

HINTERGRUNDPAPIER

Chancen und Risiken der Blockchain für die Energiewende

Hendrik Zimmermann und Janna Hoppe

Zusammenfassung

Die Blockchain, eine Art gemeinsam geschriebenes, digitales Buch, ist eine Transaktionstechnologie, die in den nächsten Jahren zahlreiche Branchen grundlegend verändern könnte. Nicht selten wird ihr das Potenzial zugesprochen, die Welt in gleichem Ausmaß zu verändern, wie es ab 1990 das Internet getan hat. Blockchain-Anwendungen setzen auf dezentrale Peer-to-Peer-Netzwerke, Kryptografie und Spieltheorie und versprechen neben Transparenz und Manipulationssicherheit ein signifikantes Kostensenkungspotenzial, indem Intermediäre durch Software-Lösungen ersetzt werden. Dies könnte etablierte Dienstleister wie Banken, Notariate oder Börsen in vieler Hinsicht obsolet machen und die Art und Weise ändern, in denen zwei und mehr Personen weltweit interagieren.

Auch der Energiesektor ist von diesen Veränderungen betroffen und erste Start-ups zeigen, dass Stromhandel zwischen Privatpersonen ohne ein beteiligtes Energieunternehmen denk- und machbar ist. Ferner kann die Blockchain eingesetzt werden, um Speichertechnologien in dezentrale Energiesysteme einzubinden, die Balancierung von Angebot und Nachfrage zu vereinfachen, Ladungen und Abrechnungen im Bereich der Elektromobilität automatisiert durchzuführen oder die Echtheit von Grünstromzertifikaten zu gewährleisten.

Neben Funktionsweise, möglichen Anwendungsbereichen und entsprechenden Chancen, zeigt dieses Hintergrundpapier auch auf, welche Risiken adressiert werden müssen und wo noch Handlungsbedarf in der Entwicklung der Technologie liegt. So kann ein Blockchain-Netzwerk zum Beispiel nur mithilfe einer immensen Rechenleistung aufrechterhalten werden, die in einem hohen Energieverbrauch und damit einhergehendem ökologischen Rucksack resultiert. Auch ist die Blockchain-Technologie ungeeignet, um große Mengen an Daten zu speichern und zudem für viele Einsatzmöglichkeiten noch zu langsam. Ebenso ist der Rechtsrahmen unklar und die Frage nach Datenschutz und Transparenz muss auch in diesem Kontext neu gestellt und berücksichtigt werden.

Die Energiewende könnte durch Blockchain-Technologien eine neue Dynamik entfalten. Die Blockchain hat das Potential, Machtstrukturen und Rollen in der Energielandschaft zu verändern. Auch dies birgt Chancen und Risiken. Wer sich mit Substanz in die politische, ökonomische und technologische Gestaltung dieses Zukunftsthemas einbringen möchte, sollte sich mit dem Thema Blockchain jetzt beschäftigen.

Impressum

AutorInnen:

Hendrik Zimmermann und Janna Hoppe

Redaktion:

Hanna Fuhrmann

Herausgeber:

Germanwatch e.V.

Büro Bonn:

Dr. Werner-Schuster-Haus

Kaiserstr. 201

D-53113 Bonn

Telefon +49 (0)228 / 60 492-0, Fax -19

Büro Berlin:

Stresemannstr. 72

D-10963 Berlin

Telefon +49 (0)30 / 28 88 356-0, Fax -1

Internet: www.germanwatch.org

E-Mail: info@germanwatch.org

März 2018

Bestellnr: 18-3-01

ISBN 978-3-943704-62-4

Diese Publikation kann im Internet abgerufen werden unter:

www.germanwatch.org/de/15043



**Bundesministerium
für Bildung
und Forschung**

Mit finanzieller Unterstützung des Bundesministeriums für
Bildung und Forschung
Für den Inhalt ist alleine Germanwatch verantwortlich.

Inhalt

| | |
|--|-----------|
| Abbildungsverzeichnis | 5 |
| Glossar | 6 |
| 1 Digitalisierung in der Energiewirtschaft | 11 |
| 1.1 Smart Meter und Smart Home | 11 |
| 1.2 Smart Grids und dezentrale Energiesysteme | 12 |
| 1.3 Gefahren der Digitalisierung und die Relevanz der Blockchain | 13 |
| 2 Was ist die Blockchain? | 15 |
| 2.1 Überblick | 15 |
| 2.2 Abwicklung von Transaktionen | 16 |
| 2.2.1 Proof-of-work-Konsensmethode | 16 |
| 2.2.2 Proof-of-stake-Konsensmethode | 22 |
| 2.3 Beispiele für Blockchains | 23 |
| 2.3.1 Bitcoin | 23 |
| 2.3.2 Ethereum | 26 |
| 2.4 Private vs. öffentliche Blockchains | 29 |
| 2.5 Forschung und Anwendung | 30 |
| 3 Relevanz für die Energiewende | 32 |
| 3.1 Die deutsche Energielandschaft | 32 |
| 3.2 Anwendungsmöglichkeiten der Blockchain in der Energiewirtschaft | 33 |
| 3.2.1 Pilotprojekt: Brooklyn Microgrid | 34 |
| 3.2.2 Weitere Projekte im Energiesektor | 36 |
| 4 Chancen und Potenziale | 39 |
| 4.1 Systemintegrität und Ersetzen von Intermediären | 39 |
| 4.2 Transparenz | 39 |
| 4.3 Effizienzsteigerungen und Kostensenkungspotenziale | 40 |
| 5 Risiken und Schwachstellen | 43 |
| 5.1 Energieintensität | 43 |
| 5.2 Unveränderlichkeit /Trägheit und kritische Größe für Sicherheit | 45 |
| 5.3 Skalierbarkeit und Sicherheit | 46 |
| 6 Zusammenfassung der Chancen und Potenziale, Risiken und Schwachpunkte | 48 |
| 7 Fazit und Ausblick | 50 |

| | |
|-------------------------|-----------|
| Referenzen | 52 |
| Quellen..... | 52 |
| Interviews | 58 |

Abbildungsverzeichnis

| | |
|--|----|
| Abbildung 1: Berechnen von Hash-Werten kurzer Texte mithilfe einer vereinfachten Version der Hash-Funktion SHA256 | 18 |
| Abbildung 2: Aufbau eines Merkle-Baums und Erstellung eines Blocks..... | 19 |
| Abbildung 3: Netzwerkstrukturen..... | 23 |
| Abbildung 4: Bitcoin-Euro-Wechselkurs von März 2017 bis Februar 2018 | 25 |
| Abbildung 5: Ether-Euro-Wechselkurs von März 2017 bis Februar 2018 | 29 |
| Abbildung 6: Bereiche der Energiewirtschaft, in denen Blockchain-Technologien prinzipiell eine Rolle spielen können..... | 34 |
| Abbildung 7: Verschiebung der Marktstruktur durch Einführung des dezentralen Transaktionsmodells | 38 |
| Abbildung 8: Anstieg des Stromverbrauchs von Bitcoin von Anfang Februar bis Anfang März 2018 | 43 |
| Abbildung 9: Gesamter Stromverbrauch des Bitcoin-, Ethereum- und VISA- Netzwerks pro Jahr in Relation zum Stromverbrauch eines durchschnittlichen US-Haushalts (der Betrieb von Banken wird bei der Untersuchung des VISA Netzwerks nicht berücksichtigt) | 44 |
| Abbildung 10: Chancen und Potentiale, Risiken und Schwachpunkte der Blockchain..... | 49 |

Glossar

Altcoins: Altcoins stehen für "Alternative Coins" und beschreiben Zahlungsmittel, die durch Kopie und ggf. Veränderung des frei verfügbaren Bitcoin-Codes entstanden sind.

Bestandsdaten: Bestandsdaten beschreiben den derzeitigen Stand von Besitzverhältnissen. Sie ähneln Kontoauszügen, die lediglich wiedergeben, wie hoch der aktuelle Kontostand ist.

Block Rewards: Block Rewards bilden den Anreiz für Miner, eine mathematische Aufgabe zu lösen, um einen neuen Block in der Blockchain zu kreieren. Der Block Reward wird an den Miner vergeben, der die Aufgabe am schnellsten gelöst hat. Der Block Reward variiert bei verschiedenen Blockchains, beinhaltet aber meistens mindestens die Transaktionskosten des Blocks. Zusätzlich darf der erfolgreiche Miner z. B. bei der Bitcoin-Blockchain durch die Coinbase-Transaktion Coins schaffen und auf sein Konto überweisen.

Blockchain: Die Blockchain kann als gemeinsam geschriebenes, digitales Buch beziehungsweise Konto begriffen werden, das Transaktionen dokumentiert und verifiziert (Wiedmaier 2017: 14). Es beruht auf einer dezentralen Speicherung von Informationen. Dabei liegen die Transaktionsdaten nicht auf einem bestimmten Server, sondern sind auf tausenden oder Millionen von Rechnern eines Netzwerkes verteilt.

Coinbase-Transaktion: Die Coinbase-Transaktion ist die Transaktion, die die „Auszahlung“ des Block Rewards zusammen mit den Transaktionsgebühren des Blocks ausmacht. Der erfolgreiche Miner überweist eine festgelegte Anzahl an Coins aus dem Nichts an sein Konto, wodurch die insgesamt verfügbaren Coins erhöht werden. Diese festgelegte Anzahl halbiert sich beim Bitcoin alle vier Jahre, sodass die mögliche Anzahl an Bitcoins im System begrenzt ist.

DAO: DAO steht für „decentralized autonomous organization“. DAOs sind Organisationen, deren Gesellschaftsverträge oder Satzungen durch einen Smart Contract abgebildet werden.

DApps: DApps sind dezentrale Anwendungen, bei denen alle Aktionen vom Unterbau der App bis hin zur Benutzeroberfläche über eine Blockchain ablaufen.

Demand-Side-Management: Demand-Side-Management ist das Management der Anpassung der Nachfrage an das Angebot elektrischer Energie. Während heute häufig Kraftwerksleistungen an die Nachfrage angepasst werden, so soll im Rahmen des Ausbaus Erneuerbarer Energien verstärkt die Nachfrage an das Angebot angepasst werden, damit Schwankungen des Angebots besser ausgeglichen werden können.

Forger: Forger sind Miner, die in einem Blockchain-System arbeiten, das eine proof-of-stake-Konsensmethode verwendet.

Hash-Funktionen: Hash-Funktionen sind Computerprogramme, die beliebige Informationen einer beliebigen Länge in eine Nummer einer bestimmten Länge, einen sogenannten Hash-Wert, transformieren (Kaulartz 2016: 2).

Hashing: Als Hashing wird der Prozess bezeichnet, im Zuge dessen durch eine Hash-Funktion beliebige Informationen einer beliebigen Länge in eine Nummer einer bestimmten Länge, einen sogenannten Hash-Wert, transformiert werden (Kaulartz 2016: 2).

Hash-Referenz: Eine Hash-Referenz entsteht durch die Kombination von einem Hash-Wert eines Datensatzes mit dem Speicherort dieses Datensatzes. Wenn eine Information innerhalb einer Transaktion verändert wird, dann verweist die Referenz in Form eines Hash-Werts nicht

mehr auf den richtigen Speicherort. Eine nicht mehr funktionierende Hash-Referenz ist ein eindeutiges Indiz dafür, dass Daten nachträglich verändert wurden.

Hash-Wert: Ein Hash-Wert ist das Ergebnis eines Hashings. Es handelt sich um eine Nummer, die bei der häufigsten Hash-Funktion aus den Zahlen 0 bis 9 sowie den Buchstaben A bis F besteht (16 verschiedene Zeichen), 64 Zeichen lang ist, keine Rückschlüsse auf die ursprüngliche Nachricht zulässt und die sich auch bei kleinen Änderungen im Originaltext komplett und unvorhersehbar verändert.

Initial Coin Offering (ICO): Ein Initial Coin Offering (ICO) ist ein dezentrales Crowdfunding, bei dem DAOs Tokens an Interessierte verkaufen, um finanzielle Mittel z. B. für den Betrieb eines Unternehmens zu erlangen. Die erworbenen Tokens entscheiden über die Stimmrechte im DAO nach dem Prinzip "one (wo)man /one token".

Intermediäre: Intermediäre sind Mittelsfrauen/-männer oder auch VermittlerInnen (Menschen oder Organisationen), die die Interaktion zwischen zwei oder mehreren Personen organisieren, steuern oder erst möglich machen. Zu den bekannten Beispielen gehören Banken, Börsen, Plattform-Unternehmen oder (Zwischen-)HändlerInnen. Intermediäre stellen oft Produkte oder Informationen zusammen und erheben für ihre Dienstleistungen i. d. R. Gebühren.

Kryptowährung: Eine Kryptowährung ist ein virtuelles Zahlungsmittel, das durch ein rechenleistungsbasierendes Validierungsverfahren durch private AkteureInnen geschaffen wird (Wilson 2017). Dafür werden Prinzipien der Kryptografie angewandt, also der Verschlüsselung und Sicherung von Informationen.

KWK-Anlage: Bei der Kraft-Wärme-Kopplung (KWK) wird eingesetzte Energie in mechanische oder elektrische Energie umgewandelt und gleichzeitig die entstehende Wärme mithilfe eines thermodynamischen Prozesses genutzt (Umweltbundesamt 2017b). Diese Wärme kann zur Beheizung oder für Produktionsprozesse genutzt werden. Diese simultane Strom- und Wärmegewinnung findet in der Regel in einem Heizkraftwerk statt und trägt dazu bei, Schadstoffemissionen zu verringern.

Ledger: „Ein Distributed Ledger (wörtlich „verteilt Kontobuch“) ist ein öffentliches, dezentral geführtes Kontobuch. Er ist die technologische Grundlage virtueller Währungen und dient dazu, im digitalen Zahlungs- und Geschäftsverkehr Transaktionen von Nutzer zu Nutzer aufzuzeichnen, ohne dass es einer zentralen Stelle bedarf, die jede einzelne Transaktion legitimiert. Blockchain ist der Distributed Ledger, welcher z. B. der virtuellen Währung Bitcoins zugrunde liegt.“ (BaFin 2016)

Market-clearing-price: Der market-clearing-price ist der Markträumungspreis, der den Grenzkosten des teuersten Kraftwerkes entspricht, für dessen Stromerzeugung es noch eine Nachfrage gibt. Alle Kraftwerke bekommen dann diesen Preis ausgezahlt, auch wenn sie selbst zu geringeren Grenzkosten Strom produzieren konnten (Next Kraftwerke 2017).

Microgrids: Microgrids sind regionale Netzwerke aus EnergieversorgerInnen, VerbraucherInnen und ProsumerInnen. Microgrids sind i. d. R. an ein übergeordnetes Netz angeschlossen. Bei einem Ausfall des übergeordneten Netzes fungiert das Microgrid für einen begrenzten Zeitraum als Inselnetz und kann so die VerbraucherInnen weiterhin mit lokal erzeugtem Strom versorgen.

Miner: Ein Miner verifiziert die Transaktionen, fasst diese zu einem Blockkandidaten zusammen, führt das Hashing-Verfahren durch und überprüft, ob der Hash-Wert die Anforderungen erfüllt. Der Anreiz für den Miner, diese Schritte auszuführen, ist, dass der erfolgreiche Miner den Block Reward bekommt. Das Blockchain-System profitiert, da ein für alle Nodes gültiger

Block erstellt wird, welcher der Blockchain angehängt und von allen Nodes übernommen wird, wodurch widersprüchliche, zeitgleich versendete Transaktionen vermieden werden.

Mining: Zum Hinzufügen von Informationen bzw. eines neuen Blocks zu einer Blockchain muss eine Aufgabe gelöst werden. Dieses Lösen der Aufgabe nennt man Mining. Die Aufgabe kann nur durch das Trial-and-Error-Prinzip gelöst werden, bei dem verschiedene Lösungswege ausprobiert werden und kein Node dem anderen informationstechnisch überlegen ist.

Nodes: Nodes sind Rechner von NetzwerkteilnehmerInnen, die miteinander verbunden sind und prinzipiell zu jedem Zeitpunkt über dieselben Informationen verfügen. Nicht jeder Node ist mit jedem anderen verbunden, sondern hält mindestens acht und im Durchschnitt 32 Kontakte zu anderen Nodes, die über die Welt verteilt sind und zu denen außerhalb des Netzwerks in aller Regel kein persönlicher Kontakt besteht (Berentsen und Schär 2017: 88ff.).

