Forschungsbereich
MaschinenbauInformatik
und Virtuelle
Produktentwicklung
Univ.-Prof. Dr.-Ing. Detlef Gerhard

Anwendungsmöglichkeiten der Blockchain – Technologie im industriellen Kontext

Eine Betrachtung des gesamten Product Life Cycle

Diplomarbeit

Alexander PORSCH

Matrikel-Nr.: 0827422

Ich habe zur Kenntnis genommen, dass ich zur Drucklegung meiner Arbeit unter der Bezeichnung

Diplomarbeit

nur mit Bewilligung der Prüfungskommission berechtigt bin.

Ich erkläre weiters Eides statt, dass ich meine Diplomarbeit nach den anerkannten Grundsätzen für wissenschaftliche Abhandlungen selbstständig ausgeführt habe und alle verwendeten Hilfsmittel, insbesondere die zugrunde gelegte Literatur, genannt habe.

Weiters erkläre ich, dass ich dieses Diplomarbeitsthema bisher weder im In- noch Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe und dass diese Arbeit, mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Einleitende Bemerkungen

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Personenbezeichnungen verzichtet. Sämtliche Ausdrücke besitzen dabei für beide Geschlechter idente Gültigkeit.

Die vorliegende Arbeit verwendet englische Begriffe, ohne dass diese an gleicher oder anderer Stelle ins Deutsche übersetzt werden. Da die Anfänge diverser, in die Arbeit einbezogener Technologien vorrangig im englischen Sprachraum stattfanden und die Termini bei der Übersetzung beibehalten wurden, kam es zur flächendeckenden verwendung der englischen Begriffe in der Fachliteratur. Dies wird auch in der vorliegenden Arbeit beibehalten.

Danksagung

Mein Dank gebührt…

… meiner Familie, die mich über die Jahre meiner Ausbildung an der TU Wien auf jede ihnen mögliche Weise unterstützt hat. Allen voran mein Vater Karl-Heinz, der durch seinen unermüdlichen Einsatz Dinge ermöglich hat, die auf anderem Wege nur viel schwerer zu schaffen gewesen wären.

… Univ.-Prof. Dipl.-Ing. Dr.-Ing. Detlef Gerhard für die Betreuung dieser Arbeit und das Ermöglichen, diese Arbeit in einer sehr freien und selbstständigen Art gestalten zu können. Ebenso für die Möglichkeit, mich im Rahmen meiner universitären Aktivitäten sowie meiner Tätigkeit am Institut für Maschinenbauinformatik mit spannenden, innovativen Themen beschäftigen zu dürfen.

… dem gesamten Institut für Maschinenbauinformatik und Virtuelle Produktentwicklung. Da ich besonders während meiner Zeit am Institut unglaublich viel lernen durfte und gleichzeitig auch immer viel Spaß an der Arbeit hatte und die unzähligen Diskussionen sehr bereichernd waren.

… meinen Studienkollegen, mit denen so manche Höhen und Tiefen durchzustehen waren, auf deren Unterstützung ich zählen durfte und denen ich hoffentlich im Gegenzug selbst eine gute Stütze sein durfte.

Abstract - deutsch

In den vergangenen Jahren wurde der Begriff „Blockchain“ stark durch Kryptowährungen und Finanzspekulation geprägt. Das dahinter liegende Konzept einer Kombination an vorher bereits bekannten Mechanismen, die in ihrer Summe eben den Begriff Blockchain gebildet haben, wird dabei weitaus weniger betrachtet.

Dabei steht hinter der Blockchain eine Form von Informationssystemen, das sich auf mehrere Weise auf grundsätzliche Art von vielen derzeit im Einsatz befindlichen Informationssystemen unterscheidet. Dazu zählen vor allem die Dezentralität, der Einsatz gewisser kryptografischer Mechanismen und die Art, wie Teilnehmer innerhalb des Netzwerks miteinander agieren.

Durch einen gewissen Technologie-Push hat die Nutzung dieser Technologie nun einen medial wirksamen Aufschwung erlebt, wobei jedoch zu bemerken ist, dass die Anwendungsfälle nicht ganz klar sind. Insbesondere durch die Neuartigkeit der Technologie sind verschiedenste Ausprägungen von Blockchain-Systemen am entstehend, die zusätzlich nicht immer eindeutig den entsprechenden Anwendungsmöglichkeiten zugeordnet werden können.

Die vorliegende Arbeit beschäftigt sich mit der Frage, welchen Nutzen unterschiedliche Blockchain-Systeme in Bezug auf die Anwendung im industriellen Umfeld besitzen könnten. Dabei wird die Betrachtung nicht auf einzelne Aspekte der Industrie begrenzt, sondern es wird der gesamte Product Life Cycle betrachtet.

Hierfür werden die verschiedenen Blockchain-Konzepte auf ihre Basis heruntergebrochen, um eine möglichst vollständige Sammlung der Nutzen und Hemmnisse der Blockchain-Technologie zu liefern. Unter dieser Betrachtungsweise werden bestehende und potenzielle Use Cases gesammelt und generische Nutzungsmöglichkeiten identifiziert und kategorisiert.

Als Abschluss dienen konkrete, selbstentwickelte Use Case zur Veranschaulichung wie die Technologie im Rahmen des Product Life Cycle genutzt werden kann.

Abstract - english

In recent years the term “blockchain” was shaped primarily by cryptocurrencies and financial speculation. The underlying concept as a combination of previously known mechanisms, which in their sum de facto form the term blockchain, is much less considered.

The background of blockchain is a form of information system that differs in several ways in a fundamental way from many information systems currently in use. This includes, above all, decentralization, the use of certain cryptographic mechanisms and the way in which participants interact with each other within the network.

With a certain push of technology, the use of blockchain systems has now experienced a media caused upswing, but it should be noted that a lot of use cases are not clearly defined. In particular, due to the novelty of the technology, the most diverse forms of blockchain systems are emerging, which in addition cannot always be clearly assigned to the corresponding application possibilities.

The work on hand deals with the question, what benefits different blockchain systems could have in terms of application in an industrial environment. The consideration is not limited to individual aspects of the industry, but the entire product life cycle is considered.

For this the various blockchain concepts are broken down to their base in order to provide a as complete as possible collection of the benefits and obstacles of blockchain technology. Under this perspective, existing and potential use cases are collected, and generic uses identified and categorized.

Furthermore, concrete, self-developed use cases serve to illustrate how the technology can be used in the context of the product life cycle.

Inhaltsverzeichnis

1 Einleitung

Thema dieser Arbeit ist die Betrachtung und Einschätzung der Blockchain Technologie im industriellen Umfeld. Dabei soll die Technologie „Blockchain“ in ihrer Gesamtheit analysiert und auf ihre eigentlichen generisch-technologischen Spezifikationen heruntergebrochen werden. Zum Zeitpunkt der Erstellung dieser Arbeit Ende des Jahres 2018 und Anfang 2019 stellt die Blockchain noch eine relativ neue Technologie dar, die bis zum jetzigen Zeitpunkt primär Anwendungsmöglichkeiten im Finanzbereich und besonders im Bereich der Kryptowährungen gefunden hat.

Jedoch stellt sich darüber hinaus die Grundfrage, für welche Einsatzmöglichkeiten das Konzept Blockchain oder ggf. einzelne Aspekte der Technologie noch geeignet ist. Mit eben jener Frage beschäftigt sich diese Arbeit. Ganz konkret wird dabei der generische Product Life Cycle betrachtet und wie in diesem Kontext die Blockchain sinnvoll eingesetzt werden kann.

Allgemein formuliert kann man sagen, dass es sich bei der Blockchain-Technologie um ein neuartiges Konzept eines Informationssystems handelt. Da auch der Einsatz von Informationssystemen im industriellen Kontext seit vielen Jahren mehr und mehr an Relevanz erlangt und diese Systeme auch tendenziell für die laufenden Prozesse im Product Life Cycle erfolgskritisch sind, bestehen berechtige Gründe, warum die Blockchain-Technologie wichtige Einsatzmöglichkeiten im industriellen Umfeld liefern kann.

Dabei stellt der Umgang mit der Technologie eine besondere Herausforderung dar, da sie sowohl Kenntnis der Prozesse selbst, entsprechende IT Kenntnisse, fundierte Überlegungen über die Integration in das vorhandene Business Model und den wirtschaftlichen Nutzen im Unternehmen voraussetzt. Diese Notwendigkeit an Interdisziplinarität lässt vermuten, dass es eine erhöhte Hemmschwelle innerhalb von Unternehmen gibt, sich mit der Thematik tiefergehend zu beschäftigen und große Kapital- und Humanressourcen für die Entwicklung konkreter Anwendungen in die Hand zu nehmen.

Anzumerken ist hier, dass im Rahmen dieser Arbeit im notwendigen Maße auf die darunter liegenden IT-Aspekte eingegangen wird, jedoch der Fokus ganz klar auf den Product Life Cycle und die Anwendbarkeit gelegt wird.

Soweit notwendig, wird entsprechend auf weiterführende Quellen oder Erklärungen im Text verwiesen, welche zum tiefergehenden Verständnis der technologischen Aspekte der Blockchain beitragen können.

1.1 Problemstellung

Bisherige Untersuchungen und Arbeiten zur Blockchain-Technologie beschäftigen sich im Großteil mit der ursprünglichen Anwendungsmöglichkeit von Finanz- und Wert-Transaktionen. Dies ist auch bedingt durch die Verbreitung der Bitcoin-Blockchain, die die Technologie das erste Mal stark ins Interesse der Öffentlichkeit gesetzt hat. Insbesondere durch den Hype vieler Kryptowährungen und den dazugehörigen Investitionsmöglichkeiten, hat dieser Aspekt in den letzten Jahren rasch Fahrt aufgenommen.

Darüber hinaus gibt es noch verhältnismäßig wenige veröffentlichte Überlegungen zur Anwendung im industriellen Kontext. Unbestreitbar ist natürlich, dass es vereinzelte Use Cases von etablierten Unternehmen oder Start-Ups gibt, die eine nutzenbringende Anwendung der Blockchain in eben jenem Kontext darstellen. Besonders in jenen (Geschäfts-)Prozessen, die Transaktionen beliebiger Art erfordern, konnten bereits Erfolge verzeichnet werden. Diese betreffen soweit vor allem Aspekte des Supply-Chain Management und Logistik, handelsbezogene Prozesse, wie etwa den Energiehandel oder auch bereits vereinzelt Anwendungen im Bereich des Internet of Things.

Eine grundlegende Ursache, warum über die Anwendungsmöglichkeiten noch keine große Klarheit herrscht, stellt sicher der Umstand dar, dass es sich im Fall der Blockchain-Technologie um eine starke Technology-Push Entwicklung handelt. Durch die erste verbreitete und öffentlich bekannte Blockchain in Form der Bitcoin-Blockchain wurde eine neue Technologie präsentiert, bei der zu diesem Zeitpunkt noch keine andere Anwendungsmöglichkeit bekannt war. Somit gab es auch keine konkreten Kundenbedürfnisse, zu denen die Blockchain vorerst zugeordnet werden konnte.

Dieser Aspekt bedingt, dass durch die Anwendung der Blockchain theoretisch hohes Ertragspotenzial möglich sein könnte, wobei die Beantwortung dieser Frage sicher mit hohem Zeitaufwand und entsprechenden unternehmerischen Risiken verbunden ist. Entweder muss ein neuer Markt geschaffen werden, oder eben ein bestehender gefunden werden, wo die Technologie gewinnbringen eingesetzt werden kann.

Um diese Aspekte zu beurteilen, müssen im ersten Schritt konkrete Anwendungsmöglichkeiten gefunden werden. Aber darüber hinaus stellt sich auch die Frage der allgemeinen Sinnhaftigkeit in Bezug auf Performance, Ressourcenaufwand und Umsetzbarkeit. Insbesondere im erwähnten industriellen Kontext scheinen hier noch verhältnismäßig wenige Überlegungen stattgefunden zu haben.

Dementsprechend stellt es einen besonders interessanten Aspekt dar, wie man die Technologie nicht nur nutzen, sondern eine im Vergleich zu den derzeit verwendeten Technologien verbesserte Performance liefern kann.

1.2 Zielsetzung

Ziel dieser Arbeit ist die wissenschaftliche Bearbeitung der Fragestellung, inwiefern die Blockchain-Technologie in der Industrie zum Einsatz kommen kann. Außerdem auch die Frage, welche Potenziale und Hemmnisse die Blockchain-Technologie zum derzeitigen Stand der Technik zu haben scheint.

In weiterer Folge sollen die möglichen Einsatzfelder der Blockchain-Technologie im industriellen Umfeld eruiert und typische bzw. bereits bestehende Use Cases angeführt werden. Darauf aufbauend soll möglichst einfach und stichhaltig beurteilt werden, wie zielführend und sinnvoll die Anwendung der Blockchain-Technologie in diesen Use Cases ist und wie diese Aspekte in anderer Form im Rahmen des Product Life Cycle Anwendung finden könnten.

Die sich daraus ergebenden Ziele sind:

- Allgemeine Beschreibung der Blockchain Technologie sowie deren Ausprägung in den verschiedenen entwickelten Konzepten.
- Beantwortung der Frage: Welche möglichen typischen Use Cases gibt es für Blockchain im industriellen Umfeld.
- Erarbeitung einer Einschätzung der Vor- & Nachteile der Blockchain in den entsprechenden Anwendungsfällen bzw. gegenüber allfälligen zentralisierten Technologien.
- Beurteilung und Beschreibung relevanter Use Cases
- Identifizierung der sinnvollsten Anwendungsfelder der Technologie im industriellen Umfeld, sowie Aufzeigen entsprechender Limitierungen
- Erstellung fiktiver Fallstudien und Entwicklung dieser bis zu einem hohen Reifegrad
- Einschätzung, wie die Technologie weiters einsetzbar wäre, um eine verbesserte Performance zu generieren
- Dabei sollen nicht nur die Unterschiede, sondern vor allem auch die Potenziale der Blockchain-Technologie betrachtet werden.

1.3 Vorgehensweise

- In Kapitel 2 „Grundlagen“ der Arbeit soll die Blockchain Technologie möglichst generisch betrachtet und auf deren einzelnen Aspekte analysiert werden. Dies ist insofern besonders relevant, da sich Systeme, die als Blockchain bezeichnet werden, aus mehreren Konzepten zusammensetzen. Um einige kurz zu erwähnen, dabei handelt es sich unter anderem um Peer-to-Peer Netzwerke, Hashing, Consensus-Mechanismen, Smart Contracts und weitere, auf die dann im entsprechenden Teil der Arbeit weiter eingegangen wird.
  Durch diese Analyse sollen die entsprechenden Technologiemerkmale identifiziert werden, welche dann entsprechend der sich zeigenden Vorteil und Limitierungen zu beurteilen sind. Dabei soll wie bereits erwähnt der Fokus auf einer allgemeinen Betrachtungsweise liegen und nicht zu sehr auf einzelne Details oder Ausprägungen verschiedener Blockchains eingegangen werden.

Hierbei sollen die Aspekte der Blockchain-Technologie sowie deren Ausprägungen beschrieben und für den Leser verständlich dargestellt werden. Dabei soll vor allem darauf geachtet werden, eine möglichst allgemeingültige Definition darzustellen und daraus abweichende Spezialfälle konkret zu titulieren.

- Im praktischen Teil ab Kapitel 3 „Beurteilung, Kategorisierung und Extrapolation“ werden bereits existierende Projekte und Blockchains betrachtet und auf ihren Nutzen im industriellen Umfeld beurteilt werden. Dabei werden diese Anwendungsmöglichkeiten wieder auf ihre generisch betrachteten Grundlagen heruntergebrochen, um so eine Kategorisierung möglicher Anwendungsmöglichkeiten bzw. Teilprozesse darzustellen.
  Weiters werden in Kapitel 3.3 „Eigene Überlegungen zu Anwendungsmöglichkeiten und Extrapolation“ dann zwei Fallstudien präsentiert, die die Konzepte der Blockchain Technologie im industriellen Umfeld im Rahmen des Product Life Cycle darstellen. Dabei handelt es sich um möglichst generische Fallstudien, die auf typischen Aufgabenstellungen bzw. Prozessen im erwähnten Umfeld aufbauen.
  Diese sollen dann soweit entwickelt werden, dass die Darstellung bzw. Beschreibung der Fallstudien dem Detailierungsgrad einer Implementierungsspezifikation entsprechen.

2 Grundlagen

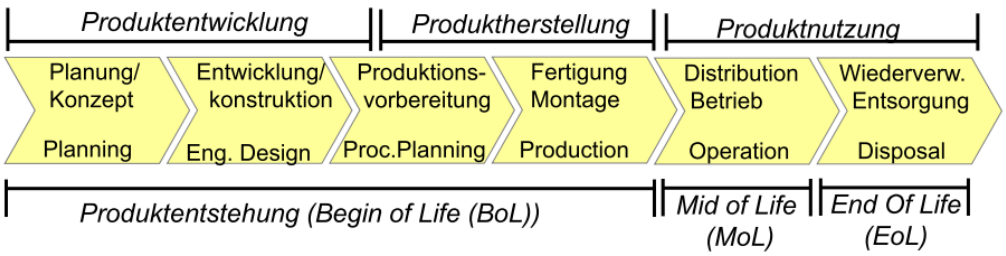
2.1 Beschreibung des industriellen Umfeldes

Fokus dieser Arbeit liegt dezidiert auf der Anwendung im industriellen Umfeld bzw. auf den Schritten entlang eines industriellen Product Life Cycle.
Dementsprechend sollen hier zu Beginn die allgemeinen und das Thema umfassenden Begriffe kurz beschrieben werden. Das hat den Zweck, die Begriffe im Rahmen dieser Arbeit konkret abzugrenzen, da diese umgangssprachlich in verschiedener, nicht immer eindeutiger Weise verwendet werden. Ebenso soll für branchenunbekannte Leser eine Wissensbasis geschaffen werden, die dem Verständnis und der Nachvollziehbarkeit nutzen soll.

2.1.1 Produktlebenszyklus / Product Life Cycle

Entsprechend Abbildung 2-1 bezieht sich im Rahmen dieser Arbeit der Begriff Product Life Cycle (Deutsch: Produktlebenszyklus) auf die Beschreibung der Abschnitte der Produktentwicklung, Produktherstellung und der Produktnutzung, die ein Produkt durchläuft. Diese umfassen im Detail die Phasen von der Idee und der Konzepterstellung mit entsprechender Dokumentation, den gesamten Entwicklungs- & Herstellungsprozess, die Supply Chain, den Betrieb und eine eventuelle notwendige Wartung des Produktes und schließlich die Entsorgung.[1]

Abbildung 2-1: Darstellung des Product Life Cycle[2]



[1] ANMERKUNG: Hierbei ist auch explizit nicht nur der betriebswirtschaftliche Lebenszyklus in der Zeit, in der ein Produkt am Markt vertreten ist, sondern es ist eben das gesamte Spektrum gemeint.
[2] Abb. 2-1 aus Gerhard D., 2019, Lehrveranstaltungs-Unterlagen: 307.490: Product Lifecycle Management VO, TU Wien

Insbesondere die Aufnahme und Weitergabe der notwendigen Information über die Prozess- und Unternehmensgrenzen hinweg stellt dabei einen kritischen Aspekt dar, der in dieser Arbeit im Speziellen betrachtet wird.[1]
Ebenso wie die Einbindung nicht direkt dem Produktentstehungsprozess zugehöriger Unternehmensbereiche wie Vertrieb, Marketing, Kundenservice und Supply Chain Management werden in Zukunft immer mehr berücksichtigt werden müssen.[2]

Diese gesamtheitliche Betrachtung ist für diese Arbeit auch insofern von Bedeutung, da durch die stetig steigende Produkt- und Prozesskomplexität die Unterstützung durch verschiedene IT-Lösungen immer mehr Relevanz erlangt. Konkret zu erwähnende Aspekte sind hier nach Eigner M. & Stelzer R.: „…die Unterstützung des Cross Enterprise Engineering, der zunehmenden Virtualisierung und der Prozessintegration.“[3]
Allgemeiner formuliert, werden nach Vajna et al. alle Systeme der Rechnerunterstützung in einem Unternehmen als CAx-Systeme kategorisiert, wie es in dem Buch „CAx für Ingenieure“ detailliert beschrieben wird.[4]

Im Laufe dieser Arbeit wird eruiert, ob und in welcher Form Blockchain-Technologie zur Nutzung in diesem Rahmen herangezogen werden kann. Insbesondere im Kapitel „Ziele & Herausforderungen im Rahmen des Product Life Cycle“3.1.2 wird auf die derzeitigen Herausforderungen in diesem Zusammenhang eingegangen um darauffolgend die konkreten Vor- Und Nachteile von Blockchain-Technologie im Kontext des Product Life Cycle zu eruieren.

2.1.2 IoT – Internet of Things

Im Rahmen dieser Arbeit wird auch immer wieder der Begriff IoT bzw. Internet of Things erwähnt werden. Dieser Begriff beschreibt im Allgemeinen ein Netzwerk, in dem IoT-Geräte durch Machine-to-Machine-Kommunikation (M2M communication) miteinander kommunizieren, wobei die Anwendung sowohl in der Industrie direkt als auch beim Endverbraucher möglich ist.[5]

Diese Beschreibung greift jedoch ein wenig zu kurz. So haben Gubbi J. et al. nach Betrachtung diverser verbreitetere Definitionen IoT in ihrem Paper 2013 wie folgt definiert: “Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications…”[6] Diese Definition hebt somit den Begriff der Verknüpfung und der Informationsweitergabe explizit hervor. Der in dieser Arbeit verwendete Begriff der Vernetzung kann sich

[1] vgl. Eigner M. & Stelzer R., 2009, S.9f
[2] vgl. Eigner M. & Stelzer R., 2009, S.9f
[3] vgl. Eigner M. & Stelzer R., 2009, S.9f
[4] vgl. Vajna et al., 2018, S.1
[5] vgl. https://www.itwissen.info/Internet-of-things-IoT-Internet-der-Dinge.html zuletzt gelesen am 01.12.2018
[6] vgl. Gubbi J. et al., 2013, S. 3

sowohl auf den Industrie- als auch auf den Endverbraucher-Kontext beziehen, da durch den Product Life Cycle die Nutzung in beiden Bereichen abgedeckt wird.

Notwendiges Kriterium, damit ein Gerät als IoT-Gerät bezeichnet werden kann, stellt nach anderen Definitionen auch die eigenen Rechenfähigkeit, also einen integrierten Prozessor sowie die Möglichkeit zur Vernetzung dar.[1]

Weiters beschreiben außerdem Mattern F. und Floerkemeier C. in ihrem Artikel „From the Internet of Computers to the Internet of Things" als primäre Herausforderungen für die Nutzung unter anderem „Skalierbarkeit, Interoperabilität, Sicherheit, Datenschutz und Ausfallsicherheit.[2] Diese Aspekte stellen unter anderem konkrete Vorteile dar, die Blockchain Netzwerke potenziell bieten könnten. Demensprechend wird im Zuge dieser Arbeit auch die Anwendung von Blockchain-Systemen im IoT-Bereich betrachtet.

2.1.3 Industrie 4.0

Industrie 4.0 ist ein Begriff für die vierte industrielle Revolution und bezeichnet einen Zustand, in dem verschiedene Aspekte in einer Industriellen Umgebung etabliert wurden und betrifft dabei primär die wesentlichen Wertschöpfungsprozesse Entwicklung, Logistik, Produktion und Service.[3]

Die „Plattform Industrie 4.0" bezeichnet den Zustand als „die intelligente Vernetzung von Maschinen und Abläufen in der Industrie mit Hilfe von Informations- und Kommunikationstechnologie."[4]

Nach Kaufmann T. handelt es sich bei den für Industrie 4.0 relevanten Aspekten um:[5, 6]

- Intelligente Maschinen/Geräte/Werkstücke unter dem Begriff „cyber-physische Systeme"
- Machine-to-Machine Kommunikation (M2M)
- Internet der Dinge / Internet of Things
- Big Data
- Selbstlernende Systeme
- Augmented Reality

---

[1] vgl. https://www.itwissen.info/Internet-of-things-IoT-Internet-der-Dinge.html zuletzt gelesen am 01.12.2018
[2] vgl. Mattern F. & Floerkemeier C., 2010, S.7ff
[3] vgl. Kaufmann T. 2015, S.4
[4] vgl. https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html;jsessionid=D7ED4118DED525F176F382A8F939369D zuletzt gelesen am 02.12.2018
[5] vgl. Kaufmann T., 2015, S.15f
[6] ANMERKUNG: Anzumerken ist hier, dass es keine absolut gültige Beschreibung von Industrie 4.0 gibt und eine exakte Definition und Abgrenzung nicht möglich ist.

Als Ausblick auf die weiteren Kapitel kann man entsprechend dieser Aufstellung und der Definition durch die Plattform Industrie 4.0 nun die Frage stellen, ob die Nutzung der Blockchain-Technologie gewisse Vorteile mit sich bringt, um dadurch zumindest manche der angeführten Aspekte zu verwirklichen. Insbesondere da es sich dabei um eine neuartige Art der Vernetzung handelt und Vernetzung als logische Schlussfolgerung die zentrale Rolle in der Industrie 4.0 spielt.[1]

2.2 Blockchain – Grundbegriffe

Um eine allgemeine Basis zu schaffen, werden in diesem Teil alle notwendigen Begriffe vorgestellt und definiert. Insbesondere, da sich oft noch keine allgemeingültige Definition entwickelt hat, wird hier die Basis für die Verwendung der Begrifflichkeiten im Rahmen dieser Arbeit gelegt. Dabei wird hier nicht der Anspruch verfolgt primär eine Einleitung in das Thema zu geben, sondern die einzelnen Begriffe genau abzugrenzen und ihnen eben im Rahmen dieser Arbeit eine klar definierte Bedeutung zuzuschreiben.

Hierbei entspricht die Tiefe der Beschreibung dem notwendigen Umfang, um die weiteren Gedankengänge nachvollziehen zu können. Alles darüber hinaus gehende, wird durch entsprechende Verweise und Zitierungen so gekennzeichnet, dass der Leser für etwaige tiefergehende Beschäftigung mit einzelnen Aspekten die entsprechenden Quellen zu Rate ziehen kann. Aufgrund des großen Umfangs und der Dynamik in der Blockchain Thematik, scheint es nicht sinnvoll auf jede Ausprägung eines Aspekts im Detail einzugehen.

Ebenso ist anzumerken, dass aufgrund der Schnelllebigkeit der Entwicklungen in diesem Bereich zum Zeitpunkt der Entstehung dieser Arbeit beschriebene Konzepte in der Zukunft schnell überholt sein können. Darum bezieht sich diese Arbeit konkret auf den Stand der Technologie zum Beginn des Jahres 2019 und bietet nur vereinzelt Ausblicke und Referenzen auf zukünftige potenzielle Entwicklungen.

Um hier bereits einen groben Rahmen um den Begriff Blockchain zu ziehen, kann ein System allgemein als Blockchain betrachtet werden, wenn es folgende Aspekte erfüllt:[2]

- Es handelt sich um ein Peer-to-Peer Netzwerk und wir nicht von einer einzelnen Instanz kontrolliert und verwaltet.
- Die Daten in der Blockchain werden in Form eines Distributed Ledgers gespeichert, welcher im gesamten Netzwerk geteilt wird.
- Im Rahmen des Informationsaustausches bzw. der Datenspeicherung wird ein Consensus-Mechanismus genutzt, um Datenintegrität zu gewährleisten und eine gemeinsame Datenbasis zu schaffen.

[1] vgl. https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html;jsessionid=D7ED4118DED525F176F382A8F939369D zuletzt gelesen am 02.12.2018

[2] ANMERKUNG: Auf diese Aspekte und Begriffe wird im Rahmen der Arbeit noch im Detail eingegangen. Diese Aufzählung dient einem ersten Überblick.

- Es werden kryptografische Mechanismen genutzt, um das System vor unerlaubtem Lese- und Schreibzugriff zu schützen und korrekte Authentifizierungen durchzuführen.
- Transaktionen werden in sogenannten Blöcken gesammelt und zur namensgebenden Blockchain verknüpft, welche alle bisherigen Transaktionen und Daten beinhaltet und nicht abänderbar ist.

Natürlich gibt es entsprechend viele Ausprägungen dieser Aspekte und ebenso einige Projekte die zwar umgangssprachlich als Blockchain bezeichnet werden, aber im engeren Sinne nicht einem solchen System entsprechen.

Darum wird in weiterer Folge genauer auf die einzelnen Konzepte hinter der Blockchain-Technologie eingegangen, um konkret jene Punkte hervorstreichen zu können, welche in einem industriellen Umfeld eines Product Life Cycle besonders von Nutzen erscheinen.

2.2.1 Ursprünge des Begriffs Blockchain: Bitcoin

Sobald man über den Begriff Blockchain spricht, kommt man nicht umhin über Bitcoin zu sprechen. Die Vorstellung von Bitcoin durch Satoshi Nakamoto 2008 in seinem Whitepaper „Bitcoin: A Peer-to-Peer Electronic Cash System“, kann als der erste öffentlichkeitswirksame Anstoß unter dem Begriff „Blockchain“ für alle weiteren Entwicklungen in diesem Bereich angesehen werden.

In seinem Paper beschreibt Nakamoto das Ziel, das er mit Bitcoin erreichen will als: “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. “[1]

Dabei soll mit Bitcoin alles getan werden können, was mit herkömmlichen Währungen auch möglich ist. Also sowohl die Transaktion von Bitcoins zwischen einzelnen Parteien als auch das Eintauschen von Bitcoins gegen Waren, Produkte oder andere Währungen.

Die ursprünglichen Überlegungen zu Bitcoin und somit zur Blockchain beziehen sich somit klar auf Transaktionen von Einheiten die einen finanziellen Wert darstellen. Um dies zu ermöglichen hat Nakamoto mehrere Konzepte vereint, um ein System zu entwickeln, das solche Transaktionen ohne eine zentral verwaltende Stelle wie einer Bank möglich machen soll.

Diese Konzepte entsprechen im Groben den im vorherigen Kapitel vorgestellten Aspekten einer Blockchain, wobei der Nutzung des Consensus-Mechanismus als die signifikante Innovation bei Bitcoin angesehen werden kann. Dadurch ist es auf einem praktischen Weg möglich, innerhalb eines Peer-to-Peer Netzwerks einen Konsens über die durchgeführten Transaktionen zu erreichen. In Folge dessen kann das bereits von Nakamoto erwähnte Adressieren des Prob-

[1] vgl. Nakamoto, 2008, S.1

lems „double spending“, also die eindeutige Zuordnung der Bitcoins zu deren Besitzer, garantiert werden.[1, 2] Zusätzlich kann dieser Konsens herbeigeführt werden, ohne der Notwendigkeit einer zentralen Autorität, die die Transaktionen kontrolliert und bestätigt.[3]
Darauf, wie diese beiden Aspekte im Speziellen bei Bitcoin technisch gelöst werden, wird in Kapitel „Consensus“ eingegangen. Insbesondere, da mittlerweile mehrere Möglichkeiten entwickelt wurden, um diese Probleme der unerwünschten Wertvermehrung zu adressieren, und Bitcoin eben nur eine der ersten Ansätze darstellt.

Antonopoulos A. beschreibt in seinem Buch „Mastering Bitcoin“, welches als eines der ersten Standard-Werke in dem Bereich gilt: „Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called bitcoins are used to store and transmit value among participants in the bitcoin network.”[4]
Dabei können diese Transaktionen mittels dem Bitcoin-Protokoll sowohl über das Internet als auch über diverse andere Netzwerke erfolgen, wie etwa Mobilfunk, Mesh-Netzwerken oder sogar Amateur-Radiofrequenzen.[5]
Ebenso bei der Auswahl der Endgeräte ist man für Nutzung des Bitcoin Netzwerks recht flexibel. Insbesondere, da Transaktionen bereits mit relativ leistungsschwachen Geräten, wie etwa Smartphones, durchgeführt werden können. Dadurch ist vor allem auch die technologische Hürde, um am Netzwerk teilzunehmen, relativ gering.

Ein Bitcoin, als Währungseinheit selbst, wird komplett digital dargestellt. Dabei ist anzumerken, dass Bitcoins nicht als eigene Entitäten existieren, sondern durch Transaktionen impliziert definiert werden. In der Bitcoin-Blockchain sind alle bisherigen Transaktionen aufgezeichnet. Erst aus der Summe aller Transaktionen ergibt sich die jeweilige Menge an Bitcoin die die einzelnen Netzwerk-Teilnehmer besitzen.[6]
In den folgenden Kapiteln werden auf die technischen Aspekte der Transaktionen im Speziellen eingegangen.

Durch die vorgestellten Mechanismen, wie sie erstmalig in der Form in der Bitcoin-Blockchain eingesetzt werden, wurde eine Lösung für zwei konkrete Hürden präsentiert, die im Allgemeinen bei der Nutzung von digitalen Währungen zu überwinden sind:[7]

- Kann man sicher sein, dass die Währung authentisch ist und nicht gefälscht ist?
- Kann man sicher sein, dass niemand sonst behauptet im Besitz meines Geldes zu sein?

Diese Hürden sind besonders in einer sich zunehmen digital vernetzen und arbeitenden Welt von Bedeutung. Digitale Güter, und wie in diesem Fall Bitcoins, können theoretisch beliebig oft

[1] vgl. Nakamoto, 2008, S.1
[2] ANMERKUNG: Double Spending bezeichnet die Situation in der ein Nutzer den selben Bitcoin mehrere male transferieren könnte und somit das von ihm besessene Bitcoin-Vermögen aus dem nichts erhöht.
[3] vgl. Antonopoulos A., 2015, S.3
[4] vgl. Antonopoulos A., 2015, S.1
[5] vgl. https://usethebitcoin.com/sending-bitcoin-without-internet-or-satellite-is-now-a-reality/ zuletzt gelesen am 16.12.2018
[6] vgl. Antonopoulos A., 2015, S.2
[7] vgl. Antonopoulos A., 2015, S.2

kopiert werden und würden somit den immanenten Wert ad absurdum führen. Darum ist es bei digitalen Währungen, und in weiterer Folge allen digitalen Gütern, von signifikanter Bedeutung diese Vervielfältigbarkeit zu unterbinden und somit den Wert zu schützen. Bei physischen Währungen und Gütern, stellte das auf natürliche Weise bisher ein verhältnismäßig kleineres Problem dar. Ein Produkt oder eine Währungseinheit in Form einer Münze oder eines Geldscheins, lässt sich nicht ohne Ressourcenverbrauch kopieren bzw. fälschen. Außerdem ist durch physische Werteinheiten kein Double Spending möglich, wie digitalen Aufzeichnungen oder Werteinheiten.

Im Falle der bisherigen Währungen und dem Aufkommen des digitalen Bankings, wurde es jedoch notwendig, dass zentrale Stellen, in diesem Fall Banken, die Transaktionen durchführten und für die Sicherheit und Zuverlässigkeit des Systems Sorge tragen mussten. Diese zentralen Stellen agieren dabei als Treuhänder und verhindern eben das Double Spending im Zuge der digitalen Transaktionen. Auch wenn diese Tätigkeit zumeist im Hintergrund stattfindet, ist der administrative Aufwand nicht zu unterschätzen und stellt einen erheblichen Kostenfaktor dar.

Hinzu kommt natürlich auch die Anfälligkeit dieser zentralen Systeme für Angriffe von außen etwa durch Hacking oder Social Engineering.[1] Auch diesem Problem wurde in der Bitcoin Blockchain Rechnung getragen, indem Kryptografie-Mechanismen in das System integriert wurden. Dabei ist es nur durch ein bestimmtes Schlüsselpaar (siehe: Kapitel „Transaktionen und Blöcke – Abschnitt „Public und Private Keys“) für den jeweiligen Nutzer möglich Transaktionen von einem Account durchzuführen. Und durch die Art der eingesetzten Kryptografie - im Fall von Bitcoin der SHA256-Alhoritmus – ist es mit heutigen Mitteln auch nicht in realistischem Rahmen möglich diese Verschlüsselung zu knacken. Selbstverständlich ist es nach wie vor möglich, dass die notwendigen Schlüssel in falsche Hände geraten und somit zu unautorisierten Transaktionen verwendet werden. Diese Betrugsfälle beziehen sich jedoch auf Fehler der Nutzer außerhalb des Systems.

All diese Aspekte kann man jedoch weiterdenken, wenn man die Anwendung nicht auf Währungen beschränkt. Im praktischen Teil dieser Arbeit wird betrachtet, inwiefern jene Aspekte eben auch im industriellen Kontext relevant sein können. Anstelle die Blockchain zur Darstellung von Währungen zu nutzen, kann man beliebige Datensätze heranziehen und mittels einer Blockchain sicher gehen, dass diese authentisch und nicht gefälscht sind. Bitcoin stellt dem entsprechend nur die Spitze des Eisberges dar. Bereits in der Einleitung zu Antonopoulos „Mastering Bitcoin “, schreibt der Autor, “I see bitcoin as akin to the Internet of money, a network for propagating value and securing the ownership of digital assets via distributed computation. There’s a lot more to bitcoin than first meets the eye.”[2]

Um in das Thema tiefer einzusteigen wird nun im Folgenden in einer möglichst generischen Form dargelegt, wie die Blockchain Technologie im Allgemeinen funktioniert und welchen Nutzen diese Aspekte eventuell für die Anwendung im Product Life Cycle und im industriellen Kontext darstellen.

---

[1] vgl. https://www.gdata.at/ratgeber/was-ist-eigentlich-ein-social-engineering, gelesen am 15.12.2018

[2] vgl. Antonopoulos A., 2015, S.2

2.2.2 Grundlegende Aspekte der Blockchain

Wie bereits im oben angeführten ersten Zitat von Antonopoulos zu lesen, bildet sich die Bitcoin-Blockchain, so wie alle anderen Blockchain-Systeme, aus einer Kombination mehrerer mehr oder weniger neuer Konzepte. Bitcoin stellt im Speziellen also nicht die eigentliche Definition der Blockchain dar, sondern sozusagen den ersten Use Case, der unter dem Begriff „Blockchain“ der allgemeinen Öffentlichkeit bekannt wurde. Im Folgenden werden die wichtigsten dieser Konzepte angeführt und für die weitere Verwendung in dieser Arbeit abgegrenzt. Die Gesamtheit dieser Konzepte bildet dann das technologische Fundament der Blockchain-Technologie und aller Anwendungsmöglichkeiten. Sei es in Bezug auf Finanztransaktionen und sogenannte Kryptowährungen[1] oder den für diese Arbeit relevanten Anwendungsmöglichkeiten.

Dazu werden in weiterer Folge die zum Verständnis für das Thema notwendigen Begriffe angeführt und abgegrenzt. Die Reihenfolge der Begriffe orientiert sich hier von einer eher allgemeinen Basis hin zu spezielleren Ausprägungen der Technologie. Da eine solche Reihung jedoch nur bis zu einem gewissen Grad möglich ist, sollte der Reihenfolge keine allzu große Bedeutung zugedacht werden. Besonders wichtig ist es jedoch, die Blockchain-Technologie und ihre Anwendungsmöglichkeiten möglichst in ihrer Gesamtheit zu begreifen. Viele der beinhalteten Konzepte stellen eigene große Thematiken in der Informatik dar, die nicht im Umfang dieser Arbeit im Detail erläutert werden können. Für tiefergehende Beschäftigung mit den einzelnen Aspekten wird auf die Literaturverweise bzw. die Ergänzungen in den Fußnoten verwiesen. Außerdem besteht durch die Neuartigkeit und stetige Weiterentwicklung der Technologie eine solche Dynamik, dass es nicht sinnvoll erscheint im Rahmen dieser Arbeit auf alle Aspekte und Eventualitäten einzugehen. Insbesondere da sich einzelne Details noch monatlich ändern können. Etwaige Adaptionen oder Einzelheiten werden bei Bedarf bei den einzelnen Use Cases oder bei der Vorstellung spezieller Blockchain-Lösungen angeführt. Auf gebräuchliche und allgemein akzeptierte Definitionen und Abgrenzung der Blockchain-Technologie als Gesamtes wird im Anschluss auf die Darlegung der einzelnen Aspekte eingegangen.

Wie bereits in der Einleitung des Kapitels „Blockchain – Grundbegriffe“ erwähnt, hat eine Blockchain im Allgemeinen folgende Komponenten, die nun systematisch im Detail vorgestellt werden:

- Peer-to-Peer - Netzwerk[2]
- Distributed Ledger[3]
- Kryptografie[4]

---

[1] ANMERKUNG: Siehe Kapitel “Kryptowährungen“
[2] Siehe Kapitel “Verteilte Systeme”
[3] Siehe Kapitel „Distributed Ledger“
[4] Siehe Kapitel „Transaktionen und Blöcke“ – Abschnitt „Private und Public Key“

- Consensus[1]
- Aneinanderreihung von Blöcken zur Blockchain[2]

Verteilte Systeme

Im Prinzip stellt ein Blockchain-System ein Netzwerk von Computern dar. Also ein System, welches durch gewisse Kommunikation und Transferprotokolle über mehreren physischen oder virtuellen Computern verteilt ist. Diese Systeme können im Allgemein als verteilte Systeme klassifiziert werden und bilden den Grundstock der heutigen digitalen Welt.

Coulouris et. al gaben 2001 in deren Werk „Distributed Systems: Concepts and Design" als möglichst allgemeine Definition folgende an: „We define a distributed system as one in which hardware or software components located at networked computers communicate and coordinate their actions only by passing messages."[3]

Diese Definition umfasst dementsprechend alle gebräuchlichen Netzwerke, die heutzutage im Einsatz sind. Als Beispiele können angeführt werden:

- Intranet
  - internes Netzwerk innerhalb einer Organisation
  - zum Beispiel einer Fabrik, eines Unternehmens oder sogar nur einer Maschine mit mehreren Komponenten, die getrennte Computer besitzen
- Internet
- Mobilfunknetzwerk
- Blockchainnetzwerke

Die allen gemeinsame Motivation entspringt dem Wunsch, Ressourcen irgendeiner Art zu teilen. Dabei kann es sich um die gemeinsame Nutzung spezieller Hardware handeln (zB. ein Drucker), das Teilen von Daten, Arbeitsaufteilung oder der Transfer von Informationen.[4]
Diese Ziele implizieren, dass es innerhalb des Systems zu einer Kollaboration der einzelnen Teilnehmer, auch Nodes genannt, kommen muss.[5]
Als Teilnehmer sind hier explizit die sich im Netzwerk befindlichen Computer gemeint, und nicht der Nutzer, der das Netzwerk als physische Person nutz.

