Eine Marktübersicht der Blockchain in der Energie-wirtschaft

Von der Idee zum Geschäftsmodell, von der Technologie zur aktuellen Anwendung

Andreas Corusa
Johannes Predel
Nikolas Schöne

Technische Universität Berlin
Institut für Energietechnik,
Fachgebiet für Energiesysteme

Berlin, August 2020

Autoren
Technische Universität Berlin
Institut für Energietechnik, Fachgebiet Energiesysteme
Andreas Corusa (andreas.corusa@tu-berlin,de)
Johannes Predel (j.predel@campus.tu-berlin.de)
Nikolas Schöne (n.schoene@tu-berlin.de)

Design
Ellery Studio GbR., Berlin
Gaja Vičič, Konzept und Layout
David Ramirez, Infografik

DOI-Nummer
http://dx.doi.org/10.14279/depositonce-10542

Förderkennziffer
03SIN537

Acknowledgement
Dieses Dokument beruht auf Arbeiten, die mit Unterstützung des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des SINTEG-Programms „Schaufenster intelligente Energie - Digitale Agenda für die Energiewende“ im Schaufenster WindNODE erstellt wurden. Es wurde vor seiner Veröffentlichung den WindNODE-Partnern zur Durchsicht und Kommentierung zur Verfügung gestellt. Die hier enthaltenen Ansichten der Verfasser spiegeln nicht notwendigerweise die Ansichten des BMWi oder der übrigen WindNODE-Partner wider.

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

WindNODE

Peer-Review-Paper

Eine Marktübersicht der Blockchain in der Energiewirtschaft

Von der Idee zum Geschäftsmodell, von der Technologie zur aktuellen Anwendung

SINTEG
SCHAUFENSTER INTELLIGENTE ENERGIE

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Publikationen bei WindNODE Die Publikation von Ergebnissen der WindNODE-Projektarbeit durch Verbundpartner, assoziierte Partner und Unterauftragnehmer erfolgt in drei Kategorien, die sich insbesondere in der Abstimmung unter den Partnern, dem Layout und der begleitenden Kommunikation über WindNODE-Kanäle unterscheiden.

Partner-Papers werden innerhalb einer Institution geschrieben, das heißt unilateral erarbeitet. Die entsprechenden Texte sind vor einer Veröffentlichung nicht notwendigerweise mit weiteren WindNODE-Partnern abgestimmt worden. Die Qualitätssicherung erfolgt durch die Autoren/Institution bzw. gegebenenfalls durch ein externes Lektorat. *Partner-Papers* werden im Layout der jeweiligen Institution veröffentlicht.

Peer-Review-Papers sind unilateral erarbeitete Dokumente, die einen WindNODE-internen Qualitätssicherungsprozess in Form eines „Peer Review" durch andere WindNODE-Partner durchlaufen haben. Die Partner haben fachliches Feedback zum Dokument gegeben, das berücksichtigt wurde. *Peer-Review-Papers* werden im ursprünglichen Layout der Institution veröffentlicht und mit einem einheitlichen (türkisen) WindNODE-Schutzumschlag versehen, veröffentlicht.

Signature-Papers werden im Rahmen der WindNODE-Koordinierungskomitees erarbeitet und dienen der übergeordneten Ergebniszusammenführung des Verbundprojekts. In den Koordinierungskomitees findet eine fortlaufende Qualitätssicherung und Abstimmung der Dokumente statt. *Signature-Papers* werden in einem einheitlichen (weißen) WindNODE-Schutzumschlag veröffentlicht.

Vorgelegt von Technische Universität Berlin, Institut für Energietechnik, Fachgebiet für Energiesysteme, Einsteinufer 25, 10587 Berlin

Autoren Andreas Corusa, TU Berlin, Johannes Predel, TU Berlin, Nikolas Schöne, TU Berlin

Dieses Dokument beruht auf Arbeiten, die mit Unterstützung des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen des SINTEG-Programms „Schaufenster intelligente Energie - Digitale Agenda für die Energiewende" im Schaufenster WindNODE erstellt wurden. Es wurde vor seiner Veröffentlichung den WindNODE-Partnern zur Durchsicht und Kommentierung zur Verfügung gestellt. Die hier enthaltenen Ansichten der Verfasser spiegeln nicht notwendigerweise die Ansichten des BMWi oder der übrigen WindNODE-Partner wieder.

Inhalt

Vorwort

Diese Studie wendet sich vor allem an interessierte Leser mit energiewirtschaftlichem Hintergrund, Grundkenntnissen zum Thema Blockchain und Interesse an der Konzeptionierung eines Blockchain-basierten Geschäftsmodells. In erster Linie dient es als Anleitung zur Überprüfung von Geschäftsmodellen und deren Kompatibilität mit einer entsprechenden Blockchain-Lösung. Durch den – in Anlehnung an die technische Konstruktionsweise von Blockchains – modularen Aufbau der Studie ist es auch für technisch weniger versierte Leser verständlich. Unserer Meinung nach war es wichtig die Einstiegsbarriere der Blockchain-Technologie zu senken und in einem Dokument kondensiert auch für diejenigen verfügbar zu machen, die vor der Informationsvielfalt und Komplexität der Technologie zurückschrecken. Im zweiten Teil der Studie zeigen wir die aktuellen Blockchain-Anwendungen in der Energiewirtschaft. Dies kann Anwendern dazu dienen, nach Prüfung des eigenen Geschäftsmodells den Markt nach bereits vorhandenen Lösungen zu durchleuchten.

Zusammenfassung

Eine Blockchain besteht aus ineinandergreifenden Bausteinen. Wir definieren im ersten Teil die technischen Module Protokoll & Code Lizenz, Turing-completeness & Softwarearchitektur, Infrastruktur, sowie Konsensmechanismus. So wird deutlich, warum die Technologie sehr viele Anwendungsmöglichkeiten (in der Energiewirtschaft) bietet. Wir etablieren einen Entscheidungspfad zum schnellen Überprüfen, Einordnen und Vergleichen einer Geschäftsidee bzw. eines Anwendungskonzepts. Damit lässt sich beispielsweise unterscheiden, ob der Zugang zur identifizierten Blockchain-Anwendungen eigenständig oder mit Hilfe eines spezifischen Anbieters, der die Blockchain-Lösung als Service anbietet, erfolgen kann bzw. sollte. Für möglichst flexible Geschäftsmodelle sind dabei insbesondere eine agile bzw. skalierbare Architektur und turing-completeness wichtig.

Der zweite Teil präsentiert eine Marktübersicht von Blockchain-Anwendungen in der Energiewirtschaft. Zu den Ergebnissen zählen: Die Ethereum-Blockchain dominiert, wobei insgesamt die meisten Projekte als Peer-to-Peer Lösungen umgesetzt werden. Aus energiewirtschaftlicher Perspektive ist dabei besonders auffällig, dass heute schon speziell für den Energiesektor zugeschnittene Lösungen verfügbar sind. Allerdings herrscht noch immer eine gewisse Intransparenz. So bieten viele der untersuchten Projekte keine oder deutlich veraltete Information zur eingesetzten Blockchain-Technologie. Dies macht insbesondere eine Abschätzung der Ressourcenintensität der jeweiligen Lösungen schwierig, die jedoch vor allem bei energieintensiven Konsensmechanismen sehr wichtig ist.

Die Rolle der Blockchain in der Energiewirtschaft

1

Auch im Kontext der Energiewirtschaft wird die Blockchain-Technologie lebhaft diskutiert, die ganz offensichtlich für viel mehr als bloß für Kryptowährungen eingesetzt werden kann. Schon heute dient die Blockchain als Grundstein für ein breites Spektrum an technologischen Möglichkeiten und den daraus resultierenden Geschäftsmodellen. Die Energiewirtschaft bietet entlang der gesamten Wertschöpfungskette viele Applikationsmöglichkeiten für Blockchain-Anwendungen. Dies erkennt auch die Bundesregierung und spricht in ihrem Strategiepapier von einem „bedeutenden“ Potenzial der Blockchain in der Energiewirtschaft (BMWi und BMF 2019). Damit schließt sie sich der Meinung etablierter Institutionen der Energiewirtschaft an, wie zum Beispiel der Deutsche Energie-Agentur (dena), der Forschungsstelle für Energiewirtschaft (FfE) oder auch dem Bundesverband der Energie- und Wasserwirtschaft (BDEW) (Ffe 2018a; dena 2019, 2016; BDEW 2017). Alle diese Einrichtungen schreiben der Blockchain in dem ohnehin viel diskutierten Themenfeld der Digitalisierung das

Potenzial zu disruptiven Lösungen zu. Aktuelle Herausforderungen der Energiewende über das gesamte Spektrum der Wertschöpfungskette könnten durch die Blockchain technisch effektiv und anwendungsfreundlich gelöst werden.
Ein mögliches Anwendungsbeispiel ist Produkttracking, beispielsweise im Bereich von Grünstromzertifikaten. Blockchain-basierte Herkunftsnachweise böten den Beteiligten der Wertschöpfungskette die Möglichkeit, Netzentgelte und damit die real anfallenden Stromkosten – nach Ansicht einiger Autoren – „fairer“ zu gestalten (Zeiselmair et al. 2018). Wer Strom aus der Region bezieht, könnte perspektivisch niedrigere Netzentgelte bezahlen, weil er nur lokale Stromnetze nutzt und nationale Netze weniger stark beansprucht. Solch eine „dynamische Netzentgeltregelung“ würde zu dezentralen – und somit zumeist regenerativen – Energieversorgungslösungen anregen. Der Anreiz zu solch einer Reform wird stetig größer. So kommen Jahn et al. (2019) zu dem Schluss, dass die Netzentgelte für Haushaltskunden seit 2016 konstant gestiegen sind. Durch entsprechende Herkunftsnachweise könnte diesem Trend entgegengewirkt werden.
Weiterhin werden Peer-to-Peer Lösungen als ein großes Handlungsfeld für die Blockchain gesehen, wie auch in dieser Studie belegt wird. Bei solchen Peer-to-Peer Plattformen ist es essenziell eine neutrale Instanz für den einzelnen Peer, also den Anwender (z. B. Verbraucher), zu schaffen, die die Einstiegsbarriere durch technologische und operative Unterstützung verringert und überdies die Verantwortung für die Versorgungssicherheit übernehmen kann. Diese Instanz muss gewährleisten, dass während des kleinteiligen Stromhandels der Strombedarf der Kunden zu jeder Zeit gedeckt ist und den

Teilnehmern regulatorische Pflichten, wie beispielsweise das Bilanzkreismanagement, abnehmen. Solche Anwendungen können zukünftig in Quartierslösungen erwartet werden, oder aber auch von großflächig aktiven Energieversorgungsunternehmen adaptiert werden.

1.1 Motivation der Studie

Die Energiewirtschaft steht noch ganz am Anfang der Implementierung

Zwar ist der Blockchain in der Energiewirtschaft technisch ein enormes Potenzial zuzutrauen – dies wird durch die rasante und stetige technologische Entwicklung bezeugt – jedoch bleiben die tatsächlichen Anwendungen in der Energiewirtschaft bislang hinter den Erwartungen zurück. Entsprechend wurde eine deutliche Diskrepanz zwischen erwartetem und tatsächlich genutztem Potenzial der Blockchain beobachtet (BDEW 2017). Aus Sicht der Autoren dieser Studie ist dies nicht ausschließlich auf unreife regulatorischen Rahmenbedingungen zurückzuführen, sondern auch darauf, dass potenzielle Akteure vor der Umsetzung zurückschrecken. Die Anwendung von Kenntnissen hin zu einem marktfähigen Geschäftsmodell auf Blockchain-Basis gelingt bislang oft nicht. Ursächlich dafür sehen die Autoren den zugleich größten Vorteil der Blockchain-Technologie: Ihr modularer Aufbau. Die Technologie besteht aus modularen Bausteinen, deren Zusammenhang nicht trivial zu verstehen ist und in der Literatur auch nur selten konsistent und vollständig erläutert wird. Entsprechend sind potenzielle Marktakteure verunsichert, ob sie die Technologie ihrerseits tatsächlich vollständig durchdrungen haben und Konsequenzen aller Änderungen vorab erkannt wurden. Erschwerend kommt hinzu, dass die Erläuterungen der derzeitigen Blockchain-Plattformanbieter zwecks Übersichtlichkeit nur selten bis in die technischen Einzelheiten ihres Produkts reichen. Dabei ist das Begreifen dieses Konstrukts gerade essenziell, um die geeignete Lösung und den geeigneten Blockchain-Anbieter für das eigene Geschäftsmodell zu finden. Nur dann kann ein Einsatz gelingen.
Ziel der vorliegenden Studie ist es, potenziellen Marktakteuren die Umsetzung ihrer Idee in das reale Blockchain-basierte Marktumfeld zu erleichtern. Dazu wird dem Leser das notwendige technische Verständnis an die Hand gegeben. Die entscheidenden Unterschiede derzeitiger Plattformanbieter, wie beispielsweise Tendermint oder Energy Web Foundation, werden erläutert und visualisiert.
Als Ausgangspunkt dienen dieser Studie bestehende Marktanalysen, die sich mit der Dynamik des Marktes im Hinblick auf den Einsatz der Blockchain beschäftigen. Hierzu hat der BDEW in Zusammenarbeit mit (PWC) im Jahr 2017 erstmalig das „Blockchain-Radar“ für die Branchen Energie und Mobilität, veröffentlicht, in der Absicht, aktuelle Akteure der Energiewirtschaft darzustellen. Dabei ist der Fokus der Studie eine Übersicht der aktiven Akteure geografisch differenziert nach Europa, Amerika sowie dem Rest der Welt. Innerhalb dieser geografischen Cluster werden die jeweilig mittels Blockchain-Technologie gelösten Anwendungen der Akteure skizziert. Dabei wird deutlich, dass die Blockchain-Technologie in der Energiewirtschaft insbesondere für

Peer-to-Peer (P2P) Plattformen eingesetzt wird. Im gesamten Bereich „Mobilität“ (Stand 2017) wurden nur wenige aktive Projekte identifiziert. Einige Monate später veröffentlichten die Autoren eine aktualisierte Version des „Blockchain-Radar“ für das Folgejahr 2018. In der überarbeiteten Version fällt insbesondere bei Betrachtung der Anwendungsfelder die Unterschied zur Vorstudie auf, dass kein Akteur mehr in der Rubrik „Anlagenmanagement“ vertreten ist. Das jüngst veröffentlichte „Blockchain-Radar“ aus dem Jahr 2020 führt im Vergleich zu seinen Vorgängern viele neue Unternehmen und Projekte auf, die sich mit der Blockchain beschäftigen. Der geografische Fokus beschränkt sich in der aktuellen Version des „Blockchain-Radar“ auf Europa, insbesondere auf Deutschland. Um potenziellen Akteuren einen Überblick über bereits existierende Geschäftsmodelle zu ermöglichen, wird auch in dieser Studie eine aktuelle Übersicht der Anwendungen der Blockchain im Kontext der Energiewirtschaft gegeben. Dabei nutzen wir als Ausgangspunkt die bisherigen „Blockchain-Radars“ und ergänzen diese mit einer eigenen Literaturrecherche. Dieser Ansatz ermöglicht es, den dynamischen Charakter des Marktumfelds aufzuzeigen. Ergänzend zum „Blockchain-Radar“ beschreibt die vorliegende Studie sowohl die Veränderungen innerhalb der Anwendungsfelder als auch den Wandel und Weiterentwicklungen der zugrundeliegenden technologischen Besonderheiten der Blockchain. Dies soll es dem Leser ermöglichen, die Konsequenzen technologischer Weiterentwicklungen in der Anwendung zu begreifen und potenzielle zukünftige Trends des Markts und der Anwendungsmöglichkeiten abzuschätzen.

1.2 Aufbau der Studie

Ein zweistufiger Ansatz hilft, Entscheidungen für marktkonforme Lösungen zu finden

Die Studie besteht aus zwei Teilen. In einem ersten Teil wird die grundlegende Struktur der Blockchain-Technologie erläutert. Dabei wird innerhalb der Kapitel 2.1 bis 2.5 scharf zwischen einzelnen Abschnitten der Technologie differenziert, und zwar der *Protokoll & Code Lizenz, Turing-completeness & Softwarearchitektur, Infrastruktur* sowie *Konsensmechanismus*[1].

Vor der Umsetzung einer Idee in ein Geschäftsmodell müssen jedoch zusätzliche Fragen gestellt werden, beispielsweise ob eine eigene kryptographische Währung (*Coin*) benötigt wird, auf eine herkömmliche Währung zugegriffen werden soll oder gar kein Vergütungssystem etabliert werden muss. Um auch solche Fragestellungen einzubeziehen, wird in Kapitel 2.6 ein Entscheidungspfad skizziert, welcher potenziellen Marktakteuren die notwendige Kombination der technologischen Module für das eigene Geschäftsmodell aufzeigen soll. In

1 Da aktuelle Literatur im Bereich der Blockchain-Technologie vor allem auf englischer Sprache verfügbar ist, bedienen sich auch wir vereinzelnd gängiger englischer Fachbegriffe, um Missverständnisse zu vermeiden. Solche Fachbegriffe, englisch wie deutsch, werden aus Übersichtsgründen durch kursive Schrift gekennzeichnet.

dem Entscheidungspfad werden die momentanen Strukturen aktueller Blockchain-Plattformanbieter, wie z. B. Ethereum und der Energy Web Foundation (EWF) hinterlegt.
Im zweiten Teil der Studie, wird in Anlehnung an das „Blockchain-Radar“ eine Übersicht über die Akteure im Bereich der Blockchain in der Energiewirtschaft vorgestellt, differenziert nach Plattformanbieter, geografischer Verortung und Schwerpunkt. Aus einem quantitativen Vergleich zur Vorläuferstudie werden Trends und Entwicklungen abgeleitet und das dynamische Marktumfeld beschrieben. Die Studie umfasst dabei den globalen Kontext und bezieht sich in ihrem Aufbau vornehmlich auf die Ausgabe des „Blockchain-Radar“ aus dem Jahr 2017. Die neuen Erkenntnisse aus dem „Blockchain-Radar“ 2018 sowie 2020 wurden ergänzend berücksichtigt.
Vertiefend werden erkennbare Entwicklungen innerhalb der gewählten Blockchain-Plattform dargelegt und erörtert. Gleiches geschieht für die derzeit vorherrschenden *Konsensmechanismen*. Letzterer Teil wird dabei durch eine Diskussion um die Ressourcenintensität der jeweiligen *Konsensmechanismen* ergänzt.
Die Entwicklungen der Blockchain-Plattformen sowie *Konsensmechanismen* helfen, in Kapitel 4 einen Ausblick in technologische Weiterentwicklungen und daraus resultierenden Trends im Blockchain-basierten Markt zu geben.

Von der Technologie zum Geschäftsmodell

2

Das nachstehende Kapitel erfüllt den Zweck, die Blockchain als Technologie und das Umfeld des potenziellen Marktes der Blockchain in der Energiewirtschaft einzuführen, um einen Transfer von technologischem Verständnis in ein Geschäftsmodell zu ermöglichen. Dazu müssen zunächst grundlegende technologische Aspekte unter Berücksichtigung ihrer Vor- und Nachteile in ihrer Funktion erläutert werden. Alsdann werden Fragen formuliert, mit denen ein potenzieller Marktakteur bei der Entwicklung eines Blockchain-basierten Geschäftsmodells konfrontiert wird. Diese Fragen orientieren sich an den vorab beschriebenen technologischen Erläuterungen. Die Beantwortung dieser Fragen stellt einen Zusammenhang zwischen Technologie und Geschäftsmodell her.

2.1 Die modulare Struktur der Blockchain-Technologie

Erleichtertes Verständnis durch Modularität

Die Blockchain ist eine spezielle Form unter den vielen Ausprägungen der *Distributed-Ledger-Technologien*. *Distributed-Ledger-Technologien* zeichnen sich im Besonderen dadurch aus, dass Daten oder Informationen über Transaktionen innerhalb von Netzwerken bei einer Vielzahl der teilnehmenden Netzwerkakteure dezentral verteilt gespeichert werden. Damit unterscheidet sich die *Distributed-Ledger-Technologie* wesentlich von konventionellen *Centralized-Ledger-Technologien*. Bei diesen dient ein Knoten des Netzwerks als zentrale Einheit, welche alle weiteren teilnehmenden Knoten *(node)* separat koordiniert und verfügbare Daten zentral speichert. Diese diktatorische Struktur, welche mit der zentralen Speicherung und Koordination durch einen Knoten einhergeht, ist bei *Distributed-Ledger-Technologien* nun nicht mehr vorgegeben. Die Blockchain-Technologie bildet somit einen Spezialfall innerhalb der *Distributed-Ledger-Technologien*. Auch sie basiert auf dem Konzept einer dezentralen Speicherung von Daten bei allen teilnehmenden Akteuren eines Netzwerks. Jedoch beinhaltet die Blockchain-Technologie noch weitere essenzielle charakteristische Bestandteile, so skizziert in Abbildung 1.