Nonce: Eine Nonce ist eine Nummer, die zusammen mit den unveränderbaren Bestandteilen der Identifikationsnummer den Hash-Wert eines Blocks ergibt. Es handelt sich meist um eine laufende Nummer, was heißt, dass erst eine kleine Nummer ausprobiert wird und diese dann gesteigert wird, bis der Hash-Wert des Blocks die Anforderungen für die Blockgeneration erfüllt (Berentsen und Schär 2017: 208ff.).

Power-to-X-Maßnahmen: Power-to-X-Maßnahmen sind Maßnahmen, im Zuge derer Strom in eine andere Energieform (Wärme, Gas, flüssige Kraftstoffe) umgewandelt wird. Das X steht hier für die jeweilige Energieform oder einen Verwendungszweck (z. B. chemische Rohstoffe). Bei Power-to-Gas-Maßnahmen wird beispielsweise mit Strom Wasser in Wasserstoff und Sauerstoff gespalten und ein Brenngas hergestellt, das später wieder in elektrischen Strom umgewandelt werden kann.

Privater Schlüssel: Ein privater Schlüssel ist ein individueller Schlüssel, der wie der öffentliche Schlüssel nur für eine Transaktion generiert wird, jedoch im Gegensatz zum öffentlichen Schlüssel im Besitz der/s VersenderIn ist und geheim gehalten wird.

Proof-of-stake-Konsensmethode: Im Zuge dieser Methode wird Vermögen bewiesen. Bei der proof-of-stake-Konsensmethode wird die Rechenleistung im Vergleich zur proof-of-work-Konsensmethode dadurch reduziert, dass sich Mitglieder des Netzwerks nicht in einem ständigen Wettlauf um korrekte Hash-Werte befinden. Es müssen keine komplizierten kryptografischen Aufgaben von zahlreichen Minern gelöst werden, sodass Miner nicht mehr zwingend die neueste Hardware benötigen. Das Mining wird dadurch erreicht, dass von vornherein der Miner mit dem größten Vermögen bestimmt wird und dieser den Block gewinnt.

Proof-of-work-Konsensmethode: Bei dieser Methode wird Arbeit bewiesen. Jeder Miner fasst Transaktionen zu einem Blockkandidaten zusammen, führt das Hashing-Verfahren durch und überprüft, ob der Hash-Wert die Anforderungen erfüllt. Es gibt also mehrere konkurrierende Blocks mit unterschiedlichen Transaktionen. Wenn der Block die Anforderungen erfüllt, hat der erfolgreiche Miner Arbeit bewiesen, und der Block dieses Miners wird von allen anderen Nodes übernommen (Konsens entsteht). Sind die Anforderungen nicht erfüllt, verändert der Miner die Nonce und überprüft die Anforderungen erneut. Die Aufgabe kann nur durch das Verändern der Nonce und Ausprobieren gelöst werden. Der schnellste Miner gewinnt den Block.

Prosumer: Prosumer sind Personen, die sowohl KundInnen (Consumers) sind, indem sie Strom verbrauchen oder speichern, als auch ErzeugerInnen (Producers), indem sie zum Beispiel elektrische Energie ihrer PV-Anlage ins Netz einspeisen.

Relay Chain: Relay Chains dienen der Verknüpfung von verschiedenen Blockchains mit dem Ziel, die Nutzung eines Zahlungsmittels einer Blockchain in einer DApp einer anderen Blockchain zu ermöglichen. Hierbei wird mit einzelnen Informationen aus einem Block und nicht mit gesamten Blöcken gearbeitet, wodurch das Volumen und der damit einhergehende Stromverbrauch gesenkt werden.

Schwierigkeit: Als Schwierigkeit bezeichnet man die Summe der Bedingungen, die der für einen Block generierte Hash-Wert erfüllen muss, um im Zuge der jeweiligen Konsensmethode in die Blockchain integriert und von allen Nodes übernommen zu werden. Die Schwierigkeit dient dazu, die Zeit künstlich zu verlängern, die die Erstellung eines Blocks technisch benötigt. Dadurch wird festgelegt, wie viele Transaktionen in einem Block zusammengefasst werden können.

Side Chain: Eine Side Chain bezeichnet ein Netzwerk mit einer verringerten Anzahl an Rechnern, die mit einer Haupt-Blockchain verlinkt sind und dadurch die notwendigen Sicherheitsanforderungen erfüllen.

Smart Contract: Smart Contracts sind Computerprotokolle, mithilfe derer digitale Verträge über die Blockchain geschlossen und ausgeführt werden können. Dabei einigen sich die Vertragsparteien zunächst über die Vertragseinzelheiten, wie beispielsweise die beteiligten Personen, Mengen und Preise. Aktionen werden automatisch ausgeführt, sobald eine bestimmte Bedingung erfüllt ist oder ein bestimmtes Ereignis eintritt (Wenn-dann-Funktion).

Smart Grids: Smart Grids sind Energienetze, in denen Energieflüsse und Netzzustandsdaten automatisch erfasst werden und Energieangebot, -speicherung und -nachfrage entsprechend angepasst werden können. Durch die Integration von Smart Metern werden ProduzentInnen, KonsumentInnen und Prosumer in Echtzeit über Energieangebot und -nachfrage – und damit Preise – informiert und bekommen so Anreize, ihre Aktivitäten an Schwankungen von Angebot und Nachfrage anzupassen. Diese Anpassung kann auch durch den Netzbetreiber oder einen Algorithmus erfolgen, z. B. zum Zwecke der Vermeidung von aus Netzsicht teuren Lastspitzen.

Smart Home: Der Begriff Smart Home bezeichnet die Vernetzung von elektronischen Haushaltsgeräten, kleinen Stromerzeugungsanlagen und ggf. Elektrofahrzeugen sowie deren effiziente und tageszeit- oder wetterabhängige Nutzung mithilfe von Smart Metern. Über eine zentrale Steuereinrichtung können die Geräte an- und ausgeschaltet werden. Die variable Nutzung der Geräte kann durch variable Stromtarife honoriert werden.

Smart Meter: Ein Smart Meter ist ein intelligenter Stromzähler, der das Ziel hat, eine sichere und standardisierte Kommunikation zwischen Netzakteuren zu verwirklichen. Er kann Privathaushalten mehr Transparenz in Bezug auf ihren Stromverbrauch und ihre Einsparpotentiale bieten. Zudem legen Smart Meter, bei Integration in Smart Homes, die Grundlage für flexible Stromtarife, die sich am Börsenstrompreis orientieren und so die VerbraucherInnen incentivieren, Geräte mit hohem Stromverbrauch in Zeiten von Stromüberschüssen zu verwenden.

Tokens: Token ist Englisch für „Jeton“ oder „Wertmarke“. Der Begriff Token wird häufig im Sinne eines Anteils an einem Produkt oder einer Dienstleistung benutzt. Er ist damit nicht exakt gleichzusetzen mit einem Coin, der in seiner Funktion eher einer Münze entspricht.

Transaktionsdaten: Transaktionsdaten beschreiben den Transfer von Besitz. Sie ähneln jenen Kontoauszügen, die alle Abhebungen, Einzahlungen und Überweisungen auflisten und die gesamte Transaktionshistorie offenlegen. Während Bestandsdaten Besitzansprüche behaupten, beschreiben und rechtfertigen Transaktionsdaten diese Besitzansprüche.

Öffentlicher Schlüssel: Ein öffentlicher Schlüssel ist ein Schlüssel, der für eine einzelne Transaktion angepasst ist, den empfangenden Nodes bekannt ist und dafür verwendet wird, eine mit einem persönlichen Schlüssel verschlüsselte Nachricht zu entschlüsseln und so zu verifizieren, dass die Absendenden die Nachricht auch wirklich in der entsprechenden Form in Auftrag gegeben haben.

1 Digitalisierung in der Energiewirtschaft

Mit dem neuen Gesetz zur Digitalisierung der Energiewende vom 1. September 2016 hoffte die Bundesregierung ein „Startsignal für Smart Grid, Smart Meter und Smart Home“ zu setzen und „so die digitale Infrastruktur für eine erfolgreiche Verbindung von über 1,5 Millionen Stromerzeugern und großen Verbrauchern“ zu schaffen (BMWi 2017a). Durch dieses Gesetz sollen zwei zentrale Zukunftsthemen miteinander verknüpft und der Weg zu einer emissionsarmen und vernetzten Gesellschaft geebnet werden. Im 31-Seiten langen Dokument findet sich jedoch nicht einmal die Erwähnung des Wortes „Blockchain“ – und das, obwohl die Blockchain schon seit 2015 als „das neue Internet“ (Tapscott 2016) gehypt wird und von einer „basisdemokratischen Revolution ganzer Branchen“ (Stiftung Neue Verantwortung 2017) die Rede ist. Ist das neue Gesetz in Anbetracht der Außerachtlassung der Blockchain-Technologie, welche allein bis September 2016 über 1,2 Milliarden US-Dollar an Risikokapital-Investitionen vorweisen konnte¹, „out of date even before it took effect“ (Reetz o.J., zitiert nach Amelang 2017)?

Digitalisierung, also die Transformation von analogen Informationen in eine digitale Form, ist gerade auch für den Energiesektor interessant, weil es dort eine Vielzahl von Daten (Performance-Daten von Kraftwerken, Verbrauchsdaten, Temperaturdaten, Wetterdaten, etc.) gibt, deren kluges Management eine potenziell enorme Effizienzsteigerung und Kostensenkung mit sich bringt (Peters und Mohr 2015: 9). Vor allem aber kann die Digitalisierung „Enabler“ für eine Flexibilisierung sein und letztere wiederum dabei helfen, volatile erneuerbare Energiequellen besser zu integrieren (Mielke/Zimmermann 2016). Durch Flexibilisierungsmaßnahmen wie „**demand-side-management**“, Stromspeicher, **Power-to-X-Maßnahmen** oder grenzüberschreitenden Handel (Next Kraftwerke 2016) können mehr Erneuerbare integriert werden, was den Weg zum Ziel ebnet, bis zum Jahr 2030 65 % des in Deutschland verbrauchten Stroms aus erneuerbaren Energiequellen zu beziehen (Koalitionsvertrag 2018).

1.1 Smart Meter und Smart Home

Der Einbau von **Smart Metern** (intelligenten Stromzählern) ist für VerbraucherInnen mit einem Jahresstromverbrauch von über 10.000 kWh und ErzeugerInnen wie PV-AnlagenbesitzerInnen mit einer installierten Leistung zwischen 7 und 100 kW bereits ab 2017 verpflichtend, Haushalte mit kleineren Anlagen werden ab 2020 ausgestattet; die freiwillige Installation ist grundsätzlich immer möglich (Messstellenbetriebsgesetz 2016). Mit der Installation dieser Smart Meter soll eine sichere und standardisierte Kommunikation zwischen verschiedenen NetzakteurInnen ermöglicht werden. VerbraucherInnen können auf den in ihren Haushalten installierten Geräten ablesen, wie hoch ihre aktuellen und vergangenen Energieverbrauchswerte sind und waren. So können Einsparpotentiale aufgezeigt sowie besonders energieintensive Geräte identifiziert werden. Ferner können StromkundInnen ihre Abrechnungen leichter überprüfen und mit ihren Energielieferanten variable Stromlieferarife abschließen, die besser zu ihrem individuellen Verbrauch passen und das wetterabhängige Dargebot volatiler Erneuerbarer Energien besser berücksichtigen. Der Abschluss solcher Tarife ist laut VerbraucherschützerInnen bisher ausgeblieben, da variable Tarife

¹ Vgl. Statista (2017a): <https://de.statista.com/statistik/daten/studie/654326/umfrage/venture-capital-investitionen-in-blockchain-technologien-weltweit> (abgerufen am 24.10.2017)

wirtschaftlich und technisch noch zu kompliziert und nicht rentabel sind (Mielke, Zimmermann et al. 2016b: 22f.). Mittelfristig soll auch eine Spartenbündelung von Strom, Gas, Heiz- und Fernwärme durch die Smart Meter möglich sein (Bundesnetzagentur 2017).

Smart Home meint die Vernetzung von elektronischen Haushaltsgeräten und deren effiziente und tageszeit- oder wetterabhängige Nutzung. So werden zum Beispiel bei Sonnenschein und einem hohen Angebot an elektrischer Energie die Waschmaschine automatisch an- oder die Geräte beim Verlassen des Hauses automatisch abgeschaltet. Dafür müssen die Haushaltsgeräte durch ein zentrales Gerät, wie zum Beispiel das Smartphone, steuerbar sein, während eine installierte App Auskunft über Energieverbrauchsdaten, Temperatur oder Helligkeit in einzelnen Räumen gibt (Ropenus 2017b: 108). In Smart Home-Systeme lassen sich auch Ladestationen für Elektroautos integrieren. Die Integration von Smart Metern ist die Grundlage für die zeitnahe Einführung finanzieller Anreize für NutzerInnen von Elektrofahrzeugen, diese dann zu laden, wenn das Dargebot an flexiblen Erneuerbaren Energien am größten und die Nachfrage nach Strom am geringsten ist. Dies hat das Potential, Emissionen, Kosten und Netzkapazitäten einzusparen.

1.2 Smart Grids und dezentrale Energiesysteme

Haushalte der Zukunft sollen ebenso wie große und kleinere StromerzeugerInnen, die Elektromobilität oder auch die Industrie Teil von **Smart Grids**, also intelligenten Stromnetzen, werden. Bei einer zunehmend dezentralen Stromerzeugung müssen immer mehr **Prosumer** in das Gesamtsystem integriert werden. Dies sind Personen, die sowohl KundInnen (Consumers) sind, indem sie etwa zur rechten Zeit für ihr Haus oder Fahrzeug Strom „tanken“, als auch ErzeugerInnen (Producers), indem sie zum Beispiel elektrische Energie ihrer PV-Anlage ins Netz einspeisen. Angebot und Nachfrage können mithilfe von Informations- und Kommunikationstechnologien (IKT) besser aufeinander abgestimmt werden. Der Fluktuation der Erneuerbaren Energien kann mithilfe der oben genannten Flexibilisierungsmaßnahmen ausgleichend entgegengewirkt werden (Mielke, Zimmermann et al. 2016: 15).

Durch die Energiewende erhöht sich die Anzahl an Stromerzeugungsanlagen erheblich und die Verteilung und Steuerung des Stroms muss neu organisiert werden (BDEW 2017). In der mehr und mehr dezentralen Erzeugungslandschaft können digitale Technologien dabei helfen, die Abstimmung von Elektrizitätserzeugung und -nutzung zu vereinfachen und Überlastungen von Stromnetzen zu verhindern. Eine Akkumulation und Digitalisierung von Daten kann ein demand-side-management unterstützen, indem Lastprognosen verbessert und eine Steuerung bzw. Anreizrahmensetzung der Stromnachfrage realisiert werden kann. Des Weiteren können mithilfe der Digitalisierung die Sektoren Strom, Gas, Wärme, Industrie und Mobilität miteinander verknüpft werden, sodass, auch unter Zuhilfenahme von Speichertechnologien, Energie automatisch und effizient dorthin geleitet werden kann, wo sie gerade gebraucht oder besonders kostengünstig genutzt werden kann (Mielke, Zimmermann et al. 2016a: 17). Damit ließe sich Überschussstrom volkswirtschaftlich effizient nutzen.

Manche BeobachterInnen betonen die Chancen, durch die Digitalisierung auch soziale Verbesserungen zu realisieren. Einige heben hervor, die Vereinfachung der Teilhabe am Energiemarkt könne Demokratisierungsprozesse anstoßen und die Abhängigkeit von VerbraucherInnen vom Markt reduzieren (Rifkin 2015: 7). Sie verweisen darauf, dass intelligente Technologien eine engere Kooperation zwischen allen NetzteilnehmerInnen – also ErzeugerInnen, VersorgerInnen, NetzbetreiberInnen und VerbraucherInnen – ermöglichen und diese miteinander kommunizieren lassen können (enviaM 2017). Sie sehen das Potential, dass sich so gleichzeitig technische, ökologische und soziale Verbesserungen erzielen.

