HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Herr
Richard Paul Schmidt

Potenzial von Smart Contracts als Blockchain-basierte Anwendungen in der Finanzwirtschaft

Mittweida, 2020

Fakultät Wirtschaftsingenieurwesen

BACHELORARBEIT

Potenzial von Smart Contracts als Blockchain-basierte Anwendungen in der Finanzwirtschaft

Autor:
Herr

Richard Paul Schmidt

Studiengang:
Betriebswirtschaftslehre

Seminargruppe:
BW17w4-B

Erstprüfer:
Prof. Dr. rer. oec. Johannes Stelling

Zweitprüfer:
Thomas Meier, M.A.

Einreichung:
Mittweida, 29.09.2020

Verteidigung/Bewertung:
Mittweida, 2020

Faculty Industrial Engineering

BACHELOR THESIS

Potential of smart contracts as blockchain-based applications in the financial undustry

author:
Mr.

Richard Paul Schmidt

course of studies:
Business Administration

seminar group:
BW17w4-B

first examiner:
Prof. Dr. rer. oec. Johannes Stelling

second examiner:
Thomas Meier, M.A.

submission:
Mittweida, 29.09.2020

defence/ evaluation:
Mittweida, 2020

Bibliografische Beschreibung:

Schmidt, Richard Paul:
Potenzial von Smart Contracts als Blockchain-basierte Anwendungen in der Finanzwirtschaft. - 2020. - 10, 45 S.
Mittweida, Hochschule Mittweida, Fakultät Wirtschaftsingenieurwesen, Bachelorarbeit, 2020

Referat:

Die vorliegende Bachelorarbeit hat die sogenannten Smart Contracts, welche als automatisierte Verträge verstanden werden können, zum Thema. Zunächst wird sich mit der Blockchain, welche eine Grundlage der Smart Contracts darstellt, auseinandergesetzt und darauf aufbauend werden die Smart Contracts genauer beleuchtet. Folgend werden ausgewählte Anwendungsszenarien für Smart Contracts in der Finanzwirtschaft vorgestellt. Abschließend werden Handlungsempfehlungen für den bestmöglichen Umgang mit der Blockchain und den Smart Contracts im Unternehmensumfeld dargestellt.

Inhaltsverzeichnis

Inhaltsverzeichnis I

Abbildungsverzeichnis III

Tabellenverzeichnis IV

Abkürzungsverzeichnis V

Einleitung 1

1 Die Grundlagen der Blockchain - Technologie 2

1.1 Die Distributed Ledger Technologie 2

1.2 Der Anwendungsbereich Blockchain 4

1.2.1 Ein Überblick über die Historie der Blockchain 5

1.2.2 Technologische Grundlagen der Blockchain Technologie 6

1.2.2.1 Die Ansätze der Private- und der Public-Blockchain 6

1.2.2.2 Die Hashfunktion 7

1.2.2.3 Merkle-Tree und Merkle-Proof 9

1.2.2.4 Digitale Signaturen 11

1.2.3 Wichtigste Merkmale und Eigenschaften der Blockchain 12

1.3 Aktueller Stand und Potenzial 14

2 Smart Contracts als Blockchain-basierte Anwendungen 17

2.1 Grundlagen von Smart Contracts 17

2.1.1 Begriffserklärungen und Funktionsweise 17

2.1.2 Technologische Grundlagen von Smart Contracts 18

2.1.3 Smart Contracts auf einer Blockchain 19

2.1.4 Oracles als Informationslieferanten der Umwelt 20

2.1.5 DApp als unabhängige Programme 20

2.1.6 DAOs als sich selbst steuernde Unternehmen 21

2.2 Charakteristika und Merkmale 21

2.2.1 Transparenz 21

2.2.2 Automatisierung 22

2.2.3 Anonymität 22

2.2.4 Beschränkung auf die Prüfung von „true/false“ Ereignissen 22

2.3 Chancen und Risiken von Smart Contracts 23

2.3.1 Nutzen von Smart Contracts ... 23
2.3.1.1 Eliminierung des Menschen als unberechenbare Fehlerquelle ... 23
2.3.1.2 Kostensenkungen ... 23
2.3.1.3 Zeiteinsparungen ... 24
2.3.1.4 Sicherheit ... 24
2.3.1.5 Erhöhung der Vertragssicherheit ... 24
2.3.2 Risiken und Herausforderungen ... 24
2.3.2.1 Programmierung ... 24
2.3.2.2 Skalierbarkeit ... 24
2.3.2.3 Rechtliche Herausforderungen ... 25
2.3.2.4 Standards ... 27
2.3.2.5 Änderung von Vertragsinhalten und Rückabwicklung ... 28
2.3.2.6 Technologische Ressourcen ... 28
2.4 Fazit und Potential ... 29

3 Einbindung von Smart Contracts in ausgewählten Bereichen der Finanzwirtschaft ... 30

3.1 Leasing und Mieten von Vermögensgegenständen ... 32
3.2 Effizienzerhöhung des Zahlungsverkehrs ... 33
3.3 Neue Wege der Unternehmensfinanzierung ... 34
3.4 Automatisierung der Inanspruchnahme von Versicherungsleistungen ... 35
3.5 Fairere Gestaltung des Rating-Prozesses ... 36

4 Handlungsempfehlungen ... 39

4.1 Allgemeine Handlungsempfehlungen ... 39
4.1.1 Anregungen und Förderungen für Projekte schaffen ... 39
4.1.2 Rechtliche Auslegung ... 40
4.1.3 Ausbildung von Experten ... 40
4.1.4 Bildung von Netzwerken und Kooperationsgemeinschaften ... 40
4.2 Stufenmodell zur Einbindung der Blockchain Technologie ... 41
4.3 Welcher Ansatz besitzt die bessere Eignung? Private vs. Public-Blockchain 42
4.3.1 Entscheidungskriterien ... 42

Schlussbetrachtung ... 44

Literaturverzeichnis ... 47

Selbstständigkeitserklärung

Abbildungsverzeichnis

Abbildung 1: Centralized Ledger 3

Abbildung 2: Distributed Ledger 4

Abbildung 3: Beispiel eines Merkle-Trees 9

Abbildung 4: Priorisierung in Unternehmen 14

Abbildung 5: Investitionsüberlegungen in Unternehmen ausgewählter Länder 15

Abbildung 6: Branchenübergreifender Vergleich von Anwendungen auf Blockchain-Basis 30

Abbildung 7:Umfrage an Unternehmen zum Voranbringen der Blockchain-Technologie . 39

Abbildung 8:Vorgehen bei der Einbindung der Blockchain-Technologie 41

Tabellenverzeichnis

Tabelle 1: Diffusionsprinzip 7

Tabelle 2: Unterschiedliche Input Länge 8

Abkürzungsverzeichnis

Bspw.	Beispielsweise
Bzw.	Beziehungsweise
DLT	Distributed Ledger Technologie
D.h.	Das heißt
DAO	Decentralized autonomous organization
DApp	Decentralized Application
EU	Europäische Union
ICO	Initial Coin Offering
SHA	Secure Hash Algorithmus
TPS	Transactions per second
US	United States
Usw.	Und so weiter
U.a.	Unter anderem
Z.B.	Zum Beispiel

Einleitung

Das Thema Smart Contracts ist für die meisten Personen, welche nicht gerade einen Exkurs über Digitalisierung und Automatisierung absolvierten, Neuland. Vielleicht haben Interessierte in Verbindung mit der Blockchain mal etwas über Smart Contracts gehört, doch reicht die Kenntnis meist nicht tiefer, als dass diese irgendetwas mit Verträgen zu tun haben könnten, hergeleitet allein über die Bezeichnung. Falsch ist dies nun in keinem Fall, doch ist das, was hinter Smart Contracts in Verbindung mit einer Blockchain steht, ungemein größer und so kratzt diese Aussage doch eher nur an der Oberfläche der Thematik.

Was Smart Contracts insbesondere im Einsatzfeld der Finanzwirtschaft zu leisten vermögen, und wo sie an ihre Grenzen stoßen, sind Fragen, zu deren Beantwortung diese Bachelorarbeit eine Hilfestellung geben soll. Dazu befassen wir uns anfangs mit der Grundlage von Smart Contracts: der Blockchain. Was steckt dahinter und wie funktioniert diese? Welche Eigenschaften sind besonders für die Smart Contracts von hoher Relevanz und was könnte die Zukunft bringen?

Darauf aufbauend blicken wir genauer auf Smart Contracts und deren Funktionsweise sowie die prägenden Merkmale und Eigenschaften, aufgrund derer den Smart Contracts so ein ungemeines Potenzial zugesprochen wird. Doch kommt nicht jede neue Technologie ohne Herausforderungen aus, welche bewältigt werden müssen, bevor das komplette Potenzial ausgemacht und genutzt werden kann. Diese Herausforderungen werden genauer beleuchtet und es wird aufgezeigt, wie diese bewältigt können.

Anschließend werden fünf Einsatzmöglichkeiten von Smart Contracts im Bereich der Finanzwirtschaft vorgestellt, welche in der Theorie und Praxis als erfolgreich erachtet werden. Manche sind in einer frühen Planungsphase, manche werden getestet und manche werden tagtäglich eingesetzt.

Abschließend zum Thema Smart Contracts werden noch ein paar Handlungsempfehlungen für den Umgang mit der Blockchain und den Smart Contracts vorgestellt, durch welche sich Unternehmen und staatliche Institutionen einen Vorteil im nationalen und internationalen Wettbewerb schaffen könnten.

1 Die Grundlagen der Blockchain - Technologie

In diesem Kapitel verschaffen wir uns einen kleinen Überblick über die Grundlagen der Blockchain Technologie. Dies umfasst neben den technologischen Grundlagen und den wichtigsten Merkmalen und Eigenschaften sowie eine Beschreibung der Funktionsweise, eine kurze Erläuterung der historischen Entwicklung und einen Überblick über den aktuellen Stand. Abschließend beschäftigen wir uns noch mit dem Potential und den Zukunftsaussichten.

1.1 Die Distributed Ledger Technologie

Eine Distributed Ledger Technologie, kurz DLT, zu denen die Blockchain als der wohl bekannteste Vertreter gehört, heißt übersetzt *Technik verteilter Kassenbücher*[1]. Dies bedeutet, dass Transaktionen in einem dezentralisierten Netzwerk, bestehend aus vielen, voneinander unabhängigen Rechnern, gespeichert werden[2]. Somit entfällt, im Gegensatz zum aktuellen Standard, in der Regel eine zentrale Instanz oder ein zentraler Knotenpunkt, welcher als einziger eine Lese- und Schreibberechtigung besitzt, durch welchen jede Transaktion laufen muss und welcher als einziger über ein vollständiges Register der Transaktionen verfügt[3], wie in Abbildung 1 zu sehen ist. Infolgedessen agiert jeder einzelne Rechner oder Transaktionsteilnehmer als Knotenpunkt, von welchem die Transaktion bestätigt werden muss, bevor sie als gültig angesehen werden kann.

[1] Vgl. Burgwinkel 2016, S. 9.

[2] Vgl. Brühl 2017a, S. 140.

[3] Vgl. Priem 2020, S. 7–10.

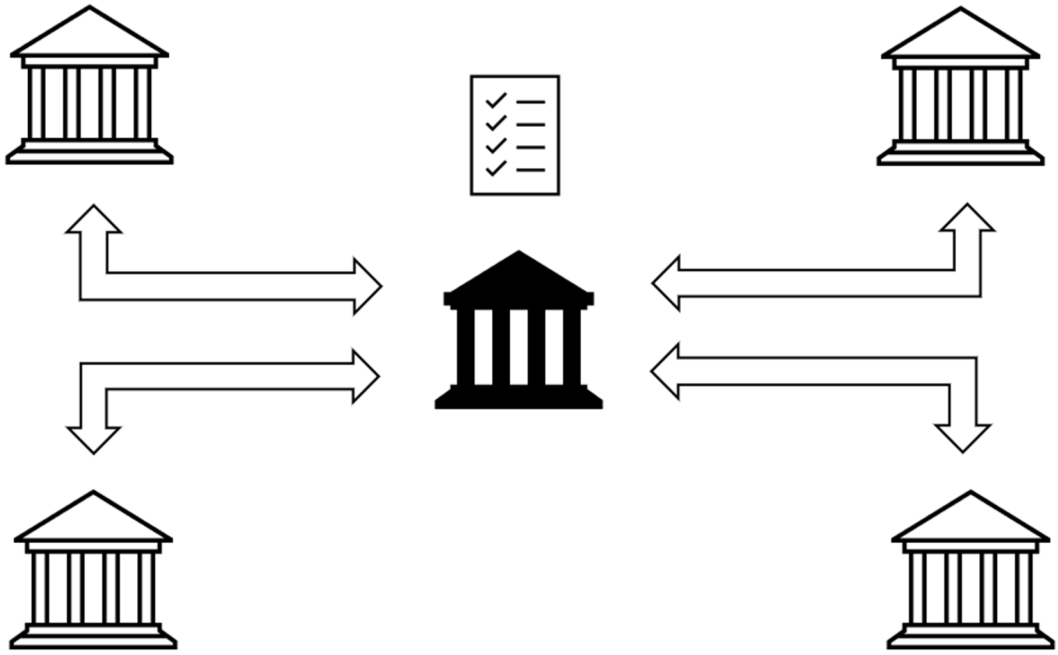

Abbildung 1: Centralized Ledger[4]

So wird das Kontenbuch, welches Transaktionsregister genannt wird, nicht nur auf einem Rechner oder Server gespeichert, wie es zumeist der Fall ist, sondern auf jedem Rechner innerhalb des Netzwerkes. Folglich bekommt jeder Netzwerkteilnehmer eine immer aktuelle Kopie des Registers, wie in Abbildung 2 zu sehen ist. Ebenso müssen neue Transaktionen vom gesamten Netzwerk bestätigt bzw. validiert werden. Zudem können die Daten, Informationen und Transaktionen immer als richtig angesehen werden, da sie a) unveränderlich sind und b) von allen auf ihre Richtigkeit überprüft wurden[5].

[4] Eigene Darstellung in Anlehnung an Priem 2020, S. 7–10.

[5] Vgl. Urban 2020, S. 15–17.

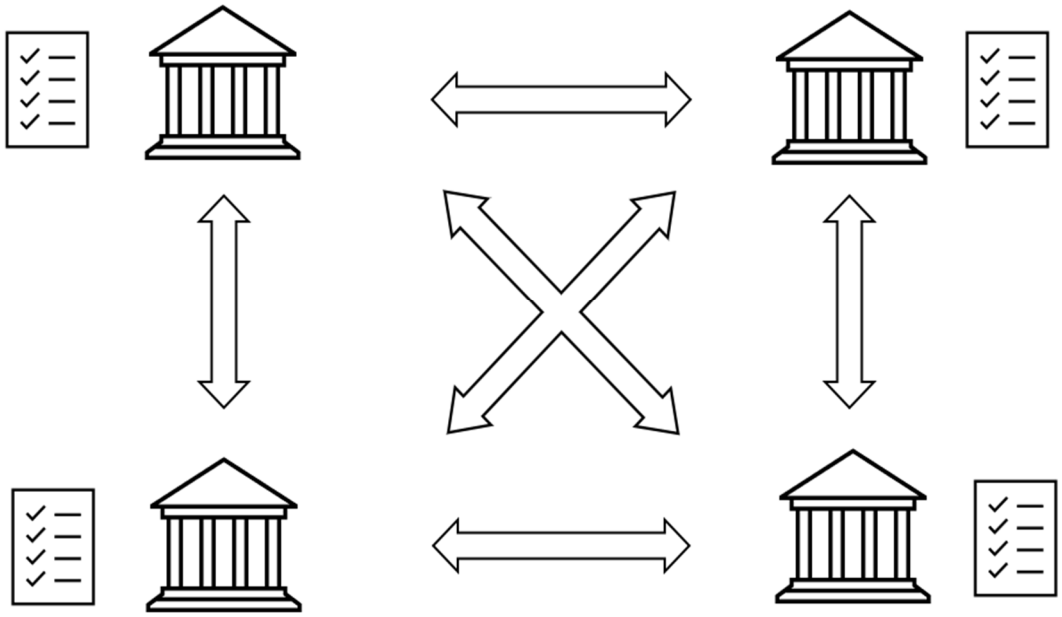

Abbildung 2: Distributed Ledger[6]

1.2 Der Anwendungsbereich Blockchain

Die mit Abstand bekannteste Anwendungsform, hinter welcher eine Form der DLT steht, stellt die Blockchain dar. Deswegen steht in dieser Arbeit Blockchain synonym für die DLT. Der Allgemeinheit wurde sie durch die Kryptowährung Bitcoin bekannt, deren Transaktionen in einer Blockchain gespeichert werden.

In einer Blockchain werden die einzelnen Datensätze (u.a. Transaktionen) in namensgebenden Blöcken zusammengefasst, welche eine hohe Anzahl von Transaktionen enthalten können. Diese Blöcke, einmal abgeschlossen, werden kryptografisch sequenziell miteinander verkettet, um eine zeitlich einheitliche Darstellung sowie die Datenintegrität sicherzustellen. Wurden neue Transaktionen zu einem neuen Block zusammengefasst, wird dieser Block abgeschlossen und an die bestehende Kette angehängt[7].

