DONAU-UNIVERSITÄT KREMS
Department für E-Governance in Wirtschaft und Verwaltung
Dr.-Karl-Dorrek-Str. 30
A - 3500 Krems

Blockchain als Treiber von (Open) Innovation

Eine Analyse des Potentials der Distributed-Ledger-Technologie vor dem Hintergrund unternehmensgrenzüberschreitender Innovationsprozesse

Master Thesis
im Rahmen des universitären Weiterbildungsprogramms
Professional MSc Management und IT,
Spezialisierung – IT Consulting

eingereicht von:
Robert Buchner

Betreuer:
Mag. Dr. Alexander Pfeiffer, MA, MBA

1. September 2019

EIDESSTATTLICHE ERKLÄRUNG

Ich, Robert Buchner, geboren am 29. Juni 1982 in Wels erkläre,

1. dass ich meine Master Thesis selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,

2. dass ich meine Master Thesis bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

3. dass ich, falls die Master Thesis mein Unternehmen oder einen externen Kooperationspartner betrifft, meinen Arbeitgeber über Titel, Form und Inhalt der Master Thesis unterrichtet und sein Einverständnis eingeholt habe.

....

Ort, Datum Unterschrift

DANKSAGUNG

Vorweg möchte ich meinen Großeltern und meiner Lebensgefährtin Elisabeth großen Dank aussprechen; sie haben mich durch alle Phasen des Studiums hinweg unterstützt und indem sie nicht aufhörten an mich zu glauben, gaben sie mir stets Kraft um voranzuschreiten. Ich danke meinen beiden Töchtern (Melissa und Marianne) u.a. für ihr Verständnis, dass ihr Vater die letzten Monate weniger Zeit mit ihnen verbringen konnte, und es diesen Sommer hindurch relativ wenig Familien-Ausflüge, sowie leider auch keinen Familien-Urlaub gab. Speziell meiner jüngeren Tochter, möchte ich hier für die Nächte danken, in denen sie ruhig schlief und nicht schrie, und es mir dadurch möglich war, mich besser zu konzentrieren und daher mehr Arbeitsfortschritt (wie in ‚lauteren' Nächten) erzielen konnte. Meinen Freunden (Gösta und Gertrud), die trotz des schönen Sommer-Wetters und ihren Alltags-Verpflichtungen ausreichend Zeit fanden, um meine Arbeit Korrektur zu lesen, möchte ich auf diesem Weg ebenfalls für ihre Unterstützung anerkennenden Dank aussprechen.

Ich danke meiner Mutter im Nachhinein, dass sie mir an ihrem Sterbebett noch das Versprechen entlockte, einen akademischen Bildungsweg einzuschlagen und einen universitären Abschluss zu erlangen. Dies sorgte, neben der ohnehin vorhandenen intrinsischen Motivation u.a. auch für ausreichendes Durchhaltevermögen, um das gesetzte Ziel, trotz eines weiteren Schicksaalschlages (Fahrradunfall während Studienzeit), zu keiner Zeit aus den Augen zu verlieren. Ein ebenso unübliches „Danke" richte ich an all jene, die in der Vergangenheit, nicht an mich geglaubt haben, dafür, dass sie dadurch meinen Studien-Fortschritt nicht maßgeblich vereiteln oder mich vom Kurs abbringen konnten. Ein höchst persönliches Dankeschön gilt zudem meinem, seit meinem Fahrradunfall, lädierten Arm bzw. Handgelenk, welches es mir aber letztendlich nach mehrjähriger Genesung nun doch ermöglicht hat, wieder längere Schreib-Episoden bei erträglichen oder geringen Schmerzen zu absolvieren.

Spezielle Anerkennung möchte ich Herrn Mag. Dr. Alexander Pfeiffer aussprechen, da er mir als überaus kompetenter und hilfsbereiter Fachbetreuer Materialien zur Verfügung stellte und mehrmals Zeit fand, mich bei anfallenden Fragen zu unterstützen. Dabei möchte ich mich abschließend bei ihm und den Mitarbeitern in der wissenschaftlichen Programm-Koordination meines Institutes, für die mir entgegen gebrachte Geduld und den mir ermöglichten Freiraum im Rahmen der Erarbeitung dieser These, mit dem inhaltlich doch sehr komplexen und zugleich noch relativ jungen Forschungsbereich der Blockchain-Technologie in Verbindung mit ihren speziellen Anwendungsmöglichkeiten, bedanken.

Kirchschlag bei Linz im September 2019
Buchner Robert

KURZBESCHREIBUNG

Eine wissenschaftlich fundierte und aus sozioökonomischer Perspektive geleitete Beleuchtung der noch relativ jungen Blockchain-Technologie und ihres mittlerweile seit dem ersten Einsatz (Bitcoin) drastisch erweiterten Anwendungshorizonts, soll dazu beitragen, dass Unternehmer eine mögliche Nutzbarmachung der Distributed Ledger Technologien (vor allem durch das aufzeigen und ableiten konkreter Potentiale, sowie der Ermittlung des Innovationscharakters), gegenüber einem von überschwänglicher Euphorie geblendeten Hype, sowie betreffend eines vorherrschenden *Buzzwordings* rund um das komplexe Thema (mit Begriffen wie u.a. Blockchain 2.0 bzw. 3.0, „internet of value“, „technology of governance“, „Blockchain-as-a-Service“ etc.), speziell vor dem Hintergrund unternehmerischer Innovation besser einordnen und mögliche Veränderungsszenarien (u.a. eine drohende, branchenspezifische Disruption durch den Einsatz der Technologie) künftig treffender bewerten können. Auf Basis des Verständnisses, dass Innovation als ein unsicherer Prozess betrachtet werden kann, der häufig nur dann von Erfolg gekrönt ist, wenn eine Mehrzahl an Akteuren kollaboriert und zudem über Möglichkeiten verfügt, ihr Wissen zu teilen; und geleitet von der (u.a. durch diese Arbeit bestätigten) Erkenntnis, dass die Blockchain als soziotechnisches System, neben Transaktionen (von jeglichen Werten und Informationen), auch eine auf Konsensfindung ausgerichtete zudem anonym und vertrauenslos aber dennoch transparent und nachvollziehbar funktionierende Zusammenarbeit zwischen einander unbekannten Akteuren ermöglicht, gilt es zudem, konkrete Synergien der beiden behandelten Forschungsgebiete (jenem der Open Innovation und dem der Blockchain-Technologie) ausfindig zu machen.

Neben bereits im Titel vorhandenen, für diese Arbeit zentralen Begriffen (*Blockchain, Distributed-Ledger-Technologie* und *Open Innovation*) können folgende **Schlagworte** definiert werden: *Co-Creation, Transaktionssystem, IP-Management, Disintermediation, Disruption*

ABSTRACT

A science-based and socio-economic perspective led investigation of the still relatively young Blockchain technology and its now, since the first use (Bitcoin) drastically extended horizon of application, should help entrepreneurs to evaluate the possible utilizations of Distributed Ledger technologies (especially by showing and deriving concrete potential, furthermore by the determination of the innovation character), against a hype blinded by exuberant euphoria, as well as regarding the prevailing buzzwording around the complex topic (with terms such as Blockchain 2.0 or 3.0, "internet of value", "technology of governance "„Blockchain-as-a-Service“ etc.), especially in the context of entrepreneurial innovation, it should help to be able to classify possible change scenarios (including a threatening, industry-specific disruption through the use of this technology) in the future. Based on the understanding that innovation can be seen as an insecure process that often only succeeds when a large number of actors collaborate and also has opportunities to share knowledge; and guided by the realization (which could be confirmed by this writing) that the blockchain, viewed as a socio-technical system, in addition to transactions (of any values and information), enables an consensus-finding, anonymous and trustless but still transparent and comprehensible way to gain cooperation between unknown actors in economy it is important to identify concrete synergies between the two selected areas of research (open innovation and blockchain technology) through the research for this academic paper.

In addition to the terms already in the title, which are central to this writing (*blockchain, distributed-ledger technology* and *open innovation*), the following **keywords** can be defined: *co-creation, transaction system, IP management, disintermediation, disruption*

GENDERERKLÄRUNG

Im Interesse einer besseren Lesbarkeit wird in dieser Arbeit auf eine geschlechtsneutrale Formulierung verzichtet, wobei jedoch, im Sinne der Gleichbehandlung stets beide Geschlechter gleichermaßen angesprochen werden.

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS (IM AUFBAU & UNVOLLSTÄNDIG)

API	application programming interface (Schnittstelle zur Programmierung von Anwendungen)
ARDR	Coin/Token bzw. Währungseinheit von Ardor
ASIC(s)	application-specific integrated circuit(s)
BaaS	Blockchain-as-a-Service
BC(s)	Blockchain(s)
BTC	bitcoin (Währungseinheiten)
DAG	Directed acyclic graph
dApp(s)	distributed App(s)
DLT(s)	Distributed Ledger Technologie(n)
DNS	Domain Name System
DAO(s)	Dezentralized Autonomous Organisation(s)
EVM	Ethereum Virtual Machine
ICO	Initial Coin Offering
IoT	Internet of Things
IoV	Internet of Value
IP(R)	Intellectual Property (Rights)
KMU	Kleine und mittlere Unternehmen
NDA	non disclosure agreement (Geheimhaltungsvertrag)
OI	Open Innovation
P2P	Peer-to-Peer
PoS	Proof of Stake (Konsensmechanismus)
PoW	Proof of Work (Konsensmechanismus)
SaaS	Software-as-a-Service
SC	Smart Contract
SPoF	Single Point of Failure
STO	Security Token Offering
TTP	Trusted-Third-Party
URL	Uniform Resource Locator (Web-Adresse)

GLOSSAR

Augmented-Reality

benennt eine computerunterstützte Darstellung oder Wahrnehmung, welche die Realität um virtuelle Aspekte ausdehnt.[1]

Asset(s) (digital Assets)

Im Kontext dieser Arbeit wird der Begriff des (digitalen) Assets im Zusammenhang mit dem Handel und der Transaktion von jeglichen Vermögenswerten, welche mit Hilfe der Blockchain-Technologie digitalisiert und verwaltet werden können verwendet.[2] Genauere, weiterführende Definition siehe *Kapitel.2.2.1: „Definitionen zu Kryptowährungen und Assets."*

ASICs(-Resistant)

ASICs (Abkürzung für den englischen Begriff: application-specific integrated circuits) beschreiben Schaltkreise, die für einen konkreten Anwendungsfall bzw. Algorithmus konzipiert wurden und eine bestimmte Rechenaufgabe (und nur diese eine, dafür besonders effizient) ausführen können. Im Bereich der Kryptowährungen wird ASIC-Hardware entwickelt, um die Rechenaufgabe im Rahmen des Minings z.B. der Kryptowährung Bitcoin (schneller und effizienter als mit herkömmlicher Consumer-Hardware möglich) berechnen zu können. ASIC-resistent beschreibt die Eigenschaft (neuerer) Kryptowährungen bzw. von Mining-Algorithmen, gegen das sog. ASIC-Mining und somit einer Abbildung in Spezial-Hardware „immun" zu sein.[3] Siehe *Kapitel 2.5.11.a „Der Prozess der Minings".*

Bärenmarkt

Bärenmarkt (auch Baisse genannt) beschreibt anhaltende sinkende Kurse an der Börse (Abnahme oder Rückgang).[4] Siehe *Kapitel 2.2.4. „Marktkapitalisierung und Kursentwicklungen auf den Krypto Märkten"*

---

[1] vgl. Daniel Markgraf, „Definition: Augmented Reality", Gabler Wirtschaftslexikon, zugegriffen 21. August 2019, https://wirtschaftslexikon.gabler.de/definition/augmented-reality-53628.

[2] vgl. „Digital Asset", in *Wikipedia*, 17. April 2019, https://en.wikipedia.org/w/index.php?title=Digital_asset&oldid=892808963.

[3] vgl. John Ma, „ASIC-Resistant - Definition", Binance Academy, zugegriffen 21. August 2019, https://www.binance.vision/glossary/asic-resistant.

[4] vgl. „Bullen- und Bärenmarkt", in *Wikipedia*, 7. August 2019, https://de.wikipedia.org/w/index.php?title=Bullen-_und_B%C3%A4renmarkt&oldid=191127475.

Bitcoin und bitcoin (BTC)

Bitcoin großgeschrieben steht für das auf Basis des Whitepapers von Nakamoto implementierte Transaktionssystem, das zugrunde liegende (P2P-)Netzwerk und die Softwareplattform; bitcoin kleingeschrieben steht für die von dem Transaktionssystem Bitcoin verwaltete Währungseinheit mit dem Kürzel „BTC".

Blockchain (BC) / Die Blockchain-Technologie (BC-Technologie)

Ist ein (bzw. eine Technik für ein) verteiltes Datenbanksystem mit einer auf vielen Computern gleichzeitig verwalteten Datei, in welcher sämtliche Transaktionen aller Teilnehmer vom gesamten, zugrunde liegenden Peer-to-Peer-Netzwerk per Mehrheitskonsens validiert werden und in weiterer Folge für alle Teilnehmer transparent und im Nachhinein unveränderlich abgespeichert werden. Jegliche Transaktionen werden mittels kryptographischer Verfahren in Blöcken verschlüsselt und sind jeweils miteinander untrennbar verkettet; daher die Bezeichnung Blockchain[5] Für eine weiterführende Definition siehe *Kapitel 2.5.3 „DLT-basierte Definition der Blockchain"*

Blockchain-Bloat

Wesentliche Eigenschaften der Blockchain machen es grundsätzlich erforderlich, dass jeder Netzwerkteilnehmer eine vollständige Transaktionsliste (d.h. die vollständige Blockchain, bestehend aus Transaktions-Datenblöcken bis zur ersten Transaktion im ersten „Genesis"-Block zurück) als Datenbasis im Speicher, des für Transaktionen benutzten Endgeräts vorhält. Die so erzielte Redundanz der mehrfach vollständig replizierten Transaktionshistorie innerhalb des verteilten Netzwerkes markiert insgesamt zwar einen wesentlichen Grundpfeiler in der Blockchain-Architektur u.a. betreffend der Datensicherheit und Unmanipulierbarkeit, kann jedoch mit fortwährender Dauer (durch jede weitere Transaktion bzw. jeden weiteren Block der gespeichert werden muss) zu Speicherproblemen bzw. Speicherengpässen auf den jeweiligen genutzten Endgeräten (auch Nodes bzw. Netzwerkknoten) führen. Dieses Phänomen wird „Blockchain-Bloat" genannt.[6]

Block Reward

Ein Block Reward (Deutsch: Blockvergütung) wird als Anreiz für diejenigen verwendet, die ihre Rechenleistung für das sog. Mining zur Verfügung stellen, also,

---

[5] vgl. Shermin Voshmgir, „Blockchains, Smart Contracts und das Dezentrale Web" (Technologiestiftung Berlin 2016), 8, zugegriffen 29. November 2018, https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf.