1.3 Gefahren der Digitalisierung und die Relevanz der Blockchain

Im Zusammenhang mit Smart Grids warnen etwa Gewerkschaften vor einer Entsolidarisierung von Wohlhabenden, welche sich durch Eigenerzeugung in Kombination mit Speichern und digitalen Technologien in ihrer Nachbarschaft ganz oder weitgehend energieautark versorgen und die Kosten für Ausbau und Instandhaltung des Stromnetzes und die öffentliche Energieversorgung nicht mittragen (Mielke, Zimmermann et al.: 16). In einem solchen System könnte es dazu kommen, dass die Kosten auf all jene umgelegt werden, die nicht in der Lage sind, sich selbst zu versorgen. Noch problematischer wäre es, wenn die Wohlhabenden gerade dann, wenn ohnehin zu wenig erneuerbarer Strom vorhanden ist (z. B. im Kontext einer Dunkelflaute), doch auf die Kapazität der Stromnetze zurückgreifen wollen würden, ohne dafür gezahlt zu haben.

Es bestehen Bedenken, dass eine zunehmende Technikabhängigkeit auch immer stärker die Privatsphäre dominiert und ein Gefühl der Fremdsteuerung aufkommt (ebd.: 15). Gegenwärtige Tendenzen der Kontrolle der Bevölkerung etwa in China durch den Ausbau der Digitalisierung verstärken diese Befürchtungen². Darüber hinaus könnte es auch im Energiekontext zu Hackerangriffen kommen. So verfügen zum Beispiel Smart Meter über unzureichende Sicherheitsmaßnahmen zum Schutz vor böswilligen und manipulativen Angriffen (Interview 2). Auch die Frage nach der ökonomischen oder politischen Nutzung von Daten ist bislang nicht ausreichend geklärt. Wenn die neu erhobenen Daten bei wenigen Unternehmen zusammenlaufen, so besteht die Gefahr einer zunehmenden Marktmacht dieser.

Die **Blockchain** bietet in diesem Kontext neuartige Lösungen (z. B. in Bezug auf Sicherheit und Datenschutz). Sie bzw. funktionale Äquivalente, die die gleichen Vorteile mit weniger Nachteilen erreichen, sollten in Diskussionen zur Digitalisierung der Energiewende daher stets mitgedacht werden. Ihre Fähigkeit, durch programmierte Codes **Intermediäre** zu ersetzen und damit Transaktionskosten zu senken, kann sich als revolutionär erweisen. In einer Studie der Deutschen Energie-Agentur (dena) wurden 70 EntscheidungsträgerInnen aus der deutschen Energiewirtschaft zu ihrer Einschätzung bezüglich des Potenzials der Blockchain befragt. Etwa 60 % der TeilnehmerInnen gehen von einer Verbreitung von Blockchain-Anwendungen aus, während 21 % die Blockchain als "Game-Changer" für die Energiewirtschaft sehen und 14 % erwarten, dass die Technologie auf Nischenanwendungen beschränkt bleiben wird. Lediglich 5 % schätzen das Potenzial auf sehr gering bis inexistent. Von den befragten Personen gaben 50 % an, bereits mit Blockchain-Anwendungen zu experimentieren oder dies zu planen (dena 2016: 18f.).

Am 29. Juni 2017 hat sich aus der Mitte der Deutschen Blockchain-Community der Blockchain Bundesverband gegründet, welcher die Vernetzung von privaten und öffentlichen Einrichtungen mit der Blockchain in einem gesellschaftlichen Rahmen und auf rechtssicherem Boden fördern will (Blockchain Bundesverband 2017a). Zu den zentralen Forderungen des in Berlin ansässigen Vereins gehört der „Einsatz der Blockchain-Technologie im öffentlich-rechtlichen Bereich“ bis 2020 sowie die „Förderung von Ausbildung und Wissenschaft zum Thema Blockchain“ und die „Schaffung von innovationsfreundlicher Rechtssicherheit im zivilrechtlichen, steuerlichen und regulatorischen Bereich, um Deutschland als attraktiven Wirtschaftsstandort für das Blockchain Ökosystem

² Mithilfe des 2015 verabschiedeten „Gesetzes zur Nationalen Sicherheit kann die Regierung nahezu jede öffentliche Handlung – zum Beispiel in den Bereichen IT, Finanzen, Umwelt – im Namen der nationalen Sicherheit verbieten. Die Zentralregierung arbeitet an einem großanlegten System zur Überwachung und Klassifizierung ihrer Bevölkerung: Durch Daten über Freundeskreise in sozialen Medien, Surfverhalten oder Geldtransfers sollen die Bürger und ihr Verhalten berechenbarer werden – ökonomisch wie politisch.“ (Die Zeit 2017)

zu etablieren“ (ebd. 2017b: 1). Für den Energiebereich sieht der Bundesverband vielfältige Einsatzmöglichkeiten von Blockchain-Technologien, welche dazu beitragen können „Versorgungssicherheit und Netzstabilität in Zeiten der Energiewende zu gewährleisten“ (ebd. 2017c: 12).

2 Was ist die Blockchain?

2.1 Überblick

Selbst Fachleute sind sich nicht sicher, wie groß der potentielle Nutzen der Blockchain ist. Eine PwC-Studie von März 2016 kam zu dem Ergebnis, dass 57 % der EntscheiderInnen aus der Finanzbranche das Potenzial der Blockchain noch nicht einschätzen können und auch noch nicht wissen, wie sie auf diese neue Entwicklung reagieren sollen (PwC 2016: 3). Dabei ist bei der Nutzung und in der Erforschung von Anwendungsfeldern der Finanzsektor am weitesten fortgeschritten.

Die der Blockchain zugrundeliegenden Theorien und komplexen Wirkungsmechanismen sollen in diesem und folgendem Kapitel vereinfacht erläutert werden.

Die Blockchain kann als gemeinsam geschriebenes, digitales Buch beziehungsweise Konto (der sogenannte **Ledger**) begriffen werden, das Transaktionen dokumentiert und verifiziert (Wiedmaier 2017: 14). Es beruht auf einer dezentralen Speicherung von Informationen. Dabei liegen die Transaktionsdaten nicht auf einem bestimmten Server, sondern sind auf tausenden oder Millionen von Rechnern eines Netzwerkes abgelegt. Die Mitglieder dieser Netzwerke kennen und vertrauen sich nicht zwingend von vornherein, können sich aber gegenseitig kontrollieren, was den Aufbau einer vertrauensvollen Beziehung im weiteren Verlauf begünstigt, aber nicht zwingend voraussetzt, wie bei einer Überwachung durch eine zentrale Instanz (Wilson 2017). Entwickelt wurde die Technologie auch als Reaktion auf die weltweite Finanzkrise von 2008, die das Vertrauen in den Finanzsektor stark schädigte (Tapscott und Tapscott 2016: 5) und besonders das Ansehen der Banken als vertrauenswürdige Institutionen schwanken ließ.

In der Vergangenheit wurden Datenbanksysteme stets von Institutionen bereitgestellt, die dann auch die gesamte Kontrolle über das System besaßen und selber für Ressourcen wie den Server oder variable Kosten (z. B. Strom für den Betrieb oder die Kühlung der Elektronik) aufkommen sind. Die meisten sozialen Medien, Emailprogramme und Websites werden derart betrieben³ und Änderungen unterliegen allein der Entscheidung der jeweiligen BetreiberInnen (Wilson 2017).

Der zugrundeliegende Gedanke bei allen Blockchain-Anwendungen ist, dass vermittelnde Instanzen nicht mehr notwendig sind, da durch tausendfache Speicherungen Informationen nicht verloren gehen, Transaktionen dezentral abgewickelt werden und das Kollektiv die erforderliche Rechenleistung gemeinsam aufbringt. Jedes Mitglied im Netzwerk verfügt über eine vollständige Kopie der gesamten Datenbank und keines der Mitglieder braucht eine Erlaubnis, die Daten einzusehen. Alle **Nodes**, also Rechner der NetzwerkteilnehmerInnen, sind miteinander verbunden und verfügen prinzipiell zu jedem Zeitpunkt über dieselben Informationen. Es werden regelmäßig Mitteilungen in das Netz gespeist, die Informationen über den Wert einer Transaktion sowie die beteiligten Parteien enthalten und von allen gelesen werden können.

Bislang hat sich noch keine einheitliche Definition der Blockchain durchgesetzt, während eine Vielzahl von Meinungen über Attribute zirkuliert. Eine solide Arbeitsdefinition, die einen ersten und verständlichen Überblick verschafft, liefert Daniel Drescher in seinem Buch „Blockchain Basics. A Non-Technical Introduction in 25 Steps“ (2017: 35):

³ Bei Open-Source-Programmen wie beispielsweise Wikipedia ist dies anders.

“The blockchain is a purely distributed peer-to-peer system that utilizes a software unit that consists of an algorithm, which negotiates the informational content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its integrity.”

2.2 Abwicklung von Transaktionen

Für NutzerInnen sind auf der Anwendungsebene keine Unterschiede zu anderen Technologien erkennbar, da die Architektur der Software der/m EntwicklerIn obliegt und die Benutzeroberfläche beliebig gestaltet werden kann. Sie stellen jedoch unterschiedliche Anforderungen an die Sicherheit eines Systems und nutzen unterschiedliche Maßnahmen, um diese zu gewährleisten (Drescher 2017: 16). Eine der zentralen Eigenschaften ist die Dezentralität der Blockchain. Auch andere Systeme und Plattformen, wie zum Beispiel Airbnb, die Community-Plattform für die Vermietung von Privatunterkünften, sehen auf den ersten Blick dezentral aus, da sich private NutzerInnen scheinbar selbstständig mit anderen vernetzen. Hinter diesem dezentralen Netzwerk steht bei Airbnb jedoch eine zentrale Plattform, ohne die eine Interaktion der NutzerInnen gar nicht erst möglich wäre. Derzeit hat Airbnb Zugriff auf sämtliche Daten und könnte das Netzwerk von einer Sekunde auf die andere lahmlegen (Voshmgir 2016: 10). Und hier kommen Neuerungen durch die Blockchain ins Spiel.

Die Blockchain ist nicht die einzige Technologie, die grundlegende dezentrale Systeme anbietet. Es gibt einige Alternativen im breiten Feld der „distributed ledger technologies“, also der dezentralen Logbuch-Technologien, die jedoch bisher noch nicht viel Aufmerksamkeit bekommen haben. Dabei bieten diese Alternativtechnologien andere Merkmale und somit unterschiedliche Vor- und Nachteile. Im direkten Vergleich ist die Blockchain in der Entwicklung ein paar Jahre voraus. Einige ExpertInnen argumentieren, dass dies die Wahrscheinlichkeit einer Durchsetzung auf dem Markt erhöhe (Interview 2). Es gibt verschiedene Methoden, durch welche das dezentrale Blockchain-System aufrechterhalten werden kann. Eines davon ist die **proof-of-work**-Konsensmethode, die im Folgenden erklärt wird und die das am meisten verbreitete Verfahren darstellt (PwC 2016: 6). Es ist jedoch anzunehmen, dass sich „die Phase der Variation weiter fortsetzen wird“ – die Einschätzungen variieren, wie grundsätzlich diese Variationen sein werden – und wir von einem dominanten Design noch entfernt sind (dena 2016: 30f.).

2.2.1 Proof-of-work-Konsensmethode

2.2.1.1 Aufbau und Weiterleitung von Transaktionen

Nach der proof-of-work-Konsensmethode sind alle Mitglieder im Netzwerk über das Internet miteinander verbunden und können sich jederzeit vom System trennen und diesem wieder beitreten. Dabei ist nicht jeder Node mit jedem anderen verbunden, sondern hält mindestens acht und im Durchschnitt 32 Kontakte zu anderen Nodes, die über die Welt verteilt sind und zu denen außerhalb des Netzwerks kein persönlicher Kontakt besteht (Berentsen und Schär 2017: 88ff.). Jeder Rechner hat eine unabhängig von anderen geführte Liste von Rechnern, mit denen er kommuniziert. Jeder Node, der eine Nachricht erhält, leitet sie an alle verbundenen Nodes weiter. Diese empfangenden Nodes schicken die Nachricht wiederrum an alle Nodes in ihrer Kontaktliste weiter. Dieses führt dazu, dass irgendwann alle Nodes im Netzwerk die Nachricht erhalten haben, wobei Mehrfachsendungen einfach ignoriert werden. Durch einen in der Nachricht enthaltenen Zeitstempel werden eingehende Informationen chronologisch sortiert. Zu jeder Zeit kann ein neuer Rechner dem Netzwerk beitreten, indem er eine Art Kontaktanfrage an beliebige andere Nodes im

Netzwerk schickt. Diese bestätigen den Kontakt und das System ist um einen Node gewachsen (Drescher 2017: 149f.). Ein Vorteil der Blockchain gegenüber anderen Netzwerken ist, dass der beitretende Rechner alle Informationen zu vergangenen Transaktionen einsehen kann und somit ein vollständiges Update bekommt.

Eigentumsverhältnisse lassen sich auf verschiedene Arten beschreiben: unter anderem über **Transaktionsdaten** oder **Bestandsdaten**. Bestandsdaten beschreiben den derzeitigen Stand von Besitzverhältnissen. Sie ähneln Kontoauszügen, die lediglich wiedergeben, wie hoch der aktuelle Kontostand ist. Transaktionsdaten wiederum beschreiben den Transfer von Besitz. Sie ähneln jenen Kontoauszügen, die alle Abhebungen, Einzahlungen und Überweisungen auflisten und die gesamte Transaktionshistorie offenlegen. Diese beiden Formen unterscheiden sich darin, dass Bestandsdaten Besitzansprüche behaupten, während Transaktionsdaten sie beschreiben und damit rechtfertigen (Drescher 2017: 64f.). Die Blockchain arbeitet mit Transaktionsdaten, welche nicht nur auf den Kontoauszügen der an einer Transaktion Beteiligten, sondern auf dem digitalen Ledger aller Netzwerkmitglieder erscheint.

Dadurch, dass jedes Mitglied über die gesamte Transaktionshistorie verfügt, wird eine neue Art der Beweisführung angewandt. Nach dem Motto „Ein Zeuge ist gut, viele sind besser“ können keine Transaktionen im Geheimen durchgeführt oder als ungültig angefochten werden. Jede Übertragung muss im Register dokumentiert werden, denn ein veraltetes Register kann kein vertrauenswürdiger Zeuge sein (ebd.: 41). Will Person A Person B Geld überweisen, so speist sie eine Nachricht (zum Beispiel: „Person A sendet 100 Einheiten von X an Person B“) in das Netzwerk ein. Dies geschieht jedoch über technische Umwege, welche die Anonymität der beteiligten Personen und die Integrität des Systems schützen sollen. Ziel ist es, Transaktionsinformationen unverwechselbar und schnell durch ihren „digitalen Fingerabdruck“ (Drescher 2017: 71) zu identifizieren.

2.2.1.2 Hash-Funktionen und Hash-Werte

Hierbei kommen **Hash-Funktionen** zum Einsatz. Hash-Funktionen sind Computerprogramme, die beliebige Informationen einer beliebigen Länge in eine Nummer einer bestimmten Länge, einen sogenannten **Hash-Wert**, transformieren (Kaulartz 2016: 2). Diese Nummer ist bei der am häufigsten verwendeten Hash-Funktion stets 64 Zeichen lang und besteht aus den Zahlen 0–9 sowie den Buchstaben A bis F, um 16 verschiedene Zeichen zu erlangen. Bei identischem Input sind auch die resultierenden Hash-Werte identisch. Wird eine Kleinigkeit im Originaltext verändert, so ändert sich der resultierende Hash-Wert komplett und unvorhersehbar. Es ist nicht möglich, aufgrund der 64-stelligen Zahlen-Buchstaben-Kombination Rückschlüsse auf den Inhalt der Originalnachricht zu ziehen (Drescher 2017: 73). Es gibt verschiedene Hash-Funktionen, die unterschiedlich lange Ziffernkombinationen produzieren. Sie sind untereinander nicht vergleichbar, weshalb innerhalb eines Blockchain-Systems stets die gleiche Hash-Funktion verwendet wird.

Die Anwendung von Hash-Funktionen hilft dabei, Datensätze miteinander zu vergleichen. So müssen nicht zwei ähnlich aussehende Texte Wort für Wort, Seite für Seite miteinander verglichen werden. Stattdessen reicht ein Vergleich der beiden Hash-Werte, um sofort zu erkennen, ob die beiden zugrundeliegenden Datensätze identisch sind. Die mögliche Anzahl von Hash-Werten beträgt 2256, was bedeutet, dass es so gut wie unmöglich ist, dass zwei verschiedene Texte den gleichen Hash-Wert ergeben (Kaulartz 2016: 2). Dieses **Hashing** macht Transaktionen besonders sicher: Wird zum Beispiel nur eine Kleinigkeit der Transaktionsdetails verändert (wird beispielsweise bei der Menge eine weitere Null hinzugefügt), so wird dies sofort identifiziert, was betrügerisches Verhalten massiv erschwert.