[6] Eigene Darstellung in Anlehnung an Priem 2020, S. 10–14.

[7] Vgl. Burgwinkel 2016, S. 6

1.2.1 Ein Überblick über die Historie der Blockchain

Etwa 40 Jahre Forschung und Entwicklung haben zu dem geführt, was wir heute unter einer Blockchain verstehen. 1979 hatte sich Ralph C. Merkle das Prinzip der Hash-Trees, inzwischen besser bekannt als Merkle-Trees, patentieren lassen[8]. Diese sind unter anderem für die Authentifizierung einer Nachricht oder Transaktion in der Blockchain verantwortlich. Aber dazu mehr in Kapitel 1.2.2.3 . Mehr als 10 Jahre später, genauer gesagt im Jahr 1991, publizierten Stuart Haber und W. Scott Stornetta einen wissenschaftlichen Artikel zum Thema „linked timestamping“. Damit ist das Versehen von Dokumenten mit einem Zeitstempel, sowie das Verketten dieser gemeint[9]. 1997 wurde dann von Nick Szabo eine Schrift publiziert, welche sich erstmals mit „Smart Contracts“ und deren Einsatzmöglichkeiten im E-Commerce beschäftigte. Er wollte damit Möglichkeiten aufzeigen, wie Vertragsprozesse durch Unterstützung des Internets verbessert werden können[10]. Im Jahr 2007 wurde in Estland die erste in eine Anwendung implementierte Blockchain als kommerzielles System in Betrieb genommen. Dabei handelte es sich um ein Software-Sicherheitsunternehmen, welches ein digitales Signatursystem entwickelte[11].

Das Ereignis, welchem die wohl vorerst größte Aufmerksamkeit im Bereich der Blockchain zuteilwurde, war das Veröffentlichen des White Papers „Bitcoin: A Peer-to-Peer Electronic Cash System”. In dem 2009 von dem Pseudonym “Satoshi Nakamoto” veröffentlichten Artikel wird die Funktionsweise des auf einer Blockchain basierenden Bitcoin Systems beschrieben, welches die erste öffentlich nutzbare Kryptowährung darstellte[12]. Dann war es ein paar Jahre ruhig, bis 2013 das Projekt „Ethereum“ gegründet wurde. Dabei handelt es sich um eine Plattform für Blockchain-Anwendungen, die weltweit und für jeden zugänglich ist[13]. 2015 wurde dann schließlich von Linux das Hyperleger Projekt gegründet, welches ein Dachprojekt für das Entwickeln einer „Open-Source“ Blockchain ist und bei welchem namenhafte Partner wie IBM, SAP oder Intel mitwirken[14]. Im selben Jahr erweiterten Microsoft und IBM ihr jeweiliges Angebot im Bereich der Clouddienste um Blockchain Anwendungen[15]. 2016 feierte eine auf einer Blockchain basierende Anwendung im Bereich des Zahlungsverkehrs ihre Weltpremiere. Die Deutsche ReiseBank AG schickte eine Überweisung

[8] Vgl. Merkle 1979.

[9] Vgl. Haber und Stornetta 1991, S. 99–111

[10] Vgl. Szabo 1997.

[11] Vgl. Burgwinkel 2016, S. 12

[12] Vgl. Nakamoto 2008.

[13] Vgl. Antonopoulos und Wood, S. 3.

[14] Vgl. The Linux Foundation 2015.

[15] Vgl. Redman 2016.

von Frankfurt am Main an die im kanadischen Calgary ansässige Bank ATB Financial[16]. Der Betrag von 1.000 kanadischen Dollar war innerhalb von 8 Sekunden auf dem Konto des Empfängers gutgeschrieben, sodass er es abheben konnte. Im noch nach wie vor gängigen SWIFT-Verfahren hätte die Überweisung mehrere Tage gedauert. Dies geschah auf Grundlage der weiterentwickelten Ripple-Blockchain, welche ein speziell für die aktuellen Währungen entwickeltes Zahlungsnetzwerk ist.

1.2.2 Technologische Grundlagen der Blockchain Technologie

1.2.2.1 Die Ansätze der Private- und der Public-Blockchain

Grundlegend kann zwischen zwei verschiedenen Arten von Blockchains differenziert werden. Zum einen gibt es die Public-Blockchains, welche sich dadurch auszeichnen, dass jeder, der ein internetfähiges Gerät besitzt, in dem Netzwerk lesen, schreiben oder daran teilnehmen kann und es keine zentrale Instanz gibt, die dieses verwaltet[17]. Das prominenteste Beispiel dafür ist die Blockchain der Kryptowährung Bitcoin.

Auf der anderen Seite haben wir die sogenannten Private-Blockchains, welche von einer Institution, einer Regierung oder einem Unternehmen aufgesetzt und betrieben werden. Daran teilnehmen kann nur, wer eingeladen wurde und eine Genehmigung für das Lesen oder Schreiben erhalten hat[18]. Ein Beispiel hierfür ist das Businessnetzwerk des Konsortium R3, welches in Kapitel 1.2.4. noch eingehender beschrieben wird.

In einem Netzwerk mit Private-Blockchain Ansatz ist durch die begrenzte Anzahl von Knotenpunkten, durch welche die Transaktionen laufen und auf ihre Integrität geprüft werden, die Leistungsfähigkeit höher als in einer Public-Blockchain. Das Ripple Netzwerk zum Beispiel, welches eine Softwareanwendung für Transaktionen darstellt, hat im Vergleich zu „klassischen Blockchains“ eine viel höhere Skalierbarkeit[19].

Im engeren Sinne erfüllen Private-Blockchains nicht die Idee der Dezentralität einer Blockchain und werden von manchen daher kritisch beurteilt, und zumeist nur als weiterentwickelte Datenbanken mit Distributed Ledger Technologie angesehen.

---

[16] Vgl. Boberach 2016.

[17] Vgl. Burgwinkel 2016, S. 48.

[18] Vgl. Burgwinkel 2016, S. 57.

[19] Vgl. Ripple 2020.

1.2.2.2 Die Hashfunktion

Eine in der Blockchain verwendete technologische Funktionsweise ist die Hashfunktion. Dabei handelt es sich um eine kryptografische Verschlüsselungsmethode, welche die Integrität der Informationen in der Blockchain sicherstellen soll.

Dazu wird ein sogenannter Hashwert erzeugt. Dieser ist eine Zahlen-Buchstaben-Kombination von fixer Länge, welche die Abbildung beispielsweise eines Textdokumentes ist und aus einer beliebig großen Menge an Eingabedaten besteht. Dieser ganze Vorgang geschieht mit geringem Aufwand an Rechenleistung und ist sehr effizient. Dabei werden bestimmten Eingabedaten bestimmte Zahlen- und Buchstabenfolgen zugeordnet, welche sich verändern, wenn die Eingabedaten geringfügig verändert werden, wie in Tabelle 1 zu sehen ist. Das wird als Diffusionsprinzip bezeichnet[20]. Durch den Vergleich der erzeugten Hashwerte kann schnell erkannt werden, ob etwas an den Eingabedaten verändert wurde oder eine Manipulation stattgefunden hat. Stimmen sie nicht überein, wurden die Eingabe- oder Ursprungsdaten verändert.

Input – Datenmenge	**Output – Hashwert**
Smart Contracts!	2a422d9e619190843de323241797eebd72f29a295b0362e7d6d8ff8511f93df4
Smart Contracts?	9bf368832ecd323261be637d06c89b9fd623943d124533286e7a6f5e2abcd328

Tabelle 1: Diffusionsprinzip[21]

Im Folgenden gehen wir auf drei der wichtigsten Eigenschaften der Hashfunktionen ein.

- **Kompressionseigenschaft**

Eine Hashfunktion ist eine Kompressionsfunktion. Das bedeutet im Fall der Blockchain, dass sie beliebig lange Eingabedaten in eine Zeichenkette mit einer festen Länge umrechnet; dies ist in unserem Fall der Hashwert[22].
Dies wird in Tabelle 2 verdeutlicht.

[20] Vgl. Beutelspacher et al. 2010, S. 71.

[21] Eigene Darstellung auf Grundlage des errechneten Hashwertes von SHA-256 hash calculator | Xorbin 2020.

[22] Vgl. Beutelspacher et al. 2010, S. 176.

- **Einwegfunktion**

Im Idealfall ist eine in der Blockchain verwendete Hashfunktion eine Einwegfunktion. Das heißt, dass es so gut wie unmöglich ist, die Eingabedaten (Input) zu finden, wenn als Grundlage nur der Hashwert (Output) vorhanden ist[23].

- **Kollisionsresistenz**

Eine starke Kollisionsresistenz im Kontext der Hashfunktion einer Blockchain ist dann gegeben, wenn es nahezu unmöglich ist, zwei verschiedene Eingabedaten zu finden, welche den gleichen Hashwert besitzen[24].
Im Gegensatz zu einer starken Kollisionsresistenz gibt es des Weiteren eine schwache Kollisionsresistenz, welche aber in dieser Arbeit nicht von Relevanz ist.

Die Technologie, die hinter der Erzeugung des Hashwertes steckt, nennt sich SHA-256 (Secure Hash Algorithmus) und erzeugt für beliebige Eingabedaten einen 64 Zeichen langen hexadezimalen Hashwert[25]. Die Anzahl der erzeugten Zeichen ist unabhängig von der Menge der Eingabedaten. Wie in Tabelle 2 zu sehen ist, sind die Eingabetexte unterschiedlich lang, der SHA-256 wandelt diese aber in Hashwerte der gleichen Länge um.

Input – Datenmenge	**Output – Hashwert**
Smart Contracts	7b1f6bccca57ba5ede73be50e1daf87a099d1031181f721f9637661fa679f6af
Potential von Smart Contracts als Blockchain-basierte Anwendungen in der Finanzwirtschaft	9832b0d2cc9e592c008fb76b1bd204f7a2dfa23fdd0d82a957cca49c216e455a

Tabelle 2: Unterschiedliche Input Länge[26]

[23] Vgl. Wenzel-Benner und Dr.-Ing. Wasserrab 2015

[24] Vgl. Beutelspacher et al. 2010, S. 110.

[25] Vgl. Brühl 2017b, S. 372.

[26] Eigene Darstellung auf Grundlage des errechneten Hashwertes von SHA-256 hash calculator | Xorbin 2020.

1.2.2.3 Merkle-Tree und Merkle-Proof

Eine weitere technologische Grundfunktion der Blockchain, die die Datenintegrität gewährleistet, ist die des Merkle-Trees oder Merkle-Proof, nach dem Erfinder Ralph Merkle benannt.

Grundsätzlich ist ein Merkle-Tree oder Hash-Tree, eine Datenstruktur, in welcher Informationen und Datensätze zusammengefasst und in einem erzeugten Hash dargestellt werden.

Durch diesen lässt sich auf einfache und effiziente Art und Weise feststellen, ob Daten innerhalb einer Blockchain geändert oder manipuliert wurden. Er stellt also einen zentralen Bestandteil der Blockchain zur Überprüfung der Gültigkeit und schnellen Lokalisierung von Transaktionen dar [27].

- **Aufbau und Entstehung**

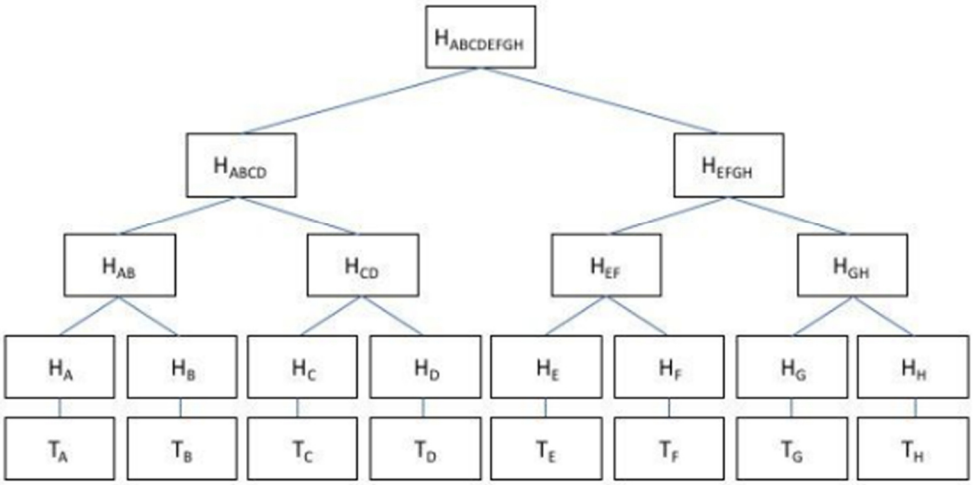

Abbildung 3: Beispiel eines Merkle-Trees[28]

Der Aufbau eines Merkle-Trees lässt sich am besten anhand einer Grafik erklären. In Abbildung 3 ist ein Merkle-Tree abgebildet. Am unteren Ende des Merkle-Trees befinden sich einzelne Transaktionen oder Datensätze, welche hier mit T_A-T_H markiert sind. Jedem dieser Datensätze wurde durch die Verschlüsselung mit dem Hash-Verfahren ein spezifischer Hashwert zugeordnet, hier mit H_A-H_H bezeichnet. Im Folgenden werden zwei der erzeugten spezifischen Hashwerte aneinandergehängt und als Input der Hashfunktion verwendet,

[27] Vgl. Urban 2020, S. 21.

[28] Vgl. Choudhary 2020.

welche dann als Output einen neuen Hashwert bilden, hier mit H_{AB}, H_{CD}, H_{EF} und H_{GH} markiert. Von diesen vier neuen Hashwerten werden ebenfalls wieder zwei zu einem neuen Hashwert zusammengefasst, in diesem Fall zu H_{ABCD} und H_{EFGH}. Und um den Merkle-Tree zu vervollständigen, werden die beiden noch übrigen Hashwerte zu einem zusammengeführt, dem sogenannten Wurzel-Hash oder Merkle-Root, im Beispiel mit $H_{ABCDEFGH}$ bezeichnet. So erhalten wir einen vereinfacht dargestellten Merkle-Tree[29].

- **Funktionsweise**

Durch das Erzeugen des oben genannten Wurzelhash besteht die Möglichkeit, alle darin zusammengefassten Daten auf ihre Integrität zu überprüfen. Würden Anwender z.B. nur eine kleine Änderung im Datensatz T_E vornehmen, würde sich nicht nur der jeweilige Hash des einzelnen Datensatzes ändern, sondern der des gesamten Pfades, vom Datensatz bis zum Merkle-Root-Wert. Am Beispiel aufgezeigt wären das H_E, H_{EF}, H_{EFGH} und $H_{ABCDEFGH}$. Nun müssten bei einer Überprüfung nicht alle Dokumente bzw. Transaktionen auf der untersten Ebene einzeln überprüfen, um festzustellen, ob es eine Änderung gibt oder nicht, sondern nur den Wurzelhash. Falls es eine Änderung gibt, muss anschließend nur der jeweilige Pfad bis zu dem Datensatz, in welchem die Änderung stattgefunden hat, überprüft werden[30].

Mithilfe der Eigenschaften des Merkle-Trees kann sich zudem vergewissert werden, ob bestimmte Datensätze in der beschriebenen Datenstruktur enthalten sind, ohne deren Inhalt zu kennen, was in Anbetracht des sich ausweitenden Datenschutzes von großer Bedeutung ist. Dazu müssen nur die Hashwerte des Merkle-Trees bekannt sein, welche keine Rückschlüsse auf den Inhalt geben. Zur Überprüfung eines Dokumentes müsste beispielsweise nur dessen Hashwert gebildet und die unterste Ebene des vorgegebenen Merkle-Trees auf die Existenz dieses Hashwertes kontrolliert werden. Ein Nutzer kann noch weitergehen und aus dem eben generierten Hashwert und dem Hashwert des Nachbardokumentes den gemeinsamen Hashwert erzeugen und mit demjenigen vergleichen, der schon in der Datenstruktur enthalten ist. Dies kann bis zum Merkle-Root oder zur Hashwurzel fortgeführt werden. Stimmen alle Hashwerte überein, ist zweifelsfrei bewiesen, dass das Dokument Teil des Merkle-Trees ist. Diese Art der Überprüfung wird als Merkle-Proof oder Zero-Knowledge Proof bezeichnet, da bei der Beweisführung kein Wissen über die Inhalte der Dokumente vorhanden sein muss, sondern nur der Datensatz des zu überprüfenden Dokumentes[31].

[29] Vgl. Merkle 1987, S. 369–378.

[30] Vgl. Merkle 1987, S. 369–378.

[31] Vgl. Merkle 1987, S. 369–378.

Im Fall des Anwendungsszenarios von einer Blockchain-Technologie in der Finanzwirtschaft ist diese Art von Datenstrukturen sehr vorteilhaft, da z.B. Finanztransaktionen, welche in der Blockchain enthalten sind, schnell und einfach auf ihr Vorhandensein sowie ihre Authentizität überprüft werden können.