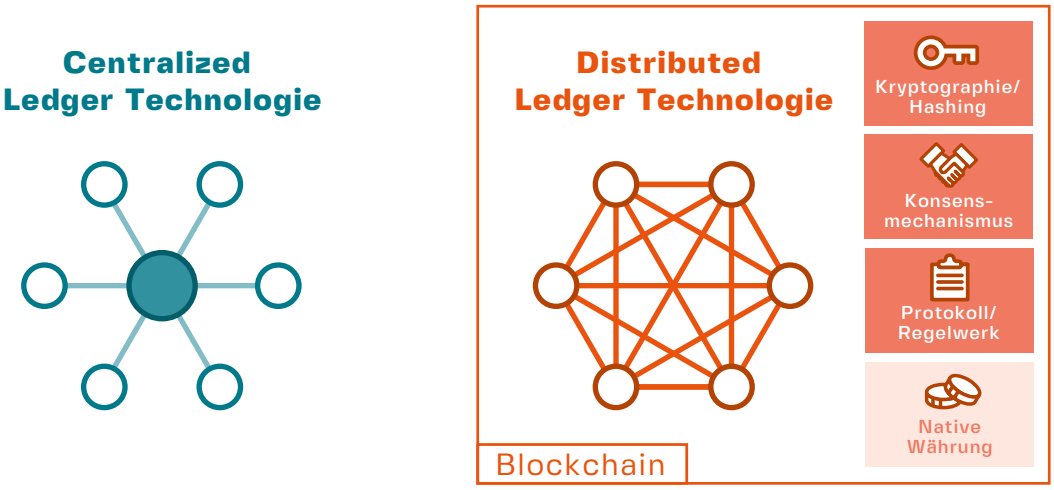

Abbildung 1: Gegenüberstellung der Centralized-Ledger-Technologie zur Distributed-Ledger-Technologie und Spezialform der Blockchain. In Anlehnung an (Ffe 2018b)

Fundamentale Eigenschaft der Blockchain ist, dass keine Daten, die im gemeinsamen Ledger aufgezeichnet wurden, hinterher geändert werden können (*immutability*). Dies heißt, dass kein Teilnehmer eine Transaktion rückwirkend ändern oder manipulieren kann. Transaktionen können also nur korrigiert werden, indem neue, ausgleichende Transaktionen getätigt werden (Gupta 2018). Die Daten oder Transaktionen

sind dabei von allen Teilnehmern des Netzwerks einsehbar. Somit ist garantiert, dass alle Knoten im Netzwerk dieselben Informationen besitzen und sich darauf verlassen können, dass jegliche Informationen, die in einem Ledger erscheinen, mit den Informationen aller anderen übereinstimmen. Das Vertrauen in das System wird somit nicht dadurch gegeben, dass einer zentralen Instanz vertraut wird, sondern durch die Überprüfbarkeit und öffentliche Einsehbarkeit der Informationen für alle Beteiligten (*trustlessness*) (Werbach 2019). Zusätzlich liegt der Blockchain ein kryptographisches Prinzip zu Grunde. Inhalte der kommunizierten Elemente in einem Dokument werden durch einen sogenannten *hashing*-Mechanismus kryptographisch verschlüsselt.

Exkurs: hashing-Algorithmus

Kryptographische *hashing*-Algorithmen sind Funktionen, die eine Zusammenfassung (engl. *digest*) eines Dokuments erstellen. Der *Digest* ist in der Regel eine kurze Zeichenkette, deren Inhalt abhängig von dem verwendeten *hashing*-Algorithmus ist. Ein populäres Beispiel ist der *hashing*-Algorithmus namens SHA256, der bei dem Blockchain-Netzwerk Bitcoin eingesetzt wird. Dieser erzeugt, gemäß einer definierten mathematischen Beziehung, aus einem Dokument beliebiger Größe einen individuellen *Digest* von 64 Zeichen Länge. Die kleinste Änderung am Dokument führt zu einem grundlegend anderen *Digest*. Entsprechend bildet ein *Digest* unverkennbar ein bestimmtes Dokument ab. Im Umkehrschluss ist es aber unmöglich, ein Dokument aus seinem *Digest* zu rekonstruieren. Die *Digests* enthalten dazu schlichtweg zu wenige Informationen, um alle individuellen Inhalte des Originaldokuments abbilden zu können. Der *Digest* erlaubt also durch den Vergleich des *hashes* einer Kopie des Dokuments mit dem *hash* des Originaldokuments zu erkennen, ob der Inhalt des verschlüsselten Dokuments geändert wurde. Auf diese Weise werden kryptographische *hashes* verwendet, um eine gültige Kopie zu verifizieren. (Caetano 2015)

Transaktionsinformationen, welche verschlüsselt in einem Blockchain-Netzwerk ausgetauscht werden, werden regelmäßig in neu generierten Blöcken zusammengefasst und gespeichert. Nachdem ein Block[2] erstellt wurde, stellt sich für Teilnehmer des Netzwerks stets die Frage nach der Korrektheit des Blockinhalts, und ob dieser Block für das Netzwerk „gültig“ ist. Diese Gültigkeit eines Blocks wird geprüft, um Manipulationen oder fehlerhafte Einträge zu verhindern. Die Art und Weise, wie die Gültigkeit der Blöcke verifiziert wird, wird durch den *Konsensmechanismus* festgelegt.
Oftmals ist es Teil der Blockchain-Anwendung, dass zwischen Teilnehmern des Netzwerks Vergütungen fließen. Es ist nicht zwingend

[2] *Jeder gelöste* hash *repräsentiert einen Block, eine Reihe von verarbeiteten Transaktionen, die von allen gültigen Knoten belegt wurden. Die kryptographischen Informationen zu jedem Datensatzblock basieren auf den Informationen, die dem letzten Block zugeordnet sind und einen eindeutigen Zeitstempel enthalten. Die Visualisierungen der Blöcke sehen wie Glieder in einer Kette aus. Daher rührt auch der Begriff “Blockchain”, der auf der Idee einer kryptographisch gesicherten Aufzeichnungskette von Blöcken basiert.*

der Fall, jedoch eine revolutionäre Entwicklung und charakteristische Abgrenzung zu allgemeinen *Distributed-Ledger*-Netzwerken, dass die Netzwerke sich dazu nicht über eine Schnittstelle an herkömmlich gehandelten Fiat Währungen bedienen, sondern eigene native Währungen etablieren. Derartige *Coins* erregten in der Vergangenheit medial große Aufmerksamkeit, da sie in einer Art börslichen Struktur gehandelt werden. Diese soeben beschriebenen neuartigen technologischen Konstrukte bedürfen einer geregelten Koordinierung, um zusammenhängend verwendet werden zu können. Im Unterschied zu *Centralized Ledger Technologien* geschieht diese Koordinierung jedoch nicht durch eine zentrale Instanz, sondern durch ein vorab definiertes Regelwerk, in welchem die Abläufe innerhalb des Netzwerks, so z. B.. auch der zu wählende *Konsensmechanismus*, festgelegt werden. Dieses Regelwerk ist gemeinhin als *Protokoll* bekannt.

Abbildung 2: Module der Blockchain-Technologie

Die eben beschriebenen Bestandteile der Blockchain verdeutlichen bereits den modularen Charakter dieser Technologie. Während die Verschlüsselung (speziell: Kryptographische *hashfunktion*) unbedingter Bestandteil eines jeden Blockchain-Netzwerks ist, sind andere Module optionale Bestandteile.
Zusätzlich zu diesen Blockchain-spezifischen Modulen existieren noch weitere übergeordnete Teile der Netzwerkstruktur, so zum Beispiel die Zugänglichkeit zu dem Netzwerk. Um einen differenzierten Blick auf die Vor- und Nachteile einzelner Ausprägungen technologischer Module und eine bessere, auf den Anwendungsfall bezogene, Analyse zu ermöglichen, werden im Folgenden die einzelnen Module, auf welche entscheidender Einfluss genommen werden kann, näher beleuchtet. Entsprechend der notwendigen Granularität dieser Studie definieren wir die Module *Protokoll & Code Lizenz, Turing-completeness & Softwarearchitektur, Infrastruktur* sowie *Konsensmechanismus* (vgl. Abbildung 2). Weitere Untersuchungen der Blockchain als Software und entsprechende Klassifizierung der Blockchain wird von Labazova et al. (2018) vorgenommen. Weitere Ansätze für eine mögliche Taxonomie finden sich in Wang et al. (2019) sowie Xu et al. (2017).

2.2 Protokoll & Code Lizenz

Das grundlegende Regelwerk der Blockchain

In einem Blockchain-Netzwerk gilt ein übergeordnetes Regelwerk, in welchem Arbeitsabläufe und deren Reihenfolge bestimmt werden. Dieses Regelwerk wird als *Protokoll* bezeichnet. Zu den wesentlichen Operationen, die sich somit je nach *Protokoll* zwischen den verschiedenen Blockchain-Netzwerken unterscheiden können, gehören unter anderem der anzuwendende *hashing*-Mechanismus und der Schwierigkeitsgrad des Validierungsprozesses d.h. die Schwierigkeit des zu lösenden kryptographischen Rätsels im Falle eines *Proof-of-Work Konsensmechanismus* sowie in welcher Weise die Teilnahme an der Validierung vergütet wird (*rewarding*). Entsprechend ist im *Protokoll* auch die Art und Weise, nachdem die Validität eines Blocks durch das Netzwerk (*Konsensmechanismus*) bestätigt wird, festgehalten.
Beispielhaft für ein *Protokoll* sei hierbei auf das von der Firma Tendermint entwickelte Tendermint Core verwiesen (siehe Kapitel 2.6.4 Tendermint). In Tendermint Core ist verankert, welcher *Konsensmechanismus* benutzt wird und auf welche Weise die Kommunikation im Netzwerk geregelt ist. Im Falle von Tendermint Core basiert der *Konsensmechanismus* auf der Lösung eines aus der Literatur bekannten Problems, dem sogenannten *Byzantine Fault Tolerance (BFT) Problem* (Buchman 2016). Ziel dieser Lösung ist es, dass sich ein dezentrales Netzwerk über die Korrektheit einer Anfrage einig wird, unter der Vermutung, dass einige Teilnehmer des Netzwerks schadhafte Absichten verfolgen bzw. nicht in einem vorgegebenen Zeitintervall auf die Anfrage reagieren. Tendermint Core legt dazu „Spielregeln“ fest, wie sich das *Distributed-Ledger*-Netzwerk zu verhalten hat, um einen Konsens zu finden. Dabei wird insbesondere der zeitliche Ablauf der Aktionen festgehalten, welcher in Folge einer bestimmten Aufgabe im Netzwerk zu tätigen ist, die jeweilige Rolle der einzelnen Teilnehmer bei diesen Aktionen, Strafen bei Nichtbeachtung des *Protokolls* oder Abwesenheit während eines bestimmten Zeitintervalls, sowie die Datenstruktur der einzelnen Blöcke. Tendermint bezeichnet dieses Regelwerk selbst als „Peer-to-Peer Netzwerk *Protokoll*“ (Cosmos 2018).
Um nachträgliche Änderungen am Protokoll zu ermöglichen, muss eine existierende Blockchain geteilt werden. Ein neuer, parallel zur initialen Kette existierender Pfad wird geschaffen. Der Prozess dazu wird als *fork* bezeichnet, die koexistierende Blockchain als *side fork*. Man unterscheidet grundsätzlich in zwei Arten von *forks*: den internen *soft forks* sowie den *hard forks*. Bei einem *soft fork* bestehen die validierten Blöcke einer Blockchain nur temporär in einer *side fork*. Nach einer bestimmten Zeit[3] werden diese Abzweigungen wieder konsolidiert, sodass langfristig nur eine gültige Kette besteht (Frankenwald 2019).

[3] *Die Zeit hängt maßgeblich von den nodes im Netzwerk ab und wie lange diese benötigen, um auf die neuen Regeln zu aktualisieren. Erst wenn 51% der Teilnehmer das geänderte Protokoll verstehen und akzeptieren wird die soft fork aufgelöst. Solange es jedoch keine Mehrheit gibt, läuft eine soft fork-Blockchain parallel zur alten.*

Solche *soft forks* werden regelmäßig in dem Netzwerk von Bitcoin beobachtet. *Hard forks* dagegen haben Verzweigungen zur Folge, welche nicht einfach konsolidiert werden können. Diese entstehen, wenn es im Zuge der Anpassung der Blockchain zu Änderungen des *Protokolls* oder des *Konsensmechanismus* kommt. Dies führt zur permanenten Separation zwischen den Knoten, welche das ursprüngliche Konzept verfolgen und denen, welche bereits das aktualisierte Konzept adaptiert haben. Entsprechend der nun koexistierenden *Protokolle* erstellen die jeweiligen Knoten auch unterschiedliche Blöcke, die miteinander nicht kompatibel sind. Folglich bilden sich zwei parallel existierende Blockchains, welche nicht zusammengeführt werden können, bis alle Knoten nach einem einheitlichen Konzept arbeiten. Derartige *hard forks* sind die Basis für die Weiterentwicklung von Ethereum. Ein *hard fork* kann durchaus ein Problem für die Teilnehmer darstellen, die Zahlungsterminals und -schnittstellen erstellt haben, welche nun auf den alten Regeln für Transaktionen basieren. Sie müssen ihre Backend-Software[4] aufrüsten, um kompatibel zur neuen Entwicklung zu bleiben und um mit den neuen Regeln für einen reibungslosen Übergang der eingehenden Abrechnungseinheit (z. B. Bitcoin) sicherzustellen (Dhillon et al. 2017).
Zur Erprobung von Änderungen am Protokoll ohne Durchführung eines *hard forks* kann auch auf sogenannte *Sidechains* zurückgegriffen werden. *Sidechains* bestehen neben der originalen Blockchain, welche in diesem Zusammenhang als *Mainchain* bezeichnet wird. Bei der Gründung einer Sidechain trennt sich ihr Verlauf von der *Mainchain*. Im Gegensatz zum *fork*, kann sie jedoch zu einem späteren Zeitpunkt wieder mit der *Mainchain* verknüpft werden. Solange sie getrennt sind, haben beide keinen Einfluss aufeinander, sodass Änderungen an der Sidechain vorgenommen werden können, ohne die Funktionstüchtigkeit der *Mainchain* zu gefährden (Back et al. 2014). Die Verknüpfung erfolgt durch einen Transfer von *Coins* auf die Sidechain (Singh et al. 2020). Bei der Zusammenführung zu einem späteren Zeitpunkt, also die Verknüpfung an einen zukünftigen Block der *Mainchain*, können die *Coins* wieder zurückgetauscht werden. Die Kosten zur Erprobung neuer Eigenschaften werden durch diese Herangehensweise reduziert (Johnson et al. 2019).

Die Blockchain wird vor allem als Open-Source entwickelt, sodass der Quellcode frei zugänglich ist. Dies verringert den Ressourceneinsatz für die Entwicklung, reduziert jedoch auch die Selbstbestimmung und Individualität im Hinblick auf das Protokoll. Die *Code Lizenz* spiegelt daher auch die Anforderungen an eigene Anpassungen wider. Somit sind *Protokoll* und Quellcode miteinander verbunden und nur schwer voneinander trennbar.

[4] *Die Backend-Software ist die Software, welche näher am System ist und sich um die Verarbeitung der Daten kümmert.*

2.3 Turing-completeness und Softwarearchitektur

Gestaltungsmöglichkeiten der Applikationen werden zugänglicher und flexibler

Die beiden wohl bekanntesten Blockchain-Netzwerke sind das Bitcoin- und das Ethereum-Netzwerk. Wie in nachstehendem Kapitel 2.6 verdeutlicht wird, ist der Aufbau der beiden Netzwerke beinah gleich. Jedoch unterscheiden sie sich in einem wesentlichen Punkt, mit der Folge, dass Ethereum in der Energiewirtschaft genutzt wird, um Geschäftsmodelle zu entwickeln, Bitcoin jedoch keinerlei Anwendung findet.
Im Unterschied zu Bitcoin ist es bei Ethereum möglich, Programme auszuführen. Ermöglicht wird dies durch die sogenannte „*Ethereum Virtual Machine*“ *(EVM)*, eine Art virtuellem Computer. Die *EVM* ist auf jedem Knoten vorhanden, der am Validierungsmechanismus teilnimmt. Die *EVM* ist, wie ein Computer auch, in der Lage, Programmcodes auszuführen (Buterin 2013). Computer und Programmiersprachen, die in der Lage sind, jegliche Berechnungen durchzuführen, die auch von einer *Turing Machine* durchgeführt werden können, werden als *turing-complete* bezeichnet. Dieser Begriff ist abgeleitet aus den Arbeiten von Alan Turing aus dem Jahr 1936, welcher in seiner Arbeit eine Maschine (genannt *Turing Machine*) vorstellt. Die *Turing Machine* ermöglicht es, jedes Problem zu lösen, welches sich durch berechenbare Zahlen darstellen lässt (Singh 2019). Als berechenbare Zahlen *(computable numbers)* bezeichnet Turing hierbei „alle reellen Zahlen, deren Ausdrücke als Dezimalzahl mit endlichen Mitteln berechenbar sind“ (Turing 1937). Vereinfacht ausgedrückt kann *turing-completeness* also als eine Art „Zertifikat“ gesehen werden, mit dem bestätigt wird, dass Berechnungen durchgeführt und somit Programme ausgeführt werden können. Bei einer *Turing Machine* geschieht dies unter der Annahme, dass genügend Zeit und Rechenkapazität zur Verfügung steht. Durch die Eigenschaft der *turing-completeness* ist es also möglich, auf der Ethereum-Blockchain Programmcode auszuführen. Im Falle von Ethereum kommen die Programmiersprachen Solidity und Serpent zum Einsatz. Beide sind *turing-complete* und vergleichbar mit JavaScript bzw. Python (Wang 2017). Die Arbeit von Entwicklern wird dadurch erheblich vereinfacht und die Programmierung von Blockchain basierten Lösungen anwendungsfreundlicher. Im Vordergrund der Entwicklungen stehen Applikationen, also Programme, die für den Endnutzer gedacht sind. Im Falle von Blockchain spricht man von *decentralized Applications (dApps)* (Chen 2018). Alle Blockchain Plattformen, welche *dApps* anbieten, sind also *turing-complete*. Dies gilt beispielsweise auch für Energy Web Chain, Hyperledger Fabric und Tendermint.
Im Gegensatz zu den genannten Blockchain-Plattformen basiert

Bitcoin auf Bitcoin Script. Im Vergleich zu Solidity und Serpent ist diese Programmiersprache nicht *turing-complete*, sodass auch keine Berechnungen durchgeführt werden können, die nicht schon zvorher in der Programmiersprache verankert sind. Bitcoin ist daher nicht *turing-complete* (Singh 2019; Allen 2017).

Sind die grundsätzlichen Voraussetzungen für das Ausführen von Programmen und Applikationen auf der Blockchain durch die *turing-completeness* gegeben, gilt es noch zu verstehen, ob sich diese auf der bestehenden Blockchain ausführen lassen oder ob dazu Modifikationen an der *Infrastruktur* oder dem *Konsensmechanismus* nötig sind. Dies wird durch die *Softwarearchitektur* beschrieben.
Durch die *Softwarearchitektur* wird entschieden, ob zukünftig weitere Applikationen auf der Blockchain ausgeführt werden können, ohne hierbei die *Infrastruktur* oder den *Konsensmechanismus* ändern zu müssen. Anbieter von Blockchain-Plattformen bieten den Nutzern die Möglichkeit, Applikationen mittels sogenannter *Software Development Kits (SDKs)* auf ihrer Blockchain zu schreiben. Die *SDKs* stellen sicher, dass die Applikationen mit der zugrunde liegenden Blockchain kompatibel sind und den Anforderungen des *Protokolls* genügen. Ebenso gilt, dass spätere Änderungen in der *Infrastruktur* oder im *Konsensmechanismus* keinen negativen Einfluss auf die Funktionstüchtigkeit der Applikation haben. In einem solchen Fall, in dem die Applikationsebene vom *Konsensmechanismus* und der *Infrastruktur* getrennt ist, spricht man von einer polylithischen (*polylithic*) Architektur (Tasca und Tessone 2017). Eine polylithische Architektur ermöglicht es, dass spätere Anpassungen an der Infrastruktur oder dem *Konsensmechanismus* keinen Einfluss auf die Lauffähigkeit der Applikation haben.
Der gegenteilige Fall, wird als monolithisch (*monolithic*) bezeichnet (Tasca und Tessone 2017). Eine monolithische Architektur bietet sich also für einen potenziellen Nutzer dann an, wenn er seine Applikation auf einer bestehenden Blockchain ausführen möchte. Er geht hierbei jedoch das Risiko ein, dass bei Änderungen der Blockchain seine Applikation möglicherweise nicht mehr funktioniert. Eine polylithische Architektur dagegen ist vorteilhaft, wenn neue Applikationen kreiert werden sollen, ohne dabei jedoch vollständig in die Blockchain eingreifen zu müssen. Die Blockchain-Plattform selbst kann somit als eine Art Service für den jeweiligen Anwender gesehen werden und kann sich vollständig auf die Entwicklung der gewünschten Applikation konzentrieren. Somit müssen keine Ressourcen aufgewendet werden, um die gesamte Blockchain zu modifizieren.
Weitere Trennungen sind möglich. Hyperledger Fabric bietet nicht nur die Möglichkeit, die Applikationsebene von der *Infrastruktur* zu trennen, sondern baut sogar den *Konsensmechanismus* modular auf. Je nach Anwendungsfall kann also der *Konsensmechanismus* angepasst werden.

2.4 Infrastruktur

Die Infrastruktur definiert den Zugang und die Rechte der Teilnehmer im Netzwerk

Die Zugriffsrechte auf Netzwerkdaten sowie die Rechte für andere Aktivitäten der Teilnehmer eines verteilten Netzwerks, wie ein Blockchain-Netzwerk, können bei dessen Gründung definiert werden und so die Infrastruktur des Netzwerks grundlegend festgelegt werden. Abbildung 3 fasst die unterschiedlichen Ausgestaltungen zusammen. So kann schon die bloße Teilnahme am Netzwerk für äußere Akteure bereits beschränkt sein; man spricht in diesem Fall von einem privaten (*private*) Netzwerk. Dies bedeutet eine Einschränkung im Grundprinzips einer *Distributed-Ledger-Technologie*, da der Ledger nun nicht mehr öffentlich, sondern nur einer oder mehreren zentralen Instanzen zugänglich ist (Ffe 2018b). Private Blockchain-Netzwerke eignen sich somit zum Beispiel für unternehmensinterne Anwendungen, in denen nur eine auserwählte Gruppe Zugang zu bestimmten Daten erhalten soll. Eine mögliche Anwendung ist, dass unternehmensintern eine private Gruppe von Teilnehmern gemeinsame Buchhaltung führen soll.