Unter www.blockchain-basics.com/Hashing.html kann man mithilfe einer verkürzten Version der Hash-Funktion SHA256 verschiedene Texte in ein Textfeld eingeben (Input) und den korrespondie-

renden Hash-Wert (Output) ermitteln. Es wird sofort erkenntlich, dass der Output keine Rückschlüsse auf den Originaltext zulässt und dass eine kleine Veränderung in der Originalnachricht in einem vollständig veränderten Output resultiert.

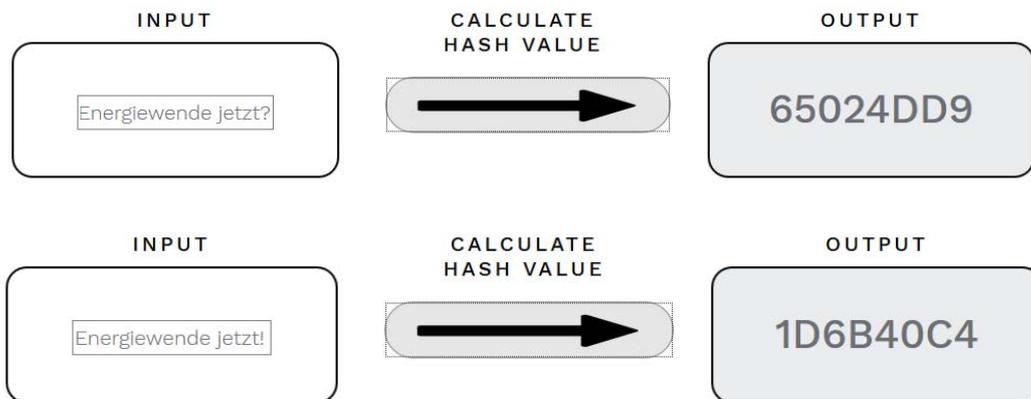


Abbildung 1: Berechnen von Hash-Werten kurzer Texte mithilfe einer vereinfachten Version der Hash-Funktion SHA256⁴

Hashing wird jedoch nicht nur zum Vergleich von Informationen genutzt, sondern auch, um diese auffindbar und manipulationssicher zu speichern. Dabei wird der Hash-Wert eines Datensatzes mit dem Ort der Speicherung kombiniert und so eine **Hash-Referenz** generiert. Drescher (2017: 83f.) vergleicht dies mit Garderobenmarken. Wer seine Jacke an der Garderobe abgibt, erhält ein Kärtchen, welches Auskunft über den Aufbewahrungsort der Jacke gibt. Dabei ist es nicht nötig, dass sämtliche Informationen über die Jacke oder den Aufbewahrungsort auf dem Kärtchen stehen – es genügt ein einfaches System, welches auf einen ganz bestimmten und einzigartigen Haken verweist. Auch hier wird sichergestellt, dass Daten nicht nachträglich verändert werden. Wenn eine Information innerhalb einer Transaktion verändert wird, dann verweist die Referenz in Form eines Hash-Werts nicht mehr auf den richtigen Speicherort. Eine nicht mehr funktionierende Hash-Referenz ist ein eindeutiges Indiz dafür, dass Daten nachträglich verändert wurden.

2.2.1.3 Von einzelnen Transaktionen zur Kette

Schließlich wird aus allen Transaktionsdaten eine Kette gebildet, die sogenannte Blockchain. Dabei sind die Blöcke ähnlich wie Seiten eines Buches miteinander verknüpft. Wer ein Buch liest, der merkt sofort, wenn eine Seite fehlt, da die seitenübergreifenden Sätze keinen Sinn mehr ergeben und zudem zwei Seitenzahlen fehlen. So ähnlich funktioniert auch die Blockchain (Drescher 2017: 34). Eine bestimmte Anzahl von Transaktionen wird zu einem Block zusammengefasst. Dieser Block mit neuen Transaktionen wird an eine Kette mit vergangenen Blöcken, bestehend aus einzelnen Transaktionen, gehängt. Dabei verweist jeder Block auf den jeweiligen Vorgänger, in dem er den Hash-Wert des Vorgänger-Blocks beinhaltet. Der erste Block einer Kette hat keine Referenz, und ist damit der einzige, der nicht auf alle vorher durchgeführten Transaktionen verweist. Der zweite Block verweist auf den ersten, der dritte auf den zweiten, usw.

Es gibt weitere Sicherheitsmechanismen, die bei der Erstellung von Blöcken zur Anwendung kommen. Wird eine Transaktion durchgeführt, so wird für diese sofort ein Hash-Wert erstellt. Als

⁴ Quelle: Eigene Darstellung

nächstes werden jeweils zwei Transaktionen zusammengefasst. Diese zwei Transaktionen werden miteinander verknüpft und es wird ein weiterer Hash-Wert erstellt. Dieser Prozess der Kombination von jeweils zwei Hash-Werten wird mit mehreren Transaktionen so lange durchgeführt, bis es nur noch einen Hash-Wert gibt. Dieser Wert ist dann die Wurzel eines sogenannten Merkle-Baums (Drescher 2017: 88).

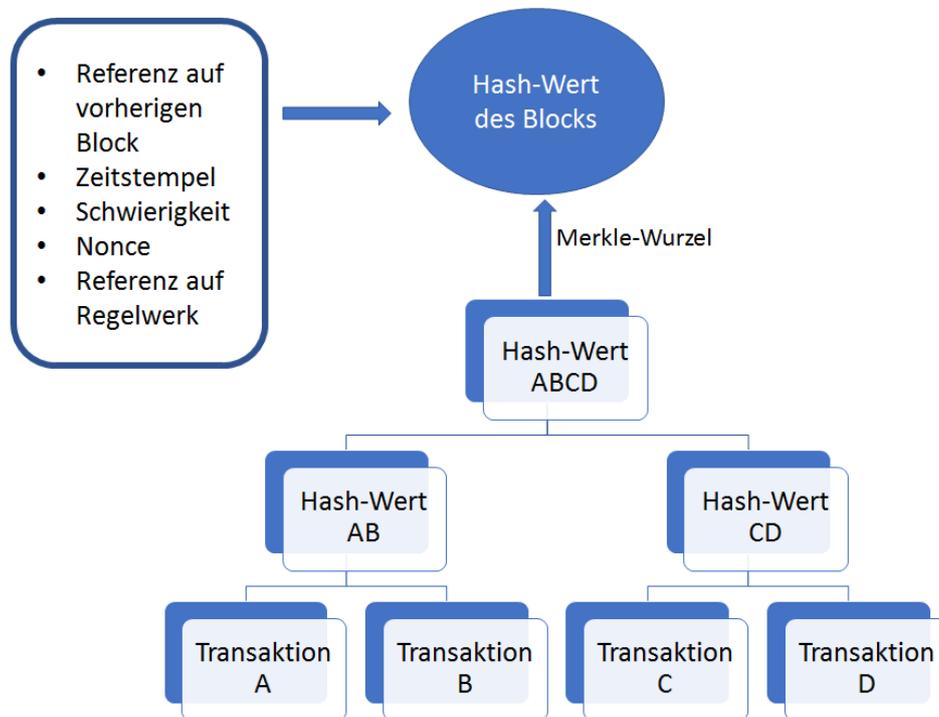


Abbildung 2: Aufbau eines Merkle-Baums und Erstellung eines Blocks⁵

Ein neuer Block wird kreiert, indem die Wurzel eines Merkle-Baums mit der Hash-Referenz zum vorherigen Block und einem Zeitstempel kombiniert wird (Berentsen und Schär 2017: 202). Diese Informationen können jedoch nur von einem **Miner** der Blockchain-Struktur hinzugefügt werden. Zunächst erstellt jeder Miner Blockkandidaten, also Blöcke, die sie/er gern zu der Blockchain hinzufügen würde. Dann nimmt sie/er an einem Wettbewerb um die Lösung einer Aufgabe teil. Diese Aufgabe kann nicht aufgrund von Daten, Wissen oder IQ gelöst werden. Stattdessen basieren sie auf einem Trial-and-Error-Prinzip (Chuen und Deng 2018: 150), bei dem verschiedene Lösungswege ausprobiert werden und kein Node dem anderen informationstechnisch überlegen ist. Dies lässt sich mit dem Beispiel eines Zahlenschlosses vergleichen: Wer den einzigartigen Code nicht kennt, dem hilft auch kein Nachdenken, um die richtige Zahlenkombination zu ermitteln. Also werden nacheinander verschiedene Zahlenkombinationen ausprobiert. Sicher ist jedoch auch, dass man mit dieser Methode zwar langsam, aber doch stets zu einem Erfolg kommt (Drescher 2017: 89).

Die zu lösende Aufgabe hat verschiedene Elemente: Zunächst gibt es eine Information, die unbedingt unverändert bleiben muss und Informationen über Transaktionen enthält. Dies sind der Zeitstempel, die Referenz zum letzten Block, die Merkle-Wurzel und die Referenz auf das Regelwerk, wie in Abbildung 2 dargestellt. Dann gibt es eine Hash-Funktion, die genutzt wird, um die

⁵ Quelle: Eigene Darstellung

richtige Lösung zu bekommen. Schließlich müssen bestimmte Bedingungen erfüllt und das ganze über veränderbare Daten gelöst werden. Diese veränderbaren Daten heißen **Nonce** und haben, wenngleich in Form eines Hash-Wertes, einen beliebigen Inhalt. Das Ziel ist es, verschiedene Nonce-Ziffernkombinationen mit dem Hash-Wert der unveränderbaren Daten zu kombinieren und einen Hash-Wert zu ermitteln, der bestimmte Nebenbedingungen erfüllt. Diese Bedingungen werden auch **Schwierigkeit** genannt. Es ist sehr einfach, den kombinierten Hash-Wert von zwei zuvor einzelnen Hash-Werten zu berechnen – dazu wäre ein einfaches Smartphone in der Lage (Berentsen und Schär 2017: 203ff.). Um künstlich den Bearbeitungszeitraum einer Transaktion zu verlängern, werden Bedingungen aufgestellt, die dafür sorgen, dass pro Sekunde nur etwa sieben Transaktionen (in der Bitcoin-Blockchain⁶) durchgeführt werden können (PwC 2016: 11). Dies verhindert, dass Daten unzureichend durch das Netzwerk geleitet werden, weil jeder Node nur mit dem Lösen solcher Aufgaben beschäftigt wäre, für welche es finanzielle Anreize gibt.

Die Schwierigkeit wird durch eine natürliche Zahl ausgedrückt und meint die Anzahl von Nullen, mit denen der zu ermittelnde Hash-Wert beginnen soll. Bei einer Schwierigkeit von 1 muss mindestens eine Null vorne stehen. Da es 16 verschiedene Ziffern gibt, beträgt die Wahrscheinlichkeit, einen solchen Hash-Wert zu ermitteln 1/16 (Berentsen und Schär 2017: 143ff.). Bei einer Schwierigkeit von zehn müssen mindestens zehn Nullen vorne stehen. Je höher die Schwierigkeit ist, desto mehr Rechenleistung muss aufgebracht werden, um die Aufgabe zu lösen. Schwierige Aufgaben benötigen entsprechend mehr Zeit und es entsteht ein Wettlauf zwischen den Nodes (Vranken 2017: 2).

In der Praxis ist das Funktionsprinzip wie folgt: Ein **Miner** kreiert aus den in Abbildung 2 angegebenen Bestandteilen einen Hash-Wert für einen neuen Block, mit einer beliebigen laufenden Nummer als Nonce (Berentsen und Schär 2017: 209). Dieser Hash-Wert wird dann mit einem Schwellenwert verglichen, welcher sich aus der Schwierigkeit ergibt (ebd.: 208ff.). Erfüllt der Hash-Wert die Anforderungen, wird er der Kette hinzugefügt und von allen anderen Nodes übernommen. Erfüllt der Hash-Wert die Anforderungen nicht, kreiert der Miner einen neuen Hash-Wert und somit auch einen neuen Blockkandidaten, bei dem alle Bestandteile bis auf die Nonce gleich bleiben. Dieses Verfahren wird solange durchgeführt, bis der generierte Hash-Wert die Anforderungen erfüllt.

Da alle Miner bei dieser Methode in Konkurrenz zueinander stehen und generierte Blöcke nur bei Erfüllung der Schwierigkeit angenommen werden, kann man die einzelnen generierten Blöcke als Blockkandidaten bezeichnen, da sie Kandidaten dafür sind, der Kette angehängt und von allen Nodes übernommen zu werden. Es ist also nicht so, dass nur einmal die unveränderbaren Einheiten aus Abbildung 2 zu einem Hash-Wert verarbeitet werden und dann wie bei einem Tresor Zahlenkombinationen ausprobiert werden. Stattdessen muss für jeden Versuch ein neuer Hash-Wert und dementsprechend auch ein neuer Blockkandidat generiert werden (ebd: 208).

Wer als erste/r einen Blockkandidaten erstellt, der die Anforderungen der Schwierigkeit erfüllt, bekommt einen **Block Reward**. Der/die BetreiberIn eines Nodes darf dem jeweiligen Blockkandidaten eine sogenannte **Coinbase-Transaktion** hinzufügen. Diese Transaktion wird als letzte Transaktion in den neu erstellten Block integriert und sagt aus, dass der Gewinner x Einheiten, welche aus dem Nichts geschaffen werden, an sein eigenes Konto schickt. Im Bitcoin-System entspricht die Belohnung derzeit 12,5 Bitcoin-Einheiten, was am 14.03.2018 ca. 84.900 Euro entsprach⁷, wobei sich die Menge an Coins, also an systemimmanenten Geldeinheiten, alle vier Jahre hal-

⁶ Bitcoin ist zum einen die bekannteste virtuelle Währung und zum anderen die erste Blockchain Technologie überhaupt, Vgl. dazu Punkt 2.3.1

⁷ Vgl. aktuellen Bitcoin-Euro Wechselkurs unter Finanzen.net, www.finanzen.net/devisen/bitcoin-euro/chart (abgerufen am 09.12.2017)

biert. Die verschiedenen Blockchains haben jeweils unterschiedliche Methoden, ihre Miner zu entlohnen.

In der Regel bekommen erfolgreiche Miner eines Blocks jedoch stets die Transaktionsgebühren der darin enthaltenen Transaktionen. Derjenige, der Besitz überträgt, kommt für die Transaktionsgebühr auf. Dabei handelt es sich um eine Art Residualbetrag, welcher sich aus der Summe aller Transaktionsinputs abzüglich der Summe aller Transaktionsoutputs ergibt (Berentsen und Schär 2017: 215f.). Wer eine Transaktion initiiert, spricht diese Transaktionsgebühren in der Regel aus, um dadurch den Anreiz zur Verarbeitung ihrer Transaktion zu erhöhen. Während es relativ schwierig und zeitaufwendig ist, einen Hash für einen vorliegenden Block zu ermitteln, ist das Überprüfen, ob ein Hash-Wert korrekt ist, vergleichsweise leicht, was die Weiterleitung im Netzwerk erleichtert. Miner werden incentiviert, von anderen errechnete Hash-Werte für neue Blöcke zu überprüfen, da es ihnen die Chance bietet, bei der Identifizierung eines Fehlers von vorne zu beginnen, um ihrerseits einen korrekten Hash zu ermitteln und damit den Block Reward für sich zu beanspruchen. Hier kommen spieltheoretische Erkenntnisse ins Spiel, die beschreiben, warum durch Anreizschaffung die Miner das System stabilisieren und „mitspielen“.

Schließlich enthält das Blockchain-System noch einen Mechanismus, der Transaktionen autorisiert und mithilfe dessen sichergestellt wird, dass ein/e TransaktionsinitiantIn eine Transaktion auch wirklich durchführen wollte. Jede Person besitzt einen öffentlichen und einen privaten Schlüssel. Interessanterweise dienen die Schlüssel nicht der Geheimhaltung von Daten, sondern der Verifizierung des Ursprungs (Berentsen und Schär 2017: 55). Wird eine Nachricht mit dem **öffentlichen Schlüssel** verschlüsselt, kann sie nur mit dem privaten Schlüssel entschlüsselt werden. Wer lediglich in Besitz eines einzigen Schlüssels ist, kann entweder nur Nachrichten ver- oder entschlüsseln, weshalb man auch von asymmetrischer Kryptografie spricht. Letztendlich funktionieren beide Schlüssel gleich, sie werden nur durch ihre jeweilige Anwendung zum privaten bzw. öffentlichen Schlüssel. Während der öffentliche Schlüssel an andere weitergegeben und mit einer Art Kontonummer verglichen werden kann, verbleibt der private Schlüssel im eigenen Besitz und wird geheim gehalten (Voshmgir 2016: 13).