1.2.2.4 Digitale Signaturen

Das letzte Thema im Bereich der technologischen Grundlagen, auf welches ich eingehen möchte, behandelt die Digitalen Signaturen und wie sie im Zeitalter der Digitalisierung, unabhängig von einer Blockchain, essenziell geworden sind.

- **Grundlagen und Eigenschaften**

Mechanismen wie digitale Signaturen werden in Zukunft eine immer größere Bedeutung bekommen, denn je digitaler die Wirtschaft und die Gesellschaft wird, umso mehr werden Verträge und Vertragsabschlüsse in die digitale Welt verlagert. Dies erfordert folglich stärkere Sicherheitsvorkehrungen und Vorschriften zur Abwicklung solcher. Ebenfalls in Hinsicht auf elektronische Transaktionen, die meist über Distanzen getätigt werden, welche eine herkömmliche Verifizierung unmöglich machen, sind digitale Signaturen zum Vertrauensaufbau unumgänglich, um z.B. dem Geschäftspartner garantieren zu können, dass man die Person ist, für welche sich ausgegeben wird. Zudem sind sie dann von besonderer Bedeutung, wenn es darum geht, die Integrität von elektronischen Verträgen zu gewährleisten.

Die grundlegende Anforderung an eine digitale Signatur ist die Fälschungssicherheit. Es darf niemandem, außer dem Berechtigten, möglich sein, diese Art „Unterschrift“ zu leisten. Quasi wie die eigenhändige Unterschrift, die im Normalfall niemand auf genau die gleiche Weise duplizieren kann. Zudem muss diese „Unterschrift“ von jedem Teilnehmer auf ihre Echtheit überprüfbar sein und die Person, die die Unterschrift geleistet hat, darf nicht leugnen können, dass es ihre Unterschrift ist. Eine Signatur ist immer an ein bestimmtes Dokument gebunden und ist nur für dieses gültig.

Daraus ergeben sich drei grundlegende Eigenschaften[32]:

- Nachweis zur Echtheit der Nachricht
- Eindeutigkeit der geleisteten Unterschrift
- Manipulationssicherheit der Nachricht

[32] Vgl. Badev und Chen 2014, S. 8.

- **Funktionsweise**

Bei einer digitalen Signatur wird ein Verfahren der asymmetrischen Kryptografie, die Public-Key-Verschlüsselung, verwendet. Dabei besteht der Schlüssel aus zwei Teilen, welche nicht miteinander identisch sind, einem zum Unterschreiben und einem zum Prüfen. Dadurch kann mit einem digitalen Verifikationsschlüssel eine Unterschrift dem Schlüssel einer Person zweifelsfrei zugeordnet und deren Identität bestätigt werden[33].

Im Zuge der Public-Key-Verschlüsselung wird ein Schlüsselset, bestehend aus Public- und Private-Key erstellt[34]. Dabei wird aus dem Private-Key heraus der Public-Key erzeugt. So kann aus dem Privat-Key heraus auf den Public-Key geschlossen werden. Damit aber alle Anforderungen an die Sicherheit gegeben sind, darf der Private-Key vom Public-Key aus nicht identifizierbar sein. Der erzeugte Private-Key wird dann zum einmaligen Signieren des Dokumentes verwendet und der Public-Key wird dann an alle Teilnehmer, die die Echtheit verifizieren müssen, weitergegeben.

Hat ein Sender nun ein Dokument, welches digital signiert werden muss, erzeugt dieser ein nur für dieses Dokument passendes Schlüsselpaar, bestehend aus Private-Key und Public-Key. Mit dem Private-Key, welchen der Sender geheim hält, verschlüsselt er das Original des Dokumentes und versendet dies mit dem Public-Key an den Empfänger. Im Bitcoin Netzwerk wird bspw. der Public-Key veröffentlicht, sodass theoretisch alle Netzwerkteilnehmer das Dokument auf dessen Echtheit überprüfen können. Die Beteiligten prüfen nun die Authentizität der Nachricht mithilfe der sogenannten Verifizierungsfunktion[35]. Dazu werden die Nachricht und der Public-Key als Eingabewerte herangezogen und die möglichen Antworten "Annahme" oder "Ablehnung" erscheinen als binärer Output.

1.2.3 Wichtigste Merkmale und Eigenschaften der Blockchain

Im Folgenden verschaffen wir uns einen kleinen Überblick über die Eigenschaften und Merkmale der Blockchain-Technologie, welche sie auszeichnen und dafür sorgen, dass es so viele Einsatzmöglichkeiten und Interessengruppen gibt, die an einer Umsetzung interessiert sind.

- **Dezentralität**

Da in einer Blockchain, insbesondere bei dem Ansatz der Public-Blockchain, alle Netzwerkteilnehmer in ihrer Funktion gleichberechtigt sind, entfällt eine zentrale Kontrollinstanz. Weiterhin haben die Teilnehmer die Möglichkeit, das Netzwerk jederzeit zu verlassen oder ihm

---

[33] Vgl. Schacht und Lanquillon 2020, S. 10.

[34] Vgl. Fill und Meier 2020, S. 9.

[35] Vgl. Fill und Meier 2020, S. 10.

beizutreten. Diese Eigenschaften bewirken, dass es so gut wie unmöglich wird, dass das Netzwerk der Kontrolle einer einzigen Instanz unterliegt[36]. Zudem ist es sehr unwahrscheinlich, dass ein Netzwerk dieser Art einer politischen oder organisatorischen Kontrolle unterworfen werden würde, da es über Landes-, Unternehmens- und Organisationsgrenzen hinaus agiert. Eine Ausnahme bilden Private-Blockchains von Unternehmen oder Regierungen, welche ggf. einer partiellen Regulierung bedürfen könnten.

- **Belastbarkeit**

Durch die in der Regel hohe und steigende Anzahl an Teilnehmern und Knotenpunkten innerhalb eines Blockchain-Netzwerkes wird die Wahrscheinlichkeit eines Ausfalles auf ein Minimum begrenzt und die Belastbarkeit bzw. Ausfallsicherheit immer weiter erhöht.

- **Transparenz**

Begründet durch die oben genannte Eigenschaft der Dezentralität sind die Daten der Blockchain für jeden Netzwerkteilnehmer von überall einsehbar[37], wobei die Daten natürlich in verschlüsselter Form vorliegen. So kann jeder, der an einer bestimmten Transaktion beteiligt war und daher über den entsprechenden, zu der Transaktion passenden kryptografischen Schlüssel verfügt, die Einzelheiten der Transaktion nachvollziehen.

- **Unveränderlichkeit**

Die Datensätze, die von allen Teilnehmern verifiziert wurden sind „by design“ nicht im Nachhinein veränderbar, sondern nur einsehbar. „By design“ bedeutet hier, dass es sich dabei um eine programmtechnische Grundeigenschaft jeder Blockchain handelt. So sind die Informationen auf der Blockchain vor nachträglicher Manipulation geschützt[38].

[36] Vgl. Voshmgir 2016.

[37] Vgl. Voshmgir 2016.

[38] Vgl. Fill und Meier 2020, S. 73.

1.3 Aktueller Stand und Potenzial

Obwohl die Technologie der Blockchain noch mehr oder weniger in den Kinderschuhen steckt, erfährt sie eine rasante Entwicklung. Mehr und mehr Unternehmen, in unserem Interessengebiet in erster Linie welche aus der Finanzindustrie, machen sich die vielen positiven Eigenschaften zunutze und arbeiten an einer Einbindung in ihre Geschäftsprozesse. Indes gewinnt die Forschung stetig neue Erkenntnisse und findet vielfältige weitere Einsatzgebiete für Blockchain Anwendungen. In der Folge drängt immer mehr Investitionskapital auf den Markt.

Werden die Zahlen der aktuellen Blockchain Survey von Deloitte betrachtet, wird schnell ersichtlich, dass der Großteil der Befragten das Potential der Blockchain erkannt hat. Allein der Vergleich der Studien von 2018 und 2019 zeigt auf, welch rapide Entwicklung aktuell im Bewusstsein der jeweiligen Entscheider stattfindet, wie in Abbildung 4 zu sehen ist. Innerhalb eines Jahres hat sich die Einschätzung der Relevanz der Blockchain-Technologie deutlich verändert. Bemerkenswert ist insbesondere der Anstieg der Anzahl an Personen, die die Blockchain ganz oben in den Strategieprioritäten ihres Unternehmens ansiedeln, von 43% auf 53%.

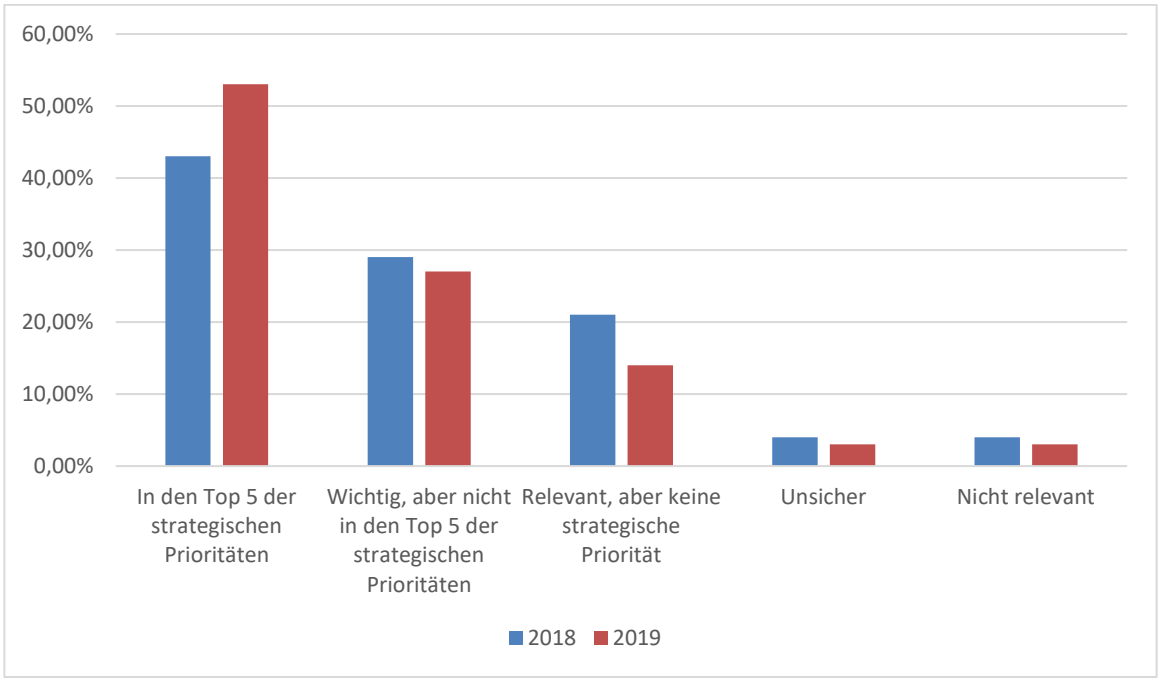

Abbildung 4: Priorisierung in Unternehmen[39]

Der Blick auf die geplanten Investitionen im Bereich der Blockchain-Technologie, zu sehen in Abbildung 5, zeigt auf, welche Bedeutung dem Thema inzwischen beigemessen wird. Erwähnenswert ist besonders die Menge der geplanten Investitionen in Luxemburg, welche

[39] Vgl. Pawczuk et al. 2018.

in erster Linie mit der Stärke der dortigen Finanzwirtschaft zusammenhängt und daher ein hohes Potential für Blockchain Einbindungen besitzt.

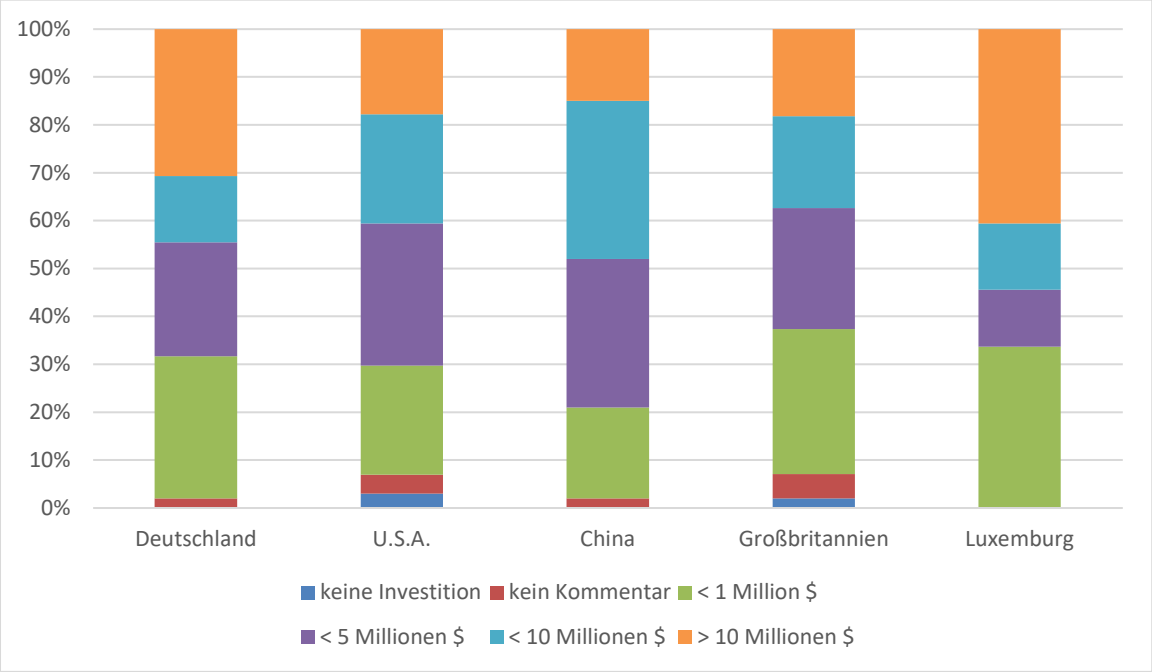

Abbildung 5: Investitionsüberlegungen in Unternehmen ausgewählter Länder in US-Dollar[40]

Ein Beispiel für das steigende Interesse ist das Konsortium R3, welches sich mit Anwendungen im Bereich der Blockchain beschäftigt und diese unter anderem auf Amazons Web Service Plattform veröffentlicht[41]. Im Jahr 2014 hatte es drei Banken als Gründungsmitglieder, bis 2016 stieg die Anzahl schon auf 50 Banken. Inzwischen haben sich mehrere hundert Unternehmen daran beteiligt und bilden ein starkes und innovatives Netzwerk[42]. Ebenso sind Zentralbanken und verschiedene staatliche Institutionen an Projekten der R3 beteiligt und nutzen diese[43].

Natürlich gibt es für eine flächendeckende Einbindung der Technologie noch einige Hürden, angefangen bei regulatorischen Hindernissen im Bereich der Gesetzgebung, über technische Erfordernisse bei der Implementierung in die jeweilige IT-Infrastruktur, bis hin zur Abstimmung der Eigenschaften der Blockchain-Anwendungen auf die Anforderungen der jeweiligen Einsatzgebiete. Doch es werden erkennbar mehr und mehr Anstrengungen

[40] Vgl. Pawczuk et al. 2018.

[41] Vgl. Burgwinkel 2016, S. 12

[42] Vgl. R3 2020.

[43] Vgl. Alun 2020.

unternommen, um diese Problemstellungen abzubauen und die Technologie für den breiten Einsatz zu optimieren.

2 Smart Contracts als Blockchain-basierte Anwendungen

Im zweiten Kapitel dieser Arbeit wird das beleuchtet, was unter Smart Contracts, zu Deutsch „intelligente Verträge“, zu verstehen ist. Dazu werden anfangs einige grundlegende Definitionen und Begrifflichkeiten erläutert. Darauffolgend wird die Funktionsweise von Smart Contracts und deren technologischen Grundlagen thematisiert. Aufbauend darauf werden die Chancen aufgezeigt, welche Smart Contracts bieten können und welche Herausforderungen zu bewältigen sind.

2.1 Grundlagen von Smart Contracts

2.1.1 Begriffserklärungen und Funktionsweise

Wenn heutzutage Diskussionen über Thematiken wie Distributed Ledger oder Blockchain geführt werden, lässt das Schlagwort „Smart Contract“ meist nicht lange auf sich warten. Obwohl diese Begriffe zumeist erst seit dem digitalen Wandel Einzug in den Sprachgebrauch erhalten haben, ist das grundlegende System, auf welchem Smart Contracts beruhen, wesentlich älter als das Prinzip der Blockchain.

