann verschlüsselt werden. Anschließend werden für die verschlüsselten Dateien Hashwerte gebildet, die zur Identifikation sowie der Sicherstellung der Integrität der Dateien dienen – ohne das auf die Dateien selbst zurückgegriffen werden muss und deren Inhalt sichtbar wäre. Anschließend wird durch einen Konsensmechanismus Ablageort und die Integrität der Dateien bestimmt. Die Preise für die Nutzung des fremden Festplattenspeicherplatzes werden dabei durch Angebot und Nachfrage bestimmt. Anbieter von Speicherplatz können den minimalen Preis festlegen, den sie für ihre Ressourcen erhalten möchten, Kunden den maximalen Preis, den sie zu zahlen bereit sind (Berkeley University of California - Sutardja Center for Entrepreneurship & Technology, 2015).

Die Blockchain könnte allerdings nicht nur zur verteilten Speicherung von Daten genutzt werden sondern auch zu einer verteilten Auslagerung von Rechenleistung. Die Blockchain kann ein anonymes, peer-to-peer basiertes Vertrauen bieten und große, komplexe Netzwerke verwalten, in dem Geräte sicher miteinander kommunizieren und sich selbstständig organisieren können. So könnten ähnlich zur verteilten Datenspeicherung über die Blockchain auch freie Rechenleistung angeboten und Datenzentren eingespart werden.

Insbesondere in der Verbreitung des Internet der Dinge schlummert dabei enormes Potenzial: Wenn in Zukunft Milliarden in unterschiedlichsten Geräten integrierte Computer über das Internet kommunizieren, wird die verfügbare Rechenleistung deutlich steigen – insb. da diese Computer nicht rund um die Uhr ausgelastet sein werden. Die frei werdende und nicht genutzte Rechenleistung könnte durch eine Blockchain organisiert werden und gleichzeitig wäre es denkbar, die intelligenten Geräte im IoT zu einem gewaltigen Rechnernetzwerk zu verbinden (Ernst & Young, 2016).

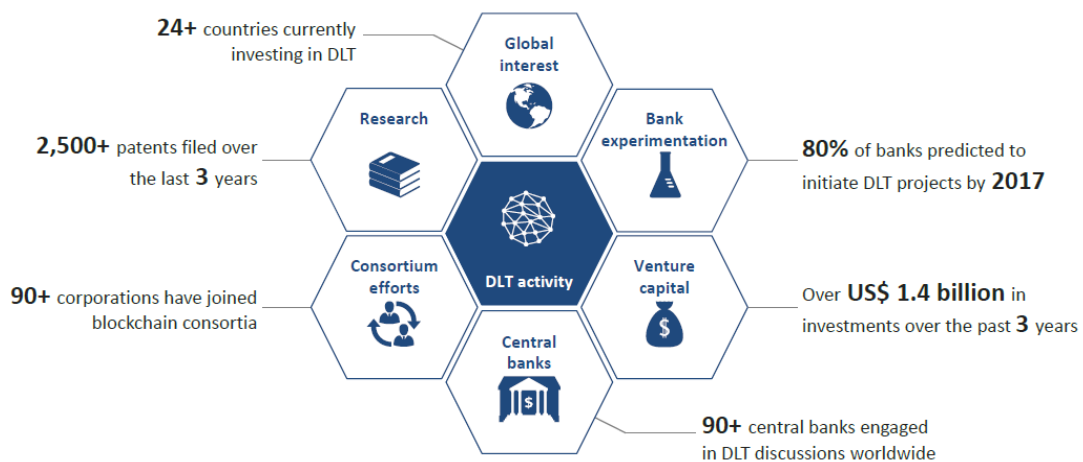


4 Key Players im Bereich der Blockchain

Die Blockchain hat in den vergangenen Jahren zunehmend an Aufmerksamkeit erfahren – zuerst vor allem aus der Finanzwelt, mittlerweile beschäftigen sich aber zahlreiche große Technologieunternehmen und Regierungen mit der Thematik. Estland gilt als ein Vorreiter beim Einsatz der Blockchain im Bereich der öffentlichen Verwaltung und verlässt sich schon seit mehreren Jahren auf die Sicherung der Integrität seiner Daten mittels Blockchain-basierten Technologien. Immer mehr Regierungen unternehmen nun erste Schritte, um den Einsatz der Blockchain in der Verwaltung voranzutreiben. Dazu gehört auch die Regierung Englands, die sich umfassend mit den Möglichkeiten von Distributed-Ledger Systemen befasst und andenknt, in Zukunft kritische Infrastrukturen durch die Blockchain überwachen zu lassen²¹. 2016 investierten bereits mehr als 24 Staaten in Blockchain-basierte Systeme.

Auch die Wirtschaft sieht in der Blockchain hohes Zukunftspotenzial, alleine zwischen 2014 und 2016 wurden über \$ 1,4 Mrd. an Venture Capital in Blockchain- und verwandte Start-ups investiert und über 2.500 Patente im Bereich Distributed Ledger Systeme angemeldet.

Abbildung 8: Aktivitäten rund um die Blockchain und Distributed Ledger Systeme (Stand 2016)



Quelle: (Credit Suisse, 2016)

²¹ <https://guardtime.com/blog/guardtime-and-future-cities-catapult-partner-to-develop-blockchain-based-cybersecurity-for-uk-critical-infrastructure>



4.1 Key Players im Bereich der Blockchain

Auf den nächsten Seiten werden einige internationale Unternehmen dargestellt, die sich mit der Anwendung der Blockchain-Technologie befassen.