Eine Person, die ihr Eigentum an eine andere Person übertragen möchte, erstellt zunächst eine Nachricht und eine korrespondierende digitale Unterschrift. Dabei wird zunächst die Nachricht in einen Hash-Wert umgewandelt und dieser mit dem privaten Schlüssel verschlüsselt. Diese digitale Unterschrift ist einzigartig und kann nur zu der/m einen AbsenderIn zurückverfolgt werden, da ein einzigartiger **privater Schlüssel** verwendet wurde. Sowohl die Nachricht als auch die digitale Unterschrift werden in einem Ordner zusammengefasst, welcher dann an die benachbarten Nodes versendet und im Netzwerk verbreitet wird. Wer den öffentlichen Schlüssel dieser Person kennt, kann ihn dazu benutzen, ihren Text wieder zu entschlüsseln. Empfangende Nodes können verifizieren, dass diese Nachricht von dem sendenden Node autorisiert wurde, indem sie den Hash-Wert der Nachricht selbst bestimmen und dann die digitale Unterschrift der/s SenderIn mithilfe seines öffentlichen Schlüssels entschlüsseln. Dann werden beide Hash-Werte miteinander verglichen. Sind sie identisch, weiß die/der EmpfängerIn, dass die Nachricht von der/m SenderIn unterschrieben wurde und dass die Nachricht, die von der/m SenderIn geschickt wurde, tatsächlich auch die ist, die sie/er senden wollte (Drescher 2017: 105ff.). Unterscheiden sich die beiden Hash-Werte, wird festgestellt, dass es einen Hack gab und die/der SenderIn die Nachricht nicht autorisiert hat, weshalb sie ihr/m auch nicht zugerechnet wird.

Ein entscheidender Vorteil der Blockchain ist, dass sie nicht zwischen verschiedenen NutzerInnen differenziert. Sie interessiert nur die Richtigkeit und Konsistenz aller Hash-Werte, was eine wertvolle Eigenschaft ist. Wenn eine Transaktion nachträglich manipuliert wird, dann ändert sich auch der Hash-Wert dieser Transaktion. Und damit die des zusammengefassten Transaktions-Paares. Und damit die des wiederrum zusammengefassten Hash-Wert-Paares. Schließlich ändert sich auch der

Hash-Wert des gesamten Merkle-Baums und damit die Überschrift jedes Blocks und dessen Referenz sowie jede einzelne Referenz, die auf diesen Block verweist. Eine Änderung ist also mit prohibitiv hohen Kosten und Aufwand verbunden.

Wenn die Schwierigkeit jedoch herabgesetzt wird, also zum Beispiel eine Aufgabe gelöst werden muss, die nur die Nebenbedingung hat, dass eine einzige Null am Anfang steht, so ist eine Manipulation nicht mehr mit so viel Rechenleistung und Zeitaufwand verbunden. Wenn anders herum die Schwierigkeit jedoch zu hoch ist, dann sind die Kosten für die aufzubringende Rechenleistung so hoch, dass es keinen Anreiz gibt, einen neuen Block hinzuzufügen (Drescher 2017: 142). Bei dem Design einer neuen Blockchain gilt es, diese beiden Aspekte zu berücksichtigen und eine geeignete Balance zu finden. Dies wird durch die Tatsache erschwert, dass technische Neuerungen und verbesserte Hardware leistungsfähiger sind und schneller Hash-Werte errechnen können. Deswegen beinhalten einige Blockchains Mechanismen, die den Schwierigkeitsgrad automatisch anpassen, um in einem bestimmten Abstand (zum Beispiel durchschnittlich alle 10 Minuten) einen neuen Block zu kreieren.

2.2.2 Proof-of-stake-Konsensmethode

Die bekannteste Alternative zum proof-of-work-Validierungsmechanismus ist die **proof-of-stake-Methode**, in der keine Arbeit (work), sondern Vermögen (stake) bewiesen wird. Bei der proof-of-stake-Konsensmethode wird die Rechenleistung dadurch reduziert, dass Mitglieder des Netzwerks sich nicht in einem ständigen Wettlauf um korrekte Hash-Werte befinden. Es müssen keine komplizierten kryptografischen Aufgaben von allen Minern gelöst werden, sodass Miner nicht mehr zwingend die neuste Hardware benötigen. Die Schwierigkeit ist individuell für jede/n NutzerIn festgelegt: nämlich umgekehrt proportional zum Alter der Coins oder alternativ der Anzahl der besessenen Coins. Im Vorfeld wird ein einziger Miner dazu bestimmt, einen neuen Block zu minen – die Rechenleistung kann also dadurch drastisch gesenkt werden, dass unnötige Rechenleistung von Tausenden von Minern vermieden wird.

Das Vermögen der Miner (die in diesem System **Forger** genannt werden, aber hier der Einfachheit halber weiterhin als Miner bezeichnet werden) wird entweder durch das "Coin Age" oder die Anzahl der besessenen Coins bestimmt. Dieses Coin Age ergibt sich aus der Menge der Coins mal der Zeitperiode, in der die Coins vom jeweiligen Nutzer nicht genutzt wurden (King und Nadal 2012: 1f.). Je älter die Coins, desto höher die Chance, einen Block zu gewinnen. Wenn ein Block jedoch gewonnen wird, wird das Alter der Coins des Gewinners zurückgesetzt, was regelmäßig neue Chancen für alle Teilnehmenden schafft (Vranken 2017: 7). Es vergehen in der Regel mindestens 30 Tage, bis sich ein solcher Coin wieder an einer Transaktion beteiligen kann. Wird ein Block erstellt, erhält der Miner keinen Block Reward, sondern lediglich die Gebühren für die Transaktionen, die in diesem Block enthalten sind. Ein Schutzmechanismus vor Hacker-Angriffen wird dadurch eingebaut, dass alle Nodes bei jeder Transaktion eine erstattungsfähige Gebühr zahlen müssen, sodass es sich ökonomisch nicht lohnt, das System zu manipulieren (Wiedmaier 2017: 51f.).

Es gibt zahlreiche Kritikpunkte auch gegenüber diesem System und innerhalb der Community herrscht Uneinigkeit darüber, welche der beiden Konsensmethoden resistenter gegenüber Angriffen ist⁸. Um das proof-of-work-System manipulieren zu können, benötigt eine Person oder Institu-

⁸ Die Kritik lässt sich z. B. in Blogs wie diesen finden:

<https://sjkelleyjrblog.wordpress.com/2017/09/16/criticisms-of-proof-of-stake/>

<https://medium.com/@tuurdemeester/re-buterins-criticism-of-my-pos-piece-4ee70d6fd289>

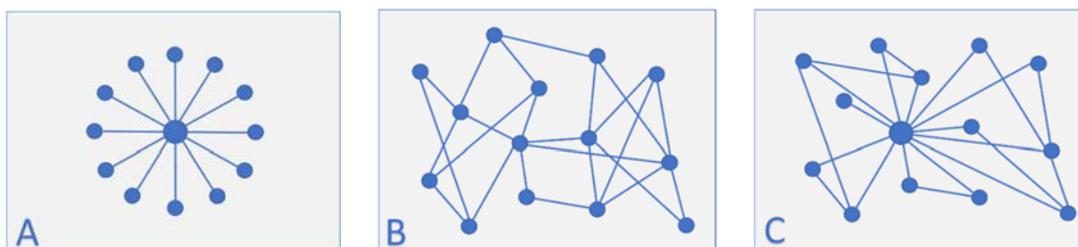
tion so viel Geld, sich Mining-Hardware kaufen zu können, die über 50 % der Coins schürft. Bei der proof-of-stake-Methode hingegen müssen über die Hälfte der sich im Umlauf befindenden Coins gekauft werden. Beides gilt als so gut wie unmöglich, da „[t]he most important weapon of the blockchain against dishonest nodes is the power of the honest majority and the effects of reward and punishment“ (Drescher 2017: 162).

Neben den beiden bislang am meisten verbreiteten Konsensmethoden proof-of-work und proof-of-stake gibt es noch Kombinationen dieser sowie gänzlich neue Konzepte wie proof-of-space, proof-of-space-time, proof-of-burn oder proof-of-identity (Vranken 2017: 7; Mengelkamp et al. 2017a: 4). In diesem dynamischen Umfeld ist es durchaus möglich, dass sich letztlich nicht eine der beiden bislang führenden Konsensmethoden durchsetzen wird.

2.3 Beispiele für Blockchains

2.3.1 Bitcoin

Bitcoin ist nicht nur die beliebteste **Kryptowährung** oder das prominenteste Beispiel eines Blockchain-basierten Systems, sondern auch die Geburtsstunde der Technologie selbst. Im Jahr 2008 veröffentlichte eine Person oder eine Gruppe von Personen unter dem Pseudonym „Satoshi Nakamoto“ ein White Paper mit dem Titel „Bitcoin: A Peer-to-Peer Electronic Cash System“ und verschickte es über eine Mailing-Liste für Kryptographie, bevor die erste Bitcoin-Version im Januar des nächsten Jahres online ging (Wilson 2017). Nakamoto selbst sah keine gesonderte Rolle für sich vor, weshalb sein Entwurf später von Dritten modifiziert und weiterentwickelt wurde (Berentsen und Schär 2017: 67). Die Entstehung von Bitcoin lief zeitlich parallel zu anderen disruptiven digitalen Geschäftsmodellen, die einige etablierte Unternehmen vor neue Herausforderungen stellten. Mit „Airbnb“ (2008) wurden MieterInnen zu VermieterInnen, mit „Uber“ (2009) AutobesitzerInnen zu TaxifahrerInnen und mit „ebay Kleinanzeigen“ (2009) KäuferInnen zu VerkäuferInnen. Diese neue Art des Handels setzte auf den direkten Kontakt zwischen BenutzerInnen und brachte den oben genannten Start-ups erhebliche Gewinne ein.



- A) Zentralisiertes Netzwerk
- B) Dezentrales Netzwerk
- C) Dezentrales Netzwerk mit einem zentralen Element

Abbildung 3: Netzwerkstrukturen⁹

<https://cointelegraph.com/news/the-inevitable-failure-of-proof-of-stake-blockchains-and-why-a-new-algorithm-is-needed>
www.coindesk.com/short-guide-blockchain-consensus-protocols/

⁹ Quelle: Eigene Darstellung

Bitcoin unterscheidet sich jedoch insofern von ihnen, als dass es keine zentrale Kontrolle über das System gibt. Die Bitcoin Foundation hat zwar eine Governance-Struktur, die zur Standardisierung und zum Schutz von Bitcoin dient, die aber keine Zahlungsmittel ausgibt und auch sonst nicht als zentrale Bank agiert (Vranken 2017: 1). Die Mitglieder des Netzwerks müssen eigene Ressourcen aufbringen, um Handlungen vorzunehmen. Für das Mining werden sie mit den in Kapitel 2.1.2 (Von einzelnen Transaktionen zur Kette) bereits erwähnten Block Rewards kompensiert, welche sie dann in „wirkliche“ Währungen umtauschen können. Mit einem Volumen von umgerechnet etwa 215 Milliarden Euro (Stand 09.12.2017)¹⁰ ist die Bitcoin-Währung im Vergleich zum kumulierten Gesamtwert der Euro-Währung in Höhe von 10.900 Milliarden Euro (Trentmann et al. zitiert nach dena 2016: 28) zwar nicht annähernd so groß, aber eben auch nicht unbedeutend. Mittlerweile gibt es eine wachsende Anzahl an Hotels, Geschäften und Restaurants, die Bitcoins als Zahlungsmittel akzeptieren. Mit Zug, einer Gemeinde in der Schweiz, nimmt die erste Behörde Bitcoins als Zahlungsmittel an (PwC 2016: 11).

Wer mit Bitcoins handeln möchte, erhält ein Wallet, also quasi eine elektronische Geldbörse (ebd.: 11). Die Bitcoin-Adresse ist dabei der öffentliche Schlüssel, auf den nacheinander zwei Hash-Funktionen angewandt werden. Der doppelte Hash sorgt dafür, dass von der Bitcoin-Adresse nicht auf den öffentlichen Schlüssel geschlossen werden kann (Einwegfunktion). Durch die Bitcoin-Adresse muss der öffentliche Schlüssel erst zum Zeitpunkt einer Transaktion bekannt gegeben werden (Berentsen und Schär 2017: 126). Für jede Transaktion wird ein neues Schlüsselpaar erstellt, was verhindert, dass durch Nutzungsmuster Rückschlüsse auf die Identität eines Nodes gezogen werden können (ebd.: 129).

Das Bitcoin-Protokoll beinhaltet einen Algorithmus, der die Schwierigkeit, einen gültigen Hash-Wert zu berechnen, anpasst, sodass etwa alle zehn Minuten ein neuer Block entsteht. Wird die Hardware leistungsfähiger, werden die mathematischen Probleme, die gelöst werden müssen, schwerer. Der Block Reward lag ursprünglich bei 50 BTCs (Bitcoins), wobei er alle 210.000 Blocks halbiert wird (ca. alle vier Jahre) und bis 2140 unter 1–8 BTC fallen wird, welches die kleinste Einheit des Bitcoins (namens „satoshi“) ist (Vranken 2017: 2). Dann ist die Obergrenze an Bitcoins, die je im System zirkulieren wird, mit 21 Millionen Bitcoins erreicht, da neue Bitcoins ausschließlich über Block Rewards generiert werden können. Ab 2140 wird nur noch die Transaktionsgebühr ein finanzieller Anreiz für die Miner sein, ihren Beitrag zur Systemstabilität zu leisten.

Der Wechselkurs unterliegt wie bei allen Kryptowährungen starken Schwankungen und liegt am 14.03.2018 bei knapp 6.800 Euro¹¹. Dennoch ist ein klarer Aufwärtstrend mit exponentieller Tendenz erkennbar. Durch das Wachstum des Netzwerkes ist der Wandlungspreis um 4.000 % innerhalb von acht Jahren gestiegen (Wilson 2017). Ein Vorteil der Bitcoins gegenüber „echten“ Währungen könnte es sein, dass es eine feste Anzahl von Bitcoins gibt, was die Kryptowährung vor einer Inflation schützt. Einige sehen in Bitcoin eine Weltreservewährung (Interview 2), was auch durch die Beobachtung gestützt wird, dass der Kurs rasant stieg, als die Verhandlungen um einen möglichen Brexit aufgenommen wurden, im Zuge dessen Marktunsicherheiten entstanden (Berentsen und Schär 2017: 90).

¹⁰ Dieser Zahl zugrunde liegt eine kumulierte Gesamtmenge an Bitcoins von 16,71 Millionen am 09.12.2017 (vgl. Statista 2017b: <https://de.statista.com/statistik/daten/studie/283301/umfrage/gesamtzahl-der-bitcoins-in-umlauf/>, abgerufen am 09.12.2017) und ein Wechselkurs von 12.922 Euro/BTC (vgl. Finanzen.net. www.finanzen.net/devisen/bitcoin-euro/chart, abgerufen am 09.12.2017).