Vereinfacht gesagt sind Smart Contracts nicht wie der Name sagt „intelligente Verträge“, sondern eine Computerroutine, welche in Form von festgesetzten, automatisierten Handlungsanweisungen auf einer Blockchain aufgesetzt wurden. Nach dem Implementieren des Algorithmus, welcher je nach Anwendungsfall geschrieben wird, können sie vollkommen autonom agieren und die Vertragsbestandteile kontrollieren und ausführen. In einer einfacheren Form gibt es diese Idee schon länger und die meisten werden sicher schon mit ihr interagiert haben. Beispielhaft hierfür ist das Prinzip von Getränkeautomaten. Möchte ein Kunde ein Getränk erhalten, muss dieser eine fixe Bedingung erfüllen, nämlich eine bestimmte Summe Geld einwerfen. Wird dies nicht getan, weil es sich um zu wenig oder gar kein Geld handelt, erhält dieser folglich keine Gegenleistung. Dieser Prozess wird von dem Automaten vollkommen autonom überwacht. Ein Vertrag kommt also nur zustande, wenn alle Bedingungen, die zur Erfüllung notwendig sind, vollständig erfüllt werden.

Letztendlich wird mit Smart Contracts der gleiche Gedanke verfolgt wie bei der Blockchain oder bei Bitcoin. Ziel ist das Erfüllen von Verträgen und Austauschen von Daten, Informationen und Werten ohne das Einschalten von Intermediären.

2.1.2 Technologische Grundlagen von Smart Contracts

Die technologischen Grundlagen eines Smart Contracts sind Algorithmen und Programmcodes, in welchen alle vertragsrelevanten Informationen enthalten sind. Ein Smart Contract folgt einer „Wenn-Dann-Logik“. Die Resultate sind also an verschiedene Bedingungen geknüpft und von deren Erfüllung abhängig[44]. Wird eine grundlegende Bedingung erfüllt, so tritt folgend eine vorher im Programmcode festgelegte Reaktion ein[45].

Im folgenden Beispiel ist der Programmcode eines Smart Contracts skizziert, welcher auf einer Bedingung beruht und nur eine Folge, je nach Erfüllung oder Nichterfüllung der Bedingung[46], hat.

```
pragma solidity ^0.4.18;

contract muenzwurf;

function();

var einsatz = msg.value;

if (block.timestamp % 2 == 0);

msg.sender.send(2 * einsatz);

else;

return;
```

[44] Vgl. Borkert 2018, S. 41.

[45] Vgl. Sattler 2018, S. 2249.

[46] Vgl. Kaulartz und Heckmann 2016, S. 619.

Hier wird die eben schon erwähnte „Wenn-Dann-Logik“ aufgegriffen, die als Grundlage für dieses vom Umfang her einfache Beispiel dient. Der initiierende Vorgang dieses Smart Contracts ist die Transaktion eines Geldbetrages, ausgehend von einem Glücksspieler. Geschieht dies, generiert der Smart Contract eine Zufallszahl. Nun sind an diese Zufallszahl Bedingungen geknüpft, welche vom Smart Contract geprüft werden. Ist die Zufallszahl durch zwei teilbar, wird der Einsatz des Glücksspielers verdoppelt. Ist sie es nicht, behält der Smart Contract den Einsatz ein.

Wie schon erwähnt, ist dies ein sehr einfach gehaltenes Beispiel, da der Umfang an Parametern geringgehalten wurde und je nach Vertragsart und Vertragsbestandteilen noch eine Vielzahl an Bedingungen hinzugefügt werden kann. Grundsätzlich kann an diesem Beispiel die Funktionsweise eines Smart Contracts gut nachvollzogen werden.

2.1.3 Smart Contracts auf einer Blockchain

Grundsätzlich müssen Smart Contracts nicht in Verbindung mit einer Blockchain „betrieben“ werden, doch unterstützen die Charakteristika der Blockchain-Technologie die Ausführung und Integrität maßgeblich. Insbesondere die Manipulationssicherheit der zugrundeliegenden Blockchain-Infrastruktur ist von großem Vorteil[47]. Damit die Smart Contracts mit der jeweiligen Blockchain-Infrastruktur zusammenarbeiten können, müssen sie an diese angepasst werden. Dazu wird das sogenannte „compiling“ verwendet. Dies bedeutet, dass der Code des Smart Contracts so umgeschrieben wird, dass er der Programmiersprache der Blockchain entspricht[48]. Anschließend wird er in das Netzwerk implementiert und agiert als neuer Teilnehmer, ganz nach den Regeln, nach denen er programmiert wurde.

Um Verträge und Algorithmen in eine Blockchain einzubringen, bedarf es eines besonderen Typus von Blockchains, welche die Möglichkeit zulassen, zwei verschiedene Arten von Accounts anzulegen.

Dies wären:

- **Externe Accounts**

Dies sind die Accounts, die Nutzer und Teilnehmer eines Netzwerkes anlegen und welche Public- und Private-Keys zur Anmeldung und Interaktion miteinander nutzen. Dies ist z.B. der einzige Typ Account, welcher bei der Bitcoin Blockchain angelegt werden kann[49].

[47] Vgl. Fries und Paal 2019, S. 3

[48] Vgl. Antonopoulos und Wood, S. 29.

[49] Vgl. Wilkens und Falk, 2016, S. 10

- **Contract Accounts**

Diese Accounts besitzen ebenfalls einen Public-Key, können also von anderen Nutzern gefunden und bei Transaktionen mit einbezogen werden. Aber anders als Externen Accounts wird ihnen kein Private-Key zugeordnet, da es nicht gewünscht ist, dass ein Smart Contract nach der Codierung verändert werden kann oder andere Eigenschaften aufweist als die bei der Programmierung festgelegten[50]. Contract Accounts können also nur auf Grundlage ihres Codes und der Bedingungen mit anderen Netzwerkteilnehmern interagieren. Die weiterentwickelte und 2015 erschienene Ethereum Blockchain bietet die Möglichkeit, beide Arten von Accounts anzulegen. Smart Contracts sind immer Contract Accounts[51].

2.1.4 Oracles als Informationslieferanten der Umwelt

Als Oracles werden Schnittstellen bezeichnet, die Informationen aus der Realität automatisch der Blockchain sowie den Smart Contracts zuführen, diese verifizieren und nutzbar machen, wenn sie benötigt werden. Dies wird notwendig, wenn eine Bedingung für einen Smart Contract geprüft werden muss, weil eine Folge an die Erfüllung oder Nichterfüllung der Bedingung gebunden ist[52]. Oracles stellen also gewissermaßen eine Brücke zur realen Welt dar.

Als Beispiel wäre die Auszahlung einer Versicherungssumme bei einer Unwetterversicherung heranzuziehen. Angenommen, die Auszahlung ist an eine Mindestwindstärke gebunden, so ist ein Oracle dafür verantwortlich, dass diese Informationen wie Windgeschwindigkeit und -richtung von einer Wetterstation zu der Blockchain kommen und der Smart Contract nun die Erfüllung der Bedingung anhand dieser Daten überprüfen und gegebenenfalls eine Auszahlung einleiten kann.

2.1.5 DApp als unabhängige Programme

Eine DApp (decentralized application) ist eine Blockchain Anwendung, bei welcher alle Daten, unter anderem der Quellcode, auf einer Blockchain und somit auf allen teilnehmenden Rechnern gespeichert sind und nicht, wie gewöhnlich, nur auf dem Server oder im Netzwerk des Entwicklers und Anbieters. Das bedeutet, dass keine einzelne Person oder zentrale Gruppe bzw. Institution die im Netzwerk gespeicherten Daten kontrolliert[53], sondern die

[50] Vgl. Wilkens und Falk 2019, S. 11.

[51] Vgl. Wilkens und Falk 2019, S. 10.

[52] Vgl. Schuster et al. 2020, S. 137

[53] Vgl. Antonopoulos und Wood, S. 267–271

Anwendungen von allen Nutzern der Blockchain beaufsichtigt, kontrolliert und finanziert werden.

2.1.6 DAOs als sich selbst steuernde Unternehmen

DAO steht für „decentralized autonomous organization“ und ist eine Unternehmens- und Organisationsform, welche nur digital auf der Grundlage von DApps auf einer Blockchain existiert und sich selbst über Smart Contracts steuert. DAOs besitzen kein Management, keinen Firmensitz und keine anderweitige Verwaltungseinheit, und sind trotzdem voll funktionsfähig. Ihre Handlungen werden über den hinterlegten Code gesteuert[54]. Jeder kann sich finanziell an einer DAO beteiligen und erhält dafür Token, welche eingesetzt werden können, um über bestimmte Leistungen zu verfügen, sich an automatisierten Abstimmungen über die Verwendung des Kapitals der DAO zu beteiligen oder an Gewinnen teilzuhaben[55]. Entscheidend dafür ist immer der Zweck und Code, für welchen eine DAO geschaffen wurde.

Das Mittweidaer Blockchain Unternehmen Slock.it um den Gründer Steffen Jentzsch gehörte 2016 zu den ersten, die eine DAO auf Grundlage der Blockchain etablierten. Jentzsch schuf die DAO, um eine automatisierte Plattform für Crowdfoundig-Projekte zu schaffen, auf welcher Vorschläge eingereicht, verwaltet und bewertet werden konnten. Die Investoren, welche aus der Ethereum Community kamen, wurden bei erfolgreichen Projekten am Gewinn beteiligt[56].

2.2 Charakteristika und Merkmale

2.2.1 Transparenz

Durch das Implementieren von Smart Contracts in eine Blockchain gehen die Eigenschaften der Blockchain auf die Smart Contracts über. Dazu zählt ebenfalls die Transparenz, da die Transaktionen dauerhaft und unveränderlich protokolliert werden und für jeden einsehbar sind[57]. Das ist insbesondere der Fall bei einer öffentlichen Blockchain, auf die theoretisch jeder zugreifen kann. Und da bei Verträgen auch der Punkt der Rechtssicherheit mit in den Mittelpunkt rückt, bietet sich ein auf einer Blockchain geschriebener, unveränderlicher Smart Contract noch mehr an, da die Beteiligten auf eine unverfälschte

[54] Vgl. Fill und Meier 2020, S. 52

[55] Vgl. Wilkens und Falk 2019, S. 30.

[56] Vgl. Antonopoulos und Wood, S. 326–327

[57] Vgl. Heckmann und Schmid 2017, S. 14.

Transaktionssicherheit und Ausführung vertrauen können. Die Voraussetzung dafür ist, dass der Smart Contract fehlerfrei und im Sinne aller programmiert wurde[58].

2.2.2 Automatisierung

Die Verbindung der Eigenschaft der Automatisierung von Smart Contracts und den Eigenschaften der Blockchain, unter anderem Integrität und Verlässlichkeit, garantiert im Optimalfall eine problemlose Ausführung der Anwendung. Dadurch entfällt, bis auf den Punkt der Programmierung, die Möglichkeit menschlicher Fehler und Ungenauigkeiten im Vertragsablauf, die diesen beeinträchtigen könnten. Zudem muss es keine Vertrauensbasis zwischen den Parteien geben, da diese für eine reibungslose Vertragserfüllung nicht von Bedeutung ist[59].

2.2.3 Anonymität

Da es in der Charakteristik der Blockchain liegt, dass die Teilnehmer anonym agieren, nur Transaktionsdaten wie Betrag und Zeitpunkt gespeichert werden und es nicht möglich ist, einen Public-Key einer spezifischen Person zuzuordnen, gilt dies auch für die auf der Blockchain agierenden Smart Contracts[60]. Natürlich ist dies nur für einen Teil aller Verträge möglich, da es oft unumgänglich ist, dass sich die Vertragsparteien kennen.

2.2.4 Beschränkung auf die Prüfung von „true/false“ Ereignissen

Smart Contracts und deren Programmcode können nur dann „Entscheidungen“ treffen, bzw. der „Wenn-dann-Logik“ folgen, wenn es sich bei den auftretenden Ereignissen und prüfbaren Bedingungen um Prozesse handelt, welche sich mit „Ja“ oder „Nein“ beantworten lassen. Elemente des Abwägens, der komplexeren Entscheidungsfindung oder der Einschätzung von Fällen, welche sich als nicht eindeutig herausstellen, lassen sich nicht in Smart Contracts abbilden[61].

---

[58] Vgl. Kaulartz und Heckmann 2016, 619 f.

[59] Vgl. Heckmann und Schmid 2017, S. 13.

[60] Vgl. Wilkens und Falk 2019, S. 14–15.

[61] Vgl. Paulus und Matzke 2018, S. 1905.

2.3 Chancen und Risiken von Smart Contracts

Natürlich bringt jede neue Technologie mit viel Potenzial nicht immer nur neue Chancen mit sich, obwohl Smart Contracts davon zweifellos einige besitzen. Auch die Herausforderungen und Risiken, die in Erscheinung treten, müssen berücksichtigt werden, um eine einwandfreie Anwendung zu sichern.

2.3.1 Nutzen von Smart Contracts

Smart Contracts besitzen das Potenzial, Vertragsausführungen, wie sie aktuell rund um den Globus gehandhabt werden, vollkommen zu verändern. Selbstredend hängt das immer von der Vertragsart ab und davon, ob es sinnvoll ist, einen Smart Contract als Grundlage zu implementieren. Das ist eine Frage, welche in diversen Fallbeispielen in Kapitel 3 behandelt wird. Doch können durch sie die gewohnten Abläufe für alle Vertragsparteien in der Regel kostengünstiger und einfacher dargestellt und sicherer durchgeführt werden.

2.3.1.1 Eliminierung des Menschen als unberechenbare Fehlerquelle

Eine der wohl größten Fehlerquellen, welche für viele Probleme in jeglicher Art bei Transaktionen verantwortlich ist, ist menschliches Versagen[62]. Es ist unmöglich einzuschätzen, wie viel Zeit und Geld durch Smart Contracts und deren automatisiertes Handeln eingespart werden kann, doch das Potenzial ist enorm.

2.3.1.2 Kostensenkungen

Durch das Wegfallen von Intermediären, die die Vertragsbestandteile wie Transaktionen und Gegenleistungen überwachen oder durchführen, werden unmittelbar die Kosten gesenkt. Auch eventuelle Folgekosten entfallen, da bspw. eine nachträgliche Anfechtung eines Smart Contracts bei einer fehlerfreien Programmierung nicht möglich, oder zumindest nicht aussichtsreich wäre[63].

Einer Analyse der spanischen Banco Santander zufolge würden sich die Infrastrukturkosten für Banken durch eine flächendeckende Einführung von Smart Contracts und Blockchains bei internationalen Finanztransaktionen um bis zu 20 Milliarden Dollar jährlich reduzieren. Dies schließt ebenfalls die Abwicklungskosten mit Clearing und Settlement ein[64].

---

[62] Vgl. Tagliaferri 2019, S. 148.

[63] Vgl. Scherk und Pöchhacker-Tröscher 2017, S. 27.

[64] Vgl. Belinky et al. 2015, S. 15.

2.3.1.3 Zeiteinsparungen

Mit dem Entfallen von Intermediären, Clearingstellen und anderen Institutionen, welche für Vermittlung und Kontrolle von Vertragsgeschäften zwischen mehreren Parteien zuständig sind, erübrigen sich viele Arbeitsschritte, was schlussendlich zu deutlich geringeren Bearbeitungszeiten führt.

2.3.1.4 Sicherheit

Dadurch, dass Smart Contracts auf einer Blockchain aufgesetzt werden, übernehmen sie auch deren Eigenschaften, unter anderem im Punkt der Sicherheit. Zum einen haben durch die schon erwähnte Transparenz alle Parteien Einsicht und können sich über alle Transaktionen informieren. Des Weiteren kann im Nachhinein nichts mehr verändert werden, zumindest im Falle einer unmodifizierten Blockchain. Somit besteht eine starke Manipulationssicherheit.

2.3.1.5 Erhöhung der Vertragssicherheit

Da Smart Contracts ihre „Leistungen“ nur erbringen, wenn bestimmte Bedingungen erfüllt werden, ist die Einhaltung der Vertragsleistungen für alle teilnehmenden Parteien garantiert und der Ausfall von Leistungen kann so gut wie ausgeschlossen werden[65].

2.3.2 Risiken und Herausforderungen

2.3.2.1 Programmierung

Die ersten Probleme können schon bei der Programmierung des Codes für einen Smart Contract auftreten, weshalb insbesondere hier sehr umsichtig gearbeitet werden muss. Denn wenn es bei der Programmierung zu einem Fehler kommt, welcher unbemerkt bleibt und dann in die Blockchain implementiert wird, kann dieser nicht mehr behoben und nur durch einen vollkommen neuen Code ausgebessert werden[66]. Dies resultiert in einem grundsätzlich vermeidbaren Mehraufwand und führt zu weiteren Kosten.

2.3.2.2 Skalierbarkeit

Ein weiteres Problem tritt mit dem Faktor der Skalierbarkeit auf. Damit ist die theoretische Anzahl der Transaktionen in einem Netzwerk gemeint, welche maximal geleistet werden können. Wenn hier ein Vergleich zwischen den größten Blockchain-Netzwerken und den „klassischen“ Kreditkartenanbietern wie Visa und Mastercard herangezogen wird, wird schnell ersichtlich, dass diese noch einen großen Vorsprung besitzen. Laut eigenen

---

[65] Vgl. Furrer und Deck 2020, S. 286.

[66] Vgl. Wilkens und Falk 2019, S. 11.