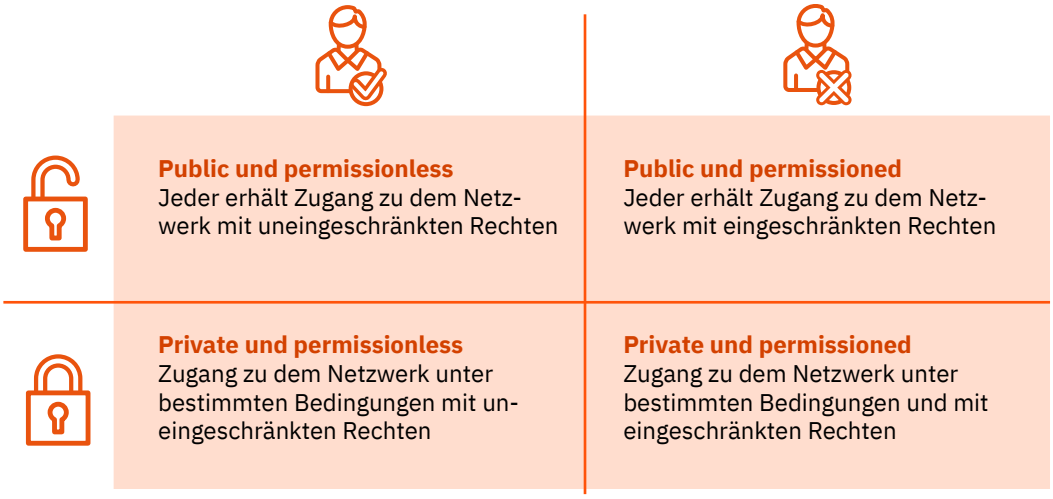

Abbildung 3: Mögliche Konstellationen der Blockchain-Netzwerk Infrastruktur. Nach (Ffe 2018b)

Eine Sonderform der privaten Blockchain bildet die *consortium*-Blockchain, die konsortial (*consortial*) aufgebaut ist. Die Aufgabe der zentralen Instanz zur Haltung des Ledgers und Validierung ist hier nicht auf eine juristische Person beschränkt, sondern auf ein Konsortium innerhalb des Netzwerks aufgeteilt.
Der gegenteilige Fall zu einem privaten Netzwerk, also ein Netzwerk, in dem keinerlei Restriktionen hinsichtlich der Teilnahme herrschen, wird als öffentliche (*public*) Infrastruktur bezeichnet. Die uneingeschränkte Expansion derartiger Netzwerke ist Fluch und Segen zugleich.

[5] *Validatoren dienen zur Überprüfung der Transaktionen gemäß des jeweils gewählten Konsensmechanismus (siehe nächstes Kapitel)*

Aufgrund der hohen Redundanz von Knoten und Validatoren[5] erhöhen sich Sicherheit und Verfügbarkeit des Netzwerks. Jedoch erschwert dies Änderungen an der Blockchain. Zum Beispiel zwecks Verbesserungen, aber auch um einen potenziellen Missbrauch zu verhindern, ist eine Umsetzung der Veränderungen, verglichen zu kleineren privaten Netzwerken, aufgrund des gültigen Mehrheitsprinzips oft erschwert (Ffe 2018b; M. Blederbeck 2016).
Neben dem allgemeinen Zugang zum Netzwerk bestimmt die Infrastruktur die Rechteverteilung innerhalb des Netzwerks. Sie bestimmt explizit, ob es allen Akteuren erlaubt ist am zentralen Validierungsmechanismus von Blöcken bzw. Daten teilzunehmen (*permissionless*) oder ob nur bestimmte Akteure dazu befähigt sind (*permissioned*).

Erfolgt ein Austausch der Daten neben den Mitgliedern auch mit anderen Blockchains spricht man von Intraoperabilität (*Intraoperability*) (Tasca und Tessone 2017). Das von Tendermint entwickelte Cosmos bietet beispielsweise die Möglichkeit solcher Kommunikation zwischen zwei Blockchains, ohne dass hierfür die Blockchains zusammengelegt werden müssen. Teilnehmende Blockchains werden dazu über sogenannte *Hubs* an Cosmos angeheftet. Die Blockchains können dadurch zwar untereinander kommunizieren, sind jedoch individuell entsprechend ihrer gewünschten Problemlösung einsetzbar.
Eine weitere Schnittstelle stellt die Interoperabilität (*Interoperability*) dar. Interoperabilität bezeichnet die Fähigkeit einer Blockchain, mit Systemen außerhalb von Blockchain-Netzwerken zu kommunizieren (Tasca und Tessone 2017). Beispielsweise können Windkraft- oder Photovoltaikanlagen an die Blockchain angeschlossen sein, die ihre Daten übermitteln. Für eben solche Kommunikationszwecke hat die EWF die Energy Web Link entwickelt. Energieerzeugungsanlagen werden dabei Teil des Netzwerks, indem sie eine eigene digitale Identität bekommen und befähigt werden mit der Blockchain zu kommunizieren.

2.5 Konsensmechanismus

Es gibt viele Möglichkeiten eine Einigung im Netzwerk zu erreichen

Der *Konsensmechanismus* ist die zentrale und kritische Funktion der Blockchain. Zur Einordnung: Die medial präsente Diskussion um den Stromverbrauch von Blockchain-Netzwerken bezieht sich ausschließlich auf den *Konsensmechanismus* des Netzwerks, nicht auf andere Bereiche der Blockchain (vgl. Kapitel 3.2.4 Entwicklung in den Konsensmechanismen: Die Notwendigkeit zur Anpassung). Er bestimmt, wie sich die Akteure eines Netzwerks auf die Gültigkeit eines Blocks einigen und somit eine allgemein gültige Version der Blockchain für das gesamte Blockchain-Netzwerk schaffen. Ausgehend vom zuerst eingeführten *Proof-of-Work (PoW)* haben sich in den vergangenen Jahren verschiedenste alternative *Konsensmechanismen* etabliert. Die populärsten unter diesen sind der *Proof- of-Stake (PoS)* und der *Proof-of-Authority (PoA) Konsensmechanismus*. In der jüngeren Historie werden allerdings auch weitere Alternativen, vor allem *der Practical Byzantine Fault Tolerance (PBFT), Delegated Proof-of-Stake (DPoS), Proof-of-Elapsed-Time (PoET)* sowie der *Ripple*-Mechanismus als erfolgversprechend beschrieben. Diese Studie beschränkt sich auf die erst genannten vier *Konsensmechanismen*, da diese in der Literatur und in der Praxis besonders viel verwendet und beschrieben werden.

2.5.1 Proof-of-Work (PoW)

Grundidee des *PoW* ist es, dass ein Teilnehmer eines Netzwerks einen physischen Aufwand betreiben und nachweisen muss, um am Validierungsprozess teilnehmen zu können. Der Aufwand des jeweiligen Teilnehmers (hier: *miner*[6]) ist dabei Rechenleistung, die dazu genutzt wird, ein kryptographisches Rätsel zu lösen. Dessen gültige Lösung wird dazu benötigt, Informationen aus anstehenden Transaktionen und dem vorgehenden Block in einem neuen Block zu schreiben und diesen mit den vorherigen Blöcken zu verknüpfen. Der Prozess des Lösens, einschließlich des Validierens des kryptographischen Rätsels, wird auch als *mining* bezeichnet (Ffe 2018b).

Als Kompensation für die erbrachte Rechenleistung („*hashing-power*"), welche zur Ausführung der Rechenoperationen der Rätsellösung notwendig ist, erhält derjenige Knoten, welcher als erstes die valide Lösung des Rätsels errechnet, eine fest definierte (monetäre) Gegenleistung sowie die Transaktionsgebühr jeder in diesem Block validierten Transaktion.

[6] *Während alle Knoten helfen, das Bitcoin-Netzwerk aufzubauen, können einige Knoten sich dafür entscheiden, nach neuen Bitcoins zu „suchen". Diese Knoten werden dann miner genannt. Dabei wird verschiedene Hardware eingesetzt, die von CPU und GPU-Lösungen bis hin zu speziell für Kryptowährungen eigens entwickelter Hardware (z. B.. Antminer) reicht*

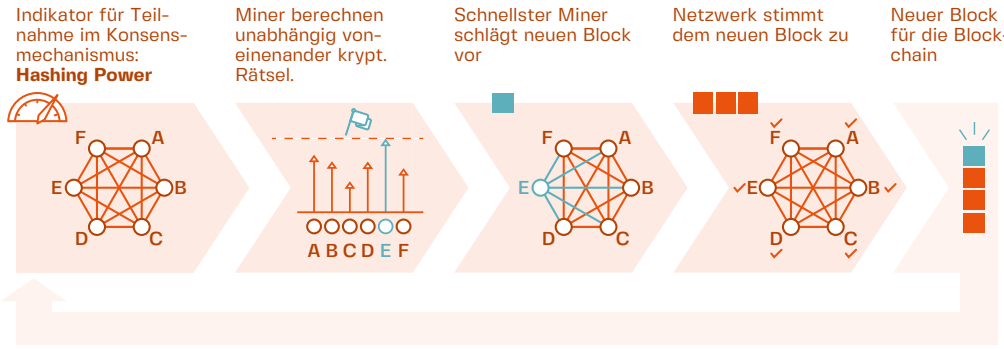

Abbildung 4: Funktionsschema des *Proof-of-Work Konsensmechanismus*

Für den Fall, dass mehrere Akteure gleichzeitig die gültige Lösung des Rätsels finden und in der Folge mehrere parallele Ketten entstehen, gilt der Grundsatz, dass immer die längste Blockkette als gültige Version vom Netzwerk akzeptiert wird. Die Kette, für die als nächstes eine Blocklösung gefunden wird, wird sich in der Folge also behaupten (Ffe 2018b). Abbildung 4 stellt dar, dass die *miner* während der Berechnung im gegenseitigen Wettbewerb stehen. Durch diese grundlegende Struktur, in der private Aufwendungen als Glaubwürdigkeitsnachweis ausreichen und von einer weiteren Authentifizierung abgesehen werden kann, eignet sich der *PoW-Konsensmechanismus* vor allem für öffentliche (*public*) *Infrastrukturen*, in denen eine große Anzahl unabhängiger Akteure teilnimmt und keine Vertrauensbasis zwischen den Knoten besteht *(trustless)*. Wie im Kapitel 3 aufgezeigt wird, sind derartige öffentliche *Infrastrukturen* im Energiesektor jedoch nur bedingt attraktiv. Die Sicherheit eines *PoW*-basierten Netzwerks korreliert positiv mit der Größe des Netzwerks. Um die Validierung oder Blöcke eines Netzwerks manipulieren zu können, bedarf es mindestens 51% der gesamten Rechenleistung, sogenannte *miningpower*, des Netzwerks. Je größer ein Netzwerk wird, desto höhere Ausgaben in physische Assets müssen getätigt werden, um 51% der *miningpower* zu besitzen und schadhaft in das Netzwerk eingreifen zu können (Ffe 2018b). Entsprechend eignet sich der *PoW-Konsensmechanismus* vor allem für Netzwerke mit einer hohen Teilnehmeranzahl. Die Kosten für eine solche „51% Attacke“ können für populäre Blockchain-Netzwerke u.a. auf der Website „Crypto51“ eingesehen werden. Für das Bitcoin Netzwerk belaufen sich die Kosten für einen Angriff pro Stunde, Stand Februar 2020, zum Beispiel auf etwa $800.000 (Crypto51 2020).
Ein weiterer Kritikpunkt ist die Ressourcenintensität des *PoW-Konsensmechanismus* (A. de Vries 2018; Reetz 2019). Da alle *miner* in einem Wettbewerb zum Lösen des kryptographischen Rätsels, der sogenannten *hash calculation*, stehen, führt dies zu einem erheblichen Einsatz von Rechenleistung. Diese Rechenleistung geht mit entsprechend hohem Stromverbrauch einher (vgl. Kapitel 3.2.4 Entwicklung in den Konsensmechanismen: Die Notwendigkeit zur Anpassung).

2.5.2 Proof-of-Stake

Um die Strom- und Ressourcenintensität des Validierungsprozesses zu verringern, wurde der *PoS-Konsensmechanismus* entwickelt. Anstelle eines Rechenwettbewerbs wird per gewichtetem Zufall abwechselnd ein Akteur des Netzwerks gewählt, welcher die fällige Transaktion bearbeitet und einen neuen Block erstellt.

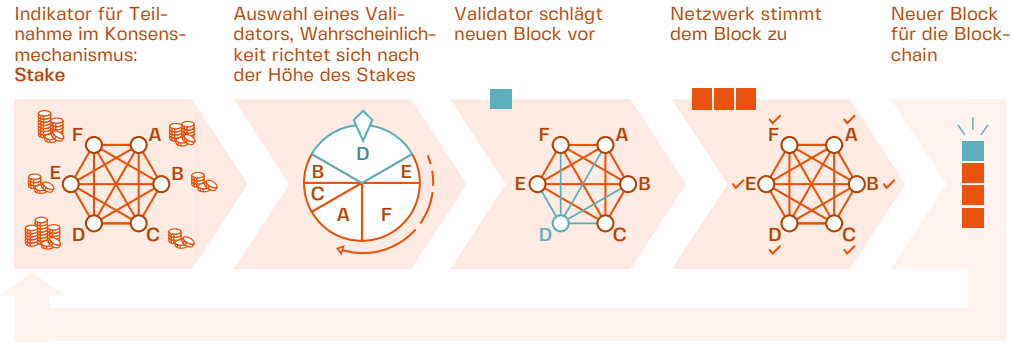

Abbildung 5: Funktionsschema des Proof-of-Stake *Konsensmechanismus*

Vertrauen in die Glaubwürdigkeit des jeweiligen Akteurs wird dadurch geschaffen, dass dieser zwar nicht in Hardware und Strombezugskosten investieren muss, jedoch durch Hinterlegung eines Pfands (*Stake*) auf einem Konto (*Wallet*)[7] ein monetäres Risiko eingehen muss, um am Validierungsprozess teilnehmen zu dürfen. Wie Abbildung 5 skizziert, steigt die Wahrscheinlichkeit für die Auswahl eines Knotens zur Durchführung der Validierung, je höher sein *Stake* ist. Falls ein Akteur Missbrauch betreibt, wird dessen hinterlegter *Stake* gelöscht (Ffe 2018b). Dieser Konsens erlaubt, dass deutlich weniger Berechnungen für Transaktionen benötigt werden und der notwendige Stromeinsatz zur Validierung des Blocks deutlich verringert werden kann. So geht Vitalik Buterin, Gründer des Ethereum Netzwerks, davon aus, dass der Energieverbrauch des Netzwerks nach dem Umstieg von *PoW* auf *PoS* innerhalb der *Casper* Implementierung um 99 % fallen wird (P. Fairley 2019). Bei einer *PoS* basierten Blockchain ist ebenfalls vorteilhaft, dass die Gefahr von 51% Attacken sinkt, da ein manipulierender Akteur eine Marktmacht von 51% nur durch das Erwerben von 51% aller vorhandenen *Coins* erreichen könnte, welches im Allgemeinen von steigenden Preisen begleitet werden würde (V. Vavilov et al. 2015) und ihn in der Folge ein Angriff, durch den Verlust seines Pfandes (*Stakes*) selbst massiv schädigen würde (Buterin 2016).

Ein verwandter Mechanismus, der *Delegated Proof-of-Stake* erlaubt die demokratische Abstimmung all jener Teilnehmer, die *Tokens*[8] an der Blockchain halten. Die Anzahl der *Tokens* entspricht der Menge ihrer Stimmrechte. Diese können im Netzwerk dazu genutzt werden, für einen bestimmten Validator zu wählen, welcher für die Erstellung und Validierung des neuen Blocks zuständig ist.

[7] *Eine Wallet ist ein Konto für das Verwahren von Kryptowährungen. Statt eines Bankkontos besteht die Adresse des Wallets aus einer Kette aus Zahlen und Buchstaben.*

[8] *Ein Token ist eine Art digitales Asset, das auf einer vorhandenen Blockchain aufgebaut ist.*

2.5.3 Proof-of-Authority

Im Rahmen der konsortialen (*consortial*) *Infrastrukturen*, welche ohnehin nur einer auserwählten Menge an Akteuren zugänglich ist, wurde der *PoA-Konsensmechanismus* entwickelt. Leitgedanke ist, dass nur eine bestimmte Anzahl von Akteuren, sogenannte „*authorities*“, das Recht zur Validierung von Blöcken erhalten und die Blockchain somit fortführen können. Die Teilnahme am Netzwerk mit dieser Aufgabe ist also *permissoned*, während die Nutzung der Blockchain immer noch frei zugänglich gestaltet werden kann. Die Identität dieser *authorities* ist dem Netzwerk bekannt, sodass das Vertrauen des Netzwerkes auf der Reputation der *authority* beruht. Ein schadhaftes Verhalten gegenüber dem Netzwerk würde entsprechend den Ruf der *authority* schädigen (POA Network 2017). Jeder der berechtigten Akteure ist abwechselnd an der Reihe einen Block vorzuschlagen, dessen Korrektheit von einer Mehrheit der übrigen *authorities* bestätigt werden muss. Auch dieser Mechanismus dürfte, den Energieverbrauch erheblich zu reduzieren. So gibt die EWF beispielsweise einen um den Faktor 2 bis 3 geringeren Energieverbrauch bei gleichzeitiger Steigerung der Performance an im Vergleich zur *PoW*-Anwendung des Ethereum-Netzwerks (energy web foundation 2019).

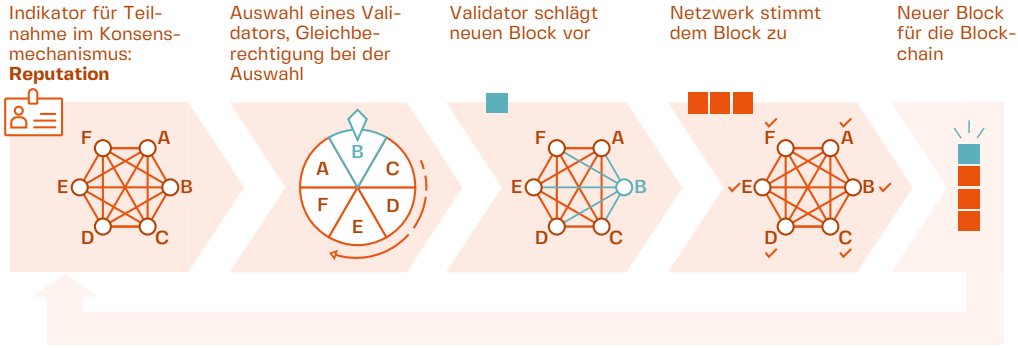

Abbildung 6: Funktionsschema des Proof-of-Authority *Konsensmechanismus*

2.5.4 Practical Byzantine Fault Tolerance

Bei der Verwendung des *Practical Byzantine Fault Tolerance (PBFT) Konsensmechanismus* werden die Akteure des Netzwerks sukzessive dazu aufgefordert, eine anstehende Transaktion durchzuführen und einen Block zu erstellen. In mehrrundigen Abfragen werden einige validierungsberechtigte Akteure befragt, welchen Block sie präferieren, wie in nachstehender Übersicht erläutert und in Abbildung 7 visualisiert (basierend auf Khullar 2019).

1. Die Knoten führen untereinander Transaktionen aus. Jeder Knoten erstellt daraus einen Pool an Transaktionen.
2. Nach einer bestimmten Zeitspanne einigt sich das Netzwerk auf einen sogenannten *Proposer*. Der *Proposer* bündelt Transaktionen in dem Netzwerkpool in einem Block und sendet diesen mit einer „*Pre-prepare Message*“ an andere Knoten. Diese Knoten wiederum schicken ihrerseits eine Message an andere Knoten. Sobald ein Knoten eine bestimmte Anzahl an *Pre-prepare Messages* erhalten hat, wechselt sein Status zu *Pre-prepared*.
3. Die *Pre-prepared* Knoten überprüfen den Block, welcher vom *Proposer* erstellt und an das Netzwerk geschickt wurde. Sofern sie dem Block zustimmen, senden sie eine *Prepare Message* an weitere Knoten des Netzwerks. Eine Zustimmung erfolgt nach Abgleich der vorgeschlagen Transaktionen mit dem eigenen Pool an Transaktionen. Auch hier ändern sie ihren Status nach einer bestimmten Anzahl von Nachrichten zu *Prepared*.
4. Die *Prepared* Knoten senden im Anschluss eine *Commit Message*, mit welcher sie dem Netzwerk mitteilen, dass sie bereit sind, den Block an die vorhandene Blockkette anzuhängen. Wenn genügend *Commit Messages* bei einem Knoten angekommen sind, fügt er den Block der Kette hinzu und ändert seinen Status zu *Final Committed*.
5. Ein *Final Committed* Knoten ist dann verfügbar für eine neue Runde nach gleichem Schema.

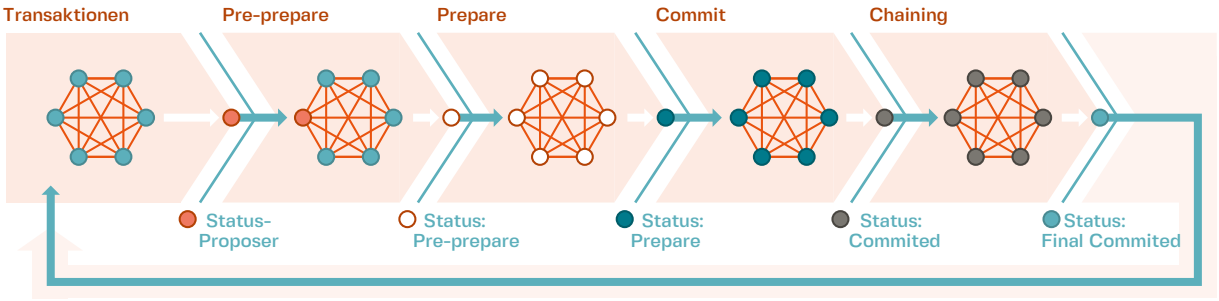

Abbildung 7: Funktionsschema des Practical *Byzantine Fault Tolerance Konsensmechanismus*

Durch die rundenbasierte Konsensfindung können fehlerhafte oder manipulierte Blöcke keinen Zuspruch erhalten, sofern nicht eine bestimmte Anzahl an Teilnehmern im Netzwerk dem Block zustimmt. Der *PBFT* setzt voraus, dass alle Akteure des Netzwerks miteinander in Verbindung stehen, bzw. ihre Informationen untereinander austauschen können. Der *PBFT-Konsensmechanismus* wird unter anderem unter dem Namen (Hyperledger) Sawtooth PBFT in einem Projekt von Hyperledger weiter entwickelt (Seeley 2019).
Eine Variation des PBFT ist der *Delegated Byzantine Fault Tolerance (DBFT),* in der unter den Akteuren eine Hierarchie besteht. Nach einem Abstimmungsverfahren ernennt die Allgemeinheit, sogenannte *ordinary nodes,* die *professional nodes*, welche gesondertes Recht auf Validierung von Blöcken erhalten (Buntinx 2017).