* Guardtime

Guardtime ist ein Cyber-Security Unternehmen, das die Blockchain als Basis seiner Produkte nutzt. Es wurde 2007 in Estland gegründet und hat seinen Hauptsitz in Amsterdam. Kern des Produktportfolios von Guardtime ist das digitale Signatursystem Keyless Signature Infrastructure (KSI), eine Blockchain-Technologie zur Verifizierung der Datenintegrität auf hoher Skalierbarkeit.

Guardtime bietet basierend auf der KSI-Technologie verschiedene Produkte für die Zielbereiche e-Government, Telekommunikation, Finanz- und Versicherungsmärkte, die Rüstungs- und Flugzeugindustrie und weitere an. Die estnische Regierung nutzt KSI von Guardtime etwa, um öffentliche und interne Daten zu sichern, Insider-Gefahren zu bekämpfen und die Operabilität des Systems sicherzustellen. In Zukunft soll die KSI-Technologie zum Schutz von Atomkraftwerken und anderen kritischen Infrastruktureinrichtungen in England zum Einsatz kommen

Weiters ist Guardtime mit dem schwedischen IKT-Riesen Ericsson eine strategische Kooperation eingegangen. Inhalt der Kooperation ist die Integration der KSI von Guardtime in die Cloud-Angebote von Ericsson, um die Datenintegrität insb. bei Big Data Anwendungen für Unternehmen und im Bereich Industrie 4.0 sicherzustellen.²²

* R3 CEV

R3 CEV ist ein 2014 gegründetes Technologie-Start-Up aus New York mit dem Ziel, dezentrale Systeme für die Finanzwelt zu entwickeln. Hinter dem Unternehmen steht ein Industriekonsortium mit über 75 beteiligten Banken und Technologieunternehmen. Zu diesem zählen die großen Namen des Finanzsektors, u.a. sind UBS, Credit Suisse, HSBC, J.P. Morgan, Deutsche Bank, UniCredit, RBS, Barclays und BNP Paribas Mitglieder des Konsortiums.

Den Schwerpunkt des Unternehmens bildet die gemeinsame Entwicklung von Technologien und Standards im Bereich der Blockchain, zudem agiert das Unternehmen auch als Investor für andere Blockchain-Start-ups im FinTech-Bereich. R3 CEV hat insb. die Distributed-Ledger Plattform „Corda“ für Finanzdienstleistungen, im Speziellen für die Aufzeichnung, Verwaltung und Synchronisierung von komple-

²² <https://guardtime.com/s>



nen finanziellen Vereinbarungen zwischen regulierten Finanzeinrichtungen entwickelt.²³

* IBM

Der IT-Riese IBM ist einer der bedeutendsten globalen Akteure im Bereich der Blockchain. Aus Sicht von IBM kann die Blockchain in allen Geschäftsbereichen des Unternehmens eingesetzt werden. In erster Linie nutzt IBM die Blockchain im Bereich internationale Finanzierung und um Wertschöpfungsketten von Unternehmen effizienter zu gestalten. IBM hat bereits mehrere Prototypen-Systeme von Blockchain Anwendungen – insb. im Kontext des Internets der Dinge – entwickelt und ist Teil des Hyperledger Projekts der Linux Foundation zur Weiterentwicklung der Blockchain als Open Source Standard für verteilte Datenbanken.

IBM bietet eine Blockchain-Plattform für Unternehmen an, um Geschäftsnetzwerke durch die transparente Verteilung von Informationen und Abwicklung von Transaktionen effizienter zu gestalten. Unternehmen können sowohl vorgefertigte Services in Anspruch nehmen als auch ihre eigenen Blockchain-Anwendungen entsprechend ihrer Bedürfnisse entwickeln.²⁴

Besonders aktiv ist IBM im Bereich des Blockchain-Einsatzes für das Internet der Dinge. Zusammen mit Samsung hat IBM im Projekt ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) ein Konzept entwickelt, in der die Blockchain als Backbone für ein dezentrales IoT-Netzwerk dient. Dabei sind die verbundenen Geräte in der Lage, ohne den Eingriff einer zentralen Autorität miteinander zu kommunizieren, Daten zu teilen und sich untereinander zu organisieren.

IBM setzt sogar den Supercomputer Watson für die Verbindung von IoT und Blockchain ein. Über die Watson IoT Plattform können IoT-Daten, die zB aus RFID-Anwendungen, Barcode-Scans und von intelligenten Geräten stammen, in eine private Blockchain zugefügt werden. Über die Plattform können Geräte miteinander kommunizieren und Smart Contracts ausführen.²⁵

* Microsoft

Microsoft bietet auf seiner Cloud-Plattform Azure verschiedene „Blockchain as a Service“ (BaaS)-Modelle an, die spezifische unternehmerische oder technische Anforderungen adressieren sollen. Die BaaS-Plattform dient dabei in erster Linie als Entwicklungs-, Erprobungs- und Anwendungsplattform für Organisationen, um

²³ <http://www.r3cev.com/>

²⁴ <https://www.ibm.com/blockchain/>

²⁵ <https://www.ibm.com/internet-of-things/platform/private-blockchain/>



gemeinsam mit unterschiedlichen Technologien, von Smart Contracts bis zu Blockchain-basierten Steuerreporting-Systemen zu arbeiten. Dabei bietet Microsoft seine Services nicht im Alleingang an, sondern mit zahlreichen verschiedenen Partnern und Blockchain-Organisationen, um individuelle Angebote für verschiedene Branchen und Problemstellungen zu schaffen.