Angaben besitzt das größere Visa-Zahlungsnetzwerk eine theoretische Kapazität von 65.000 Transaktionen pro Sekunde (TPS)[67]. Diese enorm hohe Kapazität kann aber nur unter idealen Bedingungen erreicht werden und so liegt der aktuelle Durchschnitt bei ca. 2.000 TPS[68].

Wenn wir nun auf die Skalierbarkeit von ausgewählten Blockchain-Netzwerken blicken, lassen sich aktuelle Unterschiede nicht von der Hand weisen. Die Leistung des Bitcoin-Netzwerkes ist durch die klar festgelegte Größe eines Blockes von einem Megabyte und der durchschnittlichen Größe einer Transaktion von ca. 400 Byte begrenzt[69]. In jedem Block können so ca. 2.500 Transaktionen untergebracht werden, und etwa alle 10 Minuten wird ein Block abgeschlossen, angehängt und einer neuer eröffnet[70]. Daraus lässt sich auf eine etwaige Transaktionsanzahl von 4 - 5 Stück pro Sekunde schließen. Etwas leistungsfähiger ist das Ethereum Netzwerk, welches aktuell bis auf 20 TPS kommen kann[71].

2.3.2.3 Rechtliche Herausforderungen

Die wohl größte Herausforderung, die vor einer flächendeckenden Nutzung von Smart Contracts bewältigt werden muss, ist die Vereinbarkeit mit den jeweiligen gesetzlichen Bestimmungen. Aktuell ist die deutsche Rechtsprechung nicht darauf ausgelegt, dass Verträge autonom durchgeführt werden. Genau hier muss der Gesetzgeber ansetzen und Grundlagen für eine umfängliche Nutzung schaffen.

Die rechtlich notwendigen Thematiken lassen sich grundsätzlich in die Segmente Datenschutz und Verantwortlichkeit unterteilen.

- **Datenschutz**

Die Transparenz sowie die Unveränderlichkeit, also auch die Nichtlöschung, als grundlegende und prägende Eigenschaften einer Blockchain stehen grundsätzlich dem Punkt des Datenschutzes entgegen, weswegen eine Prüfung der Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) erfolgen muss.

Die 2018 erlassene DSGVO dient in erster Linie dem Schutz von personenbezogenen Daten. Hier stellt sich nun die Frage, ob die Daten, welche in einer Blockchain offengelegt werden und im Falle einer Public-Blockchain für jeden einsehbar sind, einer Person

---

[67] Vgl. VISA Fact Sheet 2020.

[68] Vgl. Ploom 2016, S. 142.

[69] Vgl. Vukolic 2016, S. 113.

[70] Vgl. Fill und Meier 2020, S. 11.

[71] Vgl. Ploom 2016, S. 139.

zugeordnet werden können. Grundsätzlich ist dies nicht der Fall, da durch den Charakter der Blockchain eine Pseudonymisierung der Teilnehmer stattfindet [72]. Dennoch muss, je nach Anwendung und Spezifikation eines Smart Contracts, eine weitere sorgfältige Prüfung stattfinden. Auch ist zu beachten, dass bei Transaktionen gegebenenfalls eine Online-Geldbörse oder ähnliche digitale Wertaufbewahrungsmittel vonnöten sind, über welche theoretisch eine eindeutige Zuordnung möglich ist. Zudem können mit etwas Mehraufwand über die IP-Adresse des Computers, über welchen an der Blockchain teilgenommen wird, die Nutzer identifiziert werden[73]. Im Falle einer Private-Blockchain stellt sich die Frage der Anwendbarkeit des Datenschutzes nicht, da eine vorherige Identifizierung stattgefunden hat und die Zuordnung von Nutzerkennung und Identität dem Administrator des Netzwerkes bekannt ist[74].

- **Verantwortlichkeiten**

Die nächste rechtliche Problematik kommt mit der Frage auf, wer die Verantwortung über die Blockchain, bzw. die darauf aufgesetzten Smart Contracts, besitzt und im Schadensfalle als Anspruchsgegner gilt. Die Merkmale der Verantwortung bestehen gemäß Artikel 4 Nr.7 DSGVO aus der Kontrolle über den Zweck und die Mittel der Verarbeitungen in der Blockchain.

Wenn es sich um eine Private-Blockchain handelt, ist der Verantwortliche in der Regel entweder der Produzent der Software oder derjenige, der für die Zugangsrechte sowie den Betrieb der Blockchain und der zugehörigen Smart Contracts zuständig ist, bzw. dessen Auftraggeber. In solchen Fällen ist die Rechtslage grundsätzlich klar und eindeutig[75].

Bei einer Public-Blockchain ist der Fall wesentlich schwieriger zu beurteilen. So erfüllt in der Regel keiner der möglichen Anspruchsgegner bzw. Teilnehmer alle Anforderungen, die ihn laut Gesetz auszeichnen müssten.

Der Programmierer oder Entwickler einer Blockchain gibt die Verantwortung nach Programmierung dieser aus der Hand und kontrolliert so nicht mehr den Verwendungszweck und die Mittel der Anwendung. Ebenso scheidet auch der einzelne Teilnehmer als potenziell verantwortlich aus, da er nur eine Transaktion vornimmt, aber ebenfalls keine Kontrolle über Zweck und Mittel der Blockchain hat. Als nächstes müsste die Zuständigkeit der Miner geprüft werden, aber da diese nur für das „Verketten“ der Blöcke innerhalb der Blockchain verantwortlich sind und keinen Einfluss auf den Inhalt der Datensätze haben, sind auch sie

[72] Vgl. Kaulartz 2016, S. 474–479.

[73] Vgl. Petrlic und Sorge 2017, S. 84–85.

[74] Vgl. Kaulartz 2016, S. 474–480.

[75] Vgl. Martini und Weinzierl 2017, S. 1251–1255.

nicht als Verantwortliche zu betrachten. Als letztes kommen damit nur noch die Nodes, also die Teilnehmer am Netzwerk, welche ein Exemplar der Blockchain auf ihrem Rechner gespeichert haben, infrage. Diese sind zum einen für die Validierung, also die Prüfung der von den Minern erzeugten Blöcke, als auch für das Teilen der Blöcke mit dem Netzwerk verantwortlich. Damit haben sie eine gewisse Kontrolle über die Verwendung der Datensätze, da sie die Blöcke auf ihren Rechnern speichern und anschließend verteilen[76].

- **Code is law**

Zudem stellt sich die Frage, ob eine Rechtsprechung auf Grundlage der Maxime „Code is law" Sinn ergäbe. Dies lässt sich größtenteils verneinen, da in dieser Form der Rechtsauslegung nur der zugrunde liegende Code des Contracts für die Parteien bindend wäre und dieser sich so über die staatliche Rechtsprechung hinwegsetzen würde. Somit hätte der Code des Smart Contracts bei Implementierung den staatlichen Regelungen zu entsprechen und müsste bei auftretenden Programmierfehlern verändert bzw. verbessert aufgesetzt werden[77].

2.3.2.4 Standards

Des Weiteren muss darauf hingearbeitet werden, einen gewissen Standard für die Programmierung von Smart Contracts zu schaffen. Es gibt viele verschiedene Blockchains, deren Protokolle es zulassen, dass auf ihnen Smart Contracts aufgesetzt werden können. Das Problem dabei ist, dass in der Regel all diese Blockchains unterschiedliche Programmierschnittstellen und Formate erfordern, um Smart Contracts hinzuzufügen. So fällt es Unternehmen, die Blockchain-basierte Anwendungen auf den Markt bringen wollen, schwer, die Anwendungen an jedes einzelne Interface anzupassen. Dies ist nicht nur eine zeitraubende und kostenintensive Arbeit, sondern auch sehr fehleranfällig. So muss es künftig das Ziel sein, eine gewisse Homogenität für die Implementierung der Anwendungen herzustellen[78]. Die Lösung ist eine Schnittstelle, welche die Kommunikation und Interaktion von Smart Contracts auf unterschiedlichen Plattformen vereinheitlicht: das sogenannte „Smart Contract Invocation Protocol"[79].

2.3.2.5 Änderung von Vertragsinhalten und Rückabwicklung

Da Smart Contracts nach der Implementierung nicht mehr verändert werden können, wenn dies bei der Programmierung nicht vorgesehen war, kann es keine individuellen und

[76] Vgl. Martini und Weinzierl 2017, S. 1254–1255.

[77] Vgl. Wilkens und Falk 2019, S. 30.

[78] Vgl. Falazi et al. 2020, S. 135.

[79] Vgl. Falazi et al. 2020, S. 135.

nachträglichen Anpassungen der Vertragsbestandteile geben[80]. So können z.B. keine außerordentlichen Rückzahlungen von Krediten vorgenommen werden, wenn der Schuldner seinen Kredit vorzeitig tilgen möchte. Ebenso könnten Kundenbeziehungen darunter leiden, wenn der Käufer in Zahlungsverzug gerät. Smart Contracts würden in solchen Fällen den Schuldner unmittelbar in Verzug setzen oder sanktionieren, unabhängig davon, wer der Kunde ist. Bei traditionellen Verträgen kann individuell entschieden werden, welche und ob überhaupt Maßnahmen ergriffen werden. Somit stehen Smart Contracts aktuell noch entgegen der anhaltenden Zunahme der Flexibilität im Wirtschaftsalltag[81].

Smart Contracts können zwar auch bei Rückabwicklungen zum Einsatz kommen, doch betrifft dies aktuell nur einfachste Vorgänge, wie zum Beispiel das Erkennen von eingegangenen Rücksendungen im Wareneingang und das darauffolgende Auslösen von Rückzahlungen an den Kunden. Um aber die Komplexität von Anfechtungsrecht, Gewährleistungsrecht und Widerrufsrecht sowie deren Voraussetzungen und Rechtsfolgen in einem Smart Contract unterzubringen, müssen noch viele programm- und rechtstechnische Hürden überwunden werden, was zum aktuellen Zeitpunkt unrealistisch ist[82].

Des Weiteren ist es gerade bei öffentlichen Blockchains problematisch, fehlerhafte Transaktionen, welche aufgrund der Charakteristika des Smart Contracts und der zugrundeliegenden Blockchain anonym vorgenommen wurden, rückgängig zu machen, wenn diese programmtechnische Spezifikation der Rückabwicklung nicht vorgesehen wurde und der Vertragspartner nicht bekannt ist.

2.3.2.6 Technologische Ressourcen

Ein weiteres Problem, welches aktuell als eine der größten Herausforderungen bei der Implementierung der Blockchain-Technologie angesehen wird, ist die lückenlose Bereitstellung der Infrastruktur, um einen optimalen Einsatz zu gewährleisten. Dazu gehört zum einen die große Rechnerkapazität, die benötigt wird, um die teilweise doch immense Datenmenge, welche eine Blockchain darstellen kann, auf den Rechnern der Netzwerkteilnehmer speichern zu können. Die Ethereum Blockchain besitzt beispielsweise aktuell eine Größe von etwas mehr als 400 Gigabyte und wächst mit jedem neuen Block, was bei einer Zunahme von Verwendungsmöglichkeiten und Anwendungen exponentiell ansteigen könnte[83]. Zum anderen ist eine ständige, lückenlose und leistungsfähige Internetverbindung von Nöten, um die Integrität der Blockchain zu wahren.

---

[80] Vgl. Fill und Meier 2020, S. 124.

[81] Vgl. Fill und Meier 2020, S. 124.

[82] Vgl. Kaulartz und Heckmann 2016, S. 623.

[83] Vgl. BitInfoCharts 2020.

2.4 Fazit und Potential

Zusammenfassend kann gesagt werden, dass das Potenzial von Smart Contracts klar erkennbar ist und viele ihrer Eigenschaften sicherlich gewinnbringend eingesetzt werden könnten. Angefangen bei der Automatisierung und dem damit einhergehenden Zeitgewinn, bis hin zu den enormen Kosteneinsparungen, welche durch das Wegfallen einiger Instanzen im Vertragsablauf zustande kommen, sind die Vorteile der Technologie offenkundig. Doch mindestens in gleichem Maße stehen wir im Bereich der Smart Contracts vor Herausforderungen, welche vor einer Einbindung in das alltägliche Vertragswesen beseitigt werden müssen.

Dem aktuellen Stand nach bieten sich Smart Contracts vor allem in Bereichen an, in denen es nicht zwingend erforderlich ist, dass sich die Parteien kennen, und in denen deren Identität nicht von Belang ist. Andersherum ist ein gewinnbringender Einsatz auch oder gerade dann möglich, wenn sich beide Parteien schon kennen und somit Ihre Identitäten offengelegt haben[84]. Zum derzeitigen Zeitpunkt ist vorrangig eine Implementierung in Segmenten, in denen grundsätzlich ein geringes Schlechtleistungsrisiko besteht, empfehlenswert, da die rechtlichen Grundlagen im Fall eines Vertragsbruchs noch nicht vollends ausgearbeitet wurden[85].

[84] Vgl. Kaulartz und Heckmann 2016, S. 620.

[85] Vgl. Kaulartz und Heckmann 2016, S. 620.

3 Einbindung von Smart Contracts in ausgewählten Bereichen der Finanzwirtschaft

Ist die Finanzwirtschaft heutzutage noch größtenteils von Intermediären wie Banken oder Clearingstellen gekennzeichnet, so könnte sich das in naher Zukunft ändern. Dafür verantwortlich ist unter anderem die in Kapitel 1.1 erklärte Distributed Ledger Technology alias Blockchain mit ihren Smart Contracts und all den gewinnbringenden und kosteneinsparenden Eigenschaften, in welchen enormes Potential steckt.

Es besteht die Möglichkeit, dass Smart Contracts zukünftig in immer mehr Bereichen des Alltags anzutreffen sind, ohne dass es der Mehrzahl der Menschen überhaupt bewusst ist, dass sie mit einem Smart Contract interagieren. Dies zeigt sich allein an den vielen möglichen Verwendungsszenarien und der Tatsache, dass laufend weitere neue Anwendungsfelder gefunden werden. Angefangen beim Internet der Dinge, bei welchem physische und virtuelle Objekte miteinander kommunizieren können[86], über eine dezentrale Energieversorgung, bei der nicht zentrale Energieversorger als Lieferanten gelten, sondern Privatpersonen, die über Photovoltaikanlagen und ähnliches selbst Strom produzieren[87], bis hin zum Anwalts- und Notariatswesen, welches durch die Blockchains und die damit einhergehende Integrität der Smart Contracts teilweise ersetzt werden könnte[88].

Im Folgenden setzen wir uns mit einigen aktuellen und geplanten Anwendungsszenarien für Smart Contracts auseinander, welche sich in erster Linie auf die Finanzwirtschaft konzentrieren, da diese einer der größten Profiteure der Technologie werden kann. Schon zum jetzigen Zeitpunkt finden wir, abgesehen von der IT-Branche selbst, einen verhältnismäßig hohen Anteil von Blockchain-Anwendungen im Finanzsektor wieder, was in Abbildung 6 veranschaulicht wird[89].

[86] Vgl. Scherk und Pöchhacker-Tröscher 2017, S. 8.

[87] Vgl. Heckmann und Schmid 2017, S. 9.

[88] Vgl. Scherk und Pöchhacker-Tröscher 2017, S. 28.

[89] Vgl. Schlatt et al. 2016, S. 19–20.

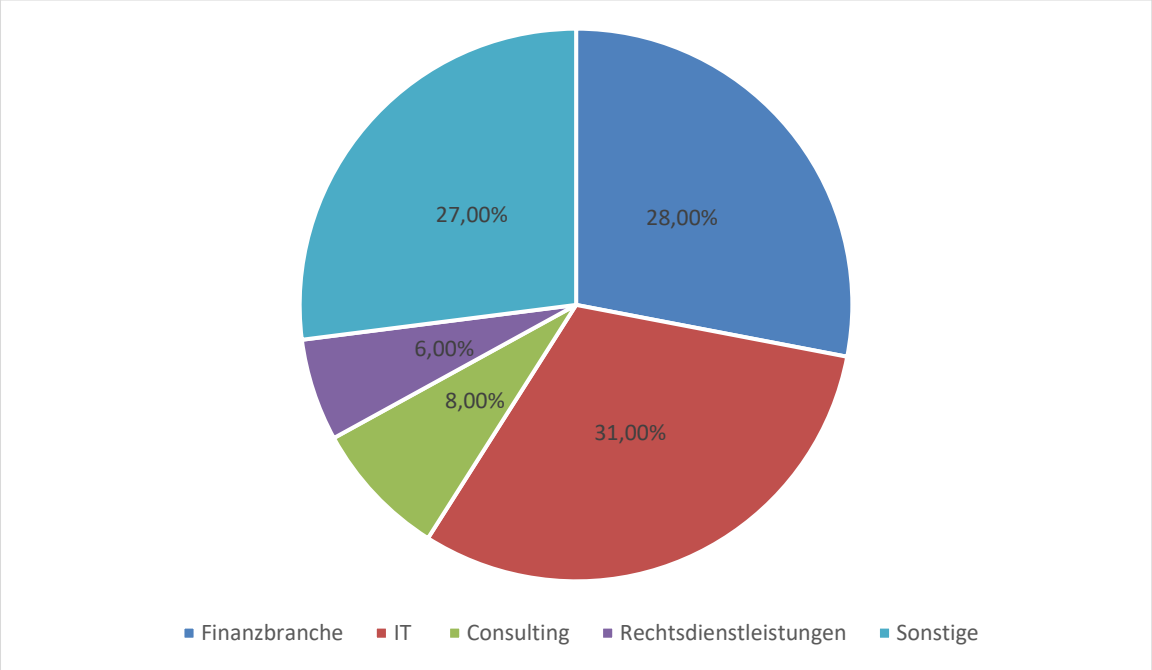

Abbildung 6: Branchenübergreifender Vergleich von Anwendungen auf Blockchain-Basis[90]

So wird deutlich, dass, obwohl wir uns noch am Anfang der Entwicklung und Einbindung von Smart Contracts befinden, ein vergleichsweise hoher Anteil an Anwendungsmöglichkeiten innerhalb der Finanzbranche zu finden ist. Dieser könnte in Zukunft durch die Schaffung neuer Implementierungsmöglichkeiten für die Blockchain-Technologie im Finanzwesen sogar noch zunehmen.