[6] vgl. Aran DaviesBlockchain Expert | Developer | Writer | Photographer, „Can Blockchain Bloat Ever Be Solved?", *DevTeam.Space* (blog), 22. April 2019, https://www.devteam.space/blog/can-blockchain-bloat-ever-be-solved/.

die sogenannten Miner. Sie bekommen den Block Reward dann, wenn sie einen, neuen gültigen Block finden, der (sofern er korrekt und ausreichend schnell berechnet wurde) anschließend an die bestehende Blockchain anhängt wird. Der Anteil der Belohnung variiert, in Abhängigkeit davon, für welche Kryptowährung es „gemined" wird und ob der Miner alleine oder mit mehreren Miner im Verband versucht einen neuen Block zu berechnen bzw. zu finden.[7]
Siehe Kapitel 2.5.11.a „Der Prozess des Minings"

Bullenmarkt

Bullenmarkt oder Hausse bedeutet Anstieg oder Steigerung und steht an der Börse für anhaltend steigende Kurse, er ist der Gegenpart zum Bärenmarkt.[8]
Siehe *Kapitel 2.2.4. „Marktkapitalisierung und Kursentwicklungen auf den Krypto Märkten"*

Buzzwording

Buzzwords sind Schlagworte oder Phrasen mit denen besondere Beachtung erzeugt werden soll Sie werden verbreitet, um Sachverhalte prägnant und überzeugend zu vermitteln. Da ihrer Verwendung eine (oft unbewusste) Überzeugungsabsicht zugrunde liegt, verkürzen oder vereinfachen diese Worte den zu beschreibenden Sachverhalt oft auf zweifelhafte Art zugunsten des Wohlklangs und zu Lasten der damit vermittelten Information.[9] Siehe *Kapitel 2.6.4.a „Kritik an Cloud BaaS"*

Coopetition

Coopetition, Kooperationswettbewerb, auch Koopkurrenz, bezeichnet die Dualität von Konkurrenz und Kooperation auf Märkten oder innerhalb von Netzwerken. Coopetition ist ein Kofferwort das, aus den Begriffen cooperation (Kooperation) und competition (Wettbewerb).[10]

---

[7] vgl. Memo Özbek, „▷ Was ist ein Block Reward (Blockvergütung)? | Definition", *Decentralbox* (blog), 10. Februar 2019, https://decentralbox.com/bitcoin-glossar/block-reward/.
[8] vgl. „Bullen- und Bärenmarkt", in *Wikipedia*, 7. August 2019, https://de.wikipedia.org/w/index.php?title=Bullen-_und_B%C3%A4renmarkt&oldid=191127475.
[9] vgl. „Schlagwort (Linguistik)", in *Wikipedia*, 28. Juli 2019, https://de.wikipedia.org/w/index.php?title=Schlagwort_(Linguistik)&oldid=190813244.
[10] vgl. „Coopetition", in *Wikipedia*, 16. August 2017, https://de.wikipedia.org/w/index.php?title=Coopetition&oldid=168204029.

Cost-to-Market

Die Gesamtkosten betreffend der Herstellung bzw. Konzeption eines Produktes oder einer Dienstleistungen, von der Planung bzw. ersten Idee bis zur Einführungen in den Markt (Kosten des Innovationsprozesses, Kosten für Forschung & Entwicklung, Kosten für Prototyping, Produktionskosten etc.)

Cross-Functional-Integration

Bezeichnet den Prozess des Kombinierens von diversen funktionalen Geschäftsaktivitäten innerhalb der Organisation durch Überbrückung der Grenzen und dem Ermöglichen des Informationsflusses, zwischen den verschiedenen organisatorischen Funktionen.[11]

DAOs (Dezentralized Autonomous Organizations)

DAOs stellen eine neue, vollständig automatisierte Form von Organisationen dar, deren Statuten, Gesellschaftsvertrag, die Geschäftsordnung oder Satzung durch Smart Contracts abgebildet und von einer Blockchain, unabänderbar ausgeführt werden. DAOs benötigen kein zentral organisiertes Management des Tagesgeschäftes, ihre Geschäftsausübung kann daher auch nicht einfach (im Nachhinein) oder unmittelbar von Teilhabern oder Regierungen gesteuert oder beeinflusst werden.[12] Sie stellen die höchste und komplexeste Form von Smart- Contracts dar. Im Bereich von DAOs besteht noch viel Entwicklungs- und Forschungsbedarf, zudem sind technologische Netzwerkeffekte von Nöten, bevor diese Art der Nutzbarmachung von Blockchains für eine breite Maße relevant werden könnte.[13] Siehe *Kapitel 2.4.5. „DAOs (Dezentralized Autonomous Organizations)“*

dApps (decentralized Apps)

dApps sind dezentrale Anwendungen die von Backend bis User Interface auf einer (öffentlichen) Blockchain laufen, daher nicht wie sonst üblich von einem zentralen Anbieter betrieben, gewartet oder weiterentwickelt werden.[14] dApps verwenden im Hintergrund einen oder mehrere Smart Contracts. Da sie dezentral und verteilt auf

---

[11] vgl. „What is Cross-Functional Integration | IGI Global“, zugegriffen 23. August 2019, https://www.igi-global.com/dictionary/cross-functional-integration/38877.

[12] vgl. „Dezentralisierte Autonome Organisation“, in *Wikipedia*, 5. Oktober 2018, https://de.wikipedia.org/w/index.php?title=Dezentralisierte_Autonome_Organisation&oldid=181524102.

[13] vgl. Voshmgir, „Blockchains, Smart Contracts und das Dezentrale Web“, 14.

[14] vgl. „DApp“, in *Wikipedia*, 3. Dezember 2018, https://de.wikipedia.org/w/index.php?title=DApp&oldid=183371819.

einem Peer-to-Peer-Netzwerk laufen kann keine zentrale Stelle Anwender aussperren, zensieren, Daten manipulieren oder die Applikation beenden/löschen. dApps erfüllen die Richtlinien von Open Source und gelten als „unzerstörbar“.[15]
Siehe *Kapitel 2.4.4. „dApps (Decentralized Apps)“*

Defensivpublikation

Ist eine von Unternehmen (meist KMUs) genutzte Strategie, bei der durch die (teilweise) Veröffentlichung eigentlich patentfähiger Erfindungen oder Inhalte die Patentierbarkeit gegenüber andere erlischt, bzw. die Anforderung, (bezüglich der Neuheit bei Patentanmeldungen durch andere) einer Erfindung nicht mehr erfüllt werden kann. Defensivveröffentlichungen ermöglichen somit, einen gewissen Schutz von geistigem Eigentum, (intellectual property, IP) ohne die üblicherweise hohen Kosten für Patentregistrierungen tragen zu müssen.[16]

Denial-of-Service Attacke

Der Denial-of-Service-Angriff (DoS-Angriff) bezeichnet einen Cyberangriff, bei dem der Täter versucht, eine Maschine oder Netzwerkressource für seine vorhergesehenen Nutzer nicht mehr verfügbar zu machen, die Dienste eines mit dem Internet verbundenen Hosts werden, so auf unbestimmte Zeit unterbrochen. Denial-of-Service wird in der Regel dadurch erreicht, indem die Zielmaschine oder -ressource mit überflüssigen Anforderungen überflutet wird, die Systeme werden somit überlastet und es wird verhindert, dass einige oder alle Service-Anfragen erfüllt werden können.[17]

Disintermediation

Bei Disintermediation handelt es sich um ein Konzept aus dem Bereich der Wirtschaftswissenschaft, welches den Bedeutungsverlust bzw. ggf. kompletten Wegfall von Intermediären (Vermittlern zwischen verschiedenen Akteuren) in Wirtschaftssystemen beschreibt, dabei zum Wegfall einzelner Stufen und zur Steigerung der Transaktionskosten-Effizienz in Wertschöpfungsketten beitragen kann. [18] & [19]

---

[15] vgl. Voshmgir, „Blockchains, Smart Contracts und das Dezentrale Web“, 14.
[16] vgl. „Defensivpublikation“, in *Wikipedia*, 13. Juli 2019, https://de.wikipedia.org/w/index.php?title=Defensivpublikation&oldid=190402362.
[17] vgl. „Denial-of-Service Attack“, in *Wikipedia*, 21. August 2019, https://en.wikipedia.org/w/index.php?title=Denial-of-service_attack&oldid=911888090.
[18] vgl. „Disintermediation“, in *Wikipedia*, 3. Januar 2019, https://de.wikipedia.org/w/index.php?title=Disintermediation&oldid=184331113.
[19] vgl. „Disintermediation“.

Disruption

Disruption wird ein Vorgang genannt, bei dem ein bestehendes Geschäftsmodell oder ein gesamter Markt durch eine extrem stark wachsende Innovation abgelöst bzw „zerschlagen“ wird und durch diese, im Sinne einer „schöpferischen Zerstörung“ neuformiert bzw. transformiert wird. Der Begriff leitet sich vom englischen Wort „disrupt“ (d.h.„zerstören“, „unterbrechen“) ab und bezeichnet einen Vorgang, der besonders mit dem Umbruch der Digitalwirtschaft in Zusammenhang gebracht wird: Traditionelle Geschäftsmodelle, Produkte, Technologien, Dienstleistungen werden von innovativen Erneuerungen abgelöst oder nur zum Teil verdrängt. Auffallend oft findet man diesen Begriff in der Startup-Szene, da er revolutionäres Gedankengut birgt.[20]

Distributed-Ledger-Technologie (DLT)

DLTs Beschreiben Techniken für das dezentrale Führen von Kontobüchern (engl. ledgers) bzw. Transaktionsdatenbanken. Die Blockchain stellt eine konkrete Ausprägungsform der DLTs dar und wird in weniger technisch versierten Kreisen häufig als Synonym zur Blockchain-Technologie verstanden.[21] Für eine genauere (für das Verständnis der ersten Kapitel jedoch unerhebliche) Definition und Abgrenzung des Begriffes zu Blockchain siehe *Kapitel 2.5.1. „Vom Ledger zu den DLT“*

Double-Spending-Problem

Das „Double-Spending“ (zu Deutsch die Doppelausgabe) beschreibt das Risiko/Problem, dass ein Währungsbetrag, (fälschlicherweise) zweimal ausgegeben/aufgewendet werden kann. Dies ist ein Problem, welches nur bei digitalen Währungen auftritt, da sich digitale Informationen normalerweise relativ leicht manipulieren bzw. reproduzieren lassen. Bis zur Vorstellung der dezentral verwalteten Kryptowährung Bitcoin, konnte das Problem im Bereich digitaler Währungen bzw. Transaktionssysteme nur durch die Einschaltung einer zentralen Instanz als Clearingstelle bzw. einer sog. Trusted Third Party gelöst werden. (siehe *Kapitel 2.1.4 „Historische Meilensteine am Weg zur ersten Blockchain-Anwendung“)* Kryptowährungen lösen das Double-Spending-Problem indem sie auf sog. Konsens-

[20] vgl. „Disruption Definition“, Gründerszene Magazin, zugegriffen 23. August 2019, https://www.gruenderszene.de/lexikon/begriffe/disruption.

[21] „Distributed-Ledger-Technologie“, in *Wikipedia*, 30. April 2019, https://de.wikipedia.org/w/index.php?title=Distributed-Ledger-Technologie&oldid=188072711.

mechanismen setzten und dabei die Echtheit jeder Transaktion prüfen und Doppelzählungen bzw. -ausgaben vermeiden.[22] Siehe *„Kapitel 2.5.4. Der Transaktionsprozess auf der Blockchain“*

Fiat- Geld

Vom Lateinischen fiat (es werde!) Abgeleitet, bezeichnet alle von Regierungen emittierten bzw. unterstützten Währungen (z.B.: Euro, US-Dollar, Schweizer Franken etc.). Dabei umschreibt Fiat-Geld ein (aus dem Nichts erstelltes und theoretisch aufwandslos und unendlich produzier- bzw. emittier bares) Objekt ohne tatsächlichen inneren Wert und steht im Gegensatz zu sog. Warengeld, welches aufgrund seines inneren Wertes bzw. seiner Limitation zum Tauschhandel verwendet werden kann. (z.B.: Gold) Der Begriff Fiat Geld wird in Krypto-Communities häufig (mit leicht abwertender Konnotation) verwendet, um den zumeist ungedeckten und rein assoziativen Wert von herkömmlichen, zentral bzw. staatlich kontrollierten Währungen zu betonen, und diese Währungen von den meist dezentral verwalteten, häufig auf eine maximale Stückzahl begrenzten und bei ihrer Emittierung zumeist an erheblichen Aufwand (z.B.: durch das sog. Mining) gebundenen Kryptowährungen abzugrenzen.[23&24]

Fit-to-Market

Auch product / market fit genannt, (zu Deutsch Produkt- / Marktanpassung) bedeutet, ein Produkt (eine Dienstleistung) anzubieten, für welche(s) großer Bedarf vorherrscht, um das Wachstum des anbietenden Unternehmens anzukurbeln.[25]Siehe *Kapitel 1.2. „Relevanz vor dem Hintergrund unternehmerischer Innovation.“*

Funding (Fundraising)

bezeichnet das zur Verfügung Stellen von Ressourcen, meist in Form von Geld (Finanzierung).[26]

---

[22] vgl. Jake Frankenfield, „Double-Spending“, Investopedia, zugegriffen 23. August 2019, https://www.investopedia.com/terms/d/doublespending.asp.

[23] vgl. „Fiatgeld“, in *Wikipedia*, 26. August 2019, https://de.wikipedia.org/w/index.php?title=Fiatgeld&oldid=191700278.

[24] vgl. Jörg Hermsdorf, „Was ist der Unterschied zwischen Fiat- und Kryptogeld wie Bitcoin?“, Paymentandbanking, 5. Juli 2018, https://paymentandbanking.com/was-ist-der-unterschied-zwischen-fiat-und-kryptogeld-wie-bitcoin/.

[25] vgl. Bob Ruffolo, „Product/Market Fit: What It Means and How to Measure It in 2019“, 10. August 2016, https://www.impactbnd.com/blog/product-market-fit.

[26] vgl. „* Funding (Börse) - Definition,Bedeutung - Online Lexikon“, zugegriffen 25. August 2019, https://de.mimi.hu/borse/funding.html.

Hashing, Hashwert, Hashing-Power, kryptographische Hash-Funktion

Die *kryptographische Hash-Funktion* ist eine mathematische bzw. kryptographische Funktion, welche aus beliebigen (beliebig langen) Eingabewerten, einen stets gleich langen Ausgabewert erstellt (*Hashwert*). Es ist unmöglich mittels des Hashwertes, den ursprünglichen Eingabewert zu ermitteln bzw. wiederherzustellen. Mittels Hashwert kann jedoch jederzeit, die Korrektheit des ursprünglich gehashten Inputs verifiziert werden. Die BC Netzwerken mittels Konsensmechanismen zur Verfügung gestellte Rechenleistung (verteilte Rechenleistung) für das Erstellen von Hashwerten (Hashing ist der Vorgang für das Erstellen von Hashwerten), wird auch *Hashing-Power* genannt.[27][28][29] Für eine genauere, weitreichendere Definition, siehe *Kapitel 2.5.7. „Die kryptographische Hash-Funktion“*.

ICOs & STOs

ICOs: Initial Coin Offering wird auch Initial Public Coin Offering (IPCO) genannt. Es ist die Bezeichnung einer unregulierten Methode des Crowdfundings, die häufig von Unternehmen, welche auf Blockchain-Basis arbeiten angewendet wird. Mit dieser Methode der Kapitalaufnahme vermeiden diese Firmen den ansonsten sehr streng regulierten Ablauf der Kapitalaufnahme. In ICOs wird ein Anteil einer Kryptowährung im Austausch gegen staatliche Währungen oder auch anderen Kryptowährungen an Anleger verkauft. STOs: Ein Security Token Offering ist in den Grundzügen einem ICO sehr ähnlich, jedoch in wesentlichen Punkten sehr unterschiedlich. Bei dem STO wird, wie beim ICO, ein Investment gegen Tokens einer neuen Kryptowährung, die auf einer BC gehalten werden, getauscht. ICOs und STOs haben ansonsten aber kaum Gemeinsamkeiten. Anders als ICOs gleichen STOs eher den Wertpapieren. Sie sind kryptographische Tokens, die den Käufer zu einem Prozentsatz an den Gewinnen beteiligen, Kredite geben oder Erträge ausschütten. Bei STOs erhalten Käufer tatsächlich Anteile an den Unternehmen in die sie investieren.[30][31] Siehe *Kapitel 2.2.6. „Tokenisierung ICO’s & STO’s“*

---

[27] vgl. Agnieszka Czernik, „Hashwerte und Hashfunktionen einfach erklärt“, Datenschutzbeauftragter, 2. September 2016, https://www.datenschutzbeauftragter-info.de/hashwerte-und-hashfunktionen-einfach-erklaert/.

[28] vgl. „Hashfunktion“, in *Wikipedia*, 28. April 2019, https://de.wikipedia.org/w/index.php?title=Hashfunktion&oldid=188018488.

[29] vgl. Sudhir Khatwani, „Bitcoin Hash Rate or Hashing Power In Cryptocurrencies Explained“, *The Money Mongers* (blog), 20. Januar 2019, https://themoneymongers.com/hash-rate-hash-power/.