Laut eigener Aussage ist es das Ziel von Microsoft, die Azure-BaaS-Plattform als „Marktplatz“ für zertifizierte Blockchain-Anwendungen auszubauen. Unter anderem können Unternehmenskonsortien bereits ein auf der Ethereum-Blockchain basierendes Netzwerk aufstellen und entsprechend ihrer Anforderungen konfigurieren. Das Netzwerk besteht aus einem Set von Transaktionsknoten, mit denen eine Applikation oder ein Benutzer interagieren kann, um Transaktionen durchzuführen sowie einem Satz von Mining-Knoten pro Konsortialmitglied, um Transaktionen aufzuzeichnen.²⁶

*** Hyperledger Projekt**

Das Projekt „Hyperledger“ wurde von der Linux-Foundation gegründet und soll die Blockchain-Technologie vorantreiben, indem es einen offenen Standard für Blockchains definiert und eine Plattform schafft, die eine Vielzahl von Anwendungsfällen verschiedener Branchen bedienen soll.

Das Hyperledger Projekt ist eine globale Kollaboration von mehr als 100 Unternehmen u.a. aus dem Finanzsektor, der Industrie sowie Technologiefirmen und führenden Unternehmen in den Bereichen Internet of Things und Supply Chains. Zu den Mitgliedern gehören etwa Accenture, Airbus, Gruppe Deutsche Börse, Daimler, Fujitsu, IBM, Intel, J.P. Morgan, R3CEV, Cisco, Guardtime, Nokia und Samsung.

Hyperledger ist dabei als „Community of Communities“ organisiert, d.h. unterschiedliche Gruppen arbeiten an verschiedenen Themenstellungen. Zum einen betrifft dies die Implementierung von spezifischen Blockchain-Konzepten und –plattformen, zum anderen arbeiten Arbeitsgruppen an generellen Themen im Bereich der Blockchain, zB an Standards und der Weiterentwicklung der Blockchain-Architektur.²⁷

²⁶ <https://azure.microsoft.com/en-us/solutions/blockchain/>

²⁷ <https://www.hyperledger.org/>



✱ **Blockchain Insurance Industry Initiative (B3i)**

Die Blockchain-Initiative der Versicherungsbranche B3i (Blockchain Insurance Industry Initiative) wurde im Oktober 2016 von den Versicherungsunternehmen Aegon, Allianz, Munich Re, Swiss Re und Zurich gegründet, um gemeinsam zu untersuchen, wie sich mit Hilfe der Distributed-Ledger-Technologie der Datenaustausch zwischen Erst- und Rückversicherern noch effizienter gestalten lässt und schnellere und bessere Services für Kunden angeboten werden können. Mittlerweile sind zehn weitere Erst- und Rückversicherer der Initiative beigetreten, u.a. Generali, Liberty Mutual, SCORB und andere.

Initiative ist eine Plattform zum Austausch von Erfahrungen mit der Blockchain und möglichen anderen Technologien, entsprechenden Pilotprojekten und Forschungsergebnissen und zielt auch darauf ab, den Übergang von begrenzten Anwendungsfällen aus den einzelnen Unternehmen hin zu durchführbaren Lösungen, die sich auf die gesamte Wertschöpfungskette der Versicherung beziehen, zu ermöglichen.²⁸

✱ **Blockchain Collaborative Consortium**

In Japan wurde im April 2016 von 34 Gründungsmitgliedern das Blockchain Collaborative Consortium gegründet. Mittlerweile beteiligen sich 109 japanische Unternehmen aus dem Finanzsektor, Industrie und dem Dienstleistungssektor an der Initiative. Das Ziel des Konsortiums ist die Steigerung der Awareness für die Blockchain Technologie sowie die Adaptierung und die Erforschung der Blockchain voranzutreiben. Dazu wurde durch das Konsortium auch ein „Blockchain-Universitäts-Programm“ gegründet, das bereits mehr als 100 Absolventen vorweist. Mitglieder sind u.a. Japan Microsoft, Mitsui Sumotomo Insurance, PwC, Bitbank and ConsenSys.²⁹

✱ **Enterprise Ethereum Alliance**

Im Februar haben führende Technologie- und Finanzunternehmen die Enterprise Ethereum Alliance gegründet, um den professionellen Einsatz der Blockchain in der Wirtschaft zu fördern. Ziel der Mitglieder ist es, für das Ethereum-System Standards und Best Practices entwerfen und fördern, auch eine Referenzarchitektur namens EntEth 1.0 ist geplant. EntEth soll ebenfalls auf Ethereum basieren. Ziel ist der professionelle Einsatz in Unternehmen zum Beispiel für Smart Contracts. Dabei

²⁸ <https://www.allianz.com/de/presse/news/engagement/sponsoring/170206-Blockchain-Initiative-gewinnt-weltweit-neue-Mitglieder/>

²⁹ <http://www.prnewswire.com/news-releases/blockchain-collaborative-consortium-membership-reaches-109-companies-and-organizations-300423902.html>



soll der Fokus insb. auf die Einhaltung des Datenschutzes und die Vertraulichkeit der Informationen sowie die Skalierbarkeit und Sicherheit der Technik gelegt werden. Auch hybride Systeme mit Public und Permissioned Netzwerken sind angedacht.