[90] Eigene Darstellung in Anlehnung an Schlatt et al. 2016, S. 19–20.

3.1 Leasing und Mieten von Vermögensgegenständen

Durch den Fortschritt im Bereich der Blockchain haben sich effizientere Möglichkeiten zur Finanzierung von Vermögensgegenständen aufgetan. So können in Verbindung mit dem Internet der Dinge Geräte über Smart Contracts Vertragsbestandteile überwachen und bei Bedarf eingreifen. Wird beispielsweise eine Leasingrate eines Autos nicht gezahlt und nach wiederholter Mahnung der offene Betrag nicht beglichen, kann der Smart Contract über die im Auto eingebaute Software das Fahrzeug fahruntüchtig machen und den Standort an den Leasinggeber weiterleiten, damit das Auto wieder eingezogen wird[91]. Dadurch werden enorme Kosten gespart. Wo sonst noch Mahn- und Gerichtskosten entstehen, können so die vertragsrechtlichen Ansprüche durchgesetzt werden, ohne weitere Kosten zu verursachen[92].

Ebenfalls im Bereich von flexiblen Mietverträgen können Smart Contracts zukünftig für mehr Fairness sorgen. Dazu werden Smart Contracts implementiert, welche über Oracles mit einem dafür geschaffenen Register für Immobilienwerte verbunden werden. Diese können den Mietpreis immer an den aktuellen Wert der Immobilie anpassen oder sich zumindest daran orientieren[93] .

[91] Vgl. Blockchain-Technologie 2020.

[92] Vgl. Fill und Meier 2020, S. 121.

[93] Vgl. Sellnow 2020.

3.2 Effizienzerhöhung des Zahlungsverkehrs

Der Zahlungsverkehr ist einer der Bereiche, welcher durch die Einbindung von auf Blockchains basierenden Smart Contracts am meisten profitieren könnte. Sind beispielsweise Überweisungen innerhalb einer Landesgrenze inzwischen schneller oder günstiger geworden, so sind vor allem grenzüberschreitende Zahlungen immer noch verhältnismäßig teuer und ineffizient. Eine simple internationale Überweisung kann schon mal mehrere Tage in Anspruch nehmen, da in der Regel mindestens zwei Banken mit einer Vielzahl an Prozessen involviert sind und menschliches Versagen als Fehlerquelle noch hinzukommen kann. So kann eine Überweisung, beispielsweise von Deutschland nach China, in Höhe von 300 € schnell Transaktionskosten im mittleren zweistelligen Bereich verursachen und sich auf eine Dauer von bis zu acht Tagen erstrecken[94]. Im schnelllebigen Wirtschaftsalltag gleicht dieser Zeitraum einer Ewigkeit.

Während in den letzten Jahren schon vermehrt an Systemen gearbeitet wurde, welche die Geschwindigkeit, Sicherheit und Kosten von Geldtransfers optimieren sollen, so stellen Programme auf Grundlage einer Distributed Ledger Technologie wie Ethereum oder Ripple den wohl größten Fortschritt dar, der in der jüngeren Vergangenheit in diesem Bereich gemacht wurde.

Und genau hier setzt die Royal Bank of Scotland an[95]. Diese hat einen Clearing- und Verarbeitungsmechanismus geschaffen, welcher mit Smart Contracts auf Grundlage der Ethereum-Blockchain arbeitet und enorme Vorteile in den Punkten Kosten und Geschwindigkeit bringt. Dazu wurde der Mechanismus in ein dafür geschaffenes Netzwerk aus sechs Banken eingebracht und in diesem unzählige Transaktionen herumgeschickt. Im Ergebnis wurde es möglich, 100 Transaktionen pro Sekunde zu bearbeiten und gleichzeitig die Dauer einer Transaktion auf einen Zeitrahmen von drei bis acht Sekunden zu begrenzen. Dies stellt einen enormen Geschwindigkeitszuwachs im Vergleich zum aktuell gängigen SEPA Verfahren dar, welches in der Regel einen Arbeitstag in Anspruch nimmt[96]. Es wird geschätzt, dass Banken bis zu 60% ihrer Kosten für internationale Zahlungen durch Abwicklungsprozesse auf Blockchain-Basis einsparen könnten[97].

---

[94] Vgl. Damm 2017.

[95] Vgl. Creer et al. 2016.

[96] Vgl. Wirth 2020.

[97] Vgl. Long 2016.

3.3 Neue Wege der Unternehmensfinanzierung

Smart Contracts in Verbindung mit einer Blockchain bieten neue und effizientere Möglichkeiten, um finanzielle Mittel in das Unternehmen zu holen. Dies funktioniert über das Ausgeben von sogenannten „Token“, ähnlich klassischen Wertpapieren, und nennt sich, bei erstmaligem Angebot, „Initial Coin Offering“ (ICO)[98].

Dabei gibt es zwei Arten von Token, die von besonderer Relevanz sind.

- **Utility Token**

Diese sind an zukünftige Dienstleistungen gebunden, zu deren Nutzung der Besitzer der Token berechtigt ist, und können, ähnlich wie Aktien, weiterverkauft werden - im besten Falle mit Gewinn. Sie haben also den Charakter eines Vorabverkaufs oder des Verkaufs einer limitierten Version eines Produktes des Unternehmens[99].

- **Security Token**

Diese ähneln mehr den klassischen Wertpapieren. Sie sind mit einem Zahlungsanspruch gegenüber dem Unternehmen verbunden, welcher an Gewinn, Umsatz oder eine andere Kennzahl gekoppelt ist[100].

Es werden bei ICOs meistens beide Arten von Token ausgegeben, weswegen hier von einer Mischform aus Wertpapieremission und Vorabverkauf gesprochen werden kann.

Da die gesamte Abwicklung eines ICOs über Smart Contracts abläuft, kann auf Intermediäre wie Banken und Börsen verzichtet werden. Auch gibt es keine Vorschriften über die Mindestgröße des ausgebenden Unternehmens. Somit eignet sich ein ICO für Start-Ups und Kleinunternehmen oder Gründer, die nicht mehr als eine Idee und einen Plan vorweisen können, sowie für Konzerne, die Kapital auf neuem Wege beschaffen wollen. Voraussetzung ist nur, dass das Unternehmen oder Projekt auf einer Blockchain agiert bzw. basiert[101].

---

[98] Vgl. Hahn und Wons 2018, S. 3

[99] Vgl. Schuster et al. 2020, S. 139

[100] Vgl. Schuster et al. 2020, S. 139

[101] Vgl. Hahn und Wons 2018, S. 5

3.4 Automatisierung der Inanspruchnahme von Versicherungsleistungen

Dass Versicherungsverträge und deren Vertragstexte oft schwierig zu verstehen sind, dürfte den meisten Menschen klar sein. Zudem ist vielen im Falle eines Schadens nicht immer eindeutig klar, ob die Versicherung jetzt zahlt oder nicht, da die Auszahlungsbedingungen, abhängig von der Versicherung, kompliziert und vielschichtig sein können. Auch ist es oft ein Problem, besonders für den Versicherungsnehmer, dass im Schadensfall viel Zeit vergeht, bis die Versicherung leistet. Grund dafür ist zum einen die Versicherungsgesellschaft, die als Intermediär dient und zu einer verlängerten Bearbeitungszeit des Anspruches beiträgt, und zum anderen die Bank, die für die Auszahlung der Versicherungssumme zuständig ist und somit als weiterer Intermediär fungiert, wodurch die vielleicht dringend benötigte Zahlung weiter hinausgezögert wird.

Und genau hier könnte die Implementierung eines Smart Contract auf Blockchain-Basis große Vorteile mit sich bringen. Dieser könnte auf Grundlage seines Codes vollkommen objektiv entscheiden, ob die Bedingung, die für eine Auszahlung notwendig ist, erfüllt wurde, und anschließend eine unmittelbare Auszahlung veranlassen[102]. So können im Schadensfall viel Zeit und finanzielle Mittel eingespart werden.

Der Versicherungskonzern AXA hat genau diese Vorteile aufgegriffen und ein eigenes Produkt entwickelt, das auf der Ethereum Blockchain aufbaut und über Smart Contracts gesteuert wird[103]. „Fizzy“, wie das Projekt genannt wird, ist für die Versicherung von Flugverspätungen verantwortlich und bearbeitet die Schadensfälle vollkommen autonom. Dazu muss der Kunde nur den Flug erfassen, seine Deckung wählen und seine Prämie bezahlen. Als nächster Schritt wird dann auf Grundlage dieser Daten der Smart Contract abgeschlossen und in die Blockchain implementiert. Darauf aufbauend überwacht der Smart Contract über ein Oracle die Flugdaten und Verspätungen mittels einer Datenbank. Wenn dann die festgesetzten Bedingungen für eine Verspätung eingetreten sind, wird die Zahlung automatisch ausgeführt.

[102] Vgl. Schuster et al. 2020, S. 137

[103] Vgl. Temperli 2018.

3.5 Fairere Gestaltung des Rating-Prozesses

Als letztes Beispiel dafür, was Smart Contracts und die Blockchain an sich für ein Potenzial im Bereich des Finanzsektors besitzen, beschäftigen wir uns mit dem Verfahren zur Bonitätsprüfung.

Unternehmen und sogar ganze Staaten sind auch davon abhängig, zu welchen Konditionen sie Fremdkapital von Kreditgebern beziehen können. Diese Konditionen richten sich nach dem Rating, welches durch Ratingagenturen festgelegt wird. So haben diese Ratingagenturen eine große Macht über die Geschicke der Unternehmen und Staaten und besitzen für sie eine zentrale Bedeutung. Entscheidend für die Bewerteten, aber auch für die Integrität des gesamten Systems, ist die Objektivität dieses Ratings. Diese kann jedoch durch eine Vielzahl an Faktoren beeinflusst werden, wodurch eine Reihe von mehr oder minder offensichtlichen Problemen resultiert[104].

- **Oligopol**

Der Markt an Ratingagenturen ist für solch einen wichtigen und zentralen Wirtschaftsbestandteil verhältnismäßig klein. Weltweit gibt es Schätzungen zufolge ca. 150 anerkannte Ratingagenturen[105]. Diese Zahl mag zunächst nicht allzu klein erscheinen, es ergibt sich jedoch ein anderes Bild, wenn bedacht wird, dass 3 dieser 150 Unternehmen, nämlich Fitch, Standard&Poors und Moody´s, in den USA mehr als 95%, in Europa ca. 92% und weltweit 93,5% des gesamten Umsatzes unter sich ausmachen[106]. So besitzen diese drei Agenturen eine unverhältnismäßig hohe Marktmacht und bilden ein Oligopol in diesem Bereich.

- **Interessenkonflikte**

Weiterhin stellt sich die Frage, inwiefern Ratingagenturen objektiv und ohne Einflüsse bewerten können, wenn diese doch von den Unternehmen bezahlt und beauftragt werden, ein Rating zu erstellen. Der Interessenkonflikt gestaltet sich so, dass zum einen das Rating qualitativ hochwertig sein und einem gewissen Standard der Ratingagentur entsprechen muss, zum anderen aber das beauftragende Unternehmen die Agentur bezahlt und grundsätzlich ein zufriedenstellendes Ergebnis erwartet[107].

---

[104] Vgl. Schellinger et al. 2019, S. 291–292.

[105] Vgl. Siebert 2015, S. 19

[106] Vgl. U.S. Securities and Exchange Commission und Office of Credit Ratings 2020.

[107] Vgl. White 2010

- **Meinungsäußerung**

Ein weiteres, aber weniger offensichtliches Problem, ist die Tatsache, dass die entstandenen Ratings der Agenturen nur als fundierte Meinungsäußerungen verstanden werden dürfen, aber von den Kreditgebern selten als solche betrachtet werden. Die drei großen Ratingagenturen kommunizieren dies auch auf ihren Internetpräsenzen[108], wodurch in der Regel die Haftungsfrage bei fehlerhaften Ratings entfällt. In der US-Gerichtsbarkeit gelten Ratings nur als Meinungsäußerung und Empfehlung und können daher nicht als Grundlage für Prozesse im Falle von Schädigungen ~~a~~angesehen werden[109].

- **Mangelnde Transparenz**

Als letztes größeres Problem kristallisiert sich die fehlende Transparenz des Bewertungsprozesses von Rating-Agenturen heraus. Die Agenturen haben auf ihren jeweiligen Internetpräsenzen einen groben Leitfaden veröffentlicht, welcher den Ablauf darstellen soll, aber an detaillierten Angaben, nach welchen Methoden bewertet wird, fehlt es. Folglich kann in der Regel nicht einwandfrei nachvollzogen werden, wie ein Rating zustande kommt, und Herabstufungen können zu erhöhten Kreditkosten führen, ohne dass der Grund dafür bekannt oder nachvollziehbar ist[110]. Seit geraumer Zeit werden die Rating-Agenturen, insbesondere die drei Platzhirsche, u.a. durch die EU-Finanzmarktaufsicht dazu angehalten, die Prozesse zum Zustandekommen ihrer Ratings offener zu gestalten[111].

Und hier kommt die Thematik des Smart Ratings ins Spiel, welches Ratingabläufe automatisieren und komplett objektiv gestalten soll.

- **Smart Rating - Netzwerk, Teilnehmer und deren Aufgaben**

Beim Smart Rating handelt es sich um eine DAO, welche vier verschiedene Typen von Teilnehmern enthält: die Ratingexperten, die Rater, die Emittenten und die Abonnenten. Die Ratingexperten entwerfen einen allgemeinen Ablaufplan für Ratings und benennen und gewichten die unterstützenden Kennzahlen qualitativer und quantitativer Art wie Umweltfaktoren und Erfahrungswerte, welche in das Rating einfließen. Die Rater sind Personen, welche aus der Branche kommen und diese kennen. Sie sind für die Beurteilung anhand des Ablaufplanes zuständig. Jeder Rater hat eine Netzwerkreputation, welche über die Gewichtung seiner Beurteilung entscheidet und über seine Entlohnung bestimmt. Ein weiterer wichtiger Teilnehmer ist der Emittent, welcher die Ratings in Auftrag gibt und die darin einfließenden Daten auf einer Blockchain bereitstellt. Zudem hinterlegt er auf dieser die

[108] Vgl. Moody´s Investors Service 2018; Fitch Ratings 2020; S&P Global Ratings 2020.

[109] Vgl. Däubler 2012, S. 19.

[110] Vgl. Schellinger et al. 2019, S. 293.

[111] Vgl. Handelsblatt 2012.

Bezahlung, welche für das Rating erforderlich ist. Zuletzt existieren noch die Abonnenten, welche entgeltlich Einsicht in die entstandenen Ratings anfordern können. Zumeist sind dies die Kreditgeber[112].

[112] Vgl. Schellinger et al. 2019, S. 294–301.

4 Handlungsempfehlungen

Im abschließenden Kapitel geht es um allgemeine Handlungsempfehlungen und Implementierungsabläufe, welche den Umgang mit Smart Contracts und der Blockchain-Technologie erleichtern sollen.

4.1 Allgemeine Handlungsempfehlungen

4.1.1 Anregungen und Förderungen für Projekte schaffen

Da die Forschung und Entwicklung von Projekten, welche mit Smart Contracts arbeiten und auf einer Blockchain basieren, auch für etablierte Unternehmen und besonders für Start-Ups eine kostenintensive Angelegenheit ist, sollte die öffentliche Hand hier als initiierender Akteur tätig werden und Unterstützungsarbeit leisten. Ob dies durch finanzielle Mittel geschieht oder durch Kooperationen, um gemeinsame Projekte anlaufen zu lassen, hängt immer vom jeweiligen Zweck ab. Wie wichtig die Politik als initiierender Akteur ist, zeigt die folgende Grafik. In deren Grundlage wurden Unternehmen zur Rolle der politischen Ebene beim Vorantreiben der Blockchain-Technologie befragt.