¹¹ Für den aktuellen Wechselkurs vgl. www.finanzen.net/devisen/bitcoin-euro/chart

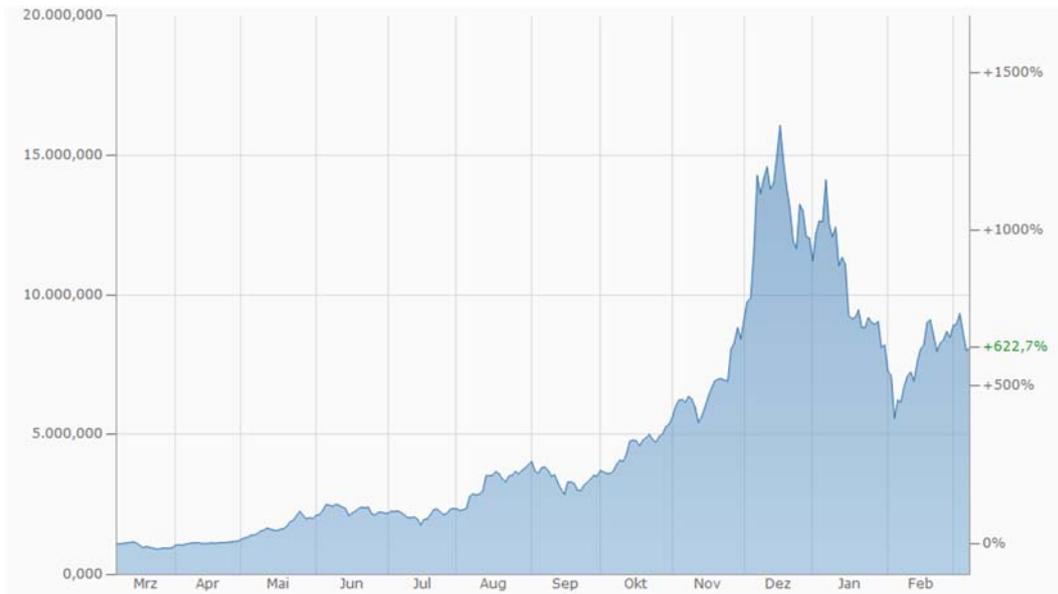


Abbildung 4: Bitcoin-Euro-Wechselkurs von März 2017 bis Februar 2018¹²

Viele der Bitcoin-Miner, also jene, die die mathematischen Aufgaben mithilfe einer starken Rechenleistung lösen, befinden sich in Regionen in unmittelbarer Nähe zu günstigen Energiequellen – etwa in der Nähe von Chinas großen Staudämmen oder den geothermischen Energiequellen Islands. Das Minen, also das „Schürfen“ (Erstellen) von Blocks, ist in Deutschland nicht sehr lukrativ, da der Preis für Strom mit 29 Cent pro kWh um ein Dreifaches höher liegt als in Island (Pannewick und Herbst 2017). Es gibt hohe Eintrittsbarrieren in den Markt, da der Investitionsaufwand für Hardware stetig steigt, weshalb sich ein oligopolistischer Markt herausgebildet hat (Vranken 2017: 4). Nach Angaben von Bitcoinchain.com generierten die größten fünf Miner über 85 % der Blocks von 2016. Dies widerspricht fundamental der zugrundeliegenden Idee einer dezentralen Wertschöpfung.

Die ursprüngliche Form des Solo-Minings betreiben zudem nur Rechner, die über eine entsprechend hohe Rechenleistung verfügen. Aufgrund dieser Entwicklung schließen sich Privatpersonen zunehmend in Netzwerken, wie zum Beispiel dem „BitClub Network“, zusammen, um mit den gebündelten Kräften Bitcoins zu schürfen und diese dann unter den Teilnehmenden anteilig aufzuteilen. Dadurch steigt für die Teilnehmenden die Planungssicherheit und es handelt sich nicht länger um ein Lotteriespiel, bei dem lange Zeiträume ohne Entlohnung überbrückt werden müssen (Berentsen und Schär 2017: 222). Auch dies führt jedoch zu schleichenden Zentralisierungstendenzen des Bitcoin-Systems.

In der gesamten Geschichte von Bitcoin kam es nie zu dem Fall, dass eine Transaktion nachträglich manipuliert wurde oder das System gar ganz abgeschaltet wurde. Tatsächlich gab es aber eine Reihe von Hacker-Angriffen auf Handelsbörsen, über die dann Bitcoins im Wert von mehreren Millionen US-Dollar entwendet wurden (Berentsen und Schär 2017: 87ff.). Um das System lahmzulegen, müsste allerdings etwas in der Größenordnung eines weltweiten Stromausfalls geschehen (BlockchainHub 2017).

Dennoch ist Bitcoin nicht unumstritten. Erstens wird immer häufiger der immense Stromverbrauch des Netzwerks kritisiert (vgl. Pannewick und Herbst 2017, Vranken 2017:1). Zweitens wird kritisiert,

¹² Quelle: Finanzen.net 2018a

die extreme Kursvolatilität sei mit spekulativem Zocken von Privatleuten verbunden, welche die Risiken aufgrund der Komplexität des Systems nicht richtig einschätzen könnten (vgl. z. B. Spiegel Online 2017b). Drittens wird darauf hingewiesen, dass insbesondere die darknet-Plattform „Silk Road“ Bitcoin zur schnellen Ausbreitung verhalf. Mithilfe von Bitcoin konnten illegale Stoffe und Dienste völlig anonym gehandelt werden (Berentsen und Schär 2017: 83). Es gibt jedoch auch Gegenbeispiele, in denen Bitcoin nicht die Intransparenz illegaler Geschäfte, sondern die Transparenz gegenüber problematischen Vorgängen fördert. So hat Bitcoin erheblich zur Unterstützung von Wikileaks beigetragen, deren Spendenkampagnen nicht länger von Paypal getragen wurden (ebd.: 83f.). Viertens: Bitcoin ist bislang ungeeignet für Echtzeit-Transaktionen, da es zwischen der Einspeisung einer Transaktion ins Netzwerk und einer Bestätigung dieser Verzögerungen von mehreren Minuten gibt. Allerdings kann Geld so innerhalb von einigen Minuten einmal um die Erde geschickt werden. Darin ist Bitcoin den klassischen Banküberweisungen weit voraus. Dies sind nur einige größtenteils Bitcoin-spezifische Vor- und Nachteile von Blockchain-Anwendungen. Auf einige wird in Kapitel 4 (Chancen und Potenziale) und Kapitel 5 (Risiken und Schwachstellen) expliziter eingegangen, wobei dort ein Schwerpunkt auf dem Thema Energie liegen wird.

Das Bitcoin-System kann durch jede Person einfach kopiert werden. Dadurch werden aber keine neuen Bitcoin-Einheiten geschaffen, weshalb ein neues Netzwerk keine Bedrohung für die Systemstabilität von Bitcoin darstellt, sofern die Marktdominanz von Bitcoin nicht durch einen Konkurrenten gefährdet wird. Der Bitcoin Code kann übernommen und beliebig angepasst werden, was auch schon über 600 Mal passiert ist (Statista 2017c). Diese Kopien heißen **Altcoins** (Alternative Coins). Sie haben größtenteils noch keine kritische Masse erreicht, während Bitcoin von bestehenden Netzwerkeffekten profitiert (Berentsen und Schär 2017: 71).

2.3.2 Ethereum

Letztendlich ist Bitcoin jedoch „nur“ eine Kryptowährung. Die Transaktionen beschränken sich auf den Transfer von Geld von einem absendenden zu einem empfangenden Node. Dies fiel auch dem damals 18-jährigen Vitalik Buterin auf, der 2013 ein White Paper für Ethereum veröffentlichte, welches jegliche Art von Peer-to-Peer-Wertaustausch ermöglicht und eine erste wirkliche Alternativtechnologie zur Bitcoin Blockchain darstellt (Voshmgir 2016: 15). Ethereum hat innerhalb von wenigen Wochen 18 Millionen US-Dollar zusammen bekommen – die damals drittgrößte Summe, die je in der Geschichte über eine Crowdfunding-Kampagne eingenommen wurde (Bitcoin Generator 2017). Neben neuartigen Anwendungsbereichen stellt Ethereum eine Verbesserung zu der Bitcoin Blockchain auch dadurch dar, dass alle 10 Sekunden ein neuer Block kreiert wird und 1.000 Transaktionen pro Sekunde aufgenommen werden können (Ewald Hesse 2017b).

Mit Ethereum wurden weitere Funktionen und Nutzungsmöglichkeiten der Blockchain in den Fokus gerückt. So ermöglicht das Ethereum-Rechnernetzwerk die Nutzung und Etablierung von den im Folgenden diskutierten Smart Contracts, DApps und DAOs.

Smart Contracts sind Computerprotokolle, mithilfe derer digitale Verträge über die Blockchain geschlossen und ausgeführt werden können. Dabei einigen sich die Vertragsparteien zunächst über die Vertragseinzelheiten, wie die beteiligten Personen, Mengen und Preise. Aktionen werden automatisch ausgeführt, sobald eine bestimmte Bedingung erfüllt ist oder ein bestimmtes Ereignis eintritt (Wenn-dann-Funktion). Wird zum Beispiel ein Vertrag zwischen einem Energieversorgungsunternehmen und einer/m VerbraucherIn geschlossen und kommt letztere/r ihrer/seiner Zahlung nicht nach, wird von Anbieterseite kein Strom mehr geliefert. Dies kann unter sozialen und menschenrechtlichen Gesichtspunkten äußerst problematisch sein, denn die Stromversorgung wird erst wieder aufgenommen, sobald die Zahlung nachträglich geleistet wird (Sieverding und Schneidewind 2016: 2). Dieses Prinzip kann auf eine Vielzahl von möglichen Einigungen zwischen

Personen angewendet werden. Einigen sich A und B darauf, dass B eine bestimmte Aufgabe für A erledigt und dafür eine vorher festgelegte Geldsumme bekommt, so wird diese Summe zunächst von A beiseitegelegt, ohne dass B einen Zugriff darauf hat. Erledigt B die Aufgabe, kann A eine Freisetzung der Summe veranlassen. Wenn sich jedoch die Parteien nicht darüber einig sind, ob der Auftrag in vollem Umfang erfüllt wurde, kann nach einer 7-tägigen Wartezeit ein unabhängiger Richter hinzugezogen werden, der dann ein Urteil fällt (Buterin 2014).

Smart Contracts müssen auch nicht immer zwischen Parteien geschlossen werden, die sich bei Vertragsschluss schon kennen. Will Person A 100 Einheiten von Gut X an jemanden verkaufen, der ihm dafür 50 Einheiten von Gut Y bietet, dann ist dies schon ein Smart Contract (ebd.), ohne dass alle zukünftig beteiligten Personen im Vertrag genannt werden.

Die Ausführung von Smart Contracts folgt derselben Logik wie andere Transaktionen über die Blockchain: Wenn die Vertragsbedingungen erfüllt sind, wird dies im Ledger aktualisiert und ist von allen Nodes im Netzwerk zu sehen (Wiedmaier 2017: 18). Instanzen, über die vorher Verträge dieser Art abgewickelt wurden, wie NotarInnen, RechtsanwältInnen oder Bankangestellte, müssen nun nicht mehr konsultiert werden. Dies hat den Vorteil, dass Smart Contracts die Transaktionskosten für die Koordination und Durchsetzung senken und Transaktionssicherheit schaffen (BlockchainHub 2017). Zahlungsausfallrisiken werden dadurch gesenkt oder sogar eliminiert, dass vorher festgelegt wird, dass ein/e KäuferIn einen Vertrag nur dann abschließen kann, wenn sie/er über Geldmengen in Höhe des festgelegten Preises verfügt (Scholtka und Martin 2017: 117). Auch dies kann allerdings in erheblichem Ausmaß soziale Ausschlusstendenzen befördern.

Mit Smart Contracts werden viele bürokratische Hürden überwunden. Automatisierungsprozesse erleichtern die Verschlinkung und Beschleunigung von Prozessen. Allerdings ist jeder Smart Contract auch nur so smart wie die Personen, die ihn codieren (Blockchain Hub 2017). Ferner sollten sie nicht mit rechtsgültigen Verträgen verwechselt werden, solange die Technologie noch nicht gereift und der Rechtsrahmen noch nicht angepasst ist. Es ist jedoch eine Fusion von Rechtsverträgen und Smart Contracts zu erwarten (ebd.).

DApps sind dezentrale Anwendungen, bei denen alle Aktionen vom Unterbau der App bis hin zur Benutzeroberfläche über eine Blockchain laufen. Auch sie funktionieren ähnlich wie Smart Contracts (Voshmgir 2016: 14), aber unterscheiden sich in zweierlei Weise: Während Smart Contracts zwischen einer bestimmten Anzahl von Personen geschlossen werden, haben dezentrale Apps eine unbegrenzte Anzahl von Teilnehmenden. Außerdem beziehen sich Smart Contracts bisher meistens auf Finanzen, während der Anwendungsbereich von DApps wesentlich breiter ist. Smart Contracts ermöglichen den Anschluss von DApps an eine Blockchain erst; sie sind Bestandteile einer DApp.

Es handelt sich dabei um open-source Anwendungen, wobei ebenfalls keine einzelne Organisation Rechtsansprüche auf diese Verträge erheben und letztere kontrollieren kann (PwC 2016: 6). Ebenso unterliegen DApps einem dezentralen Validierungsmechanismus und Daten werden dezentral und kryptografisch gespeichert. Bislang gibt es für DApps noch keine dezentralen Benutzeroberflächen und lediglich der technische Background beruht auf Smart Contracts. Das Ziel ist es, unabhängig von Benutzeroberflächen von Drittparteien zu werden, um eine komplett dezentrale und autonome Anwendung zu schaffen (BlockchainHub 2017). Eine DApp nutzt kryptographische **Tokens**, also Kryptowährungen (Coins) wie zum Beispiel Bitcoins, Ether oder andere Altcoins, mithilfe derer die UnterstützerInnen des Systems (wie Miner) für ihren Beitrag entlohnt werden.

Das Akronym **DAO** steht für „decentralized autonomous organization“. DAOs sind eine neue Form der Organisation, deren Gesellschaftsvertrag oder Satzung durch einen Smart Contract abgebildet wird. Somit stellen DAOs die komplexeste Form von Smart Contracts dar (Voshmgir 2016: 14). Der Rechtsstatus von DAOs ist derzeit noch unklar, während das Potential groß ist. Änderungen der

Organisation können durch eine Abstimmung aller Token-Besitzer veranlasst werden (PwC 2016: 36). Das Stimmrecht bemisst sich in Proportion zu der Menge an gehaltenen Tokens. Dies kann durchaus als problematisch angesehen werden, da das Prinzip „one (wo)man, one vote“ hier quasi durch ein Prinzip „one token, one vote“ ersetzt wird. Auch wenn DAOs gänzlich neue Organisationsformen repräsentieren, haben sie selbst – zumindest in den vorliegenden Formen – keine künstliche Intelligenz und können dementsprechend nicht selbst Codes schreiben oder Produkte entwickeln (ebd.: 36). Im Gegensatz zu konventionellen Organisationen agiert eine unbestimmte Anzahl von Personen nach einem durch einen Code spezifizierten Protokoll miteinander (BlockchainHub 2017). Der Vorteil liegt darin, dass durch Informationssymmetrien keine Prinzipal-Agent-Dilemmata¹³ bestehen. Spezielle Aufgaben, die Fachwissen erfordern, werden von gewählten TeilnehmerInnen oder externen SpezialistInnen übernommen (Voshmgir 2016: 14). DAOs finanzieren sich durch ein sogenanntes **Initial Coin Offering (ICO)**, was mit einem dezentralen Crowdfunding zu vergleichen ist. Wenn eine dezentrale Organisation erst einmal aufgestellt ist, ist sie unabhängig von den Entwickelnden und kann durch externe Kräfte nicht beeinflusst werden, was sie nicht korrumpierbar macht (BlockchainHub 2017). Es gibt kein hierarchisches Management und alle Regeln, die es in Unternehmungen üblicherweise gibt, werden digital durchgesetzt.

Das berühmteste auf der Ethereum Blockchain aufbauende Projekt war eine Organisation namens „The Dao“, welche 2016 gegründet wurde und schon nach ein paar Monaten in einen großen Skandal verwickelt wurde. Die zugrundeliegende Idee von The DAO war, dass jede Person mit Internetzugang DAO-Wertmarken kaufen und darüber abstimmen konnte, welche Projekte finanziert werden sollten. Alle Stakeholder konnten auch über die Einführung neuer Regeln oder die Amtsenthebung bestimmter Personen abstimmen (Finley 2016). Es stellte sich nach wenigen Wochen heraus, dass es einen Fehler im Code gab, der bis dato unentdeckt geblieben war. Schließlich spürte ein Hacker diese Sicherheitslücke auf und es gelang ihm, dem System 60 Millionen US-Dollar zu entnehmen. Dies zeigte auf vielerlei Weise Probleme auf: Zum einen machte der Vorfall deutlich, dass selbst herausragende ProgrammiererInnen einen folgenschweren Fehler im Code übersehen können. Zum anderen stellte es die ProgrammiererInnen vor ein Dilemma: entweder sie akzeptierten den Vorfall und den Verlust der 60 Millionen oder sie griffen in das Netzwerk ein und änderten nachträglich das Protokoll. Die Mehrheit der Community stimmte für eine Änderung des Transaktionsprotokolls und den rechtmäßigen BesitzerInnen wurde ihr Geld zurückerstattet. Bei jenen, die gegen einen Eingriff stimmten, löste der Code-Bruch jedoch große Empörung aus (Hertig 2017).