Um diese Kollaboration fehlerfrei gewährleisten zu können, müssen verteilte Systeme nach Coulouris et al. gewisse Herausforderungen bestehen, die in weiterer Folge demzufolge auch hohe Relevanz für die Anwendung von Blockchain-Netzwerken hat:[6]

- Sicherheit
  - Wie sicher ist das System vor nicht gewolltem Fremdzugriff und wie sicher sind die darauf abgespeicherten Daten vor Veränderung?

---

[1] Siehe Kapitel „Consensus"
[2] Siehe Kapitel "Transaktionen und Blöcke" – Abschnitt „Blöcke"
[3] vgl. Coulouris et. al, 2001, S.2
[4] vgl. Coulouris et. al, 2001, S.2
[5] vgl. Van Stehen M. & Tanenbaum A., 2016, S.2
[6] vgl. Coulouris et al., 2001, S.16 ff

- Heterogenität
  - Wie gut kann das System mit verschieden leistungsfähigen Computern im Netzwerk umgehen?
- Fehler-Management
  - Was passiert, wenn ein Computer im Netzwerk ausfällt oder kompromittiert wird?
- Parallelität
  - Wie gut können die einzelnen Computer im Netzwerk parallel arbeiten und unabhängig voneinander Daten verarbeiten, um das Ergebnis dann zu teilen?
- Ressourcenverbrauch und Skalierbarkeit
  - Wie leistungsstark müssen die eingesetzten Computer sein und in wie fern und wie einfach kann man das Netzwerk um weitere Computer vergrößern

Die zum jetzigen Zeitpunkt am weitesten verbreitete und akzeptierte Art, um solche Architekturen aufzubauen ist das Client-Server Modell. Dabei besteht das Grundkonzept daraus, dass es mehrere verteilte Clients gibt, die die Anfragen der Nutzer aufnehmen und diese an eine zentrale Stelle weiterleiten, die diese Anfragen verarbeitet und das Ergebnis an den Client und somit den Nutzer zurücksendet.[1]

Übliche Beispiele hierfür sind beispielsweise Datenbank-Server, auf denen die Daten selbst gespeichert werden und der Client nur konkrete Abfragen an den Server sendet, um die gewünschten Daten aus der Datenbank auszulesen. Auch Änderungen der Datensätze werden zwar vom Client in Auftrag gegeben, aber zentral vom Server durchgeführt und neu abgespeichert.

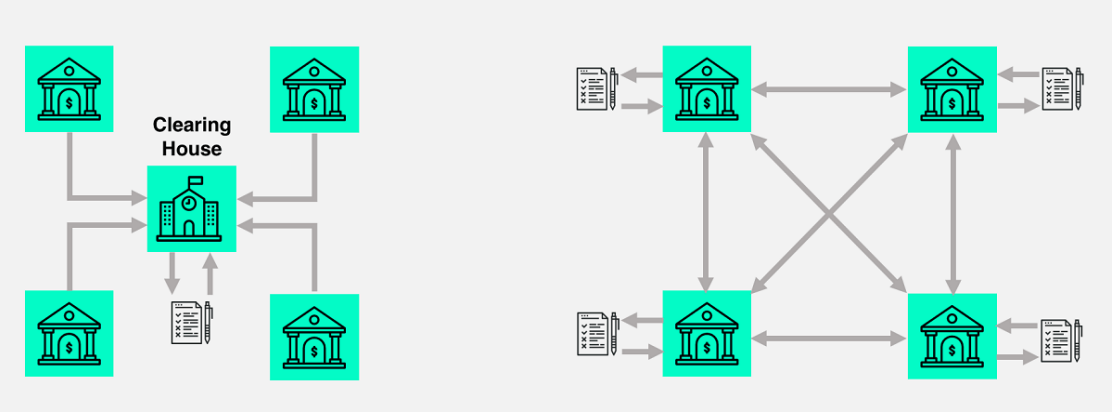
Peer-to-Peer Netzwerke, wie Blockchains, die kategorisch als solche angesehen werden können, werden von Antonopoulos als solche definiert: „… P2P, means that the computers that participate in the network are peers to each other, that they are all equal, that there are no “special” nodes, and that all nodes share the burden of providing network services.”[2]
Im Gegensatz also zum Client-Server Modell, werden die gewünschten Aktionen nicht explizit auf einer zentralen Einheit ausgeführt, sondern können von jedem Node ausgeführt werden. Wenn nun geplant ist, dass alle Nodes alle Informationen speichern und zur Verfügung haben, müssen die Ergebnisse der durchgeführten Aktionen auch wieder an alle Nodes verbreitet werden. Und genau dieses Verbreiten stellt oft eine große Herausforderung dar, da dem Ergebnis alle Nodes auch zustimmen müssen, ohne dass eine zentrale Einheit das Ergebnis vorgibt und die allgemeine Wahrheit definieren kann. In Blockchain-Systemen wird dieses Problem eben durch Consensus-Mechanismen adressiert. (Siehe Kapitel „Consensus“)

In Abbildung 2-2 ist zu sehen, welchen Unterschied eine zentraler Netzwerkaufbau (links) im Vergleich zu einem dezentralen Netzwerkaufbau (rechts) am Beispiel von Transaktionen innerhalb eines Banken-Netzwerks ausmacht. Dabei soll besonders verdeutlicht werden, dass bei der zentralen Variante eine zentrale Autorität notwendig ist, die die Transaktionen kontrolliert

[1] vgl. Gosh S., 2007, S.13
[2] vgl. Antonopoulos A., 2015, S.137

und regelt, hier in der Abbildung als „Clearing House“ gekennzeichnet. Eine solche Autorität ist bei dezentralen Netzwerken wie rechts dargestellt nicht notwendig.

Abbildung 2-2: Beispielhafte Darstellung von Banktransaktionen zum Vergleich von zentralisiert kontrollierten Transaktionen (links) und dezentralen Transaktionen (rechts) [1]



Bei dem Netzwerk mit zentraler Autorität ist erkennbar, dass diese sozusagen den Flaschenhals darstellt. Fällt diese aus, ist das gesamte System lahmgelegt. Wird auf deren Server etwas manipuliert, wird es vom gesamten System als „Wahrheit“ angesehen. Dafür ist die Leistungsfähigkeit des Systems primär nur von der Leistungsfähigkeit der zentralen Autorität abhängig und die Skalierbarkeit hängt linear zusammen mit der Skalierbarkeit der IT-Infrastruktur dieser zentralen Stelle.
Im Gegenzug dazu, müssen beim dezentralen Netzwerk alle Aktionen verbreitet und aufgezeichnet werden, was einen hohen Anspruch an die Leistungsfähigkeit der einzelnen Teilnehmer und deren IT-Infrastruktur stellt. Außerdem ergibt sich durch diese Form im Regelfall eine hohe Redundanz der Daten und eine hohe Resilienz des Gesamtsystems gegen Ausfall einzelner Teilnehmer.

Distributed Ledger

Im Zusammenhang mit dem Blockchain-Thema kommt man auch sehr oft mit dem Begriff Ledger in Verbindung der einen integralen Bestandteil der Blockchain darstellt. Ein Ledger bezeichnet in der ursprünglichen Form ein Kassabuch oder ein Konto. Also eine Aufzeichnung über Gut- und Lastschriften von Geldbewegungen.[2]

[1] vgl. https://tradeix.com/distributed-ledger-technology/ zuletzt gelesen am 10.04.2019
[2] vgl. http://www.businessdictionary.com/definition/ledger.html, zuletzt gelesen am 13.12.2018

Spricht man nun von einem Distributed Ledger, handelt es sich schlicht um ein solches Kassabuch, welches in Form eines verteilten Systems existiert. In diesem Fall explizit ein dezentrales System bzw. eine Peer-to-Peer Netzwerk. Also eine Datenbank von Einträgen, die an verschiedenen Orten abgespeichert sind und nicht von einer zentralen Instanz bearbeitet und geprüft werden.[1]

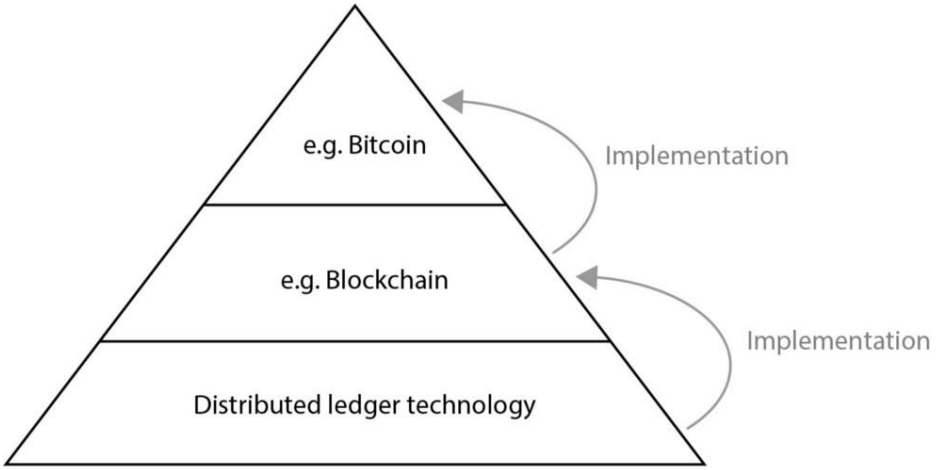
Wichtig zu erwähnen ist hierbei, dass es sich nicht zwangsläufig um Finanz-Transaktionen handeln muss, die auf einem Distributed Ledger stattfinden. Also dieses Kassabuch kann auch beliebige andere Informationen beinhalten, was für die Anwendungsmöglichkeiten im Product Life Cycle von immanenter Bedeutung ist.

Die Tatsache, dass die Einträge nicht zentral gespeichert werden, sondern die Gesamtheit aller Transaktions-Informationen an mehreren Orten gespeichert sind, birgt unter anderem den Vorteil, dass die zentrale Stelle nicht den erwähnten Flaschenhals darstellt. Bei zentralisierten Systemen fällt das gesamte System aus, wenn die zentrale Stelle ausfällt. Durch die bestehende Redundanz eines Distributed Ledger System, ist das System weiter funktionsfähig, auch wenn ein Teil des Netzwerks ausfällt. Damit das jedoch funktioniert, wird ein Mechanismus benötigt, der dafür sorgt, dass über das gesamte Netzwerk hinweg die gleichen Informationen abgebildet sind. Dieser Mechanismus wird als „Consensus“ Mechanismus bezeichnet, welcher explizit in Kapitel „Consensus“ erläutert wird. Eben dieser Mechanismus stellt auch eine der größten Herausforderungen dar, für die verschiedene Blockchain-Systeme unterschiedliche Lösungen anbieten.

Der Aufbau als Distributed Ledger allein reicht aber nicht, um bei einem Netzwerk bereits von einer Blockchain sprechen zu können und es stellt einen weit verbreiteten Irrtum dar, wenn diese beiden Begriffe komplett synonym verwendet werden. Denn die Blockchain stellt zwar eine Anwendung des Distributed Ledger Prinzips dar, jedoch stellt nicht jeder Distributed Ledger System eine Blockchain dar. Bildlich dargestellt wird diese Beziehung in einfacher Form in Abbildung 2-3. Hierbei explizit verbildlicht ist die Tatsache, dass die Blockchain im Allgemeinen eine Realisierung (engl. „Implementation“) von Distributed Ledger Technologie Konzepten darstellt und als Beispiel Bitcoin eben eine konkrete Realisierung von Blockchain Konzepten zur Erfüllung spezifischer Use Case Anforderungen darstellt.

[1] vgl. https://tradeix.com/distributed-ledger-technology/ zuletzt gelesen am 13.12.2018

Abbildung 2-3: Darstellung des Zusammenhangs zwischen Distributed Ledger und Blockchain[1]



Ziele eines Distributed Ledger Systems und somit auch der meisten Blockchains sind im Allgemeinen[2]:

- der Wegfall von zentralen Stellen die potenziell anfällig sind für Cyber-Attacken oder Fehler
- effiziente Transaktionsgeschwindigkeiten
- geringe Kosten
- hohe Sicherheit
- geringer Fehleranfälligkeit

Welche weiteren Aspekte erfüllt sein müssen, damit ein Distributed Ledger System als Blockchain bezeichnet werden kann, wird in den folgenden Kapiteln erläutert.

Transaktionen und Blöcke

Bevor nun genau auf den Transaktions-Prozess sowie die sogenannten Blöcke einer Blockchain eingegangen wird, müssen einige Begriffe abgegrenzt werden, da diese oft synonym verwendet werden, sich dahinter jedoch unterschiedliche technische Aspekte der Blockchain verbergen.

[1] vgl. https://hackernoon.com/gaining-clarity-on-key-terminology-bitcoin-versus-blockchain-versus-distributed-ledger-technology-7b43978a64f2 zuletzt gelesen am 10.04.2019

[2] vgl. Tapscott D. & Tapscott A., 2016, S.6

Nodes

Nodes wurden bereits im Unterkapitel „Verteilte Systeme“ kurz erwähnt und stellen den Begriff für die physischen Computer im Bitcoin-Netzwerk dar. Dabei haben diese Computer verschiedene Funktionen. Die wichtigsten in Bezug auf die Blockchain, stellen das In-Auftrag-geben und der Validierung von Transaktionen, die Speicherung des Ledgers und der Teilnahme am Consensus Mechanismus dar. Ebenso können diese Nodes natürlich auch alle anderen Funktionen erfüllen, die sie in einem normalen Peer-to-Peer Netzwerk auch erfüllen würden.[1] Manche Blockchain-Systeme besitzen einen zugehörigen Software-Client, der auf dem Node ausgeführt werden kann und als Benutzeroberfläche dient.

Account & Adresse

Es gibt keine allgemeine Definition, die Account und Adresse konkret unterscheidet. Oft werden diese Begriffe Synonym verwendet. Um eine klare Abgrenzung im Rahmen dieser Arbeit zu schaffen, werden die beiden Begriffe wie folgt definiert:

Der Account steht für die eigentliche Darstellung des Kontos in der Blockchain. Also in dem Zusammenhang um die eigentliche Entität, von der Transaktionen durchgeführt werden. Vergleichbar mit dem Konto bei einer Bank. Ein Account stellt somit eine Repräsentation einer externen Identität dar, wobei jedoch eine externe Identität beliebig viele Accounts erstellen und verwalten kann.[2]

Die Adresse im Gegensatz dazu bezieht sich auf die „Identifikationsnummer“ des Accounts. Die meisten Blockchain-Systeme bedienen sich dabei dem Prinzip der asymmetrischen Kryptografie aus Public Key und Private Key wie sie im Abschnitt „Hashing“ dieses Kapitels im Detail beschrieben wird. Dabei stellt der sogenannte Public Key den Ursprung für die eigentliche Adresse dar und wird aus dem Private Key generiert.[3]

Diesen Public Key kann man sich ähnlich wie eine IP-Adresse vorstellen. Dieser macht eine einzigartige Identifikation im Netzwerk möglich und ist dabei prinzipiell[4] anonym, da er automatisch generiert und aus einer zufälligen Zeichenfolge besteht. Um nun die Adresse aus dem Public Key zu generieren, nutzt man z.B. das Base58-Verfahren.[5] Dadurch lässt sich die Adresse als eine einfachere Zeichenkette darzustellen und stellt somit eine kürzere, repräsentative Form des Public Keys dar.[6]

---

[1] vgl. Bashir I., 2017, S18
[2] vgl. http://ethdocs.org/en/latest/account-management.html zuletzt gelesen am: 15.12.2018
[3] vgl. Bashir I., 2017, S17
[4] ANMERKUNG: Der Public Key ist prinzipiell anonym, durch die Erstellung des Keys durch Nutzung einer rückverfolgbaren IP-Adresse kann diese Anonymität jedoch beeinträchtigt werden.
[5] vgl. https://en.bitcoin.it/wiki/Base58Check_encoding zuletzt gelesen am: 15.12.2018
[6] vgl. https://blockchain.zendesk.com/hc/en-us/articles/360000951966-Public-and-private-keys zuletzt gelesen am: 15.12.2018

Dies kann man sich wiederum vorstellen, wie die Nutzung eines DNS[1] beim Aufrufen von IP-Adressen über das Internet. Wobei solche Methoden nicht zwangsläufig zum Einsatz kommen müssen. Ethereum zum Beispiel definiert schlicht die letzten 20 Bytes des Public Key als Adresse[2].
Zu erwähnen ist auch, dass verschiedene Blockchains auch verschiedene Arten von Adressen besitzen, da die konkrete Ausführung vom Entwickler abhängt. Diese unterscheiden sich zum Beispiel durch die Art der Darstellung und wie sie generiert werden.

Public & Private Keys

Das bereits oben erwähnte System der asymmetrischen Kryptografie auf dem viele Blockchains aufbauen, besteht wie gesagt aus dem Public Key und dem Private Key. Der Public Key, stellt in dem Kontext die Möglichkeit zur Identifikation des Accounts dar und ist öffentlich in der Blockchain einsehbar. Der Private Key wiederum ist notwendig für die Autorisierung von Transaktionen. Durch die Kenntnis dieses Schlüssels können entsprechend Transaktion von einem Blockchain-Account durchgeführt werden.[3]

Im Fall von Bitcoin wird der Private Key zuerst als Zeichenfolge mit einer Länge von 256 Bits per Zufall generiert und entspricht in etwa einer Zahl der Größe 10^{77} in Dezimalschreibweise. Wie dies geschieht ist unerheblich für die Funktion der Keys. Aus dieser Zeichenfolge wird dann mittels „Elliptic Curve Multiplication“ der Public Key erstellt. Dabei handelt es sich wiederum um eine kryptografische Funktion, die praktisch nur in eine Richtung durchführbar ist.[4]
Der Hintergrund hierfür ist, dass für die Kalkulation des Public Key relativ einfach durchführbar ist.[5] Um jedoch vom Public Key die Kalkulation zum Private Key durchzuführen, muss ein sogenanntes „Problem des Diskreten Logarithmus“ gelöst werden.[6]
Anzumerken ist jedoch auch, dass für das Prinzip der asymmetrischen Kryptografie nicht nur die von Bitcoin genutzte „Elliptic Curve Multiplication“ herangezogen werden kann. Seit der Erfindung der asymmetrischen Kryptografie wurden diverse mathematische Funktionen entdeckt, die für diesen Zweck nutzbar sind. Diese haben jedoch alle gemeinsam, dass sie in eine Richtung leicht lösbar sind, jedoch es in die andere Richtung mit heutiger Rechenleistung praktisch nicht möglich ist eine Lösung zu finden.[7]

---

[1] DNS = Domain Name System
[2] vgl. http://ethdocs.org/en/latest/account-management.html zuletzt gelesen am: 15.12.2018
[3] vgl. Antonopoulos A., 2015, S.63
[4] vgl. Antonopoulos, 2015, S.63ff
[5] ANMERKUNG: Als Beispiel für ein relativ einfach zu lösendes System: 7^{256} mod 13 =?. Dies kann vergleichsweise einfach berechnet werden mit der Lösung: 7^{256} mod 13 = 9. Möchte man jedoch bei 7^x mod 13 = 9 die Variable x berechnen stellt das eine schwierigere Aufgabe dar, die die Anwendung spezieller Lösungsmethoden bedarf. Stellt nun die Kalkulation die Aufgabe $(x^3 +7)$ mod p = y^2 mod p dar, wie sie zum Beispiel in der Bitcoin Blockchain so definiert ist, wobei p einer Zahl in etwa der Höhe 10^{77} entspricht, ist es nach heutigem Stand der verfügbaren Rechenpower nicht möglich die Gleichung zu lösen.
[6] vgl. Antonopoulos A., 2015, S.65
[7] vgl. Antonopoulos A., 2015, S.62

Die genaue Nutzung dieses Key-Paares im Zuge der Durchführung der Transaktionen wird im „Signatur“-Abschnitt dieses Kapitels genauer beschrieben.

Hashing

Ein weiteres kryptografisches Werkzeug, welches im Rahmen der Blockchain-Technologie genutzt wird, ist das Hashing. Damit wird allgemein die Methodik beschrieben, wodurch von einem Input relativ schnell auf ein Ergebnis, einen Output, geschlossen werden kann. Jedoch vom Output auf den ursprünglichen Input zurückzuschließen, stellt sich als praktisch nicht durchführbar dar.[1]
Zusätzlich wird mit einem Daten-Input beliebiger Größe ein Output generiert, der eine fixe Größe besitzt. Dieser Output wird dann als Hash bezeichnet. Dabei kann der Input von einer einzelnen Ziffer bis hin zu der Gesamtheit der Daten einer Datenbank und darüber hinaus variieren. Zur Anwendung kommen dabei diverse Hashing Algorithmen, je nach Notwendigkeit und Anwendungsfall.[2]

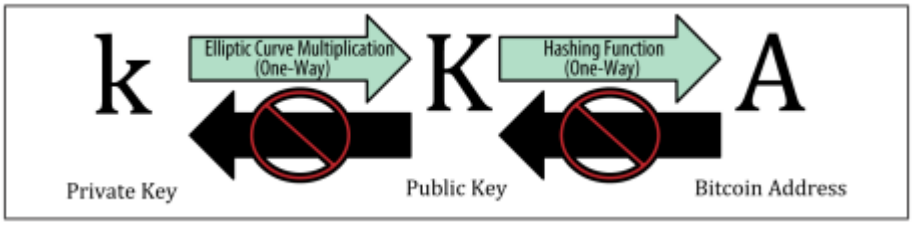
Einer der ersten verwendeten Hashing-Algorithmen bei Blockchain-Systemen hat die Bezeichnung SHA256, welche eine Zeichenkette der Länge von 256 Bits ausgibt. Dieser wird zB. auch bei Bitcoin verwendet. Durch die Anwendung dieser Methode, kann ebenso wie bei der zuvor erwähnte Elliptic Curve Multiplication relativ einfach ein Output gefunden werden. Und das unabhängig von der Datengröße des Inputs.[3]

Eine typische Anwendung von Hash-Funktionen ist die Überprüfung von Daten-Integrität und der Erstellung digitaler Signaturen. Da ein konkreter Input immer exakt denselben Output liefert, würde bei einer Veränderung des Inputs, also der Daten, auch eine Veränderung der Signatur zur Folge haben.

Einer der Gründe, warum Hashing des zur Sicherheit der Blockchain beiträgt ist, dass zu jedem Zeitpunkt ein Hash besteht, der alle bisherigen Transaktionen der Blockchain als Input hat. Dieser Hash wird benutzt, um für alle Nutzer eine gemeinsame Version der Blockchain über den aktuellen Status zu generieren. Würde die Blockchain nun verändert werden, ändert sich auch der Hash und die Manipulation würde erkennbar werden. Im Endeffekt müssen also die Nutzer der Bitcoin-Blockchain somit nur eine Sequenz von 256-bit überprüfen, um die Richtigkeit aller bisherigen Transaktionen zu überprüfen. Und das funktioniert komplett unabhängig von der Größe der Blockchain. Als Beispiel hat die Ethereum Blockchain zu Beginn des Jahres 2019 eine Gesamtgröße im zweistelligen Gigabyte-Bereich. Dennoch kann der Status der Blockchain durch ihren Hash von 256-bits überprüft werden.[4]

[1] vgl. Watternhofer R., 2016, S.84
[2] vgl. https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ zuletzt gelesen am 19.12.2018
[3] vgl. Bashir I., 2017, S.186
[4] vgl. https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ zuletzt gelesen am 19.12.2018

Abbildung 2-4: Prozess der Generierung der Keys und der Bitcoin Adresse[1]



Im Fall von Bitcoin wird nicht nur die Blockchain selbst gehasht, auch die Bitcoin Adresse wird aus dem Public Key mittels Hashing generiert. Abbildung 2-4 zeigt in diesem Zusammenhang den gesamten Prozess vom Private Key, hier mit k bezeichnet, bis hin zur Bitcoin Adresse mit der Bezeichnung A.

Blöcke

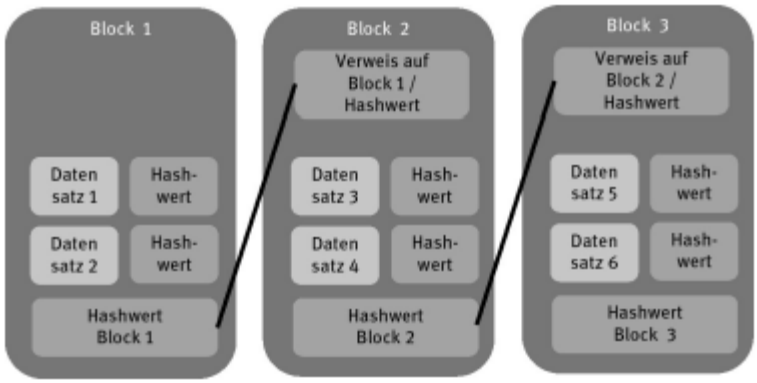
Die sogenannten Blöcke stellen sozusagen den Kern einer jeden Blockchain dar. Auf eine möglichst generische Betrachtung heruntergebrochen, handelt es sich bei einem Block um eine gehashte Sammlung von Transaktionen innerhalb der jeweiligen Blockchain. Im Zuge der Durchführung der Transaktionen werden diese Blöcke von ausgewählten Nutzern generiert (siehe: Consensus-Mechanismus im Kapitel „Consensus). Im Zuge dieser Generierung werden die Transaktionen verifiziert und durchgeführt.[2]

In Abbildung 2-5 von Dr. Burgwinkel (2016) ist das Prinzip ersichtlich, wie die Blöcke in der einfachsten Form aufgebaut sind und wie sie zusammenhängen. Neben dem Hashwert, den jeder Datensatz, also jede Transaktion innehat, wird ebenso ein Hashwert über jeden Block gebildet. Dieser Hashwert ist für diesen speziellen Block, in dieser Ausführung, einzigartig. Würde nun der Block verändert werden, ändert sich auch der Hashwert.

Wird nun ein neuer Block gebildet, also z.B. Block 2 immer zeitlich betrachtet nach Block 1, so fließt auch der Hashwert des vorherigen Blocks in den neuen Hashwert des aktuellen Blocks mit ein. Durch diese Verkettung bezieht sich der Hash-Input nicht nur auf die aktuellen Daten, respektive Transaktionen, sondern auf die gesamten vergangenen Informationen der Blockchain. Jeder Block wird des Weiteren mit einem sogenannten Timestamp versehen, also der Information wann der Block erstellt wurde. Dadurch wird auch sichergestellt, dass der Block 2 zum Zeitpunkt T2 erstellt wurde und die Erstellung zeitlich nach Block 1 zum Zeitpunkt T1 erfolgt ist.[3]
Diese Verkettung ist auch namensgebend für das Gesamtkonzept der Blockchain-Technologie.

[1] Abb. 2-4 aus Antonopoulos A.,2015, S.63
[2] vgl. Gupta S. & Sadoghi M., 2018, S.1
[3] vgl. Burgwinkel D., 2016, S.5

Abbildung 2-5: Schematischer Aufbau einer Blockchain[1]



Welche Informationen nun genau in den einzelnen Blöcken enthalten sind und wie die Generierung der Blöcke stattfindet, unterscheidet sich teilweise erheblich zwischen den einzelnen Systemen. Sofern für den Einsatz im Product Life Cycle relevant, werden die Inhalte der abgebildeten Daten bei der Beschreibung der Use Cases in weiterer Folge konkret angeführt.

Transaktionen

Aufbauend auf den vorhergehenden Beschreibungen und Abgrenzungen können nun die eigentlichen Abläufe bei Transaktionen betrachtet werden. Der ursprüngliche Beweggrund hierfür war, wie bereits erwähnt, bei Bitcoin die Möglichkeit zur Transaktion von Wert, was somit die zentrale Funktion der Bitcoin-Blockchain darstellt. Neben der Transaktion von Wert können über die Blockchain wie bereits erwähnt beliebige Daten ausgetauscht und gespeichert werden. Darum ist das Konzept, wie Transaktionen auf der Blockchain durchgeführt werden, auch im Kontext des Product Life Cycle und der entsprechenden Use Cases von großer Bedeutung.

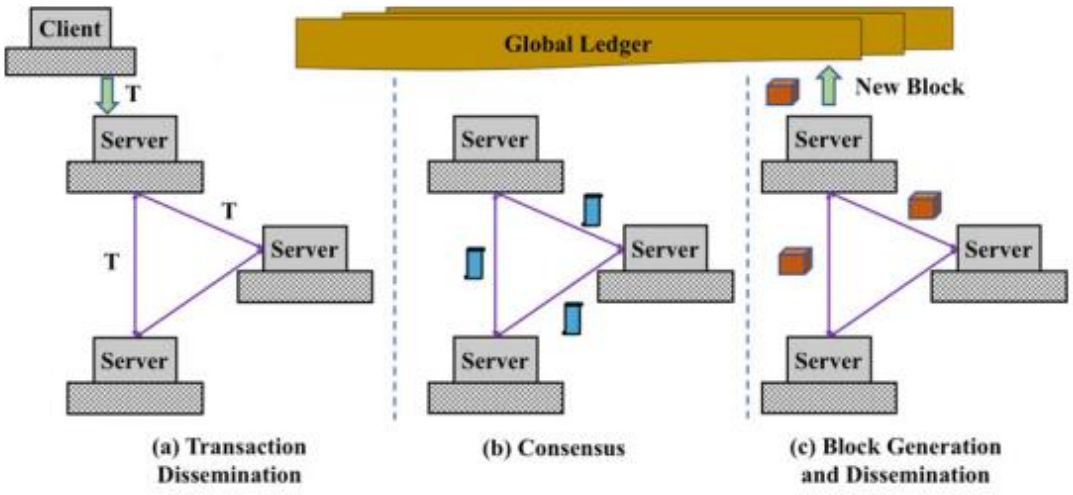
Antonopoulos schreibt dazu bereits über Bitcoin: „Everything else in bitcoin is designed to ensure that transactions can be created, propagated on the network, validated, and finally added to the global ledger of transactions (the blockchain). Transactions are data structures that encode the transfer of value between participants in the bitcoin system."[2]
Damit beschreibt der Autor bereits im Groben die grundsätzlichen Phasen die generisch bei den meisten bestehenden Blockchain-Systemen für die Durchführung von Transaktionen durchlaufen werden.

[1] Abb. 2-5 aus Burgwinkel D.,2016, S.5
[2] vgl. Antonopoulos A, 2015, S.109

Möglichst allgemein beschrieben, werden typische Blockchain Transaktionen nach der folgenden Sequenz durchgeführt, wie auch in Abbildung 2-6 zu sehen:[1,2]

- (a): Eine Anfrage für die Durchführung einer Transaktion wird von einem Client an einen der direkt an der Blockchain teilnehmenden Server (Entsprechen dem oben vorgestellten „Nodes“) gesendet[3]
  Der Server sendet die Anfrage an alle anderen teilnehmenden Server, welche die erhaltenen Transaktionsinformationen vorläufig speichern. (Diese Phase wird auch „transaction dissemination“ genannt)
- (b): Sobald alle Server die Anfrage erhalten haben, wird über einen Consensus-Mechanismus (siehe Kapitel „Consensus“) festgelegt, welcher Server den nächsten Block erstellt.
- (c): Dieser ausgewählte Server übernimmt dann den Schreibprozess, wobei meist mehrere Transaktionen zu einem Block zusammengefasst werden. Danach sendet er die Information zum neu erstellten Block an alle anderen Server wodurch der neue Block der Blockchain hinzugefügt wird. („Block Generation and Dissemination“)

Abbildung 2-6: Ablauf einer Transaktion[4]



[1] vgl. Gupta S. & Sadoghi M., 2018, S.3f
[2] vgl. Nakamoto S., 2008, S.3
[3] ANMERKUNG: in diesem Fall wird von zwei unterschiedlichen Arten von Teilnehmern in der Blockchain ausgegangen. Zum einen sogenannte Full-Nodes, hier als „Server“ bezeichnet, die direkt in der Blockchain teilnehmen, das dezentrale Netzwerk bilden und Transaktionen durchführen und verifizieren. Außerdem Lite-Nodes, hier als Client bezeichnet, die Transaktionen in Auftrag geben können und einen „Kontostand“ in der Blockchain besitzen, jedoch nicht an den Schreib- & Verifikationsprozessen teilnehmen und somit auch nicht die gesamte Blockchain lokal bei sich speichern müssen.
[4] Abb. 2-6 aus Gupta S. & Sadoghi M, 2018, S.3

In der Abbildung 2-6 ist auch besonders gut zu erkennen, wie ein Blockchain-Netzwerk als Ganzes arbeitet. So ist es zum einen möglich, das Netzwerk nur mit gleichgestellten Nodes zu realisieren. Eine andere spezielle Ausprägung eines Blockchain Netzwerks ist hier in Teil (a) der Abbildung zu sehen. Dabei sendet ein Client eine Transaktion an einen Server, der diese übernimmt und in die Blockchain einträgt. Dadurch muss der hier als Client bezeichnete Computer nicht selbst die Blockchain-Transaktion durchführen, kann aber trotzdem mit dem Netzwerk verbunden sein. Auf diese Weise lassen sich gegebenenfalls manche Vorteile der Blockchain Methodiken, mit machen Vorteilen des zentrale Client-Server Modells kombinieren. Üblicherweise werden in solchen Architekturen die hier als Server bezeichneten Computer als „Full"-Nodes bezeichnet und der hier als Client bezeichnete Computer als „Lite"-Node.

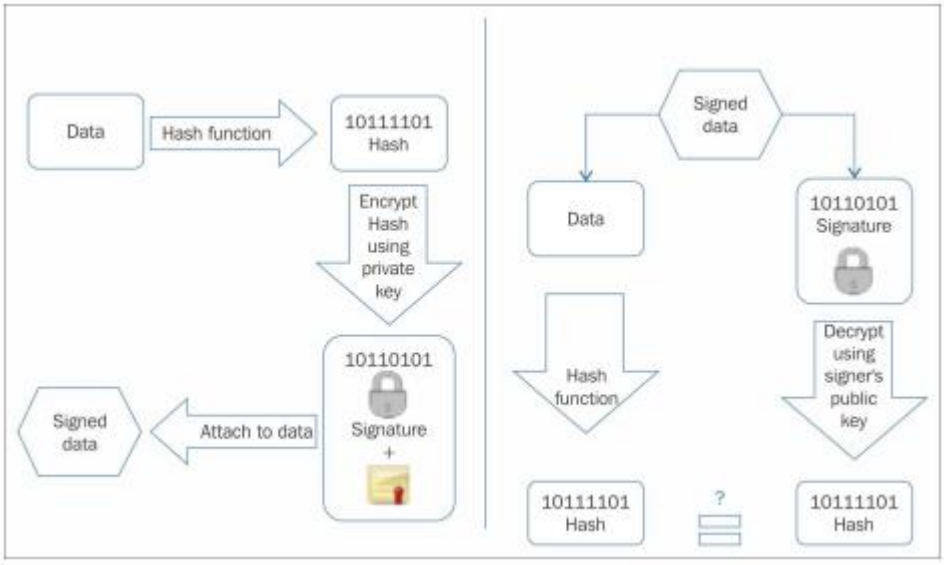
Signatur

Ein weiteres Element die die Sicherheit von Blockchain Systemen gewährleistet sind die eingesetzten Signaturen. Dadurch kann sichergestellt werden, dass die Transaktion valide ist und auch wirklich vom Sender so in Auftrag gegeben wurde. Hier wird die sogenannte „Public Key Encryption" verwendet oder auch „Asymmetrische Kryptografie" genannt.

Dabei ist zu erwähnen, dass diese Form der Verschlüsselung bereits seit Längerem in verschiedenen Protokollen (zB. SSH, OpenPGP, S/MIME and SSL/TLS) eingesetzt wird und dabei zur End-to-End Verschlüsselung vieler Übertragungen beiträgt, die über potenziell unsichere Kanäle geschickt werden.[1]

[1] vgl. https://searchsecurity.techtarget.com/definition/asymmetric-cryptography zuletzt gelesen am: 19.12.2018

Abbildung 2-7: Signatur[1]



In Abbildung 2-7 ist schematisch zu sehen, wie der Signatur-Prozess abläuft. Links zu sehen ist der Verschlüsselungsprozess des Absenders. Zuerst werden die zu übermittelnden Daten gehasht. Dieser Hash, oft auch „Digest“ genannt, wird dann unter Verwendung des Public Keys verschlüsselt, wodurch die eigentliche Signatur entsteht. Diese wird dann den zu übermittelnden Daten angehängt. Im Zusammenhang der Blockchain wird eben die Transaktion mit dem Private Key des Senders nach diesem Schema signiert.

Rechts zu sehen ist der Validierungsprozess des Empfängers. Dabei wird zum einen derselbe Hash-Algorithmus wie beim Absender auf die erhaltenen ursprünglichen Daten angewendet, wodurch der gleiche Hash als Output herauskommen muss, wie beim Absender. Außerdem wird die übermittelte Signatur mittels des erhaltenen Public Keys entschlüsselt mit einem weiteren Hash als Output. Wenn dieser Hash nicht dem Hash der ursprünglichen Daten entspricht, ist das ein Zeichen, dass die Daten in irgendeiner Form verändert wurden oder der Public Key nicht dem Private Key der Signatur entspricht.

Als Beispiel im Bitcoin-Netzwerk, veröffentlicht der aktuelle Bitcoin-Besitzer den Public Key und die Signatur an das gesamte Netzwerk. Durch den Signatur-Prozess kann jeder Teilnehmer im Netzwerk die Transaktion überprüfen, ohne dass der Besitzer den Private Key offenlegen muss.[2]

[1] Abb. 2-7 aus Bashir I.,2017, S.199
[2] vgl. Antonopoulos A., 2015, S.62

Über die gesamte Blockchain hinweg, kann man, im speziellen Fall von Bitcoin, dadurch außerdem die Besitzinformationen eines einzelnen Coins überprüfen und so sichergehen, dass der Absender auch wirklich im Besitz des Coins ist.[1]

Durch diesen Signatur-Mechanismus wird also im Endeffekt sichergestellt, dass die Daten auch wirklich vom Sender erstellt wurden, die Daten nicht abgeändert wurden und der Sender auch nicht abstreiten kann die Daten in der Form so geschickt zu haben.

Dementsprechend kann in Bezug auf Hashing und den digitalen Signaturen die Abgrenzung stattfinden:

Hashing trägt zur Sicherstellung bei, dass die Daten nicht veränderbar sind und dient als Instrument in manchen Consensus-Mechanismen wie zum Beispiel Proof of Work. (Siehe Kapitel „Consensus“) Digitale Signaturen hingegen ermöglichen eine Validierung von Transaktionen und Sicherstellung, dass nur derjenige mit der notwendigen Berechtigung die Transaktionen durchführen kann. Diese beiden Aspekte tragen also gemeinsam signifikant zur Sicherheit und Unveränderbarkeit der Blockchain bei.[2]

Consensus

Wie bereits mehrfach erwähnt, stellt die Sicherung der Vollständigkeit und Integrität der Daten auf jedem Node in einem verteilten System eine besondere Herausforderung dar. Besonders wenn es sich um ein Peer-to-Peer Netzwerk wie eine Blockchain handelt.

Hierfür wurden für die verschiedenen Blockchain Netzwerke mehrere Methoden entwickelt die alle unter dem Begriff „Consensus“ (deutsch: Konsens) zusammengefasst werden. Im Folgenden wird konkret auf den „Proof of Work“ Consensus Mechanismus der Bitcoin-Blockchain eingegangen. Dieser stellt im Rahmen der Blockchan-Technologie den ersten angewendeten Consensus-Mechanismus dar und bildet in gewisser Weise die Grundlage für die Entwicklung fortführender Consensus Mechanismen, auf die in weitere Folge ebenso eingegangen wird.[3] (Siehe Kapitel „Alternative Proofs“)

Im Allgemeinen handelt es sich bei einem Consensus-Mechanismus um einen Prozess, durch den sich verteilte Nodes auf einen gemeinsamen Status der geteilten Daten einigen. Dadurch kann sichergestellt werden, dass zB. im Fall von Bitcoin ein Coin nicht „zweimal ausgegeben wird“, ohne dass die Transaktionen von einer zentralen Autorität beobachtet und verifiziert werden müssen.[4]

---

[1] vgl. Nakamoto S., 2008, S.2

[2] https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ zuletzt gelesen am 19.02.2018

[3] ANMERKUNG: Wobei Consensus-Mechanismen bereits seit Jahrzehnten erforscht werden., wie etwa Paxos oder RAFT. Der Proof of Work Mechanismus ist nur der erste, der im Rahmen von Blockchain-Netzwerken verwendet wurde. Siehe Bashir, I, 2017, S.8f

[4] vgl. Nakamoto S., 2008, S.2

Dabei muss ein Consensus Mechanismus laut Bashir I., 2017 folgende Voraussetzungen erfüllen, um den gewünschten Nutzen zu bringen:[1]

- Übereinkommen: Alle ehrlichen Nodes einigen sich auf denselben Wert
- Abschluss: Alle ehrlichen Nodes schließen den Prozess ab und gelangen zu einer Entscheidung
- Gültigkeit: Alle ehrlichen Nodes einigen sich auf einen Wert, der im Laufe des Prozesses unverändert bleibt und exakt dem ursprünglich verkündeten Wert entspricht
- Fehlertoleranz: der Prozess muss auch dann funktionieren, wenn fehlerhafte oder bösartige Nodes beteiligt sind
- Integrität: Ein Node kann die jeweilige Entscheidung nur einmal im Laufe des Prozesses durchführen.

Der Proof of Work Mechanismus der Bitcoin Blockchain erfüllt diese Voraussetzungen nun indem er folgendermaßen durchgeführt wird:[2, 3]

Der Mechanismus wird explizit von speziellen Nodes ausgeführt, sogenannten „Minern“. Dabei wird die Rechenpower dieser Nodes genutzt, um den Consensus-Mechanismus durchzuführen. Diese Miner bekommen als Gegenleistung neuerstellte Bitcoins.