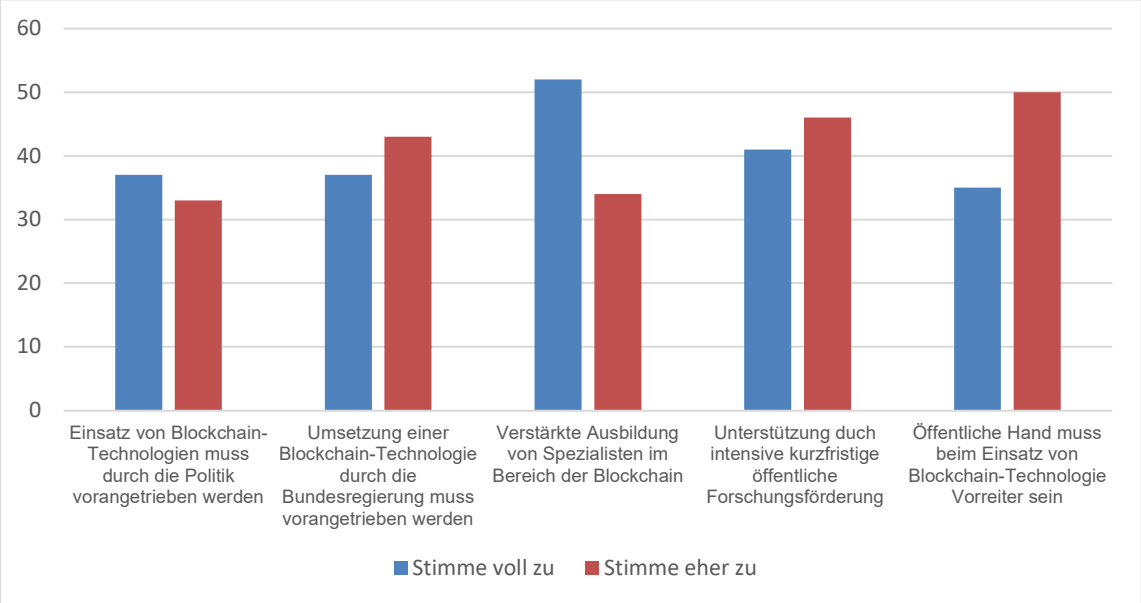

Abbildung 7: Umfrage an Unternehmen zum Voranbringen der Blockchain-Technologie[113]

[113] Eigene Darstellung in Anlehnung an Daten von Gentemann 2019, S. 61.

4.1.2 Rechtliche Auslegung

Wie in Kapitel 2.3.2.3 schon erwähnt, ist u.a. die deutsche Rechtsprechung nicht auf automatisierte und dezentrale Konstrukte wie Blockchains und Smart Contracts ausgelegt. So muss hier die Gesetzgebung, optimalerweise in Kooperation mit privatwirtschaftlichen Akteuren im Bereich der DLT, aktiv werden und nationale Standards etablieren, um Entwicklung und Anwendung nicht zu behindern, sondern zu fördern und einen sicheren Rechtsrahmen zu schaffen. Im Optimalfall würden diese Standards auf nationaler Ebene etabliert, sodass Deutschland eine Vorreiterrolle im internationalen Vergleich einnehmen könnte.

4.1.3 Ausbildung von Experten

Der Einbindung von Thematiken wie DLT, Blockchain und Smart Contracts in das Bildungs- und Ausbildungssystem sollte eine größere Bedeutung beigemessen werden. So ist es äußerst wichtig, Studierende und zukünftige Arbeitnehmer mit den notwendigen Kenntnissen und Fähigkeiten der Theorie und Anwendung von DLT und Blockchains auszustatten, indem diese in verstärktem Maße mit in den Lehrplan aufgenommen werden. Distributed-Ledger orientierte Studiengänge sind bis dato die Seltenheit. Der Studiengang „Blockchain & Distributed Ledger Technologies (DLT)“ an der sächsischen Hochschule Mittweida gilt beispielsweise als einer der ersten Studiengänge dieser Art in ganz Europa. Auch hier empfehlen sich Kooperationen von Bildungseinrichtungen und Wirtschaftsakteuren, um gemeinsame Projekte zu ermöglichen.

4.1.4 Bildung von Netzwerken und Kooperationsgemeinschaften

Das in Kapitel 1.2.4 vorgestellte Konzept des Konsortium R3 zeigt, dass das Bilden von Forschungs- und Entwicklungsnetzwerken ein effektives Mittel ist, um von den Synergieeffekten der Netzwerkteilnehmer zu profitieren. So können die Kosten gesplittet und das Know-How gesammelt werden. Zudem unterstützt eine gemeinsame Entwicklung den Punkt der Standardisierung und verhilft zu erhöhter Effizienz.

4.2 Stufenmodell zur Einbindung der Blockchain Technologie

Das folgende Stufenmodell stellt den möglichen Ablauf eines Implementierungsprozesses bei einem Pilotprojekt im Bereich der Blockchain-Technologie dar.

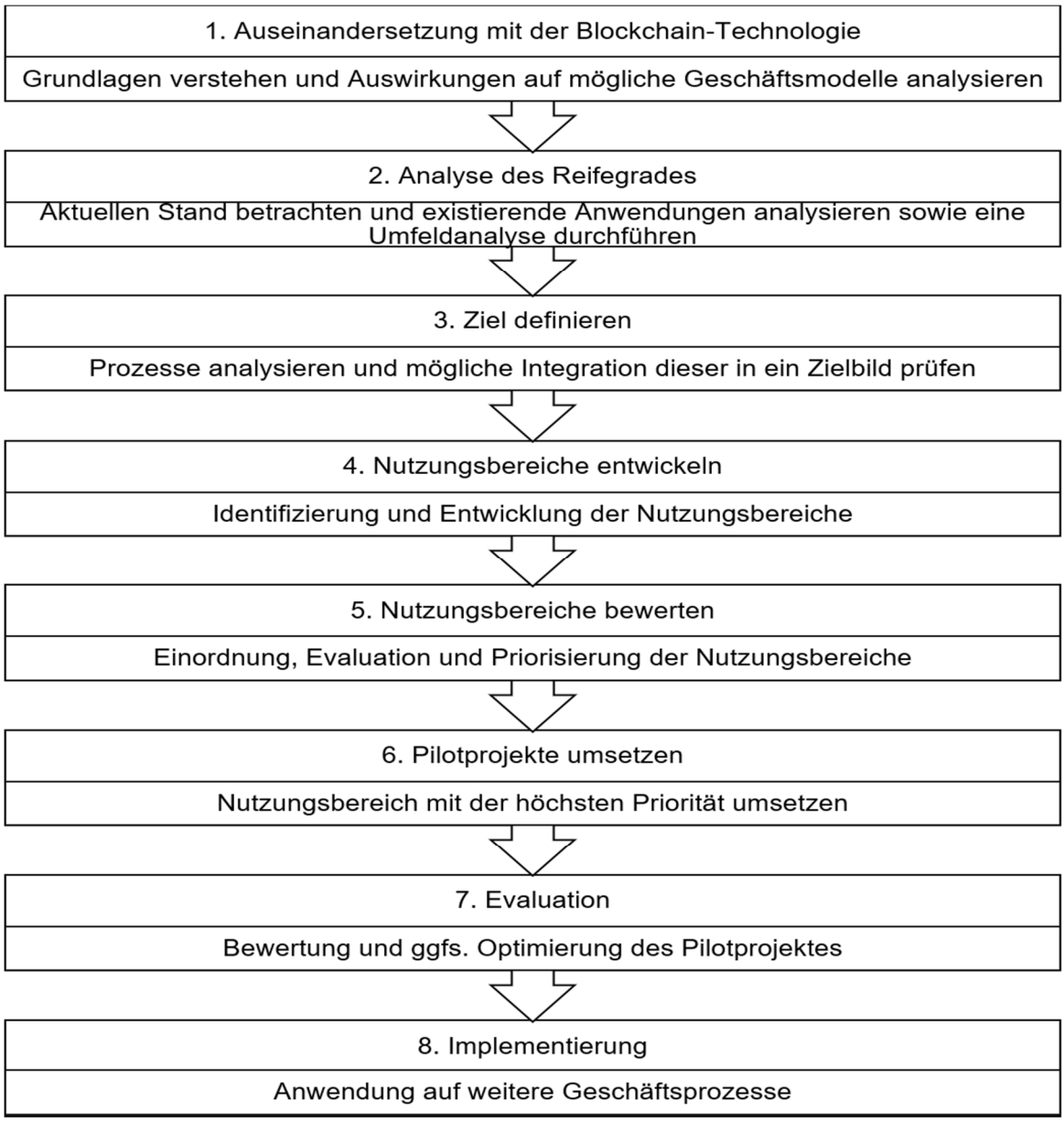

Abbildung 8: Einbindung der Blockchain-Technologie in Unternehmensprozesse[114]

Aufgrund des unausgeprägten Reifegrades der Blockchain-Technologie und den offensichtlichen Herausforderungen, vor welchen potenzielle Anwender stehen, ist es äußerst

[114] Eigene Darstellung in Anlehnung an Fill und Meier 2020, S. 141–145.

wichtig, dass eine strukturierte Vorgehensweise den Einsatz in Unternehmen begleitet und einen Leitfaden für den richtigen Umgang bietet.

4.3 Welcher Ansatz besitzt die bessere Eignung? Private- vs. Public-Blockchain

Um Smart Contracts über eine Blockchain in die Unternehmensprozesse und Produkte einzubringen, stellt sich als erstes die Frage, ob sich eine öffentliche oder eine geschlossene Blockchain besser eignet. Hier müssen die Vor- und Nachteile miteinander verglichen werden. Grundsätzlich besteht die Möglichkeit, eine schon bestehende Blockchain zu nutzen oder eine eigene zu entwickeln. Letzteres ist aber (noch) nicht zu empfehlen, da sie in Sachen Robustheit und Ausfallsicherheit den bewährten und getesteten Blockchains in der Regel nachstehen[115]. Selbstredend muss die Blockchain auch die Möglichkeit anbieten, Smart Contracts einzubinden.

4.3.1 Entscheidungskriterien

Um öffentliche mit geschlossenen Blockchains zu vergleichen, müssen Kriterien vorformuliert werden, anhand derer die jeweilige Eignung festgestellt werden kann. Eine häufig auszumachende Unterteilung ist die in operative und strategische Kriterien, welchen Unterkriterien wie Effizienz, Sicherheit, Hierarchie und Verwaltung zur Seite stehen. Im Folgenden wird diese Unterteilung zur Entscheidungsfindung aufgenommen[116]. Während die Art der Blockchain von den operativen Kriterien abhängig ist, müssen die strategischen Kriterien innerhalb der jeweiligen Institutionen und Unternehmen ausgemacht werden, welche an dem Netzwerk beteiligt werden sollen. Hier geht es allein um den sachlichen und eigenschaftenbezogenen Vergleich der Blockchains.

- **Transaktionseffizienz**

Dem aktuellen Stand der Technik nach, sind geschlossene Blockchains den öffentlichen in einigen Punkten voraus. Ein wichtiger Vorteil ist, dass eine Transaktion nicht von allen Teilnehmern validiert werden muss, was eine höhere Geschwindigkeit und eine potenziell bessere Skalierbarkeit zur Folge hat. So besteht ein direkter Zusammenhang zwischen der Anzahl an Knotenpunkten und der Leistungsfähigkeit des Netzwerkes[117]. Untersuchungen ergaben, dass Blockchains, die auf Basis der Hyperledger arbeiten, welche eine Plattform zum Erstellen von Private-Blockchains darstellt und Smart Contracts aufnehmen kann, eine

[115] Vgl. Fill und Meier 2020, S. 71

[116] Vgl. Thießen 2020, S. 5–6

[117] Vgl. Vukolic 2016, S. 114.

bedeutend höhere Transaktionsdurchlässigkeit haben, als Blockchains auf einer öffentlichen Basis wie Ethereum oder Bitcoin. Ein Netzwerk, welches aus 15 Knotenpunkten bestand, schaffte so 100.000 TPS[118], was ein enormer Vorteil im Gegensatz zu den ca. 20 TPS von Ethereum ist.

- **Sicherheit und Anonymität**

Im Gegensatz zur öffentlichen Blockchain sind die Teilnehmer einer geschlossenen in der Regel bekannt und so kann nachverfolgt werden, wer welche Transaktionen getätigt hat. So ist der Punkt der Anonymität, welcher bei einer öffentlichen Blockchain als Pluspunkt gilt, hier wiederum keiner mehr. Die Tatsache, dass eine zentrale Instanz grundsätzlich die Kontrolle über das Netzwerk hat, könnte hier Anlass für Sicherheitsbedenken geben, denen jedoch durch entsprechende Datenschutzkonzepte begegnet werden kann. Eine Private-Blockchain bietet sich vor allem für Unternehmen an, welche sensible Daten handhaben und die Möglichkeit umgehen wollen, dass Unberechtigte Einsicht erhalten können.

- **Problembewältigung und Korrigierbarkeit**

Da eine geschlossene Blockchain programmtechnisch an besondere Erfordernisse angepasst werden kann, besteht die Möglichkeit, Fehler rückgängig zu machen. Insbesondere im Fall einer eigens aufgesetzten Blockchain bietet sich das an.

[118] Vgl. Kienzler 2016, S. 120.

Schlussbetrachtung

Smart Contracts, in der Form, wie sie in dieser Abschlussarbeit beschrieben werden, sind zweifelsohne eine der interessantesten Begleiterscheinungen der Digitalisierung und insbesondere der vermehrt aufkommenden Distributed Ledger Technologie. Sie stellen eine enorme Weiterentwicklung im Vergleich zum klassischen zentralisierten Datenbankmodell dar.

Neben der Automatisierung, die die Smart Contracts u.a. so attraktiv macht, entwachsen die gewinnbringendsten Eigenschaften von Smart Contracts deren Grundlage, einer Blockchain. Diese ist die eigentliche Innovation und erst mit ihr entfalten Smart Contracts ihr volles Potenzial. Durch die enge thematische Verbindung von Smart Contracts und der Blockchain-Technologie wird ihnen ebenso ein Disruptionspotenzial nachgesagt, wie der Blockchain an sich. Aktuell sind die Herausforderungen jedoch noch zu zahlreich, um an mehr als eine Verwendung bei einfacheren Rechtsgeschäften und weniger komplexen Vorgängen zu denken.

Zudem mag der Begriff Smart Contracts mit zu vielen Erwartungen verbunden sein, da diese Verträge im eigentlichen Sinne nicht selbstständig und intelligent sind, sondern nur einen vorher festgelegten Ablaufplan bzw. Algorithmus abarbeiten und nicht eigene Entscheidungen treffen oder sich ohne äußeres Zutun weiterentwickeln können. So wäre, um überzogene Erwartungen verhindern zu können, eine Bezeichnung wie „automatisierte Handlungsanweisung“ oder ähnliches wohl besser geeignet.

Dennoch besitzen Smart Contracts die Fähigkeit, eine Vielzahl von aktuell noch notwendigen Prozessen, vor allem innerhalb der Finanzwirtschaft, effizienter zu gestalten und eine Vielzahl von Geschäftsabläufen auf das Nötigste zu rationalisieren. So können einzelne Handelsgeschäfte oder Bestandteile dieser, sei es das Überweisen eines Geldbetrages oder das Generieren neuer finanzieller Mittel, durch das Ausschalten einer Vielzahl von Intermediären kostengünstiger und zeitsparender gestaltet werden. Weiterhin wird durch das Einbinden von Blockchain-basierten Prozessen die Transparenz der Entscheidungen und Abläufe erhöht und nachvollziehbarer gestaltet. Zudem setzen Blockchain-basierte Smart Contracts im Bereich der Manipulationssicherheit neue Maßstäbe.

Doch sollten sie nicht als eine Art heiliger Gral der Zukunft der Finanzbranche gesehen werden, denn das sind sie nicht. Zumindest noch nicht. Angefangen bei der noch ausbaubaren Komplexität, über die noch fehlende Vereinheitlichung der Programmierschnittstellen bis hin zu den regulatorischen und rechtlichen Hürden, gibt es zum jetzigen Zeitpunkt noch einige Probleme, welche einer breiteren Nutzung im Wege stehen.

Schlussendlich können Smart Contracts als Innovation nur dann den größtmöglichen Nutzen bringen, wenn alle Parteien, welche an einer erfolgreichen Einbindung interessiert sind, gemeinsame Pläne ausarbeiten, initiieren und nach vorher ausgearbeiteten Handlungsweisen Projekte realisieren. Zudem müssen durch den Staat die Rahmenbedingungen geschaffen werden, damit eine Umsetzung unter Beachtung aller betriebsrelevanter Parameter erfolgreich verlaufen kann.

Literaturverzeichnis

Alun, John (2020): Hong Kong, Thai central banks closer to using Hong Kong, Thai central banks closer to using digital currencies for cross-border payments. Reuters. Online verfügbar unter https://www.reuters.com/article/asia-banks-digital-idUSL4N29R2QO, zuletzt aktualisiert am 10.08.2020, zuletzt geprüft am 10.08.2020.