Das Vertrauen in die Stabilität der Ethereum zugehörigen Kryptowährung Ether wurde außerdem durch eine Falschmeldung im Netz in Mitleidenschaft gezogen. Im Juni 2016 wurde die Falschnachricht verbreitet, Buterin sei bei einem Autounfall ums Leben gekommen (Quartz 2016). Zwar ist er weder Eigentümer von Ethereum noch hält er ein Amt inne, jedoch gilt er als genialer Kopf des Netzwerks. Dass Ethereum binnen weniger Stunden an Marktwert in Höhe von vier Billionen US-Dollar verlor, zeigt, wie instabil selbst ein komplett dezentrales System sein kann, welches postuliert, von zentralen Instanzen und Personen unabhängig zu sein. Zwar ist es für den Aufbau von Funktionen wie Smart Contracts oder DApps nicht zwingend notwendig, dass die systemzugehörige Kryptowährung stabil ist oder stetig im Kurs steigt, doch wird eine gewisse Zahl von Minern benötigt, um das System aufrecht zu erhalten und Sicherheit zu gewährleisten. Ohne eine

¹³ Prinzipal-Agent-Theorie: Bei Beziehungen zwischen zwei Parteien hat eine Partei der anderen gegenüber einen Informationsvorsprung. Durch diese Asymmetrie entstehen Ineffizienzen bei der Vertragsdurchführung. Wenn der Auftraggeber (Prinzipal) die Handlungen des Auftragnehmers (Agent) nicht überwachen kann, können Handlungen im Verborgenen durchgeführt werden (Hidden Action). Beide können Informationen bewusst zurückhalten (Hidden Information) und die Leistungsfähigkeit des Agenten ist nur diesem bekannt (Hidden Characteristics) (vgl. Gabler Wirtschaftslexikon 2017).

entsprechende finanzielle Entschädigung fehlt der Anreiz, ein Netzwerk zu stabilisieren. Andererseits gelang es dann Buterin, seine Unversehrtheit mittels einer kryptographischen Signatur seines Etherums zu beweisen, was durch einen Post auf sozialen Medien oder ein Video nicht so einfach und fälschungssicher möglich gewesen wäre. Der Kurs erholte sich deutlich, blieb aber volatil.



Abbildung 5: Ether-Euro-Wechselkurs von März 2017 bis Februar 2018¹⁴

2.4 Private vs. öffentliche Blockchains

Sowohl bei Bitcoin als auch bei Ethereum handelt es sich um öffentliche Blockchains. Öffentlich bedeutet, dass alle Personen mit Internetzugang Zugriff auf Daten und Leistungen haben, es keine zentrale Organisation gibt und die Identitäten der Teilnehmenden anonym sind. Die Validierung geschieht (bislang) entweder über proof-of-stake- oder proof-of-work-Konsensmethoden (vgl. Kapitel 2.1 und 2.2). Dem gegenüber stehen private Blockchains, deren Zugang zum Beispiel durch eine Gebühr oder den Erwerb von Soft- oder Hardware erkaufte werden muss (Sieverding und Schneidewind 2016: 2). Die Validierung wird zumeist durch vorher festgelegte NutzerInnen vorgenommen, weshalb die Identitäten der Teilnehmenden in der Regel bekannt sind.

Private Blockchains wurden zuerst auf Initiative von Unternehmen des Finanzsektors entwickelt. Dort sind es zum Beispiel Banken, die einer Person den Zugang zur Blockchain erst ermöglichen, wenn diese eindeutig identifiziert wurde. Dadurch, dass keine aufwändigen, komplett dezentralen Validierungsschemata durchlaufen werden müssen, können Transaktionen noch schneller und zu geringeren Kosten durchgeführt werden (PwC 2016: 9). Mithilfe von privaten Blockchains wird es möglich sein, dass etablierte Unternehmen wie Banken oder Börsen ihre Marktmacht verteidigen, indem sie ihre KundInnen auf die von ihnen kontrollierte Blockchain umleiten, für deren Nutzung sie Gebühren erheben können. Es ist allerdings auch denkbar, dass neue Unternehmen sich über von ihnen kontrollierte Blockchains Marktmacht mit innovativen Anwendungen „erobern“.

¹⁴ Quelle: Finanzen.net 2018b

Des Weiteren wird die Manipulationssicherheit und Unveränderlichkeit des Blockchain-Protokolls dadurch in Frage gestellt, dass die Regeln zumindest prinzipiell jederzeit von der übergeordneten Instanz geändert werden können. Es liegt in der Entscheidungshoheit des jeweiligen kontrollierenden Unternehmens, ob die Transaktionshistorie einsehbar ist und eine gewisse Systemtransparenz erhalten bleibt. Private Blockchains ähneln eher konventionellen Cloud-Strukturen (Sieverding und Schneidewindt 2016: 2). Cloud-Anwendungen basieren auf zentraler Datenspeicherung, wobei Daten über das Internet auf Servern gespeichert werden, deren Standort irrelevant ist (Voshmgir 2016: 9). Hinter Cloud-Anbietern wie Google Drive, Dropbox oder der iCloud steht jeweils ein gewinnorientiertes Unternehmen, dessen Zusammenarbeit mit Geheimdiensten vermutet oder nicht ausgeschlossen wird und bei dem die Frage der Wahrung der Privatsphäre nicht hinreichend beantwortet wird. Außerdem ist zu vermuten, dass die eigentlichen Verbesserungen in Sachen Sicherheit und Resilienz nur inkrementell im Vergleich zu konventionellen Systemen sind (BlockchainHub 2017).

Für eine Anwendung im Energiesektor, die vor allem den VerbraucherInnen zugutekommen soll, wäre es erstrebenswert, die Etablierung öffentlicher Blockchains zu fördern und den Handlungsspielraum für private BlockchainanbieterInnen einzuschränken. Transparenz kann, muss aber nicht zwingend auf privaten Blockchains gewährleistet werden, während öffentliche Blockchains komplett transparente open-source-Anwendungen sind. Andererseits ist schneller mit geglückten Anwendungen und Ergebnissen zu rechnen, wenn Blockchains zunächst als private oder Konsortial-Blockchains entwickelt werden (Interview 2).

Eine Konsortium-Blockchain, gebildet von meist führenden Unternehmen einer Branche, liegt hinsichtlich der Eigenschaften zwischen privaten und öffentlichen Blockchains und ähnelt je nach individueller Ausgestaltung der einen oder anderen Seite mehr. Gerade für große, kommerzielle Anwendungen bietet die Blockchain großes Potenzial in Bezug auf Verbesserungen aufgrund von Standardisierung, Automatisierung, Rationalisierung von Prozessen und Kostenreduktion (Drescher 2017: 247). Es bleibt jedoch fraglich, ob sich die öffentlichen Blockchains durchsetzen können, wenn einige Unternehmen zunächst ihre Marktstellung mithilfe von privaten oder Konsortial-Blockchains gesichert haben.

2.5 Forschung und Anwendung

In einem Literaturüberblick von Cao et al. (2017) wurden bisherige Veröffentlichungen zum Thema Blockchain auf Herkunft, Art der Analyse und Themenschwerpunkt untersucht. In der Literatur aus China sind 125 der insgesamt 188 Artikel dem Themenkomplex "Finanzen" zuzuordnen. Insbesondere die Bereiche Digitale Währungen, Bank und Internet-Finance sind hier zentral, weitere Themen sind Bezahlung, Rechnung und Lieferketten-Finance. Weiterhin sind 99 % der Artikel qualitativer Art, was die AutorInnen damit begründen, dass sich die Forschung zum Thema Blockchain in China noch in den Kinderschuhen befindet. In ihrer Analyse der englischsprachigen Literatur identifizieren sie über 41 % der Artikel als quantitative Forschungsergebnisse (Cao et al. 2017: 115). Auch hier stellen Artikel zum Thema Blockchain im Finanzwesen mit über 70 % die Mehrheit dar.

Eine weitere relevante Erkenntnis ist, dass die Beschäftigung mit der Blockchain-Technologie erst in 2016 so richtig Fahrt aufnahm. In den Jahren 2014 und 2015 wurden im chinesischen Raum jeweils unter fünf Artikel publiziert, während es 2016 dann 180 waren (Cao et al. 2017: 110). Dies zeigt auch die dieser Arbeit zugrundeliegende, vor allem auf europäische Veröffentlichungen zurückgreifende Recherche – mit wenigen Ausnahmen bekannter VordenkerInnen.

Auch in der Praxis sind Anwendungen im Finanzsektor dominierend. Während es sich in vielen anderen Bereichen erst um Pilotprojekte handelt, können Unternehmen aus der Finanzbranche

bereits erste Erfolge in der Implementierung und Durchführung verzeichnen (PwC 2016: 9ff.). Einsatzbereiche sind jedoch vielfältig:

Das Start-up „Onename“ beispielsweise erstellt einen virtuellen, fälschungssicheren Identitätsnachweis, womit sich NutzerInnen eindeutig identifizieren können. Eine mögliche Weiterentwicklung ist ein digitaler Führerschein oder Personalausweis (PwC 2016: 9). „Bitnation“, ein schwedisches Unternehmen, speichert öffentliche Verwaltungsvorgänge, wie zum Beispiel Versicherungen oder Urkunden, auf einer Blockchain – auch Eheschließungen über Bitnation werden seit 2015 offiziell anerkannt. Möglich sind auch elektronische Wahlen, da die Blockchain als manipulationsicher gilt – auch wenn in Deutschland noch ein großer Vorbehalt gegenüber digitalen Wahlprozessen herrscht (Simmchen 2017). In Großbritannien wurde ein Pilotprojekt initiiert, bei dem mithilfe der Blockchain Sozialhilfeleistungen nachvollziehbar und vom Staat einsehbar sind. Relativ zahlreich sind Projekte rund um den Herkunftsnachweis von Kunstgegenständen und Diamanten oder die Sicherung von geistigem Eigentum. Einige MusikerInnen bieten ihre Musik nur noch über Plattformen an, die auf der Blockchain basieren, um Raubkopien ihrer Kunst zu verhindern (vgl. Ujo Music 2017). Auch die Vereinten Nationen nutzen bereits die Blockchain – etwa in Projekten, über die die Essensausgabe in Geflüchtetenlagern in Jordanien organisiert wird (FAZ 2017).

Unterschiedliche BetrachterInnen werden zu anderen Einschätzungen kommen, welche der oben genannten Blockchain-Anwendungen sinnvoll und wünschenswert sind. Klar wird jedoch, dass es an Einsatzmöglichkeiten nicht mangelt und der Blockchain nicht umsonst das Potential zugesprochen wird, bestehende Organisationsformen und Märkte disruptiv zu verändern.

3 Relevanz für die Energiewende

3.1 Die deutsche Energielandschaft

Mit der Energiewende stehen Gesellschaft, Politik und Wirtschaft vor neuen Herausforderungen. Während die Energiewende prinzipiell – wie Meinungsumfragen immer wieder zeigen – national nach wie vor eine sehr große Akzeptanz hat und auch international oft als Erfolgsgeschichte gefeiert wird, gibt es auch Kritik aus verschiedenen Reihen. Während kaum jemand die Energiewende prinzipiell infrage stellt, geht es den einen zu langsam, den anderen zu schnell. Auf der einen Seite steht die große Zahl an BefürworterInnen der Energiewende, aus deren Sicht der Ausbau der Erneuerbaren Energien in Deutschland zu langsam voranschreitet. Argumente sind hier etwa, dass die Emissionen in Deutschland nicht ausreichend sinken, um die deutschen Klimaziele oder gar die noch ambitionierteren Ziele des völkerrechtlich verbindlichen Paris-Abkommens zu erreichen. So stieg der Anteil der Erneuerbaren Energien am Bruttostromverbrauch von 2015 auf 2016 – allerdings auch durch ein relativ schlechtes Wind- und Sonnenjahr – um lediglich 0,2 Prozentpunkte an und liegt 2016 bei 31,7 % – eine Entwicklung, die das Umweltbundesamt als „nur mäßig“ bezeichnet (Umweltbundesamt 2017a). Auf der anderen Seite stehen diejenigen unter den Energiekonzernen, deren Kerngeschäft immer noch in der Produktion von „brauner Energie“ besteht, sowie geringer werdende Teile der Industrie. Auch BürgerInnen, die zwar vermehrt, aber immer noch unzureichend in den Diskurs eingebunden werden, verschaffen sich verstärkt Gehör: So fordern auf der einen Seite viele die möglichst zügige Abschaltung aller Kohlekraftwerke, während andere den Ausbau von Windparks verhindern oder den Ausstieg aus der Kohle verlangsamen wollen.

Der Übertragungsnetzausbau geht zwar beschleunigt, aber immer noch schleppend voran und dem fluktuierenden Angebot elektrischer Energie aus erneuerbaren Quellen muss auch mit neuen Formen des Managements begegnet werden. Eine der Hauptaufgaben wird es sein, die Netze derart umzugestalten, dass eine zunehmende Anzahl von Privathaushalten mit einer geringen installierten Erzeugungsleistung ins System integriert werden kann. Inzwischen gibt es in Deutschland mehr als 1,5 Millionen Solaranlagen, etwa 27.000 Windkraftwerke und ca. 9.000 Biogasanlagen, die ins öffentliche Stromnetz einspeisen (Agora Energiewende 2017: 19). Dies erfordert einen Umbau der Netze, der dem Trend der dezentralen und regionalen Stromerzeugung Rechnung trägt.

Sowohl sozio-politische als auch physische Strukturen beeinflussen die Standortwahl von Erneuerbare-Energien-Anlagen. Dabei spielen die Verfügbarkeit von Sonne und Wind und auch eine Reihe von anderen Faktoren wie Einwohnerdichte, Wirtschaftsentwicklung einzelner Gebiete, rechtliche Bestimmungen und schließlich auch die Ausgestaltung des Erneuerbaren-Energie-Gesetzes (EEG) eine Rolle (Ropenus 2017a: 59f.). Zwar korrelieren Standortoptimum und installierte Leistung aus Erneuerbaren, deckungsgleich sind sie jedoch keineswegs.

Dadurch, dass etwa 89 % der Erneuerbare-Energien-Anlagen an das Verteilnetz angeschlossen sind, verändert sich der Stromfluss immer häufiger, was zu einem „Gegenverkehr durch bidirektionale Lastflüsse“ führt (ebd.: 64). Auch entsteht ein erhöhtes Risiko von Netzengpässen bei hoher gleichzeitiger Einspeisung von Erneuerbaren Energien und konventionellen Kraftwerken, denen mit einer Reihe von Instrumenten begegnet werden kann. Besonders relevant sind hierbei aktuell noch die kurzfristigen Redispatch-Maßnahmen und das Einspeisemanagement. Beim Redispatch passen die Übertragungsnetzbetreiber die Einspeisung von konventionellen Kraftwerken an, wobei sich nur die örtliche Verteilung und nicht die Summe der eingespeisten Energie verändert. Zwischen 2010 und 2015 haben sich Redispatch-Eingriffe fast verzehnfacht, was im Jahr 2015 zu

Kosten in Höhe von über 400 Millionen Euro geführt hat (Bundesnetzagentur 2016: 8). 2016/17 haben sie sich allerdings wieder verringert. Im Zuge des Einspeisemanagements werden Erneuerbare-Energien-Anlagen und **KWK-Anlagen** abgeregelt, obwohl grundsätzlich Einspeisevorrang für Erneuerbare Energien gilt. Dies ist kostspielig, weil auch für den nichtgelieferten Strom gezahlt werden muss. Andererseits setzt genau dies – anders als etwa in China, wo eine um eine Größenordnung stärkere Abregelung von erneuerbarem Strom stattfindet – einen starken Anreiz für die Netzbetreiber, möglichst viel erneuerbaren Strom einzuspeisen und in ermöglichende Maßnahmen zu investieren sowie langfristige Handlungsoptionen – wie etwa Power-to-X – voranzubringen.