Der Ablauf den ein einzelner Miner durchläuft:[4,5,6]

- Der Mining-Node sammelt die publik gemachten Transaktionen und bündelt diese in einem Block.
- Der Node adaptiert einen Wert im Block, die sogenannte Nonce, so lange, bis der Hash für den neuen Block gewisse Kriterien erfüllt ist. Dieser gefundene Hash wird dann Target Hash genannt.
    - Bei Bitcoin ist das Kriterium eine gewisse Anzahl an Nullen, mit der der Hash-String beginnen muss. Die Anzahl der Nullen stellt die aktuelle Schwierigkeit des Proof of Work dar.[7] Im Allgemeineren steigt die Schwierigkeit mit der Anzahl der Nullen exponentiell, während zur Überprüfung nur ein einzelner Hash berechnet werden muss.
    - Bei der Findung der richtigen Nonce hat nur trial and error Sinn, da man durch keine mathematische Methodik abschätzen kann, welche Nonce die geforderte Anzahl an Nullen liefert. Diese Versuche sind sehr Rechenaufwändig bis man zufällig die richtige Nonce trifft. Die Prüfung aber, ist sehr schnell möglich, da man nur einen einzigen Hash bilden muss.
- Der erfolgreiche Miner schickt die gefundene Nonce und den Target Hash an alle anderen Miner, die die Eingaben prüfen.

---

[1] vgl. Bashir I, 2017, S.8f

[2] vgl. Antonopoulos A., 2015, S.174f

[3] vgl. https://blockchainhub.net/blog/blog/consensus-mechanisms-2/ zuletzt gelesen am: 18.12.2018

[4] vgl. Antonopoulos A., 2015, S.174

[5] vgl. Nakamoto S., 2008, S.3

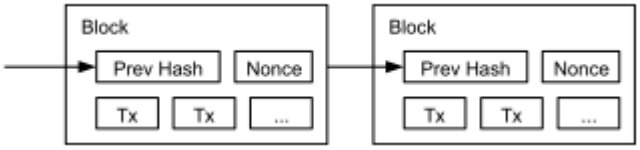
[6] vgl. http://ethdocs.org/en/latest/mining.html zuletzt gelesen am 18.12.2018

[7] ANMERKUNG: die Schwierigkeit des Proof of Work, also die notwendige Anzahl an Nullen die im Target Hash zu finden sind, wird im Fall von Bitcoin automatisch angepasst. Ziel dabei ist es, dass dadurch in etwa alle 10 Minuten ein Block gefunden wird. Siehe Unterkapitel: „Consensus“

  - Geprüft werden dabei sowohl Nonce & Target Hash als auch ob alle Transaktionen valid sind und kein Double Spending vorliegt (siehe: Kapitel „Transaktionen und Blöcke“ - Abschnitt „Signatur“)
- Die anderen Miner zeigen ihre Akzeptanz, indem sie den nächsten Block in der Blockchain berechnen und dabei den gerade gefundenen Target Hash als Vorgänger Hash verwenden.

In Abbildung 2-8 ist ein schematischer Aufbau der Blöcke in der Bitcoin-Blockchain zu sehen, wie er im Paper von Nakamoto zu finden ist.

Abbildung 2-8: Schematischer Aufbau der Bitcoin-Blockchain[1, 2]



Durch diese Methodik können somit Transaktionen ohne zentrale Stelle validiert und gezeichnet werden. Sie stellt dadurch einen dezentralen Sicherheits-Mechanismus dar, der einen Konsens in dem Peer-to-Peer Netzwerk erst möglich macht.[3]

Wie die Problematik des Consensus Mechanismus in anderen Blockchains gelöst wird, wird in Kapitel „Alternative Proofs“ beschrieben. Dies ist insofern besonders wichtig, da in vielen Use Cases, besonders im industriellen Kontext, natürlich keine Miner oder finanzielle Vorteile für die Miner zur Verfügung stehen und darum ein anderer Ansatz gewählt werden muss.

Unterscheidung zwischen Private Blockchains und Public Blockchains

Ein weiterer Aspekt zur Beschreibung der Anwendungsmöglichkeiten der Blockchain Technologie, insbesondere im Zusammenhang mit der Nutzung im industriellen Umfeld, stellt die Unterscheidung zwischen Private Blockchain und Public Blockchain dar.

Um Public Blockchains handelt es sich, wenn es keine Einschränkungen gibt, wer an der Blockchain teilnehmen kann und darf und für wen die beinhaltenden Daten einsehbar sind. Dabei kann jede beliebige Person den Open Source Code downloaden, einen Node betreiben und am Consensus-Protokoll teilnehmen. Diese Form bietet somit größtmögliche Transparenz und Dezentralisierung.[4]

[1] Abb. 2-8 aus Nakamoto S., 2008, S.3
[2] ANMERKGUN: Tx = Transactions
[3] vgl. Antonopoulos A., 2015, S.174
[4] vgl. Voshmgir S. & Kalinov V., 2017, S.14

Bei Private Blockchains wird im Gegensatz dazu der Zugang zum Netzwerk (je nachdem Lese- oder Schreibberechtigung) reglementiert und steht nur einer ausgewählten Liste von Teilnehmern zur Verfügung. Diese Art von Blockchain ist tendenziell innerhalb von Organisationen zu finden, die ein abgeschlossenes System betreiben, aber gleichzeitig gewisse Vorteile eines Blockchain Netzwerks nutzen wollen. Dabei kann zB. auch nur die Schreibberechtigung innerhalb der Organisation gehalten werden, die Leseberechtigung aber öffentlich zugänglich sein.[1]

Als Zwischenstufe können Consortium Blockchains angesehen werden. Von diesen wird gesprochen, wenn die In-Auftrag-Gabe von Transaktionen, sowie das Senden und erhalten von Daten frei zugänglich ist, der Consensus-Mechanismus und die Verifikation von Transaktionen aber nur einer bestimmten Gruppe unterliegt. Somit handelt es sich dabei um eine Mischform zwischen Privaten und Public Blockchains, welche je nach Ausprägung jeweils die speziellen Vorteile nutzen kann.[2]

In Abbildung 2-9 sind die sich daraus ergebenden Unterschiede zwischen Public und private Blockchains angeführt.[3]

Abbildung 2-9: Vergleich Public und Private Blockchain[4]

	PUBLIC	PRIVATE
Access	Open read/write	Permissioned read and/or write
Speed	Slower	Faster
Security	Proof of Work Proof of Stake Other consensus Mechanisms	Pre-approved participants
Identity	Anonymous Pseudonymous	Know identities
Asset	Native Asset	Any Asset

Einen besonders wichtigen Punkt stellt hier der „Speed“ Aspekt dar. Dieser, der auch stark im Zusammenhang mit dem Thema Skalierung steht, stellt abgesehen von einer allgemeinen Blockchain-Architektur ein wichtiges Kriterium dar, ob eine Blockchain im industriellen Umfeld

[1] vgl. Voshmgir S. & Kalinov V., 2017, S.14
[2] vgl. Voshmgir S. & Kalinov V., 2017, S.14
[3] ANMERKGUN: im Vergleich dazu können Consortium Blockchains nicht so einfach abgegrenzt werden, da es hier sehr auf die konkrete Ausprägung ankommt. Bezüglich der Vor- und Nachteile dieser Art von Blockchain müssen tendenziell die einzelnen Lösungen im Speziellen betrachtet werden.
[4] Abb. 2-9 aus Voshmgir S. & Kalinov V., 2017, S.15

überhaupt einsetzbar ist. Insbesondere, da Public Blockchains wie Bitcoin im Vergleich zu den derzeit zum Großteil eingesetzten Systemen eine vergleichsweise geringe Anzahl an Transaktionen schaffen und diese zudem über den Proof of Work Mechanismus verhältnismäßig aufwändig zu betreiben sind. Zu erwähnen ist natürlich hierbei, dass es auch bei Public Blockchains starke Bestrebungen gibt, diese besser skalierbar zu machen.[1]

In jenen Fällen, in denen jedoch größtmögliche Transparenz und die Möglichkeit für ein Agieren im Netzwerk, ohne Vertrauen in alle Teilnehmer, notwendig ist und man dabei längere Transaktionszeiten und tendenziell höhere Kosten in Kauf nehmen kann, ist eine Public Blockchain dann eventuell doch von höherem Nutzen. Darum gilt es immer von Fall zu Fall zu unterscheiden und es ist keine allgemein gültige Aussage möglich.[2]

2.2.3 Spezielle Ausprägungen der Blockchain

Im vorherigen Kapitel wurden die Grundlagen erläutert, die in verschiedenen Ausprägungen in Blockchain-Konzepten zu finden sind. Darüber hinaus gibt es jedoch auch Entwicklungen und Lösungen für Anwendungsfälle, die nur in speziellen Situationen oder entsprechendem Bedarf relevant sind. Um diese bei der Betrachtung in Bezug auf die Anwendbarkeit im Product Life Cycle miteinbeziehen zu können, werden sie auch hier angeführt.

Smart Contracts

Bei Smart Contracts handelt es sich um eine Funktionalität, die über die Basisfunktionalitäten einer Blockchain hinausgeht. Dabei spricht man, möglichst generisch beschrieben, von auf der Blockchain gespeicherten ausführbaren Code in Form von Programmen oder Skripten. Also kleine Anwendungen, die über das Blockchain-Netzwerk verteilt werden, wobei die Inputs innerhalb von Transaktionen zu durch die Smart Contracts definierte Outputs führen. Das Hyperledger Netzwerk, nennt solchen Code auch „Chain Code“. Dabei wird der Code ebenso dezentral von allen Nodes im Netzwerk ausgeführt. Durch diese Redundanz entsteht der Vorteil, dass wenn die Mehrheit der Nodes zu dem gleichen Ergebnis kommen, kann diesem Output vertraut werden und die darauffolgende Aktion sicher ausgeführt werden.[3]

Die dabei verwendeten Programmiersprachen beginnen bei relativ einfachen und systemnahen Varianten wie die sogenannte „Scripting“-Sprache auf der Bitcoin-Blockchain. Das für Smart Contract vermutlich bekannteste Netzwerk ist die Ethereum Blockchain, welche die Programmiersprache „Solidity“ verwendet. Diese bietet bereits höherwertige Programmkonstrukte und ist teilweise mit JavaScript vergleichbar.[4]

---

[1] vgl. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ zuletzt gelesen am 20.12.2018
[2] vgl. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ zuletzt gelesen am 20.12.2018
[3] vgl. Ploom T., 2016, S.128ff
[4] vgl. Ploom T., 2016, S.128ff

In Bezug auf Ethereum wird beschrieben, dass somit Nodes die als „Contract Accounts“ fungieren, die Voraussetzungen erfüllen müssen, untereinander Nachrichten auszutauschen und Turing-vollständige Berechnungen durchzuführen. Dabei werden die Contracts im Fall von Ethereum in Solidity geschrieben und dann in ein spezielles binär-Format kompiliert, um auf die Blockchain hochgeladen zu werden.[1]

Durch diesen Aspekt erweitert sich die Funktionalität eines Blockchain-Systems über simple Transaktionen von Daten hinaus. Dadurch können Vereinbarungen zwischen mehreren Parteien auf einer Blockchain gespeichert werden, welche unter bestimmten Bedingungen automatisch, ohne Zeitverlust und ohne notwendige Verifikation einer zwischengeschalteten Autorität ausgeführt werden.[2]

Ein einfaches Beispiel im Zusammenhang mit dem Product Life Cycle wäre die automatische Durchführung einer Zahlung bei Nutzung einer Maschine die ähnlich dem SaaS-Prinzip[3] von der Herstellerfirma zur Verfügung gestellt wird, aber nicht in den Besitz der Nutzer übergeht. Aufgrund dieses Zusatznutzens, der die Anwendungsmöglichkeit innerhalb eines Blockchain-Systems erheblich erhöht, spricht Swan M. in ihrem Buch bei Blockchain-Netzwerken mit der Möglichkeit zum Einsatz von Smart Contracts auch von Blockchain 2.0. Im Gegensatz dazu stellen einfache Kryptowährung-Netzwerke Blockchains 1.0 dar.[4]

Alternative Proofs

Durch den Peer-to-Peer Aufbau von Blockchain Netzwerken ist wie in Kapitel „Consensus“ beschrieben ein Mechanismus notwendig, durch den alle Nodes sich auf einen Stand der Daten, also eine gemeinsame Wahrheit, einigen müssen, damit das System funktioniert. Neben dem bereits erwähnten Proof of Work, gibt es noch andere Mechanismen, die diese Funktion erfüllen können. Einige davon sind bereits im Einsatz, andere befinden sich noch in der Entwicklung.

Allen hier vorgestellten Consensus-Mechanismen gemein ist jedoch, dass sie eine Methodik liefern, welcher Node den nächsten Block vorschlägt. Die Überprüfung der Richtigkeit der Daten durch alle anderen Nodes erfolgt unabhängig von der Art des Consensus-Mechanismus. Prinzipiell werden im Folgenden auch nur ein paar Consensus-Mechanismen vorgestellt, um zu verdeutlichen, dass es zahlreiche Varianten gibt. Es soll also erwähnt werden, dass es viele weiter Consensus-Mechanismen gibt, auf die hier nicht eingegangen wird.

Proof of Stake (PoS)

Unter Proof of Stake versteht man mehrere Methoden zur Konsens-Findung, die alle auf der Idee aufbauen, dass die Nodes mit dem größten Anteil an Coins oder Tokens in der Blockchain

[1] vgl. http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html zuletzt gelesen am 20.12.2018
[2] vgl. Swan M., 2015, S.16ff
[3] ANMERKUNG: SaaS = Software as a Service
[4] vgl. Swan M., 2015, S.1

am Wahrscheinlichsten mit der Erstellung oder Validierung der neuen Blöcke beauftragt werden. Dabei „investieren“ die Nodes pro Block einen gewissen Anteil ihres Vermögens. Sollte der Block dann aber aufgrund der Ablehnung der Verifikation abgelehnt werden, würde der Node den investierten Betrag verlieren, was die Wahrscheinlichkeit eins böswilligen Verhaltens reduziert. Dabei gibt es auch Kombinationen mit Proof of Work, zufälliger Auswahl der Blöcke mittels Zufallsalgorithmen, die vergangene Zeit, seitdem ein Coin oder Token im Besitz des Nodes ist, oder in Kombination mit einem Reputations-System in dem von allen Nodes ein Pool von vertrauenswürdigen Nodes gewählt werden, die für die Block-Erstellung zuständig sind („Delegated Proof of Stake“).[1, 2, 3]

Diese Abwendung von der Nutzung von CPU-/GPU-Power hin zu einer anderen Methodik, macht Systeme mit Proof of Stake kostengünstiger und leichter skalierbar als Proof of Work Systeme, was prinzipiell ein signifikanter Vorteil für die Verwendung dieses Consensus-Mechanismus im industriellen Umfeld darstellt. Zum derzeitigen Wissensstand fehlen jedoch noch entsprechend ausreichende Erfahrungswerte, ob sich diese Vorteile auch in der Praxis auf lange Sicht realisieren lassen.

Proof of Elapsed Time

Proof of Elapsed Time hat eine möglichst simple Zufallsauswahl des nächsten blockerstellenden Nodes als Ziel. Dabei generieren die teilnehmenden Nodes eine zufällige Wartezeit pro Block. Derjenige Node mit der geringsten Wartezeit erstellt dann den nächsten Block.[4]

Dieser Consensus-Mechanismus ist ein gutes Beispiel dafür, dass nicht notwendigerweise ein finanzieller oder anderweitiger Anreiz für die teilnehmenden Nodes bestehen muss, um den blockerstellenden Node zu bestimmen. Natürlich haben alle Mechanismen konkrete Vor- und Nachteile. In Bezug auf Einfachheit und Skalierbarkeit stellt z.B. Proof of Elapsed Time eventuell eine gute Alternative zum weit verbreiteten Proof of Work dar.

Proof of Importance

Bei Nutzung dieses Mechanismus werden den einzelnen Nodes Werte für „Wichtigkeit“ (=Importance) zugeschrieben. Dieser Wert wird durch den Anteil am System im Sinne von Währungseinheiten, sowie die Aktivität im System, als auch das Verhalten selbst definiert. Je höher der Wichtigkeits-Wert desto wahrscheinlicher kommt ein Node zur Blockerstellung.[5, 6]

---

[1] vgl. https://blockchainhub.net/blog/blog/consensus-mechanisms-2/
[2] vgl. Voshmgir S. & Kalinov V., 2017, S.19
[3] vgl. Burgwinkel D., 2016, S. 143
[4] vgl. https://blockchainhub.net/blog/blog/consensus-mechanisms-2/
[5] vgl. Bashir I., 2017, S.36f
[6] vgl. NEM: Technical Reference, 2015, S.26ff

Proof of Authority

Bei Proof of Authority müssen die teilnehmenden Nodes innerhalb des Netzwerks identifizierbar sein und diese Identität muss überprüfbar sein. Durch die Offenlegung der Identität dürfen die Nodes an der Erstellung der neuen Blöcke teilnehmen und werden hier ebenfalls mit einem Reputationswert versehen. Die Identität und der Reputationswert bestimmen dann in weitere Folge die Wahrscheinlichkeit einen Block zu erstellen.[1]

Diese Abkehr von der möglichst hohen Anonymität hin zu öffentlich jederzeit einsehbaren und gewissen Identitäten zuordenbaren Aktionen kann je nach Anwendungsfall natürlich ein Vor- oder ein Nachteil sein und muss von Fall zu Fall beurteilt werden.

Delegated Byzantine Fault Tolerance

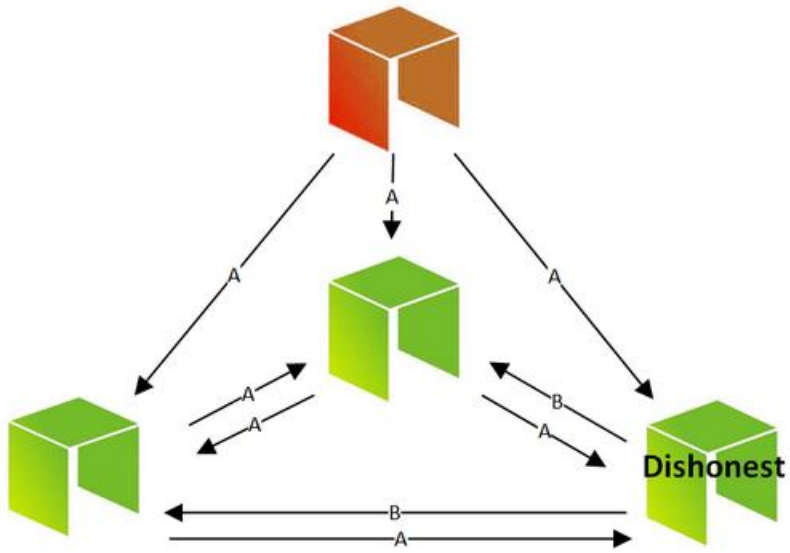
Dieser Consensus-Algorithmus baut auf dem Prinzip des „Byzantine Fault“[2] auf, der im Kontext von Blockchain einen unehrlichen Node beschreibt.

Das Prinzip des Delegated Byzantine Fault Tolerance Mechanismus ist, dass ein Node zufällig ausgewählt wird, um den nächsten Block zu schreiben. Die entsprechenden Informationen werden von diesem Node an die anderen Nodes ausgesendet. Bei einer Bestätigung von mehr als 2/3 der Nodes (66,666%) wird der Block angenommen. Bei weniger als 66% läuft der Algorithmus von vorne. Ebenso wird im Zuge des Prozesses der schreibende Node von den empfangenden Nodes überprüft, da auch dieser bösartig handeln könnte.[3, 4]

Abbildung 2-10 zeigt schematisch einen Consensus-Prozess mit nur 4 Teilnehmern. Rot dargestellt der Node der den neuen Block schreibt, grün die Nodes die die Verifizierung durchführen. Sobald zwei Verifikations-Nodes (=2/3 der Verifikations-Nodes) ehrlich handeln, ist das bösartige Verhalten des als „Dishonest“ gekennzeichneten Node erkennbar. Dieses Prinzip lässt sich beliebig hoch aufskalieren.

[1] vgl. https://blockchainhub.net/blog/blog/consensus-mechanisms-2/ zuletzt gelesen am 21.12.2018
[2] ANMERKUNG: für eine detaillierte Beschreibung des Byzantine Fault“ siehe: https://github.com/neo-project/docs/blob/master/en-us/basic/consensus/whitepaper.md
[3] vgl. https://docs.neo.org/en-us/basic/consensus/whitepaper.html zuletzt gelesen am 03.01.2019
[4] vgl. https://docs.neo.org/en-us/basic/consensus/consensus.html zuletzt gelesen am 03.01.2019

Abbildung 2-10: Delegated Byzantine Fault Tolerance Consensus Mechanismus[1]



Im Zuge der Überprüfungen kann auch durch Beobachtung der Nodes erkannt werden wie oft ein Node eine fehlerhafte Angabe im Vergleich zu den >2/3 der anderen Nodes macht. Dadurch könnten tendenziell bösartige oder einfach nur fehlerhafte Nodes ausgemacht werden.

Fork

Aufgrund der Mechanismen in der Consensus-Findung gewisser Blockchains kann es dazu kommen, dass kurzzeitig verschiedene Versionen der Blockchain zwischen den Nodes existieren. Dies passiert vor allem dann, wenn zwei Nodes, die an einem Proof of Work teilnehmen, nahezu zur gleichen Zeit den Target Hash finden. Um diesen unerwünschten Status abzuwenden, wird bei bestehenden Blockchain-Systemen wie etwa Bitcoin die längste Blockchain als relevante Blockchain ausgewählt, in die als Schlussfolgerung die meiste Rechenleistung geflossen ist. Dadurch konvergiert das Netzwerk immer zu einem gemeinsamen Status, auch wenn immer wieder kurzfristig mehrere Versionen der Blockchain existieren.[2, 3]

Im Zusammenhang mit dem Begriff Fork ist auch zu erwähnen, dass nicht nur der oben beschriebene Fall als Fork bezeichnet wird. Ebenso Änderungen in den Consensus-Regeln, die eine Teilung der Blockchain zwischen jenen die die Regeln akzeptieren und jene die es nicht tun zur Folge hat sowie Erstellung einer neuen Blockchain aufbauend auf einer existierenden werden im Sprachgebrauch als Fork bezeichnet.[4]

---

[1] Abb. 2-10 aus https://docs.neo.org/en-us/basic/consensus/consensus.html zuletzt gelesen am 18.12.2018
[2] vgl. Antonopoulos A., 2015, S.199f
[3] ANMERKUNG: im Fall der Bitcoin Blockchain wird die für jeden Block festgesetzte Schwierigkeit im Block selbst mitgespeichert. Dadurch kann die kumulierte Rechenleistung einfach berechnet werden. (Siehe: Antonopoulos A., 2015, S.199)
[4] vgl. https://bitcoin.org/en/glossary/fork zuletzt gelesen am 21.12.2018

Sidechain oder Childchain

Bei sogenannten Sidechains oder Childchains handelt es sich Blockchains, die in Erweiterung einer „Masterchain“ existieren. Dabei bleibt die ursprüngliche Blockchain nicht wie bei einem Fork komplett erhalten. Die Sidechain fungiert in dem Fall als zusätzliche Funktionalität. Meistens wird eine Sidechain dazu genutzt spezielle Aufgaben zu übernehmen, wobei es von Vorteil ist, diese nicht auf der Masterchain auszuführen. Zum Beispiel handelt es sich dabei etwa um Testläufe von Softwareupdates. Diese Herangehensweise ist ein weiterer Versuch die Skalierbarkeit vieler Blockchain-Netzwerke zu erhöhen.[1, 2]

Primär werden diese Sidechains derzeit in Kryptowährung-Systemen verwendet. Es ist aber vorstellbar, dass eine Sidechain-Konstruktion im industriellen Kontext etwa dazu genutzt werden kann, dass spezielle Aufgaben wie Berechnungen oder nicht veröffentlichbare Daten auf einer Sidechain abgehandelt werden und nur ausgewählte Daten über die Verbindung zur Masterchain dann allen öffentlichen Teilnehmern verfügbar gemacht werden.

Cross Ledger / Cross Chain

Hierbei handelt es sich um ein recht neues Forschungsfeld im Rahmen der Blockchain-Technologie. Grundgedanke ist die Verbindung bzw. die Übertragung von Daten zwischen zwei Unabhängigen Blockchain-Netzwerken (= zwei unterschiedlichen Ledgern). Dies ist natürlich besonders von Bedeutung, sobald man sich mit Consortium Blockchains beschäftigt oder einen Use Case mit mehreren Blockchain-Netzwerken hat.[3]

Eines der einfachsten Beispiele stellt sicherlich eine Cross-Chain Transaktion zwischen zwei Kryptowährungen dar. Etwa von Bitcoin auf Ether. Große Anwendungsvielfalt dürfte sich aber bei anderen Anwendungen ergeben.

Besonders in Zukunft, wenn verschiedene Blockchain-Netzwerke verschiedene Lösungen für gewisse Abläufe bieten, aber keine Gesamtlösung für den aktuellen persönlichen Bedarf. Dann wird es notwendig sein, die verschiedenen Systeme zu verbinden und Datenaustausch möglich zu machen.

Derzeitige sich in der Entwicklung befindliche Lösungen sind Notary Schemes, Sidechains/Relays, Hash-Locking und Distributed Private Key Control.[4] (siehe Deng et al., 2018, S.145f)

[1] vgl. https://thenextweb.com/hardfork/2018/12/11/blockchain-sidechains-explained-basics/ zuletzt gelesen am 16.12.2018
[2] vgl. https://hackernoon.com/what-are-sidechains-1c45ea2daf3 zuletzt gelesen am 16.12.2018
[3] vgl. Deng et al., 2018, S.144ff
[4] vgl. Deng et al., 2018, S. 145f

Decentralized Application (DApp), Decentralized Autonomous Organization (DAO) & Decentralized Autonomous Corporations (DAC)

Bei den Begriffen DApp, DAO und DAC handelt es sich um Wortschöpfungen, die im Vergleich zu einfachen Blockchain-Systemen eine hohe Komplexität aufweisen. Dabei werden automatisierte Smart Contracts, vorprogrammierte Prozesse und erweiterte Funktionalitäten genutzt, um spezifische Aufgaben zu erfüllen, also einen Schritt weiter zu gehen als das einfache Ausführen von Transaktionen. Je nach Definition stellt bereits das Ausführen von Smart Contracts auf einer Blockchain eine DApp dar.[1]

Einige Beispiele für spezielle Blockchain Anwendungen die als DApps zu verstehen sind:[2]

- OpenBazar – dezentrales Willhaben
- LaZooz – dezentrales Uber
- Twister – dezentrales Twitter
- Bitmes sage – dezentralisierter Nachrichtendienst
- Stori – dezentralisierter Datenspeicher

Oracle

In Bezug auf die Blockchain-Technologie bezeichnet Oracle eine Quelle oder Schnittstelle von Daten und Informationen von außerhalb des Blockchain-Netzwerks. Besonders im Zusammenhang mit Smart Contracts sind diese Quellen von großer Bedeutung, da der im Smart Contract gespeicherter Code oft durch solche externen Informationen getriggert wird. So sicher die Blockchain somit auch ist, wenn die Information von Außerhalb fehlerhaft oder bösartig ist, kommt es zu falschen Smart Contract Ausführungen. Darum stellt eine sicherere und wahrheitsgetreue Informationsbereitstellung das wichtigste Kriterium für ein Oracle dar.[3]

Zu unterscheiden ist hier auch zwischen Inbound und Outbound Oracles, die beide Schnittstellen von der Blockchain zur externen Welt darstellen. Wobei Inbound Oracles jedoch Daten von außerhalb an die Blockchain liefern, haben Outbound Oracles die Funktion die Output-Daten von Smart Contracts an die Außenwelt zu übermitteln.[4]

Als Beispiel für ein Outbound Oracle führen Voshmgir S. & Kalinov V.,2017 ein Smart Lock an. Dieses würde eine eigene Adresse auf einer Blockchain besitzen. Sobald nun eine Zahlung auf diese Adresse eingeht, würde durch einen Smart Contract die Öffnung des Schlosses ausgelöst und mittels einem Outbound Oracle an das Smart Lock in der Realität geschickt.

Eine Möglichkeit, um die Sicherheit bezüglich Wahrheitsgehaltes von durch Oracles gelieferte Informationen zu erhöhen, stellen dezentralisierte Oracles oder Consensus Based Oracles dar. Dabei werden mehrere Oracles genutzt, um durch ein dezentrales Netzwerk die Informationen

[1] vgl. Swan M., 2015, S.23f
[2] vgl. Swan M., 2015, S.23f
[3] vgl. Voshmgir S. & Kalinov V., 2017, S.28f
[4] vgl. Voshmgir S. & Kalinov V., 2017, S. 28

zu sammeln wobei diese innerhalb des Netzwerks überprüft werden bevor sie an das Blockchain-Netzwerk weitergegeben werden.[1, 2]

Oder aber die Informationsquelle der Oracles ist selbst wieder eine Blockchain die die Authentizität der Daten gewährleistet und diese Daten dann für andere Blockchains über spezielle Oracles verfügbar macht.[3]

2.2.4 Kryptowährungen und finanzbezogene Aspekte der Blockchain-Technologie

Allgemein ist hier nochmal zu erwähnen, dass der Fokus dieser Arbeit wie bereits erwähnt im Speziellen auf den Anwendungsmöglichkeiten in einem industriellen Umfeld entlang des Product Life Cycle liegt. Nichts desto trotz sollen hier auch kurz die Begriffe der Blockchain Technologie erwähnt werden, die speziell im Bereich des Finanzmarktes bzw. in der Transaktion von finanziellen Mitteln ihre Anwendung finden, um hier die Abgrenzung zu schaffen.

Da bisher im Rahmen des Auftauchens der Blockchain-Technologie besonders die Aspekte von Finanz- & Wert-Transaktionen im Fokus standen, wurde in diesem Bereich bereits verhältnismäßig viel Forschungs- und Entwicklungsarbeit betrieben. Dem gegenüber stehen relativ wenige Quellen und Projekte im industriellen Umfeld. Für eine weitere Beschäftigung mit diesem speziellen Themengebiet der Kryptowährungen und finanzbezogenen Aspekte sei nochmal explizit auf die Quellen Antonopoulos A., 2015, Masterin Bitcoin sowie die Paper: Risius M. & Spohrer K., 2017, „A Blockchain Research Framework“ und Johansen S., 2016, „A Comprehensive Literature Review on the Blockchain Technology as an Technological Enabler for Innovation” verwiesen. Diese beschäftigen sich eingehend mit den verfügbaren Quellen in Bezug auf das Thema Finanzen.

Wallet

Der oft verwendete Begriff Wallet bezeichnet meist schlicht einen Teil der Client-Software, die den Zugang zur Blockchain und somit die Konten verwaltet. Darum handelt es sich dabei explizit nicht um den Account selbst oder die Adresse. Ebenfalls stellt die Wallet keine Darstellung der Identität eines Nutzers dar.[4,5]

---

[1] vgl. Bashir I., 2017., S.352f
[2] vgl. Voshmgir S. & Kalinov V., 2017, S.28
[3] vgl. Bashir I., 2017, S.351
[4] vgl. Rosenberger P., 2018, S.23
[5] ANMERKUNG: zusätzlich zu den erwähnten Client-Wallets existieren außerdem noch Versionen in Form von Hardware-Wallets, Mobile Wallets und Paper Wallets. Informationen zu diesen speziellen Wallets sind zu finden in weiterführenden Quellen wie: Rosenberger P., 2018, S.22ff

Kryptowährungen

Dabei handelt es sich um einen Sammelbegriff für Einheiten in einem Blockchain-System mit denen Wert übertragen werden kann, wobei Swan M., 2015, S.70 es explizit so formuliert: „“a unit of value that can be earned and used in a certain economic system.“, was eine allgemeingütliche Definition aller Kryptowährungen darstellt, selbst wenn diese keinen finanziellen Wert im Sinne von eine Umtauschbarkeit in stattliche Währungen besitzen.
Diesen Wert bestimmt je nachdem der Ersteller oder der freie Markt. Irreführend dabei ist die Tatsache, dass Kryptowährungen oftmals nicht nur die Werteinheit selbst, sondern auch das Protokoll bzw. die Software bezeichnet wird, die die Transaktionen durchführt.[1]
Ethereum unterscheidet hier im Speziellen zwischen der Blockchain bzw. dem System unter dem Namen „Ethereum“ und der Währung unter dem Namen „Ether“.[2]

Exchanges und Börsen

Bei Exchanges und Börsen handelt es sich um Handelsplätze für Kryptowährungen. Also stellen diese Organisationen keine Blockchains-Netzwerke dar, sondern um Plattformen auf denen Nutzer Kryptowährungen gegeneinander oder gegen FIAT-Geld tauschen können.

Unterschied Coin oder Token

In Bezug auf die Benennung der Werteinheit innerhalb einer Blockchain werden die Begriffe Coin und Token verwendet. Diese Bezeichnungen stellen jedoch tendenziell unterschiedliche Konzepte dar.

Coins bezeichnen Blockchain-immanente Elemente, die in der Funktion der Blockchain selbst verankert sind. Die Blockchain die einen Coin verwendet benötigt diese Einheit um ihr Protokoll überhaut durchführen zu können. Beispiele hierfür sind Bitcoin und Ethereum.[3]

Token hingegen bezeichnet Elemente, die zwar Wert besitzen können, jedoch nicht notwendig sind, um die Blockchain per se zu betreiben. Sie sind also nicht notwendigerweise ins Protokoll des Blockchain-Systems eingebunden. Wobei dies aber natürlich möglich ist. Diese Tokens werden auch nicht im Zuge des Consensus-Mechanismus mittels Mining erstellt, sondern von einer autorisierten Person erzeugt.[4]
In der Ethereum Blockchain zum Beispiel existiert der Blockchain-immanente Coin „Ether“ der für die Funktion der Blockchain notwendig ist. Zusätzlich können aber unter Nutzung der Ethereum Blockchain Token erstellt werden die eine gewisse Funktionalität erfüllen und von einer Person zur anderen übertragen werden können.[5]

---

[1] vgl. Swan M., 2015, S.1
[2] vgl. https://www.ethereum.org/ether zuletzt gelesen am 12.12.2018
[3] vgl. Voelkel O., 2017, S.103f
[4] vgl. Voelkel O., 2017, S.104
[5] vgl. Voelkel O., 2017, S.104

Entgegen dem allgemeinen Irrglauben ist aber nicht für jedes Blockchain-System ein Coin notwendig. Es gibt auch Netzwerke, die die Blockchain-Kriterien erfüllen und auf andere Weise funktionieren, wie diverse Blockchains des Hyperledger Kollektivs (Siehe Kapitel „Technische Besonderheiten ausgewählter Blockchain-Netzwerke“)

2.2.5 Allgemeine Definitionen der Blockchain-Technologie

Aufbauend auf den umfangreichen Teil an Begriffsdefinitionen und Beschreibungen der einzelnen Aspekte in den vorherigen Kapiteln, wird nun der Versuch unternommen eine Abgrenzung zu schaffen, wann nun ein System als „Blockchain“ bezeichnet werden kann. Insbesondere, da es natürlich leicht sein kann, dass man viele Use Cases eigentlich mit einem herkömmlichen Peer-to-Peer Netzwerk lösen kann und man dabei dann fälschlicherweise von einer Blockchain spricht. Wie bereits auch erwähnt, hat sich für die Blockchain-Technologie noch keine allgemeingültige Definition etabliert und es gibt oft signifikanten Unterschiede wie eine Blockchain beschreiben wird.

Vereinzelt sind aber auch in wissenschaftlichen, peer-reviewed Arbeiten Definitionen zu finden. So schreiben Seebacher S. & Schüritz R. in ihrem Paper „Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review” (2017):

“A blockchain is a distributed database, which is shared among and agreed upon a peer-to-peer network. It consists of a linked sequence of blocks, holding timestamped transactions that are secured by public-key cryptography and verified by the network community. Once an element is appended to the blockchain, it cannot be altered, turning a blockchain into an immutable record of past activity.” (vgl. Seebacher S. & Schüritz R., 2017, S.14)

Eine weitere umfangreiche Definition lässt sich in „BlockChain Technology: Beyond Bitcoin“ (2015) von Crosby M. et al. finden:

“A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.” (vgl. Crosby M. et al., 2015, S.3)

Ebenso versucht Viktor Buterin, der Gründer von Ethereum, 2014 eine allgemeine Definition der Blockchain zu liefern:

„The blockchain is a distributed ledger technology in the form of a distributed transactional database, secured by cryptography, and governed by a consensus mechanism. A blockchain is essentially a record of digital events. However, it is not ‘‘just a record,’’ since it can also contain so-called smart contracts, which are programs stored on the blockchain that run as implemented without any risk of downtime, censorship, or fraud.” (vgl. Beck R. et al., 2017, S.381)

Aus diesen Beschreibungen wird ersichtlich, dass es nicht die „eine“ Blockchain und auch nicht die „eine“ Definition von Blockchain-Technologie gibt. Vielmehr muss ein System gewisse Eigenschaften besitzen, um als Blockchain, so wie sich der Begriff in den letzten Jahren etabliert hat, bezeichnet werden zu können.

Dementsprechend wird im Rahmen dieser Arbeit nun ein Blockchain-System durch folgende Eigenschaften definiert:[1]

- Peer-to-Peer Netzwerk dargestellt durch einen verteilten Ledger
- Sammlung von Daten-Paketen zu Blöcken und Aneinanderreihung dieser Blöcke zu einer Blockchain die die nachträgliche Änderung unmöglich macht
- Consensus-Mechanismus, der sicherstellt, dass sich alle Teilnehmer auf die gleiche Daten-Wahrheit einigen
- Kryptografische Mechanismen (Hashing, Signatures) die die Sicherheit und Validierbarkeit der Transaktionen gewährleisten.

Somit müssen im weiteren Verlauf der Arbeit Netzwerke dieser Definition genügen, um tatsächlich von einer Blockchain-Lösung sprechen zu können.

2.3 Technische Besonderheiten ausgewählter Blockchain-Netzwerke

Bevor in weitere Folge auf konkrete, bereits bestehende Use Cases eingegangen wird, werden hier eine Reihe ausgewählter Blockchain-Lösungen vorgestellt. Jede dieser Lösungen wurde für einen bestimmten Zweck erstellt und durch die Unterschiedlichkeit der verschiedenen Blockchains wird bis zu einem gewissen Grad das Spektrum der verschiedenen Ausprägungen dieser Technologie dargestellt. Im Zuge der Vorstellung wird der Fokus konkret auf den dahinterliegenden Zweck und die technischen Spezifikationen gelegt und weniger zum Beispiel auf den geschichtlichen Hintergrund. Dieser kann im Bedarfsfall durch die zugrunde liegenden Quellen nachgelesen werden.

Selbstverständlich stellt diese Liste keinen Anspruch auf Vollständigkeit in Bezug auf die Gesamtheit aller erwähnenswerten Blockchains dar. Insbesondere da es durch Forks und diverser ICOs[2] in den letzten Jahren zu einer Unzahl von Projekten, Blockchains und Konzepten gekommen ist, würde eine detailliertere Auflistung den Rahmen dieser Arbeit sprengen.

Tendenziell handelt es sich bei diesen Netzwerken auch um Plattformen, die genutzt werden können, um verschieden Use Cases zu erfüllen. Diese können also tendenziell für die Erstel-

[1] ANMERKUNG: Die Nutzung von Smart Contracts, wie durch Buterin beschrieben, wird im Rahmen dieser Arbeit explizit nicht als notwendiger Aspekte für eine Blockchain herangezogen.

[2] ANMERKUNG: ICO = Initial Coin Offering – Stellt die erste Ausschüttung von Token im Rahmen einer neu veröffentlichten Blockchain dar.

lung konkreter Blockchain-Anwendungen herangezogen werden. Ganz konkrete Use Case Lösungen werden dann in Kapitel „Identifizierte Use Cases im Rahmen des Product Life Cycle“ behandelt.

2.3.1 Bitcoin

Obwohl Bitcoin bereits in der Beschreibung der Grundlagen oft erwähnt wurde, sollte dieses Netzwerk auch hier nochmal angeführt werden. So stellt dieses Netzwerk das erste System dar, dass als Blockchain bekannt wurde. Darum bilden die hier eingesetzten Mechanismen die Basis für eine Vielzahl von Entwicklungen und stellen sozusagen eine Ausgangsbasis für viele weitere Plattformen dar.

Wichtige Eigenschaften der Bitcoin-Blockchain sind jedenfalls[1]:

- Es handelt sich um eine Public Blockchain
- Die Nutzer müssen zur Nutzung nicht ihre echte Identität preisgeben und werden nur durch die Nutzung des Public Keys identifiziert
- Die Zeitspanne, in der in etwa ein Block generiert wird, beträgt rund 10 Minuten
- Durchschnittliche Transaktionsgröße: 500 Bytes
- Blockgröße limitiert auf 1 MB
- Die Bitcoin Blockchain verfügt nur über eine limitierte Scripting Sprache

Die ursprüngliche Idee für Bitcoin, und auch bis heute den primären Nutzen, stellt die Möglichkeit zur Transaktion von Wert dar. Diese Ausrichtung hat aber nur begrenzt einen Zusammenhang mit Use Cases im Kontext des Product Life Cycle, wie sich in Kapitel „Beurteilung, Kategorisierung und Extrapolation“ zeigen wird.[2]

Selbst, wenn man diese Überlegung auf die generische Transaktion von Daten umlegt, stellt diese alleinige Möglichkeit nur begrenzt Anwendungsmöglichkeiten im industriellen Kontext dar.

Geht man nun von einer durchschnittlichen Transaktionsgröße von 500 Bytes aus und einer maximalen Blockgröße von 1 MB aus, entspricht das in etwa 2000 Transaktionen pro Block oder 3-4 Transaktionen pro Sekunde.[3]
Diese Transaktionsgeschwindigkeit wäre für viele Anwendungen, besonders im IoT-Bereich viel zu gering und nur begrenzt skalierbar.

Zu erwähnen ist jedoch, dass mittels Off-Chain Transaktionen durch spezielle externe Transaktionskanäle, wie es durch das sogenannte Lightning Netzwerk genutzt wird, die endgültige Transaktionsgeschwindigkeit erhöht werden kann.[4]

[1] vgl. Ploom T., 2016, S.312f
[2] vgl. Nakamoto S., 2008, S.1ff
[3] vgl. Ploom T., 2016, S. 126
[4] vgl. Poon J. & Dryja T., 2016, S.3ff

Ob dieser Workaround jedoch das Problem der Skalierbarkeit für einen konkreten Use Case erfüllt, muss von Fall zu Fall beurteilt werden.