Antonopoulos, Andreas M.; Wood, Gavin: Mastering Ethereum. Building Smart Contracts and Dapps. Cambridge, LaVergne: O'Reilly Media, Incorporated; Ingram Publisher Services [distributor].

Badev, Anton; Chen, Matthew (2014): Bitcoin: Technical Backround and Data Analysis. Federal Reserve Board. Washington, D.C. Online verfügbar unter https://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf, zuletzt geprüft am 15.08.2020.

Belinky, Mariano; Rennick, Emmet; Veitch, Andrew (2015): The-Fintech-2-0-Paper. rebooting financial services. Banco Santander; Oliver Wyman; Anthemis Grop. Online verfügbar unter https://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf, zuletzt geprüft am 15.08.2020.

Beutelspacher, Albrecht; Neumann, Heike B.; Schwarzpaul, Thomas (2010): Kryptografie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. 2., überarbeitete Auflage. Wiesbaden: Vieweg + Teubner.

BitInfoCharts (2020): Ethereum / Ether (ETH) - Marktpreis, Anzahl der blöcke, Schwierigkeit, Hashrate. Online verfügbar unter https://bitinfocharts.com/de/ethereum/, zuletzt aktualisiert am 17.08.2020, zuletzt geprüft am 17.08.2020.

Blockchain-Technologie (2020). Online verfügbar unter https://www.bafin.de/DE/Aufsicht/FinTech/Blockchain/blockchain_node.html, zuletzt aktualisiert am 31.07.2020, zuletzt geprüft am 31.07.2020.

Boberach, Frank (2016): Reisebank mit Ripple. In acht Sekunden über den Atlantik - Innovationsblog der DZ BANK Gruppe. ReiseBank AG. Online verfügbar unter https://innovationsblog.dzbank.de/2016/09/19/reisebank-mit-ripple-in-acht-sekunden-ueber-den-atlantik/, zuletzt aktualisiert am 16.08.2020, zuletzt geprüft am 16.08.2020.

Borkert, Kristian (2018): Crowdfounding goes Blockchain - Teil 1. In: *IT-Rechts-Berater* 2018 (2/2018), S. 39–43.

Brühl, Volker (2017a): Bitcoins, Blockchain und Distributed Ledgers. In: *Wirtschaftsdienst* 97 (2), S. 135–142. DOI: 10.1007/s10273-017-2096-3.

Brühl, Volker (2017b): Virtual Currencies, Distributed Ledgers and the Future of Financial Services. In: *Intereconomics* 52 (6), S. 370–378. DOI: 10.1007/s10272-017-0706-3.

Burgwinkel, Daniel (Hg.) (2016): Blockchain technology. Einführung für Business- und IT Manager. De Gruyter Oldenbourg. Berlin, Boston: De Gruyter Oldenbourg. Online verfügbar unter http://www.degruyter.com/search?f_0=isbnissn&q_0=9783110487312&searchTitles=true.

Choudhary, Pankaj (2020): Implementation of Hash Tree | C++ | cppsecrets.com. Online verfügbar unter https://cppsecrets.com/users/14811009711546971091051165749575764103109971051084699111109/Implementation-of-Hash-Tree.php, zuletzt aktualisiert am 28.07.2020, zuletzt geprüft am 28.07.2020.

Creer, David; Crook, Richard; Hornsby, Mark; Avalis, Gonzales; Simpson, Mark; Weisfeld, Nick et al. (2016): Proving Etherum for the Clearing Use Case. Emerald Performance Testing Technical Paper 2016. Online verfügbar unter https://emerald-platform.gitlab.io/static/emeraldTechnicalPaper.pdf, zuletzt geprüft am 30.07.2020.

Damm, Christoph (2017): Ein Berliner Bitcoin-Startup könnte die Banken-Branche ins Wanken bringen. Business Insider. Berlin.

Däubler, Wolfgang (2012): Rechtskontrolle von Rating-Agenturen? In: *KJ* 45 (1), S. 18–25. DOI: 10.5771/0023-4834-2012-1-18.

Falazi, Ghareeb; Breitenbücher, Uwe; Daniel, Florian; Lamparelli, Andrea; Leymann, Frank; Yussupov, Vladimir (2020): Smart Contract Invocation Protocol (SCIP): A Protocol for the Uniform Integration of Heterogeneous Blockchain Smart Contracts. In: Schahram Dustdar, Eric Yu, Camille Salinesi, Dominique Rieu und Vik Pant (Hg.): Advanced Information Systems Engineering, Bd. 12127. Cham: Springer International Publishing (Lecture Notes in Computer Science), S. 134–149.

Fill, Hans-Georg; Meier, Andreas (Hg.) (2020): Blockchain. Grundlagen, Anwendungsszenarien und Nutzungspotenziale. 1. Auflage 2020. Wiesbaden: Springer Fachmedien Wiesbaden GmbH; Springer Vieweg (Edition HMD).

Fitch Ratings (2020): Rating Definitions. Online verfügbar unter https://www.fitchratings.com/products/rating-definitions, zuletzt aktualisiert am 05.08.2020, zuletzt geprüft am 05.08.2020.

Fries, Martin; Paal, Boris P. (Hg.) (2019): Smart Contracts. Tübingen: Mohr Siebeck.

Furrer, Vincent; Deck, Klaus-Georg (2020): Das Potenzial von Smart Contracts an einem Beispiel aus der Finanzbranche – Smart Rating. In: Jochen Schellinger, Kim Oliver

Tokarski und Ingrid Kissling-Näf (Hg.): Digitale Transformation und Unternehmensführung. Wiesbaden: Springer Fachmedien Wiesbaden, S. 285–304.

Gentemann, Lukas (2019): Blockchain in Deutschland – Einsatz, Potenziale, Herausforderungen. Hg. v. Bitkom e.V. Bitkom e.V. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/2019-06/190613_bitkom_studie_blockchain_2019_0.pdf, zuletzt geprüft am 07.08.2020.

Haber, Stuart; Stornetta, W. Scott (1991): How to time-stamp a digital document. In: *J. Cryptology* 3 (2), S. 99–111. DOI: 10.1007/BF00196791.

Hahn, Christopher; Wons, Adrian (2018): Initial Coin Offering (ICO). Unternehmensfinanzierung auf Basis der Blockchain-Technologie. 1. Auflage. Wiesbaden: Springer Gabler (essentials).

Handelsblatt (2012): Fehlende Transparenz: Ratingagenturen sollen Urteile besser erläutern. Online verfügbar unter https://www.handelsblatt.com/politik/international/fehlende-transparenz-ratingagenturen-sollen-urteile-besser-erlaeutern/6363076.html?ticket=ST-325924-XZbrXH3YJJcRDoWRTSip-ap5, zuletzt aktualisiert am 05.08.2020, zuletzt geprüft am 05.08.2020.

Heckmann, Dirk; Schmid, Alexander (2017): Blockchain und Smart Contracts. Recht und Technik im Überblick 2017. Online verfügbar unter https://www.vbw-bayern.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Wirtschaftspolitik/2019/Downloads/190509-Blockchain-und-Smart-Contracts_neu.pdf, zuletzt geprüft am 29.07.2020.

Kaulartz, Markus (2016): Die Blockchain-Technologie. In: *Computer und Recht* 32 (7). DOI: 10.9785/cr-2016-0727.

Kaulartz, Markus; Heckmann, Jörn (2016): Smart Contracts – Anwendungen der Blockchain-Technologie. In: *Computer und Recht* 32 (9). DOI: 10.9785/cr-2016-0923.

Kienzler, Romeo (2016): Hyperledger - eine offene Blockchain Technologie. In: Daniel Burgwinkel (Hg.): Blockchain technology. Einführung für Business- und IT Manager. Berlin, Boston: De Gruyter Oldenbourg, S. 111–121.

Long, Monica (2016): Ripple and XRP Can Cut Banks' Global Settlement Costs Up to 60 Percent. Online verfügbar unter https://ripple.com/insights/ripple-and-xrp-can-cut-banks-global-settlement-costs-up-to-60-percent/, zuletzt aktualisiert am 19.08.2016, zuletzt geprüft am 30.07.2020.

Martini, Mario; Weinzierl, Quirin (2017): Die Blockchain-Technologie und das Recht auf Vergessenwerden. Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen. In: *Neue Zeitschrift für Verwaltungsrecht : NVwZ : vereinigt mit Verwaltungsrechtsprechung* 36 (17), S. 1251–1259. Online verfügbar unter

https://www.businessinsider.de/wp-content/uploads/2017/07/bitwala-international-money-transfer-blockchain-technologie.png.

Merkle, R. C. (1987): A Digital Signature Based on a Conventional Encryption Function. In: *Proceedings Advances in Cryptology* 1987.

Merkle, Ralph Charles (1979): Secrecy, authentication, and public key systems. Stanford, Calif. (Technical report / Information Systems Laboratory, Stanford Electronics Laboratories, Stanford University, SEL-79-017).

Moody´s Investors Service (2018): Rating Process. Online verfügbar unter https://www.spglobal.com/ratings/en/about/intro-to-credit-ratings, zuletzt geprüft am 05.08.2020.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. In: *SSRN Journal*. DOI: 10.2139/ssrn.3440802.

Paulus, C.; Matzke, R. (2018): Smart Contracts und Smart Meter - Versorgungssperre per Fernzugriff. In: *Neue Juristische Wochenschrift* 2018 (27), S. 1905–1911.

Pawczuk, Linda; Massey, Rob; Holdowsky, Jonathan (2018): Deloitte´s 2019 Global Blockchain Survey. Blockchain gets down to business. Deloitte Insights. Online verfügbar unter https://www2.deloitte.com/de/de/pages/innovation/contents/global-blockchain-survey.html.

Petrlic, Ronald; Sorge, Christoph (2017): Datenschutz. Wiesbaden: Springer Fachmedien Wiesbaden.

Ploom, Tarmo (2016): Blockchain - wichtige Fragen aus IT-Sicht. In: Daniel Burgwinkel (Hg.): Blockchain technology. Einführung für Business- und IT Manager. Berlin, Boston: De Gruyter Oldenbourg, S. 123–148.

Priem, Randy (2020): Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. In: *Financ Innov* 6 (1). DOI: 10.1186/s40854-019-0169-6.

R3 (2020): History of R3 Blockchain Platform & Corda Enterprise | R3. Online verfügbar unter https://www.r3.com/history/, zuletzt aktualisiert am 10.08.2020, zuletzt geprüft am 10.08.2020.

Redman, Jamie (2016): Microsoft & IBM Declare Blockchain Open for Business. Online verfügbar unter https://news.bitcoin.com/microsoft-ibm-declare-blockchain-open-business/, zuletzt aktualisiert am 17.02.2016, zuletzt geprüft am 04.09.2020.

Ripple (2020): XRP | Ripple. Online verfügbar unter https://ripple.com/xrp#, zuletzt aktualisiert am 03.09.2020, zuletzt geprüft am 03.09.2020.

S&P Global Ratings (2020): Understanding Ratings. Online verfügbar unter https://www.fitchratings.com/products/rating-definitions, zuletzt aktualisiert am 05.08.2020, zuletzt geprüft am 05.08.2020.

Sattler, Andreas (2018): Der Einfluss der Digitalisierung auf das Gesellschaftsrecht. In: *Betriebs-Berater* 2018 (39), S. 2243–2253.

Schacht, Sigurd; Lanquillon, Carsten (2020): Blockchain und maschinelles Lernen. Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren. Berlin: Springer-Verlag GmbH.

Schellinger, Jochen; Tokarski, Kim Oliver; Kisslin-Näf, Ingrid (2019): Digitale Transformation und Unternehmensführung. Trends und Perpektiven für die Praxis. Wiesbaden: Springer Gabler.

Scherk, Johannes; Pöchhacker-Tröscher, Gerlinde (2017): Die Blockchain - Technologieumfeld und wirtschaftliche Anwendungsbereiche 2017. Online verfügbar unter https://www.p-ic.at/uploads/simplex/images/BMVIT%20Dossier%20Blockchain%202017%20FINAL.pdf, zuletzt geprüft am 29.07.2020.

Schlatt, Vincent; Schweizer, André; Urbach, Nils; Fridgen, Gilbert (2016): Blockchain: Grundlagen, Anwendungen und Potenziale. Fraunhofer institute for applied information technology. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf, zuletzt geprüft am 15.08.2020.

Schuster, Philipp; Theissen, Erik; Uhrig-Homburg, Marliese (2020): Finanzwirtschaftliche Anwendungen der Blockchain-Technologie. In: *Schmalenbachs Z betriebswirtsch Forsch* 72 (2), S. 125–147. DOI: 10.1007/s41471-020-00090-5.

Sellnow, Bianca (2020): Smart Contracts sind die Verträge der Zukunft. Online verfügbar unter https://www.hanseaticbank.de/klarmacher/wissen/vertraege-der-zukunft-was-smart-contracts-koennen, zuletzt aktualisiert am 04.08.2020, zuletzt geprüft am 04.08.2020.

SHA-256 hash calculator | Xorbin (2020). Online verfügbar unter https://xorbin.com/tools/sha256-hash-calculator, zuletzt aktualisiert am 28.07.2020, zuletzt geprüft am 28.07.2020.

Siebert, Jan (2015): Ratingagenturen auf den internationalen Finanzmärkten. Ihre Rolle in der Finanz- und Eurokrise. Hamburg: Diplomica Verlag GmbH.

Szabo, Nick (1997): Formalizing and Securing Relationships on Public Networks. In: *First Monday* 2 (9). DOI: 10.5210/fm.v2i9.548.

Tagliaferri, Jerome (2019): Blockchain und maschinelles Lernen – Ein Literaturüberblick. In: Sigurd Schacht und Carsten Lanquillon (Hg.): Blockchain und maschinelles Lernen. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 143–166.

Temperli, Daniel (2018): AXA - Wieso ist Blockchain für Versicherungen so interessant? Online verfügbar unter https://www.axa.ch/de/unternehmenskunden/blog/gruendung-und-innovation/blockchain-versicherungen-schweiz.html, zuletzt aktualisiert am 31.07.2020, zuletzt geprüft am 31.07.2020.

The Linux Foundation (2015): Linux Foundation Unites Industry Leaders to Advance Blockchain Technology. The Linux Foundation. Online verfügbar unter https://web.archive.org/web/20170717193806/https://www.linuxfoundation.org/news-media/announcements/2015/12/linux-foundation-unites-industry-leaders-advance-blockchain, zuletzt aktualisiert am 14.08.2020, zuletzt geprüft am 14.08.2020.

Thießen, Friedrich (2020): Öffentliche vs. Private Blockchains der Finanzwirtschaft 2020. Online verfügbar unter https://www.econstor.eu/bitstream/10419/221762/1/1702836762.pdf, zuletzt geprüft am 06.08.2020.

U.S. Securities and Exchange Commission; Office of Credit Ratings (2020): 2019 Annual Report on Nationally Recognized Statistical Rating Organizations 2020. Online verfügbar unter https://www.sec.gov/files/2019-annual-report-on-nrsros.pdf, zuletzt geprüft am 05.08.2020.

Urban, Nicklas T. (2020): Blockchain for Business. Erfolgreiche Anwendungen und Mehrwerte für Netzwerkteilnehmer identifizieren. Wiesbaden, Germany: Springer Gabler.

VISA Fact Sheet (2020). Online verfügbar unter https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf, zuletzt geprüft am 19.08.2020.

Voshmgir, Shermin (2016): Blockchains, Smart Contracts und das Dezentrale Web 2016. Online verfügbar unter https://www.technologiestiftung-berlin.de/fileadmin/daten/media/publikationen/170130_BlockchainStudie.pdf, zuletzt geprüft am 19.08.2020.

Vukolic, Marko (2016): The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In: Jan Camenisch und Doğan Kesdoğan (Hg.): Open Problems in Network Security. Cham: Springer International Publishing (9591).

Wenzel-Benner, Christian; Dr.-Ing. Wasserrab, Daniel (2015): Kryptographische Hashfunktionen: Historie, Angriffe und aktuell sichere Standards. Online verfügbar unter https://pdfs.semanticscholar.org/b559/5b38e93d53c4db04b33066c11f3a3e81de59.pdf, zuletzt geprüft am 28.07.2020.

White, Lawrence J. (2010): Markets: The Credit Rating Agencies (2). Online verfügbar unter https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.24.2.211, zuletzt geprüft am 05.08.2020.

Wilkens, Robert; Falk, Richard (2019): Smart Contracts. Grundlagen, Anwendungsfelder und rechtliche Aspekte. 1. Auflage 2020. Wiesbaden: Springer Fachmedien Wiesbaden GmbH; Springer Gabler (essentials).

Wirth, Sophie von (2020): So lange brauchen Banken in Deutschland für Überweisungen. Online verfügbar unter https://www.handelsblatt.com/finanzen/banken-versicherungen/zahlungsverkehr-das-sollten-bankkunden-zu-ueberweisungen-wissen/25362764.html?ticket=ST-16489273-4YoJK7fZLMvVilSt3DO4-ap5, zuletzt aktualisiert am 30.07.2020, zuletzt geprüft am 30.07.2020.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Montag, den 21.09.2020

Richard Schmidt