[30] vgl. Prasanna, „Was ist der Unterschied zwischen STO und ICO? - CryptoTicker“, *https://cryptoticker.io/de/* (blog), 10. Januar 2019, https://cryptoticker.io/de/unterschied-sto-ico/.

[31] vgl. „Initial Coin Offering“, in *Wikipedia*, 9. Mai 2019, https://de.wikipedia.org/w/index.php?title=Initial_Coin_Offering&oldid=188388076.

Internet of Things (IoT)

Das Internet of Things (zu Deutsch Internet der Dinge) Umschreibt das Ergebnis, fortschreitender Vernetzung “intelligenter” Gegenstände (Smart Devices). Dieses Kommunizieren miteinander und auch mit dem Internet. Diverse Alltags-Gegenstände, aber auch Maschinen in Produktion und Fertigung, werden mit Prozessoren und Sensoren ausgestattet, und in die Lage versetzt Informationen betreffend ihres Status auszutauschen und miteinander zu kommunizieren.[32] Siehe Kapitel 2.7.2. *„Aktuelle Use-Cases nach Geschäfts- und Gesellschaftsbereichen“* Abschnitt: Internet of Things und Industrie 4.0

IP(R)-Management

Der Begriff IP-Managements beziehet sich auf das Steuern und Verwalten von „Intellectual Property“ (IP, zu Deutsch geistigem Eigentum) und beschäftigt sich u.a. mit Aspekten betreffend den Schutz, die Sicherung und die Verwertung (Lizensierung) von geistigem Eigentum. Das IPR-Management zielt aufbauend auf die Lösung von Fragen betreffend des Patent-, Urheberrechts und gewerblichen Rechtsschutzes ab („Intellectual Property Rights“, IPR).[33]

Krypto-Anarchismus

Umschreibt eine vor über 30 Jahren gegründete Form des praktizierten Anarchismus im Bereich von Internet-Foren und Communities. Aussagen und Erkenntnisse von Mitgliedern des Krypto-Anarchismus beruhen auf der Beobachtung eines wachsenden Missverhältnisses bei der Nutzung von Informationstechnologien, betreffend eine staatliche Ermächtigung und Geheimhaltung einerseits und eine zunehmende staatliche Entmündigung bzw. Überwachung andererseits. Die jüngere sog. Cypherpunk-Bewegung beruft sich ideologisch auf Ansichten des Krypto-Anarchismus und hat es sich zur Aufgabe gemacht, aktiv mit den Möglichkeiten von Kryptographie und auf Basis vorhandener Vernetzung (z.B. durch Nutzung des Internets), das von Krypto-Anarchisten angeprangerte Missverhältnis umzukehren; in manchen Fällen, um Staatsgeheimnisse zu veröffentlichen, anonym im Internet agieren zu können, in Verbindung mit der Einschränkung der Pri-

[32] vgl. „Internet of Things Definition“, Gründerszene Magazin, zugegriffen 26. August 2019, https://www.gruenderszene.de/lexikon/begriffe/internet-of-things.

[33] vgl. Anke Reich, „Was ist unter IP-Management zu verstehen? | Kanzlei Dr. Anke Reich | Markenrecht, Datenschutzrecht, Internetrecht, Urheberrecht, Lauterkeitsrecht“, zugegriffen 27. August 2019, https://www.dr-reich.com/wissenswertes/ip-management/.

vatsphäre stehende Gesetze zu umgehen oder Software zur anonymisierten Nutzung des Internets frei zu Verfügung zu stellen.[34] Siehe Kapitel 2.1.3. Die Ideologie: Vom Krypto-Anarchismus zur Cypherpunk-Bewegung.

Kryptowährung

Unter dem Begriff Kryptowährungen werden Ausprägungen virtueller Währungen verstanden, welche kryptographische Techniken für die sichere Autorisierung und Verifizierung von Transaktionen einsetzten und deshalb ohne zentrale Instanz bzw. *Trusted Third Party* zur Abwicklung und das ansonsten nötige Vertrauen in ebensolche Intermediäre auskommen.[35] Siehe Kapitel 2.2. Kryptowährungen, Tokens & ICOs – die Blockchain-Assets.

Lead-User

Bezeichnet User, deren Bedürfnisse als repräsentativ für den Markt angesehen werden können und die hohe Kaufbereitschaft für zukunftsträchtige Produkte vorweisen. Durch die Einbeziehung dieser Personen in den Entwicklungsprozess von Innovationen können wesentliche Wettbewerbsvorteile erreicht werden. Lead User erkennen Bedürfnisse, schon vor Ihrem auftreten am Markt.[36]

Marktkapitalisierung (Marktkap.)

Im Englischen market capitalisation bzw market cap genannt, (im Zusammenhang mit herkömmlichen anteilswerten auch Börsenkapitalisierung oder Börsenwert), bezeichnet im Zusammenhang mit der vorliegenden Arbeit den Gesamtwert aller auf betreffenden Märkten (u.a. sog. Kryptobörsen) verfügbaren, bereits emittierten Anteile (sog. Coins oder Token) einer Kryptowährung oder BC-Plattform zum jeweiligen Kurswert.[37] Siehe Kapitel 2.2.3. *„Marktkapitalisierung und Kursentwicklungen auf den Kryptomärkten“*

Mining(-Farmen)

Mining-Farmen sind meist gemeinschaftlich betriebene Rechenzentren, welche für die Gewinnung des sog. *Block Rewards* durch sog. *Mining* (zu Deutsch schürfen,

[34] vgl. „Krypto-Anarchismus“, in Wikipedia, 4. März 2019, https://de.wikipedia.org/w/index.php?title=Krypto-Anarchismus&oldid=186248076.
[35] Salomon Fiedler, Klaus-Jürgen Gern, und Ulrich Stolzenburg, „Kryptowährungen – Geld der Zukunft?“, *Wirtschaftsdienst* 98, Nr. 10 (1. Oktober 2018): 752, https://doi.org/10.1007/s10273-018-2362-z.
[36] vgl. Kirchgeorg, „Definition: Lead User“, Gabler Wirtschaftslexikon, zugegriffen 28. August 2019, https://wirtschaftslexikon.gabler.de/definition/lead-user-37917.
[37] vgl. „Marktkapitalisierung“, in *Wikipedia*, 30. März 2019, https://de.wikipedia.org/w/index.php?title=Marktkapitalisierung&oldid=187070476.

eine begriffliche in Anlehnung an den im Rahmen des Bergbaus, aufwendigen Gewinnungsprozess von Edelmetallen) von Bitcoins oder anderen Kryptowährungen ausgestattet sind. (Betreffend Mining siehe *Kapitel 2.5.11a „Der Prozess des Minings“*) Die Strategie des Zusammenschlusses von Minern zu Mining-Farmen kann als Reaktion auf den Umstand gewertet werden, dass der Miningprozess (bei genutzten *Konsensmechanismen* wie dem des sog. *Proof of Work*), bei zunehmender Verbreitung bzw. Nutzung einer Blockchain zunehmend mehr technische, energetische und finanzielle Ressourcen erfordert um erfolgreich oder kostendeckend zu sein.[38] Siehe u.a. *Kapitel 2.5.10 „Konsensmechanismen“* und *Kapitel 2.5.11 „Proof of Work“*

Micropayment

Der Begriff Micropayment bedeutet Kleinbetragszahlung. Es handelt sich meistens um Transaktionen im E-Commerce-Bereich bei denen der zu zahlende Betrag in der Regel die Summe von fünf Euro nicht übersteigt. Des Weiteren existieren die Bezeichnungen Nanopayment oder Picopayment, um auf Bezahlbeträge von meist nur wenigen Cent hinzuweisen.[39]

NDA non-disclosure agreement (Geheimhaltevertrag)

Die Geheimhaltungsvereinbarung (NDA) ist ein rechtlicher Vertrag zwischen zumindest zwei Parteien, die vertrauliches Material, Wissen oder Informationen, (d.h. schützenswertes geistiges Eigentum, IP) welches die Parteien für bestimmte Zwecke benötigen, untereinander teilen möchten, hierbei jedoch Dritte vom Zugang zu diesen sensiblen Informationen vertraglich ausschießen wollen.[40] Tätigkeiten betreffend den Abschuss und die Verwaltung von NDAs können zum Bereich des *IP(R)-Managements* gezählt werden.

Netzwerkeffekt

Ein Effekt, bei dem der Nutzen bzw. Nutzwert eines Gutes oder einer Dienstleistung mit steigender Nutzerzahl zunimmt (positive Netzwerkeffekte). Dieses Phänomen ist insbes. bei Internetplattformen zu beobachten.[41]

---

[38] vgl. „Mining Farm for Bitcoin and Crypto Mining – BitcoinWiki“, zugegriffen 26. August 2019, https://en.bitcoinwiki.org/wiki/Mining_farm.

[39] vgl. „Micropayment Definition“, Gründerszene Magazin, zugegriffen 26. August 2019, https://www.gruenderszene.de/lexikon/begriffe/micropayment.

[40] vgl. „Non-Disclosure Agreement“, in *Wikipedia*, 23. August 2019, https://en.wikipedia.org/w/index.php?title=Non-disclosure_agreement&oldid=912203805.

[41] vgl. Clausen, „Definition: Netzwerkeffekte“, Gabler Wirtschaftslexikon, zugegriffen 26. August 2019, https://wirtschaftslexikon.gabler.de/definition/netzwerkeffekte-51385.

Nerd

Auch Computerfreak, ist eine Bezeichnung für Sonderlinge die an Spezialinteressen hängen und sozial nicht sehr umgänglich sind. Der Terminus kann positiver wie auch negativer Konnotation angewandt werden. In Computerkreisen wird er jedoch häufig als Kompliment gewertet. (Positiv: Nerd = Individualist, welcher durch Besitz überdurchschnittlicher bzw. besonders herausragender Fachkenntnisse, gesellschaftlicher Anerkennung genießt. Negativ: Nerd = stereotype Bezeichnung eines eigenartig anmutenden Einzelgängers, welcher sozial unbeholfen, u.a. ständig vor dem Computer sitzend, daraus resultierend sozial isoliert wirkt.)[42]

New-to-Market (Innovation)

Zu Deutsch „Neu auf dem Markt" ist ein Begriff, bezogen auf Produkte, Dienstleistungen (oder Unternehmen), welche in einen (für sie) neuen Markt oder ein (für sie) neues Marktsegment eintreten. Diese Vorgangsweise ist hilfreich bei der Erweiterung des Geschäfts und der Kundenbasis von Unternehmen. In Zusammenhang mit Innovationen beschreibt der „New to Market"-Faktor den von Kunden bzw. Nachfragern wahrnehmbaren Neuheitsgrad eines, nach der Beendigung des Innovationsprozesses auf den Markt neu eingeführten Produktes oder einer neu eingeführten Dienstleistung.[43] Grundlegend neue Produkte auf Basis radikaler Innovation können im Vergleich zu, lediglich auf Produktverbesserungen (inkrementelle Innovation) basierenden „neuen" Produkten den „New-to-Maket" Faktor als Ergebnis des Innovationsprozesses erheblich steigern.

Node

Im Deutschen: Netzwerkknoten oder Netzknoten. Bezeichnet einen Verbindungspunkt in einem Netzwerk, welcher (je nach Netzwerkarchitektur und eingenommener Position) ein Umverteilungspunkt oder Endpunkt bei der Datenübertragung sein kann. Ein Node besitzt die Fähigkeit, Übertragungen von und für andere Netzwerkknoten zu erkennen, zu verarbeiten und schließlich weiterzuleiten. Ein Netzwerkknoten hat mindestens zwei, zumeist aber mehr Verbindungen zu anderen Netzwerkelementen bzw. Netzwerkteilnehmern. Nodes bezeichnen im Zusam-

[42] vgl. „Nerd", in *Wikipedia*, 24. August 2019, https://de.wikipedia.org/w/index.php?title=Nerd&oldid=191644453.
[43] vgl. „New to Market Status Explained", *The Business Professor* (blog), zugegriffen 27. August 2019, https://thebusinessprofessor.com/knowledge-base/new-to-market-defined/.

menhang mit der vorliegenden Arbeit, die für die Aufrechterhaltung von BC-basierten Transaktionsnetzwerken u.a. zur Validierung von Transaktionen nötigen Netzwerkknoten bzw. Netzwerkteilnehmer. Dabei kann (je nach zugeteilter Funktion innerhalb eines BC-Netzwerkes) zwischen sog. „full Nodes" und sog. „leigthweight nodes" unterschieden werden. Siehe Kapitel 2.5.4: „*Der Transaktionsprozess auf der Blockchain"*, Abschnitt: „*Nodes validieren Transaktionen im BC-Netzwerk"*[44]

Peer-to-Peer-Netzwerk (P2P-Netzwerk)

Ein dezentrales, sich selbst organisierendes Netz, („Self Organized Network", SON) welches ohne zentrale Instanz (Server) auskommt und in dem alle Netzwerkteilnehmer (engl. Peers) gleichberechtigt sind. Einzelne Rechner stellen sich im Netzwerk gegenseitig Betriebsmittel, Ressourcen und Dateien zur Verfügung. Daten können so auf viele Rechner verteilt werden, wobei sie aufgrund der Netzwerkstruktur bei Bedarf direkt d.h Peer-to-Peer übertragen werden können. [45]&[46]

Peer-to-Peer-Ökonomie (P2P-Ökonomie)

Eine Peer-to-Peer-Ökonomie (P2P-Ökonomie) ist ein dezentrales Modell, bei dem mindestens zwei Personen interagieren, um Waren und Dienstleistungen gegen Geld, direkt miteinander auszutauschen, ohne dass eine *Trusted Third Party* oder ein Intermediär in den Transaktionsprozess miteinbezogen wird. Käufer und Verkäufer können im Rahmen des Transaktionsprozesses direkt miteinander verhandeln und Preise und Modalität zur Gänze selbstständig festlegen.[47]

Proof of Existence

Ermöglicht den Nachweis der Existenz von Dateien und Dokumenten zu einem bestimmten Zeitpunkt mittels unmanipulierbaren und jederzeit (unabhängig von

---

[44] vgl. Rouse ,Eckert, „Was ist Node (Netzwerkknoten)? - Definition von WhatIs.com", ComputerWeekly.de, Juli 2016, https://www.computerweekly.com/de/definition/Node-Netzwerkknoten.

[45] vgl. „Peer-to-Peer-Netz :: P2P (peer to peer network) :: ITWissen.info", zugegriffen 11. Juni 2019, https://www.itwissen.info/Peer-to-Peer-Netz-peer-to-peer-network-P2P.html.

[46] vgl. „Peer-to-Peer", in *Wikipedia*, 13. April 2019, https://de.wikipedia.org/w/index.php?title=Peer-to-Peer&oldid=187531892.

[47] vgl. Will Kenton, „Peer-to-Peer (P2P) Economy", Investopedia, 1. April 2018, https://www.investopedia.com/terms/p/peertopeer-p2p-economy.asp.