Ebenso die Sinnhaftigkeit der Nutzung eines Proof of Work Consensus-Mechanismus sollte von Fall zu Fall geprüft werden. Insbesondere, da es durch die notwendige CPU-Leistung zu einem hohen Energieverbrauch kommt. Auch hier muss somit von Fall zu Fall überprüft werden, ob nicht die Nutzung eines anderen Consensus-Mechanismus zielführender ist.

2.3.2 Ethereum

Die Intention zur Erstellung von Ethereum war eine offene Blockchain Plattform, die es ermöglicht DApps mittels Blockchain-Technologie verfügbar zu machen und dabei leicht adaptierbar und flexibel zu sein. Ziel dabei ist die Verfügbarmachung einer Plattform die verschiedenen komplexere Berechnungen und Anwendungen ermöglicht.[1]
Zwei Beispiele stellen Swarm, eine Möglichkeit zur verteilten Speicherung von Daten oder Whisper, eine Peer-to-Peer Kommunikationsplattform dar.

Den Kern der Ethereum Blockchain stellt die Ethereum Virtual Machine (EVM) dar, die auf jedem Node im Ethereum Netzwerk ausgeführt wird. Dabei kann Ethereum als Turing-vollständig angesehen werden, wodurch die gewünschten Applikationen mittels verbreiteter Sprachen wie JavaScript oder Python modelliert werden können.[2]
Da alle über die EVM durchgeführten Berechnungen auf jedem Node ausgeführt werden, muss die Rechenleistung im Vergleich zu herkömmlichen Servern als weit weniger effizient angesehen werden.

Eine weitere spezielle Eigenschaft von Ethereum stellen spezielle Contract Accounts dar. Dabei handelt es sich um komplett codebasierte Accounts, die Smart Contracts beinhalten. Diese führen also die beinhalteten Smart Contracts aus, sobald sie dazu beauftragt werden. Kontrolliert werden diese Accounts entsprechend wieder von sogenannten Externally Owned Accounts (EOAs), die von menschlichen Nutzern mittels Private Key zugänglich sind.[3]

Wichtige Eigenschaften der Ethereum Blockchain sind außerdem:[4]

- Es kann entweder die Public Blockchain von Ethereum genutzt werden oder ein eigenes geschlossenes Netzwerk erstellt werden
- Die Nutzer müssen nicht ihre Echte Identität angeben
- Maximale Anzahl an Transaktionen: 10-20 pro Sekunde
- Zykluszeit in der ein neuer Block entsteht: 12 Sekunden
- Bis zu 89 Kilobyte pro Transaktion

[1] vgl. http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html zuletzt gelesen am 03.01.2019
[2] vgl. http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html zuletzt gelesen am 03.01.2019
[3] vgl. http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html zuletzt gelesen am 03.01.2019
[4] vgl. Ploom T., 2016, S.132f

- Consensus-Mechanismus: Proof of Work; Ziel: zukünftiger Wechsel auf Proof of Stake
- Programmiersprache zur Smart Contract Erstellung: Solidity.

Werden nun Applikationen über die Ethereum-Blockchain realisiert, weisen diese somit eine geringe Fehleranfälligkeit der Transaktionen, keine Systemausfälle und unveränderbare Speicherung der Daten auf der Blockchain auf.[1]

Ethereum stellt somit eine etablierte, einfach zugängliche Plattform zur Erstellung und Nutzung von Applikationen innerhalb eines Blockchain-Netzwerkes dar. So sind zu Beginn des Jahres 2019 auf der Plattform „State of the DApps“ für Ethereum über 2100 Applikationen registriert.[2]

Durch die im Vergleich zu Bitcoin erweiterten Anwendungsmöglichkeiten sowie die Möglichkeit zur Nutzung einer Turing-vollständigen Programmiersprache, stellt Ethereum eine gute Möglichkeit dar, um mit möglichst geringen Hürden kleine Blockchain-Applikationen im Rahmen des Product Life Cycle erstellen zu können.

Dadurch können die oben erwähnten Vorteile solcher Applikationen genutzt werden, ohne ein eigenes Blockchain-Netzwerk erstellen zu müssen, was tendenziell mit höherem Kosten- und Personalaufwand einhergehen würde. Besonders für Proof of Concept Projekte innerhalb einer Organisation kann es durchaus eine Überlegung wert sein, das Ethereum Netzwerk zu nutzen.

2.3.3 NEO

Direkt im Vergleich zu Ethereum steht NEO. Eine Blockchain-Plattform, die sehr stark der Ethereum-Plattform ähnelt und besonders in China stark verbreitet ist, wo die Plattform durch die Regierung unterstützt wird. NEO bietet dabei so wie Ethereum die Möglichkeit der Erstellung von Applikationen mittels Smart Contracts und nutzt hierfür die NeoVM (Neo Virtual Machine).[3]

Die gravierendsten Unterschiede zwischen NEO und Ethereum stellen der genutzten Consensus-Mechanismus dar, sowie die Tatsache, dass Entwickler bei NEO die verbreiteten Programmiersprachen C#, Java oder Python verwenden können. NEO hat laut eigenen Angaben den Anspruch die Entwickler-freundlichste Plattform für Blockchain-Applikationen zu sein.[4]

Der bei NEO genutzte Consensus-Mechanismus ist der Delegated Byzantine Fault Tolerant Consensus-Mechanismus, wie er in Kapitel „Alternative Proofs“ beschrieben wird. Dieser Aspekt ist unter anderem ein Grund, warum NEO angibt bis zu 10.000 Transaktionen pro Sekunde ausführend zu können.[5] (Ethereum im Vergleich dazu wie oben beschreiben etwa 10-20)

In Bezug auf Skalierbarkeit und Einsteigerfreundlichkeit, hat NEO somit klare Vorteile gegenüber Ethereum. Insbesondere durch die Verbreitung in China und der damit einhergehenden

[1] vgl. http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html zuletzt gelesen am 03.01.2019
[2] vgl. https://www.stateofthedapps.com/de/rankings/platform/ethereum?page=1 zuletzt gelesen am 03.01.2019
[3] vgl. https://neo.org/ zuletzt gelesen am 03.01.2019
[4] vgl. https://neo.org/ zuletzt gelesen am 03.01.2019
[5] vgl. https://coinsutra.com/neo-vs-ethereum-differences/ zuletzt gelesen am 03.01.2019

Marktmacht dürfte davon auszugehen sein, dass NEO in Zukunft eine wichtige Rolle im Blockchain-Bereich spielen wird.

2.3.4 NEM

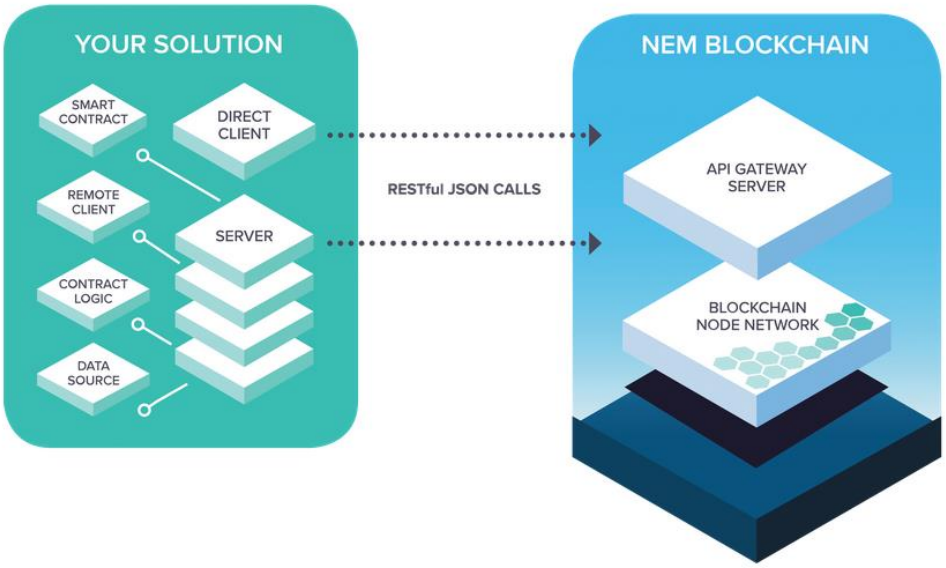
NEM unterscheidet sich in mehreren Aspekten von den meisten Smart Contract fokussierten Blockchains. Dabei versteht sich NEM als Plattform für Anwendungsentwickler mit hoher Skalierbarkeit und vielen Funktionalitäten.[1]

Zum einen nutzt NEM als Consensus-Mechanismus Proof of Importance (Siehe Kapitel „Alternative Proofs“), der die hohe Skalierbarkeit ermöglichen soll.[2]
Zusätzlich zu diesem, im Vergleich zu Proof of Work energieeffizienteren und durch die festgelegte Zykluszeit von 1 Minute schnelleren Consensus-Mechanismus, nutzt NEM den sogenannten Eigentrust++ Algorithmus, um den einzelnen Nodes einen Vertrauens-Index zuzuordnen. Durch diese Bewertung können potenziell bösartige Nodes leichter identifiziert werden.[3]

NEM bietet auch einige Aspekte, die potenziellen Nutzern die Nutzung des Netzwerks sowie die Erstellung der gewünschten Applikationen erleichtern soll, um besonders die Nutzung des NEM-Netzwerks durch Unternehmen zu forcieren. Wie in Abbildung 2-11 zu sehen, bietet NEM die Möglichkeit mittels RESTful JSON API Calls die NEM Blockchain direkt aus der eigenen Applikation aufzurufen. Dadurch können die eigenen Prozesse zum Beispiel durch beliebige Programmiersprachen abgebildet werden und dann mittels der NEM API zur Blockchain verknüpft werden.

[1] vgl. https://nem.io/ zuletzt gelesen am 04.01.2019
[2] vgl. NEM: Technical Reference, 2015, S.26ff
[3] vgl. NEM: Technical Reference, 2015, S.21ff

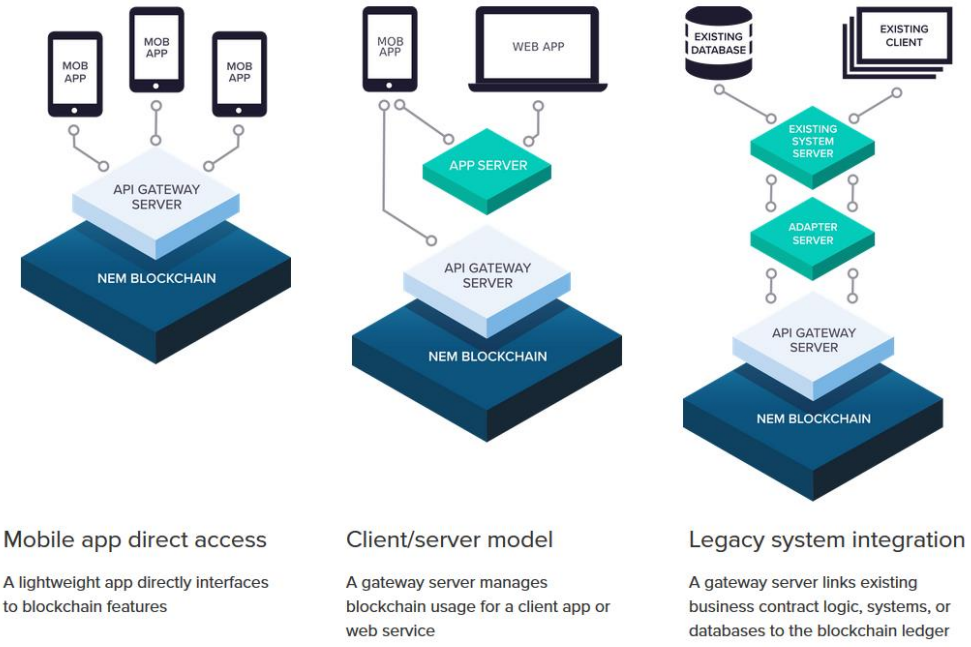
Abbildung 2-11: Aufbau des NEM Netzwerks[1]



Entsprechend Abbildung 2-12 können somit bereits existierende Datenbanken und Server mit dem NEM-Netzwerk verbunden werden. Vorteil hierbei ist auch, dass nicht alle Daten selbst auf die Blockchain gespeichert werden müssen. Je nach Use Case kann zB. eine Datei selbst im unternehmensinternen Datencenter gespeichert werden, eine entsprechende Hash-Referenz aber dann auf der Blockchain, um die Unveränderbarkeit der Daten zu gewährleisten. Außerdem muss durch diese Struktur nicht die gesamte Blockchain für die Nutzung derselben heruntergeladen werden, was wiederum der Skalierbarkeit zuträglich ist.

[1] Abb. 2-11 aus https://nem.io/technology/ zuletzt gelesen am 04.01.2018

Abbildung 2-12: Mögliche NEM Lösungsarchitekturen[1]



Je nach Use Case bietet NEM auch die Möglichkeit, entweder die Public Mainchain von NEM zu nutzen oder die Erstellung einer Private Blockchain angeknüpft an die Mainchain. Dadurch wäre es zum Beispiel möglich, dass zwei unterschiedliche Unternehmen die NEM Mainchain nutzen, um Daten auszutauschen, ohne sich jeweils gegenseitig Zugriff auf die Private Chain geben zu müssen oder alle Daten offenlegen zu müssen.[2]

Ein weiterer Aspekt mit dem NEM darauf abzielt die Usability zu erhöhen ist das Smart Asset Konzept, durch das es ermöglicht einzelne Applikations-Building-Blocks durch Blockchain-Adressen in eine Art Container zu verpacken. Dadurch können komplexere Anwendungen vergleichsweise einfach modular durch diese Building-Blocks zusammengefasst werden.[3]
Eine solche Konstruktion ermöglicht eine einfachere Nutzung der Blockchain-Technologie im Unternehmenskontext.

[1] Abb. 2-12 aus https://nem.io/technology/ zuletzt gelesen am 04.01.2019
[2] vgl. https://nem.io/technology/ zuletzt gelesen am 04.01.2019
[3] vgl. https://nem.io/technology/ zuletzt gelesen am 04.01.2019

2.3.5 EOS

EOS stellt sich als betriebssystem-ähnliches System dar, das darauf ausgelegt ist sowohl vertikal (mehr CPU Leistung) als auch horizontal (höhere Anzahl an CPUs) skalierbar zu sein. Aufgrund dieser Skalierbarkeit und Struktur des Netzwerks, gibt EOS an, im Endeffekt mehrere Millionen Transaktionen pro Sekunde ausführen zu können.[1]
Dies würde sogar die Anforderungen übersteigen, die z.B. ein Kreditkartenunternehmen mit einer hohen Anzahl an Transaktionen stellen müsste. Entsprechend einem Mybroadband Artikel führt Visa im Schnitt 1700 Transaktionen pro Sekunde aus.[2]
Mit einer Transaktionsgeschwindigkeit die EOS angibt, würde das Blockchain-Netzwerk die Effizienz heutiger bestehender Systeme erreichen und übertreffen. Dadurch könnte EOS, sollte das System diesen Punkt wirklich erreichen, als Proof of Concept für die Skalierbarkeit von Blockchain-Systemen fungieren. Insbesondere in dem Zusammenhang, dass dadurch die Nutzbarkeit im Rahmen des IoT-Kontextes erhöht wird, da in diesem Bereich tendenziell sehr hohe Transaktionsgeschwindigkeiten notwendig sind. Dadurch könnten zukünftige Applikationen im industriellen Ausmaß ermöglicht werden.[3]

EOS nutzt, um diese Skalierbarkeit zu erreichen, den Delegated Proof of Stake Consensus-Algorithmus, der laut Anmerkung im Technical White Paper von EOS der einzige Algorithmus ist, der diesen Effizienzanforderungen genügen kann und zusätzlich unter normalen Umständen keine Forks auftreten lässt. Durch einen Blockbildungs-Zyklus von exakt 0,5 Sekunden besitzt das EOS Netzwerk außerdem eine vergleichsweise sehr geringe Latenz, die mit zentralisierten Systemen durchaus mithalten kann.[4]

Die EOSIO Software zur Teilnahme am Netzwerk bietet außerdem vorgefertigte Funktionalitäten, wie Authentifizierungs-Möglichkeiten, Datenbanken, Asynchrone Kommunikation und die Verteilung von Applikationen über eine Anzahl von CPU-Kernen oder -Clustern.[5]

Sollte nun EOS den sich selbst gesetzten Anforderungen gerecht werden, stellt die Plattform eine effiziente und vor allem leistungsstarke Möglichkeit zur Nutzung von Blockchain-Technologie im industriellen Ausmaß dar.

---

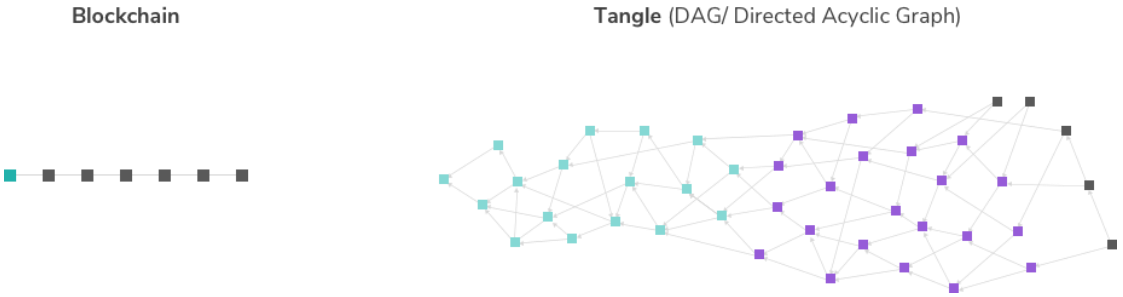
[1] vgl. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md zuletzt gelesen am 04.01.2019
[2] vgl. https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html zuletzt gelesen am 04.01.2019
[3] vgl. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md zuletzt gelesen am 04.01.2019
[4] vgl. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md zuletzt gelesen am 04.01.2019
[5] vgl. https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md zuletzt gelesen am 04.01.2019

2.3.6 IOTA

IOTA stellt eine Abweichung von den bisher beschriebenen Blockchain-Konzepten dar. Im oben beschriebenen Sinne, ist IOTA auch nicht als Blockchain zu klassifizieren, sondern stellt einen Distributed Ledger dar, der das Tangle-Konzept nutzt. Dabei fokussiert sich die Nutzung von IOTA besonders auf Machine-to-Machine Kommunikation sowie gebührenfreie Mikrotransaktionen und hat somit ausgeprägte Use Cases im IoT-Bereich.[1]

Das Tangle-Konzept, oder auf DAG (Directed Acyclic Graph) genannt, unterscheidet sich von üblichen Blockchains insofern, dass die durchgeführten Transaktionen nicht zu Blöcken zusammengefasst und zu einer Kette aneinandergereiht werden, sondern, dass die einzelnen Transaktionen miteinander verstrickt (engl. entangled) werden. Abbildung 2-13 stellt diesen Zusammenhang bildlich dar.[2, 3]

Abbildung 2-13: Vergleich Blockchain und Tangle[4]



Das Prinzip der Verifikation ist im Tangle so aufgebaut, dass man, um eine eigene Transaktion zu verifizieren, zwei vorhergegangene Transaktionen verifizieren muss. Die Zustimmung zu einer Transaktion setzt voraus, dass alle ihr vorhergegangenen Transaktionen ebenfalls als valide anerkannt werden. Sobald nun durch diesen Prozess eine Transaktion durch eine große Anzahl neuer Transaktionen verifiziert wurde, entsteht ein allgemeiner Konsens über den Status und diese Transaktion ist de facto nicht mehr abänderbar. Ähnlich wie in Blockchain-Netzwerken.[5]

Die Verbindung der Transaktionen erfolgt ähnlich wie die Verbindung von Blöcken in einer Blockchain. Jede Transaktion besitzt eine Referenz auf vorhergehende Transaktionen bzw.

[1] vgl. https://docs.iota.org/docs/getting-started/0.1/introduction/what-is-iota zuletzt gelesen am 04.01.2019
[2] vgl. https://docs.iota.org/docs/getting-started/0.1/introduction/what-is-iota zuletzt gelesen am 04.01.2019
[3] ANMERKUNG: Eine Weitere Form von DAG stellt das Hashgraph Protocol dar, welches jedoch nicht so bekannt und verbreitet ist wie IOTA. Nähere Informationen hierzu siehe: https://www.swirlds.com/whitepapers/ zuletzt gelesen am 04.01.2019
[4] Abb. 2-13 aus https://www.iota.org/get-started/what-is-iota zuletzt gelesen am 04.01.2019
[5] vgl. https://www.iota.org/research/meet-the-tangle zuletzt gelesen am 04.01.2019

deren Hash. Definiert durch gewisse Attribute („branchTransaction“ und „trunkTransaction“) innerhalb der Transaktionsinformationen.[1]

Bei der Weiterführung des Tangles durch neue Transaktionen wird eine sogenannte „Tip Selection“ durchgeführt. Also die Auswahl der Spitzen (der letzten vorhergehenden Transaktionen) an die die neuen Transaktionen angehängt werden. Pro Transaktion werden zwei Random Walks[2] ausgehend von der ersten durchgeführten Transaktion (Genesis Transaction) durchgeführt. Dabei hat der Random Walk die Tendenz sich entlang der stärkeren Vernetzung (mehr „cumulative weight“) fortzusetzen, da Äste mit weniger Verknüpfungen tendenziell weniger stark verifiziert werden und eventuell ganz verschwinden. Dadurch wird der Tangle entlang eines Hauptstranges geführt und verzweigt sich nicht willkürlich.[3]

Auf diesem Weg wird ein Konzept geschaffen, in dem keine Gebühren und keine signifikante Rechenleistung notwendig ist, um die eigene Transaktion durchzuführen, wodurch ein Tangle prinzipiell eine hohe Skalierbarkeit aufweist, wobei nach diesem Prinzip die Transaktionen umso schneller verifiziert werden, umso höher die Anzahl der aktiven Teilnehmer im Netzwerk ist. Im Gegensatz zu vielen Blockchain-Systemen wird die Skalierbarkeit und Transaktionsgeschwindigkeit des Tangles nicht durch Mining oder anderweitige Restriktionen begrenzt.[4] Zusätzlich ist es möglich beliebige Informationen über die Transaktionen zu versenden oder größere Datenmenge auch über gebündelte oder verlinkte Transaktionen zu transferieren.[5]

Bezüglich der Einsatzfähigkeit und Anwendbarkeit von IOTA ist zu sagen, dass sich das Netzwerk und die Technologie an sich noch in der Entwicklungsphase befindet und viele Konzepte der Technologie sich noch in der Testphase befinden. Auf https://www.iota.org/research/roadmap sind die aktuellen Forschungs- und Entwicklungsprojekte der IOTA Foundation zu finden. Einfache Anwendungen wie simple Transaktionen und die Nutzung von IOTA-Token sind prinzipiell möglich, aber abgesehen von ein paar Forschungsprojekten bietet IOTA keinen so einfachen Zugang zum Netzwerk und Entwicklungstools wie andere Plattformen.

Somit lässt sich derzeit nicht abschätzen, in wie fern IOTA für industrielle Anwendungen in der Realität tatsächlich nutzbar sein wird. In Bezug auf einfache Proof of Concepts oder Versuchs-Projekte innerhalb eines Unternehmens kann man argumentieren, sich auf bereits etabliertere Plattformen wie Ethereum, NEM oder EOS zu konzentrieren.

[1] vgl. https://docs.iota.org/docs/the-tangle/0.1/introduction/overview zuletzt gelesen am 04.01.2019
[2] ANMERKUNG: hier konkret ein Markov Chain Monte Carlo Random Walk; Siehe: Popov S., 2017, S.20ff
[3] vgl. https://www.iota.org/research/meet-the-tangle zuletzt gelesen am 04.01.2019
[4] vgl. https://docs.iota.org/docs/getting-started/0.1/introduction/what-is-iota zuletzt gelesen am 04.01.2019
[5] vgl. https://docs.iota.org/docs/getting-started/0.1/introduction/what-is-iota zuletzt gelesen am 04.01.2019

2.3.7 Hyperledger - IBM Blockchain

Bei Hyperledger handelt es sich selbst nicht um eine Blockchain oder eine Nutzbare Plattform zur Nutzung eines Blockchain-Netzwerkes wie Ethereum, sondern um ein Open Source Kollaborativ das von der Linux Foundation gehostet wird.[1]

Dabei setzt Hyperledger den Fokus auf Blockchain-Anwendungen im industriellen Bereich und grenzt sich explizit von auf Kryptowährungen fokussierte Blockchains ab. Insbesondere sind die von Hyperledger definierten Ziele unter anderem die Erstellung von Frameworks, Code Bases und Open Source Infrastruktur, um die Weiterentwicklung der Blockchain-Technologie voranzutreiben.[2]

Zwei der am weitesten fortgeschrittenen Projekte im Hyperledger Kollaborativ, sind Hyperledger Fabric, das von IBM betreut wird, und Hyperledger Sawtooth, ein Netzwerk das primär von Intel entwickelt wurde. Natürlich gibt es aber noch viele andere Projekte mit unterschiedlichem Entwicklungsstand.[3]

Eine Besonderheit der Hyperledger-Projekte stellt die Tatsache dar, dass Hyperledger-Blockchains die Möglichkeit bieten, dass Smart Contracts andere Applikationen über Web Service APIs oder REST aufrufen können und tausende Transaktionen pro Sekunde durchführen können, was für viele Geschäftsprozesse essenziell sein kann. Somit ist es einfacher möglich Blockchain-Applikationen in die eigenen Prozesse zu integrieren.[4]

Hyperledger Fabric bietet ein modulares Framework zur Erstellung eigener Anwendungen mit Plug-and-play Komponenten durch die Nutzung von Containerisierung.[5, 6]

Hyperledger Sawtooth stellt vor allem einen Proof of Concept für einen Proof of Elapsed Time Consensus-Mechanismus dar, mit dem Fokus auf Internet of Things Anwendungen und ebenfalls mit modularem Aufbau.[7]

Vor allem bietet Hyperledger die Möglichkeit zur Erstellung von geschlossenen und halb öffentlichen Blockchain-Netzwerken, was im Unternehmenskontext durchaus ein Vorteil zur Verringerung der Einstiegshürden sein kann, da viele Unternehmen explizit diese Form der Blockchain fordern.

Durch die von Hyperledger zur Verfügung gestellte Infrastruktur und dem besonderen Fokus auf Blockchain-Anwendungen im Unternehmens-Kontext, stellt Hyperledger eine gute Möglichkeit dar, um verhältnismäßig schnell und modular eigene Anwendungen zu ermöglichen.

---

[1] vgl. https://www.hyperledger.org/ zuletzt gelesen am 05.01.2019
[2] vgl. https://www.hyperledger.org/about zuletzt gelesen am 05.01.2019
[3] vgl. https://www.hyperledger.org/projects zuletzt gelesen am 05.01.2019
[4] vgl. Ploom T., 2016, S.144f
[5] vgl. https://www.hyperledger.org/projects/fabric zuletzt gelesen am 05.01.2019
[6] ANMERKUNG: Containerisierung im Sinne der softwaretechnischen Verkapselung
[7] vgl. https://www.hyperledger.org/projects/sawtooth zuletzt gelesen am 05.01.2019

Besonders auch, dass einige Hyperledger-Projekte weit fortgeschritten sind, eine entsprechende Skalierbarkeit für die industrielle Nutzung und laut eigenen Angaben als stabil zu bezeichnen sind, stellt eine gute Basis für die Nutzung der Frameworks dar. Der Fokus auf Unternehmensanwendungen tut sein Übriges, um eine gute Möglichkeit zur Nutzung von Blockchain-Technologie im industriellen Kontext darzustellen. Natürlich muss das von Fall zu Fall und entsprechend des bereitgestellten Frameworks individuell geprüft werden.

3 Beurteilung, Kategorisierung und Extrapolation

In diesem dritten Teil der Arbeit werden nun die bisherig genannten allgemeinen Aspekte mit bereits bestehenden und potenziellen Anwendungsmöglichkeiten zusammengeführt. Als Ergebnis sollen sich abzeichnende Use Case Kategorien identifiziert werden und diese auf die tatsächliche Anwendbarkeit im Product Life Cycle beurteilt werden. Aufbauend auf diese Erkenntnisse werden im Anschluss zwei selbst entwickelte, generische Use Cases vorgestellt, welche mittels UML dargestellt werden.

3.1 Beurteilung der Blockchain-Technologie im Rahmen des Product Life Cycle

In diesem Kapitel wird auf die konkrete Einschätzung der Nutzbarkeit der Blockchain-Technologie im Rahmen des Product Life Cycle eingegangen. Insbesondere, da die ersten und verbreitetsten Anwendungsgebiete der Blockchain sich auf den Finanzmarkt und Finanztransaktionen beziehen, wird hier eine genaue Abgrenzung durchgeführt und gefundene Use Cases werden ggf. auf Anwendungsmöglichkeiten im industriellen Umfeld umgelegt.

3.1.1 Methodische Vorgehensweise

Zuerst werden die Ziele und Herausforderungen im Rahmen des Product Life Cycle aus einschlägiger Fachliteratur gesammelt. Anschließend wird auf den aktuellen Stand der Blockchain-Technologie sowie auf die Vor- und Nachteile in Bezug auf die im Kapitel „Ziele & Herausforderungen im Rahmen des Product Life Cycle“ identifizierten Aspekte aufgezeigt. Als zusätzliches Kriterium wird auch ein Entscheidungsmodell über die Anwendung der Blockchain-Technologie vorgestellt.

Zur Beurteilung der konkreten Anwendungsmöglichkeit der Blockchain-Technologie im Product Life Cycle, wurden hierfür bestehende oder potenzielle Use Cases gesammelt und entsprechend kategorisiert. Die Basis hierfür bilden wissenschaftliche Publikationen sowie Fachliteratur. Die hierfür herangezogenen Quellen wurden nochmal explizit im Anhang angegeben.

Besonders zu erwähnen sei hier das Paper „Blockchain Technology – Beyond Bitcoin“ von Crosby M et al. welches bereits einige „Non-Financial Applications“ der Blockchain auflistet:

- Applications in the music industry
- Decentralized proof od existence of documents
- Decentralized storage
- Decentralized IoT
- Anti-Counterfeit Solutions
- Internet Applications

Ebenso ein von „EPRS (European Parliamentary Research Service) veröffentlichter Bericht „How blockchain technology could change our lives“[1], sowie von Frankfurt School Blockchain Center herausgegebene Working Paper „Application of Blockchain Technology in the Manufacturing Industry“ die als Grundgerüst für die weitere Sammlung und Strukturierung herangezogen wurden.

Aufbauend auf diesen Quellen wurde ein erster Entwurf der Kategorisierung mittels Mind-Mapping[2] durchgeführt und durch weitere Quellen in Form von diversen Whitepaper von Blockchain-Entwicklern, Informations-Broschüren verschiedener Blockchain-bezogenen Organisationen, vereinzelte Veröffentlichungen von Consulting-Unternehmen und einer allgemeine Internet-Suche ausgebaut und konkretisiert.

Im Rahmen der Recherche mit diesen Quellen wurden die identifizierten Use Cases in der Mind-Map gesammelt und mit Kurzbeschreibungen versehen. Sobald ein Use Case eine bestehende oder potenzielle Relevanz für ein industrielles Umfeld zu zeigen schien, wurde er entsprechend in die Mind-Map aufgenommen, um bei der Kategorisierung in Betracht gezogen werden zu können. Dabei wurde vor allem auch der österreichische Markt betrachtet.

Konkret wurden jene Use Cases gewählt, für die folgende Fragen positiv zu beantworten waren:

- Ist eine Anwendung im bzw. eine Umlegung auf den industriellen Kontext möglich?
- Entspricht der Use Case einer tatsächlichen Blockchain-Anwendung?
- Ist der Use Case realistisch umsetzbar?
- Handelt es sich dabei nicht um einen reinen (finanz-)transaktionsbezogenen Use Case?[3]

Das Ziel der Sammlung war die Zuordnung der einzelnen Projekte und Anwendungen zu übergeordneten möglichst generischen Use Case Kategorien. Dabei war insbesondere nicht die Branche oder die dahinterliegende Technologie ausschlaggebende, sondern viel mehr das zugrundeliegende Ziel und der Zweck des Use Cases.

---

[1] vgl. Boucher P., 2017, S.1ff

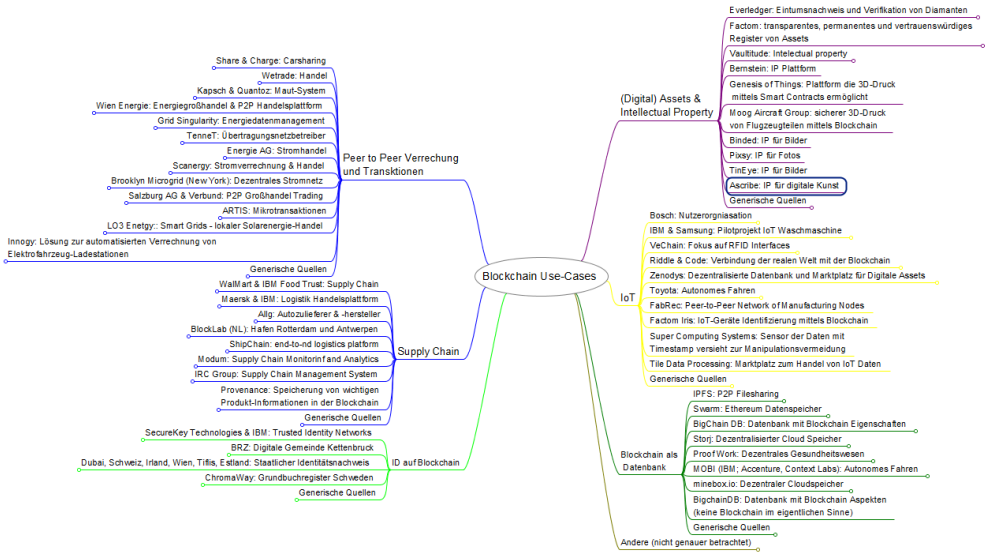
[2] ANMERKUNG: Beschreibung Mind-Mapping siehe: https://www.mindmapping.com/de/

[3] ANMERKUNG: Dem entsprechend, wurden für diese Sammlung jene Use Cases, die sich primär auf Finanztransaktionen und Kryptowährungen beziehen nicht mit einbezogen. Das trotz der Tatsache, dass diese Use Cases die am weitesten verbreiteten Anwendungsfälle darstellen.

Nach Abschluss der Sammlung der verschiedenen Use Cases wurden diese kategorisiert und entsprechend der Kategorisierung zu Ästen in der Mind-Map zusammengefasst.

Abbildung 3-1 zeigt die Mind-Map zur Use Case Sammlung.

Abbildung 3-1: Mind-Map zur Use Case Sammlung und Kategorisierung



Die Struktur der Mind-Map folgt folgenden Regeln:

> Ebene 1: Bezeichnung der Kategorie
>
> Ebene 2: Bezeichnung der konkret gefundenen Projekte und Use Cases, Knotenpunkt für generische Quellen an letzter Stelle angeführt
>
> Format zur Knotenbenennung: [Unternehmen/Organisation: Thema/Ausprägung]

In Kapitel „Identifizierte Use Cases im Rahmen des Product Life Cycle“ werden dann entsprechend der finalen Form der Mind-Map die Use Cases anhand der gefundenen Beispiele möglichst generisch beschrieben und bei Bedarf auf die Nutzung im industriellen Umfeld umgelegt.

Aufbauend auf die generische Beschreibung und die bisherigen Erkenntnisse werden zum Abschluss zwei selbst entwickelte Use Cases vorgestellt, wie konkrete Blockchain-Teilprozesse aussehen könnte. Diese Use Cases werden hierfür mittels UML dargestellt und ausführlich dargelegt.

3.1.2 Ziele & Herausforderungen im Rahmen des Product Life Cycle

Im Fachbuch „CAx für Ingenieure“ beschreiben Vajna et al. „Die wichtigste Herausforderung an Unternehmen seit vielen Jahren ist die Aufrechterhaltung, wenn möglich Steigerung der Wettbewerbsfähigkeit auf einem sich zunehmend globalisierenden Markt.“[1]

Als konkrete Aspekte in diesem Zusammenhang werden unter anderem beschrieben:[2, 3]

- Relativ hohe Kosten in den hochentwickelten Industrieländern
- Geringe Fehlertoleranz und hohe Qualitätsansprüche der Kunden
- Notwendigkeit kurzer Innovationszyklen („Time to Market“)
- Bedarf an kundenindividuelle Massenproduktion
- Näheres Zusammenrücken der vor der Produktion liegenden Unternehmensbereiche
- Neue Aufgabenverteilung innerhalb des eigenen Unternehmens und über Unternehmensgrenzen hinweg
    - Auslagerung von Entwicklungs- und Planungsaufgaben auf Zulieferer oder Dienstleister
    - Örtlich verteilte Teams für kollaborative Entwicklung/Planung
- Verstärkte Nutzung rechnergestützter Methoden und Werkzeuge über den gesamten Product Life Cycle hinweg

Als wichtiger Aspekt entsprechend der oben angeführten Aspekte wird explizit die Interaktion zwischen verschiedenen Parteien (Teams, Gruppen, Abteilungen, Unternehmen) hervorgehoben.[4]
Dementsprechend kann also der Aufbau von Netzwerken und der Austausch von Daten als Punkt mit hoher Priorität angesehen werden.

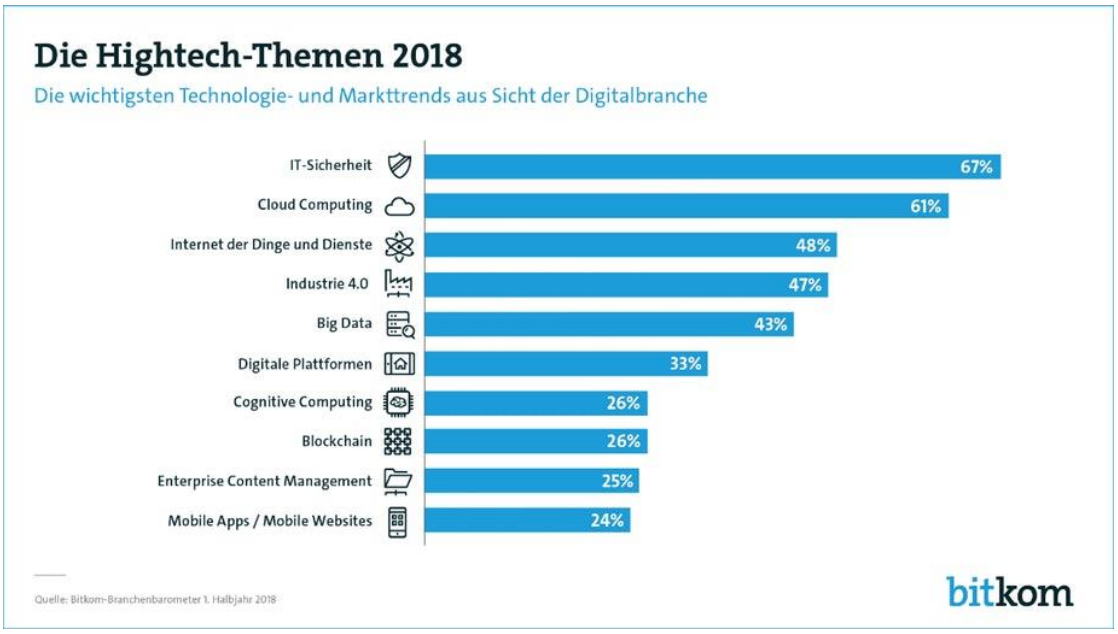
Wenn man nun generell einen Blick auf die relevantesten Digitalthemen und somit auf die künftigen Herausforderungen wirft, zeigt die die 2018 durchgeführte Umfrage von Bitkom (entsprechend Abbildung 3-2), dass das Thema Blockchain selbst bereits in den Top Ten der relevantesten Themen zu finden ist.[5]

Unter den anderen Top-Ten Themen befinden sich außerdem IT-Sicherheit, Internet der Dinge, Industrie 4.0, Digitale Plattformen und Enterprise Content Management. Da sich für diese Herausforderungen ebenfalls Blockchain-Anwendungsmöglichkeiten zeigen, können diese ebenso als relevante Aspekte in Bezug auf die Bewertung von Blockchain-Plattformen angesehen werden.

---

[1] vgl. Vajna et al., 2018, S.3ff
[2] vgl. ebenda, S.3ff
[3] ANMERKUNG: Vajna et al. beschreiben in dem Zusammenhang noch weitere Herausforderungen. Die hier angeführten entsprechen jenen, die mit etwaigen Blockchain-Lösungen in Verbindung gebracht werden können.
[4] vgl. Vajna et al., 2018, S.6
[5] vgl. https://www.bitkom.org/Presse/Presseinformation/Blockchain-wird-zu-einem-Top-Thema-in-der-Digitalwirtschaft.html zuletzt gelesen am 15.01.2019

Abbildung 3-2: Umfrage Auswertung zum Thema "Hightech-Themen 2018[1]



Ein besonderes Augenmerk kann man hier auf den Punkt IT-Sicherheit legen. Entsprechend dem Statistik-Portal Statista ist im Jahr 2017 und 2018 durch Fälle von Computerkriminalität wie Datendiebstahl, Industriespionage oder Sabotage in deutschen Unternehmen eine Gesamtschadenssumme von 43,4 Milliarden Euro entstanden.[2]
Geht man nun davon aus, dass einige der Angriffe gar nicht erst entdeckt werden, dürfte die Dunkelziffer sogar noch höher ausfallen und somit die Relevanz des Themas Datensicherheit als zentrale Herausforderung von Unternehmen in Bezug auf digitale Vernetzung weiter steigern.