Zu den Gründern gehören IT-Unternehmen wie Intel, Microsoft und BlockApps, der Finanzsektor ist zB mit J.P. Morgan, Credit Suisse und Banco Santander vertreten, dazu kommen u.a. noch Accenture, Thomson Reuters und British Petrol.³⁰

*** Accenture**

Das Beratungs-, Technologie- und Outsourcing-Unternehmen Accenture setzt ebenfalls auf die Blockchain als Zukunftstechnologie. Dazu hat das Unternehmen das „Blockchain Center of Excellence“ gegründet, das Distributed-Ledger Systeme erforscht. Das Zentrum entwickelt Lösungen für verschiedene Ledger-Systeme (öffentliche, für Konsortien und private Ledger) und Anwendungsfelder (Internet der Dinge, Transaktionen, Kommunikation etc.) und arbeitet dabei mit Blockchain-Start-ups, in Allianzen als auch mit einem Open-Community Ansatz. Zu den Partnern zählen u.a. MultiChain, Eris, Ripple, IBM und Digital Asset Holdings (DAH).³¹

*** TransActive Grid**

TransActive Grid ist ein Joint Venture zwischen LO3 Energy (einem Spezialisten für Micro-Grids) und Consensus Systems (Spezialist für Blockchain-Technologien). TransActive Grid kombiniert Mikro-Netze mit der Blockchain und will dadurch einen lokalen Markt für dezentrale Energie ermöglichen. Die offene Plattform erlaubt die Echtzeitmessung von lokaler Energieerzeugung und -nutzung, sowie weiteren relevanten Daten und ermöglicht es den Teilnehmern des Netzwerks, mit Energieguthaben zu handeln. In Brooklyn NY wurde bereits das erste Pilotprojekt gestartet: Dabei können Personen mit Solaranlagen auf ihren Dächern überschüssigen Strom an ihre Nachbarn verkaufen. 2016 wurde mit Siemens eine Kooperation über die Weiterentwicklung des Projekts vereinbart.

³⁰ <http://www.marketwired.com/press-release/newly-formed-enterprise-collaboration-drives-ethereum-blockchain-technology-best-practices-2199494.htm>

³¹ <https://www.accenture.com/us-en/service-blockchain-financial-services>



4.2 Bedeutende Blockchain-Plattformen

* Bitcoin

Bitcoin war der Wegbereiter der Blockchain und die weltweit erste dezentrale digitale Währung, die auf der Blockchain beruhte. Das Gründungsdokument von Bitcoin, „Bitcoin: A Peer-to-Peer Electronic Cash System“, das unter dem Pseudonym Satoshi Nakamoto veröffentlicht wurde (bis heute ist noch nicht gesichert, wer sich hinter dem Pseudonym verbirgt), beschrieb im Jahr 2008 erstmals das Konzept der Blockchain. 2009 startete das Bitcoin-Netzwerk mit dem sogenannten Genesis-Block. Dabei ist Bitcoin und auch das im Gründungsdokument beschriebene Blockchain-Konzept open-source, d.h. es bestehen seitens des oder der Urheber keine Eigentumsansprüche. Daher wird Bitcoin auch nicht von einem einzelnen Unternehmen oder einer Person unterhalten, vielmehr sind die Teilnehmer des Netzwerks dafür verantwortlich.

* Ethereum

Anders als das Bitcoin-Netzwerk, das sich als Zahlungssystem auf die Durchführung von Transaktionen konzentriert, verfolgt Ethereum einen universellen Ansatz der Blockchain-Technologie. Wie Bitcoin ist es ein verteiltes Netzwerk mit einer eigenen Währung (Ether), allerdings basiert das Konzept der Plattform auf der Ausführung von Smart Contracts durch eine eigene öffentliche Blockchain. Die Entwicklung wird von der Ethereum Foundation geleitet, einer Schweizer Non-profit-Stiftung.

Im Gegensatz zu Bitcoin soll Ethereum eine Blockchain mit integrierter Turing-kompatibler Programmiersprache sein (d.h. die Programmiersprache ist universell einsetzbar), mit der alle möglichen Arten von Lösungen per Smart Contracts erarbeitet werden können. Mögliche Anwendungsbereiche sind zB E-Voting-Systeme, virtuelle Organisationen, Identity-Management, IPR-Management und Crowdfunding. Neben der Umsetzung von Smart Contracts können dies auch dezentrale autonome Organisationen (DAOs) sein. Ethereum verwendet dabei die Kryptowährung Ether als Zahlungsmittel für die Rechenleistung, die Teilnehmer am verteilten System zur Verfügung stellen. Wer eigene Anwendungen in der Ethereum-Blockchain umsetzen will, muss dafür ebenfalls mit Ether bezahlen.³²

* Coinbase

Coinbase wurde 2012 ins Leben gerufen und ist eine Wallet für digitale Währungen und eine Plattform, auf der Händler und Kunden Geschäfte mit neuen digitalen Währungen wie Bitcoin und Ethereum durchführen können. Der Hauptsitz des Unternehmens liegt in San Francisco, Kalifornien.

³² <https://www.ethereum.org/>



Das Unternehmen hat bisher \$ 117 Mio. von Investoren eingenommen und wird von rund 5,9 Mio. Kunden und 45.000 Händlern genutzt. Bisher wurden über Coinbase Transaktionen im Wert von \$ 6 Mrd. ausgetauscht.