Tendermint verfolgt eine Mischform aus dem *PBFT* und dem ursprünglichen *PoS*. Mit dem Ziel weiterhin einen Anreiz für das Erstellen von fehlerfreien Blöcken zu behalten, müssen Netzwerkknoten einen *Stake* hinterlegen, welche bei unehrlichem Verhalten belangt werden. Die Höhe des hinterlegten *Stake* wird daher als Auswahlkriterium des *Proposers* herangezogen.

Auf Grundlage der eingeführten technischen Module steht im nächsten Kapitel die Umsetzung im Vordergrund und welche Fragen bei den Überlegungen hin zur Implementierung einer Blockchain-Lösung für das eigene Geschäftsmodell angestellt werden sollten.

2.6 Der Weg zur Umsetzung

Entscheidungsfragen für das Geschäftsmodell

Auf dem Weg zur Umsetzung eines Geschäftsmodells lassen sich die beschriebenen technologischen Module in Fragestellungen übersetzen, die sich jeder potenzielle Marktteilnehmer stellen muss. Die folgende Tabelle zeigt die zu Grunde liegende technologische Fragestellung (Primärfrage) entlang der in den vorherigen Kapiteln beschriebenen Module auf. Darüber hinaus müssen weitere anwendungsbezogene Fragen (Sekundärfragen) beantwortet werden.

Primärfrage Technologische Frage	**Sekundärfrage** Anwendungsbezogene Frage
Wie hoch ist der Grad der Individualität?	Soll die Entwicklung des Geschäftsmodells in Kooperation mit einem Plattformanbieter erfolgen? Besitzt mein Unternehmen die Kompetenzen und Kapazitäten eigenständig programmierte Blockchain-Lösungen zu entwickeln? Inwiefern muss das Regelwerk auf meine Bedürfnisse zugeschnitten werden?
Welche Anforderungen stelle ich an meine Applikationen?	Sieht es mein Geschäftsmodell vor, vielschichtige Applikationen zu etablieren? Möchte ich etablierte Programmiersprachen zur Erstellung meiner Applikationen nutzen? Soll meine Applikation flexibel auf Anpassungen der zugrundeliegenden Blockchain-Plattform reagieren?
Wer erhält Zugriff auf das Netzwerk und mit welchen Rechten?	Soll mein Geschäftsmodell sich an eine bestimmte Anzahl an Teilnehmern richten oder soll diese Anzahl beliebig variabel sein? Wie groß und wie heterogen ist meine Zielgruppe? Brauche ich übergeordnete Kontrolle gegenüber anderen Netzwerkteilnehmern? Darf jeder Teilnehmer Daten validieren?
Welche Schnittstellen benötigt mein Geschäftsmodell?	Wie stelle ich Vertrauen zu den Netzwerkteilnehmern her? Existiert eine Vertrauensbasis zwischen den Netzwerkteilnehmern? Wie schnell muss Konsens zu Modifikationen und Handlungen gefunden werden?
Benötigt mein Geschäftsmodell eine native Währung?	Benötigt das Geschäftsmodell ein Vergütungssystem? Soll die Vergütung in Fiatgeld stattfinden? Soll eine native Währung in börslichem Handel etabliert werden?

Tabelle 1: Technologische und anwendungsbezogene Fragestellung zur Überprüfung eines Geschäftsmodells

Ergänzend zur Tabelle 1 visualisiert Abbildung 8 die verschiedenen technologischen Blöcke, entlang derer die Fragen formuliert wurden. Entsprechend kann der Leser durch Beantwortung der Fragestellungen gemäß Tabelle 1 einen Pfad entlang der Module finden und so die geeignete technologische Konstruktion für sein Geschäftsmodell finden.

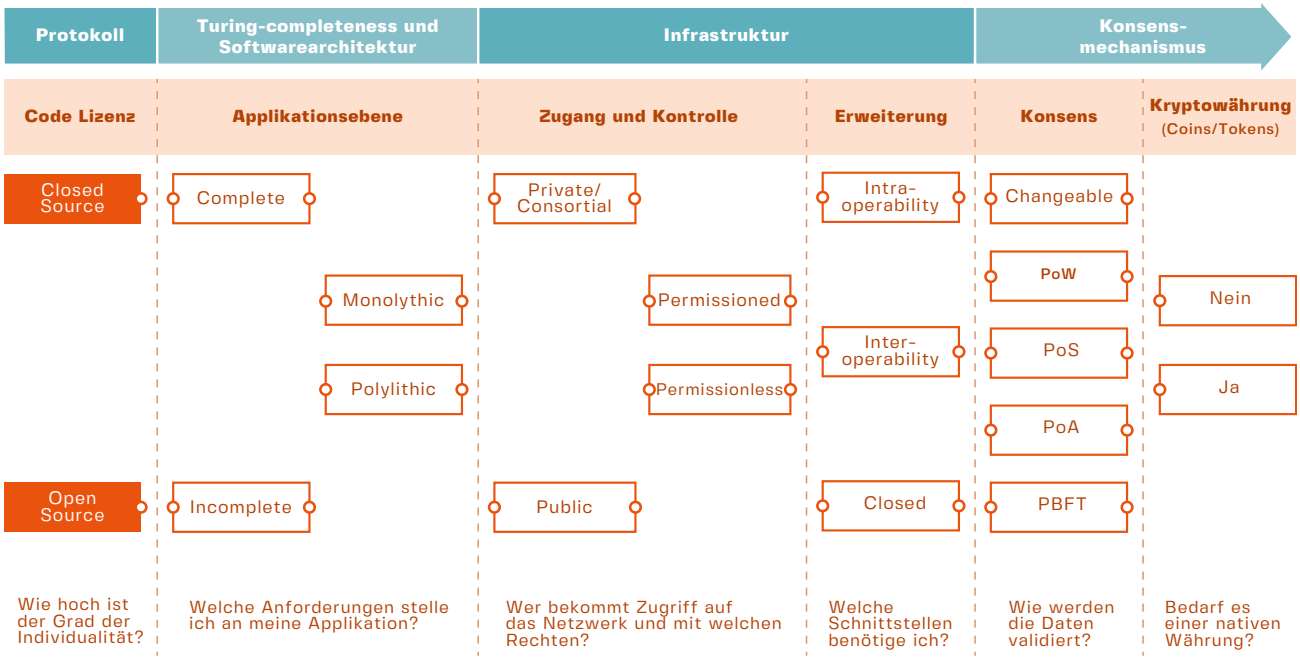

Abbildung 8: Übersicht der technischen Blockchain-Module bei der Überprüfung eines Geschäftsmodells

Wie hoch ist der Grad der Individualität?

Beginnend auf der linken Seite des Entscheidungspfads auf dem Weg der Technologiefindung muss sich ein potenzieller Marktteilnehmer die Frage stellen, ob die Applikation mit eigenem Personal verwirklicht, oder aber ein Anbieter konsultiert werden soll, der das Geschäftsmodell zumindest in den Anfängen begleitet und dabei den Quellcode zur Verfügung stellt. Intern wird diese übergeordnete Fragestellung insbesondere Fragen der eigenen Fähigkeiten und Kapazitäten aufwerfen. Ein externer Anbieter kann so zum Beispiel durch fachliches Personal beim Transfer der Ideen in Programmcode oder sogar beim laufenden Betrieb der finalen Anwendung unterstützen.
Darüber hinaus werden durch einen Open-Source Ansatz viele Aspekte des Protokolls bereits vorgegeben. Mit einem höheren benötigten Grad an Individualität kann es daher ratsam sein, einen eigenen Ansatz anstelle eines Open-Source Ansatzes zu wählen.

Welche Anforderungen stelle ich an meine Applikation?

Im zweiten Abschnitt stehen Fragen bezüglich der gewünschten Applikationen und damit dem Schwerpunkt von Geschäftsmodellen an. Ein besonderes Augenmerk ist dabei auf eine *turing-complete* Blockchain-Plattform zu richten, da diese Eigenschaft vielschichtigen Applikationen

erst ermöglicht und den Entwicklern mehr Freiheiten bezüglich der gewählten Programmiersprache bietet.
Des Weiteren muss in diesem Abschnitt des Entscheidungspfad eine Entscheidung zur Modifizierbarkeit der *Softwarearchitektur* getroffen werden. Hier gilt es zu beantworten, ob es größere Anpassungen im späteren Verlauf bedarf und inwiefern diese Anpassungen mit der gewählten Blockchain-Plattform vereinbar sind. Dabei kann es vorteilhaft sein, das Geschäftsmodell in einem Testnetzwerk oder auch einer Sidechain zu etablieren, um Anpassungsbedarfe auszumachen und dabei ökonomische Risiken zu minimieren.

Wer bekommt Zugriff und Kontrolle auf das Netzwerk und mit welchen Rechten?

Beschäftigt man sich bei den ersten beiden Primärfragen noch mit Software-bezogenen Fragen und dem grundsätzlichen Regelwerk, stehen ab der Infrastruktur externe, Anwendungsfall-bezogenen Inhalte und der finale Zweck der Blockchain-Anwendung im Vordergrund. So muss geklärt werden, wer zu einem späteren Zeitpunkt Zugriff auf das Netzwerk der entwickelten Applikation haben darf.
Die Extremfälle sind dabei eine unternehmensinterne Anwendung, zwecks interner Buchhaltung, oder aber eine öffentliche Dienstleistung, wie zum Beispiel ein standardisiertes Abrechnungsverfahren zum Laden von Elektroautos an öffentlichen Ladesäulen. Entsprechend der Größe und Heterogenität der Zielgruppe bieten sich für die beiden Extremfälle eine private *Infrastruktur* oder eben eine öffentliche *Infrastruktur* an.
Ebenso muss festgestellt werden, ob das Geschäftsmodell hierarchische Strukturen benötigt und ob einer oder mehrere Netzwerkakteure anderen gegenüber bevorzugte Rechte genießt bzw. genießen. Am Beispiel der unternehmensinternen Abrechnung sieht man, dass nur bestimmte Abteilungen oder Mitarbeiter Rechnungen erstellen oder validieren dürfen und die breite Masse der Angestellten nur Einsicht in die vorhandenen Dokumente erhalten. Solche hierarchischen Strukturen können zwecks Kontrolle des Netzwerks durch die Wahl eines adäquaten *Konsensmechanismus* weiter ausgebaut werden.

Welche Schnittstellen benötige ich?

Je nach Anwendungsfall der Blockchain muss diese über Schnittstellen verfügen, welche einen Datenaustausch zwischen der Blockchain und der Außenwelt ermöglichen.
Nicht immer ist es vorteilhaft, wenn die genutzte Blockchain über die maximal möglichen Kommunikationsschnittstellen verfügt. Mit den Schnittstellen erhöht sich auch die Angreifbarkeit des Systems von außen. Wird in der Blockchain mit äußerst sensible Daten hantiert, wie beispielsweise bei der unternehmensinternen Buchhaltung, gilt es abzuwägen, ob sich das mit den Schnittstellen verbundene Risiko tatsächlich lohnt.

Wie werden die Daten validiert?

Entsprechend ist die Wahl des *Konsensmechanismus* für Sicherheitsanforderungen des Netzwerks entscheidend. In kleinen Netzwerken könnte ein *PoW-Konsensmechanismus* zum Beispiel missbraucht werden, in dem ein Akteur mindestens als 51% der Rechenleistung stellt. Dann könnte dieser Akteur manipulativ in die Erstellung von Blöcken eingreifen (vgl. Kapitel 2.5 *Konsensmechanismus*). Bei der Frage nach dem anzuwendenden *Konsensmechanismus* muss auch die Zeit berücksichtigt werden, welche verstreichen darf, bis ein Konsens gefunden werden muss. Der *PoW-Konsensmechanismus* ermöglicht durch den Wettbewerb zur Lösung des kryptographischen Rätsels einen zeitlich definierten Konsens. Mechanismen, welche zunächst einer Mehrheitsentscheidung benötigen, wie zum Beispiel der *PoA-Konsensmechanismus* brauchen dazu in Abhängigkeit der Teilnehmeranzahl längerer Zeitspannen.

Benötige ich eine native Währung?

Sofern der Anwendungsfall über unternehmensinterne Anwendungen hinausgeht, braucht es in der Regel eines Vergütungssystems innerhalb des Netzwerks, um finanziellen Ausgleich zwischen den Teilnehmern zu ermöglichen. Diese Vergütung kann in digitaler Währung erfolgen, die durch *Smart Contracts*[9] in die Anwendung eingebunden sind. Dabei muss zwischen *Coins* und *Tokens* differenziert werden.

[9] *Der Exkurs zum Thema Smart Contracts befindet sich im Kapitel 2.6.1 Ethereum (und Bitcoin)*

Exkurs: Coin und Token

Coins sind die native Währung einer eigenen, für sich stehenden Blockchain-Plattform (Dinu 2018). Populäre Beispiele für *Coins* sind Bitcoin, Litecoin, Ether (Ethereum) oder aber auch ATOM, welche auf der Blockchain von Tendermint genutzt wird. Sie stellen somit eigenständige Kryptowährungen dar, die zum Handel vorgesehen sind.
Im Gegensatz zu *Coins* sind *Tokens* die Währung einer bestimmten Applikation bzw. eines Unternehmens, welches auf einer bereits vorhandenen Blockchain aufbaut (Ledger 2019). Die Anwendung geht dabei über die Kryptowährung hinaus, es handelt sich vielmehr um eine Art digitales Asset. *Tokens* können auch als Anteile am Unternehmen betrachtet werden und werden vor allem zu Beginn eines neuen Unternehmens im Rahmen eines *ICO* (*Initial Coin Offering*) ausgegeben. Für Projekte, die auf der Ethereum Blockchain basieren, bedeutet dies, dass sie *Tokens* benutzen, die meistens auf dem ERC-20 *Token Standard* von Ethereum beruhen (Blockchainwelt 2019).
Entscheiden sich Unternehmen zu einem späteren Zeitpunkt, eine eigene Blockchain-Plattform zu etablieren, so kann es zu einem *Coin* Swap kommen, bei dem die *Tokens* zu *Coins* umgewandelt werden (Rhodes 2018).

Einige *Konsensmechanismen* basieren darauf, dass eine native Währung vorhanden ist. Im *PoS* beispielsweise beruht das Vertrauen zu Knoten im Netzwerk und somit das Recht zum Validieren von Blöcken darauf, dass die Knoten einen auf der nativen Währung basierenden *Stake* hinterlegen, welcher im Falle eines Missbrauchs einbehalten wird. Ebenso erwartet der Validator eine Vergütung für das Erstellen und Validieren von Blöcken. Andere *Konsensmechanismen*, wie zum Beispiel der *PoA-Konsensmechanismus* bedürfen nicht bedingt einer Vergütung und entsprechend auch keiner nativen Währung. Der Validator eines Blocks ist mit seiner Identität bekannt und kann im Falle eines Missbrauchs beispielsweise vom Netzwerk ausgeschlossen werden (Natoli et al. 2019).

Um dem potenziellen zukünftigen Marktakteur den Markteintritt zu erleichtern, werden in der folgenden Grafik die Entscheidungspfade für die Zusammensetzung der unterschiedlichen Blockchain-Plattformen farblich gekennzeichnet und anschließend verglichen. Dabei sind in Abbildung 9 die bekannteren Plattformen Bitcoin und Ethereum dargestellt, während in Abbildung 10 weitere Plattformen aufgelistet sind, welche insbesondere in der Energiewirtschaft zum Einsatz kommen. Dies sind Energy Web Foundation (mit Energy Web Chain und Energy Web Link), Tendermint und Hyperledger. Die einzelnen Pfade der Blockchain-Plattformen werden in den folgenden Kapiteln näher erörtert.

2.6.1 Ethereum (und Bitcoin)

Die Bitcoin-Blockchain wurde bereits im Jahr 2008 von einer oder mehreren Personen, die sich hinter dem Synonym „Satoshi Nakamoto“ verbergen (Nakamoto 2008), entwickelt und 2009 veröffentlicht (Caetano 2015). Sie gilt damit als Blockchain der ersten Generation und Fundament der heute populären Blockchains. Die Bitcoin-Blockchain dient vor allem dem Zweck von Transaktionen (und die Speicherung dieser) mittels der Kryptowährung Bitcoin.
Zwar waren die technischen Grundlagen der Blockchain-Technologie teilweise bereits in den siebziger Jahren bekannt (Wensley et al. 1978), jedoch konnte die Bitcoin-Blockchain tatsächlich zum ersten Mal nachweisen, dass innerhalb eines anonymen und dezentralen Netzwerks ein Konsens gefunden werden kann (Buchman 2016).

Exkurs: Smart Contracts

Schon bevor die Blockchain-Technologie Verbreitung gefunden hat, wurden der Begriff und die Technologie von *Smart Contracts* diskutiert. Im Jahr 1997 beschrieb Szabo die grundlegende Idee und Einsatzfelder von *Smart Contracts* (Szabo 1997). Zur Anwendung im Bereich der Blockchain bedurfte es jedoch der Gründung von Ethereum im Jahr 2015. Seitdem findet das Konzept breite Verwendung in der Blockchain-Gemeinschaft.
Ein Smart Contract ist ein Programm, das auf einem Blockchain-Protokoll basiert und grundsätzlich durch eine Mehrzweck-Berechnung, die auf der Blockchain stattfindet, ermöglicht wird. Er kann die Überweisung digitaler Währung zwischen zwei Parteien ausführen, wenn die im Programm/Vertrag festgelegten Anforderungen erfüllt sind. *Smart Contracts* sind also programmierbare Vertragswerkzeuge, also Verträge, die in Software-Code eingebettet sind. Daher muss ein Smart Contract die vertragliche Vereinbarung selbst enthalten; von der Definition der Erfüllung der vertraglichen Verpflichtungen bis zur tatsächlichen Ausführung des Vertrags (Koulu 2016).
Smart Contracts sind also selbstausführende Systeme, die perspektivisch sehr effizient sein können und viele neue Möglichkeiten eröffnen. Allerdings gibt es auch potenzielle Risiken von/bei *Smart Contracts*. Das Ausführen von Anweisungen ohne menschliches Eingreifen oder Kontrolle könnte zu potenziellen Problemen und Risiken führen und muss eingehender untersucht werden (Werbach 2019).

Innovativ war bei der Bitcoin-Blockchain also nicht die kryptographische Methodik, sondern die *Distributed-Ledger-Technologie*, die im Zusammenspiel mit einem auf dem *PoW* basierten *Konsensmechanismus* dezentral, autark und ohne gegenseitiges Vertrauen arbeiten konnte.
Die Ethereum-Blockchain wurde im Jahr 2015 öffentlich zugänglich. Sie ähnelt der Bitcoin-Blockchain sehr. So basiert auch Ethereum auf dem *PoW-Konsensmechanismus*, wobei es bereits seit Gründung Bestrebungen gibt, den *Konsensmechanismus* auf *PoS* umzustellen (Sharma 2019). Im Unterschied zu Bitcoin ist Ethereum jedoch durch die *EVMs turing-complete*, sodass *Smart Contracts* ausgeführt und entsprechend komplexe Applikationen ausgeführt werden können. Wegen dieses neuartigen Prinzips wird Ethereum auch als Blockchain der zweiten Generation bezeichnet (Bashir 2017). Durch diese Applikationsmöglichkeit spricht Ethereum ein anderes Nutzungsfeld an als Bitcoin. Bitcoin wurde ausschließlich zu dem Zweck konzipiert, Transaktionen zu ermöglichen und eine von Fiat-Währungen unabhängige Währung zu kreieren, wohingegen Ethereum darauf ausgelegt ist, mittels *Smart Contracts* diverse automatische Aktionen zwischen zwei oder mehreren Parteien ablaufen zu lassen. Für solche Anwendungen, in denen diversere Aktionen statt nur Transaktionen getätigt werden, ist das

Ethereum-Netzwerk geeigneter als das Bitcoin-Netzwerk. Daher greift die Energiewirtschaft, nicht auf die Bitcoin-Plattform, sondern auf die Ethereum-Plattform zurück.
In anderen technologischen Modulen sind die beiden Plattformen, in der groben Granularität dieser Studie, identisch. Beide Blockchain-Technologien sind öffentlich verfügbar. Es existieren keine Zugangsbeschränkungen zur Teilnahme am Netzwerk (*public*) und Gleichberechtigung unter allen Nutzern (*permissionless*). Die *Softwarearchitektur* beider Blockchains ist monolithisch aufgebaut. Spätere Änderungen von Bitcoin oder Ethereum könnten daher zu Kompatibilitätsproblemen von Applikationen führen.
Im *Protokoll* des Bitcoin-Netzwerkes ist festgelegt, dass ca. alle zehn Minuten ein neuer Block vom Netzwerk erstellt wird. Dieser zeitliche und speichertechnische Flaschenhals wurde von Ethereum quasi aufgehoben, da die Zeit zur Generierung eines neuen Blocks nur ca. 10 bis 20 Sekunden dauert und somit die Geschwindigkeit für die Ausführung und Validierung von Transaktionen erhöht wird. Dies wäre auch möglich, wenn die Größe des Blocks, also die Anzahl der zusammengefassten Transaktionen in einem Block angehoben wird. Durch den Open-Source-Ansatz bei der Weiterentwicklung der Plattformen ist es möglich, den zugrunde liegenden Code selbst weiter zu entwickeln. Dadurch ist es grundsätzlich auch möglich, beispielsweise einer auf Ethereum basierenden Blockchain Zugangsbeschränkungen hinzuzufügen. Hierdurch kann jedoch nicht mehr von einer Plattform gesprochen werden. Private Weiterentwicklungen auf Grundlage von den genannten Plattformen sind daher nicht in die Gegenüberstellung in Abbildungen 9 und 10 mit eingeflossen, um den Vergleich einheitlich zu visualisieren.