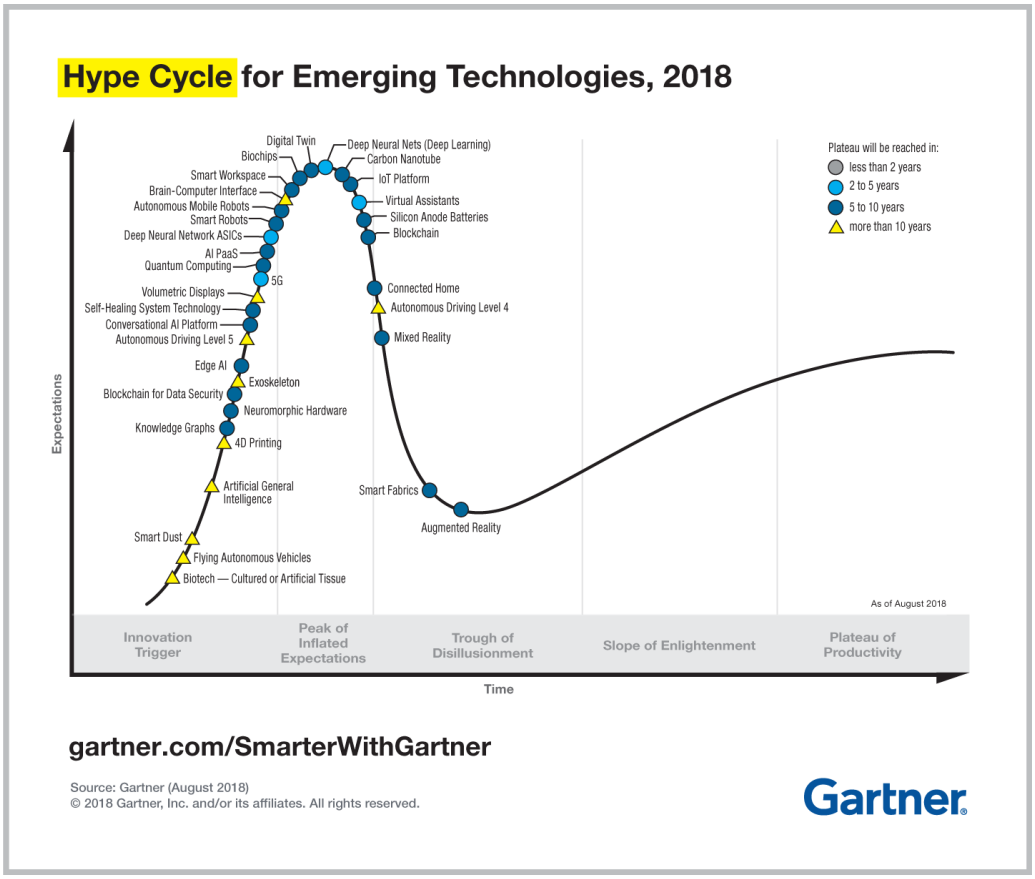
3.1.3 Stand der Entwicklung der Blockchain-Technologie

Bevor man nun die konkreten Vor- und Nachteile der Blockchain-Technologie in Bezug auf den Product Life Cycle betrachtet, sollte man die Entwicklung dieser recht neuen Technologie in einen zeitlichen Kontext setzen.

[1] Abb. 3-2 aus https://www.bitkom.org/Presse/Presseinformation/Blockchain-wird-zu-einem-Top-Thema-in-der-Digitalwirtschaft.html zuletzt gelesen am 15.01.2019
[2] vgl. https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/#0 zuletzt gelesen am 15.01.2019

Hierfür bietet sich der „Hype Cycle for Emerging Technologies“ von Gartner an. Dabei handelt es sich um ein Modell, dass den Verlauf der Erwartungen an neue Technologien über eine Zeitspanne von bis zu mehr als 10 Jahren beschreibt.[1]
Nach einem großen Hype und starker Medienpräsenz des Themas Blockchain und Kryptowährungen im Jahr 2017, nicht zuletzt gekennzeichnet durch einen starken Bullenmarkt, hat sich das mediale Interesse wieder einigermaßen gelegt und nun erfolgt vermutlich ein, wie Gartner es nennt, „Tief der Desillusionierung“.

Abbildung 3-3: Gartner Hype Cycle for Emergin Technologies, 2018[2]



Dabei wird die Technologie entsprechend getestet und versucht die Entwicklung auf ein marktreifes Niveau zu bringen. Die Tatsache, dass fortgeschrittene Projekte wie Hyperledger Fabric

[1] vgl. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/ zuletzt gelesen am 15.01.2019
[2] Abb. 3-3 aus https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/ zuletzt gelesen am 15.01.2019

und Sawtooth gerade einmal als „stabil“ zu bezeichnen sind und Projekte wie IOTA sich erst im Status der Forschung und Entwicklung befinden, spricht dafür.

Auch die Bemühungen diverser Plattformen den Consensus-Mechanismus weg vom energieintensiven Proof of Work hin zu effizienteren Mechanismen wie EOS Delegated Proof of Stake oder Intels Proof of Elapsed Time zu entwickeln zeigt, dass die Technologie als Ganzes noch einige Entwicklungsschritte vor sich hat um auf industrieller Ebene effektiv einsetzbar zu sein.

Insbesondere die Entwicklung laufender Second Layer Solutions, also Applikationen, die über die einfache Blockchain-Anwendung hinausgehen und eine zweite Ebene über einer Blockchain-Basis“ besitzen, befindet sich augenscheinlich erst in den Kinderschuhen, wobei sicher einige bereits existierende DApps als Second Layer Solutions bezeichnet werden können.

Die Tatsache dass die ISO-Organisation 2017 das technische Komitee „ISO/TC 307: Blockchain and distributed ledger technologies“ ins Leben gerufen hat, aber noch keiner der sich daraus entwickelnden Standards es bis jetzt über den Entwicklungsstand hinausgeschafft hat, zeigt, dass sich die Technologie auch in Bezug auf allgemeine Standards noch am Anfang befindet.

Bezüglich der Anwendungsfelder hat unter anderem auch Johansen S. in seinem Paper „A comprehensive literature review on the Blockchain as a technological enabler for innovation” festgestellt, dass sich auch in der Literatur kein spezifischer Bereich abzeichnet und generell eine Vielzahl Anwendungsmöglichkeiten in Betracht gezogen werden können.[1]
Dementsprechend scheint es von großer Bedeutung die technischen Aspekte und die spezifische Vor- und Nachteile der Blockchain-Technologie in einem bestimmten Setting zu überprüfen um beurteilen zu können, ob eine Anwendung einer Blockchain-Lösung im jeweiligen konkreten Fall auch tatsächlich von Vorteil ist.

3.1.4 Vorteile und Nutzen der Blockchain-Technologie im Rahmen des Product Life Cycle

Entsprechend den bisherigen beschriebenen Aspekten der Blockchain-Technologie ergeben sich potenzielle Vorteile und Nutzen, wenn die Technologie in Unternehmen eingesetzt wird. Hierbei handelt es sich um allgemeine Aspekte, die keinem Use Case zugehörig sind und entsprechend unabhängig davon erkennbar sind. Ob die angeführten Vorteile und Nutzen bei einem konkreten System tatsächlich genutzt werden, hängt aber auch vom Use Case und der Systemarchitektur ab.

Außerdem ist es wichtig abzugrenzen, dass die aufgelisteten Vorteile, und in weiterer Folge die Nachteile, sich zum Teil auf Werteversprechen verschiedener Plattformen stützen. Dadurch soll vor allem eine Übersicht der potenziellen Vorteile der Blockchain geschaffen werden, wie sie

[1] vgl. Johansen S., 2016, S.20f

zum jetzigen Stand kommuniziert werden. Die tatsächliche Realisierung hängt dann stark davon ab, ob sich diese Werteversprechen in der Realität auch umsetzen lassen.

Insbesondere auch in Bezug auf Datensicherheit und Datenschutz muss erwähnt werden, dass die inhärente Sicherheit einer Blockchain nur dann realisiert werden kann, wenn die Sicherheitsaspekte entsprechend üblicher Software-Entwicklung bei der Implementierung von Blockchain-Anwendungen als „Security-by-Design“ berücksichtigt wird. Dabei kann auf Blueprints und Best Practices Bezug genommen werden, wie sie in etwa bei BSI-Grundschutz-Standards oder OWASP beschrieben werden.[1, 2]

Tabelle 3-1 Vorteile und Nutzen der Blockchain -Technologie

Vorteil	Nutzen im Rahmen des Product Life Cycle
Reduzierung der Kosten und des Ressourcenbedarfs	■ IT wichtiger Kostenfaktor und betrifft die gesamte Supply Chain sowie den gesamten Product Life Cycle ■ Systeme laufen oft primär im Hintergrund. Kostensenkungspotenziale sind oft nicht direkt erkennbar ■ Potenzial zur Kostensenkung ○ Reduzierung der Komplexität des Systems ○ Weniger administrativer Aufwand durch Consensus-Automatisierung ○ Erhöhung der Sicherheit des Systems ○ Potenzieller Wegfall zentraler Stellen ○ Potenzieller Wegfall von Transaktions- & Nutzungsgebühren ■ Evtl. Möglichkeit zur Reduzierung der Time to Market
Erhöhte Sicherheit	■ System besitzt immanente Sicherheit gegen Angriffe von außen und bösartigen Veränderungen im System ■ Erschwert Beeinträchtigung des Systems ■ Reduziert nicht nur Sicherheitsrisiken durch Cyberkriminalität, sondern auch durch simple menschliche Fehler ■ Sicherheitsmechanismen durch automatisierte Prozesse gewährleistet. Der menschliche Faktor wird reduziert

[1] Siehe: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[2] Siehe: https://www.owasp.org/index.php/Main_Page

Datenintegrität und Datenkonsistenz	■ Sicherstellung, dass die in der Supply Chain erhalten Daten integer sind ■ Besonders: Gewährleistung der Datenintegrität in Bezug auf Besitzverhältnisse (physisch und digital) [1] ■ Durchführung von Verifikationsprozessen ■ Konsistente Synchronisierung von Daten ■ Aufwand für Prüfung/ Revision gering („Auditability“) ■ Gesicherte Datenintegrität über die Supply Chain hinweg ■ Unabänderbarkeit ○ Fälschungssichere Datenspeicher ○ Keine (unabsichtliche) Änderung der Daten innerhalb des eigenen Systems (z.B. durch Fehler)
Ausfall-Stabilität und Fehler-Widerstand	■ System bleibt im Normalfall stabil einsatzbereit, auch im Fall, dass ein Node ausfällt ■ System ist fehlerresistenter durch kontinuierliche Prüfung der Transaktionen und Angaben durch alle Systemteilnehmer
Peer-to-Peer Netzwerke	■ Möglichkeit zur Teilnahme der Kunden im Entstehungsprozess (kundeinindividuelle Massenproduktion) ■ Mögliche Einbindung aller Stakeholder und Kollaboratoren über den gesamten Product Life Cycle hinweg
Hohe Transparenz	■ Lückenlose Dokumentation aller Transaktionen ■ Bei Open Source/Public Blockchain: alle Prozesse einsehbar und Systemlogik öffentlich ○ Kein „Zurückhalten von Informationen“ möglich ■ Aufwand für Prüfung/ Revision gering („Auditability“) ■ Fehlerentstehung in Produkten potenziell leichter nachforschbar ■ Fehlerquellen in der Produktentstehung potenziell leichter identifizierbar
Anonymität / Pseudonymität	■ Möglichkeit zur Teilnahme am Blockchain Netzwerk entweder durch direkte Identifikation oder mittels Pseudonyms (Public Key) ■ Möglichkeit der Erhöhung der Anonymität durch spezielle Systemarchitektur.[2]
Realtime-Transaktionen / Automatisierte Smart Contract Ausführung	■ Einigung über Transaktionen in Realtime ■ Automatisierte Ausführung einer festgelegten Programmlogik durch Smart Contracts ohne Notwendigkeit einer zusätzlichen Bestätigung einer weiteren Instanz ■ Bietet Möglichkeiten zur potenziell erhöhten Kollaboration, besonders im Rahmen der Produktentstehung ■ Festlegung von Szenarien und automatische Ausführung

[1] vgl. Ploom T., 2016, 131f
[2] Siehe: Monero, Bitcoin Cash, The Verge, Zcash

Mikrotransaktionen	■ Möglichkeit zur automatisierten Übertragung von Mikrotransaktionen ○ Früher ohne Blockchain aufgrund des hohen administrativen Aufwandes tendenziell unpraktikabel ■ Möglichkeit zur Nutzung von IoT-Geräten
"Trustlessness" [1]	■ Möglichkeit zum Agieren innerhalb eines Netzwerkes ohne die anderen Teilnehmer kennen oder ihnen vertrauen zu müssen ■ Anonymes Vertrauen[2]

Unter Betrachtung der oben angeführten Aspekte, fallen zahlreiche Nutzungsmöglichkeiten auf, die im Product Life Cycle zum Einsatz kommen können.

Insbesondere, da im industriellen Umfeld bereits kleine Effizienzsteigerungen einen signifikanten Marktvorteil bringen können und die Reduzierung von Folgekosten einen erheblichen finanziellen Aspekt darstellt, scheint absolut realistisches Potenzial in der Nutzung der Blockchain-Technologie zu liegen.

Insbesondere auch in Bezug auf die möglichst frühe Fehlererkennung und den dadurch verbundenen Kostenvorteil wie ebenfalls in „CAx für Ingenieure" von Vajna et al. beschrieben wird. Unter diesem Gesichtspunkt können Blockchain-Systemen durch die erhöhte Transparenz und die sichere Kollaborationsmöglichkeit ein hohes Nutzungspotenzial zugeschrieben werden.[3]

3.1.5 Nachteile und Limitierungen der Blockchain-Technologie im Rahmen des Product Life Cycle

Insbesondere durch den Hype, den die Blockchain-Technologie durch den 2017 stattfindenden Bullenmarkt erfahren hat, ist diese oft in sehr gutem Licht präsentiert worden. Dabei darf man jedoch nicht vergessen, dass diese Technologie so wie alle anderen auch ihre Schwächen und Limitierungen besitzt. Darum gilt es auch hier vor dem Einsatz die Vor- und Nachteile einer Blockchain-Anwendung gegeneinander aufzuwiegen, um beurteilen zu können, ob der Blockchain-Einsatz einen Vorteil gegenüber einem zentralisierten System bietet oder nicht doch durch ihre Limitierungen eher als nachteilig betrachtet werden muss.

Zusätzlich ist hier zu erkennen, dass manche Aspekte sowohl als Vorteil als auch als Nachteil gezählt werden können. Die entsprechende Auswirkung des technologischen Aspekts hängt somit vom jeweilige Use Case ab.

[1] vgl. Public versus Private Blockchains White Paper, 2015, Version 1.0
[2] vgl. Ploom T., 2016, S.130f
[3] vgl. Vajna et al., 2018, S. 18f

Tabelle 3-2 Nachteile und Limitierungen der Blockchain Technologie

Aspekt	Nachteil oder Limitierung im Product Life Cycle
Keine Standards und Rechtssicherheit	■ Aufgrund der Neuartigkeit der Technologie haben sich noch keine Standards entwickelt ○ ISO Organisation arbeitet an Standards, hat aber noch nichts veröffentlicht ■ Ebenso besteht noch keine rechtliche Faktenlage zur Nutzung von Blockchains ○ Insbesondere fehlen Standards und Urteile in Bezug auf Smart Contracts ■ Fehlende Standards stellen potenzielles Hindernis für branchenweite Lösungen dar ■ Fehlende Standards stellen potenzielles Hemmnis für Entscheidungen zur Nutzung der Blockchain-Technologie dar
Identität	■ Preisgabe eines Pseudonyms bei jeder Transaktion ○ Pseudonym jedoch nicht absolut anonym
Hohe Rechenpower und Redundanz	■ Je nach Blockchain: Alle (vollwertigen) Netzwerk-Teilnehmer führen alles aus ■ Je nach Blockchain: Jeder (vollwertige) Node braucht entsprechende Rechenkapazität, um am Netzwerk teilnehmen zu können
Kritische Masse an Teilnehmer muss gegeben sein, um Sicherheit zu gewährleisten	■ Erst ab einer gewissen Anzahl an Teilnehmern kann ein Blockchain-System als sicher gesehen werden. ■ Kritische Anzahl an Teilnehmern muss im Rahmen der Unternehmens-Logik möglich sein
Hohe Transparenz / reduzierte Daten-Privatsphäre	■ Alle Teilnehmer sehen alle Transaktionen und Inputs in Blockchain und Smart Contracts ○ Konkurrenten können Firmendetails und Firmenlogik sehen ■ Nur wenige Plattformen ermöglichen derzeit „private Transaktionen“
Skalierbarkeit	■ Nicht alle Systeme können beliebig auflskaliert werden bzw. sind im Zuge einer Auf-Skalierung nicht gleich effizient
Kollaboration und Zustimmung aller Beteiligten[1]	■ Jeder Teilnehmer eines potenziellen Blockchain-Netzwerks muss einer Umstellung und Teilnahme zustimmen und die entsprechende Infrastruktur schaffen ○ Vermutlich entsprechende Hemmschwellen aufgrund Neuartigkeit der Technologie ○ Schwierig mit bestehenden zentralisierten Systemen kombinierbar, sollte ein Teilnehmer nicht zustimmen

[1] vgl. McLean S. & Deane-Johns S., 2016, S.6

Schnittstellen zur realen Welt	■ In den meisten Fällen besteht Bedarf Input aus Quellen außerhalb des Blockchain-Netzwerks zu bekommen („Oracle“) ○ Dieser Input muss entsprechend sicher und verifiziert sein ○ Die Blockchain kann noch so sicher sein, wenn der gewünschte Input korrumpiert ist, unterminiert das das gesamte System ■ Physische Dinge benötigen für die Darstellung in der Blockchain eine virtuelle Repräsentation. ○ Ein geeignetes Konzept hierfür muss je nach physischem Ding gefunden werde ○ Viele Unternehmen hinken noch der Digitalisierung ihrer Prozesse und Dokumente per se hinterher. Dieser Schritt muss abgeschlossen sein, um überhaupt eine Blockchain verwenden zu können
Transaktionsgeschwindigkeit	■ Je nach Blockchain-System: Transaktionsgeschwindigkeiten liegen teilweise unter dem Niveau einer sinnvollen Nutzbarkeit ○ Auswahl eines ausreichend performanten Systems notwendig ○ Insbesondere bei IoT Anwendungen hat dieser Punkt eine hohe Relevanz
Schwächen bei Interoperabilität	■ Datenaustausch zwischen unterschiedlichen Blockchains stellt noch eine Hürde dar ○ Teilweise bestehen Möglichkeiten zum Datenaustausch zwischen Blockchains mit dem gleichen Protokoll („Sidechains“) ■ Ebenso der Datenaustausch mit bestehenden Systemen stellt noch keine gebräuchliche Standardfunktion der meisten Systeme dar
Zykluszeit (wie schnell finden Transaktionen satt?)	■ Zykluszeit, in der ein neuer Block fixiert wird, hängt stark vom Blockchain-System ab und ist bei bestehenden Systemen tendenziell nicht anpassbar. ○ Stark abhängig vom Use Case, darum tendenziell wichtiges Ausschlusskriterium
Abhängigkeit von der medialen Darstellung mit Fokus auf Kryptowährungen	■ Nach wie vor wird Blockchain medial mit Bitcoin und Kryptowährungen gleichgesetzt ○ Eigentliche Technologie steht aufgrund dieses medialen Fokus immer wieder im Hintergrund ○ Entwicklung der Technologie wird tendenziell mit der Entwicklung des Kurswertes von Kryptowährungen gleichgesetzt

Wenig vorhandenes Know-How & Personal-ressourcen	■ Allgemeines Verständnis für Blockchain-Technologie noch nicht sehr ausgeprägt ○ Verhältnismäßig wenig wissenschaftliche Publikationen ○ Begriff Blockchain wird oft mit Bitcoin gleichgesetzt ○ Wenig Know-How über mögliche Ausprägungen der Block-chain-Technologie ■ Viele potenzielle Use Cases aufgrund fehlendem Know-How noch nicht entdeckt bzw. in sehr frühem Entwicklungsstand ○ Stellt erhöhte Schwierigkeit dar zu beurteilen, ob Blockchain eine praktikable Lösung darstellt ■ Bei konkreter Anwendung: Mangel an Personalressourcen mit ent-sprechenden Kompetenzen ○ Z.B. bei Ethereum Smart Contracts Programmierung: man benötigt Entwickler mit Solidity Erfahrung
Speicherkapazität – Größe der Blockchain	■ Je nach Ausprägung und Informationsgehalt der Blöcke kann die Speicherung der gesamten Blockchain ein Problem darstellen ○ Beispiel: Anfang des Jahres 2019 beträgt die Gesamtgröße der Bitcoin-Blockchain bereits rund 200 GB, bei einer durch-schnittlichen Blockgröße von 1,22 MB und insgesamt eine Gesamtzahl von 390.000.000 Transaktionen. ○ Bei Blockchains mit einer signifikant höheren Transaktions-rate und mehr Daten pro Block reicht die Speicherkapazität handelsüblicher Computer bald nicht mehr aus ○ Besonders im IoT Bereich, ist die Speicherkapazität der Ge-räte beschränkt und somit ein Workaround tendenziell not-wendig.

Aufgrund der Neuartigkeit der Technologie und der noch fehlenden sich durchgesetzten Standards, fehlt es noch an einfach zugänglichen und allgemein verwendbaren Lösungen. Verschiedene sich in Entwicklung befindlichen Systeme haben verschiedene Ausprägungen, die nicht immer auf die konkreten Bedürfnisse anpassbar sind.

Die Tatsache, dass viele Unternehmen der Digitalisierung ihrer Prozesse per se hinterherhinken, stellt die Einführung von Blockchain-Systemen vor eine weitere große Hürde, auch wenn der Einsatz prinzipiell eine gute Lösung wäre. Dementsprechend liegt die Vermutung nahe, dass derzeit noch nicht die volle Nutzung der potenziellen Vorteile von Blockchain-Systemen möglich bzw. praktikabel ist.

3.1.6 Entscheidungsmodelle über die Verwendung von Blockchains

Betrachtet man nun die hier dargelegten Vorteile und Limitierungen der Blockchain-Technologie, stellt sich vermutlich sehr schnell die Frage, in welchen Fällen die Vorteile die Nachteile

überwiegen und ob eine jeweilige Lösung nicht auch über ein zentralisiertes System zum Beispiel mit entsprechenden Sicherheitsmechanismen einen höheren Nutzen bei geringerem Aufwand erbringen könnte.

Nach Ploom T. gibt es hier zwei Aspekte, denen man besondere Beachtung schenken sollte:[1]

- „Wie hoch ist das „Vertrauen“ innerhalb einer Organisation?“
- „Muss die Datenintegrität der durchgeführten Transaktionen nachgewiesen werden?“

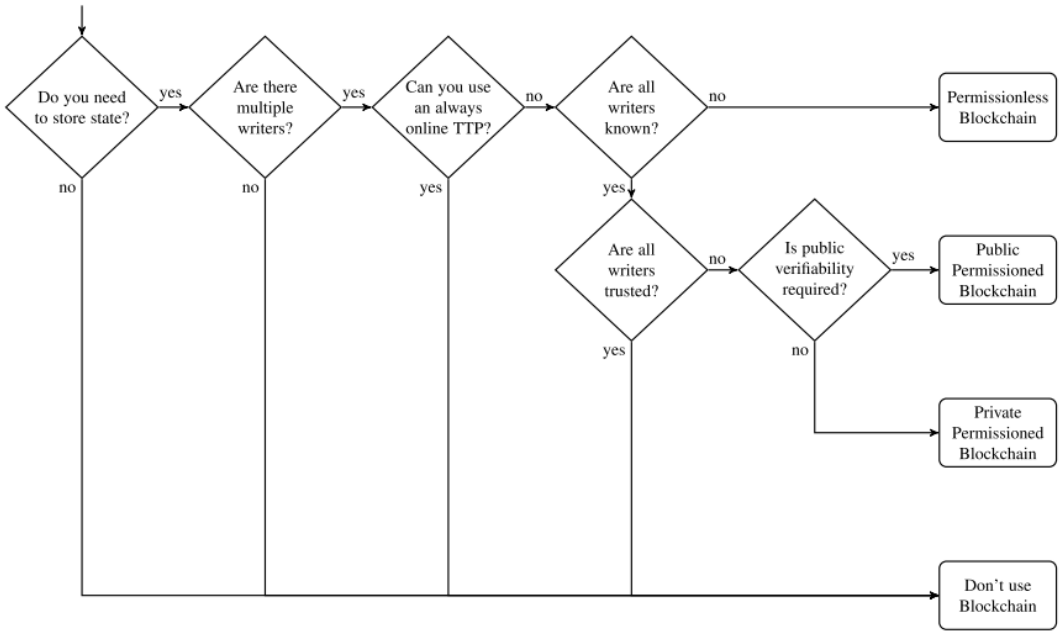
Diese beiden Fragen scheinen besonders dann von hoher Relevanz zu sein, wenn es um Datenaustausch über die Grenzen von Organisationen geht. Dabei kann die Organisationseinheit sowohl eine Unternehmensabteilung oder eine komplette Unternehmens-Gruppe sein, über deren Grenzen hinweg Daten ausgetauscht werden. Und auch der Begriff Vertrauen beschränkt sich nicht auf böswillige cyberkriminelle Aktivitäten. Ebenso simples menschliches Versagen oder technische Fehler können dazu führen, dass Daten nicht 100%ig vertrauenswürdig sind oder verloren gehen. Sobald innerhalb einer Organisation diese Punkte zu einem Risiko werden, hat es Sinn sich über die Nutzung einer Blockchain-Lösung Gedanken zu machen.

Wüst K. und Gervais A., 2017 gehen hier in ihrem Paper „Do you need a Blockchain?“ noch einen Schritt weiter und liefern einen Flow Chart durch dessen Verlauf man weitere Klarheit erlangt.[2]

Abbildung 3-4 zeigt den von Wüst und Gervais entwickelten Entscheidungsbaum, ob die Nutzung einer Blockchain sinnvoll sein kann. Neben den hier schon beschriebenen Fragestellungen gehen die dabei auch auf den Aspekt ein, ob die Blockchain-Lösung hierbei Public oder Private sein sollte und auch ob der Zugang zum Netzwerk einer Zustimmung durch eine zentrale Instanz bzw. den anderen Netzwerkteilnehmern erfolgen muss, oder keine Zustimmung notwendig ist. (Permissioned/ Permissionless)

[1] vgl. Ploom T., 2016, S.131
[2] vgl. Wüst K. & Gervais A., 2017, S.1ff

Abbildung 3-4: Entscheidungsbaum zur Frage "Do you need a Blockchain?"[1, 2]



Zu erkennen ist hierbei, dass ab dem Knotenpunkt „Can you use an always online TTP“ (TTP = Trusted Third Party) die Unterscheidung getroffen wird, ob eine zentralisierte, (relationale) Datenbank möglich ist oder nicht. Der Systemadministrator eines solchen Systems würde nämlich eine solche TTP darstellen.

Wenn nun über den gesamten Product Life Cycle mehrere Parteien an der Entstehung eines Produkts mitwirken und sichergestellt werden soll, dass volle Datenintegrität und -konsistenz gewährleistet ist, jedoch kein hundertprozentiges Vertrauen der einzelnen Parteien zueinander existiert, stellt ein Blockchain-Netzwerk eine nutzbare Lösung für die Datenübertragung dar.

Für den Beispiels-Fall, dass die Produktdaten aus Gründen der Transparenz auch öffentlich einsehbar sein sollen, etwa für potenzielle Kunden, stellt z.B. eine Public Permissioned Blockchain eine mögliche Lösung dar. Dadurch wären die Schreibrechte zwar beschränkt auf die direkten Teilnehmer in der Supply Chain, jedoch könnte sich durch die öffentlichen Leserechte jede beliebige Partei von der Datenintegrität überzeugen.

Die im Rahmen des Product Life Cycle identifizierten und kategorisierten Use Cases werden nun im folgenden Kapitel vorgestellt. Da diese Use Cases jedoch möglichst generisch beschrieben werden, ist es wichtig zu erwähnen, dass eine finale Entscheidung ob ein Blockchain-System die beste Lösung ist, vom konkreten Fall in der Realität abhängt und einzeln zu prüfen ist. Bei Problemstellungen in der Realität, die den hier beschriebenen Use Cases entsprechen,

[1] Abb. 3-4 aus Wüst K. & Gervais A.,2017, S.3
[2] ANMERKUNG: TTP = Trusted Third Party; also eine zentrale Autorität der man vertraut

kann es in der Realität durch spezielle technische oder organisatorische Eigenheiten trotzdem die bessere Wahl sein, ein zentralisiertes System zu verwenden.

3.2 Identifizierte Use Cases im Rahmen des Product Life Cycle

Aufbauend auf den im vorhergehenden Teil der Arbeit vorgestellten grundlegenden Konzepten der Blockchain - Technologie und dem durch die Beschreibung des Product Life Cycle und des Umfang von Industrie 4.0 und Internet of Things aufgespannten Rahmen, werden in diesem Teil nun bestehende Blockchain Use Cases vorgestellt und eingeordnet. Wie bereits in der allgemeinen Einleitung erwähnt, wird dabei von Use Cases mit Fokus in Richtung Finanztransaktionen abgesehen und speziell auf Use Cases fokussiert, die einen Nutzen im Rahmen eines industriellen Umfelds aufweisen.

Die Strukturierung der Use Cases erfolgte dabei wie in Kapitel „Beurteilung, Kategorisierung und Extrapolation“ beschreiben mittels der Mind-Mapping Methode, wobei im Zuge der Recherche zu dieser Arbeit die als relevant und aussagekräftig befundenen Anwendungsfälle in dieser gesammelt wurden.

Diese Sammlung erhebt jedoch keinen Anspruch auf Vollständigkeit. Insbesondere durch die Schnelllebigkeit der gesamten Thematik, wurde hier bewusst eine konkrete Auswahl getroffen, um diese in weiterer Folge im Detail und in einem dieser Arbeit entsprechendem Ausmaß zu beleuchten.

3.2.1 Peer-to-Peer Transaktionen und Verrechnung

Die erste Kategorie an Use Cases stellt die Nutzung der Blockchain in einer Form dar, die der ursprünglichen Nutzung der Blockchain-Technologie durch Bitcoin recht nahekommt.

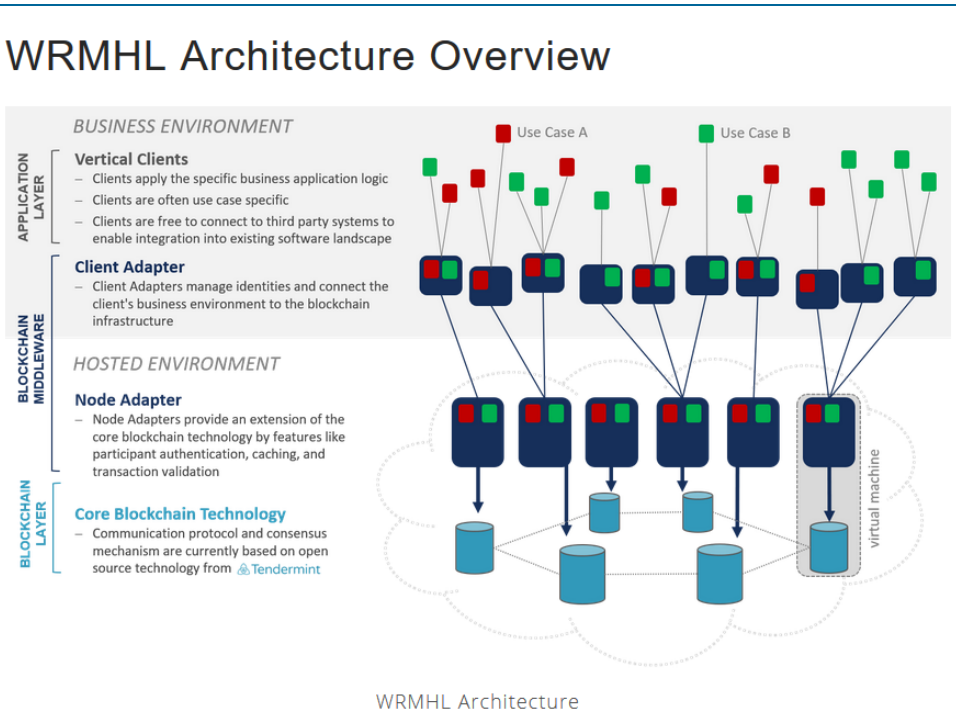
Dabei geht es vor alle darum, gewisse Werte innerhalb eines Peer-to-Peer Netzwerkes zu transferieren. Wobei es sich hier nicht um finanzielle Werte handeln muss. Sehr verbreitet ist dieser Use Case zum Beispiel im Energiesektor, wo zum einen ein Teil des Energiehandels zwischen verschiedenen Energieanbietern über eine Blockchain abgehandelt wird oder ein Peer-to-Peer Energiehandel zwischen Verbrauchern stattfinden kann. Dabei kann der Datentransfer nur die Informationen bezüglich des Energietransfers beinhalten, oder es ist natürlich tendenziell auch möglich, die Verrechnung ebenfalls gleich per Blockchain durchzuführen.

Als Beispiel für die Nutzung von Blockchain-Systemen können die Projekte von Wien Energie[1] und TenneT[2] und Grid Singularity[3] genannt werden.

Wien Energie nimmt hier zum Beispiel am „Enerchain“ Projekt des Softwareanbieters Ponton teil, wo im Rahmen der Norddeutschen Energiewende 4.0 eine Energie-Handelsplattform aufgebaut wird, über die 30+ Energiehändler Strom und Gas in einem P2P-Tradingnetzwerks handeln können. Dabei soll vor allem ein gemeinsames Netzwerk ohne Lizenzkosten geschaffen und Blockchain Know-How aufgebaut werden.[4]

Als besonders spannend stellt sich hier die von Ponton eingesetzte WRMHL Architecture heraus, wie in Abbildung 3-5 zu sehen. Diese stellt ein praktikables Beispiel für den Einsatz von Konsortium-Blockchain-Systemen dar. Durch die Trennung von Applikations-Ebene, Middleware und Blockchain- bzw. Node-Ebene können Geschäfts-Logik und Blockchain-System verbunden werden und an die notwendigen Use Cases angepasst werden.[5]

Abbildung 3-5: Ponton WRMHL Architecture als Beispiel einer Umsetzungsmöglichkeit[6]



[1] vgl.https://smartcity.wien.gv.at/site/blockchain-im-energiesektor/ zuletzt gelesen am 10.02.2019
[2] vgl https://www.tennet.eu/de/unsere-kernaufgaben/innovationen/blockchain-technologie/ zuletzt gelesen am 10.02.2019
[3] vgl. https://gridsingularity.com/about/ zuletzt gelesen am 10.02.2019
[4] vgl. https://enerchain.ponton.de/ zuletzt gelesen am 10.02.2019
[5] vgl. https://ponton.de/wrmhl/ zuletzt gelesen am 10.02.2019
[6] Abb. 3-5 aus https://ponton.de/wrmhl/ zuletzt gelesen am 10.02.2019

Ein weiteres Beispiel für diese Art von Use Cases im Energiehandel stellt die Energy Web Foundation, der das Unternehmen Grid Singularty angehört, dar. Den Fokus legt das Projekt auf Einbindung der Konsumenten in den Stromhandel. Dabei sollen die Transaktionen zwischen Produzenten und Konsumenten sowie Konsumenten untereinander über ein Blockchain Netzwerk durchgeführt werden.[1]

Dadurch kann zum Beispiel die von Solarkollektoren am Dach eines Hausbesitzers erzeugte Energie direkt an einen Nachbarn verkauft werden, ohne dabei einen Energiehändler miteinbeziehen zu müssen. Ebenso der Ausgleich von Lastspitzen und -einbrüchen kann durch verteilte Energiespeicher in Haushalten durch ein dezentrales Netzwerk durchgeführt werden.

Besonders erwähnenswert aus diesem Projekt ist, dass als technologische Basis hier der Ethereum-Code genutzt wird, jedoch entsprechende Anpassungen am Code vorgenommen wurden, um eine adaptierte Blockchain zu erstellen.[2]

Dazu zählen:[3]

- die Umstellung des Consensus-Mechanismus auf Proof of Authority zur Erhöhung der Skalierbarkeit
- Erstellung verschiedener Client-Versionen, um auch weniger leistungsstarke Geräte an die EW-Chain anbinden zu können
- Möglichkeit zur Regelung der Teilnahmeberechtigungen („Permissioning“) während die Blockchain weiterhin öffentlich einsehbar ist
- Ermöglichung von „Private Transactions“ zur Erhöhung der Privatsphäre
- Zugang zu einer Web Assembly Virtuellen Maschine die zum einen leistungsfähiger als die Ethereum Virtual Machine ist und zum anderen es Entwicklern ermöglicht mit anderen Programmiersprachen als mit Solidity zu arbeiten.

Somit zeigt dieses Projekt sehr gut die Möglichkeit, wie der Code von bestehenden Systemen (hier: Ethereum) für die speziellen Use Case Anforderungen angepasst werden kann. Die im Energy Web Chain angepassten Aspekte stellen auch potenzielle Vorteile in der Nutzung der Blockchain im industriellen Umfeld dar und können daher auch als Referenz herangezogen werden.

Dem gegenüber steht in dieser Kategorie auch der Fokus auf die automatisierte Verrechnung von Transaktionen wie etwa bei Carsharing-Diensten[4], oder etwa Mikro-Transaktionen beim induktiven Laden von Elektro-Fahrzeugen im Straßenverkehr oder bei Maut-Systemen wie es mit ARTIS[5] durchführbar wäre.

[1] vgl. https://energyweb.org/ zuletzt gelesen am 10.02 2019
[2] vgl. Hartnet S. et al., 2018, S.12
[3] vgl. Harntet S. et al., 2018, S.13f
[4] vgl. https://shareandcharge.com/ zuletzt gelesen am 20.01.2019
[5] vgl. https://artis.eco/en/dapps zuletzt gelesen am 20.01.2019

Tabelle 3-3 Generische Use Case Definition: Peer-To-Peer Transaktionen und Verrechnung

Name	Peer-to-Peer Transaktionen und Verrechnung
Ziele im Kontext	■ Sichere Transfers ■ Gemeinsames Netzwerk ■ Automatisierung
Akteure	■ Netzwerk auf Anbietern und Kunden ○ Rollen nicht fixiert und können wechseln
Kurzbeschreibung	Austausch von Daten oder Werten im Rahmen eines gemeinsamen Netzwerkes. Optional: automatisierte Verrechnung bezüglich des stattgefundenen Austausches
Merkmale	■ Fokus auf Transaktionen ■ Schneller und sicherer dezentraler Datenaustausch ■ Optional aber nicht zwingend: Automatisierte Verrechnung ■ Zusammenbringen von Anbietern und Verbrauchern über ein gemeinsames System ■ Reduzierung der Lizenzkosten ■ Einheitliches Netzwerk aller Teilnehmer

Mögliche Nutzung im industriellen Umfeld

Die oben dargelegten Anwendungsmöglichkeiten, können ebenso auf das Industrielle Umfeld umgelegt werden. Denkbar wäre hier zum Beispiel die Nutzung von Abwärme im Zuge des Produktionsprozesses, oder die Nutzung von Solarkollektoren an Fabriksdächern zur Energieerzeugung und direktem Verkauf an andere Konsumenten, um die Produktionskosten insgesamt zu senken. Der direkte Verkauf ohne Zwischenhändler hätte in dem Zusammenhang den Vorteil, die Marge direkt zu erhöhen.

Ebenso vorstellbar wäre auch die Nutzung von Mikrotransaktionen im Rahmen eines „Machine as a Service“ Konzept, bei dem Produktionsmaschinen nicht komplett gekauft werden, sondern vom Hersteller geleast und die Nutzung der Maschine direkt über eine Blockchain verrechnet wird.

Ebenso könnte zum Beispiel die Wartung von Produktionsmaschinen an einen externen Dienstleister ausgelagert sein. Mittels in der Maschine verbauter IoT-Geräte (siehe Kapitel „IoT“) könnte die Maschine über eine Blockchain die Wartung beauftragen und bei Erfüllung die Zahlung an den externen Dienstleister automatisch durchführen. Vorteil dieses Systems wäre der durch die hohe Automatisierung reduzierte administrative Aufwand, die lückenlose Aufzeichnung der durchgeführten Wartungen und die bedarfsorientierte Auftragserstellung.

3.2.2 Supply Chain

Dieser Use Case stellt eine bereits verhältnismäßig verbreitete Nutzung der Blockchain dar.

Entsprechend Santos & Eisenhardt, 2005, stellen die Hauptvorteile von IT-Nutzung im Rahmen einer Supply Chain die Reduzierung von administrativen Tätigkeiten, die Reduzierung von Kosten durch Abstimmung mit anderen Teilnehmer in der Supply Chain und die Reduzierung von menschlichen Fehlern dar.[1]

Außerdem kann davon ausgegangen werden, dass Datensicherheit, Datenintegrität und Nachverfolgbarkeit, wie es Blockchain-Systeme möglich machen, weitere Vorteile im Rahmen einer Supply Chain Infrastruktur bieten.

Wenn man davon ausgeht, dass sich viele Supply Chains über Staatsgrenzen hinweg erstrecken und somit ebenso die darauf bezogenen administrativen Prozesse wie etwa im Zoll eine signifikante Rolle spielen, erscheint das Optimierungspotenzial der Informationsweitergabe als wirtschaftlich relevanter Faktor. Durch die lückenlose Aufzeichnung und die Einsehbarkeit durch offizielle Stellen hat ein solches System das Potenzial den administrativen Aufwand zu reduzieren.

Ein bekanntes Projekt, das sich bereits in einem fortgeschrittenen Entwicklungsstadium befindet, stallt „IBM Food Trust“ dar, das IBM unter anderem in Kooperation mit WalMart betreibt.[2,3]

Diesbezüglich beschreibt IBM die immer größere werdenden Komplexität der Lebensmittel Supply Chain und der verbreiteten Datennutzung als konkrete Herausforderungen. In diesem Zusammenhang ist das Ziel von IBM Food Trust mittels einer Blockchain Plattform die Transparenz zu erhöhen und Vertrauen zu schaffen. Insbesondere auch die schnelle Aufklärung von Problemen, wie die Quelle von Verunreinigungen, stellen sich in der Branche als wichtige Punkte heraus.