Neben einer Plattform zur einfachen Bezahlung mit digitalen Währungen stellt Coinbase Apps zur Integration von Bitcoin und Ethereum in neue und bestehende andere Applikationen bereit (insg. über 9.000 bestehende Apps), die von den Teilnehmern des Netzwerks auf einer Entwicklungsplattform erstellt werden können.³³

*** 21 Inc.**

Das Unternehmen 21 Inc. wurde 2013 gegründet und erhielt – bevor es auch nur ein Produkt auf den Markt brachte – von Investoren \$ 121 Mio., so viel wie kein anderes Blockchain-Unternehmen zuvor. Im Laufe seiner Geschichte hat das Unternehmen seine Geschäftsstrategie mehrmals neu ausgerichtet. Ursprünglich war 21 Inc. als Bitcoin-Mining Unternehmen gegründet worden, um 2015 als erster Hersteller einen „Bitcoin-Computer“ auf den Markt zu bringen, einen Chip für das Mining von Bitcoins, der in die übliche Hardware von Konsumenten und Unternehmen eingebaut werden kann.³⁴

Anfang 2017 startete 21 Inc. eine neue Geschäftsidee: eine E-Mail-Plattform, auf der die Nutzer für das Beantworten von Mails bezahlt werden. Nutzer können dabei eine Inbox einrichten und Nachrichten von Unternehmen, Personalvermittlern, Verkäufern etc. empfangen – ähnlich dem Prinzip von LinkedIn. Antwortet der Nutzer auf eine Mail, zB eine Umfrage o.ä. wird er dafür in Bitcoins entlohnt. Die Absender hingegen zahlen für die Meinung der Nutzer, wobei ca. 10 % der Kosten als Vermittlungsgebühr von 21 Inc. eingehoben werden.

*** Storj**

Die Plattform Storj bietet Blockchain-basierte Cloudspeicher mit einer End-zu-End Verschlüsselung an. Im Unterschied zu konventionellen Cloud-Angeboten werden die Daten nicht etwa zentral auf den Servern von Storj gespeichert, sondern dezentral auf den Rechnern der Netzwerkmitglieder verteilt. Die Benutzer stellen Speicherkapazität zur Verfügung (bei Bitcoins ist es äquivalent die Rechenleistung) und werden dafür mit der hauseigenen Währung vergütet: Storjcoin. Dabei werden die zu speichernden Dateien verschlüsselt, in mehrere Bestandteile (genannt „Shards“) aufgeteilt und dezentral im globalen Netzwerk gespeichert. Dadurch verfügt niemand außer dem Eigentümer über eine vollständige Kopie der Daten, was ein zentrales Sicherheitskonzept des Unternehmens darstellt.³⁵

³³ <https://www.coinbase.com/?locale=de>

³⁴ <http://www.coindesk.com/linkedin-killer-bitcoin-upstart-21-takes-on-social-giant-with-paid-email-play/>

³⁵ <https://storj.io/index.html>



Tiefendossier: Die Blockchain

Das Unternehmen hat kürzlich bekanntgegeben, eine Partnerschaft mit Microsoft Azure geschlossen zu haben. Storj soll über die Azure Plattform von Microsoft verfügbar sein und das Konzept als Blockchain As a Service Modell anbieten.³⁶

* Provenance

Ziel von Provenance ist es, über eine Blockchain-basierte Plattform die Supply Chain von Produkten für den Kunden sichtbar zu gestalten. So werden Informationen wie Lieferanten, Bearbeiter, Transporteure etc. mit dem Endprodukt verbunden und dieses Ergebnis dem Endkonsumenten offengelegt.

Unternehmen ermöglicht die Plattform sich selbst, ihre Produkte und Lieferketten transparenter und nachverfolgbar darzustellen. Dabei werden zwei Datensysteme miteinander verbunden: Transparenz-Tools ermöglichen die Erstellung von Firmen- und Produktprofilen, Tracking-Instrumente die Nachverfolgung des Produkts über die gesamte Supply Chain. Produkte können auch mit Entstehungsgeschichten, Einflüssen, erhaltenen Preisen und zugrundeliegenden Standards dargestellt werden. Um die Nachverfolgbarkeit zu gewährleisten, werden die physischen Produkte mit einer individuellen ID-Nummer versehen (in Form eines Zahlencodes), sodass Nutzer durch dessen Verwendung schnellen Zugang zu den individuellen Produktinformationen haben können.³⁷

* Circle

Das Peer-to-Peer-Bezahlunternehmen Circle wurde 2013 gegründet und offeriert eine App, mit der unkompliziert Geld an Freunde und Bekannte überwiesen werden kann. Dabei unterstützt das System traditionelle Währungen wie etwa US-Dollar, Euro oder das britische Pfund.

Vom Aussehen her ähnelt die App bekannten Messaging-Applikationen wie etwa Whats-App und bietet auch ähnliche Funktionen – mit dem Unterschied, dass damit auch Geld überwiesen werden kann. Auch können Freunde um Überweisungen angefragt werden. Die Nutzer müssen sich lediglich über ihre E-Mail Adresse oder Mobilfunknummer anmelden und ein Foto ihrer EC-Karte hochladen und können dann in Form von „Geldbotschaften“ Transaktionen durchführen.³⁸

³⁶ <https://www.btc-echo.de/storj-dezentrale-cloud-waehrung/>

³⁷ <https://www.provenance.org/technology>

³⁸ <https://www.circle.com/de>



5 Herausforderungen und Risiken

Die Blockchain bietet verschiedene, vielfach disruptive Potenziale und Anwendungsmöglichkeiten. Sie kann Finanzmärkte maßgeblich verändern, Banken, Rechtsanwälte, Notare und andere Intermediäre könnten in vielen Bereichen obsolet werden. Sie könnte es intelligenten Geräten erlauben, sicher miteinander zu kommunizieren, sich zu organisieren und eigenständig Transaktionen durchzuführen und so Enabler des Internets der Dinge werden. Die Blockchain kann zum Aufbau dezentraler Energiemärkte beitragen, das Konzept der Sharing Economy weiter vorantreiben oder als Cyber Security Instrument eingesetzt werden – den Anwendungsmöglichkeiten der Blockchain sind kaum Grenzen gesetzt.