Dritten) nachvollziehbaren (mit Zeitstempel, timestamps versehenen) Transaktionsdaten in der Blockchain.[48] Der Proof of Existence kann neben dem Proof of Origin als das Ergebnis des sog. *Timestampings* erachtet werden. [49]

Proof of Origin

Auch Ursprungszeugnis genannt. Beschreibt ein im Rahmen dieser Arbeit, ein mittels BC Technologie ermöglichtes Verfahren, um den Besitz in Relation zu einem bestimmten Zeitpunkt und ermöglicht somit Rückschlüsse auf die (historische) Herkunft einer Datei oder eines Dokumentes. Der *Proof-of-Origin* kann neben dem *Proof of Existence* als Ergebnis des sogenannten *Timestampings* betrachtet werden. Hat jedoch aktuell aufgrund fehlender Anerkennung, als Schutzmaßnahme für geistiges Eigentum (noch) keinerlei Rechtsgültigkeit und ist (hinsichtlich Wirksamkeit) nicht mit dem Registrieren von Patenten, oder dem um Identitätsdaten erweiterten Proof of Ownership zu verwechseln.[50]

Proof of Ownership

Im Rahmen dieser Arbeit handelt es sich hierbei, um eine Blockchain-basierte Methode, welche das Timestamping-Verfahren zur Herstellung des eindeutigen *„Proof of Existence"* und des *„Proof of Origin"*, um Informationen aus einem Identitätsmanagement-System bzw. zusätzlich um einen Notariats-Service zur Verifizierung und Registrierung der Identitätsdaten in Verbindung mit dem „Proof of Existence" erweitert. Künstler oder Unternehmen können diese Technik für sich nutzen, um nicht nur die Integrität bzw. Authentizität, betreffend das Datum der Veröffentlichung und das Datum des Besitzes einer Datei oder eines Dokumentes nachzuweisen, sondern um das urheberrechtlich zu schützende (versionsunabhängige), an eine Identität gebundene Eigentum an Kreationen oder Verträgen, jederzeit reproduzierbar und rechtsgültig attestieren zu können. Das in München ansässige Start-Up bernstein.io kann u.a. aufgrund einer Kooperation mit einer Schweizer Rechtsanwaltskanzlei einen derartigen (erweiterten) BC-basierten Registrierungs-Service für geistiges Eigentum anbieten. Das bisherige Problem bei dieser Methode (zur Vermeidung eines sog. Single Point of Failures) ist, dass aus Ermangelung eines dezentralisierten und rechtsgültig anerkannten Indentitäts-

---

[48] vgl. „Proof of Existence", in *Wikipedia*, 17. Juni 2019, https://en.wikipedia.org/w/index.php?title=Proof_of_Existence&oldid=902167143.

[49] vgl. „Proof of Existence", in *Wikipedia*, 17. Juni 2019, https://en.wikipedia.org/w/index.php?title=Proof_of_Existence&oldid=902167143.

[50] vgl. „Certificate of Origin / Ursprungszeugnis", *Sea, Air, Transport & Service* (blog), zugegriffen 30. August 2019, https://www.sats-logistics.com/glossar/certificate-of-origin/.

Systemes (auf der Blockchain), für das zum Proof of Ownership nötige Identitätsmanagement bisher in der Praxis stets auf das Service (zusätzlicher) zentraler Instanzen bzw. einer weiteren *Trusted Third Party* zurückgegriffen werden muss. [51&52&53]

Pseudo-Anonymität oder Relative Anonymität

Der tatsächlich gebotene Level an Anonymität (und zugleich die mögliche Transparenz) bei der Nutzung von Blockchain-Technologien kann in Abhängigkeit der genutzten Blockchain-Plattform bzw. der verwendeten Blockchain-Anwendungen, je nach Ausgestaltung der Programmierung bzw. des darunter liegenden Netzwerkprotokolls sehr stark variieren (daher auch „relative Anonymität"). Grundsätzlich müssen sich Nutzer von (öffentlichen) Blockchains auf keine Art und Weise registrieren oder gar Identitätsdaten preisgeben, um am Transaktionsgeschehen in Blockchains teilzunehmen. Während dadurch eine Zuordnung benutzter Transaktionskonten (Wallets) zu tatsächlichen Personen für gewöhnliche Anwender unmöglich ist, kann jedoch mittlerweile von Fällen (betreffend der Blockchain Bitcoin) berichtet werden, in denen Ermittlungsbehörden, mit großem Aufwand und u.a. durch sog. Datamining die Identitäten von Bitcoin-Nutzer über die Transaktionshistorie (in Verbindung mit weiteren Daten) ausforschen konnten. (Daher kann im Zusammenhang mit Bitcoin auch von sog. Pseudo-Anonymität gesprochen werden) Unter den mittlerweile unzähligen Kryptowährungen, befinden sich etliche auf konkrete Anwendungsfälle spezialisierte Systeme und Protokollanpassungen. So haben sich neuere Blockchains wie z.B. Monero der vollständigen bzw. gänzlichen Anonymisierung ihrer Nutzer verschrieben, und machen eine Aufdeckung der Identität ihrer Netzwerkteilnehmer durch die Nutzung neuer Algorithmen und Mechanismen selbst für Ermittlungsbehörden nach aktuellem Wissenstand unmöglich. Die Ausgestaltung von Blockchain-Protokollen und genutzten Algorithmen unterliegt somit aktuell noch einem starken und stetigen Veränderungsprozess.[54]

---

[51] vgl. „Proof of Ownership - Bitcoin Wiki", zugegriffen 27. August 2019, https://en.bitcoin.it/wiki/Proof_of_Ownership.

[52] vgl. K. C. Tam, „Notarization in Blockchain (Part 2)", Medium, 28. August 2018, https://medium.com/@kctheservant/notarization-in-blockchain-part-2-1a06d00eb72.

[53] vgl. Joe Naylor, „Proof of Existence Is Not Proof of Ownership - IPWatchdog.Com", *IPWatchdog.Com | Patents & Patent Law* (blog), 2. Mai 2018, https://www.ipwatchdog.com/2018/05/02/proof-of-existence-is-not-proof-of-ownership/id=96265/.

[54] vgl. Shermin Voshmgir, „Blockchains, Smart Contracts und das Dezentrale Web" (Technologiestiftung Berlin 2016), 13, zugegriffen 29. November 2018, https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf.

Sharing-Economy

Der Begriff beschreibt das systematische Ausleihen sowie das gegenseitige Bereitstellen von Gegenständen, Räumen und auch Flächen, besonders durch private Personen und Interessengruppen. Der Begriff kann ebenso in Bezug auf das Teilen von Informationen und Wissen verwendet werden.[55] Siehe Kapitel 2.8.1. *"Blockchain als Revolution der Sharing-Economy"*

Single Point of Failure (SPOF)

Eine einzelne funktions-kritische Systemkomponente, deren Ausfall oder Fehlerhaftigkeit den Ausfall des gesamten (meist technischen) Systems mit sich zieht.[56]

Smart Contracts (SCs)

Smart Contracts (SCs) sind vordefinierte in Programmcode gegossene Vertragsbedingungen (Transaktionsregelwerke), die auf Blockchains mit erweiterter Funktionalität (sog. Smart-Contract-Plattformen) automatisch und unumkehrbar ausgeführt werden, sobald gewisse, zuvor definierte, Bedingungen oder Konditionen erfüllt werden. Sie erübrigen die Notwendigkeit einer zentralen, zwischengelagerten Instanz (insbesondere, wenn die vertrags- oder transaktionsbeteiligten Parteien sich nicht kennen) zur Überwachung, der Einhaltung und Umsetzung von Vertragsbedingungen. Durch Smart Contracts können u.a. die sonst üblichen Transaktionskosten drastisch reduziert.[57] Siehe Kapitel *2.4.3 „Smart Contracts"*

Snapshot-Verfahren (als Methode der Daten-Speicherung)

Snapshots sind Momentaufnahmen. Wesentlichstes Merkmal ist der Zeitpunkt der Auslösung. Sie werden in vielen technischen Anwendungen zum Festhalten und Dokumentieren eines bestimmten Zustandes genutzt. (Beispiele: Screenshot einer Bildschirmdarstellung, Frame-Grabbing von Videosequenzen, Backup von Daten usw.) Ziel von Snapshot-Verfahren ist es eine schnell, effizient und einfach umsetzbare Methode der Datensicherung zu ermöglichen.[58]

---

[55] vgl. Oliver Bendel, „Definition: Sharing Economy", Gabler Wirtschaftslexikon, 2012, https://wirtschaftslexikon.gabler.de/definition/sharing-economy-53876.

[56] „What Is a Single Point of Failure (SPOF)? - Definition from Techopedia", Techopedia.com, zugegriffen 11. Juni 2019, https://www.techopedia.com/definition/4351/single-point-of-failure-spof.

[57] vgl. Voshmgir, „Blockchains, Smart Contracts und das Dezentrale Web", 14.

[58] vgl. „snapshot :: Momentaufnahme :: ITWissen.info", 20. September 2017, https://www.itwissen.info/snapshot-Momentaufnahme.html.

Time-to-Market

Bei diesem Begriff ist die Zeit gemeint, die während eines Innovationsprozesses verstreicht, bis eine Produktidee oder ein Serviceidee ausreichende Marktreife hat und eine Platzierung des Produktes oder der Dienstleistung im Markt erfolgen kann.[59]

Timestamping

Beim Timestamping (das Versehen mit digitalisierten Zeitstempeln) wird die zeitliche Information betreffend eines Ereignisses (z.B.: Besitz einer Datei), von Computern aufgezeichnet und in Form von Metadaten gespeichert. Bei dem im Rahmen dieser Arbeit relevanten, Blockchain-basierten Timestamping werden sog. Hashwerte von Dokumenten (Textdateien, Fotos, Zertifikate etc.) an Nodes einer öffentlichen BC zur Verarbeitung übergeben. Daraufhin wird der Hashwert, gewissermaßen als „Transaktionstext" in der BC unmanipulierbar, mit einer exakten Uhrzeit und betreffendem Datum „digital gestempelt" und verewigt [60 & 61]

Ziel des BC-basierten Timestamping ist die Ermöglichung des sog. „*Proof of Existence*" und des "*Proof of Origin*", zudem kann es (in Verbindung mit weiteren Maßnahmen) die Grundlage für die Erstellung eines „Proof of Ownership" sein. Siehe u.a. Kapitel 2.7.3. *„Timestamping der vorliegenden Arbeit zur jeweiligen Version"*. Und Ausführungen ab Kapitel 4.4 *„Ergebnisdiskussion"*

Token (und Tokenisierung)

Token stellen eine digitalisierte Form von Vermögenswerten dar, denen eine bestimmte Funktion oder ein bestimmter Wert zugesprochen werden kann.[62] Das zugrundeliegende dezentral verteilte Transaktionssystem (die Blockchain), wird somit nicht nur zur Verwaltung einer „Grundwährung" (den sog. „Coins", wie z.B.: der bitcoin) benutzt, sondern es ermöglicht zudem (im Fall von sog. Smart-Contract-

[59] vgl. Ralf T. Kreutzer, „Definition: Time-to-Market", Gabler Wirtschaftslexikon, zugegriffen 28. August 2019, https://wirtschaftslexikon.gabler.de/definition/time-market-54271.
[60] vgl. „What Is a Timestamp? - Definition from Techopedia", Techopedia.com, zugegriffen 28. August 2019, https://www.techopedia.com/definition/16285/timestamp.
[61] vgl. „OpenTimestamps - Wikipedia", zugegriffen 18. August 2019, https://en.wikipedia.org/wiki/OpenTimestamps.
[62] „Tokenisierung", BaFin, zugegriffen 18. Juni 2019, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2019/fa_bj_1904_Tokenisierung.html.

Plattformen) die Digitalisierung des Verbriefungsprozesses von Besitzverhältnissen an bestimmten Gütern, Anlagegegenständen oder Rechten.[63] Wird eine Blockchain zur Verwaltung und Abbildung eines (Vermögens-)Wertes, inklusive der in diesem Wert enthaltenen Rechte und Pflichten, sowie dessen hierdurch ermöglichte Übertragbarkeit verwendet, so spricht man hierbei von der Tokenisierung.[64] Siehe Kapitel 2.2. *„Kryptowährungen, Tokens & ICOs – Die Blockchain-Assets"*

Turing-vollständiges System

Die Turing-Vollständigkeit eines Systems bezeichnet die universelle, uneingeschränkte Programmierbarkeit des Selbigen. Der Name leitet sich ab vom Mathematiker Alan Turing, der das Modell der universellen Turingmaschine eingeführt hat.[65]

Transaktionskostentheorie

eine auf Williamson O.s Forschungsarbeit beruhende und zur Organisationslehre zugehörige Theorie, in welcher der Vertrag (zur Gestaltung jeglicher Form von wirtschaftlicher Interaktion bzw. Transaktion) im Mittelpunkt des ökonomischen Forschungsinteresses steht. Ziel ist es, zu erklären, warum bestimmte Transaktionen in bestimmten institutionellen Arrangements (Organisationsformen), mehr oder weniger effizient abgewickelt und organisiert werden können. Es wird davon ausgegangen, dass jegliches Handeln in der Marktwirtschaft mit (Transaktions-)Kosten verbunden ist. In einem theoretisch vorstellbaren „vollkommenen Markt" gäbe es daraus resultierend keinerlei Transaktionskosten zur Umsetzung unternehmerischen Handelns.[66&67]

Trusted Third Party (TTP)

Bei einer Trusted Third Party (zu Deutsch: Vertrauenswürdige dritte Partei) handelt es sich um eine dritte Instanz, welcher zumindest zwei (ggf. einander unbekannte und in keinem Vertrauensverhältnis stehende) Parteien Vertrauen schenken. Erst

---

[63] „So verändert die Tokenisierung unser Finanzwesen und nicht zuletzt unser Leben", BTC-ECHO, 22. März 2019, https://www.btc-echo.de/so-veraendert-die-tokenisierung-unser-finanzwesen-und-nicht-zuletzt-unser-leben/.

[64] „Tokenisierung".

[65] *vgl. „Turing-Vollständigkeit", in Wikipedia, 12. Juni 2019, https://de.wikipedia.org/w/index.php?title=Turing-Vollst%C3%A4ndigkeit&oldid=189474947.*

[66] *vgl. „Transaktionskostentheorie", in Wikipedia, 17. Juni 2018, https://de.wikipedia.org/w/index.php?title=Transaktionskostentheorie&oldid=178384182.*

[67] *vgl. Óliver Williamson, „Transaction Cost Economics: How It Works; Where It is Headed", Berkeley Olin Program in Law & Economics, Berkeley Olin Program in Law & Economics, Working Paper Series 146 (1. Januar 1995), https://doi.org/10.1023/A:1003263908567.*

durch die Einschaltung einer dritten, vertrauenswürdigen Instanz, lassen sich im Bezug auf Transaktionen (jeglichen Wertes) oder die Übermittlung digitaler Daten (auf Basis herkömmlicher Technologien) vorhandene Probleme lösen, welche sich beim Wunsch nach zuverlässigen Transaktionen und sicherer Datenübermittlung ergeben.[68]

Trustless-Asset-Management

beschreibt die Option, Vermögensgegenstände z.B. digitalisierte Werte durch mathematische Algorithmen (ohne die Einbeziehung einer dritten Vertrauensperson) zu verwalten durch die Verwendung eines dezentralen Hauptbuches.[69]
Siehe Kapitel 2.2. *„Kryptowährungen, Tokens & ICOs – Die Blockchain-Assets"*

Usability

Beschreibt die Fähigkeit eines Techniksystems, sich durch eine simple und intuitive Anwendung an die Nutzerbedürfnisse anzupassen. Der Begriff bezeichnet die Nutzungsqualität, welcher der User bei der Interaktion mit bestimmten Techniksystemen erfährt.[70]

Volatilität

Bezeichnet ein Maß für die Schwankungsbreite eines Wertpapiers, einer Währung oder eines Index. Profi-Anleger beschäftigen sich intensiv mit den zu erwartenden Kursschwankungen des Marktes, da die zukünftigen Kursbewegungen über den Gewinn oder Verlust entscheiden können. Mit hoher Volatilität ist gemeint, dass der Kurs stets starken schwanken unterliegen kann.[71]

Wallet

Eine sog. Wallet ist eine Art digitales Portemonnaie bzw. eine Software zur Verwaltung des persönlichen Zugangs und der privaten Assets in einer Blockchain. Eine Wallet, ermöglicht Nutzern die Erstellung einer in Blockchain-Netzwerken einmaligen Adresse für das Empfangen u. Senden von Transaktionen (z.b. bitcoin).

---

[68] „Trusted Third Party", in *Wikipedia*, 16. Juli 2019, https://en.wikipedia.org/w/index.php?title=Trusted_third_party&oldid=906527212.
[69] vgl. Elfi, „Trustless Asset Management", *FinTech Academy* (blog), zugegriffen 28. August 2019, http://www.fintech.academy/lexicon/trustless-asset-management/.
[70] vgl. „Usability Definition", Gründerszene Magazin, zugegriffen 28. August 2019, https://www.gruenderszene.de/lexikon/begriffe/usability.
[71] vgl. finanztreff.de, „Definition: Volatilität | Börsenlexikon", zugegriffen 28. August 2019, http://www.finanztreff.de/wissen/boersenlexikon/volatilitaet/4981.