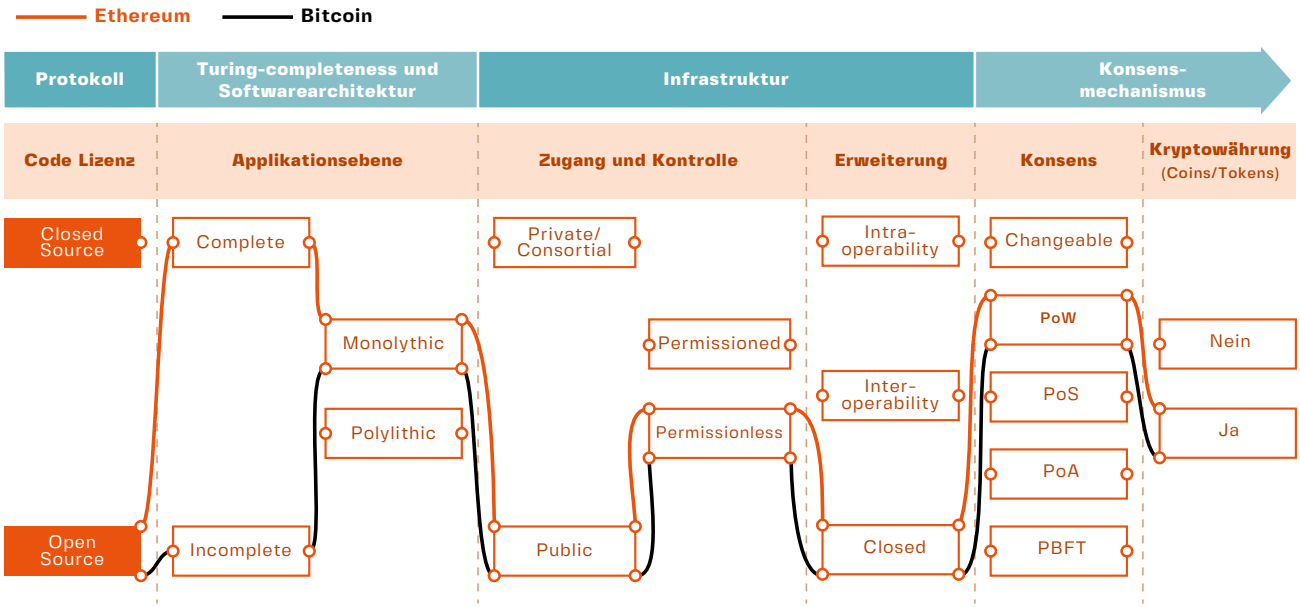

Abbildung 9: Gegenüberstellung der Blockchain-Plattformen Bitcoin und Ethereum

2.6.2 Energy Web Chain

Die EWF ist eine gemeinnützige Organisation, die im Jahre 2017 vom Rocky Mountain Institute und Grid Singularity gegründet wurde. Der Hauptsitz der Organisation ist in Berlin. Das Ziel der EWF ist es, Unternehmen aus der Energiewirtschaft die Blockchain als Software für Geschäftsideen zur Verfügung zu stellen. Die EWF hat mehr als 100 Mitglieder aus der Energiebranche.
Basierend auf dem öffentlich zugänglichen Code der Ethereum-Blockchain wurden Veränderungen vorgenommen, um Lösungen zu konstruieren, welche auf die Marktbedürfnisse, regulatorischen Anforderungen und Sicherheitsrichtlinien des Energiesektors maßgeschneidert sind. Eine dieser Lösungen ist die Energy Web Chain (EWC), welche Mitte 2019 als Open-Source-Projekt veröffentlicht wurde. Eine der größten Veränderungen im Vergleich zur Ethereum-Blockchain stellt die Umstellung des *Konsensmechanismus* von *PoW* auf *PoA* dar. Dies dient unter anderem dem Zweck, den Energieverbrauch des Netzwerks zu verringern. Nach eigener Aussage der EWF kann eine 30-fach höhere Performance bei 2-3-fach geringerem Energieeinsatz erzielt werden (energy web foundation 2019). Knoten, die für die Validierung der Transaktionen und Erstellung neuer Blöcke zuständig sind, werden Validatoren genannt. Ein Validator kann nur werden, wer Projektpartner von EWF ist und einen strengen Validierungsdurchlauf absolviert hat. Dies soll sicherstellen, dass die Validatoren bekannt sind und beispielsweise notwendige Hardwarerichtlinien erfüllen. Entsprechend ist die *Infrastruktur* der EWC *permissioned*.
Die EWF erlaubt allen Unternehmen die EWC für kommerzielle Zwecke zu nutzen. Dabei unterstützt die EWF in den Anfängen ihrer Geschäftsmodellentwicklung, zum Beispiel durch *SDKs*. Mit Hilfe dieser Toolkits können die Unternehmen individuelle Anwendungen (*dApps*) programmieren, welche auf der EWC ausführbar sind.
Für die Nutzung wird von der EWF eine Gebühr erhoben. Nutzer sind dazu verpflichtet Energy Web *Tokens* zu erwerben. Die Erlöse für diesen Erwerb werden den Validatoren des Netzwerks als Vergütung zugeführt. Außerdem werden Anteile dazu verwendet die Netzwerksicherheit zu gewährleisten. Dies wird dadurch erreicht, dass sich die Gebühr der *Tokens* nach der benötigten Rechenleistung richtet, die zur Ausführung von *Smart Contracts* notwendig ist.
Neben *Smart Contracts* ist es auf der EWC ebenfalls möglich, private und bilaterale Transaktionen durchzuführen. Dies ist vor allem in solchen Fällen, bei denen auf Datensicherheit besonders viel Wert gelegt wird, von besonderem Interesse. Bei derartigen privaten Transaktionen werden die Daten zusätzlich verschlüsselt. Zugang zu den Daten hat nur, wer auch die notwendigen Zugriffsrechte besitzt und in Besitz des Lösungsschlüssels ist. Durch die Zuteilung unterschiedlicher Privilegien ist es nicht nur möglich, die Zugriffsrechte zu beschränken, sondern zum Beispiel auch Teilnahme an bestimmten Märkten zu regulieren.

Für Unternehmen und Programmierer stehen darüber hinaus die Netzwerke Tobalaba und Volta zu Testzwecken zur Verfügung, die in einer geschlossenen Umgebung die Erprobung neuer Anwendungen ermöglichen.Neben der EWC arbeitet die EWF an weiteren Blockchain-Plattformen, die sich jeweils an Unternehmen mit unterschiedliche Anforderungen richten. So ist die Energy Web Link besonders auf die Integration von Anlagen ausgerichtet und ermöglicht die Vernetzung nach dem Prinzip des Internet of Things (IoT) auf Blockchain-Basis. Die Energy Web Origin als weitere Blockchain-Plattform von EWF ist speziell auf Herkunftsnachweise von Strom aus erneuerbaren Energien sowie dem Emissionshandel ausgerichtet.

2.6.3 Hyperledger Fabric

Hyperledger Fabric ist eine vollständig öffentlich verfügbare (Open-Source-) Plattform, welche unter dem Titel Hyperledger in der Linux Foundation angesiedelt ist. Fabric wurde von IBM in die Linux Foundation eingebracht, um die Weiterentwicklung der Hyperledger Fabric als Open-Source-Projekt weiter zu führen und dabei ein eigenständiges Produkt für Unternehmen zur Verfügung zu stellen. Seit dem Beginn im Januar 2016 ist das Projekt rasant gewachsen und umfasst heute mehr als 150 Teilnehmer (Azimdoust 2019).
Fabric ist eine *permissioned* Blockchain, die den Bedürfnissen der Anwendung angepasst werden kann. Die Knoten sind bei Fabric im Netzwerk bekannt, Anonymität einzelner Knoten ist nicht möglich.
Die *Softwarearchitektur* von Fabric ist polylithisch, jedoch mit der Besonderheit, dass nicht nur die Entwicklung von Applikationen von der *Infrastruktur* und dem *Konsensmechanismus* getrennt ist, sondern dass die sie auch frei konfigurierbar sind (Hyperledger 2019). Der *Konsensmechanismus* kann frei gewählt und der Größe des Netzwerks und dem Vertrauen innerhalb des Netzwerks angepasst werden. Eine Kryptowährung ist je nach gewählter Anwendung zwar möglich, jedoch nicht notwendig. Innerhalb eines Netzwerks ist es den Teilnehmern der Blockchain möglich, Transaktionen durch sogenannte *channels* durchzuführen. Diese *channels* sind dabei nur von den Parteien einsehbar, welche an der Transaktion teilnehmen und bieten somit die Möglichkeit zu privatem Handeln gegenüber dem Netzwerk (Belchior 2019).
Ein Alleinstellungsmerkmal von Fabric ist seine Konfigurierbarkeit als rein unternehmensinterner *Ledger*. In dieser Funktion kann Fabric auch ohne vorhandene Internetverbindung genutzt werden. Statt ein physisches Netzwerk bereitzustellen, auf dem die Blockchain ausgeführt wird (wie es beispielsweise bei Energy Web Chain der Fall ist), ist Fabric dazu gedacht, seine eigenen Rechenkapazitäten zu nutzen, auf welchem dann die Hyperledger Fabric ausgeführt wird.

2.6.4 Tendermint

Das Unternehmen Tendermint wurde von Joe Kwan und Ethan Buchman im Jahr 2014 gegründet. Tendermint bietet Tendermint Core und Cosmos an. Das dazu gehörende Cosmos SDK gibt Entwicklern die Möglichkeit, ihre Anwendungen in der Programmiersprache Golang zu schreiben und auf einer Blockchain ausführen zu lassen. Über ein Interface, dem sogenannten *Application Blockchain Interface (ABCI)* kann die Applikation auf Tendermint Core ausgeführt werden, jedoch ist dies nicht notwendig. Somit können sowohl öffentliche als auch private Anwendungen erstellt werden. Tendermint Core besteht zum einen aus einem *Konsensmechanismus* und zum anderen aus einem „*Peer-to-Peer-Netzwerk Protokoll*“. Dem Nutzer steht es frei zu entscheiden, ob er neben dem Cosmos SDK auch Tendermint Core nutzen möchte (Cosmos 2018).
Der *Konsensmechanismus* von Tendermint Core basiert auf einem PoS-Algorithmus, welcher durch seine rundenbasierte Ausführung an den *Byzantine Fault Tolerance* (BFT) angelehnt ist (vgl. Kapitel 2.5.4 *Practical Byzantine Fault Tolerance*). Die Runden sind dabei an zeitliche Vorgaben geknüpft. Wird beispielsweise kein neuer Block innerhalb einer bestimmten Zeit von dem *Proposer* vorgeschlagen, so wird dieser Block übersprungen und ein anderer Knoten als *Proposer* ausgewählt. Es ist dadurch sichergestellt, dass immer eine Runde existiert, in welcher ein Block vorgeschlagen und validiert wird. Tendermint selbst bezeichnet dies als „*BFT PoS*“ oder „Cosmos *PoS* Konsensalgorithmus“ (Interchain Foundation 2017). Während Tendermint Core monolithisch aufgebaut ist, kann der Entwickler sich auf der Applikationsebene relativ frei bewegen. Das *ABCI* sorgt in diesem Falle dafür, dass Anwendungen trotzdem auf der Blockchain ausführbar sind (Buchman 2016). Zusätzlich stellt Tendermint über Cosmos eine Art „Internet der Blockchains“ zur Verfügung. Über Cosmos können unterschiedliche Blockchains miteinander kommunizieren. Dies ist besonders dann hilfreich, wenn neue Applikationen auf einer bestehenden Blockchain hinzugefügt werden sollen. Auch kann dadurch erreicht werden, dass Blockchains für ein spezielles Problem ausgelegt sind und trotzdem in einem gemeinsamen Netzwerk innerhalb größerer Zusammenhänge kommunizieren können und als einzelne Funktionsglieder agieren.

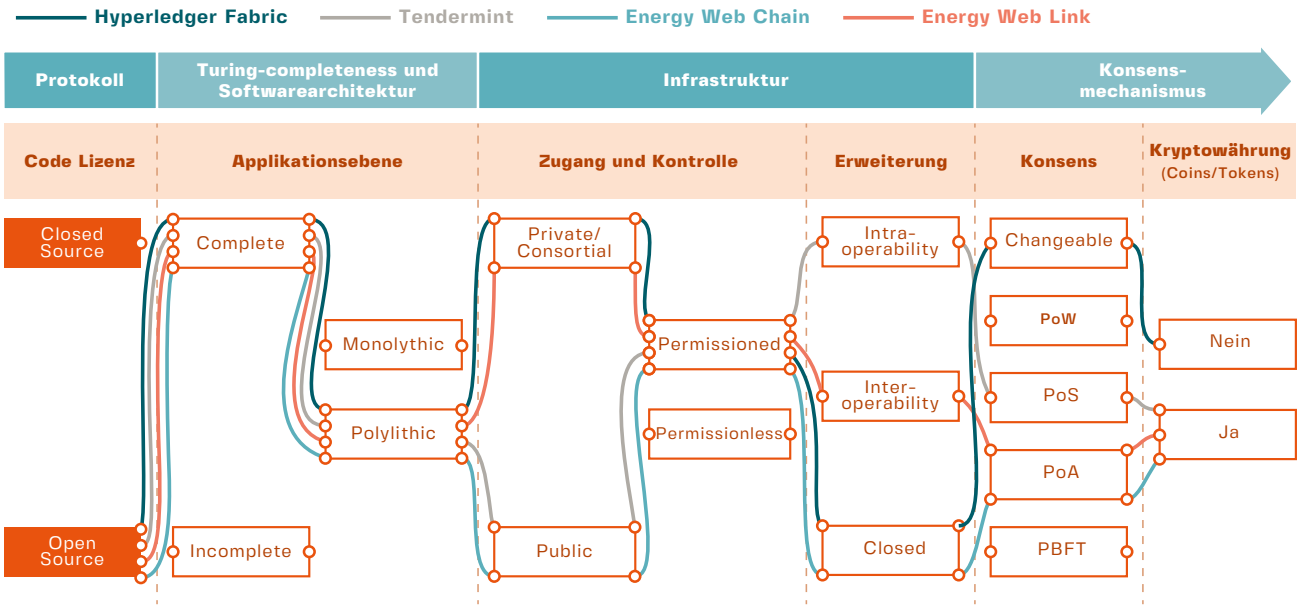

Abbildung 10: Gegenüberstellung Anbieter von Blockchain-Plattformen in der Energiewirtschaft

Folgende Erkenntnisse lassen sich ableiten:

- → Die Blockchain-Technologie ist technisch modular aufgebaut. Die Kombination der Module wirkt sich auf die möglichen Anwendungsfelder der Blockchain aus und muss entsprechend beim Konzipieren der Geschäftsidee berücksichtigt werden.
- → Je nach Blockchain-Plattform bedarf es einer Zusammenarbeit mit Plattform-Anbietern, die ihre Plattform als Service bereitstellen.
- → Es sind bereits diverse Blockchain-Anbieter am Markt verfügbar, welche ein sehr vielfältiges Spektrum an möglichen technischen Kombinationen der Blockchain-Module abdecken.
- → Für ein dynamisches und flexibles Geschäftsmodell sind insbesondere die *Softwarearchitektur* und die *Turing-Completeness* entscheidend.
- → Applikationen für die Blockchain können vermehrt mittels bekannter Programmiersprachen entwickelt werden. Dies erhöht die Anwendungs-möglichkeiten.

Status Quo und Entwicklung der Blockchain in der Energiewirtschaft

3

Nachdem dem Leser im ersten Teil der Studie das notwendige Werkzeug an die Hand gegeben wurde, um den technischen Hintergrund heutiger Anwendungen der Blockchain zu verstehen, werden nun aktuelle energiewirtschaftliche Anwendungsbeispiele aufgeführt. Dazu werden zunächst die Methodik und die Auswahlkriterien, die innerhalb der Studie gewählt wurden, beschrieben. Anschließend wird die Entwicklung der detektierten Anwendungsbeispiele im Vergleich zu den Vorläuferstudien des „Blockchain-Radar“ dargelegt. Diese dynamische Darstellung der Marktteilnehmer ermöglicht es, Trends abzuleiten sowie den Charakter des Marktumfelds zu skizzieren.

3.1 Methodik und Auswahlkriterien der Marktanalyse

Die Herangehensweise bietet eine Abgrenzung zur vorhandenen Literatur

Um potenzielle Replikationen der Studie zu ermöglichen, soll im Folgenden das Vorgehen beschrieben werden, welches bei der Erstellung der Übersicht verfolgt wurde. Dazu wird zunächst die vorausgegangene Recherche beschrieben. Anschließend werden die Auswahlkriterien, nach denen beurteilt wurde, inwiefern ein Geschäftsmodell in der Übersicht aufzunehmen ist, diskutiert.

Viele der Ideen und Entwicklungen rund um Blockchain kommen aus der Anwendung heraus. Fortschritte und Wissen in diesen Bereichen wird häufig nicht über wissenschaftliche Quellen weitergeleitet, sondern über sogenannte „graue Literatur". Graue Literatur durchläuft bei ihrer Veröffentlichung keiner Prüfung kommerzieller wissenschaftlicher Verlage (Higgins und Green 2012).

Des Weiteren ist das Thema Blockchain sehr neu und gegenwärtig, dass sich schnell weiterentwickelt. Durch Eigenschaften, wie Gegenwärtigkeit und Anwendungsbezug wurde als methodischer Ansatz eine „Multivocal Literature Review" (MLR) gewählt. Kommend aus der sozialwissenschaftlichen Forschung, wird MLR auch immer häufiger in den Informationswissenschaften angewandt (Garousi et al. 2019). Eine MLR umfasst alle zur Verfügung stehenden Informationen und beschränkt sich nicht nur auf wissenschaftliche Arbeiten (Ogawa und Malen 1991).

Die Recherche basiert daher sowohl auf zugangsbeschränkter wissenschaftlicher Literatur sowie auf Informationen, welche öffentlich zugänglich sind, wie zum Beispiel graue Literatur, Blogs oder Internetseiten jeweiliger Marktakteure. Auch wenn die Zuverlässigkeit solcher Quellen nicht unbedingt gegeben ist, lässt sich deren Sichtung für eine Blockchain-Studie nicht ausschließen, da es in diesem Umfeld durchaus üblich ist, Informationen in Foren und Blogs weiterzugeben (Andoni et al. 2019). Ebenfalls üblich ist es, dass Unternehmen, deren Geschäftsmodelle auf der Blockchain basieren, ihre Aktivitäten in einem sogenannten „White Paper" auf der jeweiligen Unternehmensseite vorstellen. Auch solche „White Paper" wurden im Rahmen der Recherche ausgewertet. Vor allem unter dieser Art der Quellen fallen auch die Angaben der geografischen Zuordnungen. Dies führt dazu, dass die Zuordnung aufgrund ungenauer geografischer Angaben nicht immer mit eindeutiger Korrektheit möglich ist. So wird beispielsweis das EU-Projekt NEMoGrid, in welchem ein Strommarktdesign auf Basis der Blockchain entwickelt wird, an drei unterschiedlichen Standorten länderübergreifend durchgeführt. Andere Akteure, wie z. B. das Start-up

Shasta, welches einen freien Strommarkt unabhängig von Landesgrenzen anbietet, veröffentlichen keine Angaben zum Geschäftsstandort. Diese beiden Fallbeispiele werden daher separat aufgeführt.
Darüber hinaus wird darauf verwiesen, dass ausschließlich Quellen in englischer und deutscher Sprache herangezogen wurden. Eine Gewähr auf Ganzheitlichkeit kann daher vor allem für den asiatischen Raum nicht gegeben werden.
Es bleibt festzuhalten, dass ein Nachteil dieser Art von Review dadurch entsteht, dass durch den weiten Betrachtungswinkel eine Vielzahl an Informationen nicht in einem angemessenen Maße erfasst werden können. Um diesen Nachteil zu reduzieren sind unterschiedliche Parameter in die Untersuchung aktueller Blockchain-Anwendungen eingegangen.

Ziel der MLR ist es, innerhalb vorhandener Geschäftsmodelle und Akteure derart zu selektieren, dass zwar möglichst umfänglich, aber auch nur solche Geschäftsmodelle berücksichtigt werden, welche in ihrem Kern tatsächlich aktuell auf der Blockchain basieren und in der Energiewirtschaft Anwendung finden. So wurde zum einen das Kriterium der „Aktualität“ angewandt sofern darauf verwiesen wird, dass ein Akteur in Zukunft eine Leistung auf Basis der Blockchain bereitstellt. Wird die Leistung derzeitig noch anderweitig generiert, wird diese Leistung in der Studie nicht berücksichtigt. Als Beispiel sei hier das Berliner Startup Lumenaza GmbH genannt, welches eine P2P-Softwarelösung anbietet, die nach eigenen Aussagen in Zukunft auch auf Basis der Blockchain-Technologie ausgeführt werden soll, derzeit jedoch durch konventionelle Prozesse funktioniert (pv Magazine 2017). Gleiches gilt, sofern ein Projekt oder Konsortium angekündigt, aber nicht nachweislich erfolgreich gestartet wurde. Dies ist beispielsweise bei einer Kooperation zwischen Tavrida Electric und Qiwi der Fall, bei der laut offizieller Ankündigung eine Kooperation zur Transaktionsverfolgung im Energiehandel auf Basis von Blockchain geplant ist, allerdings außer der Ankündigung keine weiteren Informationen zu finden sind.
Ebenso werden solche Vorhaben nicht aufgeführt, welche in der Vergangenheit stattgefunden haben, jedoch nicht weiterverfolgt werden. So wird das „PowerTree“ Projekt zum Beispiel auch im Blockchain-Radar mit Stand 2018 aufgeführt, allerdings sind über dieses Unternehmen kaum Informationen zu finden, da die letzten Informationen auf der Website aus dem Jahre 2016 stammen. Eine Übersicht über Unternehmen und Projekte, welche betrachtet, aber nicht in die Übersicht aufgenommen wurden, findet sich im Anhang.
In Anlehnung an das Blockchain-Radar wurden nur solche Anwendungsbeispiele berücksichtigt, welche der Energiewirtschaft zuzuordnen sind. Als Energiewirtschaft wurde für die Studie jener Teiler der Wirtschaft definiert, der an der Wertschöpfung der Energieversorgung beteiligt ist, sowie Dienstleistungen, die im direkten Zusammenhang hierzu stehen. Noch nicht inbegriffen, da ebenso in anderen Branchen relevant, aber perspektivisch zu integrieren, sind Anwendungen im Bereich des Emissionshandels.