Aufbauend auf Hyperledger Fabric, stellt IBM Food Trust den Nutzern eine Informationsplattform für die ganze Supply Chain hinweg zur Verfügung. Diese Plattform ist dabei in mehrere Module aufgeteilt und bietet Funktionen für Rückverfolgung von Produktwegen inkl. Echtzeit-Status, Zertifikatsvergabe und Datenaustausch mit verschiedenen anderen Teilnehmern in der Supply Chain. Dabei wird das System explizit durch Zugangsregelungen abgesichert, wodurch die Unternehmensdaten nicht öffentlich einsehbar sind, sondern nur dem Bedarf und der Erlaubnis des Datenbesitzers entsprechend.[4]

Walmart etwa nutzt die Plattform im Rahmen von zwei Pilotprojekten konkret in Bezug auf deren Mango und Schweinefleisch Supply Chains. Diese stellen zwei recht umfangreiche Cases dar, da hier die Supply Chain über stattliche Grenzen hinweg über viele Stationen besteht.[5]

---

[1] vgl. Santos M. & Eisenhardt M., 2005, S.491ff
[2] vgl. Galvin D., 2017, S.1ff
[3] vgl. https://www.ibm.com/blockchain/solutions/food-trust zuletzt gelesen am 21.01.2019
[4] vgl. About IBM Food trust, S.5ff
[5] vgl. Galvin D., 2017, S. 11f

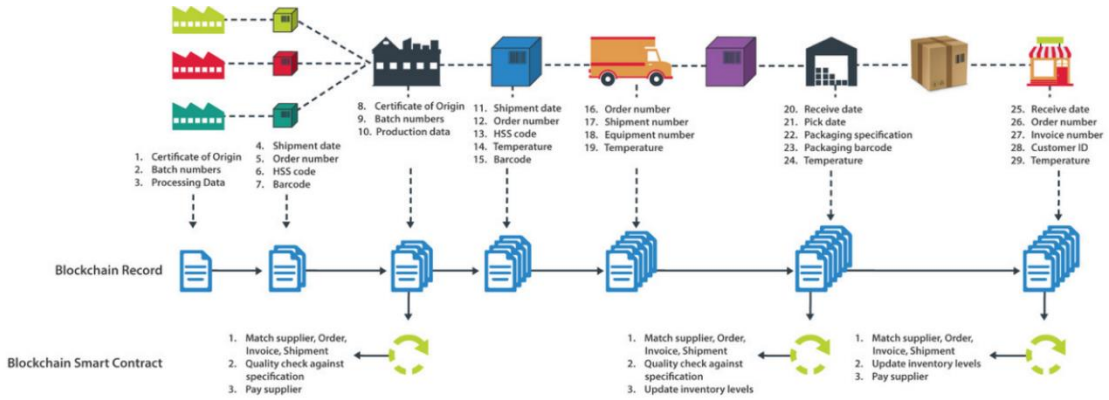
Hier zeigt sich vor allem auch der Vorteil eines gemeinsamen Systems, das von den vielen Teilnehmern genutzt werden kann, ohne eine zentrale vertrauenswürdige Autorität zu benötigen. Ein Aspekt, der mit zunehmender Globalisierung weiter an Relevanz gewinnt, wenn übliche Supply Chains sich von der Plantage, über Händler, Spediteure, Einzelhandel und Kunden erstrecken, die sich potenziell opportun verhalten könnten.

Insbesondere wäre hier auch eine Kombination mit IoT-Geräten denkbar. Wenn z.B. im Verpackungszentrum ein Sensor beigefügt wird, der die Sicherstellung der notwendigen Kühltemperatur misst und dabei auf die Blockchain überträgt. Sollte hier ein Fehler passieren, wäre das sofort im System sichtbar und nachvollziehbar. Dadurch können potenzielle Fehlerquellen schnell identifiziert werden.

Eine weitere Möglichkeit zur Nutzung er Blockchain im Supply Chain Management stellt die IRC Group vor. In der Abbildung 3-6 ist der vorgestellte generische Use Case von IRC zu sehen, wobei über die gesamte Supply Chain wie oben beschrieben Einträge in die Blockchain erfolgen. Der ergänzende Aspekt bezieht sich auf die gleichzeitige Nutzung von Smart Contracts zur Überprüfung von Lieferung und Bestellung und der automatisierten Zahlung an den Lieferanten.[1]

Betrachtet man diesen Zugang, ist davon auszugehen, dass dadurch der administrative Aufwand für die einzelnen Schritte signifikant gesenkt werden und somit die Nutzung der Blockchain ebenso als Instrument zur Kostensenkung angesehen werden kann.

Abbildung 3-6: Supply Chain Use Case von IRG Group[2]



[1] vgl. https://ircgroupglobal.com/harnessing-blockchain-in-the-scm-logistics-space/ zuletzt gelesen am 23.01.2019

[2] Abb. 3-6 aus https://ircgroupglobal.com/harnessing-blockchain-in-the-scm-logistics-space/ zuletzt gelesen am 23.01.2019

Tabelle 3-4 Generische Use Case Definition: Supply Chain

Name	**Supply Chain**
Ziele im Kontext	■ Gewährleistung der Nachverfolgbarkeit von Produkten ■ Sicherstellung der Unveränderbarkeit der Daten-Historie ■ Schnelle Aufklärung von Missständen ■ Kostenreduktion
Akteure	■ Teilnehmer der Supply Chain (Entwicklung, Produktion, Distribution, Konsumenten, After-Life)
Kurzbeschreibung	Im Rahmen des Product Life Cycle bildet ein Blockchain-System ein Informationsnetzwerk über die gesamte Supply Chain hinweg. Dabei werden die relevanten Produktdaten in die Blockchain gespeichert und sind entsprechend im Bedarfsfall zugänglich.
Merkmale	■ Netzwerk über gesamte Supply Chain ■ Digitale Abbildung eines Produktes im Verlauf ○ Abbildung des Weges ○ Abbildung des Status ■ Ermöglichung einer Vertrauensbasis über viele verschieden Teilnehmer der Supply Chain hinweg, ohne dass sich diese kennen müssen ■ OPTIONAL: Automatisierte Abrechnung nach erfolgten Transaktionen

Mögliche Nutzung im industriellen Umfeld

Der entsprechende Einsatz eines Blockchain-Netzwerks im Rahmen eines technischen Product Life Cycle ist, wie bei den beschriebenen Cases, sehr gut vorstellbar.

Geht man nun davon aus, dass sich bereits jetzt ein Großteil der technischen Produkte aus einer komplexen Kombination von Einzelteilen bestehen, die oft durch Zulieferer über eine nicht minder komplexe Supply Chain das Endfertigende Unternehmen erreichen, kann man diesem Use Case nun eine hohe Relevanz zusprechen.

Denkt man auch weiter und bezieht die externe Entwicklung von CAD-Daten, zB. für 3D Druck, mit ein, kann bereits auf Ebene der virtuellen Erstellung der Produkte eine hohe Transparenz und Nachvollziehbarkeit erreicht werden. So können durch ausgelagerte Entwickler erstellte CAD-Daten mittels Multisignatur-Mechanismen auf der Blockchain von mehreren Stellen im eigenen Unternehmen freigegeben werden und entsprechend der im Vorfeld gestellten Anforderungen verifiziert werden. Kommt es dann in weitere Folge zu einem Problem aufgrund eines Konstruktionsfehlers, kann rasch rückverfolgt werden, wo bei welchem Zulieferer die Fehlerquelle liegt. Ebenso die bei der Zulieferung ganzer Baugruppen, hätte das Unternehmen, das

mit der Endmontage beauftragt ist, die Möglichkeit den Verlauf der Einzelteile in der Baugruppe nachzuverfolgen.

Als Hemmschwelle kann man davon ausgehen, dass viele Zulieferer der Freigabe von Daten skeptisch gegenüberstehen, da dadurch etwaigen Konkurrenten unbeabsichtigt Einsicht gewährt werden könnte.

Zur weiteren Abgrenzung gibt es auch die Möglichkeit einzelne Produkte in eigenen Side-Chains abzubilden, die über eine Main-Chain kommunizieren können. Dadurch entsteht eine starke Abtrennung, ohne explizit für jedes Produkt eine komplett eigenständige Blockchain schaffen zu müssen. Sollte es in der späteren Phase des Product Life Cycle zu einem Produktrückrufs aufgrund eines konkreten Einzelteils kommen, kann durch ein solches System auch schnell nachvollzogen werden, welche Endprodukte im Endeffekt betroffen sind.

Vergleicht man nun diese Fälle mit der Realisierung in einem herkömmlichen PLM-System mit zentralisiertem Aufbau, müsst ein Teilnehmer die Verwaltungshoheit über ein System und die Funktion gewährleisten, oder eine Möglichkeit bestehen, dass die PLM-Systeme alles Teilnehmer miteinander kommunizieren können. Dieser Aufbau wäre sicherlich ebenso technisch realisierbar, dürfte jedoch einen erheblichen administrativen Aufwand darstellen. Es besteht das Potenzial, dass eine ausgereifte Blockchain-Plattform die Möglichkeit für eine einfachere und kostengünstigere umfassende Lösung zu bieten.

3.2.3 ID auf Blockchain

Einen verhältnismäßig einfachen Use Case stellt die Verifizierung von IDs mittels Blockchain dar. Dabei werden Identifikations-Informationen auf einer Blockchain abgespeichert und stehen dadurch für Identifikationsprozesse zur Verfügung. Im Gegensatz zu einem zentralen Anbieter, wie etwa Google, besitzt somit nicht der Eigentümer des Datencenters die Daten und überlasst dem Nutzer die Nutzung, sondern der ID-Eigentümer hat selbst die Kontrolle über seine Daten.

Einen kritischen Punkt stellt hierbei die Schnittstelle zur realen Welt dar, um zu gewährleisten das eine physische Person wirklich im Zusammenhang mit der Adresse, dem Public Key, auf der Blockchain steht. („Oracle“-Problem). Eine Lösung hierfür wäre die Beglaubigung der Public Keys zur Identität durch gewisse vertrauenswürdige Autoritäten.[1]
Dies würde natürlich in Bezug auf die Schnittstelle zur realen Welt die Informationseingabe entsprechend wieder zentral bündeln. Die Nutzung der so aber auf die Blockchain gelangten Daten wäre dann jedoch wieder dezentral.

Erweitern lässt sich dieses Konzept in Bezug auf die Aufzeichnung der einer ID zugehörigen Aktivitäten. Als Beispiel können hier Gesundheitsdaten von Bürgern genannt werden, die entsprechend dezentral gespeichert und verwaltet werden. Dadurch hätte der Bürger eben vollen

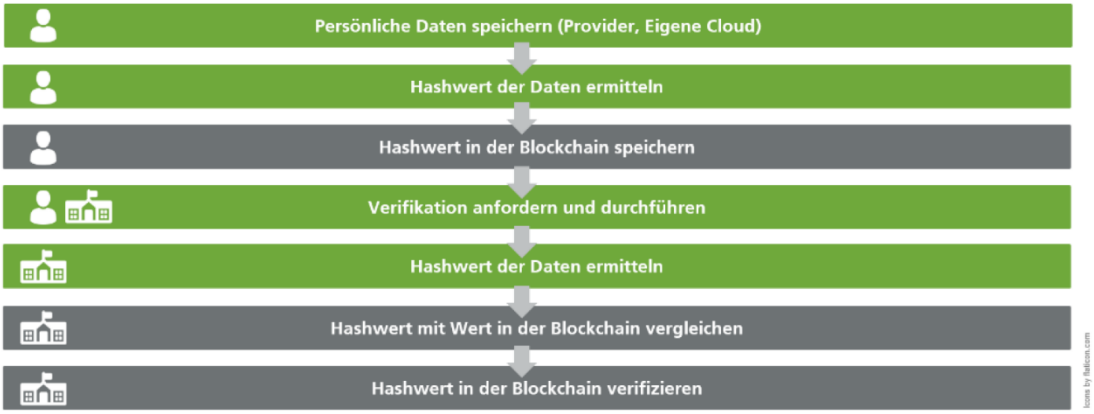
[1] vgl. https://www.informatik-aktuell.de/betrieb/virtualisierung/blockchain-trifft-digital-identity.html zuletzt gelesen am 21.02.2019

Zugriff und Kontrolle über die eigenen Daten und müsste nicht darauf vertrauen, dass eine zentrale Stelle diese sensiblen Daten korrekt und sicher verwaltet.

Dem entsprechend kann der ID-Eigentümer dann die Zugriffsrechte zu diesen Daten konkret selbst verwalten und zum Beispiel nur für einen begrenzten Zeitraum oder einen einmaligen Zweck gewähren. Aus Kapazitätsgründen ist es auch hier möglich, und je nach Fall auch erstrebenswert, nicht die Daten selbst auf der Blockchain abzulegen, sondern deren Hashwerte. Insbesondere das Speichern von personenbezogenen Daten in unverschlüsselter Form wäre ein kritischer Fall. Diese Hashwerte können jedoch äquivalent für Verifikationszwecke herangezogen werden.[1]

Abbildung 3-7 stellt einen beispielhaften Verifikationsprozess dar.

Abbildung 3-7: Verifikationsprozess mittels Hashwerts[2]



In konkreter Anwendung befindet sich eine Blockchain-basierte digitale ID zum Beispiel in der schweizer Stadt Zug. Im Zuge dieses Pilotprojekts, welches auf der Ethereum Blockchain basiert, werden bereits unter den teilnehmenden Bürgern Umfragen durchgeführt und es werden konkrete Anwendungen für die Bürger evaluiert, wie die Nutzung als Bibliotheksausweis, Park-Management und Fahrradverleih.[3]

[1] vgl. Kirstein F., Polzhofer M. & Eckert K., 2017, S.
[2] Abb. 3-7 aus Kirstein F., Polzhofer M. & Eckert K., 2017, S.12
[3] vgl. http://www.stadtzug.ch/de/bevoelkerung/dienste/digitaleid/?action=showthema&themenbereich_id=1587&thema_id=5295 zuletzt gelesen am 22.01.2019

Tabelle 3-5 Generische Use Case Definition: ID auf Blockchain

Name	**ID auf Blockchain**
Ziele im Kontext	■ Fälschungssicher ■ Kontrolle über Zugriff auf Daten in eigener Hand ■ Transparenz bezüglich der aufgezeichneten Daten ■ OPTIONAL: Sicherere Aufzeichnung der ID-bezogenen Aktivitäten
Akteure	■ ID-Eigentümer ■ Parteien mit Lese- oder Schreibrechten auf die Daten
Kurzbeschreibung	ID-bezogene Daten werden auf der Blockchain gespeichert und für Verifizierungszwecke genutzt.
Merkmale	■ Speicherung der ID-Informationen in einer Blockchain ■ OPTIONAL: Speicherung der ID-bezogenen Aktivitäten ■ Speicherung der ID-Daten an einem Ort und nicht Nutzung einer Vielzahl an Kopien

Mögliche Nutzung im industriellen Umfeld

Die Nutzung von digitaler ID auf der Blockchain ist im Rahmen der personenbezogenen Identität als eigener Use Case anzusehen. Im Rahmen des Product Life Cycle hat die alleinige Nutzung von digitaler Identität tendenziell wenig Nutzen.

Darum ist dieser Use Case im industriellen Kontext tendenziell als Sub Use Case für umfangreichere Anwendungen zu sehen und kann in spezifischer Form als Unterpunkt in den Use Cases der anderen Kategorien vorkommen.

3.2.4 (Digital) Assets & Intellectual Property

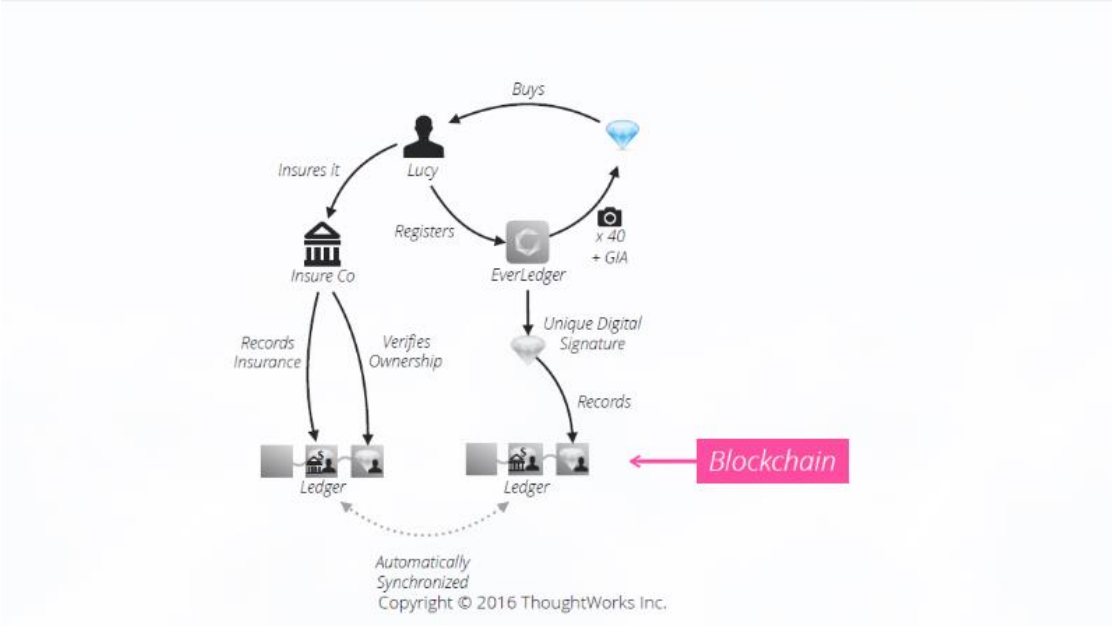
Diese Kategorie beschreibt jene Use Cases, die sich auf die Verwendung der Blockchain zum Verwalten und Nutzen von Assets beziehen. Diese Assets können entweder direkt digitale Assets beschreiben, oder auch eine Abbildung von physischen Assets darstellen und beschreiben eine beliebige Art von Vermögensgegenstand.

Ein bereits gut ausgereiftes Use Case Beispiel stellt hier die Echtheitsprüfung von Diamanten von Everledger dar.[1]
Das Unternehmen bietet eine auf IBMs Hyperledger basierende Plattform, über die die Echtheit von Diamanten verifiziert werden kann. Hierfür wird jeder Diamant mit einer Art Fingerabdruck versehen, der sich aus einer Anzahl von 40 Eigenschaften des Diamanten (Abmessungen,

[1] vgl. https://www.everledger.io/ zuletzt gelesen am 27.01.2019

Schliff, Farbe, etc.) zusammensetzt, welcher dann auf der Blockchain gespeichert wird. Dadurch wird für die physische Einheit „Diamant“ ein eindeutig zuordenbares digitales Abbild geschaffen. Diesem Abbild können nur Eigentumsrechte beigefügt werden, wodurch der rechtmäßige Eigentümer eines bestimmten Diamanten klar feststellbar ist und zum Beispiel im Fall von Diebstahl für Versicherungs-Prozesse und polizeiliche Aufklärung genutzt werden kann. Zugang zu der Plattform wird durch gebräuchliche API-Calls ermöglicht, wodurch auch die technologische Schwelle für die Nutzung geringgehalten wird.[1]
Everledger bietet diese Anwendung neben der Nutzung für Diamanten ebenso unter anderem für Edelsteine, Wein und Kunst an.[2]
Abbildung 3-8 zeigt in dem Zusammenhang die Abläufe die eine Käuferin (hier „Lucy“) auslöst, wenn sie einen Diamanten kauft und auf Everledger registriert. Sollte Lucy diesen Diamanten nun verkaufen, muss sie die auf Everledger gespeicherten Besitzrechte an den Käufer übertragen.

Abbildung 3-8: Schematische Darstellung der Everledger-Funktion[3]



Die größte Herausforderung stellt im Fall von physischen Assets sicherlich die Erstellung eines eindeutig zuordenbaren digitalen Fingerabdrucks dar. Sobald dieser Punkt erreicht ist, können die Abbildungen beliebiger physischer Dinge auf einer Blockchain gespeichert werden.

[1] vgl. https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ zuletzt gelesen am 27.01.2019
[2] vgl. https://www.everledger.io/industry-applications zuletzt gelesen am 27.01.2019
[3] Abb. 3-8 aus https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ zuletzt gelesen am 27.01.2019

Wenn es sich von vornherein um digitale Entitäten handelt, stellt die Schaffung eines Abbilds auf der Blockchain natürlich eine ungleich geringere Schwierigkeit dar. Dies hat zusätzlich zum Vorteil, dass im digitalen Zeitalter, wo Daten, Dokumente und Dateien problemlos einfach kopiert werden können, die Möglichkeit digitale Assets mit Besitzrechten zu versehen große ökonomische Relevanz hat.

So stellt zum Beispiel die Musikindustrie ein mögliches Anwendungsgebiet für eine solche Plattform für Besitzrechte dar. Dem entsprechend könnten die Musikrechte auf einer Blockchain gespeichert werden. Im Falle der Nutzung eines bestimmten Titels, können dann durch Smart Contracts automatisiert Zahlungen vom Nutzer an die betreffenden Stakeholder (wie Musiklabel, Produktionsfirma, Künstler) durchgeführt werden.[1]

Diese Stakeholder können mehrere Parteien sein, oder aber es könnte auch eine direkte Verbindung zwischen dem Ersteller und dem Nutzer geschaffen werden, ohne dass Kosten für Zwischenhändler anfallen. Dies birgt die Möglichkeit, dass sich somit die Kosten für den Endnutzer insgesamt reduzieren lassen. Im Beispiel der Musikindustrie, könnten somit die Hörer eines Titels direkte Zahlungen an den Künstler ausführen, ohne dies über Zwischeninstanzen abhandeln zu müssen.

Die Eindeutigkeit der Besitzrechte wäre durch das Hashing der Asset-Daten in Kombination mit einem Timestamp und Informationen zum Käufer eindeutig festlegbar. Dieser Hash ist dann problemlos verifizierbar.

Geht man einen Schritt weiter zu sicherheits-kritischen Informationen, können ebenso Dokumente problemlos verifiziert werden. Dabei wird ebenfalls der digitale Fingerabdruck eines Dokuments auf die Blockchain gespeichert. Etwa um zu dokumentieren, dass man zu einem gewissen Zeitpunkt im Besitz eines bestimmten Dokuments war, um über Multisignatur-Verfahren Freigabeprozesse zu koordinieren oder auch um notarielle Schritte durchzuführen.[2]

Als konkretes Beispiel kann hier Vaultitude angeführt werden. Dieses Unternehmen hat sich auf die Nutzung der Blockchain für Besitzrechts-Belange von geistigem Eigentum spezialisiert. Durch diese Plattform können die Besitzrechte für geistiges Eigentum gegenüber Dritten verifiziert, die Übertragung von geistigem Eigentum durchgeführt oder auch die Plattform zur Monetarisierung, etwa durch Lizenzrechte, genutzt werden.[3]

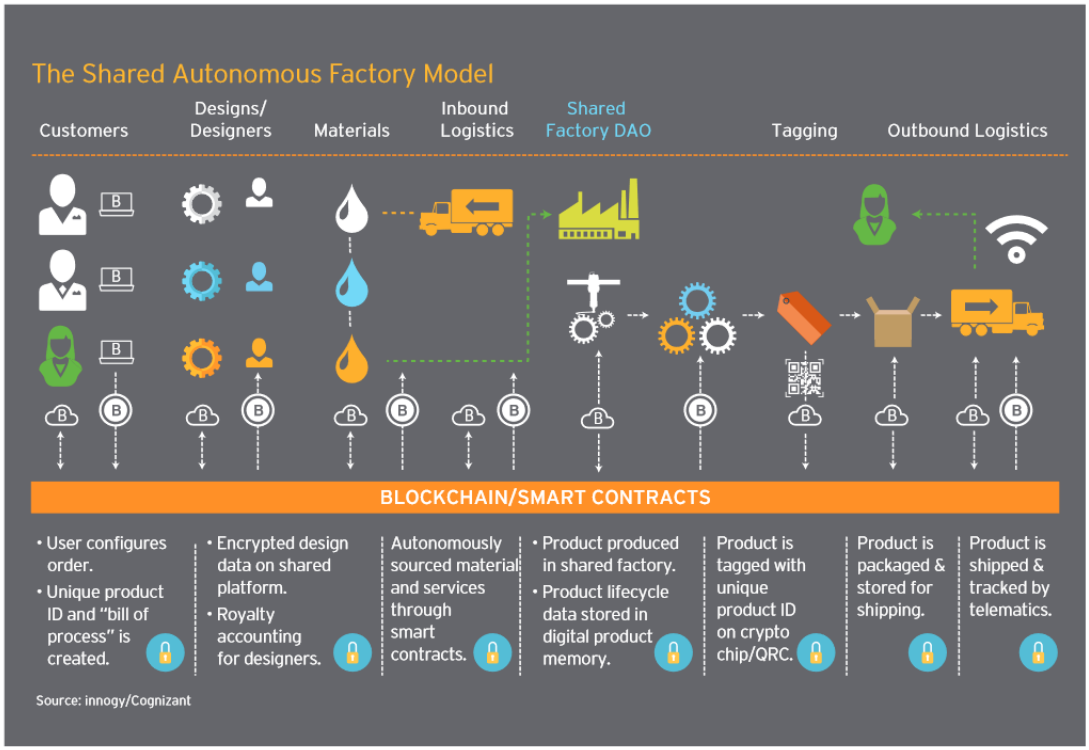
In Bezug auf die Produkterstellung ist das Projekt „Genesis of Things“ besonders erwähnenswert. Dabei handelt es sich um einen Zusammenschluss mehrerer Stakeholder mit dem Ziel eine dezentrale Plattform für Herstellungsprozesse anzubieten. Fokus liegt hierbei auf dem 3D-Druck und dem Transfer von Daten im Prozess der Erstellung der Designs sowie der Produktion selbst. Laut Angaben der Projekt-Website und des veröffentlichten White-Papers soll es möglich sein, dadurch 3D-Druck-Daten an beliebige ins System integrierte 3D Drucker zu senden,

[1] vgl. Crosby M. et al., 2015, S.15f
[2] vgl. Crosby et at., 2015, S.15
[3] vgl. https://vaultitude.com/index.html zuletzt gelesen am 27.01.2019

ohne eine menschliche Interaktion zu benötigen. Ebenso die Verrechnung des Drucks soll im Zuge dessen mittels Smart Contracts realisiert werden.[1]

Abbildung 3-9 soll in diesem Zusammenhang Konzept der angestrebten Abläuft darstellen. Insbesondere der komplett automatisierte Ablauf und die durchgehende Nutzung der Blockchain sind hier gut sichtbar.

Abbildung 3-9: Genesis of Things Factory Model[2]



Dabei befindet sich das Projekt aber noch in einem frühen Status und die publizierten Funktionen sind noch nicht im umfangreichen Maß einsatzbereit.[3]

[1] vgl. Blechschmidt B. & Stoecker C. S.2ff
[2] Abb. 3-9. Aus Blechschmidt B. & Stoecker C. S.5
[3] vgl. http://www.genesisofthings.com/ zuletzt gelesen am 02.02.2019

Tabelle 3-6 Generische Use Case Definition: (Digital) Assets & Intellectual Property

Name	**(Digital) Assets & Intellectual Property**
Ziele im Kontext	■ Eindeutige Abbildung von realen oder digitalen Vermögenswerten auf der Blockchain ■ Abwicklung und Bearbeitung von Besitzrecht-Prozesses
Akteure	■ Akteur in diesem Case sind die Entitäten selbst, die auf der Blockchain abgebildet werden ■ Inhaber der Besitzrechte (auch Verkäufer & Käufer)
Kurzbeschreibung	Abbildungen von physischen oder digitalen Assets werden auf der Blockchain gespeichert und für Besitzrechts-Prozesse oder Verifikationsprozesse genutzt
Merkmale	■ Speicherung digitaler Entitäten auf der Blockchain ○ Digitale Entitäten sind entweder digitale Assets oder digitale Abbildungen von realen Assets ○ Mit Besitzrechten versehen → Intellectual Property ■ Rechte können übertragen werden

Mögliche Nutzung im industriellen Umfeld

In Bezug auf die Nutzung im industriellen Umfeld, kann zuerst die Organisation von physischen Produkten betrachtet werden. Dies stellt einen möglichen, wenn auch nicht überaus innovativen Use Case dar. Prinzipiell ist es jedoch sicherlich möglich die Besitzrechte von technischen Produkten über eine Blockchain zu organisieren. Denkbar wäre hier als Beispiel ein digitaler Zulassungsschein für Autos oder anderen Geräten. Die am besten hierfür geeigneten Produkte wären sicherlich jene, die verhältnismäßig mobil und von hohem Wert sind. Außerdem gilt es hier auch das Netzwerk der potenziellen Teilnehmer zu betrachten. Insbesondere ob eine zentralisierte Lösung nicht besser geeignet wäre. Betrachtet man jedoch die Eigentumsrechte zu digitalen Produkten in Bezug auf das industrielle Umfeld, lässt sich eine höhere Relevanz draus schließen.

Durch die immer höher werdende Komplexität über den gesamten Product Life Cycle hinweg, sind auch immer komplexere digital abgebildet Prozesse vorhanden. So kann ein Blockchain-basiertes Dokumentenmanagement mit entsprechenden Freigabemöglichkeiten dazu beitragen den administrativen Aufwand zu reduzieren.

Dabei speichern, bearbeiten, verifizieren und übermitteln die verschiedenen Parteien die notwendigen Dokumente etwa im Rahmen der Produktentstehungsphase über eine gemeinsame Plattform, die etwa über eine Schnittstelle in bestehende PDM-Systeme integriert ist. Dadurch

wird der administrative Aufwand tendenziell dezentraler verteilt und es besteht eine für alle Parteien lückenlose Nachvollziehbarkeit.

Betrachtet man nun den Aspekt bezüglich Eigentumsrechte von digitalen Produkten, stellt die voranschreitende Entwicklung des 3D-Drucks und somit die diesbezügliche Nutzung entsprechender CAD-Daten wie oben bereits auch vorgestellt einen naheliegenden Use Case dar. So könnte etwa auch eine Abbildung einer CAD-File in einer entsprechenden Blockchain gespeichert werden und über dieses System dann die Besitz- und Nutzungsrechte organisiert werden.

Dadurch kann ein externes Entwicklerbüro die für einen konkreten Auftrag erstellte Datei bei der Übertragung mit entsprechenden Nutzungsrechten versehen, die dich nur auf die Nutzung im vereinbarten Maß beim Fertigungsunternehmen beziehen. Diese Nutzung könnte dann mit Smart Contracts auch entsprechend der tatsächlichen Stückzahl automatisiert bezahlt werden.

Insbesondere durch die schnelle (unerlaubte) Verbreitbarkeit von Entwicklungsdaten, die für das Entwicklungs-Unternehmen ja mit entsprechen Kosten zur Erstellung verbunden waren, stellt einen kritischen Punkt dar, der durch ein entsprechendes System gelöst werden könnte.

3.2.5 IoT

Wie bereits in Kapitel „IoT – Internet of Things“ erwähnt, stellt IoT einen kritischen Aspekt im Rahmen der Industrie 4.0 dar.

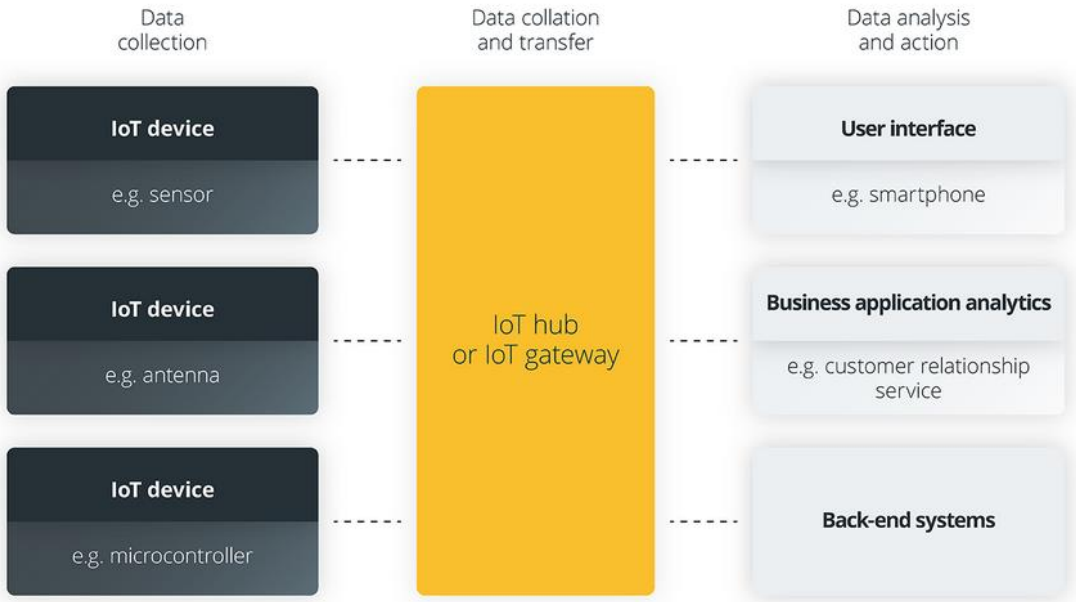
Insbesondere die Kommunikation der Geräte untereinander, sowie die Verwaltung durch Administratoren stellt eine entsprechende Herausforderung dar. Vor allem, da die Anzahl der im IoT Bereich eingesetzten Geräte sich nach mehrfachen Prognosen in den nächsten Jahren und Jahrzehnten um ein Vielfaches erhöhen wird. So prognostiziert die Statistik-Plattform Statista allein bis zum Jahr 2020 eine weltweite Anzahl von rund 20.000 Millionen Stück im Vergleich zu rund 12.000 Millionen im Jahr 2018.[1]

Bisherige Ansätze konzentrieren sich Großteils auf die Nutzung zentralisierter IoT Plattformen die als Koordinierungs-Autoritäten die Interaktionen der IoT-Geräte verwalten. Aufgrund des administrativen Aufwandes, der hierfür notwendigen technischen Voraussetzungen und der immer größeren Anzahl an Geräten, stellt sich dieser Weg tendenziell als nicht effizient heraus. Abbildung 3-10 zeigt eine solche Struktur einem zentralisierten IoT-Hub, der all Informationen selbst koordinieren muss. Dem zufolge entwickelt sich die Tendenz zur Entwicklung von dezentralisierten IoT Plattformen.[2]

[1] vgl. https://de.statista.com/statistik/daten/studie/537093/umfrage/anzahl-der-vernetzten-geraete-im-internet-der-dinge-iot-weltweit/ zuletzt gelesen am 03.02.2019

[2] vgl. Crosby M. et al, 2015, S.15

Abbildung 3-10: Darstellung der Systemstruktur bei Nutzung eines IoT-Hubs[1]



Ziel solcher Plattformen ist demnach tendenziell, die Kommunikation von IoT-Geräten zu ermöglichen, ohne die Notwendigkeit einer zentralen Instanz. Dabei könnte ein Gerät direkt im Rahmen der Produktion desselben in die Blockchain eingetragen werden, wo über die gesamte Lebensdauer Produktinformationen gespeichert und verwaltet werden. (zB. Herstellungsinformationen, Garantieinformationen, Historie, Änderungen, etc.)[2]

Ein weiteres Ziel im Rahmen der Einführung eines Blockchain Systems im IoT Bereich stellt sicherlich die Erhöhung der Datensicherheit dar. Insbesondere, da durch die Verbreitung der IoT-Geräte ein potenziell einfacherer Zugriff für Hacking-Attacken ermöglicht wird. Durch die inhärente Sicherheit die Blockchain-Netzwerke bieten, könnte somit dem unerlaubten Zugriff ins Netzwerk und schadhaftem Verhalten entgegengewirkt werden. Sollte es doch zu einem solchen unerlaubten Zugriff oder schlicht zu einem Fehler im System kommen, stellt ein Blockchain-Netzwerk keinen Single-Point-of Failure dar und würde trotz des Ausfalls eines oder mehrerer Knoten den Betrieb aufrechterhalten können. Mittels der Nutzung von Smart Contracts kann das System dann natürlich auch entsprechend automatisiert werden.

Die Blockchain stellt im Zusammenhang mit dem Potenzial zu einer effizienteren Netzwerkstruktur, unter anderem bedingt durch tendenziell weniger Overhead-Daten in Bezug auf koordinierende Zentral-Instanzen, eine signifikante Möglichkeit zur Kostenreduktion dar.

[1] Abb. 3-10 aus https://cointelegraph.com/news/how-significant-is-blockchain-in-internet-of-things zuletzt gelesen am 09.02.2019

[2] vgl. Scherk J. & Pöchhacker-Tröscher G., 2017, S.33

Aufgrund der hohen Anzahl sich im Rahmen des IoT-Umfelds ergebenden Möglichkeiten, stellt diese Use Case Kategorie somit vermutlich die komplexeste und umfangreichste der definierten Kategorien dar, die die meisten konkreten Use Cases umfasst. Sie präsentiert sich dabei in unterschiedlichsten Ausprägungen und Richtungen und könnte bei Bedarf in weitere Sub-Kategorien unterteilt werden.

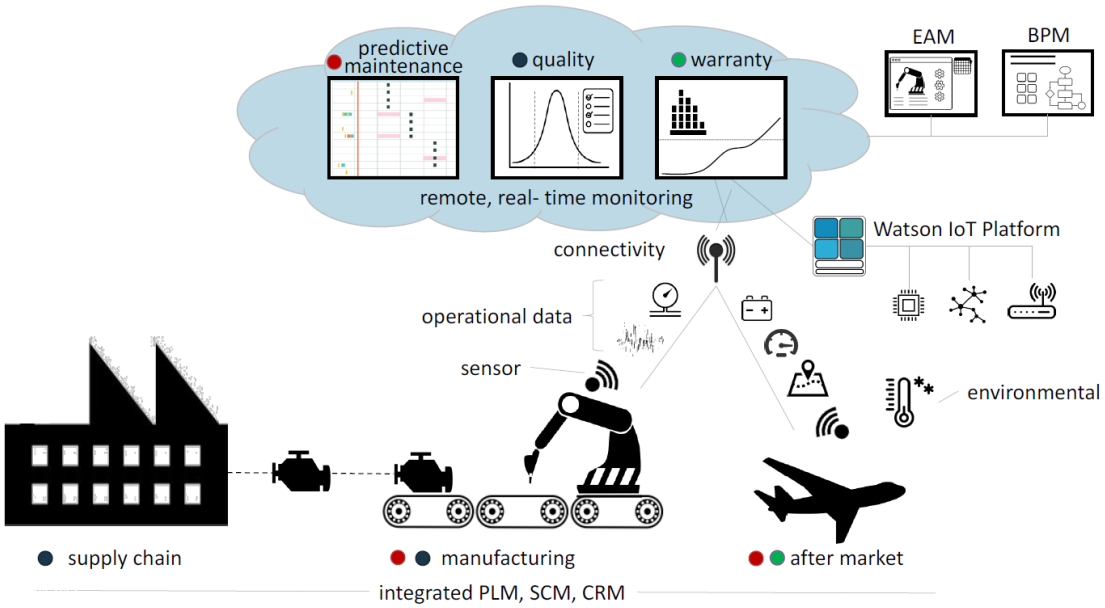
Ein erstes Beispiel stellt VeChain‘s Kühlketten-Use Case dar. Dabei werden IoT Geräte genutzt um im Rahmen von Kühlketten-Logistikketten gewünschte Messdaten, wie Temperatur, Luftfeuchtigkeit oder GPS-Koordinaten aufzuzeichnen und im Blockchain-Netzwerk zu speichern. VeChain bietet in diesem Zusammenhang auch die Möglichkeit von Benachrichtigungen, wenn gesetzte Grenzwerte überschritten werden.[1]

Eine umfangreichere Nutzung zeigt sich im Beispiel des Unternehmens Boeing, welches in Kooperation mit IBM als Ziel hat, den gesamten Product Life Cycle eines Flugzeugs auf einer IoT-fokussierten Blockchain abzubilden.[2]

Abbildung 3-11 zeigt in diesem Zusammenhang schematisch verschiedene Aspekte im Rahmen des Product Life Cycle eines Flugzeugs. Insbesondere hervorgehoben werden können die Aspekte des Qualitätsmanagements und Predictive Maintenance, die laut Robert Rechner von Boeing von großer Bedeutung sind. Dementsprechend stellt die „Reduzierung von Ausfällen und ungeplanten Wartungs-Notwendigkeiten“ den größten Nutzen eines IoT-Blockchain-Systems im Bereich Flugzeugbau dar.[3]

[1] vgl. https://www.vechain.org/ zuletzt gelesen am 10.02.2019
[2] vgl. https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/ zuletzt gelesen am 10.02.2019
[3] vgl. https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/ zuletzt gelesen am 10.02.2019

Abbildung 3-11: Schematische Darstellung eines Flugzeug Product Life Cycle[1]

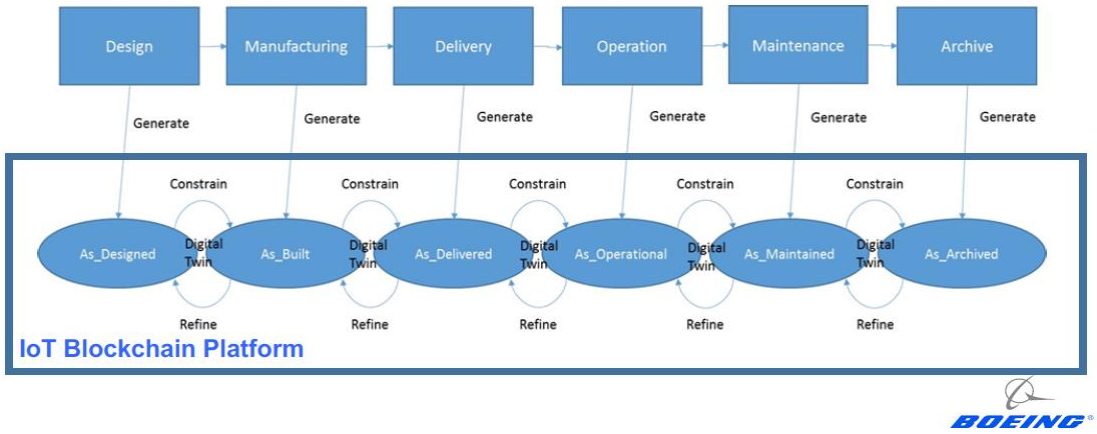


Insbesondere, da auch die Herkunft vieler Einzelteile im Flugzeugbau derzeit schwer nachvollziehbar ist, setzt Boing in diesem Zusammenhang auf die Erstellung einer Digital Twin Abbildung des Flugzeugs im Rahmen einer IoT Blockchain Plattform. Wie in Abbildung 3-12 zu sehen, werden hierfür in jeder Phase des Product Life Cycle die gesammelten Informationen in das System eingetragen und bedingen durch Verknüpfung mit den weiteren Phasen die Weiterentwicklung des Flugzeugs. Insbesondere die durch IoT-Geräte ermöglichte Messung unzähliger Sensor-Daten, sowie die darauf aufbauende Analysemöglichkeit, ermöglicht es Boing in diesem Zusammenhang Optimierungspotenziale auszuschöpfen.[2]

[1] Abb. 3-11 aus https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/ zuletzt gelesen am 10.02.2019

[2] vgl. https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/ zuletzt gelesen am 10.02.2019

Abbildung 3-12: Einbindung der IoT Blockchain Plattform bei Boeing[1]



Als Plattform-Anbieter für ein solches System kann als weiteres Beispiel Riddle&Code herangezogen werden. Dieses Unternehmen hat sich darauf spezialisiert als Schnittstelle zwischen der realen Welt und der Blockchain zu fungieren. Nach der Philosophie von Riddle&Code benötigen Maschinen vor allem Identität und Integrität, um in der Blockchain vernetzt sein zu können und Transaktionen selbstständig durchführen zu können. Hierfür bietet das Unternehmen eine Anzahl von Hardware an, die durch die mit bereitgestellter Firmware per Blockchain verbunden werden können. Dabei handelt es sich primär um verschiedene Chips zur Identitäts-Festlegung mit NFC Transponder und Möglichkeit zur Verbindung mit verschiedenster Sensorik[2]

Je nach Use Case ermöglicht dieser Zugang somit die Integration von bestehenden Dingen in ein IoT Netzwerk, ohne dass diese im Vorfeld durch deren Produktion IoT-fähig erstellt wurden. Die von Riddle&Code vorgestellten Use Cases decken dabei viele Bereiche von Dokumenten-Verifizierung bei Grenzkotrollen, Herkunfts-Nachweis bei Lebensmitteln oder Smart City Solutions, wo die Geräte der öffentlichen Infrastruktur mit dem Blockchain Netzwerk verbunden werden.[3]

Einen weiteren Ansatz zur Erstellung eines IoT Systems bietet das Unternehmen Zenodys in Form der Erstellung von Applikations-Bausteinen, von Zenodys „Digital Assets“[4] genannt. Diese können modular über die bereitgestellte grafische Entwicklungsumgebung zu Applikationen zusammengefügt werden. Dabei fungiert die hinterlegte Blockchain als eine Art Marktplatz, wo

[1] Abb. 3-12 aus https://www.altoros.com/blog/boeing-improves-operations-with-blockchain-and-the-internet-of-things/ zuletzt gelesen am 11.02.2019
[2] vgl. https://www.riddleandcode.com/faq zuletzt gelesen am 11.02.2019
[3] vgl. https://www.riddleandcode.com/Use Case-n/ zuletzt gelesen am 11.02.2019
[4] ANMEKRUNG: Der Begriff „Digital Asset“ steht in diesem Fall in einer andren Bedeutung als im Kapitel „(Digital) Assets & Intellectual Property“

Entwickler die einzelnen Module erstellen und zum Kauf anbieten, wobei diese Module entsprechend standardisiert mit den anderen Modulen interagieren können. Dadurch soll erreicht werden, dass Käufer über die grafische Entwicklungsoberfläche die gewünschten Funktionalitäten zusammenstellen kann, ohne den Code selbst bearbeiten zu müssen. Der Kauf-Prozess wird hierbei durch Smart Contracts geregelt. Abbildung 3-13 zeigt schematisch den Ablauf des Prozesses von der Erstellung Digitaler Assets links bis hin zur fertigen Applikation des Kunden reicht.[1]

Abbildung 3-13: Workflow im Rahmen der Nutzung der Zenodys Plattform[2]

Anzumerken ist hierbei, dass Zenodys sich auf die digitalen Aspekte beschränkt. Zur Integration von bestehenden IoT Netzwerken besteht jedoch die Möglichkeit Daten mit verschiedenen Quellen auszutauschen. So ist es möglich die Zenodys Plattform mit IOTA, NEO oder Ethereum zu verbinden. Dadurch können Daten aus verschiedenen Plattformen über Zenodys organisiert und verwaltet werden, was eine erhöhte Interoperabilität zwischen den einzelnen Blockchains ermöglicht.[3]

[1] vgl. Zenodys White Paper: Organizing the digital world with blockchain, Q2 – 2018, S.1ff
[2] Abb. 3-13 aus Zenodys White Paper: Organizing the digital world with blockchain; Q2 – 2018, Version: 0.95, abgerufen von: http://zz.zenodys.com/zenodys-whitepaper.pdf
[3] vgl. Zenodys technical white paper, S.41

Tabelle 3-7 Generische Use Case Definition: IoT

Name	**IoT**
Ziele im Kontext	■ Vernetzung von IoT-Geräten in der Blockchain ■ Nutzen der Blockchain-Eigenschaften zur Erhöhung der Sicherheit und verhindern eines Single-Point-of-Failures ■ Automatisierung der Abläufe ohne Koordinierung durch zentrale Stelle
Akteure	■ IoT Geräte in der Blockchain
Kurzbeschreibung	Mittels Blockchain-Netzwerks werden IoT-Geräte vernetzt und wodurch ein Betrieb des Systems ohne zwingende zentrale Stelle möglich wird.
Merkmale	■ Schaffung einer Schnittstelle zwischen Physischem Gerät und der Blockchain-Ebene ■ IoT-Geräte können untereinander kommunizieren ■ Zentrale Stelle stellt keinen Flaschenhals zur Koordinierung der Kommunikation dar

Mögliche Nutzung im industriellen Umfeld

Die Use Cases in dieser Kategorie entsprechend zum Großteil den üblichen Use Cases im Bereich IoT, wobei hier eben das System eine andere Architektur besitz im Vergleich zu zentralisierten Systemen.