Da die Technologie allerdings noch in den Kinderschuhen steckt, gilt es noch eine Reihe von Herausforderungen zu bewältigen, um die Potenziale der Blockchain vollständig zu nutzen:

Je mehr Teilnehmer eine Blockchain hat und je mehr Transaktionen durchgeführt werden, desto größer wird die Blockchain, da alle Transaktionen und Informationen dauerhaft in der Blockchain hinterlegt werden. Bei Änderungen werden bestehende Dateien nicht umgeschrieben, sondern die neuen bzw. aktualisierten Informationen kommen in Form von neuen Blöcken hinzu. So wächst das Volumen der Blockchain bei jeder Transaktion. Da die Kette als Kopie auf den Rechnern der Netzwerkteilnehmer gespeichert wird, muss dafür zunehmend Speicherplatz auf diesen für die Blockchain zur Verfügung gestellt werden (IW Köln , 2017). Bei großen Datenbanken stoßen Blockchain-Systeme oft noch an ihre Grenzen, daher ist das Thema Skalierbarkeit eines der wesentlichen in den Entwicklungstätigkeiten im Bereich der Blockchain-Technologie.

Dazu kommt, dass die Verifizierung der Datenintegrität hohe Rechenleistungen benötigt. Es gibt Vorhersagen, die den Energieverbrauch, der alleine durch das Mining im Bitcoin-Netzwerk entsteht für das Jahr 2030 auf rund 11,4 % des weltweiten Energieangebots schätzen – wenn nur 5 % der Weltbevölkerung das Netzwerk nutzen würden (IW Köln , 2017). Das Online Magazin „Motherboard“ hat berechnet, dass das Bitcoin-Netzwerk unter den derzeitigen Wachstumsraten bis 2020 so viel Energie benötigen würde wie ganz Dänemark (Credit Suisse, 2016).

Die Blockchain gilt generell zwar als sicherer als bestehende Systeme, jedoch ist dies nur der Fall, wenn der zugrundeliegende Programmiercode fehlerfrei ist. Fehler im Code stellen ein erhebliches Sicherheitsrisiko dar und können von Hackern ausgenutzt werden, um das System zu kompromittieren. In solchen Fällen kann es auch schwierig sein nachzuweisen, ob dabei eine illegale Handlung vorliegt oder das Ausnutzen von Hintertüren quasi ein Feature des Codes ist („Code ist Law“) (IW Köln , 2017)



Ein anderes Problem der Blockchain ist die Tatsache, dass sie nur sicher ist, wenn genug Teilnehmer im Netzwerk vorhanden sind. Die Entscheidung, welche Blöcke der Kette hinzugefügt werden, wird bei der Blockchain durch ein Consensus-Modell getroffen. I.d.R. muss dafür die Mehrheit des Netzwerks die Korrektheit der Daten verifizieren – wobei es dabei meist um Rechenleistung und nicht um die Anzahl der Personen geht. Ist das Netzwerk relativ klein, ist es umso einfacher für Akteure, die Mehrheit der Rechenleistung im Netzwerk aufzubringen – wodurch eine Manipulation der Daten möglich wäre (IW Köln , 2017). Die Gefahr, dass eine kritische Masse an verschiedenen Netzwerkteilnehmern nicht erreicht werden kann, kann insb. dann bestehen, wenn eine starke Fragmentierung von Blockchain-Plattformen besteht und die Nutzer sich auf viele verschiedenen Plattformen für ähnliche Anwendungsgebiete verteilen und sich nicht auf eine oder wenige Plattformen festlegen können (Credit Suisse, 2016).

Ein weiteres Risiko der Blockchain ergibt sich durch die Public-Key Kryptographie: Wird ein privater Schlüssel gestohlen oder geht verloren, so sind die betreffenden Inhalte unweigerlich nicht mehr verwendbar. Durch die Irreversibilität der Blockchain, d.h. dadurch, dass bestehende Blöcke nicht mehr veränderbar sind, sobald sie in der Kette registriert werden, können zudem Transaktionen die fehlerhaft eingegeben und abgeschickt wurden, durch den Absender nicht mehr rückgängig gemacht werden (Fraunhofer FIT, 2016).

Auch ergibt sich durch die Verschlüsselung der digitalen Signaturen eine Pseudonymität der Blockchain – insb. bei Kryptowährungen wie Bitcoin. Verbunden mit ihrer dezentralen Natur samt Fehlen einer Trusted Third Party, bestehen daher oftmals Bedenken hinsichtlich der Legalität der Transaktionen. So wurde Bitcoin in der Vergangenheit mehrmals als Medium für Geldwäsche und Schwarzmarkttransaktionen in Verbindung gebracht (Credit Suisse, 2016).



6 Schlussfolgerungen

Die Blockchain stellt eine relativ neue Technologie im Kontext der Digitalisierung dar und erlangte mit der Einführung der Kryptowährung Bitcoin im Jahr 2009 erstmals weltweite Aufmerksamkeit. Doch längst ist die Blockchain mehr als nur die Technologie hinter Bitcoin. Vielmehr wird die Blockchain als die eigentliche Innovation erachtet, die das Potenzial haben könnte, etliche Bereiche der Gesellschaft, die weit über das Gebiet digitaler Währungen hinausgehen, zu verändern.