Im Falle konsortialer Strukturen oder Kooperationen von Unternehmen wurde darauf verzichtet, die Unternehmen einzeln zu erwähnen. Stattdessen firmieren solche Zusammenschlüsse unter dem Projektnamen, sofern ein Projektname vorliegt. So steht hinter „Enerchain“ zum Beispiel ein Konsortium aus über 45 Unternehmen aus dem Energiehandel. Die separate Darstellung aller Unternehmen in der Übersicht wäre daher nicht zielführend.

3.2 Globale Übersicht über aktuelle Anwendungsfälle der Blockchain in der Energiewirtschaft

Die im Zuge der Recherche entsprechend der Ausführungen aus Kapitel 3.1 gefundenen Anwendungsfälle sind in Anlehnung an das „Blockchain-Radar“ der Version 2017 bis 2020 in fünf Bereiche eingeteilt:

- **Peer-to-Peer Business to Customer (B2C):** Stromhandel über Blockchain mit Fokus auf Endkundenbelieferung.
- **Mobilität:** Dienstleistungen im Bereich der Mobilität, von Ladesäulenmanagement für Elektroautos bis Mobilitätsanbieter.
- **Anlagenmanagement, Netze und Metering:** Infrastrukturanwendungen und Datenerhebung sowie Anwendungen im Bereich von Microgrids.
- **Stromhandel Business to Business (B2B) bzw. Customer to Business (C2B) und Zertifizierung:** Geschäftsmodelle mit Fokus auf Unternehmenskunden sowie Zertifizierung im Sinne von Herkunftsnachweisen.
- **Entwickler und Sonstige:** Projekte, Kooperationen und Unternehmen, welche sich mit der Weiterentwicklung der Blockchain beschäftigen, sowie Anwendungen, die nicht in einen der vorherigen Bereiche fallen.

Innerhalb der aufgelisteten Anwendungsbereiche werden gefundene Anwendungsbeispiele in geografischen Zonen aggregiert, wobei im Unterschied zum Blockchain-Radar 2020 Tätigkeiten über den gesamten Globus erfasst werden sollen, sodass in Zukunft Entwicklungsgeschwindigkeiten geografisch differenziert besser nachvollzogen werden können. Abbildung 11 zeigt gefundene Anwendungsbeispiele, aufgeteilt in entsprechende Anwendungsbereiche, geographischen Kontext sowie nach Blockchain-Plattform, welcher der Anwendung zugrunde liegt mit Stand vom Februar 2020.

Energy Web | Ethereum | Hyperledger Fabric | Tendermint | Sonstige | n.a.

	Anlagenmanagement / Netze / Metering	Entwickler / Sonstige	Mobilität	Peer-to-Peer B2C	Stromhandel B2B / C2B Zertifizierung
Europa	IT PROSUME CH Energy Bazaar DE Oli DE Sonnen & TenneT UK Verv DE Gridchain NLD CGI & Eneco UK Electron FINN Wirepas FR Sunchain NLD Vanderbron & TenneT ES Ampere Energy	DE fury.network DE IOTA DE StromDAO LI Lition MLT Poseidon SE ChromaWay AD ElectricChain (Solarcoin) DK M-PAYG NLD Blocklab UK 4New ES Alastria FR DAISEE NDL DAO IPCI CH MyBit DE Freeel.io CH Energy Web Foundation DE Ponton NLD Eco coin	DE BlockCharge DE Demos IT PROSUME DE Share&Charge DE Car eWallet DE Green Energy Wallet	DE slock.it DE Conjoule DE enyway UK Energimine UK VLUX CH Hive Power SI SunContract ES Pylon IT PROSUME LTU WePower NLD Alva Energy Consortium DE :elblox DE BloGPV DE Tal.Market NLD Powerpeers NLD ToBlockChain BE Toomuch.energy CH Power-ID UK Daije DE AdptEve DE LUtricity DE Restart Energy FR Stratumn LI Lition Energy Exchange NLD Jouliette DE Pebbles DE LAMP	DE Corrently DE Co-Tricity DE Key2Energy DE TRUEKEN DE stromhaltig.de BE NRGCoin PT VAKT NLD Clearwatts FR The Energy Origin NLD OneUp NLD Start.Solar EE Powerchain EE SolarDAO DE Grünstrom Jeton IT PROSUME DE Enerchain DE GridSingularity
USA	Swytch Filament ReWatt Power Eloncity	Chain of Things ENLedger Datawatt EverGreenCoin	Arcade City MOBI	Bovlabs Power2Peer Brooklyn Microgrid Drift TransActive Grid LO3Energy OMEGA Grid	ImpactPPA Avocado Classic Local-e Wattcoin Labs / Veriown Volts Markets XiWatt SolarCoin Veridium Labs
Restliche Welt	AU PowerLedger SG Torus Konsortium NeMoGrid ARG NYDRO NGA OneWattSolar KR Kepco open MG SG GreenX	KE M-PESA	AU PowerLedger IL Commuterz IL La`Zooz	SG Bittwatt SG Electfiy.Asia SG Platinum Energy Recovery AU PowerLedger BR Cosol/IORE IL Greeneum N.A Shasta TH BCPG & Sansiri JP Eneres/Fujitsu SG Solar bankers	AU PowerLedger CA CarbonX CA PetroBloq ZA The Sun Exchange CA BTL CN Energy Blockchain Lab & IBM

Abbildung 11: Aktuelle Blockchain Anwendungen in der Energiewirtschaft. (Stand: Februar 2020)

3.2.1 Geographische Technologieverbreitung

Europa nimmt weiterhin die führende Rolle in der Energiewirtschaft ein

Die Blockchain im Kontext der Energiewirtschaft ist geografisch bereits weit verbreitet. So finden sich Fallbeispiele, auf jedem Kontinent. Abbildung 11 verteilt die 132 Einträge der betrachteten Fallbeispiele, bestehend aus 125 unterschiedlichen Unternehmen, Start-ups, Projekten und Kooperationen auf ihre 32 Ursprungsländer. Die folgenden Tabelle zeigt die detaillierte Verteilung.

Deutschland	31	Spanien	2	Nigeria	1
USA	25	Konsortium/ n.a.	2	Australien	1
Niederlande	12	Portugal	1	Italien	1
Singapur	6	Südafrika	1	Slowenien	1
Schweiz	5	China	1	Litauen	1
Großbritannien	5	Malta	1	Japan	1
Frankreich	4	Dänemark	1	Argentinien	1
Belgien	3	Schweden	1	Thailand	1
Kanada	3	Andorra	1	Brasilien	1
Israel	2	Kenia	1	Finnland	1
Estland	2	Liechtenstein	1	Südkorea	1

Tabelle 2: Globale Verbreitung von Blockchain Anwendungen in der Energiewirtschaft nach Projekten in Ländern

Bemerkenswert ist die hohe Anzahl der gefundenen Fallbeispiele auf dem europäischen Kontinent. Insbesondere Deutschland (31) und die Niederlande (12) weisen äußerst hohe Aktivitäten auf. Auch in der Schweiz (5), Großbritannien (6) und Frankreich (4) findet sich eine signifikante Anzahl an aktuellen Projekten.
Auf dem amerikanischen Kontinent beschränken sich die Aktivitäten auf die nördliche Halbkugel. Die Vereinigten Staaten bündeln 25 der insgesamt 28 erkannten Projekte, die verbliebenen drei sind in Kanada verortet.
Im asiatischen Raum verzeichnet der Stadtstaat Singapur die höchste Anzahl (6) an Aktivitäten. Neben Singapur sind aus dem asiatischen Raum jedoch nur Thailand, Japan sowie China mit jeweils nur einer einzigen gefundenen Aktivität vertreten.
Auf dem australischen Kontinent konnte nur ein einziges aktives Projekt der Blockchain in der Energiewirtschaft gefunden werden. Auch der afrikanische Kontinent weist mit jeweils einem nachgewiesenen Projekt in Kenia sowie Südafrika und Nigeria nur geringe Aktivität auf.

3.2.2 Entwicklung im Anwendungsbereich

Peer-to-Peer Anwendungen beherrschen immer noch den Markt

Ähnlich dem „Blockchain-Radar“ findet auch die vorliegende Studie einen Großteil der Geschäftsmodelle im Anwendungsbereich von B2B-Plattformen in Form von P2P-Stromhandel. Mehr als ein Drittel aller gesamten Aktivitäten werden dieser Anwendung zugeschrieben. Diese überragende Anzahl Anwendungsfeld bestätigen auch die bisherigen „Blockchain-Radars“. Dies kann in jedem der Anwendungsbereiche festgestellt werden, mit Ausnahme der Elektromobilität. Teilweise erfüllten Einträge nicht das Kriterium der Aktualität, sodass es auch hier zu Veränderungen gekommen ist. Insgesamt kann unter Berücksichtigung der Quantität der Einträge ein positiver Trend zur Anwendung der Blockchain in der Energiewirtschaft erkannt werden, auch wenn viele der Einträge eine reale Anwendung noch schuldig bleiben. Der Unterschied zwischen den Einträgen liegt besonders in dem Einzugsbereich der P2P-Handelsplattform (regional, überregional, landesweit, grenzüberschreitend).

Auch im Bereich „Anlagenmanagement/Netze/Metering“ wird eine steigende Anzahl realer Anwendungen erkannt. So finden sich insgesamt 21 Fallbeispiele, welche die Blockchain in diesem Bereich anwenden, was ca. 17% der gesamten Blockchain-Anwendungen in der Energiewirtschaft entspricht.

In der Literatur wird der Blockchain insbesondere im Anwendungsfeld „Mobilität“, so zum Beispiel beim Abrechnen des Ladevorgangs von Elektroautos, ein erhebliches Potenzial zugeschrieben (BDEW 2017; Ffe 2018a). Tatsächlich lassen sich jedoch nur 7% der Aktivitäten diesem Anwendungsfeld zuordnen. Auch der Vergleich zur Studie des BDEW und PwC von vor zwei Jahren verdeutlicht die untergeordnete Rolle dieses Anwendungsbereichs für die Blockchain. Es kann keine nennenswerte Veränderung der Projekte, zu denen der vorläufigen Studie erkannt werden. Die Anzahl der Projekte aus diesem Bereich stagniert.

Mit über 20% der gesamten Blockchain-Anwendungen sind im Bereich „Stromhandel B2B/C2B und Zertifizierung“ ein großer Teil aller Projekte involviert. Grünstromjeton stellt beispielsweise eine Applikation zur Verfügung, die auf Basis von Wetterdaten, Stromerzeugung- und Verbrauch den lokalen physikalischen Anteil des erneuerbaren Stroms berechnet. Enerchain ist laut eigener Aussage die erste Blockchain-basierte Handelsplattform, die auf effiziente Weise Over-The-Counter-Handel ermöglicht, unabhängig von zentralen Instanzen. Hierdurch werden die Markteintrittsbarrieren für neue

Teilnehmer reduziert und ein technologisches Level-Playing-Field geschaffen. Das Projekt ist nach zwei jähriger Laufzeit mit Partnern aus dem europäischen Energiesektor im Mai 2019 online gegangen. Im Bereich „Entwickler / Sonstige“ befinden sich zum einen Unternehmen und Projekte, die sich mit der weiteren Entwicklung und Anwendung der Blockchain in der Energiewirtschaft beschäftigen. Zum anderen sind hier Unternehmen gelistet, die zwar der Energiewirtschaft zugeordnet, jedoch nicht in eine der klar definierten Kategorien eingeordnet werden können. Ein Beispiel hierfür ist M-PAYG. M-PAYG ermöglicht die Bezahlung von Solarstrom über das Mobilfunknetz. Bei Bezahlung werden die auf der Blockchain registrierten Batterien freigeschaltet und der Kunde kann Strom beziehen, welcher vorher von einer Photovoltaikanlage erzeugt wurde. Es entsteht ein Prepaid-Stromvertrag auf wöchentlicher oder monatlicher Auflösung. Entwickelt wurde diese Methode vor allem für den Markt in Entwicklungsländern.

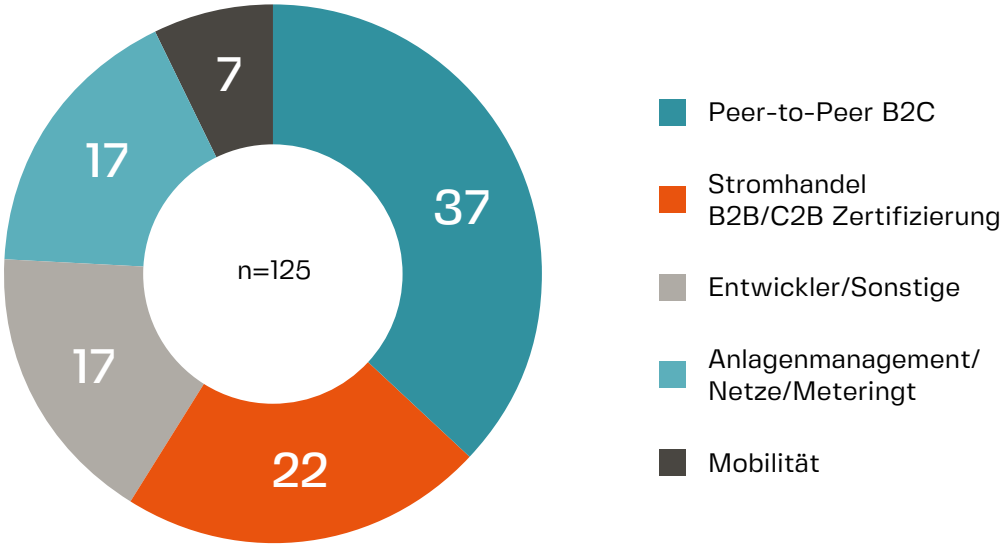

Abbildung 12: Blockchain-Anwendungen in der Energiewirtschaft nach Anwendungsbereichen in Prozent

3.2.3 Entwicklung der Blockchain-Plattformen

Unternehmen greifen häufiger auf Blockchain Lösungen zurück

Im Rahmen der Untersuchung wurde insbesondere auf Quellen zurückgegriffen, die von den ausübenden Akteuren öffentlich zur Verfügung gestellt werden, so in etwa „White Paper“ oder Internetseiten. Dabei gestaltete es sich als schwierig, fundierte Aussagen zu den jeweilig eingesetzten Plattformen der Einträge zu finden. Zwar bezeichnet die

„Blockchain-Community“ sich selbst und vor allem den Umgang mit Daten und Wissen als transparent, jedoch zeigte die Recherche, dass dies in der Realität nur bedingt zutrifft. Viele Unternehmen sind nicht dazu bereit, die von ihnen gewählte Plattformen transparent darzulegen. So konnten die genutzten Anbieter der Blockchain-Plattform, wie in Abbildung 13 dargestellt, bei 35% der identifizierten Anwendungsfälle nicht mit Sicherheit festgestellt werden.
Die Mehrheit der Unternehmen, welche die verwendete Plattform preisgeben, stützt sich auf die öffentliche Ethereum-Blockchain. 33% aller aufgeführten Unternehmen greifen somit auf den Dienst der etablierten Blockchain-Plattform zurück. In der Annahme, dass die nicht identifizierten Einträge ein ähnliches Muster aufweisen, wie die identifizierten, kann davon ausgegangen werden, dass insgesamt noch mehr Anwender auf die Ethereum Blockchain zurückgreifen. Einen wachsenden Anteil nehmen jedoch Blockchains ein, die von einem Anbieter zur Verfügung gestellt werden. Hierbei handelt es sich um Anbieter wie der EWF, Hyperledger und Tendermint, die für Anwender eine Blockchain-Lösung als Service bereitstellen.
Durch solche Services ist es für Unternehmen erheblich einfacher geworden, ihre Geschäftsmodelle auf einer Blockchain zu implementieren. Die Anbieter stellen hierfür den Unternehmen eigene Möglichkeiten zur Erstellung von Applikationen zur Verfügung und kümmern sich selbst um die dahinterliegende Blockchain. Als Unternehmen kann man sich dadurch vollkommen auf die Entwicklung der Geschäftsidee konzentrieren und benötigt innerhalb des Unternehmens kein aufwendiges Wissen für die Implementierung auf einer Blockchain. Je nach Anbieter kann hierbei auf ein vorhandenes Netzwerk zurückgegriffen werden (EWF) oder ein internes, eigenes Netzwerk nutzen, auf welchem eine Blockchain ausgeführt wird (Hyperledger).

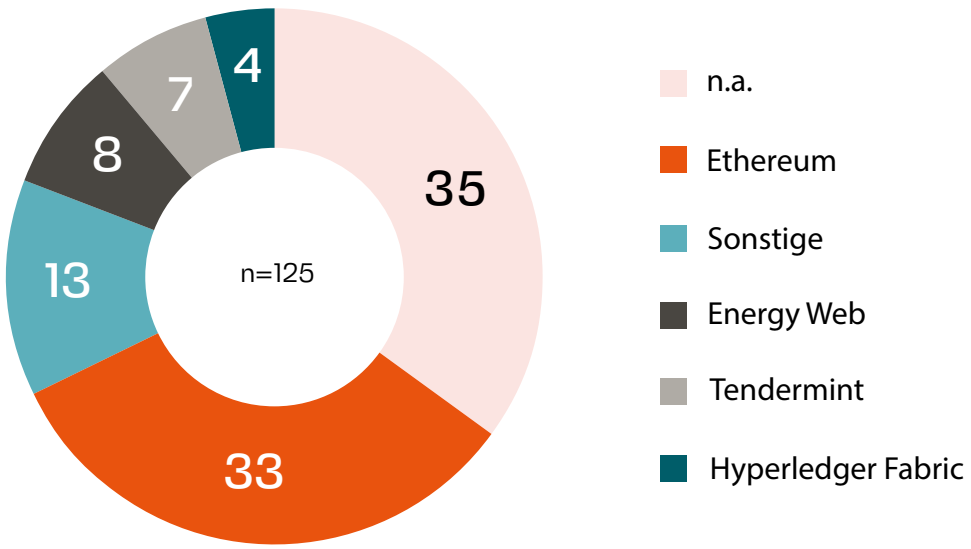

Abbildung 13: Verteilung nach genutzter Plattform in Prozent

Mit 8% der gefundenen Anwendungen hält die EWF bereits einen nennenswerten Anteil aller Blockchain-Projekte. Die von der EWF zur Verfügung gestellte Plattform „Energy Web Link“ wurde gezielt für die Anwendung im Energiesektor entwickelt, sodass sie auf die regulatorischen und rechtlichen Rahmenbedingungen angepasst ist. Auch Tendermint nimmt mit 7% bereits einen messbaren Marktanteil ein. So ist beispielsweise das Brooklyn Microgrid, das Leuchtturmprojekt im Bereich von P2P-Plattformen, in Zusammenarbeit mit Tendermint realisiert worden.
Das unter der Linux Foundation gelistete Projekt Hyperledger bietet mit Hyperledger Fabric eine private Blockchain an, die vom Unternehmen auf seine Bedürfnisse frei zugeschnitten werden kann. Insgesamt nutzen 4 % der untersuchten Marktteilnehmer diese Flexibilität, um mit Hilfe der Hyperledger Fabric ihre Idee umzusetzen.