Die primären Vorteile der Realisierung eines solchen Netzwerks mittels Blockchain-Architektur belaufen sich auf die Vermeidung von Flaschenhälsen, das Potenzial für ein hohes Maß an Automatisierung und inhärente Sicherheit durch Blockchain-Eigenschaften. Im industriellen Umfeld zeigt sich auch besonders durch die potenzielle Robustheit gegenüber Ausfällen ein klarer Vorteil von dezentralen Systemen, da z.B. ein Stillstand in der Produktion zu erheblichen Kosten führen kann, wodurch allein schon die Verhinderung solcher Situationen absolut erstrebenswert ist. Konkret ist es somit vorstellbar, dass Maschinen, die durch IoT-Sensorik mit dem Netzwerk verbunden sind durch entsprechende Automatisierung erkennen, wann sie gewartet werden müssen, diese Wartung automatisch veranlassen und ebenfalls automatisiert bezahlen. Eben durch diese Automatisierung können tendenziell in erheblichen Maße Kosten eingespart werden.

In Anlehnung an viele Supply Chain Use Cases können IoT-Geräte über den Verlauf des Product Life Cycle verschiedenste Messungen durchführen und diese auf der Blockchain ablegen, wodurch die gewünschte Dokumentierung in Verbindung zur realen Welt hergestellt werden kann. Natürlich ist bezüglich einer solchen Anwendung anzumerken, dass auf der Blockchain

selbst nicht unbedingt großen Datenmengen gespeichert werden sollten, um Kapazitätsproblemen aus dem Weg zu gehen. Insbesondere, da übliche IoT-Geräte sich auf grundlegende Hardware reduzieren und somit selbst keine ausreichende Speicherkapazität haben um als voll agierender Node in der Blockchain mitzuwirken. Demzufolge wäre es eher sinnvoll über Kombination nachzudenken, bei denen die IoT-Geräte Messungen generieren und diese Informationen an ein Blockchain-Netzwerk übertragen, das aus ausreichend leistungsstarken Nodes besteht.

Zusätzlich zu diesem Aspekt kann davon ausgegangen werden, dass die Effizienz der im IoT-Bereich verwendeten Hardware in Zukunft weiter steigen wird, wodurch sich dementsprechend mehr Spielraum für die Nutzung der Kapazitäten dieser Hardware ergeben wird.

Integriert man in diese Überlegungen von IoT und Blockchain des Weiteren auch Technologien im Zusammenhang mit AI bzw. Machine Learning, ergeben sich IT-Systeme, die für viele weitere Use Cases nutzbar sind. Man kann hier zum Beispiel an Produktionsmaschinen denken die entsprechend der über IoT durchgeführten Messungen und den damit möglich Analyse-Algorithmen selbstständig die Produktionsleistung anpassen und somit die Automation weiter erhöhen. Diese Gedanken können auf umfangreiche „Smart ERP-Systeme“ ausgeweitet werden oder auch als Werker Assistenzsysteme zur Verfügung stehen.

3.2.6 Blockchain als Datenbank

Es besteht des Weiteren auch die Möglichkeit, eine Blockchain mit dem Fokus als Datenspeicher zu nutzen ohne eine bestimmte Verwendung der Daten wie in den anderen Use Cases im Auge zu haben. Wobei man hier besonders genau abwägen muss, ob nicht eine handelsübliche Variante der Datenspeicherung (relationale Datenbanken, Cloud-Services) nicht doch besser geeignet sind, als ein Blockchain Netzwerk. Insbesondere, da es bereits sehr ausgeklügelte und verbreitete Systeme gibt, die darauf spezialisiert sind Daten zu zerstückeln, zu verschlüsseln und dann diese auf mehreren Orten abzulegen.

Der besondere Vorteil einer Blockchain in diesem Zusammenhang stellen vor allem ihre Eigenschaften dar, dass ein solcher Datenspeicher besonders ausfallsicher und manipulationssicher ist. Das hat ein dezentrales System im Vergleich zu zentralisierten Lösungen das Potenzial auch sicherer gegen Datenverlust und tendenziell weniger fehleranfällig zu sein. Ihren Ursprung hat diese Anwendung der Blockchain in gewissen Maße in den bereits seit vielen Jahren etablierten P2P-Filesharing Diensten wie etwa Napster, Kazaa oder BitTorrent, wo Nutzer anderen Nutzern Daten bereitstellen. Dabei wird ein Netzwerk direkt zwischen den Nutzern aufgebaut, ohne den Datentransfer über einen Server zu organisieren.[1]

[1] vgl. https://www.heise.de/developer/artikel/Verteilter-Speicher-Dokumente-an-der-Blockchain-3880570.html zuletzt gelesen am 24.01.2019

Eine Nutzung der Blockchain die diesem Prinzip am ehesten entspricht stellt das IPFS (Inter-Planetary File System) Projekt dar. Dabei werden selektierte Daten direkt auf den Nodes gespeichert und andere Teilnehmer im Netzwerk können durch ebenso abgelegte Index-Informationen herausfinden, welche Nodes im Netzwerk die gesuchten Daten bereitstellen.[1]

Vorteil dieses System ist, dass dadurch ein Netzwerk direkt unter den Nodes aufgespannt wird und das System nicht von zentralen Server-Strukturen abhängig ist. Sollte in einem zentralisierten File Sharing System der Server ausfallen, wäre kein Zugriff auf die Daten mehr möglich. Bei IPFS wäre ein Ausfall eines einzelnen Nodes kein größeres Problem, sofern die anderen Nodes dieselben Daten bereitstellen können.

Die Anwendbarkeit solcher Systeme zeigt sich in einem Beispiel, bei dem eine große Anzahl an Daten aus verschiedenen Quellen vereint werden sollen. Wenn nun beispielsweise zwei Unternehmen ihre Datenbanken aus Gründen des Informationsaustausches teilen wollen, ist es nicht anzunehmen, dass diese sich einfach eine Datenbank teilen. Viel wahrscheinlicher ist es, dass die Unternehmen die Datenbank des jeweils anderen Unternehmens mittels Master-Slave Nachbildung als Read-Only Kopie im eigenen System abbilden und die eigene Datenbank mit dieser Abbildung abgleichen. Was bei zwei Unternehmen noch praktikabel sein kann, stellt sich bei einer Vielzahl von Partnern als hoher administrativer Aufwand dar, da für jeden neuen Teilnehmer im System bei allen anderen Teilnehmern einen neue Read-Only Abbildung erstellt werden muss. Bei 5 Unternehmen wären das somit bereits 25 Datenbank-Instanzen insgesamt.[2]
Als Lösung würde sich ein von allen Unternehmen genutztes Blockchain - File Storage System anbieten, auf dem alle Einträge von allen Teilnehmern gesammelt und sicher ausgetauscht werden.

Ein weiteres Beispiel Stellt Storj dar, welches sich zu Beginn des Jahres 2019 noch in der Alpha Phase befindet. Den Nutzen dieser Plattform stellt das Speichern von beliebigen Daten über das Netzwerk hinweg dar. Dabei stellen Nodes Bandbreite und Speicher zur Nutzung durch andere Netzwerk-Teilnehmer zur Verfügung, und werden dafür mittels Mikrozahlungen belohnt. Die gespeicherten Daten werden dafür lokal beim Nutzer verschlüsselt und dann in gesicherter, containerisierter Form auf verschiedenen Nodes im Netzwerk abgelegt.[3]

Solche Plattformen bieten somit eine Möglichkeit an, Daten ähnlich einer Cloud in dem Netzwerk abzulegen, ohne dabei von zentralisierten Anbietern wie etwa Dropbox abhängig zu sein.

[1] vgl. Benet J., IPFS – Content Addressed, Versioned, P2P File System (Draft 3), abgerufen von: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf
[2] vgl. https://www.coindesk.com/four-genuine-blockchain-Use Cases zuletzt gelesen am 24.01.2019
[3] vgl. https://storj.io/ zuletzt gelesen am 24.01.2019

Tabelle 3-8 Generische Use Case Definition: Blockchain als Datenbank

Name	**Blockchain als Datenbank**
Ziele im Kontext	■ Dezentrales Ablegen von Daten ■ Hohe Redundanz und Ausfallsicherheit
Akteure	■ Nutzer die Daten ablegen wollen ■ Nutzer die eigenen Node zur Ablage der Daten bereitstellen
Kurzbeschreibung	Daten werden mittels Blockchain-Protokolls auf verschiedenen Nodes im Netzwerk abgespeichert.
Merkmale	■ Bereitstellung von Speicherplatz durch Nodes ■ Verteilung der Daten auf verschiedene Nodes, um Redundanz und Ausfallsicherheit zu erreichen ■ Keine Notwendigkeit einer zentralen Instanz, um Datenaustausch zu ermöglichen ■ Tendenziell weniger effizient & leistungsfähig als gängige Systeme

Mögliche Nutzung im industriellen Umfeld

Die Nutzung eines Blockchain-Systems zur Datenspeicherung hat sicherlich nicht in jedem Fall Sinn und muss von Fall zu Fall genau beurteilt werden.

Insbesondere aufgrund der derzeitig höheren Effizienz in Bezug auf Datenspeicher-Bereitstellung und Transaktionsgeschwindigkeit von bisher gängigen zentralisierten Systemen.

Denkbar wäre eine Nutzung wie im oben dargelegten Fall, wo mehrere Unternehmen die jeweiligen Datenbanken gegeneinander abgleichen wollen. Besonders in Bezug auf den Abgleich von Kundendaten, oder auch die gemeinsame Sammlung von Daten für Analytics-Zwecke wären hier sinnvolle Möglichkeiten. So könnten sich zum Beispiel mehrere Unternehmen zusammenschließen und ggf. anonymisierte Daten in einen gemeinsamen Datenpool sammeln, um diesen für entsprechende Zwecke zu nutzen. Besonders in Bezug auf Machine Learning und AI könnte dies eine gangbare Möglichkeit darstellen um ausreichend Daten zum Anlernen der Algorithmen bereitstellen zu können, wenn die Datenmenge eigenen Unternehmen nicht ausreichend hoch ist. Dieser Use Case setzt aber vermutlich noch viel Entwicklungszeit voraus, da besonders die großen Datenmengen die derzeitigen Systeme und Infrastrukturen vor eine große Herausforderung stellen würden.

Ebenso könnte natürlich ein stark IT-orientiertes Unternehmen Speicher- und Bandbreiten-Kapazität zur Verfügung stellen, um nicht genutzte Hardware monetär nutzen zu können.

Tabelle 3-9 Übersicht der Use Case Kategorien

Beispiele	Nutzen für industrielles Umfeld	Phasen des Product Life Cycle
Energiehandel & -netze (Wien Energie, Grid Singularity, Energie AG), Share & Charge (Carsharing), ARTIS (Mikrotransaktionen)	Verkauf von überschüssiger Energie, Mikrotransaktioen im Rahmen von Machine as a Service Konzepten oder Durchführung von Zahlungen an externe Dienstleister	Uneingeschränkt; tendenziell Produktherstellung und Produktnutzung
Walkart & IBM, Maerst & IBM, Modum, IRC Group	Möglichkeit zur Abbildung der Supply Chain bis zum kleinsten Einzelteil möglich. ebenso Miteinbeziehen von externen Dienstleistern (Entwicklung, Wartung) möglich. Nachverfolgbarkeit von Fehlerquellen.	Uneingeschränkt, Fokus ist die gesamte Supply Chain und somit den gesamten Product Life Cycle abzubilden
Stadt Zug (Schweiz), Grundbuchregister Schweden (ChromaWay), BRZ: Digitale Gemeinde Kettenbruck, Estland Digitale ID	Alleiniger Nutzen nur digitaler ID nicht sinnvoll. Use Case kann als Sub Use Case für größere Anwendungen gesehen werden.	ID Erstellung ab der Produktentwicklung-Phase, Nutzung tendenziell in der Produktnutzungs-Phase
Everledger, Factom, Vaultitude	Abbildung von physischen und digitalen Produkten auf der Blockchain und Verwaltung der Besitzrechte. Verifikations- und Freigabeprozesse von Dokumenten.	Uneingeschränkt, digitale Abbildung der Assets über gesamten Life Cycle hinweg sinnvoll
IBM & Samsung, Boeing, VeChain, Riddle&Code, Zenodys, FabRec	Dezentrale IoT Netzwerke, Automatisierte Durchführung von Aktionen durch Maschinen, Kombination mit AI oder Machine Learning für Analyse-Tätigkeiten	Abhängig von Use Case, tendenzieller Fokus auf Produktherstellungs-Phase, jedoch verschiedene Cases über den gesamten Product
IPFS, Swarm, Storj	Erstellung von Datenbanken die besonders ausfall- und manipulationssicher sind. Kollektive anonymisierte Datenpools für Analytics-Zwecke. Evtl. Nutzung von überschüssigen Hardware-Kapazitäten zur Monetarisierung.	Uneingeschränkt

Use Case Bezeichnung	Kurzbeschreibung
Peer-to-Peer Transaktionen und Verrechnung	Austausch von Daten oder Wertem im Rahmen eines gemeinsamen Netzwerkes. Optional: automatisierte Verrechnung bezüglich des stattgefundenen Austausches
Supply Chain	Im Rahmen des Product Life Cycle bildet ein Blockchain-System ein Informationsnetzwerk über die gesamte Supply Chain hinweg.
ID auf Blockchain	ID-bezogene Daten werden auf der Blockchain gespeichert und für Verifizierungszwecke genutzt.
(Digital) Assets & Intellectual Property	Abbildungen von physischen oder digitalen Assets werden auf der Blockchain gespeichert und für Besitzrechts- oder Identifizierungszwecke genutzt
IoT	Mittels Blockchain-Netzwerks werden IoT-Geräte vernetzt, wodurch ein Betrieb des Systems ohne zwingende zentrale Stelle möglich ist.
Blockchain als Datenbank	Daten werden mittels Blockchain-Protokolls auf verschiedene Nodes im Netzwerk abgespeichert.

Sonstige Use Cases

Kurz erwähnt seien hier auch etwaige weitere Use Cases. Die in den vorigen Kapiteln präsentierten Use Case Kategorien stellen die Mehrheit der für ein industrielles Umfeld nutzbaren Use Cases dar, stellt jedoch keinen Anspruch auf absolute Vollständigkeit.

Die weiteren im Rahmen der Recherche für diese Arbeit gefundene Use Cases fallen entweder in die Kategorie der Krypto-Währungen und Finanztransaktionen, die in dieser Arbeit bewusst nicht behandelt wurden, sowie weitere Use Cases, die keine signifikante Relevanz für die Nutzung im Rahmen des Product Life Cycle aufweisen konnten.

Weitere gefundene Use Cases betreffen unter anderem die Bereiche:

- Ticketing
- Messaging (Ethereum Whisper)
- Versicherung
- Humanitäre Hilfszahlungen (AID Coin, Hopepage)
- Crowdfunding
- Diverse Handelsplätze
- Nutzung für Wirtschaftsprüfung, Due Diligence oder Forensics
- Etc.

3.3 Eigene Überlegungen zu Anwendungsmöglichkeiten und Extrapolation

Um die Nutzbarkeit von Blockchain-Systemen im industriellen Umfeld zu verdeutlichen, werden im Folgenden nun zwei selbstentwickelte Use Cases vorgestellt. Dabei handelt es sich um generische Teilprozesse, die darauf ausgelegt sind, typische Funktionen in beispielhafter Weise darzustellen.

Zur Darstellung dieser generischen Teilprozesse wurde sich an dem Wasserfall-Modell der Softwareentwicklung orientiert, welches erstmalig von Royce 1970 so präsentiert wurde.[1] Wobei sich die folgenden Darstellungen auf die Ergebnisse der Phase „Program Design“ beziehen und eine potenzielle Basis für die nächste Phase, die Code-Erstellung und Implementierung, bildet.

Durch die folgenden Darstellungen sollen gewisse nutzbare Aspekte aufgezeigt werden. Diese können je nach Anwendungsfall an die spezifischen Bedürfnisse angepasst und in bestehende Prozesse integriert werden.

Bei der Erstellung der folgenden Modelle stand eine möglichst einfache, generische Darstellung im Fokus und nicht die nahtlose Implementierung. Auch wenn die Modelle so konzipiert wurden, dass sie tendenziell als eigene Applikation erstellt werden, so wäre eine nahtlosere Implementierung durchaus möglich. Anstatt eigener Applikationen, könnte zum Beispiel mittels Oberflächen-Customizings in bereit bestehende Programmoberflächen eigene Schaltflächen integriert werden, die die folgenden Funktionen auslösen.

Zur Darstellung der entwickelten Use Cases wurde die UML Modellierungs-Methodik verwendet.

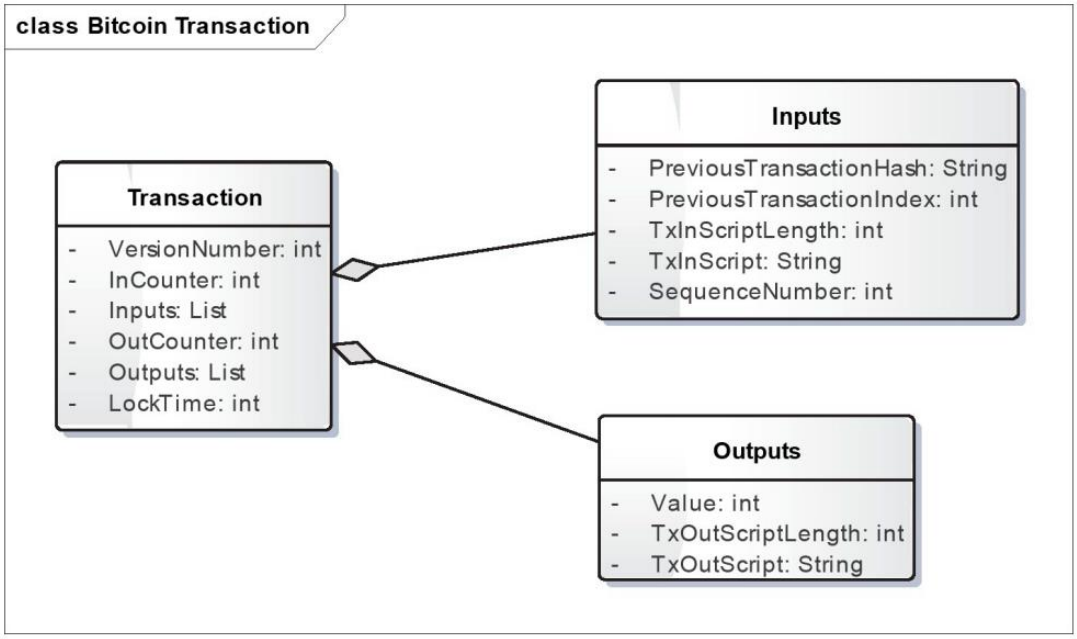
Aus Gründen der Nachvollziehbarkeit wird dabei die eigentliche Blockchain als getrenntes System betrachtet. Dadurch wird die Nutzung externer Blockchain-Systeme ebenso abgebildet, wie wenn eine selbstentwickelte Blockchain genutzt wird.

Dabei entspricht das Blockchain-Modell einer bereits vielfach genutzten Struktur wie sie zum Beispiel in Abbildung 3-14 zu sehen ist:

[1] ANMERKUNG: Die Phasen der Wasserfall-Modells nach Royce,1970:

- System Requirements
- Software Requirements
- Analysis
- Program Design
- Coding
- Testing
- Operations

Abbildung 3-14: Bitcoin Klassendiagramm[1]



Das von Burgwinkel dargestellte Modell entspricht dabei den Basis-Aspekten, die in gängigen Blockchain-Netzwerken so ebenfalls ausgeprägt sind. Bei den folgenden selbst erstellen Modellen, wird von der Nutzung einer Blockchain-Plattform mit einer ähnlichen Struktur ausgegangen. Je nach in der Realität verwendeter Blockchain-Plattform, müssen natürlich entsprechende Anpassungen zu den generischen dargestellten Datenmodellen durchgeführt werden.

3.3.1 Case 1 – Intellectual Property Management von CAD-Daten

Use Case Beschreibung

Dieser Case soll als generisches Beispiel für einen Verifikationsprozess mittels Blockchain dienen. Konkret wird der Teilprozess dargestellt, der die Verifikation der Zugriffserlaubnis auf CAD-Daten für den 3D Druck beschreibt.

Dabei ist das Szenario, dass ein Unternehmen Einzelteile bei einem Entwicklerbüro in Auftrag gibt, die CAD Daten von einem Entwickler(-büro) erstellt werden und die Fertigung mittels 3D Drucker und entsprechender Zugriffserlaubnis wieder im Auftraggeber-Unternehmen stattfindet.

[1] Abb. 3-14 aus Burgwinkel D., 2016, S.155

Hintergrund dabei ist, dass das Entwickler-Büro die Nutzung der erstellten CAD-Daten selbst kontrollieren kann und die Nutzungsrechte mittels Blockchain vergibt. Dadurch ist sichergestellt, dass die entwickelten CAD-Daten auch wirklich nur entsprechend des abgemachten Umfanges genutzt werden und zum Beispiel auch keine dritte Partei die Daten ohne das Wissen des Entwickler-Büros nutzen kann.

Hierfür stellt das Entwicklerbüro eine Applikation zur Verfügung, die die Durchführung des Prozesses erlaubt. Diese Applikation wird vom 3D-Druck Erzeuger entsprechend lokal installiert und ist vergleichbar mit einem Wallet-Client bekannter Blockchain-Systeme.

Use Case Definition:

Tabelle 3-10: Use Case Definition: IP-Management von CAD-Daten

Name	IP-Management von CAD Daten für den Gebrauch im 3D Druck
Ziele	• Zugriffsregelung auf geistiges Eigentum (hier: CAD Daten) • Möglichst automatisierter Verifikationsprozess • Kontrolle des Entwicklers über die Verbreitung der Dateien
Akteure/Rollen	• Entwickler der CAD Daten • 3D Druck – Erzeuger
Trigger	• Freigabe neuer CAD Daten • Zugriff auf erhaltene CAD Daten für den 3D Druck
Essenzielle Schritte	• Erstellung neuer CAD Daten • Verschlüsselung der CAD Daten • Erstellung der Verifikationsreferenz und Ablage auf der Blockchain • Übermitteln der CAD Daten • Entschlüsselung der CAD Daten durch Verifikation per Blockchain
Techn. Anforderungen	• Übermittlung der CAD Files über anderen Nachrichtenkanal (zum Beispiel Email) • Verifikationsprozess ○ Hier kann eine Blockchain-Plattform genutzt werden, wo auch andere Teilnehmer die Transaktion verifizieren
Entwicklungs-Anforderungen	• Schnittstellen-Entwicklung die Ver- und Entschlüsselung der CAD Daten ermöglicht • Keine eigene Blockchain-Entwicklung per se notwendig • Eigen-Entwicklung primär auf Applikations- & Schnittstellen-Ebene

Funktionalitäten/ Funktionelle Anforderungen

- Hashing von CAD Daten
- Konvertierung in STL-Format (für Nutzung zum 3D-Druck)
- Verschlüsselung der CAD File
- Entschlüsselung der CAD File
- Upload der notwendigen Informationen auf die Blockchain (Transaktion von Entwickler zu Hersteller)
    - Upload des Hash auf die Blockchain
- Verifikation des Zuganges und Druckauftrag
- Transaktion der Druck-Rechte zum Hersteller
- Zugriff auf Transaktion mittels Hersteller-Key
- Sendung des Druckauftrags an kompatible 3D-Drucker

Nicht-Anforderungen

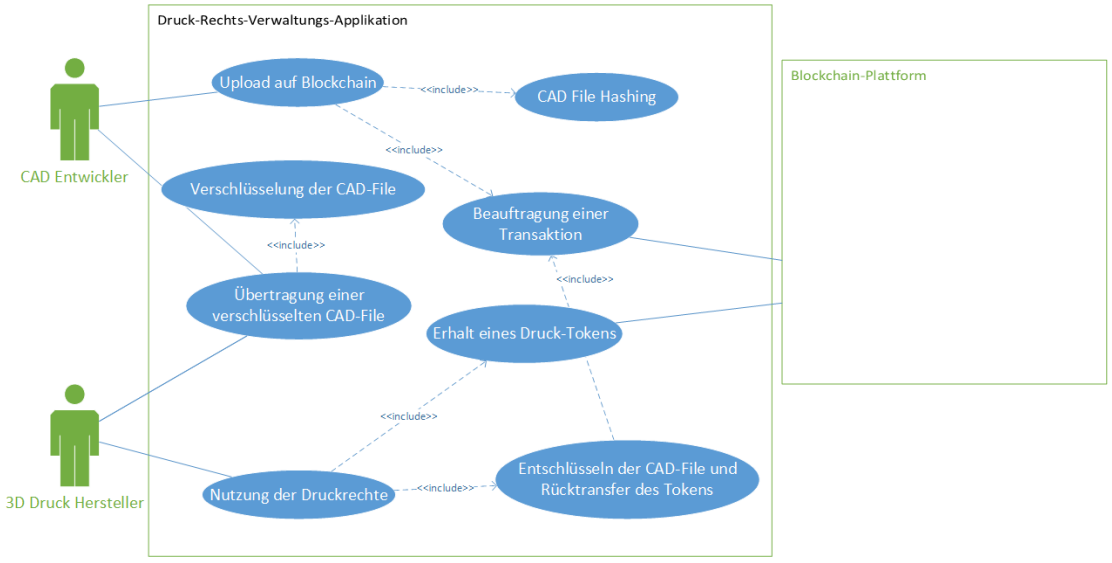
- Übertragung der CAD-Datei selbst
    - Können verschlüsselt übe anderen Kanal übertragen werden
    - Speichern der gesamten CAD-Daten auf der Blockchain nicht praktikabel
- Interface von CAD-Programm zu Blockchain-Applikation (siehe Extrapolation)

UML Beschreibung

Im Folgenden zu finden sind nun die UML-Diagramme, die den Use Case auf der „Program Design“ Ebene beschreiben. Unter den jeweiligen Abbildungen sind jeweils entsprechende Erläuterungen zu finden.

Anwendungsfalldiagramm

Abbildung 3-15: Use Case 1 - Anwendungsfalldiagramm



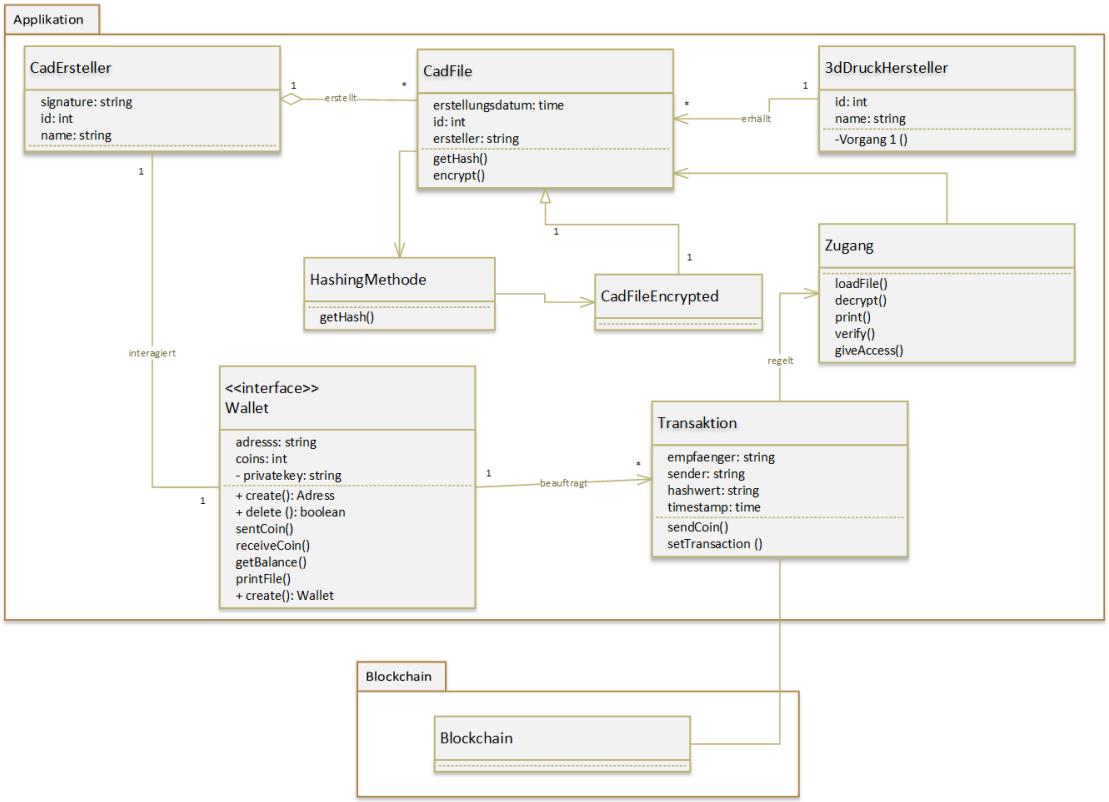
Entsprechend dem Anwendungsfalldiagramm wurden die Anwendungsfälle „Upload auf Blockchain“ sowie „Nutzung der Druckrechte“ als primäre Anwendungsfälle definiert, wobei „CAD File Hashing“, „Beauftragung der Transaktion“, „Erhalt eines Druck-Tokens“ und „Entschlüsselung der CAD-File und Rücktransfer des Tokens“ als untergeordnete Anwendungsfälle anzusehen sind. Der Anwendungsfall „Übertragung einer verschlüsselten CAD-File“ steh als eigener Anwendungsfall, da dieser Prozess einen eigenständigen Ablauf beschreibt.

Die wichtigsten Aspekte der Applikation sind folgende:

- Der CAD-Entwickler überträgt per Blockchain einen Token an den 3D-Druck-Hersteller der als Druck-Recht fungiert.
- 1 Token entspricht einem Druckauftrag.
- Per Applikation wird eine CAD-File verschlüsselt und die entsprechenden Referenz-Daten der Token-Transaktion angehängt
- Die Verschlüsselte CAD-File wird über einen üblichen Kommunikationskanal verschickt (z.B.) Email und mittels Applikation und entsprechender Zugriffs-Prüfung per Blockchain entschlüsselt
    - Begründung: Ein direktes Hochladen der CAD-Daten auf die Blockchain ist aus Kapazitätsgründen nicht als sinnvoll anzusehen.
- Der Druckauftrag wird aus der Applikation verifiziert und in Folge dessen ein Token ein Token an den Entwickler-Account-zurückübertragen, was den Verbrauch eines einmaligen Druck-Zugriffs-Rechts entspricht.
- Ebenso erfolgt der Druckauftrag aus der Applikation selbst, sodass die CAD-Daten bis zum Druckauftrag in der Applikation verkapselt sind.
    - Dies setzt voraus, dass in die Applikation entsprechend Druck-Treiber geladen werden können und die Daten aus der Applikation direkt an den Drucker übergeben werden können.
    - Dafür müssen die CAD-Daten in einem 3D-Druck kompatiblen Datenformat vorliegen bzw. importiert werden (zum Beispiel SLT-Format)
- Der Entwickler kann beliebig viele Druck-Token, also einmalige Druck-Zugriffsrechte vergeben. Die Token entsprechen somit funktionalen Token und nicht für den Consensus-Mechanismus der Blockchain notwendige Coins und stellen somit keine Werteinheit an sich dar. (vgl. Kapitel „Unterschied Coin oder Token“)
- Die Applikation kann als Eigentum des Entwicklerbüros angesehen werden, welche an Kunden verteilt wird und das Daten-Handling übernimmt
- Als Blockchain kann hier entweder eine selbst aufgesetzte private Blockchain dienen wie auch prinzipiell eine Public Blockchain wie Ethereum.
    - Da hier keine hohe Performanz oder die Möglichkeit zum Übertragen großer Datenmengen notwendig sind, eigenen sich auch bestehende Blockchain-Plattformen als Basis.

Klassendiagramm

Abbildung 3-16: Use Case 1 - Klassendiagramm

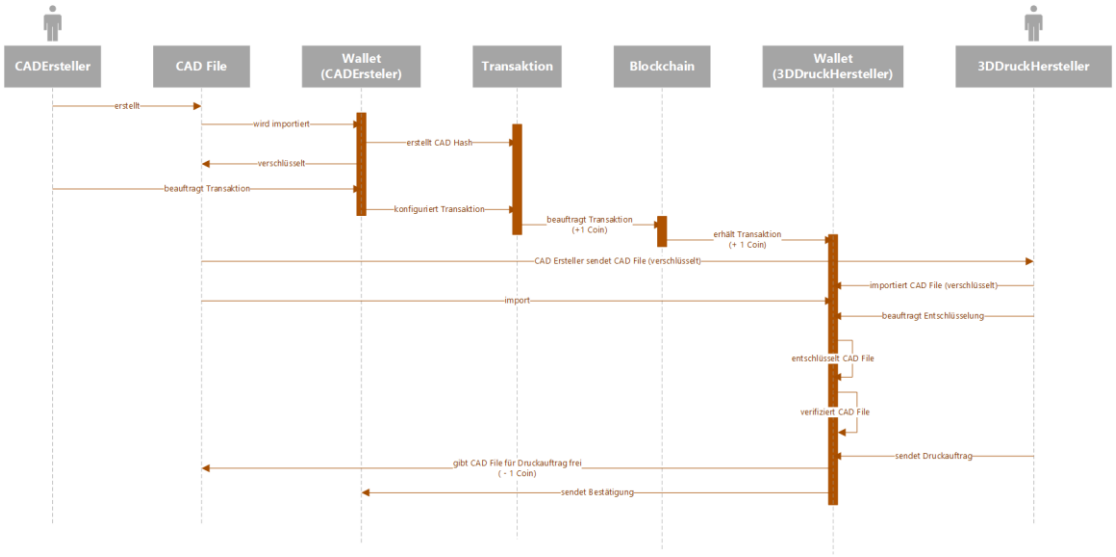


Im Klassendiagramm, wird ein Blockchain-Wallet, ähnlich dem Wallet des Bitcoin-Clients als Interface definiert. Dieses Wallet kann entsprechend der notwendigen Funktionen erstellt werden und wird genutzt, um die entsprechenden Funktionalitäten aufzurufen.

Die Klasse „Transaktion“ beinhaltet alle Informationen, die gesammelt werden, um an die Blockchain zu übergeben.

Sequenzdiagramm

Abbildung 3-17: Use Case 1 - Sequenzdiagramm



Entsprechend der Sequenzdiagrsamm ersichtlichen Abläufe, werden die in Auftrag gegebenen Abläufe primär über die als „Wallet“ bezeichneten Applikations-Oberflächen durchgeführt. Dabei erfolgt auch der Informationsaustausch mit der eigentlichen Blockchain, also die Beauftragung der Transaktion mittels der Wallet-Oberfläche.

Dieses Modell soll verdeutlichen, welche weiteren Funktionalitäten in einen im Allgemeinen als „Wallet“ bezeichneten Client von Blockchain-Applikationen zusätzlich möglich sind.

Diese generische Darstellung steht somit als Beispiel für alle möglichen Funktionalitäten, die zur Nutzung mit der Blockchain in ähnlicher Form integriert werden können.

Ebenso die Nutzung eines Tokens als Darstellung eines einmaligen „Druck-Rechtes“ soll beispielhaft für die verschiedenen Möglichkeiten zur Nutzung einer transferablen Entität stehen. Ebenso in Bezug auf diese Token-Nutzung gibt es unzählige Möglichkeiten, wie diese in anderer Form verwendet werden können.

Extrapolation

Aufbauend auf das vorgestellte Modell, sind zum Beispiel folgende Extrapolationen oder Weiterentwicklungen denkbar:

- Funktionalitäten mittels Add-Ins in die Oberfläche des CAD-Programms integrieren
- Funktionalitäten mittels Add-Ins in die Oberfläche des 3D-Druckprogrammes integrieren.

- Optionaler zeitlicher Fokus: Nutzung der 3D Daten nur innerhalb eines bestimmten Zeitraums möglich
    - Erstellung einer Smart Contract Funktionalität
- Automatisierte Zahlung pro Druckauftrag könnte ebenfalls über die Blockchain realisiert werden
- Daten-Versand und -Empfang innerhalb der Applikation anstatt über externen Kanal

3.3.2 Case 2 – Wartungs-Automatisierung mittels Smart Contract

Use Case Beschreibung

Dieser Case soll generisch den Teilprozess der Nutzung von Smart Contracts beschreiben.

Ausgangsbasis ist ein Produktions-Maschinen-Hersteller, der per Blockchain-Lösung einen automatisierten Wartungs-Service für ausgelieferte Maschinen anbieten möchte.

Dabei wird zwischen Maschinen-Hersteller und -Nutzer eine Wartungsvereinbarung getroffen und mittels Smart Contract werden die entsprechenden Wartungsintervalle koordiniert. So werden über die Blockchain automatisiert die Wartungen beauftragt und sind dabei vom Kunden (Maschinennutzer) jederzeit transparent einsehbar.