Näheres Siehe Kapitel 2.5.9 *„Digitale Signatur (Asymmetrisches Kryptosystem) und Wallets“*

Whitepaper *(im Technologie-Umfeld)*

Whitepaper stellen im Umfeld der IT einen maßgeblichen Leitfaden oder in Fachsprache gehaltenen Bericht dar, in welchem die Vorteile einer bestimmten Technologie, eines Konzeptes oder eines Verfahrens bzw. einer Richtlinie erläutert werden. Whitepaper werden häufig von Forschern, Unternehmen oder IT-Consultants verwendet bzw. veröffentlicht, um die Theorie hinter einer neuartigen Technologie oder Computermethodik zu beschreiben.[72]

51%-Attacke

Auch 51-Prozent-Angriff genannt, ist ein Begriff, der besagt, dass ein Angreifer (Hacker) in einem Netzwerk, über größere Befugnisse (z.B. eine Kontrollbeteiligung an der Erzeugung von Kapazitäten) oder über mehr Ressourcen verfügen muss, als der Rest der Netzwerkteilnehmer (mehr als die Hälfte, somit 51%). Diese Art von Angriff stellt zudem eine (je nach genutztem Konsensmechanismus) potentielle Gefahr, für die Integrität des verwalteten Datenbestandes und somit für das gesamte Transaktionssystem in Blockchain-Netzwerken dar. Z.B. ist es theoretisch denkbar, dass ein einzelner Angreifer (z.B. eine sog. *Mining-Farm*) über mehr als die Hälfte, der dem Blockchain-Netzwerk zur Verfügung stehenden Rechenleistung (Hashing-Power) für die Validierung von Transaktionen und die Erstellung neuer Blöcke (im Rahmen des *Minings-Prozesses*) verfügt. Käme es zu einem derartigen Ungleichgewicht, betreffend der Verteilung der Rechenleistung innerhalb eines Blockchain-Netzwerkes, so könnte der Angreifer neu erstellte Transaktions-Blöcke zu seinen Gunsten manipulieren und als korrekt validieren.[73] Das Problem tritt vor allem bei den von Bitocin und Ethereum aktuell genutzten Konsensmechanisums namens Proof of Work auf. Neuere Konsensmechanismen, wie das u.a. von der Smart-Contract-Plattform Ardor genutzte Proof of Stake machen 51% Attacken äußerst unrentabel und praktisch nahezu bedeutungslos. Siehe hierzu auch Kapitel 2.5.11.b „Kritik an Proof of Work als Konsensmechanismus“ und Kapitel 2.5.12 „Proof of Stake (POS)“

[72] vgl. „What Is a White Paper (in Technology)? - Definition from Techopedia“, Techopedia.com, zugegriffen 24. Juni 2019, https://www.techopedia.com/definition/5579/white-paper.

[73] vgl. „51-Prozent-Angriffe - Bitcoin wiki“, zugegriffen 28. August 2019, https://de.bitcoin-wiki.org/wiki/51-Prozent-Angriffe.

1. EINLEITUNG

Da sich die wissenschaftliche Forschung im Rahmen dieser Arbeit im Wesentlichen auf 2 Themengebiete stützt: Zum einen auf das Feld der Blockchain und Distributed-Ledger Technologien (DLTs) und zum anderen auf den Bereich unternehmerischer Innovation (dabei im speziellen auf den Ansatz der Open Innovation), ist es aus Sicht des Autors zielführend, die thematische Einführung zu unterteilen. Dabei soll der Leser zuerst in das Forschungsgebiet der Blockchain-Technologie und den der DLTs eingeführt werden (Abschnitt 1.1), bevor im 2ten Teil der Einführung, ein für den Leser nachvollziehbarer Konnex dieser komplexen Thematik, zu dem Bereich unternehmerischer Innovation im generellen und dem Paradigma der Open Innovation im speziellen, (Abschnitt 1.2) hergestellt werden kann. Anschließend soll das Kapitel noch dazu dienen, um das Ziel der Arbeit (Kapitel 1.3), die geplanten Vorgehensweisen und Methoden (Kapitel 1.4) und die behandelten Forschungs- und Teilfragen, näher zu erläutern und vorzustellen.

1.1. EINFÜHRUNG IN DAS FORSCHUNGSGEBIET DER BLOCKCHAIN-TECHNOLOGIE

Trotz eines jüngst stattgefundenen sog. *Bärenmarktes*, eingeläutet und angeführt von einem sich längerfristig fortsetzenden Kursabfall der digitalen Leitwährung *Bitcoin* (vollzogen an den weltweiten Börsen für sog. Krypto-Assets), stieg das Interesse der Öffentlichkeit an den noch relativ jungen sog. *Krypto-Währungen* fortwährend an[74].

Während sich die Tagesmedien und die Allgemeinheit hauptsächlich für Bitcoin, genutzt als alternatives, dezentral organisiertes Zahlungsmittel und digitales Asset, bzw. ggf. noch für einige, seiner mittlerweile zahlreichen Ableger, die sog. *"Altcoins",* welche ebenso als potentielle Konkurrenz zum zentralverwalteten Transaktionsgeschäft, der etablierten Finanzindustrie betrachtet werden können, interessieren, beschäftigen sich Experten aus verschiedensten Disziplinen, teils im

[74] *Horch P., 26.11.2018, „Bitcoin: Google-Suchvolumen steigt trotz Bärenmarkt" [online] entnommen am 8.12. 2018 unter: https://www.btc-echo.de/bitcoin-google-suchvolumen-steigt-trotz-baerenmarkt/*

Dienste der wissenschaftlichen Forschung, zunehmend mit der technologischen Basis dahinter: der Blockchain (BC) bzw. den DLTs.

Angesehene Kapazitäten, aus den Bereichen Management und IT prophezeien z.B. seit Kurzem eine „Blockchain Revolution“ (Tapscott D. u. Tapscott A., 2018). Sie sprechen u.a. davon, dass sich die BC (weitere Verbreitung vorausgesetzt) zu Vertrauen, ähnlich verhält bzw. verhalten wird, wie das Internet zu Information (Zitat: *„Blockchain is to trust as the Internet is to information“*, Joichi Ito, Director, MIT Media Lab; vgl. hierzu auch [75] & [76] & [77])

Aussagen und Zugeständnisse, die auf der Erkenntnis beruhen, dass die BC-Technologie als Ausprägungsform der sog. „Distributed Ledger Technologien“ (DLTs) nicht nur das Potential zur Dezentralisierung und Disintermediation der Finanzmärkte (durch die Schaffung alternativer Zahlungsmittel) bietet, sondern die Grundlage für ein eben, wesentlich breiteres Anwendungsspektrum, darstellen kann. Eine Sichtweise, die vor allem durch die Veröffentlichung von jüngeren Kryptowährungen, welche zugleich als programmierbare, dezentrale Plattformen für u.a. sog. Distributed Apps (dApps) und Smart Contracts (SCs) bzw. Smart Transactions dienen können, ihre erste große Bestätigung fand. *(Siehe u.a. Start der Ethereum-Blockchain 2015 und Erscheinung der NXT-Blockchain bereits 2013).*[78]

Von der Ermöglichung automatisiert ausführbarer Verträge über die Realisierung sog. DAOs *(personenlose, dezentralisierte autonome Organisationen bzw. Korporationen)* bis zu sog Smart Votes (Wahlen auf der BC) weiß man Folgendes: Diese Technologie wird mittlerweile, (nach aktuellem Forschungsstand) als höchst disruptiv eingeschätzt und kann dabei als Motor zur Dezentralisierung Automatisierung und Disintermediation, etlicher Wirtschafts- und Gesellschaftsbereiche erachtet werden.[79]

---

[75] „The trust machine - The Promise of the Blockchain“, *The Economist*, 31. Oktober 2015, https://www.economist.com/leaders/2015/10/31/the-trust-machine.

[76] *The Economist, 31.10.2015, [online], entnommen am 8.12.2018 unter https://www.economist.com/leaders/2015/10/31/the-trust-machine*

[77] Kevin Werbach, *The Blockchain and the New Architecture of Trust*, 1. Aufl., 2018, https://mitpress.mit.edu/books/blockchain-and-new-architecture-trust.

[78] vgl. u.a. Melanie Swan, *Blockchain: Blueprint for a New Economy*, 1. Aufl. (Cambridge: O’Reilly and Associates, 2015).

[79] vgl. u.a. Johannes Scherk und Gerlinde Pöchhacker-Tröscher, „Die Blockchain – Technologiefeld und wirtschaftliche Anwendungsbereiche“ (Im Auftrag des Bundesministerium für Verkehr, Innovation und Technologie, Bereich Innovation von Pöchhacker Innovation

Eine Begründung für die hohe Erwartungshaltung ist darin zu sehen, dass die Technologie, in Bezug auf die Verwaltung und den Austausch von jeglichen Werten zwischen einander unbekannten (Geschäfts)Partnern Vertrauen für den Werteaustausch und zudem eine Basis für kollaboratives Verhalten innerhalb eines Netzwerkes schaffen kann (und dies alles ohne den meist mit zusätzlichem Aufwand, Zeitverlust und Kosten verbundenen, Umweg über einen Intermediär, eine sog. Trusted Third Party oder eine zentrale Verwaltungs- bzw. Kontroll-Instanz).[80]

> ***"Blockchain is a vast, global distributed ledger or database running on millions of devices and open to anyone, where not just information but anything of value – money, but also titles, deeds, identities, even votes – can be moved, stored and managed securely and privately. Trust is established through mass collaboration and clever code rather than by powerful intermediaries like governments and banks."***[81] *(Tapscott & Tapscott, 2018)*

Während einige Experten nun bereits davon sprechen, wie der Game-Changer BC schon bald das uns bekannte „Internet der Information" durch ein „Internet der Werte" („Internet of Values") ersetzen wird, erwarten aktuelle Analysen und Prognosen großer IT-Konzerne und Consulting-Unternehmen für die nächsten Jahre noch keine (Markt-)Veränderungen fundamentalen Ausmaßes durch den Einfluss bzw. Einsatz der Technologie. Sie sehen Wirtschaftstreibende in Zusammenhang mit dieser Technologie aktuell noch in einer Phase des Experimentierens, bestätigen zugleich aber, dass BCs & die DLT aufgrund bisheriger Entwicklungsschritte vor dem Hintergrund einer ökonomischen Verwertbarkeit, sowie für den konkreten Einsatz im Bereich alltäglicher Geschäftsprozesse, zunehmend reifer und interessanter werden und erwarten demzufolge eine steigende Nachfrage nach BC-bzw. DLT-basierten Anwendungen für die nächsten Jahre; und dies durch Unternehmen in fast allen Branchen.[82]

Consulting GmbH, Mai 2017), https://www.bmvit.gv.at/innovation/downloads/blockchain_technologie.pdf.

[80] vgl. ua. Don Tapscott und Alex Tapscott, *Die Blockchain-Revolution: Wie die Technologie hinter Bitcoin nicht nur das Finanzsystem, sondern die ganze Welt verändert*, New enlarged edition (Kulmbach: Plassen Verlag, 2018).

[81] Don Tapscott und Alex Tapscott, „The Impact of the Blockchain Goes Beyond Financial Services", *Harvard Business Review*, 10. Mai 2016, https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.

[82] Young J. 08.10.2018, "How Big Four Auditors Delve Into Blockchain: PwC, Deloitte, EY and KPMG Approaches Compared" [online], entnommen am 06.12.2018 unter: https://cointelegraph.com/news/how-big-four-auditors-delve-into-blockchain-pwc-deloitte-ey-and-kpmg-approaches-compared

Aufbauend auf das kurz beschriebene, nun im Vergleich zu reinen Währungs- oder Bezahlsystemen, drastisch erweiterte Anwendungsspektrum der BC-Technologie, angeleitet von aktuellen Analysen und Erwartungen von Experten und namhaften IT-Consultants und gestützt auf das Wissen, dass es offenbar zu den, der BC inhärenten Eigenschaften zählt, zwischen grundsätzlich unbekannten Netzwerkteilnehmern/Akteuren eine geschäftsfähige Vertrauensstellung *(„Peer-to-Peer“* gänzlich ohne Intermediär) herzustellen, und zugleich die Basis für eine ökonomisch, zielführende Kollaboration generieren zu können, eröffnet sich dem Autor ein überaus mannigfaltiges Feld für den Bereich sozial- und wirtschaftswissenschaftlicher Forschung.

Dabei liegt es nun im Interesse des Autors diese noch relativ junge Technologie von dem vorherrschenden Hype und den (möglicherweise) überzogenen Erwartungen ungeblendet nüchtern objektiv und umfassend zu untersuchen, ihre Funktionsweise verständlich und nachvollziehbar zu erörtern, die dabei tatsächlich erkennbaren Potentiale und den sozioökonomisch anwend- und verwertbaren, technologiebezogenen Innovations-Charakter vollumfänglich zu erfassen, um, darauf aufbauend, die potentiellen Auswirkungen auf (sowie Chancen für) den Bereich unternehmerischer Innovation (u.a. speziell auf Basis unternehmensgrenzüberschreitender Innovationsprozesse) ableiten und analysieren zu können.

> ***“With the rise of a global peer-to-peer platform for identity, trust, reputation, and transactions, we will finally be able to re-architect the deep structures of the firm for innovation, shared-value creation, and perhaps even prosperity for the many, rather than just wealth for the few.”***[83] *(Tapscott & Tapscott, 2018)*

[83] Don Tapscott und Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World*, New enlarged edition (New York, NY: Portfolio, 2018), 46.

1.2. Relevanz vor dem Hintergrund unternehmerischer Innovation

Die fortschreitende Globalisierung führt zu einem stetig steigenden Wettbewerbsdruck. Sie erzeugt eine Situation, welche von Unternehmen in etlichen Branchen häufig den Einsatz moderner Methoden neuartiger Konzepte und Instrumente abverlangt, um mit dem rasanten Tempo der Märkte mithalten zu können. Strategisches Ziel ist es, häufig durch Innovationen in stetig kürzer werdenden Zeitabständen (Optimierung der *„Time-to-Market“*), Kundenbedürfnisse noch besser (Optimierung des *„Fit-to-Market“*) und effizienter (Optimierung der *„Cost-to-Market“*) als bisher befriedigen zu können, oder gar zu versuchen, sich aufgrund besonders neuartigen, „innovativen“ Entwicklungen und „radikal-revolutionären“ Angeboten oder Geschäftsmodellen, für den Kunden als herausragendes Alleinstellungsmerkmal wahrnehmbar *(„New-to-Market“*), gänzlich von der Konkurrenz abzuheben.[84]

Um den geschilderten Herausforderungen und einer stark kundenorientierten Unternehmensstrategie vor dem Hintergrund des zunehmenden Wandlungs- und Innovationsdruckes und den stetig dynamischer werdenden Umweltfaktoren besser gerecht zu werden, - u. a. kann für Innovationen, notwendiges hohes Personalvermögen und Wissen nicht immer im eigenen Unternehmen generiert oder gehalten werden (siehe demgemäß auch, die gestiegene Mobilitätsbereitschaft gut ausgebildeter Mitarbeiter)[85] – hat man bereits um die Jahrtausendwende erkannt, dass es für Unternehmen notwendig und hilfreich ist, die Innovations-gestaltung aus der Isolation und den Schranken traditioneller, interner Forschungs- und Entwicklungs-Abteilungen zu befreien, sich für externes Wissen zu öffnen und die Unternehmensgrenzen beim Durchlaufen von Innovationsprozessen durchlässig zu gestalten. Dr. Chesbrough hat diese Erkenntnis 2003 erstmals formalisiert und durch seine wirtschaftswissenschaftliche Forschung im Rahmen seiner Veröffentlichungen zu dem von ihm getauften Paradigma namens „Open Innovation“ ausgeweitet[86] und definiert den drauf beruhenden Innovationsprozess in jüngsten Publikationen folgendermaßen: *„a distributed innovation process based on purposively managed knowledge flows across organizational boudaries“*

---

[84] (vgl. Ili, Open Innovation Umsetzen, 2010)
[85] (vgl. Majid, 2010, S. 340)
[86] Henry William Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Harvard Business Press, 2003).