3.2.4 Entwicklung in den Konsensmechanismen: Die Notwendigkeit zur Anpassung

Die Ressourcenintensität ist immer noch nicht transparent darstellbar

Die medial populäre Diskussion um den immensen Ressourcenverbrauch von Blockchain-Netzwerken ist beinah ausschließlich in der Wahl des *Konsensmechanismus* begründet. Entsprechend der Ausführungen in Kapitel 2.5 unterscheiden sich die jeweiligen *Konsensmechanismen* in der Rechenintensität, die von den validierenden Teilnehmern aufgebracht werden muss. Auch wenn weitere Faktoren, wie zum Beispiel die Größe des Netzwerks, natürlich von Relevanz sind und sich entsprechend ein anderes Bild ergeben kann, ist es der *PoW-Konsensmechanismus*, der durch den Rechenwettbewerb zum Finden des Konsenses im Allgemeinen bei vergleichbaren äußeren Umständen den höchsten Stromverbrauch verzeichnet.
Um die Ressourcenintensität bzw. den Stromverbrauch eines Blockchain-Netzwerks besser zu verstehen, muss im ersten Schritt das Konzept der *difficulty* erörtert werden. Mit der Einführung von Bitcoin und anderen alternativen *Coins*, wurde auch ein Mechanismus eingeführt, der Algorithmen fortlaufend neu ausrichten kann. Bei Bitcoin wird die *difficulty* Zielzeit $T_{difficulty}$ durch die Gleichung 1 berechnet, wobei der Zeitraum der vorherigen Berechnung der Blöcke T_{alt} durch dem Zeitraum der Berechnung der aktuellen Blöcke T_{neu} dividiert wird (Walker 2015). Das Ergebnis $T_{difficulty}$ dient dann als neuer Multiplikator für die Lösung des kryptographischen Rätsels der nächsten Blöcke. Ist das Ergebnis größer als 1, steigt die *difficulty*; ist das Ergebnis kleiner als 1, sinkt sie.[10] Bei anderen Blockchain-Lösungen kann die Berechnung der *difficulty* durchaus anders aussehen.

$$T_{difficulty} = \frac{T_{alt}}{T_{neu}} \qquad (1)$$

Die Idee hinter der *difficulty* Regelung beim Bitcoin ist, dass das Erstellen von 2016 Blöcken etwa zwei Wochen dauert; das entspricht ca. 10 Minuten zwischen den einzelnen Blöcken. Im Falle, dass die Berechnung von 2016 Blöcken länger als zwei Wochen dauert, wird die *difficulty* verringert. Falls es weniger als zwei Wochen dauert, wird die *difficulty* dementsprechend erhöht. Grundgedanke dahinter ist der Versuch, der technologischen Weiterentwicklung von Hardware mit der Justierung des Algorithmus über die Blockgenerierungszeit entgegenzuwirken. Dies änderte sich grundlegend mit der Einführung von ASICs[11] Mitte 2013 (Tardi 2019). Damals stieg die *difficulty* stark an (vgl. Abbildung 14), da man nach einem lang anhaltend konstanten *difficulty* Niveau nun Hardware zur Verfügung hatte, die speziell für das *mining* von Bitcoin entwickelt wurde und deutlich schneller und effizienter bei der Berechnung von Blöcken war, als die zuvor benutzten

[10] *Die difficulty wird sich höchstens um den Faktor 4 (für alle Ergebnisse größer gleich 4) oder minimal um den Faktor 0,25 (für alle Ergebnisse kleiner gleich 0,25) anpassen. Damit soll ein abrupter Wechsel von einer difficulty zur nächsten verhindert werden.*

[11] *ASIC steht für „application-specific integrated circuit" und ist ein Gerät, das ausschließlich für den Zweck des mining von digitalen Währungen konzipiert wurde. Im Allgemeinen ist jeder ASIC-miner ausschließlich für Berechnungen einer bestimmten digitalen Währung ausgelegt. Somit kann ein Bitcoin-ASIC-Miner nur Bitcoin minen.*

handelsüblichen Computer- und Grafikkartenprozessoren. Zum Vergleich: Ein ASIC Bitcoin Miner „Antminer S9“ berechnet 13 Billionen *hashes* bei etwa 0,1 nJ (dies entspricht 10^{-9} Joule) Energieaufwand pro *hash*. Dies ist etwa 200.000 mal schneller und 40.000 mal energieeffizienter als eine hochmoderne Multi-Core-CPU (Stand 2017) (Ren und Devadas 2017). Die Gesamtentwicklung der *difficulty* im Bitcoin-Netzwerk kann der folgenden Grafik entnommen werden (BTC.com 2020):

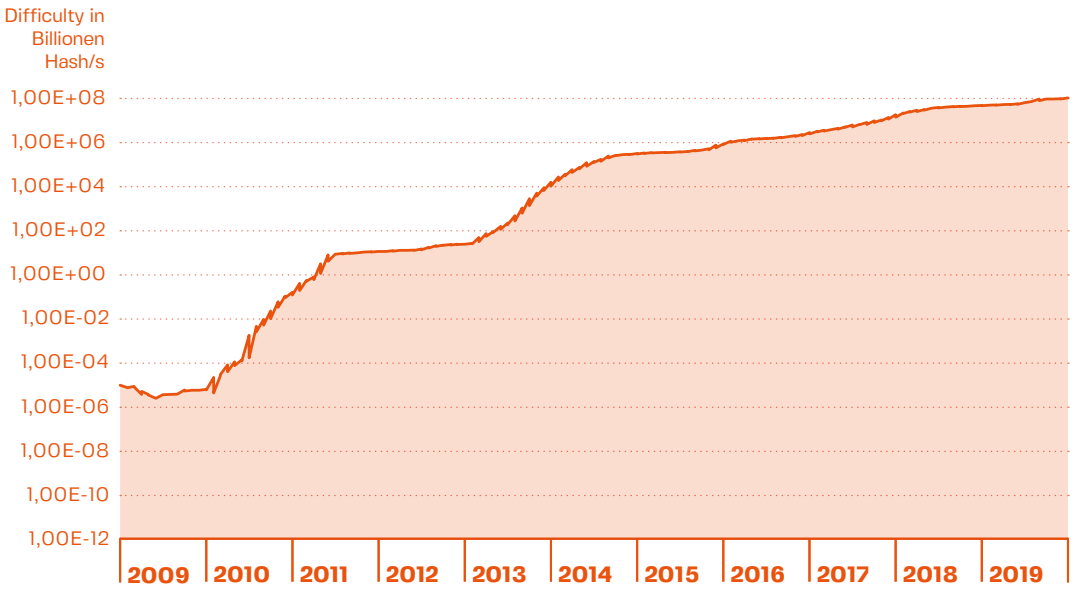

Abbildung 14: Entwicklung der durchschnittlichen hash-rate des Bitcoin Netzwerks

Zwar geht die *difficulty* das „ASICs-Problem“ mit einer ständigen Korrektur des Algorithmus an, jedoch ist ein Nachteil des *PoW-Konsensmechanismus*, dass dieser aufgrund der alleinigen Zeitrestriktion nicht ASIC-resistent ist und dies zu Machtzentralisierung führen kann. An zwei Beispielen lässt sich diese Schwäche anschaulich erklären. Erstens kann es zu Problemen bei der Einführung eines neuen *Coins* kommen, der auf dem gleichen SHA256 Algorithmus basiert wie der Bitcoin; gleiches gilt auch für andere *Coins*. Dies kann dazu führen, dass das Netzwerk um den gerade eingeführten *Coin* von *minern* dominiert wird, die den *difficulty*-Mechanismus durch den technologischen Vorsprung der Hardware unverhältnismäßig schnell verändern würden. Dieser Umstand führt unmittelbar zum zweiten Beispiel, den sogenannten Multipools[12]. Durch den gewinnbringend wechselnden Einsatz von Rechenleistung entsteht das Phänomen von „Pool-Hopping“, welches sich nachteilig auf eine Blockchain, und somit auf das Wachstum alternativer *Coins* auswirken kann. Beim Pool-Hopping treten *miner* einem Netzwerk nur bei, wenn die *difficulty* niedrig ist. Diese verlassen das Netzwerk sobald die *difficulty* nach oben korrigiert wird. Wird nach dem Verlassen nach einer definierten Zeit die *difficulty* wieder nach unten korrigiert, so treten die Pools dem Netzwerk wieder bei und nutzen die „vereinfachten“ Verhältnisse gewinnbringend aus. Verlässt der Pool an *minern* das Netzwerk komplett, da beispielsweise das Grundniveau

[12] *Ein Multipool ist eine Plattform für miner, die durch den alternierenden Abbau verschiedener Krypto-Währungen Gewinne maximiert. Miner können dabei wechselnd und barrierefrei an verschiedenen Pools teilnehmen.*

der *difficulty* eines bestimmten *Coins* zu hoch geworden ist, wird das Netzwerk für diesen einen dedizierten *Coin* nahezu unbenutzbar, da es für einzelne *miner* fast unmöglich ist profitabel im Netzwerk zu agieren und dieses im Sinne eines *node*-Netzwerks aufrecht zu erhalten (Bashir 2017). Die einzige Lösung für dieses Problem ist eine vorher bereits erwähnte *hard fork,* die allerdings von der Gemeinschaft oft als unerwünscht angesehen wird. Natürlich existieren einige Algorithmen, die zur Lösung dieses Problems entwickelt wurden. Diese Algorithmen basieren auf der Idee, verschiedene Parameter als Reaktion auf Änderungen der *hash*-rate zu verändern; diese Parameter umfassen beispielsweise die Anzahl der vorhergehenden Blöcke, Schwierigkeit der vorhergehenden Blöcke, Verhältnis der Anpassung und den Betrag, um den die Schwierigkeit nach oben oder unten angepasst werden kann. Nach Bashir (2017) sind Beispiele hierfür Komoto Gravity Well, Dark Gravity Wave, DigiShield und MIDAS, die von verschiedenen alternativen Krypto-Währungen verwendet werden. Da wir uns in dieser Studie aufgrund der Datenlage zur Ressourcenintensität nur auf Bitcoin beziehen, werden wir an dieser Stelle nicht weiter auf alternative Kryptowährungen und deren Algorithmen eingehen.
Die tatsächlichen gesamten Strombezüge teilnehmerstarker *PoW*-basierter Netzwerke, wie zum Beispiel Bitcoin oder Ethereum, lassen sich jedoch nur schwierig quantifizieren. Die Auswahl der eingesetzten Technik wird jedem *miner* selbst überlassen, sodass die individuellen Stromverbräuche teilnehmender Knoten mitunter stark voneinander abweichen können, obwohl sie im Rechenbetrieb nicht variieren, sondern stets auf voller Leistung betrieben werden müssen. Außerdem ist nicht ausgeschlossen, dass sich hinter einem teilnehmenden Knoten mehrere zusammengeschlossene Rechner verbergen, welche gemeinsam an der *hash calculation* teilnehmen. Es ist daher ein verbreiteter Ansatz, nur die untere Grenze des Stromverbrauchs zu approximieren (A. de Vries 2018). Dazu wird sich der aktuell effizientesten im Handel erhältlichen *mining* Maschine bedient; gemessen in Joule pro Gigahash, also Stromverbrauch pro gelöstes kryptographische Rätsel. Überschlägt man nun die Anzahl an Versuchen zur Lösung eines Rätsels pro Sekunde, also der *hash*-rate und der Zeit, die es bedarf einen neuen Block zu erstellen bei der gegebenen Schwierigkeit des kryptographischen Rätsels, ergibt sich aus simpler Multiplikation der Effizienz und der *hash*-rate die beschriebene untere Grenze des Strombezugs eines Netzwerks (A. de Vries 2018). Unter Annahme eines Antminer S9 mit einer Effizienz von 0.098 J/Gigahash und einer momentanen *hash*-rate von etwa 110.000.000 TH/s (Stand 28.01.2020, 01:00 Uhr) errechnet sich ein Strombezug des Bitcoin Netzwerks von 10,78 GW. Auf diesem Wege lässt sich der minimale jährliche Stromverbrauch für das Ethereum Netzwerk auf 8,16 TWh, der des Bitcoin Netzwerks auf 48,52 TWh (vgl. Abbildung 15), in etwa entsprechend des Stromverbrauchs von Österreich, approximieren (Digiconomist 2019). Eine direkte Aussage über die damit verbundenen CO_2-Emissionen ist mangels

Informationen über die Stromquellen nicht möglich. In der Literatur werden jedoch 34,733 Mio. t CO_2 aufgerufen, welche durch den *mining* Prozess innerhalb des Bitcoin-Netzwerks anfallen (Digiconomist 2019). Diese beeindruckenden Angaben zum Stromverbrauch unterschätzen die tatsächlichen Werte in jedem Fall jedoch um ein Vielfaches. In der

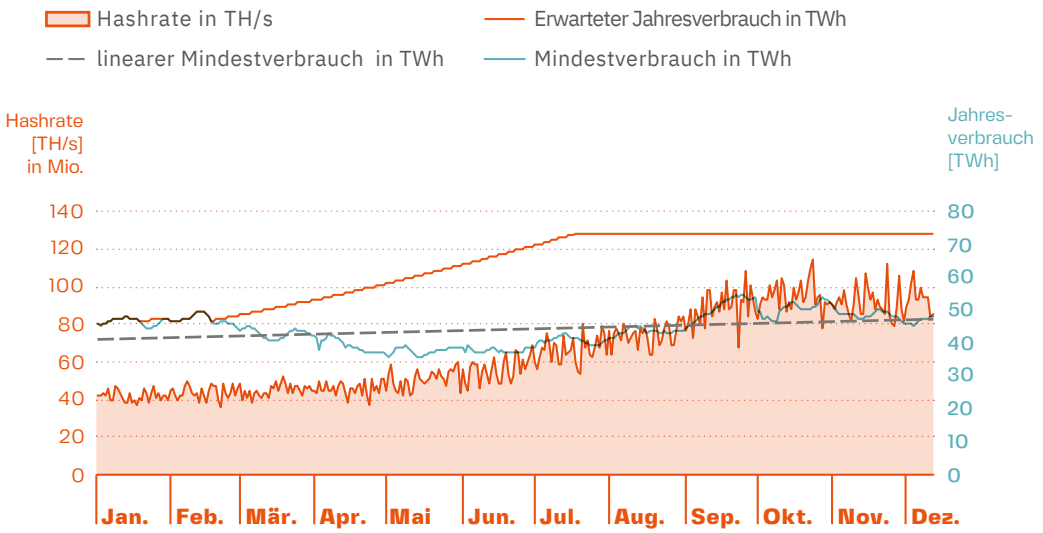

Abbildung 15: Energieverbrauch des Bitcoin Netzwerks in 2019

Regel sind teilnehmende Rechner zu Clustern zusammengeschlossen und stehen in unmittelbaren räumlichen Zusammenhang. Für den Betrieb solcher *mining*-Fabriken sind extreme Kühlaufwendungen notwendig, die ein Überhitzen der Geräte verhindern (A. de Vries 2018). Verlässliche Informationen über die so verursachten Strombezüge finden sich jedoch nicht.

Auch weitere alternative Ansätze zur Bestimmung des Stromverbrauchs der Blockchain-Netzwerke, so zum Beispiel ein ökonomischer Ansatz von A. de Vries (2018) oder Hayes (2017), welcher zur Bestimmung des *Bitcoin Energy Consumption Index* dient, können den tatsächlichen Verbrauch nur nähern, erzielen jedoch vergleichbare Resultate, wie die vorangegangenen Schätzungen.

Unter anderem wegen dieser Ressourcenproblematik entwickelten sich in der Vergangenheit die alternativen *Konsensmechanismen PoA* sowie *PoS*. Es erscheint durchaus nachvollziehbar, dass diese Mechanismen unter Umständen einen geringeren Stromverbrauch benötigen als der *PoW-Konsensmechanismus*. Genau quantifizieren lässt sich dieser jedoch nicht. So bleibt es an dieser Stelle nur die eigenen Angaben der EWF anzuführen, die angibt, mit dem *PoA*-Mechanismen einen 2 bis 3-fach geringeren Energieverbrauch zu haben, als im Fall einer *PoW*-Anwendung des Ethereum-Netzwerks (energy web foundation 2019). Ein nachweislicher quantitativer Vergleich konnte von den Autoren nicht gefunden werden, sodass an dieser Stelle weiterer Forschungsbedarf festgestellt werden kann.

Auch offenbarte die Recherche nur wenige Einblicke in die derzeit tatsächlich verwendeten *Konsensmechanismen* der jeweiligen Anwendungsbeispiele. Offenbar gilt auch hier, dass die aktiven Unternehmen zwar völlige Transparenz suggerieren, jedoch nicht tatsächlich ausüben. Somit kann nur durch Rückschluss auf die verwendete Blockchain-Plattform auf den jeweils verwendeten *Konsensmechanismus* geschlossen werden.
Für solche Netzwerke, die durch eine monolithische *Softwarearchitektur* aufweisen, lassen sich jedoch Rückschlüsse auf den eingesetzten *Konsensmechanismus* schließen. Dies ist sowohl im Ethereum als auch im Bitcoin Netzwerk der Fall. Beide Netzwerke verwenden den *PoW-Konsensmechanismus* (coindesk 2019; Ffe 2018b). Entsprechend des vorherigen Kapitels verwenden also mindestens 33 % der betrachteten Anwendungen in der Energiewirtschaft noch immer den *PoW-Konsensmechanismus*. Dies könnte sich im Zuge der Einführung von *Casper* bei Ethereum verringern, sofern sich Unternehmen entscheiden den angestrebten *hard fork* zu akzeptieren und in der Folge den *PoS-Konsensmechanismus* zu verwenden. Die EWF, in 8% der Anwendungsfälle als genutzte Blockchain-Plattform detektiert, kommuniziert bereits öffentlich ihr Vertrauen in den *PoA-Konsensmechanismus*, entsprechend der verbreiteten Anwendung in konsortiale *Infrastrukturen* (energy web foundation 2019).
Das Hyperledger Netzwerk verfolgt auch den *PoA-Konsensmechanismus*, in dem einige Knoten eines Konsortiums gesonderte Rechte besitzen. Jedoch variieren Details je nach Fallbeispiel, sodass Hyperledger selbst verschiedenste Ausprägungen des BFT als Ursprung des *Konsensmechanismus* angibt, welcher modifiziert wird. Innerhalb von Hyperledger werden so derzeit vor allem *Simplified Byzantine Fault Tolerance (SBFT)* sowie der Honey Badger BFT als *Konsensmechanismen* weiterentwickelt (Hyperledger 2018).
Ein ähnliches Konzept wird von Tendermint unterstützt. Tendermint empfiehlt in öffentlichen Netzwerken einen *PBFT* zusammen mit *PoS* mit dem Unterschied, dass die Knoten *Coins* als Einsatz hinterlegen müssen. Wird ein validierender Knoten als unehrlich befunden, wird er monetär bestraft, in dem die *Coins* einbehalten werden (Ffe 2018b) (Cosmos 2018).

3.3 Erkenntnisse aus der Marktanalyse

Ethereum weiter vorne, Markt immer noch teilweise intransparent

Die Marktanalyse offenbarte, dass Blockchain in der Energiewirtschaft bereits über den gesamten Globus verteilt in breitem Anwendungsspektrum, genutzt wird. Überragend tritt Deutschland in Erscheinung, in dem 31 der insgesamt 132 gefundenen Anwendungsfälle beheimatet sind. Die Mehrheit solcher Anwendungsfälle, nämlich 37% sind im Bereich „Peer-to-Peer B2C“ angesiedelt. Dabei handelt es sich meist um digitale Marktplätze für lokal begrenzten Stromhandel von erneuerbarem Strom. Die wenigsten Anwendungsfälle wurden im Bereich „Mobilität“ gefunden, obwohl dieser Branche medial sehr hohes Potenzial zugeschrieben wird.
Ebenso wurde in der Marktanalyse gezeigt, dass die Ethereum-Plattform und einhergehend der von Ethereum verwendete *PoW-Konsensmechanismus* mit mindestens 33 % immer noch die größte Plattform für energiewirtschaftliche Anwendungen im Blockchain-Bereich (weltweit) darstellt. Durchaus konnte auch ein Anstieg von Anbietern wie EWF, Tendermint und Hyperledger beobachtet werden, die ihre Blockchain als eine Art Service für Nutzer anbieten. Zusammen haben diese Anbieter zum heutigen Zeitpunkt (Anfang 2020) bereits einen Marktanteil von 19%. Das Gesamtbild könnte anders ausfallen, wenn die große Intransparenz des Marktes in die Analyse mit einbezogen werden könnte, da immer noch ein großer Teil der Unternehmen bzw. Projekte ihre Blockchain-Plattform für die jeweilige Anwendung nicht öffentlich bekannt geben. Dies wäre in Zeiten des Klimawandels und der damit geforderten Transparenz zum Thema Energieintensität jedoch dringend erforderlich. Auch die langanhaltende Diskussion über die Einführung von Casper, der Umstellung von Ethereum vom *PoW*-zum *PoS-Konsensmechanismus* könnte noch weitere Bewegung in den Markt bringen und gleichzeitig auch die Chance eröffnen, die Anwendung des *PoS-Konsensmechanismus* weiter zu fördern und dies ins Verhältnis mit *PoW* zu setzen. Fraglich bleibt allerdings, welche Auswirkungen dies auf bisherige Geschäftsmodelle hat, die bisher auf Ethereum aufbauen. Durch den monolithischen Ansatz der Ethereum Blockchain kann dies zu erheblichen Problemen der Kompatibilität einzelner *forks* führen. Daher ist es wahrscheinlicher, dass bisherige Anwendungen auch weiterhin auf dem *PoW-Konsensmechanismus* setzen werden. In jedem Fall wird es auch in Zukunft eine große Herausforderung sein, den Energieverbrauch von Blockchain-Lösungen wissenschaftlich hinreichend genau zu untersuchen. Eine genaue Beobachtung der weitere Entwicklung in diesem Bereich ist somit unabdingbar: nicht nur, um die bereits

etablierten *Konsensmechanismen* besser auswerten, sondern auch, um die neu eingeführten Technologien von Anfang an besser begleiten und eine Bewertung hinsichtlich der verschiedenen Blockchain-Technologien und deren Ressourcenintensität abgeben zu können.