Primäres Ziel dieses Use Case stellt die Reduzierung des administrativen Aufwandes für den Maschinennutzer dar.

Use Case Definition

Tabelle 3-11: Use Case Definition - Instandhaltungs-Automatisierung mittels Smart Contracts

Name	Instandhaltungs-Automatisierung mittels Smart Contracts
Ziele	• Automatisierte Wartungsaufträge zur Erfüllung der Maschinen-Service-Vereinbarung • Reduzierung der administrativen Schritte • Transparenz für den Kunden (=Maschinennutzer)
Akteure/Rollen	• Maschinenhersteller – führt Wartung durch • Kunden – Nutzt Maschine • Smart Contract – Node
Trigger	• Aktivierung des Services mittels Erstellung des Smart Contracts

Essenzielle Schritte	• Erstellung einer Abbildung der Maschine • Erstellung des Smart Contracts nach vereinbarten Kriterien • Auslösung des Smart Contracts nach vereinbarten Bedingungen • Ende der Laufzeit: Contract „Suicide“
Techn. Anforderungen	• Schnittstelle – Smart Contract → Wartungsbeauftragung • Nutzung einer allgemeinen Blockchain-Plattform möglich (keine eigene Blockchain notwendig)
Entwicklungs-Anforderungen	• Erstellung der Smart Contracts ○ Alternative Ereignisse – komplettausfall der Maschine müssen berücksichtigt werden

Funktionalitäten/Funktionelle Anforderungen

- Erstellung der Smart Contracts mittels Client Software
- Automatisierte Calls aus den Smart Contracts zu vorgegebenen Schnittstellen
- Möglichkeit zur Einsicht aller bestehenden Smart Contracts

Nicht-Anforderungen

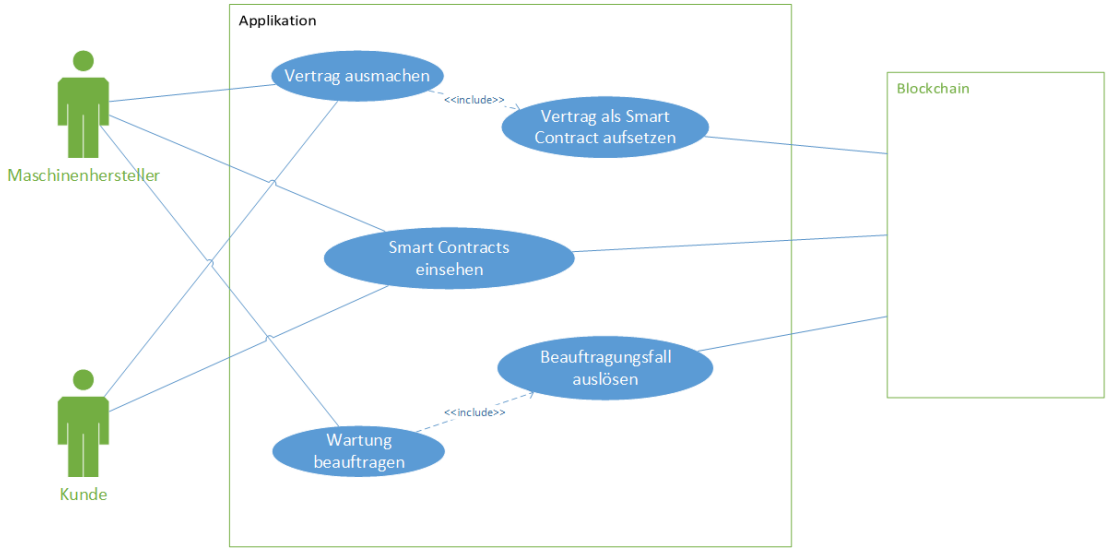
- Handling der Kommunikation und Daten nach Auftragsgabe
- Integration von IoT Geräten in den Prozess (siehe Extrapolation)

UML Beschreibung

Im Folgenden zu finden sind nun die UML-Diagramme, die den Use Case auf der Program Design Ebene beschreiben. Unter den jeweiligen Abbildungen sind jeweils entsprechende Erläuterungen zu finden.

Anwendungsfalldiagramm

Abbildung 3-18: Use Case 2 - Anwendungsfalldiagramm



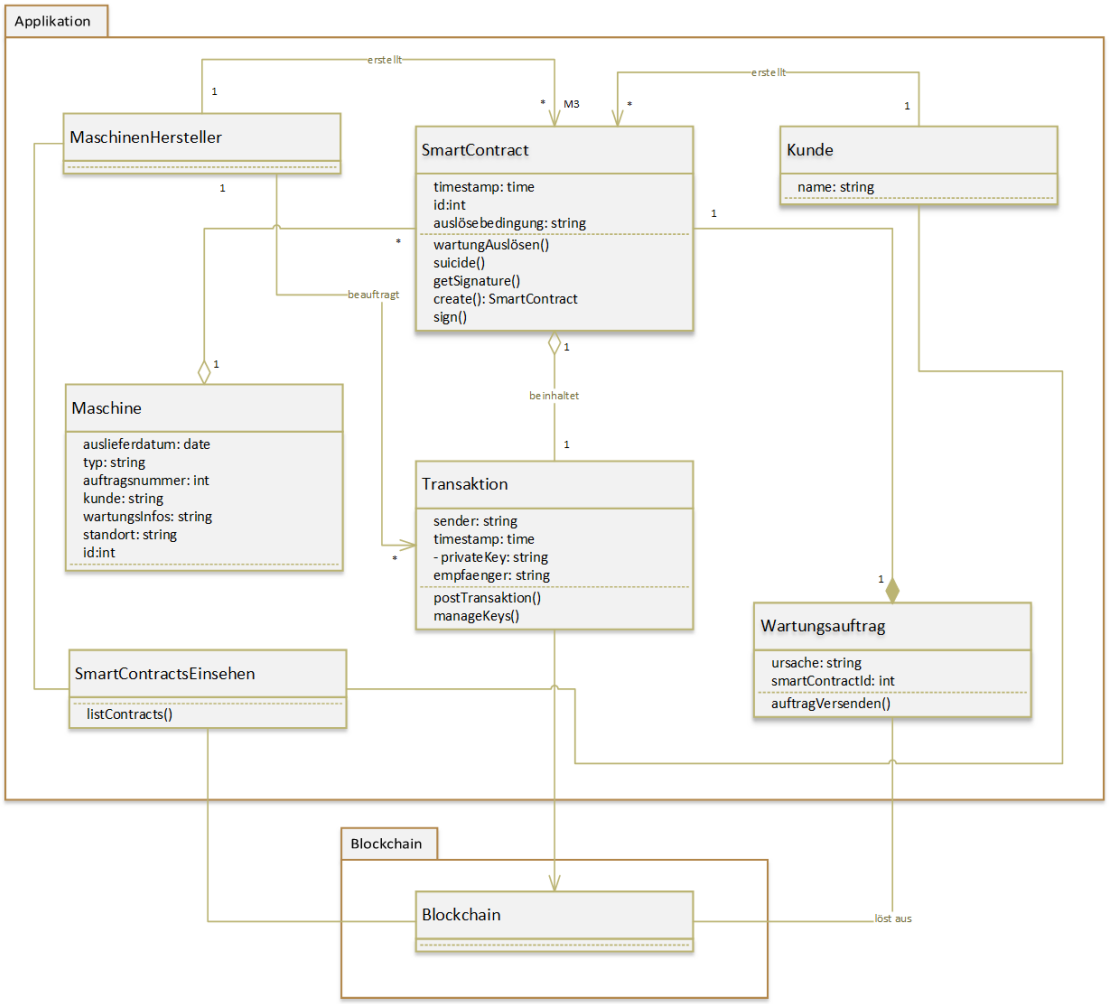
Entsprechend dem Anwendungsfalldiagramm ist zu sehen, dass die primären Anwendungsfälle die Erstellung der Smart Contracts sowie die Beauftragung der Wartung sind. Alle weiteren Anwendungsfälle sind entweder untergeordnete Fälle oder fortführende Schritte.

Die wichtigsten Aspekte der Applikation sind folgende:

- Abmachungen bezüglich Maschinenwartung wird mittels Smart Contract festgehalten
  - Maschinenhersteller und -nutzer durchlaufen hierfür einen Erstellungs-Prozess, bevor der von beiden Seiten verifizierte Smart Contract auf
- Die Abmachungen bezüglich Maschinen-Wartung beziehen sich primär auf festgelegte Zeitintervalle, nach denen automatisch die Beauftragung durchgeführt wird.
- Wird eine Beauftragung durchgeführt, wird mittels Applikations-Clients eine Nachricht an das Hersteller-Unternehmen sowie an das Nutzer-Unternehmen gesendet.
- Ebenso gibt es die Möglichkeit die einem Unternehmen zugehörigen Smart Contracts und somit die geplanten Wartungsaufträge jederzeit einzusehen.
- Als Blockchain-Netzwerk kann hier entweder eine selbst aufgesetzte Private Blockchain herangezogen oder ebenso eine öffentliche Blockchain wie Ethereum genutzt werden. Insbesondere, da die notwendige Performanz und Größe der Datenpakete relativ gering sind, ist die Leistung von Public Blockchains hier ausreichend.

Klassendiagramm

Abbildung 3-19: Use Case 2 - Klassendiagramm

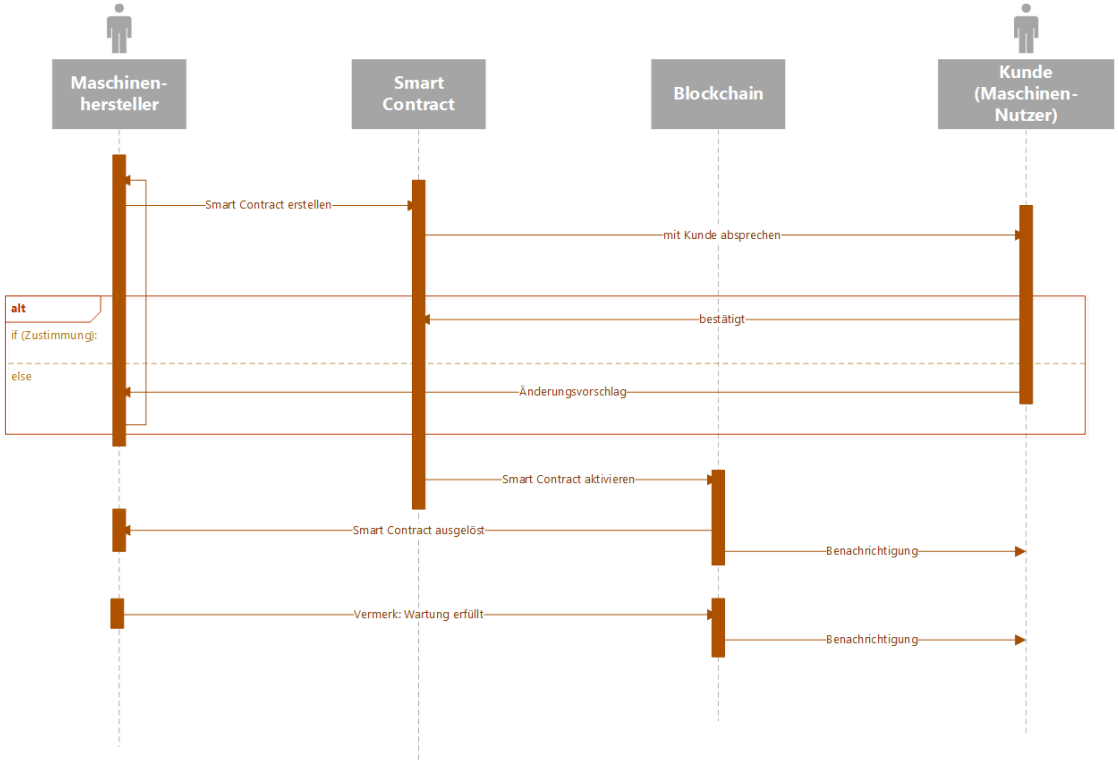


Im Klassendiagramm ist zu erkennen, dass alle relevanten Daten in der Klasse Smart Contract bzw. Transaktion gesammelt und dann an die Blockchain übergeben werden. Von dort erfolgt auch der Trigger für die Auslösung eines Wartungsauftrages.

Die Methode listContracts() dient zur Einsicht in alle bestehenden einem Unternehmen zugehörigen Smart Contracts. Diese ist auch von dem Prozess der Smart Contract Erstellung bis hin zur Wartungsbeauftragung herauszunehmen, da es sich hier um eine eigenständige Operation handelt.

Sequenzdiagramm

Abbildung 3-20: Use Case 2 - Sequenzdiagramm



Dem Sequenzdiagramm ist zu entnehmen, dass entsprechend auch der Nachrichtenfluss zu Beginn darin besteht, die notwendigen Informationen im Smart Contract zu bündeln, bevor diese Infos gesammelt an die Blockchain übergeben werden. Diese löst im Wartungsfall dann eine Transaktion (Benachrichtigung) an Maschinenhersteller und -nutzer aus und im Anschluss wird ebenso auf der Blockchain die Durchführung der Wartung auf der Blockchain vermerkt. Dadurch entsteht eine durchgängige und jederzeit einsehbare Aufzeichnung der Wartungsaktivitäten.

Extrapolation

- Durch Integration von IoT Sensorik, könnten durch andere Ereignisse ebenso Wartungen beauftragt werden. Denkbar wären hier überschreiten gewisser Grenzwerte (Temperatur, Verschmutzung im Schmierstoff oder Schwingungsanalyse) wie sie in vielfacher Form durch entsprechende IoT-Sensorik aufgezeichnet werden können.

- Einbindung weiterer Dienstleister: Maschinenhersteller kann weitere Dienstleister mit einbeziehen, wobei durch den Smart Contract eben diese Dienstleister direkt beauftragt werden können, anstatt die Wartung vom Maschinenhersteller selbst durchführen zu lassen.

4 Schlussfolgerung & Resümee

Nach wie vor ist das Thema Blockchain in den Medien und tendenziell auch in wissenschaftlichen Publikationen vor allem durch eine Betrachtung in Bezug auf Kryptowährungen und Bitcoin präsent. Diese Arbeit versucht eine Betrachtungsweise zu liefern, die weit über die Nutzbarkeit von Kryptowährungen hinausgeht.

Im Rahmen der Recherche zu dieser Arbeit hat sich gezeigt, dass der Nutzen auch oft erst im Hintergrund erkennbar wird. Wobei die eigentliche Geschäftslogik und die Prozesse die gleichen sind, jedoch die IT Architektur im Hintergrund angepasst wird, um die konkreten Vorteile der Blockchain zu nutzen.

Konkrete Vorteile im Rahmen der Nutzung entlang des Product Life Cycle zeigen sich der Natur von Peer-to-Peer Netzwerken entsprechend in jenen Fällen, wo mehrere Parteien zusammenarbeiten und Daten austauschen müssen.

Auffallend ist hierbei, dass die meisten Use Cases mit anderer, bereits länger etablierter Technologie, ebenfalls lösbar sind. Je nach konkreter Ausprägung und Anforderungen, kann die Nutzung einer Blockchain aufgrund der systematisch bedingten Eigenschaften eines solchen Systems besser geeignet sein.

Unter Umständen bietet ein Blockchain System in manchen Fällen ein Kostensenkungs-Potenzial. Insbesondere dann, wenn eine Realisierung mittels zentralistischer Lösungen eine komplexe Struktur von Datenbanken und Abgleich-Prozessen erfordert.

Ebenso die Robustheit und Resilienz gegen unerlaubtes Einwirken oder schlichte menschliche Fehler macht die Blockchain in jenen Fällen, wo auf diese Aspekte ein besonderer Schwerpunkt gesetzt wird, zu einer relevanten Möglichkeit. Dazu tragen primär die Aspekte der Nachvollziehbarkeit und die nachträgliche Unveränderbarkeit von Blockchain-Transaktionen bei.

Ebenso bemerkbar sind nach wie vor konkrete Limitierungen der Technologie. Vor allem fehlen einfach zu konfigurierende, nutzerfreundliche, umfangreiche Blockchain-Produkte, sowie etablierte Standards und Lösungen.

Bezüglich der leistbaren Effizienz von Blockchain-Systemen zeigt sich, dass es bereits Projekte und Lösungen am Markt gibt, die diese Limitierungen vereinzelt oder insgesamt zu lösen versuchen. Und das mit teilweise gut nutzbaren Ergebnissen.
Da sich die Technologie aber noch in einer relativ frühen Phase der massentauglichen Nutzung befindet, kann davon ausgegangen werden, dass sich die Effizienzprobleme mit der Zeit durch den Entwicklungsfortschritt lösen werden.

Ähnlich wie bei der Entwicklung des Computers und des Internets, die zu Beginn nur begrenzte Use Cases boten und denen große Zweifel entgegengebracht wurde, könnte es auch bei der Nutzung der Blockchain sein. Die technologische Entwicklung des Computers hat gezeigt, dass mit fortschreitender Effizienzsteigerung immer mehr Anwendungsmöglichkeiten für den Computer hervortraten. So ähnlich wird vermutlich der Fortschritt der Blockchain voranschreiten.

Ebenso die Weiterentwicklung der Hardware und Netzwerk - Kapazitäten in den Unternehmen, wird die Nutzung einer Blockchain-Lösung praktikabler machen. Wenn man nun zum Beispiel die Bitcoin Blockchain als Vergleich hernimmt, so beträgt die Größe der gesamten Blockchain Anfang des Jahres 2019 etwa 210 GB.[1]
Sie befindet sich also in einem Rahmen an notwendiger Speicherkapazität, den ein handelsüblicher Rechner jedenfalls liefern kann.

Bezüglich Übertragungsrate der Netzwerke, trägt in Zukunft vermutlich auch die Einführung von 5G Kapazitäten in etwa im Jahr 2020 zur effektiveren Nutzung von Blockchain Systemen bei. Bei einer maximalen Übertragungsrate von 1250 MB/s (Vergleich: LTE: 125MB/s) würde der Komplettdownload der Bitcoin Blockchain in der jetzigen Größe ein paar Minuten dauern.[2]

Ebenso kann man davon ausgehen, dass sich das Problem der ausreichend hohen Transaktionsgeschwindigkeiten lösen wird, wie es teilweise bei Plattformen wie NEO oder EOS schon der Fall ist. Hier bleibt jedoch abzuwarten, welcher Consensus-Mechanismus als wirklich sicher und äquivalent zum Proof of Work Mechanismus angesehen werden kann, bei gleichzeitiger Effizienzsteigerung.

Bezüglich weiterer Fortschritte kann davon ausgegangen werden, dass die Innovationstreiber entsprechend finanzstarke Schlüsselbranchen sein werden. Hier haben sich bereits die Finanzbranche, Energie, Logistik und Versicherungen etabliert. Mit fortschreitender Nutzbarkeit im Bereich IoT ist davon auszugehen, dass sich auch verstärkt die Industrie mit der Thematik beschäftigen wird. Insbesondere, da zu Beginn des Jahres 2019 erste robust arbeitende und funktionale Lösungen nutzbar sind, die für Proof of Concept Projekte herangezogen werden können.

Aufgrund der hohen Investitionskosten zeigt sich auch, dass primär große Konzerne an umfassenden Industrie-Lösung in Form von Kooperations-Projekten arbeiten. Als gutes Beispiel ist hier die Hyperledger-Foundation anzusehen, wo unter anderem IBM mit Hyperledger Fabric stark im Bereich Blockchain an Fortschritten arbeitet. Bezüglich der konkreten Nutzung im industriellen Umfeld, hat sich die Blockchain-Technologie als Enabler für Intellectual Property Anwendungen sowie die Abbildung verschiedener Entitäten im Netzwerk als mögliche Lösung herausgestellt.

Als Hemmnisse für die Technologie könnten sich im Vergleich zu den technologischen Aspekten eher soziale und organisatorische Aspekte herausstellen. So werden sich durch die veränderten Geschäftsprozesse und -modelle vermutlich neue Formen der Kooperationen unter Supply-Chain-Teilnehmern sowie eventuell auch unter Mitbewerbern ergeben. Um ein gemeinsames Netzwerk nutzen zu können, bedarf es aber natürlich der Akzeptanz aller Teilnehmer, wie sie im bisherigen Umgang noch nicht existiert hat.
Diese Art der Umstellung erfordert tendenziell auch eine gewisse Mind-Set Anpassung über technologische Aspekte hinaus. Insbesondere, wenn noch nicht genug Vertrauen in eine Technologie vorhanden ist, vor allem aufgrund fehlender umfangreicher Erprobung.

[1] Vgl. https://www.blockchain.com/de/charts/blocks-size zuletzt gelesen am 24.02.2019
[2] Vgl. https://www.lte-anbieter.info/5g/ zuletzt gelesen am 24.02.2019

Ebenso ein großes Hindernis stellt vermutlich die Tatsache dar, dass viele Unternehmen tendenziell noch nicht vollständig digitalisiert sind. Da für die Nutzung einer Blockchain eine digitale Abbildung der zu nutzenden Entitäten auf der Blockchain notwendig ist, steht also der Schritt der Digitalisierung noch zwischen vielen Unternehmen und der Einführung eines Blockchain Systems. Hier bietet sich jedoch die Gelegenheit, im Rahmen der Digitalisierung unmittelbar Blockchain-Systeme in die Infrastruktur integrieren zu können.

Insbesondere die Möglichkeit zur nahtlosen Integration von Blockchain-System in bestehende Netzwerke und die mögliche Anpassung an die Bestehenden Geschäftsprozesse wird vermutlich einen kritischen Aspekt zur Einführung von Blockchain-Systemen bilden. So ist es selbstverständlich, dass aufgrund der Transparenz einer Blockchain Unternehmen Hemmnisse haben, ihre Daten und Prozesse offenzulegen und mit allen anderen Netzwerk-Teilnehmern zu teilen. Dementsprechend werden diese eher Blockchain-Systeme nutzen, bei der eine entsprechende Privatsphäre gewährleistet werden kann.

Ebenso ist davon auszugehen, dass jene Plattformen erfolgreicher sein werden, die sich in bestehende IT-Strukturen integrieren lassen und entsprechende Schnittstellen bieten. Dass Unternehmen zur Einführung einer Blockchain-Plattform ihr gesamtes System umstrukturieren ist eher unwahrscheinlich. Diese Sichtweise lässt vermuten, dass somit nicht notwendigerweise die innovativsten Blockchain-Lösungen am ehesten genutzt werden, sondern diejenigen, da möglichst geringe Adaptions-Anforderungen stellen, die Investitionskosten niedrig halten und bestehende Systeme nicht beeinträchtigen. Dies wird vermutlich über SaaS (Software as a Service) - ähnliche Angebote und Hybrid-Blockchain Lösungen realisiert werden, in den das bestehende System mit einem Blockchain-Layer kombiniert wird.

Natürlich ist es auch möglich, dass bei Blockchain-Projekten das System selbst entwickelt wird. Dabei ist dann anzunehmen, dass der Code nicht vollständig selbst entwickelt wird. Durch die Open Source Eigenschaften ist der Code vieler Plattformen problemlos zugänglich. Als Beispiel hat im Rahmen dieser Arbeit unter anderem auch die Energy Web Foundation gedient, die aufbauend auf dem Ethereum Code eine eigen Blockchain entwickelt hat, die ihren Bedürfnissen entspricht.

Ob nun die Nutzung einer Blockchain-Plattform sinnvoll ist, hängt vor allem von den konkreten Zielen bezüglich der Anwendung ab. So ist es sicherlich nicht sinnvoll, ein gut erprobtes und funktionierendes zentralisiertes System krampfhaft umzustellen, um alles in einer Blockchain realisieren zu können. Tendenziell ist es nur dort anzuraten, wo entsprechende zentralisierte Nutzung erheblich komplexer ausfallen würde oder es entsprechende Möglichkeiten in zentralisierter Form schlicht nicht gibt.

Somit ist die Entscheidung für eine Blockchain tendenziell weniger von technischen Spezifikationen abhängig, da die meisten Use Cases über mehrere Wege gelöst werden können. Viel mehr kommt es darauf an, ob die Blockchain im betrachteten Fall mehr Vorteile bietet als zentralisierte Systeme. Hier kann vor allem die Aufstellung der Vor- & Nachteile im Kapitel Beurteilung, Kategorisierung und Extrapolation“ dieser Arbeit eine Hilfestellung bieten.

Wie bereits zu Beginn erwähnt, liefert die vorliegende Arbeit eine spezifische Betrachtungsweise und muss als konkreter Blickwinkel auf das Thema Blockchain aus der Richtung des industriellen Umfelds betrachtet werde.

Wenn auch im Zuge der Bearbeitung versucht wurde, von konkreten Projekten und Inhalten auf möglichst generische Beurteilungen und Aspekte überzugehen, schließt diese Arbeit dennoch bewusst die Betrachtung von nicht mit dem Product Life Cycle direkt in Verbindung stehenden Bereichen aus. So bestehen sicher weitere Möglichkeiten zur Kostensenkung unter anderem in Bezug auf die Nutzung im Bereich Wirtschaftsprüfung, Versicherungen und Unternehmens-Forensik.
Durch die möglichst generische Betrachtungsweise wurde versucht einen Ausblick zu geben, wie sich die Nutzbarkeit der Blockchain-Technologie darstellt und welche Vorteile und Limitierungen derzeit in Bezug auf die industrielle Nutzung bestehen bzw. in absehbarer Zeit weiter bestehen werden.

Mittels der Präsentation zweier selbst entwickelter, möglichst generischer Use Cases sollte beispielhaft dargelegt werden, wie einzelne Funktionalitäten zur Nutzung im Product Life Cycle realisiert werden.

Abzuwarten bleibt, wie sich die Entwicklung der Blockchain-Technologie weiter fortsetzen wird und wie stark die Nutzung durch Unternehmen im industriellen Umfeld ausfallen wird. Laut Schätzungen des World Economic Forum soll 2025 insgesamt 10% des weltweiten Bruttoinlandsproduktes mit Hilfe der Blockchain-Technologie abgewickelt werden.[1] In wie fern sich der Wandel zur Nutzung von Blockchain-Netzwerken sich in diesem Umfang etablieren wird bleibt ab zu warten. Auf jeden Fall wird es hierfür notwendig sein, dass die Technologie im richtigen Maß eingesetzt wird und ihren Vorteilen und Limitierungen entsprechend, wie es in dieser Arbeit aufgezeigt wurde.

[1] Vgl. https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini/ zuletzt gelesen am 28.02.2019

5 Literaturverzeichnis

- 5G Bandbreite: https://www.lte-anbieter.info/5g/ zuletzt gelesen am 24.02.2019
- About IBM Food Trust, Abgerufen von https://www.ibm.com/downloads/cas/EX1MA1OX am 21.01.2019
- Account & Adresse: http://ethdocs.org/en/latest/account-management.html zuletzt gelesen am 15.12.2018
- Adresse aus Public Key: https://blockchain.zendesk.com/hc/en-us/articles/360000951966-Public-and-private-keys zuletzt gelesen am 15.12.2018
- Antonopoulos A. (2015), Mastering Bitcoin, O'Reilly Media, Sebastopol, USA
- Anzahl der IoT-Geräte weltweit: https://de.statista.com/statistik/daten/studie/537093/umfrage/anzahl-der-vernetzten-geraete-im-internet-der-dinge-iot-weltweit/ zuletzt gelesen am 03.02.2019
- Asymatrische Kryptografie: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography zuletzt gelesen am 19.12.2018
- Base58 Coding: https://en.bitcoin.it/wiki/Base58Check_encoding zuletzt gelesen am 15.12.2018
- Bashir I. (2017), *Mastering Blockchain: Distributed ledgers, decentralization and smart contracts explained*, Packt Publishing Ltd., Birmingham, UK
- Bauernhansl T., Hompel M. & Vogel-Heuser B. (Hrsg.), 2014, *Industrie4.0 in Produktion, Automatisierung und Logistik: Anwendung, Technologien, Migration*, Springer Fachmedien, Wiesbaden, Deutschland
- Benet J., IPFS – Content Addressed, Versioned, P2P File System, Draft 3, abgerufen von: https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf
- Bitcoin Transaktion per Radio-Frequenz: https://usethebitcoin.com/sending-bitcoin-without-internet-or-satellite-is-now-a-reality/ zuletzt gelesen am 16.12.2018
- Bitkom Umfrage: https://www.bitkom.org/Presse/Presseinformation/Blockchain-wird-zu-einem-Top-Thema-in-der-Digitalwirtschaft.html zuletzt gelesen am 15.01.2018
- Blechschmidt B. & Stoecker C., How Blockchain Can Slash the Manufacturing "Trust Tax", The Genesis of Things Project White Paper, Hrsg. The Genesis of Things Project
- Boucher P., 2017, How blockchain technology could change our lives, European Parliamentary Research Service, HRSG: Scientific Foresight Unit (STOA), Brüssel, Belgien
- Burgwinkel D. (2016), *Blockchain Technology: Einführung für Business- und IT Manager*, Hrsg. Dr Daniel Burgwinkel, Basel, Schweiz
- Carsharing Use Case: https://shareandcharge.com/ zuletzt gelesen am 20.01.2019
- Computerkriminalität: https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/#0 zuletzt gelesen am 15.01.2019
- Coulouris G., Dollimore J. & Kindberg T. (2001), *Distributed Systems: Concepts and Design*, Pearson Educated Limited
- Definition Ledger: http://www.businessdictionary.com/definition/ledger.html zuletzt gelesen am 13.12.2018

- Deng et al., 2018, Research on Cross-Chain Technology Based on Sidechain and Hash-Locking, Springer International Publishing, Chem, Schweiz
- Dietricht V. et al., 2017, *Application of Blockchain Technology in the Manufacturing Industry*, Hrsg. Frankfurt School Blockchain Center, Frankfurt, Deutschland
- Digital Identity: https://www.informatik-aktuell.de/betrieb/virtualisierung/blockchain-trifft-digital-identity.html zuletzt gelesen am 21.02.2019
- Digtiale Signatur: https://blockgeeks.com/what-is-hashing-digital-signature-in-the-blockchain/ zuletzt gelesen am 19.02.2018
- Distributed Ledger: https://tradeix.com/distributed-ledger-technology/ zuletzt gelesen am 13.12.2018
- Distributed Ledger & Blockchain Zusammenhang: https://hackernoon.com/gaining-clarity-on-key-terminology-bitcoin-versus-blockchain-versus-distributed-ledger-technology-7b43978a64f2 zuletzt gelesen am 10.04.2019
- Eigner M. & Stelzer R., 2009, *Product Lifycycle Management: Ein Leitfaden für Product Development und Life Cycle Management*, Springer-Verlag Berlin-Heidelberg, Heidelberg, Deutschland
- EOS:https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md zuletzt gelesen am 04.01.2019
- Ether: https://www.ethereum.org/ether zuletzt gelesen am 12.12.2018
- Ethereum: http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html zuletzt gelesen am 03.01.2019
- Everledger Beschreibung: https://www.altoros.com/blog/a-close-look-at-everledger-how-blockchain-secures-luxury-goods/ zuletzt gelesen am 27.01.2019
- Everledger Solutions: https://www.everledger.io/industry-applications zuletzt gelesen am 27.01.2019
- Everledger: https://www.everledger.io/ zuletzt gelesen am 27.01.2019
- Forks: https://bitcoin.org/en/glossary/fork zuletzt gelesen am 21.12.2018
- Galvin D., 2017, IBM and Walmart: Blockchain for Food Safety, Abgerufen von: https://www-01.ibm.com/events/wwe/grp/grp308.nsf/vLookupPDFs/6 Using Blockchain for Food Safe 2/$file/6 Using Blockchain for Food Safe 2.pdf am 21.01.2019
- Genesis of Things: http://www.genesisofthings.com/ zuletzt gelesen am 02.02.2019
- Ghosh S. (2007), *Distributed Systems: An Algorithmic Approach*, Taylor & Francis Group, Boca Raton, USA
- Gridsingualrity: https://gridsingularity.com/about/ zuletzt gelesen am 10.02.2019
- Gubbi J. et al, 2013, Internet of Things (IoT): *A vision, architectural elements, and future directions*, Future Generation Computer Systems,Volume 29, Issue 7, Elsevier Publishing
- Gupta S. & Sadoghi M. (2018), *Blockchain Transaction Processing*, Department of Computer Science, University of California, Davis, USA
- Hartnett S. et al., 2018, *The Energy Web Chain: Accelerating the Energy Transition with an Open-Source Decentralized Blockchain Platform*, HRSG: Energy Web Foundation
- http://www.stadtzug.ch/de/bevoelkerung/dienste/digitaleid/?action=showthema&themenbereich_id=1587&thema_id=5295 zuletzt gelesen am 22.01.2019
- https://www.iota.org/get-started/what-is-iota zuletzt gelesen am 04.01.2019
- Hyperledger: https://www.hyperledger.org/ zuletzt gelesen am 05.01.2019
- Hyperledger: https://www.hyperledger.org/about zuletzt gelesen am 05.01.2019

- Hyperledger: https://www.hyperledger.org/projects zuletzt gelesen am 05.01.2019
- IBM Supply Chain Blockchain: https://www.ibm.com/blockchain/solutions/food-trust zuletzt gelesen am 21.01.2019
- Industrie 4.0: https://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html;jsessionid=D7ED4118DED525F176F382A8F939369D zuletzt gelesen am 02.12.2018
- IoT: https://www.itwissen.info/Internet-of-things-IoT-Internet-der-Dinge.html zuletzt gelesen am 01.12.2018
- IOTA: https://docs.iota.org/docs/the-tangle/0.1/introduction/overview zuletzt gelesen am 04.01.2019
- Johansen S., 2016, *A comprehensive Literature Review on the Blockchain Technology as a Technological Enabler for Innovation*, Copenhagen Business School, Kopenhagen, Dänemark
- Kaufmann T., 2015, *Geschäftsmodelle in Industrie 4.0 und dem Internet der Dinge: Der Weg vom Anspruch in die Wirklichkeit*, Springer Fachmedien Verlag, Wiesbaden, Deutschland
- Kirstein F., Polzhofer M. & Eckert K., 2017, *Digitale Identitäten in der Blockchain: Erfahrungen aus der Entwick*lung, Fraunhofer-Institut für offene Kommunikationssysteme Fokus, Berlin, Deutschland
- Mattern F., Floerkemeier C. (2010) *From the Internet of Computers to the Internet of Things*. In: Sachs K., Petrov I., Guerrero P. (eds) From Active Data Management to Event-Based Systems and More. Lecture Notes in Computer Science, vol 6462. Springer Verlag, Berlin, Deutschland
- McLean S. & Deane-Johns S., 2016, Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?, Morrison & Foerster LLP, Client Alert
- Minging: http://ethdocs.org/en/latest/mining.html zuletzt gelesen am 18.12.2018
- Nakamoto S. (2008), Bitcoin: A Peer-to-Peer Electronic Cash System
- *NEM: Technical Reference*, *Version 1.0,* 2015, Aufgerufen von https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf
- Neo Consensus: https://docs.neo.org/en-us/basic/consensus/consensus.html zuletzt gelesen am 03.01.2019
- Neo Consensus: https://docs.neo.org/en-us/basic/consensus/whitepaper.html zuletzt gelesen am 03.01.2019
- NEO: https://neo.org/ zuletzt gelesen am 03.01.2019
- Ploom T., 2016, *Blockchain Technology: Einführung für Business- und IT Manager*, Hrsg. Dr Daniel Burgwinkel, Basel, Schweiz
- Popov S., 2017, *The Tangle*, Version 1.3
- Prognose World Economic Forum: https://www.weforum.org/agenda/2018/03/blockchain-bitcoin-explainer-shiller-roubini/ zuletzt gelesen am 28.02.2019
- Public & Private Blockchains: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ zuletzt gelesen am 20.12.2018
- Public versus Private Blockchains White Paper, 2015, Version 1.0
- Rosenberger P., 2018, *Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik*, Springer Verlag, Berlin, DE
- Santos M. & Eisenhardt M., 2005, *Organizational boundaries and theories of organization*, Organization Science, vol. 16, no. 5

- Scherk J. & Pöchhacker-Tröscher G., 2017, *Die Blockchain –Technologie-feld und wirtschaftliche Anwendungsbereiche*, HRSG: Pöchhacker-Tröscher Innovation Consulting GmbH
- Sidechains: https://hackernoon.com/what-are-sidechains-1c45ea2daf3 zuletzt gelesen am 16.12.2018
- Sidechains: https://thenextweb.com/hardfork/2018/12/11/blockchain-sidechains-explained-basics/ zuletzt gelesen am 16.12.2018
- Smart Contracts: http://ethdocs.org/en/latest/contracts-and-transactions/contracts.html zuletzt gelesen am 20.12.2018
- Swan M., *Blockchain: Blueprint for a new economy*, O'Reilly Media, Sebastopol, USA
- Tapscott D. & Tapscott A. (2016), *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world,* Penguin Random House LLC, New York, USA
- The Tangle: https://www.iota.org/research/meet-the-tangle zuletzt gelesen am 04.01.2019
- Transaktionen Visa: https://mybroadband.co.za/news/security/190348-visanet-handling-100000-transactions-per-minute.html zuletzt gelesen am 04.01.2019
- Vajna S. et al., 2018*, CAx für Ingenieure: Ein praxisbezogener Leitfaden*, Springer Vieweg Verlag, Berlin, Deutschland
- Van Steen M. & Tanenbaum A. (2016), *A brief introduction to distributed systems*, Springer Verlag
- Vaultitude: https://vaultitude.com/index.html zuletzt gelesen am 27.01.2019
- VeChain: https://www.vechain.org/ zuletzt gelesen am 10.02.2019
- Vergleich: Ethereum & NEO: https://coinsutra.com/neo-vs-ethereum-differences/ zuletzt gelesen am 03.01.2019
- Voelkel O., 2017, *Initial Coin Offerings aus kapitalmarktrechtlicher Sicht*, ZTR, Ausgabe 03/2017
- Voshmgir S. & Kalinov V. (2017), *Blockchain: A Beginners Guide*, Hrsg.: https://blockchainhub.net/
- Wattenhofer R., *The Science of the Blockchain*, Inverted Forest Publishing
- Wien Energie Blockchain Projekte: Tennet Blockchain Projekte: https://www.tennet.eu/de/unsere-kernaufgaben/innovationen/blockchain-technologie/ zuletzt gelesen am 10.02.2019
- WRMHL Architecture: https://ponton.de/wrmhl/ zuletzt gelesen am 10.02.2019
- Wüst K. & Gervais A., 2017, *Do you need a Blockchain?*, Department of Computer Science, ETH Zürich, Zürich, Schweiz
- Zenodys Technical White Paper: Organizing the digital world with blockchain; Q2 – 2018, Version 0.95, abgerufen von: http://zz.zenodys.com/zenodys-technical-whitepaper.pdf
- Zenodys White Paper: Organizing the digital world with blockchain; Q2 – 2018, Version: 0.95, abgerufen von: http://zz.zenodys.com/zenodys-whitepaper.pdf

6 Abbildungsverzeichnis

7 Tabellenverzeichnis

8 Anhang

8.1 Abkürzungsverzeichnis

bzw.	beziehungsweise
etc.	et cetera
ggf.	gegebenenfalls
Evtl.	Eventuell
IT	Informations-Technologie
P2P	Peer-to-Peer
M2M	Machine-to-Machine
IoT	Internet of Things

8.2 Zitierweise

Als Zitierweise wird die Deutsche Zitierweise mit Fußnoten verwendet.

https://www.wissenschaftliches-arbeiten.org/zitieren/deutsche-zitierweise.html

8.3 Tabelle der verwendeten Quellen für Mind-Map

Titel	**Autor(en)**	**Erschei-nungsjahr**	**Dokument-Typ**	**Quelle**
Do you need a blockchain	Wüst K. & Gervais A.	2017	Paper	Google Scholar
Opportunities of Blockchain for Industry 4.0 - Energy Impacts for the Industrial Internet of Things	Rapp K.	2018	Master-Arbeit	TU Bibliothek
Application of Blockchain Technology for the Charging Infrastructure of Electric Vehi-cles	Zöhrer S.	2018	Master-Arbeit	TU Bibliothek

Evaluating the Applicability of Blockchains in the Pharmaceutical Supply Chain	Zamponi G.	2018	Master-Arbeit	TU Bibliothek
Enabling the Blockchain in the Internet of Things	Krejci S.	2018	Diplomarbeit	TU Bibliothek
Modellierung möglicher Blockchain-Applikationen im Kontext erneuerbarer elektrischer Einspeisung	Hemm R.		Diplomarbeit	TU Bibliothek
Digital Supply Chain Transformation toward Blockchain Integration	Korpela K., Hallikas J. & Dahlber T.	2017	Paper	Google Scholar
Digital Assets on Public Blockchains	BitFury Group	2016	Whitepaper	
Blockchain	Nofer M. et al	2017	Paper	Google Scholar
Blockchain Platform for Industrial Internet of Things	Bahga A. & Madisetti V.	2016	Paper	Google Scholar
Blockchain in Internet of Things: Challenges and Solutions	Dorri A., Kanhere S. & Jurdak R.		Paper	Google Scholar
Blockchain for the Internet of Things: a Systematic Literature Review	Conoscenti M. Vetro A. & De Martin J.		Paper	Google Scholar
Blockchain Revolution	Tapscott D. & Tapscott A.	2017	Fachbuch	
Building Blockchain Projects	Prusty N.	2017	Fachbuch	
Ethereum: The Insider Guide to Blockchain Technology, Cryptocurrency and Mining Ethereum	Ozer R.	2017	Fachbuch	
Blockchain: Blueprint for a New Economy	Swan M.	2015	Fachbuch	
BlockChain Technology: Beyond Bitcoin	Crosby et al.	2015	Paper	
Application of Blockchain Technology in the Manufacturing Industry	Dietricht V. et. al	2017	Working Paper	Frankfurt School Blockchain Center
Blockchain for Dummies	Laurence T.	2017	Fachbuch	
Blockchain Technology	Burgwinkel D.	2016	Fachbuch	

Mastering Blockchain	Bashir I.	2017	Fachbuch	
Blockchain: Understanding the Technology	Lee B.			
Blockchain Austria			Organisation	
Artikel: IBM: Die Blockchain verlässt das Labor			Artikel	Link
Blockchain Landscape Austria			Artikel	Link