Über 15 Jahre nach Vorstellung dieses, für das Innovations-Management etlicher Unternehmen wegweisenden, Konzeptes und nach unzähligen Anstrengungen und Projekten, den Ansatz der Open Innovation in der Praxis zu realisieren, zeigen Erfahrungswerte, dass Unternehmen häufig auf etliche Hürden und Barrieren im Zusammenhang mit Öffnung der Innovations-Prozesse (gegenüber unternehmensexternen Akteuren) und dem Verwalten unternehmensgrenzüberschreitender Informations- und Wissensflüsse stoßen. Hindernisse und Herausforderungen, welche häufig dazu führen, dass Unternehmen kaum oder nur eingeschränkt von den Potentialen des Open-Innovation Paradigmas profitieren können.[87]

Konkret stellen z.B. komplexe Geflechte, bestehend aus archaischen Prozessstrukturen, der Einsatz von veralteten unzeitgemäßen IT-Systemen und die Vermittlung inadäquat ausgerichteter Anreize, welche sich häufig unternehmensintern, vor allem aber auch unternehmensgrenzüberschreitend – über die Wertschöpfungsketten bzw. Netzwerke ganzer Industrien und Branchen hindurch - feststellen lassen, ihrerseits nicht selten, eine wesentliche Hürde für eine unternehmerisch erfolgreiche Partizipation an Innovationsprozessen, dem Schema der Open-Innovation folgend, dar. Um in derartigen Szenarien dennoch eine Chance auf erfolgreiche Open Innovation-Projekte und deren Umsetzungen generieren zu können, bedarf es u.a. der Möglichkeit, das Agieren einer Vielzahl an Teilhabern, in ebensolchen Wertschöpfungs-Netzwerken - über die Grenzen ihrer jeweiligen Unternehmen hinweg - gleichzeitig in einer für sie nachvollziehbaren, zielführenden Weise risikoarm vertrauenswürdig und dennoch effizient, orchestrieren zu können.[88]

Der Einsatz der BC-Technologie könnte sich nun in derartigen Szenarien - so wie in anderen, für die Gestaltung von unternehmensgrenzüberschreitenden Innovationsprozessen relevanten Bereichen - als erfolgsversprechende Lösung herausstellen: Die Technologie könnte dazu beitragen, Barrieren, bei denen es u.a. um einen vertrauenswürdigen sicheren und nachvollziehbaren Umgang mit sensiblen, erfolgskritischen Informationen, wie z.B. Produktentwürfen oder ähnlichem schützenswertem geistigen Eigentums (Intellectual Property [IP]) in Netzwerken mit unbekannten oder sich misstrauenden Akteuren geht, zu reduzieren oder zu umge-

[87] (vgl. Majid, 2010, S. 340)
[88] vgl. Josep Lluis De La Rosa u. a., „A Survey of Blockchain Technologies for Open Innovation“, 2017, 1.

hen und z.B. durch verschiedenste technologie-inhärente Möglichkeiten zur Incentivierung teilhabender Akteure dafür Sorge tragen, dass die Kollaboration in derartigen Netzwerken ein neues Niveau an Produktivität und Effizienz erreicht. Theoretische Überlegungen, welche den Einsatz der BC-Technologie im konkreten Bereich der Open Innovation als vielversprechend erscheinen lassen und sich aus Sicht des Autors als Grundlage für eine Nähere und wissenschaftlich fundierte Erforschung förmlich aufdrängen.

> ***"But, as with the Internet, the Web and other major technologies, the blockchain technology has now transcended its original objective. It has the potential to revolutionize the finance industry and transform many aspects of the digital economy […] the Open Innovation (OI) and the IP-industry (Intellectual Property) will also be affected"***[89] *(de la Rosa et. al., 2017)*

Auf Basis dieser Perspektive gilt es nun, im Rahmen der vorliegenden Arbeit, die vielfältigen Potentiale der Technologie Blockchain, vor dem Hintergrund unternehmerischer Innovation, generell und im Bezug auf den konkreten Anwendungsbereich - der Gestaltung von unternehmensgrenzüberschreitenden Prozessen - im speziellen, umfassend zu untersuchen und zu analysieren. Es geht darum, mögliche Synergien, beider behandelten Forschungsfelder auszuloten und darzustellen. Wobei für eine Evaluierung tatsächlich verwertbarer Stärken, Schwächen, Chancen und Risiken das Konzept eines offenen, dezentral verteilten, vertrauensschaffenden Netzwerkes, und der Ansatz für eine, auf Konsensbildung beruhende Kollaboration, unter unbekannten Netzwerkteilnehmen (jener der Blockchain-Technologie), auf das ebenfalls offene und (ebenfalls) auf etliche (unternehmensfremde) Akteure verteilte Paradigma der Open Innovation treffen soll.

[89] Lluis De La Rosa u. a., 1.

1.3. Ziel der Arbeit

Ziel ist es, durch Herausarbeitung des, der BC und DLTs inhärenten Innovations-Charakters, Potentiale für die Nutzung dieser Technologien als Motor bzw. Treiber für die Umsetzung von unternehmerischen Innovationen generell, und darauf aufbauend, speziell in Innovationsprozessen gemäß dem Open-Innovation-Paradigma aus sozioökonomischem, erkenntnisleitendem Interesse zu ermitteln und aus unternehmerischer Sicht zu bewerten.

Die Arbeit soll somit, auf genereller Ebene dazu beitragen, BCs und den durch sie eröffneten, aktuell gegebenen Möglichkeitshorizont, besser bzw. bestmöglich vollumfassend verstehen und nachvollziehen zu können, um die untersuchte Technologie, so dann - auf Basis des erlangten, weitreichenden Verständnisses - vor dem Hintergrund einer möglichen ökonomischen Verwertung, insbesondere betreffend, den aktuell erkennbaren Implikationen auf dem Handlungsfeld, unternehmerische Innovation bewerten und einordnen zu können. Darüber hinaus sollen auf spezifischer Ebene mögliche Stärken, Schwächen, Chancen, Risiken, betreffend einer möglichen Technologie-Anwendung zur Gestaltung und Umsetzung unternehmensgrenzüberschreitender Innovationsprozesse herausgearbeitet und analysiert werden.

1.4. Methoden und Vorgehensweise

Die vom Autor gewählte Vorgehensweise zur Erreichung zuvor genannter Ziele, lässt sich in 2 wesentliche Schritte unterteilen.

1.4.1. Erfassung des Innovations-Charakters von BCs

Induktives Vorgehen

In einem ersten und für die Arbeit grundlegenden Schritt soll durch eine ausführliche umfangreiche und gründliche Recherche von u.a. verfügbarer Literatur, aktuellen Berichten, Artikeln, Essays und Internet-Quellen (Blog-Beiträge, Video-Beiträge usw.) ein dem Status quo der BC und den DLTs entsprechendes sog. Big Picture generiert werden. Dabei geht es darum, die gesamte Bandbreite möglicher

Potentiale für und möglicher Implikationen auf das Feld unternehmerischer Innovation offenzulegen, und somit den Innovations-Charakter dieser noch relativ jungen Technologie aus sozioökonomischer Perspektive zu ermitteln. Der im Rahmen dieses ersten Schrittes zu generierende Informations- und Wissensfundus soll zudem eine essentielle Basis für den 2ten Schritt im Rahmen dieser Arbeit bilden.

Um den genannten Anforderungen des ersten Schrittes der Arbeit zu erfüllen, wären mit dem Themenkomplex der BC und DLTs in Verbindung stehende Domänen wie z.B.: erkundbare & auffällige Phänomene (u.a. Kryptowährungen, Prognosen und aktueller Hype etc.) sowie vorhandene Erfahrungs- und Wissensgebiete (wie u.a. Hintergründe zur Entwicklungs-Historie, der technischen Evolution, aktuelle Ausprägungsformen, Bekannte use-cases etc.) sorgfältig und dem Maßstab wissenschaftlicher Arbeit folge leistend zu untersuchen.

Die jeweiligen Ermittlungs- und Analyseergebnisse sollen sodann - gemäß induktivem Vorgehen - zu besagtem Big Picture der BC und DLTs zusammengefügt werden und stellen als Gesamtheit die Basis zur Dokumentation und Ermittlung des Innovations-Charakters dar und umfassen dabei bestmöglich alle (aktuell feststellbaren) für das Handlungsfeld unternehmerischer innovationsrelevanten Potentiale und Eigenschaften der Technologie. Siehe hierzu Abbildung 1:

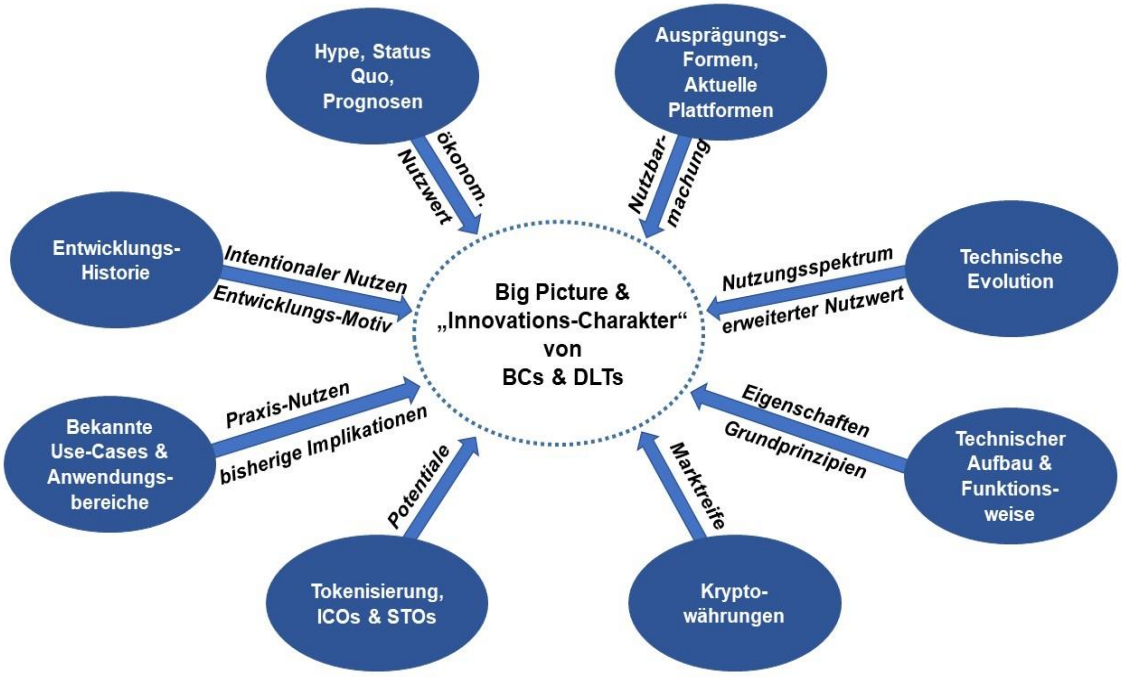

Abb. 1: Ermittlung des Innovations-Charakters mittels induktivem Vorgehen[90]

[90] eigene Darstellung

1.4.2. Analyse der Potentiale, Chancen und Risiken des Einsatzes von BCs in OI

Deduktives Vorgehen, strukturiertes Literatur-Review und Synthese

Im zweiten Schritt dieser Arbeit gilt es den spezifischen Anwendungsfall von BCs und DLTs im Bereich unternehmensgrenzüberschreitender Innovationsprozesse nach dem Paradigma der Open Innovation zu untersuchen. Dabei sollen nun aus dem, im ersten Schritt (betreffend den Innovations-Charakter der BC und DLTs) erstellten, umfangreichen Informations- und Wissensfundus durch deduktives Vorgehen relevante Potentiale abgeleitet und u.a. spezifische Stärken und Schwächen für den genannten konkreten Anwendungsfall determiniert werden.

Die erkannten Potentiale sollen dann ihrerseits auf Basis der Ergebnisse eines durchgeführten, strukturierten, nachvollziehbaren - auf den zu analysierenden Einsatzzweck stark fokussierten - Literatur-Reviews (welches ggf. ermittelbare Erfahrungswerte offen legen kann) im Rahmen einer Synthese zu konkreten Chancen und Risiken für den Umgang mit der Technologie am Feld der Open Innovation verfeinert und ausgewertet werden. Siehe hierzu Abbildung 2:

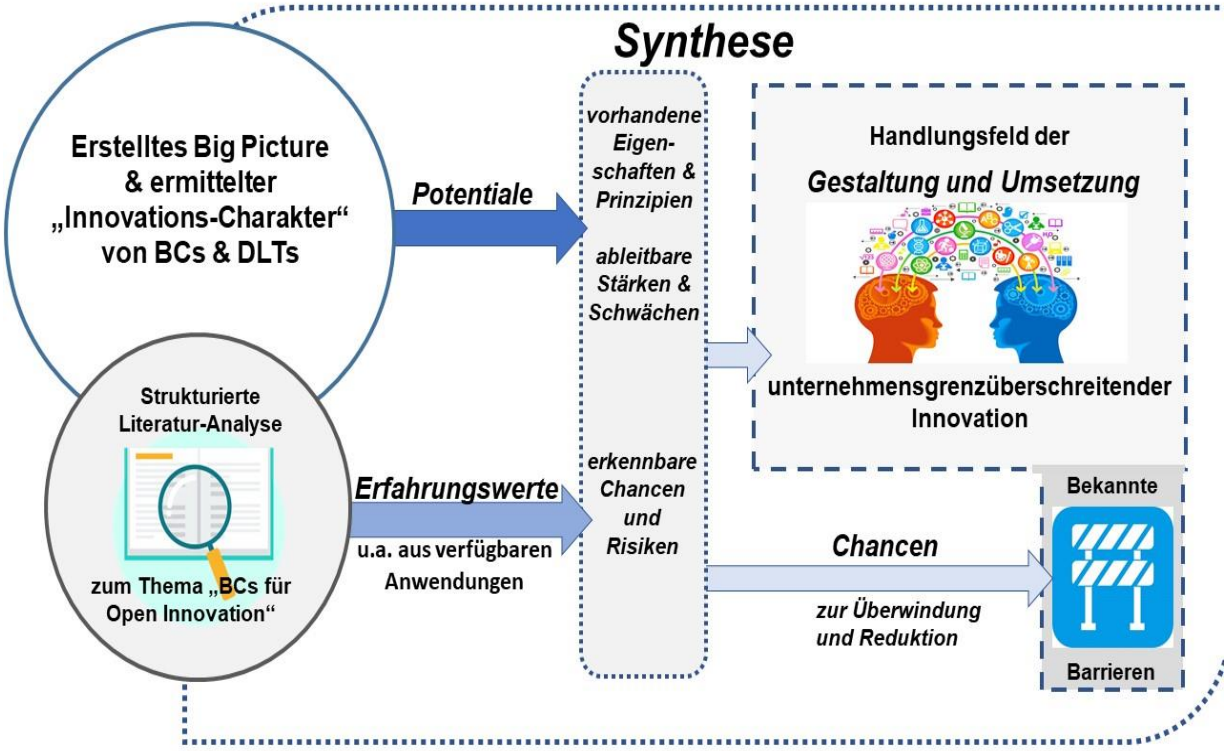

Abb. 2 : Ermittlung spezifischer Potentiale, Chancen & Risiken mittels strukturierter Literatur-Analyse und Synthese nach deduktivem Vorgehen[91]

[91] eigene Darstellung

1.5. Zentrale Forschungsfrage und Hilfsfragen

Die zentrale, für diese Arbeit erkenntnisleitende Forschungsfrage lautet folgendermaßen:

- **Welche Potentiale und Implikationen lassen sich nach aktuellem Kenntnis- und Wissensstand beim Einsatz der BC und DLTs für/auf den Bereich unternehmerischer Innovation, speziell vor dem Hintergrund unternehmensgrenzüberschreitender Innovationsprozesse, erkennen und ermitteln?**

Für die Beantwortung der zentralen Forschungsfrage können folgende Hilfsfragen definiert werden:

- *Wie funktioniert die Blockchain-Technologie?*
- *Wo liegt der Unterschied zu den sog. Distributed Ledger Technologien?*
- *Wie funktionieren Smart Contracts?*
- *Was sind Smart-Contract-Plattformen, Distributed Apps (dApps) und sog DAOs?*
- *In welcher (Ausprägungs-)Form, auf Basis welcher Angebote und in welchem Funktionsumfang können die BC-Technologie und die DLTs zur Zeit für Unternehmen zur Umsetzung (und Gestaltung) von Innovationen genutzt werden?*
- *Welche (bis dato ggf. ungenutzten) Potentiale und Implikationen lassen sich aus der Entwicklungs-Historie, der technischen Evolution, dem Technischen Aufbau und der Funktionsweise der BC-Technologie auf das Feld unternehmerischer Innovation ableiten und erkennen?*
- *In welchen Bereichen existieren bereits BC- und DLT-basierte Innovationen (Anwendungsszenarien), welchen Nutzen zeigen bereits bekannte use-cases?*
- *Worauf beruht der Innovations-Charakter der BC-Technologie: Auf Basis welcher Eigenschaften, Grundprinzipien und technologie-inhärenten Stärken ist er festzumachen?*
- *Welche Barrieren existieren zur Zeit im Bereich der Umsetzung und Gestaltung von unternehmensgrenzüberschreitenden Innovationsprozessen nach dem Paradigma der Open Innovation?*

2. DIE BLOCKCHAIN-TECHNOLOGIE

Um vorhandene Synergien, beider in dieser Arbeit behandelten Hauptfelder, in weiterer Folge besser analysieren, verstehen und ermitteln zu können, ist es unumgänglich, sich zuerst exklusiv und ausführlich mit der Blockchain (BC) und Distributed-Ledger-Technologien (DLTs) zu beschäftigen. Hier gilt es vorrangig, bisherige Entwicklungen am Feld dieser neuartigen Technologie zu beleuchten, ihre grundlegende Funktionsweise zu erörtern und die ihr inne liegenden – speziell für die Gestaltung und Umsetzung von unternehmerischer Innovation relevanten - Potentiale festzustellen. Aus Sicht des Autors, ist es der Erfassung der Tragweite des offenzulegenden Innovations-Charakters, sowie der umfassenden Bandbreite der hier behandelten Thematik dienlich, die BC bzw. die DLTs aus verschiedenen Blickwinkeln zu beleuchten: zum einen, aus einer stellenwertbezogenen, sozioökonomischen Perspektive und zum andren, aus einer eigenschaftsorientierten, sowie funktionsbezogenen, technologischen Perspektive. (Elemente, beider hier erkenntnisleitenden Disziplinen, sind auch für das, im Weiteren erläuterte Anwendungsgebiet – den unternehmensgrenzüberschreitenden, offenen Innovationsprozessen - von fundamentaler und erfolgsbestimmender Bedeutung)

Im vorliegenden Kapitel geht es vorerst darum, die Entwicklungsgeschichte und den Ursprung dieser neuartigen Technologie namens BC zu erörtern. Gemäß einer Adaption eines bekannten Zitates: *„Nur wer weiß, woher die technologische Innovation kommt, weiß wohin die technologische Innovation mit uns geht bzw. wohin sie uns bringen kann“* (Original: „Nur wer weiß, woher er kommt, weiß wohin er geht“) sollen nach Abklärung des historischen Ursprunges aktuelle Anwendungsmöglichkeiten aus der technischen Funktionsweise ableitbare Eigenschaften und Grundprinzipien, mögliches „revolutionäres“ bzw. disruptives Potential und aufgrund weiterer Recherche, aktuell ermittelbare Implikationen auf Wirtschaft und Gesellschaft, weitestgehend der Status quo, sowie, der für ökonomische Prozesse ggf. relevante Innovations-Charakter dieser Technologie, offengelegt werden.

Die wichtigsten, der im Rahmen dieses ersten Abschnittes, zum Thema BC relevanten Begrifflichkeiten wurden bereits im Glossar kurz definiert und abgegrenzt und sollen vorerst, für ein fundiertes Verständnis im Rahmen der ersten Kapitel genügen, bevor in Kapitel 2.5 „Aufbau und Funktionsweise der DLT „Die Blockchain-Technik“ für betreffende Termini weitreichendere und wissenschaftlich akkurate Definitionen erarbeitet werden.

2.1. Von der Motivation zur Innovation des Zahlungsverkehrs – die Blockchain-Historie

2.1.1. Das Whitepaper zum Verteilten Transaktionssystem

Am 31. Oktober des Jahres 2008 veröffentlichte eine bis dato unbekannte Person (oder Personen-Gruppe) unter dem Pseudonym „Satoshi Nakamoto“ ein 8-seitiges Whitepaper mit dem Titel *„Bitcoin: A Peer-to-Peer Electronic Cash System“*[92] über eine E-Mail-Verteilerliste an einen Kreis Kryptographie-Interessierter Datenschutz-Aktivisten. In diesem *Whitepaper* beschreibt Nakamoto den Community-Teilnehmern konzeptuell die Umsetzbarkeit eines verteilten Datenbank-Systems zum Austausch der Verwaltung und der Erstellung einer digitalen Währung („…an electronic coin defined as a chain of digital signatures…“), genannt *Bitcoin*, welche es unter Zuhilfenahme ausgeklügelter kryptographischer Methoden eines verteilten Konsens-Mechanismus und eines inkludierten Anreizsystems (*siehe hierzu u.a. Kapitel 2.5.10 „Konsensmechanismen“*) erlaubt, Geld-Transaktionen elektronisch, gänzlich ohne Mittelsmann, anonym aber dennoch vertrauenswürdig, nachprüfbar und fälschungssicher durchzuführen. Das beschriebene System, ermöglicht es auf der Grundlage eines sogenannten *Peer-to-Peer-Netzwerkes*, (Netzwerke wie z.B.: „Napster“, die bisher vor allem für den direkten Austausch von Datei-Kopien genutzt wurden, *siehe Kapitel 2.3. „Internet und Peer-to-Peer-Netzwerke als Fundament – Die Blockchain Prinzipien“)* elektronische Geldeinheiten direkt von Computer zu Computer bzw. Netzwerkteilnehmer zu Netzwerkteilnehmer zu senden, gänzlich ohne der Zwischenschaltung einer Bank, einer zentralen Kontrollinstanz oder einer ähnlichen, vertrauenswürdigen Institution als Dritten *(„Trusted Third Party, TTP“*).[93]

Das verteilte Transaktionssystem soll jegliche Verwaltung des Vermögens durch zwischengeschaltete Dritte für seine Nutzer überflüssig machen. Ziel ist es, die Eigenschaften von Bargeld nachzuahmen und zu digitalisieren und den Nutzern durch das Ausschöpfen technologischer Möglichkeiten (u.a. kryptographische Verfahren zur Absicherung des Systems u. ein verteiltes Netzwerk als Grundlage) das bisher höchste Maß an Freiheit in der Geldgeschichte zu bieten und dabei das Vertrauen in die Infrastruktur bestehender Finanzinstitute obsolet zu machen.[94]

---

[92] Satoshi Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System“, 2008, https://bitcoin.org/bitcoin.pdf.
[93] vgl. Nakamoto.
[94] vgl. Patrick Rosenberger, *Bitcoin und Blockchain: Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik* (Springer Vieweg, 2018), 1ff, https://www.springer.com/us/book/9783662560877.

2.1.2. FINANZKRISE ALS IDEALER VERÖFFENTLICHUNGSZEITPUNKT

> ***„What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."***[95]

Der Veröffentlichungszeitpunkt dieses revolutionären Konzeptes zur Verwirklichung eines vollständig dezentralen Transaktionssystems als mögliche Alternative zu zentralen, etablierten Zahlungs-/Transaktions-Systemen, scheint kein Zufall zu sein: Der September des gleichen Jahres, vor der Veröffentlichung dieses Whitepapers, ging als Höhepunkt[96] einer bereits über 13 Monate andauernden Weltwirtschaftskrise in die jüngste Zeitgeschichte ein, deren erkennbare Ursachen und Auswirkungen zu einer Vertrauenskrise am Interbankenmarkt führten und letztendlich das Vertrauen vieler Menschen in die etablierten Finanzsysteme grundsätzlich erschütterten.

Ein weniger bekannter Fakt, der diesen Verdacht eines bewusst intendierten Zusammenhanges zwischen Veröffentlichungszeitpunkt und dem Höhepunkt der Finanzkrise von 2008 nahe legt, ist, dass bei der Generierung des ersten (Transaktions-)Blockes, Anfang 2009 (ausgelöst durch den Start, der auf Basis des Whitepapers entwickelten „Bitcoin-Software", auf Nakamoto's eigenem Computer) jener Daten-Block, nicht nur die erste, jemals auf einer BC getätigte Transaktion speicherte, sondern von Nakamoto hierin zusätzlich eine Text-Nachricht versteckt wurde. Die hinterlegte Botschaft dient nicht nur als Nachweis des Aktivierungs-Datums, des Transaktionssystems, sondern dient durch geschickte Auswahl zugleich, als, bis heute, durch die Bitcoin-Blockchain „verewigter", Beleg, des dramatischen Zustandes des globalen Finanzsystems zum damaligen Zeitpunkt.

---

[95] Nakamoto 2008

[96] vgl. „Weltfinanzkrise", in *Wikipedia*, 17. Mai 2019, https://de.wikipedia.org/w/index.php?title=Weltfinanzkrise&oldid=188675154.


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salman Rushdie I won't marry again

Giant killing? Guide to the FA Cup third round

Der *zusätzliche Textinhalt* in diesem *Genesis-Block*, der die *Transaktionsgeschichte von Bitcoin startete*, beinhaltet eine *Schlagzeile* der britischen Tageszeitung „*The Times*“ und lautet wie folgt: *„The Times*, *03/Jan/2009*, *Chancellor on brink of second bailout for banks*.“[97]

Abb. 1: Titelseite der Tageszeitung „The Times“ vom 3. Jänner 2009

Mit der textlichen Aufnahme dieser Schlagzeile in den ersten Datenblock sollte, nach einem erneut gescheiterten Versuch, die Wirtschaft in der Krise wieder anzukurbeln, offenbar von Nakamoto nahegelegt werden: Es ist an der Zeit, was Neues zu probieren.[98]

Recherchiert man weiter, betreffend die historischen Hintergründe von digitalen Währungen und deren Entwicklungsstand zum Veröffentlichungszeitpunkt von Bitcoin, so scheint die Theorie einer zeitlich (und sogar ideologisch, siehe nächsten Abschnitt) gezielt geplanten Veröffentlichung des Bitcoin-Konzeptes immer plausibler zu sein.

Nick Szwabo, ein Informatiker und Rechtswissenschaftler, der für seine Forschungen und Veröffentlichungen im Bereich von digitalen Verträgen und digitalen Währungen bekannt ist, und zudem bereits um die Jahrtausendwende ein Konzept für ein Kryptographie gestütztes Zahlungssystem vorstellte (Zahlungssystem, namens „Bit Gold“, bereits 1998 entworfen, jedoch nie implementiert aufgrund beschriebener Mechanismen, jedoch gerne als „direkter Vorläufer der Bitcoin-Architektur“ bezeichnet), stellt sich 2011 in seinem Blog in einem Eintrag mit dem Titel *“Bitcoin what took ye so long?“*, die Frage, wie es, trotz des schon länger ausreichend vorhandenen technologischen Entwicklungsstands, bereits umfangreich, vorhandener wissenschaftlicher Vorarbeit zum Thema Kryptographie und digitale Währungen, sowie dem Vorhandensein etlicher ähnlicher Konzepte, sein konnte, dass eine erfolgreiche (da von einer gewissen Masse genutzte) Implementierung

[97] vgl. Peter Lipovyanov, *Blockchain for Business 2019: A User-Friendly Introduction to Blockchain Technology and Its Business Applications* (Packt Publishing, 2019), 24.
[98] vgl. Peter Farquhar, „In der ersten Bitcoin-Transaktion soll eine geheime Botschaft versteckt sein“, Business Insider Deutschland, zugegriffen 7. Juni 2019, https://www.businessinsider.de/der-grund-warum-bitcoin-exisitert-2017-11.

eines digitalen und alternativen Zahlungssystems seiner Ansicht nach so lang auf sich warten ließ. Hier sei angemerkt, dass z.B. die Idee zu einer chronologisch, nachvollziehbaren und unveränderlichen Dokumenten- bzw. Datenerfassung (konkret: ein Konzept, um Dokumente bzw. Datenbankeinträge mit einem Zeitstempel zu versehen, diese chronologisch miteinander zu verlinken, in Datenblöcken zusammenzufassen und dann diese Datenblöcke wiederum jeweils miteinander konsistent zu verketten) bereits 1991 von Haber und Sorretta als „linked timestamping" bezeichnet, in einem wissenschaftlichen Artikel publiziert wurde. [99] (*siehe hierzu Abschnitt 2.1.4)*

Nick Szabo attestiert nun, dass (neben dem noch fehlenden Konzept zur Lösung des sog. *Double-spending-Problems* bei vollständiger Dezentralisierung) die Hauptursache für den seiner Ansicht nach relativ späten Durchbruch vor allem darin zu suchen sei, dass die Notwendigkeit für ein derartiges Konzept bis 2008, außerhalb gewisser datenschutzinteressierter Gruppen, schlichtweg nicht gesehen wurde und zudem schätzt er, dass innerhalb der Kreise von Mathematikern und Kryptographie-Experten die Motivation, und der Bedarf zu einer komplett dezentralisierten und damit institutionslosen Lösung vor 2008 nicht ausreichend gegeben war.[41]

Es ist daher anzuzweifeln, ob sich bereits vor der Finanzkrise eine ausreichend große (interessierte) Teilnehmerzahl für ein derartiges dezentrales Transaktionssystem gefunden hätte, vor allem auch, um den, für Wert und nachhaltige Akzeptanz, eines (virtuellen) Währungsmittel essentiellen Funktions- und Sicherheitsbeweis auch ausreichend wirksam erbringen zu können. (Akzeptanz- und Funktionsbeweis). Somit darf angenommen werden, dass erst die Erschütterung des Vertrauens in die Finanzsysteme den Bedarf und die Motivation für die Nutzung eines digitalen Zahlungssystems schuf. Ein Fakt, der letztendlich, dank des plötzlichen Interesses für alternative Zahlungsmittel, getragen von *Netzwerkeffekten*, einem neuartigen Transaktions-System, namens Bitcoin, zum Durchbruch verhalf. (In Relation zu bisherigen Versuchen, ähnliche Systeme zu etablieren)

[99] vgl. Nick Szabo, „Unenumerated: Bitcoin, what took ye so long?", *Unenumerated* (blog), 28. Mai 2011, http://unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html.

2.1.3. Die Ideologie: Vom Krypto-Anarchismus zur Cypherpunk-Bewegung

> **"*Privacy is a right like any other. You have to exercise it or risk losing it.*"**[100]

Um das, von Medien häufig beschworene disruptive bzw. oft auch als revolutionär bezeichnete Potential der Blockchain, besser erfassen und nachvollziehen zu können ist es von Vorteil, sich mit den geistigen Vätern bzw. der ideologischen Kinderstube der ersten veröffentlichten Blockchain, in ihrer Ausprägungsform als Zahlungsmittel Bitcoin, näher zu beschäftigen.

Nakamoto hat, wie eingangs erwähnt, sein Whitepaper erstmalig über eine E-Mail-Verteiler-Liste veröffentlicht, wobei der Empfänger-Kreis auf dieser Mail-Liste aus Mitgliedern der sog. Cypherpunk-Bewegung bestand.