Im Vergleich zu traditionellen, zentralisierten Systemen bietet die Blockchain eine Reihe von Vorteilen und Chancen. Da die Blöcke der Blockchain eine Referenz zu dem vorherigen Block enthalten und miteinander verbunden sind, können Daten, sobald sie einmal in der Kette hinterlegt sind, nicht mehr im Nachhinein verändert oder gelöscht werden. Durch Consensus-Modelle wird sichergestellt, dass nur korrekte Daten in die Blockchain aufgenommen werden. Da die in der Blockchain hinterlegten Daten zudem nicht manipulierbar sind, wissen die Nutzer, dass die Integrität der Daten gewährleistet ist. Dadurch ist in einem Blockchain-System kein Vertrauen zwischen den Teilnehmern oder gegenüber zentralen Instanzen notwendig, wodurch dritte Parteien (Trusted Third Parties) für Aktionen innerhalb des Netzwerks und die Verwaltung der Blockchain obsolet werden.

Als Distributed Ledger wird die Blockchain als identische Kopie auf den Rechnern der Netzwerkteilnehmer hinterlegt, sodass ein potenzieller Single-Point of Failure eliminiert wird und der Ausfall einzelner Netzwerkknoten keine kritischen Auswirkungen auf das System hat. Auch werden Informationsungleichgewichte beseitigt und die Abstimmung von Datenbanken obsolet. Zudem sind alle historischen Informationen in der Blockchain hinterlegt und können jederzeit eingesehen werden, sodass die Transparenz unter den Teilnehmern des Netzwerks steigt.

Durch die Programmierbarkeit der Blockchain lassen sich komplexe, konditionale Transaktionen und Aktionen in Blockchain-Systemen gestalten, etwa durch selbstausführende Smart Contracts. Gerade diese Programmierbarkeit der Blockchain macht sie interessant. Die Blockchain kann also nicht nur für Transaktionen verwendet werden sondern für alle denkbaren Anwendungen, die auf digitalen Daten basieren: Als sichere und transparente Datenbank für Informationen aller Art, zur Kommunikation zwischen den Teilnehmern im Netzwerk und oder als Instrument zur Nachverfolgung von Daten und Aktionen. Das größte Potenzial der Blockchain könnte jedoch darin liegen, selbstausführende Verpflichtungen – sog. „Smart Contracts“ – zu ermöglichen, die eine automatische Ausführung von Handlungen bei der Erfüllung festgelegter Kriterien erlauben. Solche Smart Contracts könnten insb. im Kontext des Internet der Dinge für die Kommunikation, den Austausch von Daten sowie die Selbstorganisation intelligenter, vernetzter Geräte eingesetzt



Tiefendossier: Die Blockchain

werden.

Tabelle 1: Vorteile, Nachteile, Potenziale und Herausforderungen der Blockchain

Vorteile <ul style="list-style-type: none">• Kein Vertrauen zwischen den Teilnehmern oder gegenüber zentralen Instanzen notwendig• Immutability Of Record: Daten können nicht manipuliert oder gelöscht werden• Gewährleistung der Datenintegrität und hohe Sicherheit gegenüber Angriffen• Keine Double-Spending Problematik• (Historische) Single Source of Truth eliminiert Informationsungleichgewichte• Kein Single Point of Failure und hohe Netzausfallsicherheit• Programmierbarkeit• Zugangskontrolle• Hohe Prozessintegrität	Nachteile <ul style="list-style-type: none">• Problem der Skalierbarkeit (Blockchains wachsen mit jeder zusätzlichen Information) und hoher Speicherbedarf• Proof-of-Work Konzepte führen zu hohem Energieverbrauch• Irreversibilität von Transaktionen und Smart Contracts: Fehlerhafte Eingaben können nicht rückgängig gemacht werden
Potenziale <ul style="list-style-type: none">• Trusted Third Parties könnten in vielen Bereichen entfallen, Abläufe effizienter und transparenter gestaltet werden• Sehr breites Einsatzspektrum (IoT, Verwaltung, Sharing Economy, Energieversorgung, Finanzbranche, Versicherungen...)• Smart Contracts ermöglichen selbstausführende Handlungen• Enabler für andere digitale Technologien (IoT, Big Data, Cloud Computing, 3D-Druck)• Quelle für neue Geschäftsmodelle• Als Cyber Security Tool einsetzbar• Ermöglicht im IoT selbstständiges Agieren von intelligenten Geräten• Transparente Nachverfolgung von Geldflüssen, Eigentumsrechten und Produkten• Vielversprechender Ansatz für eine dezentrale Energieversorgung	Herausforderungen <ul style="list-style-type: none">• Sicherheit wird nur bei einer kritischen Masse an Teilnehmern bzw. Rechenleistung gewährleistet• Fehler im Programmiercode der Blockchain stellen ein erhebliches Sicherheitsrisiko dar• Pseudoanonymität und Fehlen einer Trusted Third Party führen zu Bedenken hinsichtlich illegalen Aktivitäten• Regulatorische Hemmnisse



Da die Technologie jedoch noch relativ neu ist, werden noch einige Herausforderungen zu lösen und offene Fragen zu klären sein, um das volle Potenzial der Blockchain nutzen zu können. Diese betreffen etwa Skalierbarkeit und legale Aspekte der Blockchain. Dass die Potenziale der Blockchain-Technologie jedoch überwiegen, zeigen nicht zuletzt das starke Interesse und die zahlreichen Aktivitäten aus der Wirtschaft, ob aus der Finanzbranche oder von den großen Technologieunternehmen wie Microsoft und IBM.