Abschließendes Fazit und Diskussion

Mit dieser Studie konnten wir einige interessante Einblicke in das Thema der Blockchain im Anwendungskontext der Energiewirtschaft gewinnen. Mit einer strikten Unterteilung der Blockchain-Technologie in businessrelevante Fragestellungen und den damit verbundenen Lösungsansätzen, war es unser Ziel, heutigen Entscheidungsträgern Direktionen auf dem Weg der Überprüfung zur Umsetzbarkeit einer Blockchain-Technologie für ihre Anwendung zu geben. Aus unserer Perspektive fehlte genau dieses Transparenzinstrument in einem stark fragmentierten und teilweise schwer zugänglichen Marktumfeld. Weiterhin konnte die ganzheitliche Marktanalyse zeigen, dass zwar immer noch die etablierten *Konsensmechanismen* den energiewirtschaftlichen Markt dominieren, jedoch auch neue Plattformen bereits heute in der Entwicklung und Anwendung sind. Insgesamt ist zu beobachten, dass die Anzahl der Blockchain Lösungen und die aus der Modularität hervorgegangenen Kombinationen eine Vielzahl an maßgeschneiderten Lösungen möglich machen. Dies führt unter anderem dazu, dass auch im Blockchain Markt ein stetig wachsendes Aufkommen von Plattformanbietern zu beobachten ist – ein Phänomen, dass wir aktuell weltweit in einer Vielzahl von Märkten beobachten können. Technische Lösungen, die Schnittstellen ermöglichen und Blockchains miteinander kommunizieren lassen, könnten daher in Zukunft eine besondere Rolle spielen. Tendermint ist mit Cosmos dieser Idee schon nachgekommen unter der Vermutung, dass Blockchains in Zukunft auf spezielle Problemlösungen zugeschnitten sein werden und dennoch übergeordnet koordiniert werden müssen. Ob sich mit dem Mehrangebot von Blockchain Lösungen tragfähige Geschäftsmodelle (sowohl für den Plattformanbieter als auch für den Nutzer) entwickeln, wird die Zukunft zeigen. Festzuhalten gilt, dass es keine allumfassende Blockchain-Lösung gibt, die, wie oft im Vorfeld angenommen, die Energiewirtschaft grundsätzlich umkrempelt. Vielmehr haben einzelne Module oder Besonderheiten der Blockchain (z. B. *Smart Contracts*) das Potenzial für ganz spezifische, maßgeschneiderte Lösungen unterstützend zu wirken.
Gleichzeitig herrscht aber auch eine große Intransparenz im Markt, welche dem Kredo der Blockchain – also der allgemeinen Transparenzschaffung – grundlegend widerspricht. Dies führt unter anderem dazu, dass es noch schwieriger wird, ressourcenbezogene Analysen und der damit einhergehenden Vergleichbarkeit der einzelnen Blockchain-Lösungen bzw. *Konsensmechanismen* zu erstellen. Es besteht also großer Handlungsbedarf. Hierzu wäre es wichtig im Nachgang zu dieser Studie eine detaillierte Analyse der nicht weiter spezifizierten Blockchain Plattformen (siehe Abbildung 13 in hell-orange hinterlegt) auszuführen, und gleichzeitig gemeinsam mit aktuellen Lösungen am Markt

eine Metrik zu entwickeln, mittels der man sich der ungelösten Intransparenz stellen könnte. Eine langfristige Verfolgung der Entwicklungen sowie die Erstellung weiterer wissenschaftlicher Studien ist somit sinnvoll. Weiterhin erscheint es – aufbauend auf dieser Studie – logisch, im nächsten Schritt die technische Realisierbarkeit und die damit verbundenen Implementierungsprozesse zu untersuchen. Dies würde dem Leser nicht nur eine bessere Einschätzung zu den technischen Hürden geben, sondern auch zeigen, inwiefern verschiedene *Konsensmechanismen* vergleichbar sind und welche Perfomance für welchen Anwendungsfall notwendig und realisierbar ist.

Zuletzt bleibt noch die Beobachtung, welche uns während der Arbeit mehrfach aufgefallen ist: das unübersichtliche Potpourri an Begrifflichkeiten und die damit einhergehende Zugangsbarriere. Um den Zugang zum Thema grundlegend zu erleichtern, ist es wichtig feststehende Definitionen zu formulieren und diese als Stand der Technik publik zu machen. So hat beispielsweise der „Verband der Elektrotechnik Elektronik Informationstechnik“ (VDE) eine Task Force „Energy Blockchain“ ins Leben gerufen, die Begrifflichkeiten rund um das Thema Blockchain in einem Leitfaden definiert hat (Klebsch et al. 2019), um sich nicht nur auf ein gemeinsames Wording zu einigen, sondern auch den Grundstein für eine Standardisierung in diesem Bereich einzuführen. Ein, unserer Meinung nach, sehr wichtiger Schritt für zukünftige Entwicklungen im Blockchain-Bereich.

Glossar

Anhang

Liste mit Unternehmen und Projekten, welche nicht in die Übersicht aufgenommen wurden:

Assetron Energy
Initial Coin Offering 2017, seitdem jedoch keine weiteren Fortschritte. Möglicherweise Probleme mit der gewählten Blockchain-Plattform (Waves).

Bankymoon
Blockchain-Entwickler ohne direkten Bezug zur Energiewirtschaft.

BCDC
Nicht mehr aktiv.

BLOC
Blockchain-Entwickler ohne direkten Bezug zur Energiewirtschaft.

Blockchain Future Lab
Kein direkter Bezug zur Energiewirtschaft.

CoSol
Keine Nutzung von Blockchain.

ClimateCoin
Nutzung der Blockchain zur Erstellung eines Carbon Footprint. Fällt aktuell nicht in die Definition der Energiewirtschaft.

Divvi
Es konnten keine Informationen zu dem Unternehmen gefunden werden.

Dooak
Es konnten keine Informationen zu dem Unternehmen gefunden werden.

Ecochain
Es konnten keine Informationen zu dem Unternehmen gefunden werden.

Echarge
Informationslage diffus.

Elegant
Akzeptieren Bitcoin als Zahlungsmittel.

EMotorwerk
Hersteller von Wallboxen und Zusammenarbeit mit Share&Charge.

Enercity
Akzeptieren Bitcoin als Zahlungsmittel.

EnergoLabs
Internetauftritt nicht mehr erreichbar. Wöchentliches Update auf medium.com wurde Ende 2018 eingestellt.

Energy unlocked
Start-up Accelerator ohne direkten Kontakt zur Blockchain.

Enerport
Projekt wurde planmäßig 2019 beendet.

ETH@Energy
Es konnten keine Informationen zu dem Unternehmen gefunden werden.

Etherisc
Kein direkter Bezug zur Energiewirtschaft.

Everty
Keine Nutzung von Blockchain.

Evolve Power
Es konnten keine Informationen zu dem Unternehmen gefunden werden.

Fintec4good
Blockchain-Accelerator ohne direkten Bezug zur Energiewirtschaft.

Farad
Informationslage diffus.

Fortum
Keine Nutzung von Blockchain.

Grid+
Zahlungsanbieter für Blockchain ohne direkten Bezug zur Energiewirtschaft.

GridX
Keine Nutzung der Blockchain.

Guardtime
Keine Nutzung der Blockchain.

HydroMiner
Miner, der Strom aus erneuerbaren Quellen bezieht.

Inuk
Tracking von Emissionen für Privatpersonen. Fällt nicht unter die Definition der Energiewirtschaft.

Linq
Blockchain-Plattform der NASDAQ. Kein direkter Kontakt zur Energiewirtschaft.

Lisk
Kein direkter Kontakt zur Energiewirtschaft.

Lumenaza
Keine Nutzung von Blockchain.

Lykke
Kein direkter Kontakt zur Energiewirtschaft.

Marubeni
Kein direkter Kontakt zur Energiewirtschaft.

Oursolargrid & ITP
Letzte Informationen aus 2017. Darüber hinaus konnte keine Aktivität festgestellt werden.

Oxygen Initiative
Zahlungsanbieter, der mit Share&Charge zusammenarbeitet.

Parity
Kein direkter Kontakt zur Energiewirtschaft.

PowerTree
Nicht mehr aktiv.

PRTI
Kein direkter Kontakt zur Energiewirtschaft.

Smart Solar
Letzte Informationen aus dem Jahr 2016.

TavridaElectric
Kooperation mit Qiwi, jedoch seit Bekanntwerden der Partnerschaft im Jahr 2017 keine weiteren Informationen verfügbar.

WanXiang Blockchain Labs
Kein direkter Kontakt zur Energiewirtschaft.

XinFin
Kein direkter Kontakt zur Energiewirtschaft.

Literaturverzeichnis

A. de Vries (2018): Bitcoin´s Growing Energy Problem. In: Joule (2), S. 801–809.

Allen, Ben (2017): Turing-completeness: How Ethereum does what it does. The Bitcoin Mag. Online verfügbar unter https://thebitcoinmag.com/turing-completeness-ethereum/1712/, zuletzt geprüft am 27.04.2020.

Andoni, Merlinda; Robu, Valentin; Flynn, David; Abram, Simone; Geach, Dale; Jenkins, David et al. (2019): Blockchain technology in the energy sector: A systematic review of challenges and opportunities. In: Renewable and Sustainable Energy Reviews 100, S. 143–174. DOI: 10.1016/j.rser.2018.10.014.

Azimdoust, Negin (2019): Hyperledger Fabric: Überblick und Fazit. Online verfügbar unter https://blockchainwelt.de/hyperledger-fabric-ueberblick-und-fazit/, zuletzt geprüft am 11.02.2020.

Back, Adam; Corallo, Matt; et. al (2014): Enabling Blockchain Innovations with Pegged Sidechains. Online verfügbar unter https://blockstream.com/sidechains.pdf, zuletzt geprüft am 20.03.2020.

Bashir, Imran (2017): Mastering Blockchain - Master the theoretical and technical foundations of Blockchain technology and explore future of Blockchain technology. 1st edition: Packt Publishing.

BDEW (2017): Blockchain in der Energiewirtschaft. Online verfügbar unter https://www.bdew.de/service/publikationen/blockchain-energiewirtschaft/, zuletzt geprüft am 23.06.2019.

Belchior, Rafael (2019): Hyperledger Fabric: Technical Overview. Online verfügbar unter https://towardsdatascience.com/hyperledger-fabric-technical-overview-a63046c2a430, zuletzt geprüft am 11.02.2020.

BMWi; BMF (2019): Blockchain-Strategie der Bundesregierung. Online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10, zuletzt geprüft am 10.10.2019.

BTC.com (2020): Statistik Difficulty. Online verfügbar unter https://btc.com/stats/diff, zuletzt geprüft am 11.20.2020.

Buchman, Ethan (2016): Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. Masterarbeit. The University of Guelph, Ontario. Online verfügbar unter https://atrium.lib.uoguelph.ca/xmlui/bitstream/handle/10214/9769/Buchman_Ethan_201606_MAsc.pdf?sequence=7&isAllowed=y, zuletzt geprüft am 24.01.2020.

Buntinx, JP. (2017): What is Delegated Byzantine Fault Tolerance? The Merkle. Online verfügbar unter https://themerkle.com/what-is-delegated-byzantine-fault-tolerance/, zuletzt geprüft am 27.01.2020.

Buterin, Vitalik (2013): Ethereum White Paper: A next-generation smart contract and decentralized application platform. Online verfügbar unter https://github.com/ethereum/wiki/wiki/White-Paper, zuletzt aktualisiert am 2019, zuletzt geprüft am 11.02.2020.

Buterin, Vitalik (2016): A Proof of Stake Design Philosophy. Online verfügbar unter https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51, zuletzt geprüft am 27.03.2020.

Caetano, Richard (2015): Learning Bitcoin. 1st edition: Packt Publishing.

Chen, Richard (2018): A Brief Overview of dApp Development. Online verfügbar unter https://thecontrol.co/a-brief-overview-of-dapp-development-b8ac1648322c, zuletzt geprüft am 27.04.2020.

coindesk (2019): Ethereum 101. What is Ethereum. coindesk. Online verfügbar unter https://www.coindesk.com/learn/ethereum-101/what-is-ethereum, zuletzt geprüft am 11.12.2019.

Cosmos (2018): Tendermint Explained — Bringing BFT-based PoS to the Public Blockchain Domain. Cosmos. Online verfügbar unter https://blog.cosmos.network/tendermint-explained-bringing-bft-based-pos-to-the-public-blockchain-domain-f22e274a0fdb, zuletzt geprüft am 11.02.2020.

Crypto51 (2020): PoW 51% Attack Cost. Online verfügbar unter https://www.crypto51.app/, zuletzt geprüft am 04.02.2020.

dena (2016): Blockchain in der Energiewende. Online verfügbar unter https://www.dena.de/newsroom/publikationsdetailansicht/pub/studie-blockchain-in-der-energiewende/, zuletzt geprüft am 04.05.2019.

dena (2019): Blockchain in der integrierten Energiewende. Online verfügbar unter https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2019/Studie_Blockchain_Deutsches_Executive_Summary.pdf, zuletzt geprüft am 13.05.2019.

Digiconomist (2019): Bitcoin Energy Consumption Index. Digiconomist. Online verfügbar unter https://digiconomist.net/bitcoin-energy-consumption, zuletzt geprüft am 12.11.19.

energy web foundation (2019): The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform. energy web foundation. Online verfügbar unter https://github.com/energywebfoundation/paper/blob/master/EWF-Paper-v2.pdf, zuletzt geprüft am 11.02.2020.

Ffe (2018a): Die Blockchaintechnologie - Chance zur Transfomation der Energiewirtschaft? - Berichtsteil Anwendungsfälle. Online verfügbar unter https://www.ffe.de/themen-und-methoden/digitalisierung/846-chancen-der-blockchain-technologie-in-der-energiewirtschaft-anwendungsfaelle, zuletzt geprüft am 04.03.2019.

Ffe (2018b): Die Blockchaintechnologie - Chance zur Transfomation der Energiewirtschaft? - Berichtsteil Technologiebeschreibung, zuletzt geprüft am 10.12.2019.

Frankenwald, Jake (2019): Soft Fork. Hg. v. Investopedia. Online verfügbar unter https://www.investopedia.com/terms/s/soft-fork.asp, zuletzt aktualisiert am 06.02.2020, zuletzt geprüft am 20.04.2020.

Garousi, Vahid; Felderer, Michael; Mäntylä, Mika V. (2019): Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. In: Information and Software Technology 106, S. 101–121. DOI: 10.1016/j.infsof.2018.09.006.

Gupta, Manav (2018): Blockchain for dummies. 2nd IBM limited edition. Hoboken, NJ: John Wiley & Sons, Inc (For dummies).
Hayes, Adam S. (2017): Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. In: Telematics and Informatics 34 (7), S. 1308–1321. DOI: 10.1016/j.tele.2016.05.005.

Higgins, Julian P. T.; Green, Sally (Hg.) (2012): Cochrane handbook for systematic reviews of interventions. Repr. Chichester: Wiley-Blackwell (Cochrane book series).

Hyperledger (2018): Hyperledger Architecture, Volume 1. Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus. Hyperledger The Linux Foundation.

Hyperledger (2019): A Blockchain Platform for the Eneterprise. Online verfügbar unter https://hyperledger-fabric.readthedocs.io/en/release-2.0/index.html, zuletzt geprüft am 11.02.2020.

Interchain Foundation (2017): Consensus Compare: Casper vs. Tendermint. Online verfügbar unter https://blog.cosmos.network/consensus-compare-casper-vs-tendermint-6df154ad56ae, zuletzt geprüft am 11.02.2020.

Jahn, Andreas; Lenck, Thorsten; Graichen, Patrik (2019): Netzentgelte 2019: Zeit für Reformen. Impuls. Online verfügbar unter https://www.agora-energiewende.de/fileadmin2/Projekte/2014/transparente-energiewirtschaft/Agora_Netzentgelte_2019.pdf, zuletzt geprüft am 11.01.2020.

Johnson, Sandra; Robinson, Peter; Brainard, John (2019): Sidechains and interoperability. Online verfügbar unter http://arxiv.org/pdf/1903.04077v2, zuletzt geprüft am 22.02.2020.

Khullar, Kashish (2019): Implementing PBFT in Blockchain. Online verfügbar unter https://medium.com/coinmonks/implementing-pbft-in-blockchain-12368c6c9548, zuletzt geprüft am 11.02.2020.

Klebsch, Wolfgang; Hallensleben, Sebastian; Kosslers, Sebastian (2019): Roter Faden durch das Thema Blockchain. Online verfügbar unter https://www.vde.com/resource/blob/1885856/1c616e33e550c2f387202e7b8b8ad53a/roter-faden-blockchain-download-data.pdf, zuletzt geprüft am 30.01.2020.

Labazova, Olga; Dehling, Tobias; Sunyaev, Ali (Hg.) (2018): From Hype to Reality: A Taxonomy of Blockchain Applications. 52nd Hawaii International Conference on System Sciences (HICSS 2019. Wailea, Maui, HI, USA, Forthcoming, 8.-11.01.2019.

M. Blederbeck (2016): Der DAO-Hack: Ein Blockchain-Krimi aus Sachsen. WIRED.de. Online verfügbar unter https://www.gq-magazin.de/auto-technik/article/wie-aus-dem-hack-des-blockchain-fonds-dao-ein-wirtschaftskrimi-wurde, zuletzt geprüft am 17.01.2020.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. Online verfügbar unter https://bitcoin.org/bitcoin.pdf, zuletzt geprüft am 15.04.2020.

Natoli, Christopher; Yu, Jiangshan; Gramoli, Vincent; Esteves-Verissimo, Paulo (2019): Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure. Online verfügbar unter http://arxiv.org/pdf/1908.08316v1, zuletzt geprüft am 11.03.2020.

Ogawa, Rodney T.; Malen, Betty (1991): Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method. In: Review of Educational Research 61 (3), S. 265–286. DOI: 10.3102/00346543061003265.

P. Fairley (2019): Ethereum Plans to Cut Its Absurd Energy Consumption by 99 Percent. IEEE Spectrum. Online verfügbar unter *https://spectrum.ieee.org/computing/networks/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent*, zuletzt geprüft am 11.12.2019.

POA Network (2017): Proof of Authority: consensus model with Identity at Stake. Online verfügbar unter *https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256*, zuletzt aktualisiert am 11.02.2020.

pv Magazine (2017): Wie Communities der Energiewende dienen. In: pv Magazine 09.2017, S. 52–54. Online verfügbar unter *https://www.strom.lumenaza.de/media/filer_public/a0/d2/a0d28af3-0df3-42ee-9194-2c6ca7630017/201709_pvmagazine_artikel.pdf*, zuletzt geprüft am 06.11.2019.

Reetz, Fabian (2019): Blockchain und das Klima. Online verfügbar unter *https://www.stiftung-nv.de/sites/default/files/blockchain_und_das_klima.pdf*, zuletzt geprüft am 24.11.2020.

Ren, Lin; Devadas, Srinivas (2017): Bandwidth Hard Functions for ASIC Resistance. Online verfügbar unter *https://eprint.iacr.org/2017/225.pdf*, zuletzt geprüft am 11.20.2020.

Seeley, Logan (2019): Introduction to Sawtooth PBFT. Online verfügbar unter *https://www.hyperledger.org/blog/2019/02/13/introduction-to-sawtooth-pbft*, zuletzt geprüft am 11.02.2020.

Sharma, Rakesh (2019): What Is Ethereum's "Difficulty Bomb"? Hg. v. Investopedia. Online verfügbar unter *https://www.investopedia.com/news/what-ethereums-difficulty-bomb/*, zuletzt aktualisiert am 25.06.2019.

Singh, Amritraj; Click, Kelly; Parizi, Reza M.; Zhang, Qi; Dehghantanha, Ali; Choo, Kim-Kwang Raymond (2020): Sidechain technologies in blockchain networks: An examination and state-of-the-art review. In: Journal of Network and Computer Applications 149, S. 102471. DOI: 10.1016/j.jnca.2019.102471.

Singh, Niharika (2019): Turing Completeness and the Ethereum Blockchain. Online verfügbar unter https://hackernoon.com/turing-completeness-and-the-ethereum-blockchain-c5a93b865c1a, zuletzt geprüft am 27.04.2020.

Tardi, Carla (2019): Application-Specific Integrated Circuit (ASIC) Bitcoin Miner. Hg. v. Investopedia. Online verfügbar unter https://www.investopedia.com/terms/a/asic.asp, zuletzt aktualisiert am 02.09.2019, zuletzt geprüft am 11.02.2020.

Tasca, Paolo; Tessone, Claudio J. (2017): Taxonomy of Blockchain Technologies. Principles of Identification and Classification. Online verfügbar unter http://arxiv.org/pdf/1708.04872v2, zuletzt geprüft am 29.10.2019.

Turing, A. M. (1937): On Computable Numbers, with an Application to the Entscheidungsproblem. In: Proceedings of the London Mathematical Society s2-42 (1), S. 230–265. DOI: 10.1112/plms/s2-42.1.230.
V. Vavilov et al. (2015): Proof of Stake versus Proof of Work. White Paper. BitFury Group. Amsterdam.

Walker, Greg (2015): Difficulty. A mechanism for regulating the time it takes to mine a block. Online verfügbar unter https://learnmeabitcoin.com/beginners/difficulty, zuletzt geprüft am 11.02.2020.

Wang, Kyle (2017): Ethereum: Turing-Completeness and Rich Statefulness Explained. Online verfügbar unter https://hackernoon.com/ethereum-turing-completeness-and-rich-statefulness-explained-e650db7fc1fb, zuletzt geprüft am 11.02.2020.

Wang, Naiyu; Zhou, Xiao; Lu, Xin; Guan, Zhitao; Wu, Longfei; Du, Xiaojiang; Guizani, Mohsen (2019): When Energy Trading meets Blockchain in Electrical Power System: The State of the Art. In: arXiv:1902.07233 [cs], zuletzt geprüft am 23.10.2019.

Wensley, J. H.; Lamport, L.; Goldberg, J.; Green, M. W.; Levitt, K. N.; Melliar-Smith, P. M. et al. (1978): SIFT: Design and analysis of a fault-tolerant computer for aircraft control. In: Proc. IEEE 66 (10), S. 1240–1255. DOI: 10.1109/PROC.1978.11114.

Werbach, Kevin (2019): Summary: Blockchain, The Rise of Trustless Trust? Online verfügbar unter https://repository.upenn.edu/pennwhartonppi_bschool/3/, zuletzt geprüft am 26.03.2020.

Xu, Xiwei; Weber, Ingo; Staples, Mark; Zhu, Liming; Bosch, Jan; Bass, Len et al. (Hg.) (2017): A Taxonomy of Blockchain-Based Systems for Architecture Design.

Zeiselmair, Andreas; Bogensperger, Alexander; Zarth, Jonte; Hinterstocker, Michael, Haberkorn, Florian (2018): Woher kommt mein Ökostrom wirklich? Mit Blockchain gegen Greenwashing. In: et - Energiewirtschaftliche Tagesfragen (Ausgabe 12/2018). Online verfügbar unter *https://www.ffe.de/publikationen/veroeffentlichungen/850-woher-kommt-mein-oekostrom-wirklich-mit-blockchain-gegen-greenwashing*, zuletzt geprüft am 30.01.2020.

Ansprechpartner in der WindNODE-Verbundkoordination
Niko Rogler
niko.rogler@windnode.de

WindNODE-Geschäftsstelle
c/o 50Hertz Transmission GmbH
Heidestr. 2
10557 Berlin
info@windnode.de
www.windnode.de

Eine Marktübersicht der Blockchain in der Energiewirtschaft