Cypherpunks stellen eine Gruppe IT-affiner Internet-Nutzer dar, welche sich seit ihrer Gründung 1993 für die Wahrung von Anonymität, die Verbreitung von Datenschutz und die Nutzung von kryptographischen Verfahren einsetzen; und dabei gleichzeitig versuchen, den Einflussbereich und die Macht von großen zentralen Institutionen auf einzelne Individuen einzudämmen.[101] Die Bezeichnung Cypherpunk beruht auf einer selbst gewählten Wort-Kreation, der englischen Begriffe Cyber, Cipher (englisch für Chiffre) und Punk. Die Bewegung hatte zum Zeitpunkt ihrer Gründung etwa 700 Mitglieder.[102] Ein Gründungsmitglied der Cypherpunk-Bewegung war Timothy C. May, welcher selbst jedoch bereits 1988 einen Text mit dem Titel *„The Crypto Anarchist Manifesto"* veröffentlichte und damit den Begriff des sog. *Krypto-Anarchismus* prägte.[103]

---

[100] Zitat von Paul Zimmermann, Erfinder der E-Mail-Verschlüsselungssoftware „Pretty Good Privacy" (PGP). Er gilt als erste Person welche komplexe Kryptographie-gestützte Software der Allgemeinheit zum Schutze ihrer Privatsphäre leicht zugänglich machte. https://de.wikipedia.org/wiki/Phil_Zimmermann

[101] Vgl. Elfriede Sixt, *Bitcoins und andere dezentrale Transaktionssysteme: Blockchains als Basis einer Kryptoökonomie* (Gabler Verlag, 2017), 6, https://www.springer.com/de/book/9783658028435.

[102] Rosenberger, *Bitcoin und Blockchain*, 13.

[103] vgl. „Krypto-Anarchismus", in *Wikipedia*, 4. März 2019, https://de.wikipedia.org/w/index.php?title=Krypto-Anarchismus&oldid=186248076.

Der Krypto-Anarchismus

Bereits vor über 30 Jahren wies May darin auf die Möglichkeiten und die Potentiale hin, die sich aufgrund der aufkommenden Computertechnik für Anonymität und Datenschutz im Bereich jeglicher Kommunikation und Interaktion ergeben werden und sprach bereits von einer Revolution, die bekannte Regularien und bestehende Transaktionssysteme aus den Angeln werfen wird. Konkret heißt es in seiner Veröffentlichung:

> ***"These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."***

Dabei macht er klar, dass die hierfür nötigen Methoden in der Theorie bereits seit Ende der 70er Jahre existieren:

> ***„The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade."*** [104]

Die Cypherpunk-Bewegung

Die, der Ideologie des Krypto-Anarchismus, nahestehende Cypherpunk-Bewegung wiederum beruft sich bei Ihren Aktivitäten auf ein von Eric Huges, wenige Monate nach Gründung 1993 formuliertes Manifest mit dem Titel *„A Cypher punk manifesto".* Die Cypherpunk-Bewegung unterstreicht in diesem, ihrem Manifest von 1993, nun die besondere Notwendigkeit der Privatsphäre von Individuen; so wird der erhöhte Schutz der Privatsphäre des Einzelnen, für die Aufrechterhaltung einer offenen Gesellschaft im Gesamten, in Zeiten einer fortschreitenden digitalen Vernetzung, als essentielle Notwendigkeit erachtet. Privatsphäre wird in ihrem Manifest definiert, als:

> ***„[..] the power to selectively reveal oneself to the world."***

Zur Wahrung, der von ihnen proklamierten Privatsphäre werden kryptographische Methoden erwogen und konsequenterweise für jeden Internet-Nutzer als weltweit zugänglich eingefordert. Schließlich sehen es Cypherpunks als ihren ideologischen Auftrag an, anonyme Transaktionssysteme für eine freie Gesellschaft zu erstellen. Es wird so ausgeführt:

---

[104] May Timothy C., „The Crypto Anarchist Manifesto", 1988, https://www.activism.net/cypherpunk/crypto-anarchy.html.

> **„We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money."** [105]

Tatsächlich gehen aus heutiger Sicht etliche Versuche anonyme, digitale Zahlungssysteme zu etablieren auf Mitglieder der Cypherpunk-Bewegung zurück. (Siehe hierzu nächsten Abschnitt)

2.1.4. Historische Meilensteine am Weg zur ersten Blockchain-Anwendung

Hier nun ein Überblick über die (Forschungs-)Arbeiten, Konzept-Studien und über die historischen Meilensteine, welche die Erschaffung der ersten *Distributed-Ledger*-Anwendung, der Bitcoin-Blockchain, erst ermöglichten:

Jahr	**Konzept / Forschungsarbeit / Implementierung**
1989	David Chaum (Gründer der „Internationalen Vereinigung für Kryptographie-Forschung" [„International Association for Cryptologic Research IACR"] und Erfinder einiger kryptographischer Protokolle[106]) startet mit dem Unternehmen ‚DigiCash'. Die durch Seriennummern digital dargestellten Gutscheine namens „Cybercoin", konnten hierbei bereits durch die Anwendung sog. *Public-Key-Kryptographie* (siehe Kapitel 2.5.8 Digitale Signatur) vollständig anonym erworben werden. Die Übermittlung dieser ersten digitalen Münzen war per E-Mail möglich. Zur Validierung der Transaktionen und zur Vermeidung einer doppelten Ausgabe des „Cybercoins" musste jedoch (im Vergleich zu BCs u.a. noch) ein zentralisierter Server betrieben werden. *(Der Bezahlungsdienstleister Paypal funktioniert heute ähnlich)*[107]
1997	Der britische Kryptograph Adam Beck entwickelt ein sog. *„Proof of Work"*-System (siehe Kapitel 2.5.8 Konsensmechanismen) mit dem

[105] „A Cypherpunk's Manifesto", zugegriffen 5. Juni 2019, https://www.activism.net/cypherpunk/manifesto.html.
[106] „David Chaum", in *Wikipedia*, 18. Februar 2017, https://de.wikipedia.org/w/index.php?title=David_Chaum&oldid=162781140.
[107] „eCash", in *Wikipedia*, 1. Juni 2019, https://de.wikipedia.org/w/index.php?title=ECash&oldid=189163506.

	Namen “HashCash”. Ziel dieses, von Nakamoto 2008 in seinem Whitepaper zitierten (und von Bitcoin verwendeten), Systems war es, ursprünglich mit einem, durch Rechenzeit bezahlbaren „virtuellen Porto“, (dessen „Bezahlung“ vom Empfänger durch kryptographische Methoden verifiziert werden kann), den Versand von E-Mail-Spams und das Aufkommen von *Denial-of-Service-Attacken* einzudämmen.[108]
1998	Wei Dai entwickelt ein Konzept namens „b-money“ und schlägt dabei vor, Beck’s „HashCash-Funktion“ zur Schaffung von *Kryptowährungs*-Einheiten zu nutzen, zudem sieht sein Konzept bereits die Nutzung eines Peer-to-Peer-Netzwerkes vor.
2005	Hal Finney *(welcher später zusammen mit Nakamoto, dessem Konzept folgend, den Quellcode und die gesamten Sicherheitsprotokolle mitentwickelte er gilt neben Nakamoto als einzig namentlich bekannter Mitentwickler der Kryptowährung Bitcoin*[109]*)* stellte das sog. „Reusable Proof-of-Work-Konzept“ vor und schlug damit die konkrete Schaffung einer Kryptowährung auf Basis eines verbesserten Hascash-Konzeptes und den Ansätzen von Wei Dai’s b-money vor.
1998 bis 2005	Nick Szabo arbeitet an einem digitalen Transaktionssystem namens „bit-gold“.[110] Ein System, das den Proof-of-Work Ansatz von Beck verbesserte und dadurch die mehrfache (rechtmäßige bzw. systemkonforme) Nutzung der erschaffenen digitalen Währungseinheiten erstmalig ohne Hinzuziehen einer zentralen Instanz ermöglichte. Die virtuelle Währung bit-gold wurde nie implementiert. Aufgrund ihrer Eigenschaften wird sie jedoch in der Literatur als Vorläufer-Konzept des heutigen bitcoin beschrieben. [111]

Tab. 1: Historische Meilensteine am Weg zur ersten Blockchain

[108] „Adam Back“, in *Wikipedia*, 7. Mai 2019, https://de.wikipedia.org/w/index.php?title=Adam_Back&oldid=188336147.

[109] „Hal Finney“, in *Wikipedia*, 15. April 2019, https://de.wikipedia.org/w/index.php?title=Hal_Finney&oldid=187593150.

[110] Sixt, *Bitcoins und andere dezentrale Transaktionssysteme*, 7.

[111] „Nick Szabo“, in *Wikipedia*, 29. Mai 2019, https://en.wikipedia.org/w/index.php?title=Nick_Szabo&oldid=899331368 Abschnitt „Bit Gold“.

Alle bis 2008 „Implementierten“ digitalen Währungs- und Zahlungssysteme hatten (und haben im Fall von z.B. PayPal noch heute) den wesentlichen Nachteil (gegenüber Bitcoin), dass sie stets eine zentrale Instanz oder einen vertrauenswürdigen Dritten (eine TTP, in welcher Form auch immer) benötigten. Diese Zentralisierung war unumgänglich, da die Möglichkeit einer unbeschränkten Reproduktion der digitalen Wert-Verbriefungen bzw. Währungseinheiten bestand; stellten ihrerseits jedoch gleichzeitig stets das Risiko eines *Single Point of Failure*s in Bezug auf Verfügbarkeit und Vertrauen dar. Mit dem, in seinem Whitepaper vorgeschlagenen Konzept, löste Satoshi Nakamoto nun erstmalig dieses sog. „Double-Spendig-Problem“ (Problem einer möglichen, unzulässigen Mehrfachausgabe bzw. Kopie von Währungseinheiten bzw. Transaktionen in einem digitalen Transaktionssystem).

Besonderheit von Bitcoin im Vergleich zu bisherigen digitalen Währungen

Die Architektur von Bitcoin (und somit das Blockchain-Konzept) unterscheidet sich nun insbesondere aufgrund von 2 Aspekten von sämtlichen bis 2008 vorgestellten Ideen zu digitalen Währungen und dezentralen Transaktionssystemen:[112]

- aufgrund des **Ausmaßes der Dezentralität**- u.a. durch vollständige Auslagerung der Validierung von Transaktionen an gleichberechtigte Teilnehmer des zugrunde liegenden dezentralen Peer-2-Peer-Netzwerkes *(genauere Beschreibung, betreffend Aufbau und Eigenschaften des „Netzwerk-Fundaments“ von BCs, siehe Kapitel 2.3 „Internet und Peer-to-Peer-Netzwerke als Fundament – Die Blockchain Prinzipien“)*

- durch einen **sog. Mining-Algorithmus**. Dieser Algorithmus kann als Regelwerk verstanden werden, welcher u.a., den für die Teilhabe an der Abwicklung von Transaktionen im System nötigen (wirtschaftlichen) Aufwand regelt und durch ein implementiertes Anreizsystem die Absicherung, Synchronisierung und den wertbezogenen Fortbestand des dezentralen Transaktionssystems ermöglicht. *(Genauere Beschreibung des „Minings“ siehe Kapitel 2.5.8, „Konsensmechanismen“ Abschnitt „Prozess des Minings“)*

Zusammenfassend kann jedoch festgehalten werden: das Bitcoin-Konzept (und somit die erste funktionierende & implementierte Blockchain-Anwendung) beruht

[112] Sixt, *Bitcoins und andere dezentrale Transaktionssysteme*, 8.

auf den Entwicklungen und Ideen der Cypherpunks und auf der Ideologie des sog. „Krypto-Anarchismus“.[113]

(Wikipedia listet Bitcoin und weitere Kryptowährungen als Beispiel für Krypto-Anarchismus mit dem Ziel: das Währungs- und Vertrauens-Monopol der Banken zu untergraben“) [114]

2.1.5. Ein Pseudonym als Erfinder der Blockchain-Technologie?

Zumal sich diese Arbeit ab dem 4ten Kapitel mit kollaborativen Wertschöpfungsmodellen (im Rahmen des Paradigmas der Open Innovation) auf Basis der BC und damit auch mit Möglichkeiten zum Umgang mit intellektuellen Besitztümern, geistigem Eigentum und Patent-Rechten (Intellectual Property Rights, IPR) beschäftigt, bleibt im Rahmen einer, im Sinne dieser Arbeit stehenden, Beleuchtung der BC-Historie noch folgende Frage offen: „Wer *gilt nun als der (rechtmäßige) Erfinder der Blockchain-Technologie?“*

Nakamoto selbst, hat seine Mitarbeit an der Community-gestützten Weiterentwicklung des Bitcoin-Codes im Jahre 2011 beendet. Während die Identität der meisten Programmierer, die seit der Veröffentlichung des Whitepapers an der Programmierung und späteren Weiterentwicklung der Bitcoin-Software mitwirkten, heute mittlerweile bekannt ist, ist (sind) die Person(en), welche hinter dem Pseudonym Satoshi Nakamoto steht (stehen)und somit verantwortlich für die Erstellung des grundlegenden Konzepts (Whitepaper) ist (sind), bis heute unbekannt.

Eine Person, die sich diesbzgl. seit 2015 immer wieder ins Rampenlicht drängt und dadurch bereits mehrmals für Furore innerhalb der Gemeinschaft überzeugter Bitcoin und BC-Nutzer sorgte, ist ein australischer Geschäftsmann namens: Dave Craig Steven Wright.[115] *Auch wenn Wright vor kurzem einen Urheberrechtsanspruch beim US Copyright Office anmeldete (ev lediglich als geschickte Strategie um den Wert seines eignen Blockchain-Unternehmens zu steigern*[116]*), blieb er*

[113] Rosenberger, *Bitcoin und Blockchain*, 8.
[114] „Krypto-Anarchismus“.
[115] vgl. Rosenberger, *Bitcoin und Blockchain*, 26ff.
[116] vgl. Mirco Recksiek, „Bitcoin SV Kurs explodiert: Ist Craig Wright wirklich Satoshi Nakamoto? - Patent eingereicht“, *CryptoMonday* (blog), 21. Mai 2019, https://cryptomonday.de/bitcoin-sv-kurs-explodiert-ist-craig-wright-wirklich-satoshi-nakamoto-patent-eingereicht/.

konkrete Beweise bis dato schuldig und konnte seither lediglich mehrmals rechtskräftig der Dokumentenfälschung überführt werden.[117]

Auch wenn der Begriff „Blockchain“, im von Nakamoto veröffentlichten Whitepaper kein einziges-Mal auftaucht, wurde das heute als BC bekannte technologische Konzept erstmals mit der Veröffentlichung des Bitcoin-Transaktionssystems beschrieben und ist daher unbestritten auf dieses zurückzuführen.[118] Demzufolge gilt das Pseudonym Satoshi Nakamoto gemäß der überwiegenden Mehrheit aller, im Rahmen dieser Arbeit, recherchierten Quellen, und somit aus heutiger Sicht, als der Erfinder des hinter dem Bitcoin stehenden technischen Konzeptes und wird damit als Urheber der BC-Technologie angesehen. Zudem wurde der gesamte Quellcode der Bitcoin-Software lizenzfrei und somit komplett frei zugänglich entwickelt. Dieses, dem Open-Source[119]-Gedanken entsprechende und von Nakamoto gewählte, Vorgehen sollte von Anfang an einer Vielzahl von Personen uneingeschränkt die Möglichkeit bieten, das Protokoll weiterzuentwickeln oder basierend auf dem Bitcoin-Quellcode eigene/neue Abwandlungen (siehe hierzu u.a. nächstes *Kapitel 2.2* und *Kapitel 2.5.8 „Blockchain-Forks“*) bzw. weitere/neue BC-Anwendungen zu erstellen.

[117] vgl. Christoph Bergmann, „Pseudo-Satoshi Craig Wright wird auf 10 Milliarden Dollar verklagt“, *BitcoinBlog.de - das Blog für Bitcoin und andere virtuelle Währungen* (blog), 27. Februar 2018, https://bitcoinblog.de/2018/02/27/pseudo-satoshi-craig-wright-wird-auf-10-milliarden-dollar-verklagt/.

[118] vgl. Andreas Meier und Henrik Stormer, „Blockchain = Distributed Ledger + Consensus“, *HMD Praxis der Wirtschaftsinformatik* 55, Nr. 6 (1. Dezember 2018): 1139–54, https://doi.org/10.1365/s40702-018-00457-7.

[119] „Definition: Open Source“, Gabler Wirtschaftslexikon, zugegriffen 11. Juni 2019, https://wirtschaftslexikon.gabler.de/definition/open-source-43032/version-184927.