Interessant ist die Blockchain-Technologie auch als Enabler anderer bedeutender Technologien und Trends: Sie könnte das Internet der Dinge, Cloud Computing, 3D-Druck, Big Data Anwendungen oder Konzepte wie die Sharing Economy vorantreiben und so weitere disruptive Potenziale entfalten – der endgültige Einfluss der Blockchain bleibt dennoch abzuwarten.

In Österreich beschäftigen sich einige Forschungsakteure und Experten mit der Thematik – so wurde die Blockchain-Technologie in der letzten Ausschreibung von „IKT der Zukunft 2016“³⁹ u.a. im Ausschreibungsschwerpunkt „Cyber-Physische Systeme“ angeführt. Im Herbst 2016 fand in der Steiermark ein „Blockchain Startup Contest“⁴⁰ statt, der von der FFG unterstützt wurde. Ebenso beschäftigt sich das Austrian Institute of Technology mit der Blockchain-Thematik im Forschungsschwerpunkt Data Science, wobei insb. Sicherheitsaspekte adressiert werden, etwa auch im Rahmen des deutsch-österreichischen Projekts „BITCRIME“.⁴¹ Auch verschiedene andere Akteure widmen sich dem Thema, so halten etwa Rechtsanwälte Vorträge und Seminare zur Blockchain-Technologie⁴² usw.

Aufgrund der umfassenden und disruptiven Möglichkeiten, die die Blockchain-Technologie für eine Vielzahl an Wirtschaftsbereichen und auch den öffentlichen Sektor bietet, sollten verstärkte Informations- und Kommunikationsmaßnahmen in definierten Zielgruppen (IKT-Community, Industrie, Verwaltung, kritische Infrastrukturen etc.) etwa über Medienaktivitäten, Konferenzen und Veranstaltungen überlegt werden. Auch der Austausch von Unternehmen mit internationalen Blockchain-Experten sollte unterstützt werden, um die konkreten Interessens- und Bedarfssfelder der Firmen zu erarbeiten. In weiterer Folge können die Blockchain-Technologien im Rahmen des bestehenden thematischen bzw. themenunabhängigen Forschungsförderinstrumentariums gezielt adressiert werden.

³⁹ https://www.ffg.at/sites/default/files/allgemeine_downloads/thematische%20programme/IKT/iktderzukunft2016_ausschreibungsleitfaden.pdf

⁴⁰ <http://sciencepark.at/aktuelles/news/960/blockchain-startup-contest-application-deadline-31st-october-2016>

⁴¹ [http://www.ait.ac.at/ueber-das-ait/center/center-for-digital-safety-security/?sword_list\[\]=blockchain&no_cache=1](http://www.ait.ac.at/ueber-das-ait/center/center-for-digital-safety-security/?sword_list[]=blockchain&no_cache=1)

⁴² <http://www.svlaw.at/anmelden>



Tiefendossier: Die Blockchain

Die Beschäftigung mit der Thematik zeigt jedenfalls: Die Blockchain-Technologie eröffnet viele technologische und wirtschaftliche Chancen sowie disruptive Innovationspotenziale und verdient eine gezielte Betrachtung. Auch wenn die breite Anwendung vielfach noch in den Anfängen steckt, sollte sie einen interessanten und definitiv relevanten Gegenstand für zukünftige Aktivitäten der Forschungs-, Technologie- und Innovationspolitik in Österreich darstellen.



Literatur- und Quellenverzeichnis

- Berkeley University of California - Sutardja Center for Entrepreneurship & Technology. (2015). *BlockChain Technology - Beyond Bitcoin*.
- Brave New Coin. (2015). *A Gentle Introduction To Blockchain Technology*.
- Buterin, V. (2013). *Ethereum White Paper - A Next Generation Smart Contract & Decentralized Application Platform*.
- Chamber of Digital Commerce. (2016). *Smart Contracts: 12 Use Cases for Business & Beyond. A Technology, Legal & Regulatory Introduction*.
- Cognizant. (2016). *Cognizant 20-20 insights. June 2016*.
- Credit Suisse. (2016). *Connection Series - Blockchain*.
- Deloitte. (2016). *Blockchain Technologie - Revisionssichere Archivierung*.
- Deloitte. (2016a). *Blockchain - Enigma. Paradox. Opportunity*.
- Ernst & Young. (2016). *Blockchain reaction - Tech companies plan for critical mass*.
- EU-KOM. (2010). *EUROPA 2020 - Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum*. Brüssel.
- Fraunhofer FIT. (2016). *Blockchain: Grundlagen, Anwendungen und Potenziale*.
- Goldman Sachs. (2016). *Profiles in Innovation: Blockchain - Putting Theory into Practice*.
- IBM. (2015). *Empowering the edge - Practical insights on a decentralized Internet of Things*.
- IBM. (2016b). *Making Blockchain Real for Business - Explained*.
- IW Köln. (2017). *IW Kurzberichte 2.2.17: Blockchain - Down to Earth*.
- Kaye Scholer. (2016). *An Introduction to Bitcoin and Blockchain Technology*.
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Roßbach, P. (2016). Blockchain-Technologien und ihre Implikationen. *Banking and Information Technology (BIT) Bd, 17 (1)*, pp. 54-69.
- Technologiestiftung Berlin. (2016). *Blockchains, Smart Contracts und das dezentrale Web*.
- Think Consortium. (2016). *2017 Outlook: Blockchain Impacts on Enterprise and Government*.
- UK Government Office for Science. (2016). *Distributed Ledger Technology: beyond block chain*.



Tiefendossier: Die Blockchain

World Economic Forum. (2015). *Deep Shift - Technology Tipping Points and Societal Impact*.

World Economic Forum. (2016). *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services*.