Ein Großteil der Abregelungen erfolgt im Höchstspannungsnetz. Prinzipiell möglich wäre die Etablierung mehrerer Preiszonen, was einen Anreiz zur Steuerung der zukünftigen Erzeugung und des zukünftigen Verbrauchs schaffen würde. Derzeit bildet Deutschland eine einheitliche Preiszone, in der die Kosten, etwa für den Netzausbau, sozialisiert werden und die tatsächliche physikalische Netzsituation nicht abgebildet wird (Ropenus 2017a: 64; Mengelkamp et al. 2017a: 1). Über die Etablierung einer regionalen Energiemarktstruktur, welche zusätzliche Anreize für den Ausbau von Erneuerbaren schaffen könnte, müsste die Bundespolitik entscheiden (Graichen und Zuber 2017: 88f.). Der zwischen CDU, SPD und CSU verhandelte Koalitionsvertrag spricht sich allerdings dagegen aus. Ein Argument ist, dass sehr kleinteilige Energiesysteme marktwirtschaftlich weniger effizient sind und durch kleine Märkte mit abnehmender Konkurrenz die individuelle Marktmacht von wenigen Energieunternehmen gestärkt werden könnte. Auch ist zu berücksichtigen, dass eine Etablierung von verschiedenen Preiszonen sozial unerwünschte Effekte haben könnte, da sich wohlhabende Privathaushalte oder die Industrie in Regionen mit niedrigen Stromkosten niederlassen könnten. Nicht zuletzt könnten die Regionen zu Verlierern der Energiewende werden, welche ein geringes Potential an besonders günstigen Erneuerbaren Energien – insb. der Windkraft – haben (z. B. Bayern).

VerbraucherInnen kritisieren zunehmend erhöhte Strompreise, welche auch durch Industrieausnahmen beim EEG verursacht werden. Während etwa in China Unternehmen die Stromkosten für VerbraucherInnen subventionieren, subventionieren in Deutschland die EinzelverbraucherInnen die Stromkosten der energieintensiven Industrie. Wird erneuerbarer Strom über das EEG vermarktet, verliert er seine Grünstromeigenschaft. So soll eine doppelte Vermarktung verhindert werden. Demgegenüber gibt es jedoch Regionalnachweise, die Strom aus der Region kennzeichnen und die Akzeptanz für die Energiewende vor Ort erhöhen können (Graichen und Zuber 2017: 89).

Letztlich ist der Stromsektor jedoch nur ein Teil der Energiewende, der allerdings bislang die größte mediale Aufmerksamkeit für sich beansprucht. Für das Gelingen der Energiewende muss es eine ausgeklügelte Sektorenkopplung geben, also eine enge Verflechtung der Bereiche Strom, Wärme, Industrie und Mobilität. Hierbei geht es um eine Elektrifizierung von Wärme, Industrie und Mobilität mit Strom aus Erneuerbaren Energien. Als Instrumente zur Erreichung dieser sowie zur Vermeidung von Netzengpässen werden Smart Grids immer wieder diskutiert (vgl. Kapitel 1.2 sowie Ropenus 2017b: 101).

3.2 Anwendungsmöglichkeiten der Blockchain in der Energiewirtschaft

Im Gegensatz zum Finanzsektor sind viele Aktionen im Bereich der Energiewirtschaft an eine physische Infrastruktur gebunden, wie zum Beispiel Stromnetze. Es geht um mehr als die Speicherung von Daten und den Transfer von Geld.

Bereiche der Energiewirtschaft, in denen Blockchain-Technologien prinzipiell eine Rolle spielen können:

- Handel mit Erneuerbaren Energien
- Handel mit Gas und Fernwärme
- Messdienstleistungen
- Ablese- und Abrechnungsverfahren
- Transaktionen rund um die Netze
- Dokumentation von Anlagezuständen
- Handel mit CO₂- und Ökostromzertifikaten
- Lade- und Abrechnungsverfahren für Elektromobilität
- Smart Home-Anwendungen
- Bezahlssysteme basierend auf Kryptowährungen

Abbildung 6: Bereiche der Energiewirtschaft, in denen Blockchain-Technologien prinzipiell eine Rolle spielen können¹⁵

Bislang waren insbesondere die kleineren Energieunternehmen bei neuen Technologietrends in Bezug auf Blockchain-Projekte eher zurückhaltend, da neue Technologien höchste Sicherheits- und Performanceanforderungen erfüllen müssen, um etwaige Blackouts zu vermeiden (Krauskopf 2017: 20). Die größeren und alteingesessenen Unternehmen initiieren hingegen schon etwas länger eigene Blockchain-Projekte und das „vielversprechende Potential der Technologie droht dadurch in alten Strukturen unterzugehen“ (Hesse 2017a). Hesse, Geschäftsführer von Grid Singularity und Entwickler einer Plattform für den Austausch dezentraler Energiedaten, rechnet für 2018 dennoch mit 200 bis 400 neuen Startups, die an einer Anwendung der Blockchain im Energiesektor interessiert sind.

3.2.1 Pilotprojekt: Brooklyn Microgrid

Microgrids können in einer zunehmend dezentralen Energieversorgung eine wichtige Rolle spielen. Sie umfassen in der Regel eine kleinere Gruppe von EnergieversorgerInnen und VerbraucherInnen, die z. T. auch Prosumer sein können, also sowohl Strom erzeugen als auch verbrauchen. Microgrids können die Zuverlässigkeit der Stromversorgung erhöhen, indem sie im Falle eines Blackouts des übergeordneten Netzes VerbraucherInnen weiterhin mit lokal erzeugtem Strom versorgen (Mengelkamp et al. 2017a: 2). Sie funktionieren also sowohl in Anbindung an das übergeordnete Netz als auch – zumindest für begrenzte Zeit – im „island-mode“, als in sich geschlossene und autarke Inseln. Kennzeichnend für Microgrids ist eine hohe Anzahl an kleineren EnergieerzeugerInnen mit einer installierten Leistung von unter 200 kW, was in der Regel größtenteils

¹⁵ Quelle: vgl. Sieverding und Schneidewindt 2016: 2ff. sowie PwC 2016: 16ff.

SolaranlagenbesitzerInnen sind. Der erzeugte Strom wird dann entweder selbst verbraucht oder von KonsumentInnen abgenommen, die sich in unmittelbarer geografischer Nähe befinden. Nach Graichen und Zuber (2017) gilt Strom dann als regional, wenn „der Letztverbraucher aus Anlagen beliefert wird, die sich im Umkreis von 50 Kilometern um das Postleitzahlengebiet des Verbrauchers befinden“ (S. 89).

Die Integration von Blockchain-Technologien ermöglicht den Stromhandel für sehr kleine Netze ab zwei AkteurInnen sowie die kosteneffiziente Abwicklung des Verkaufs. Das erste und berühmteste Projekt weltweit für eine Blockchain-Anwendung im Stromnetz ist das Brooklyn Microgrid Project (BMG), welches Peer-to-Peer-Energietransaktionen (P2P) abwickelt. Es wird vom Start-Up LO3 Energy, einem Technologieberatungsunternehmen, in New York durchgeführt.

In Brooklyn gibt es ein physisches Microgrid, über welches Strom verteilt wird, sowie ein virtuelles Microgrid, welches die verschiedenen Mitglieder des Netzwerks über ein Informationssystem verbindet. Das physische Netz ist über eine geringe Anzahl von Verbindungsstellen an das übergeordnete Netz gekoppelt, sodass es sich im Notfall – wie im Falle eines Stromausfalls im übergeordneten Netz – von diesem abkoppeln kann. Gleichzeitig bietet diese Kopplung Versorgungssicherheit für das Microgrid, wenn es im Grid selbst zu Problemen kommen sollte. Sowohl Stromerzeugung als auch -nachfrage werden automatisch über installierte Smart Meter gemessen. Auf Basis dieser Informationen werden individuelle Prognosen für jedes Mitglied erstellt, Überschussnachfrage oder -angebot berechnet und an alle Blockchain-AkteurInnen geschickt (Mengelkamp et al. 2017b: 3). Jeder Haushalt verfügt über einen persönlichen Account, der sowohl Informationen über Energieverbrauch oder -erzeugung (und ggf. in Zukunft verstärkt auch Speicherung) als auch über den (finanziellen) Kontostand beinhaltet. Es kann jederzeit Girogeld auf den persönlichen Account überwiesen und auch von diesem wieder entnommen werden, vorausgesetzt der Kontostand erlaubt die Durchführung angekündigter Transaktionen.

Der Handel mit Strom wird über ein Auktionssystem durchgeführt, indem Kauf- und Verkaufsaufträge eingereicht werden. KonsumentInnen geben ihr maximales Preislimit für ihre präferierte Energiequelle an und Prosumer den Minimalpreis, zu dem sie ihren Strom im Microgrid verkaufen wollen. Daraufhin funktioniert die Verteilung nach dem Merit-Order-Prinzip: der Höchstbietende wird zuerst versorgt, darauf folgt der Zweithöchstbietende, usw. Das letzte Gebot entspricht dem **market-clearing-price** für das konkrete Zeitfenster. Wer nach diesem Verteilmechanismus nicht mit Strom versorgt wird, wird im BMG mit Strom aus zusätzlichen Energiequellen wie etwa fossilen Brennstoffen versorgt (Mengelkamp et al. 2017a: 7). In einem System mit ausreichender Erneuerbaren- sowie Netz- und Speicherkapazität ließe sich der Bedarf fossiler Brennstoffe dabei minimieren.

Der gesamte lokale Handel geschieht zunächst nur virtuell. Die Geldmengen, die im Rahmen der Auktion geboten werden, gehen vom Konto der kaufenden Person ab und werden zunächst als Pfand einbehalten. Die Blockchain dient quasi als Treuhänderin, um die Abwicklung von zukünftigen Transaktionen zu gewährleisten. Nach jedem Clearing werden über die Blockchain Informationen über die zusammengeführten Angebots- und Nachfrage-Mengen von Strom sowie den Marktpreis an alle beteiligten AkteurInnen gesendet. Die Zahlungen werden über Smart Contracts automatisch ausgeführt und die Pfand-Gelder freigegeben.

Das Ziel dieses „Energy Management Trading Systems“ (EMTS) ist es, die Energieversorgung automatisch zu gewährleisten, während gleichzeitig eine spezielle Biet-Strategie (bidding strategy) implementiert wird. Basierend auf den Echtzeit-Daten über Nachfrage und Erzeugung (sowie perspektivisch Speicherung) wird eine individuelle Prognose erstellt und eine dazugehörige bidding strategy entwickelt. Ein simples EMTS würde zum Beispiel immer dann Strom kaufen, wenn die Preise unter das festgelegte Preislimit fallen. Eine Weiterentwicklung des EMTS erlaubt auch die

Berücksichtigung sozio-ökonomischer Faktoren wie beispielsweise einer Präferenz für Strom aus Erneuerbaren Energien. Um den Handel mit Strom zu automatisieren, muss das EMTS Zugang zu den Accounts der Teilnehmenden haben, woraufhin es Gebote auf Basis der individuellen Nutzenfunktionen abgibt (Mengelkamp et al. 2017a: 5). Dies ist jedoch nicht essentiell für das Funktionieren des Marktes.

Mithilfe von Blockchain-Anwendungen im Microgrid können Nachbarschaften selbst über die Zusammensetzung ihres Stroms entscheiden und diese beeinflussen. Im konkreten Fall wurde eine benutzerfreundliche und kostenlose App entwickelt, die verschiedene Szenarien modelliert und zunächst unverbindlich ausprobiert werden konnte. Mittlerweile reichen die Funktionen weiter, sodass AnwohnerInnen beispielsweise gemeinsam abstimmen können, wo demnächst eine weitere PV-Anlage installiert werden soll. Die BMG App dient auch als Informationsmedium, in dem aktuelle Projekte beschrieben und Erzeugungsprofile aktualisiert werden (Brooklyn Microgrid 2017).

Im Fall des Brooklyn Microgrids wurden innerhalb der dreimonatigen Testphase die Marktmechanismen kaum genutzt und nur ein Konsument und ein Prosumer handelten mit Strom. Zudem war der Strompreis von vornherein auf den traditionellen Preis für Erneuerbare Energien in Brooklyn fixiert. Mittlerweile wurde die Technologie jedoch weiterentwickelt und ist nach Aussage des Entwicklers Scott Kessler von LO3 Energy ausgereift. Es fehle lediglich an neuen Geschäftsmodellen und einem begünstigenden regulatorischen Rahmen (Kessler 2017).

Ein wesentlicher Vorteil der Blockchain in diesem Zusammenhang besteht, wenn sie lokale Preissignale gibt, die die wetterabhängige Verfügbarkeit von Strom repräsentieren. Dies kann sowohl den Stromverbrauch und die Kosten für VerbraucherInnen senken, als auch Anreize schaffen, in für das System wichtige Erneuerbare Energien zu investieren. Die lokalen Preissignale werden kombiniert mit den jeweiligen Zahlungsbereitschaften von StromkundInnen und smarte Haushaltsgeräte können – unter Berücksichtigung von NachfragerInnenbedürfnissen – beim Erreichen von zuvor definierten Preisober- oder Untergrenzen ab- oder zugeschaltet werden. Während es im Vergleich zu der konventionellen Stromversorgung mehr Transparenz gibt, wird die Privatsphäre dadurch geschützt, dass nur die an einer Transaktion Beteiligten die Daten dieser einsehen können – zumindest solange sie die Daten nicht weitergeben. LO3 gibt an, jegliche Art von smarten Geräten in das virtuelle Netz integrieren zu können, sodass auch der Stromverbrauch von Elektroautos oder Industriemaschinen über die Blockchain abgerechnet werden kann (ebd.).

Wesentlich hinsichtlich des Nutzens für die Energiewende ist in diesem Zusammenhang, dass die Anwendung verspricht, automatisch, schnell und zu sehr geringen Transaktionskosten erneuerbar erzeugten Strom dahin zu leiten, wo er am ehesten benötigt oder am effizientesten verwendet werden kann. So können beispielsweise im Falle einer drohenden Überlastung der Stromnetze mit entsprechenden Preisanreizen Elektro-Tankstellen oder Wärmepumpen bedient werden. Die erneuerbare Stromerzeugung muss dann nicht gedrosselt werden. Auf der anderen Seite würde vor allem dann Strom getankt, wenn geringe Nachfrage besteht, aber viel erneuerbarer Strom zur Verfügung steht. Auf diese Weise lässt sich erneuerbarer Überschussstrom volkswirtschaftlich effizient nutzen. Unterm Strich lässt sich so mehr erneuerbar erzeugter Strom nutzen, sodass weniger Strom konventionell erzeugt werden muss.

3.2.2 Weitere Projekte im Energiesektor

Nachdem Brooklyn zu einer Art Pilgerstätte für innovative Energie-Start-ups und Blockchain-EnthusiastInnen wurde, folgten weltweit ähnliche Projekte, die oft auf Microgrid-Ebene durchgeführt und über die Blockchain abgewickelt wurden.

In Deutschland kooperieren zum Beispiel TenneT, einer der vier Übertragungsnetzbetreiber aus Nordwest- bis Südost-Deutschland mit Sonnen, einem Heimspeicherhersteller aus dem Oberallgäu. Dabei werden dezentrale Batteriespeicher in das Netz integriert und es wurde mithilfe der Blockchain erstmals ein Heimspeicher für Redispatch-Maßnahmen genutzt. Die Pilotphase startete im November 2017 und soll sechs Monate andauern (TenneT 2017). Die Situation im Netz bestimmt das Management der untereinander vernetzten Speicher. So können Transportengpässe im Netz vermieden werden, indem Batteriespeicher Strom ins Netz abgeben. Anders herum kann das Speichernetzwerk in Sekundenschnelle überschüssigen Strom aufnehmen (ebd.). Redispatch-Maßnahmen sind kostspielig und insbesondere das Abregeln von Windkraftanlagen kostet den Netzbetreiber jährlich mehrere Millionen Euro (Enkhardt 2017). Speicher können dabei kurzfristige Schwankungen im Stromnetz ausgleichen und Produktionsspitzen auffangen, wie etwa bei starkem Wind. Ein weiteres Kostensenkungspotenzial ergibt sich unter Umständen dadurch, dass weniger Übertragungsnetzausbau erforderlich sein könnte, da über die Speicher ein Puffer geschaffen wird.

Anlagen könnten dabei mithilfe der Blockchain dezentral oder auch überregional gesteuert werden. BesitzerInnen von Speichern profitieren von deren Bereitstellung insofern, als dass sie mit Strom zu Grenzkosten nahe Null entlohnt werden. Die anderen VerbraucherInnen müssen perspektivisch weniger für Netzentgelte zahlen, da Redispatch-Maßnahmen seltener werden. Noch werden konventionelle Kraftwerke von Übertragungsnetzbetreibern gezielt angefragt, wenn sie ihre Leistung erhöhen sollen, um Angebot und Nachfrage zu balancieren. Werden Großkraftwerke im Zuge der Klimapolitik abgeschaltet, so ist eine mögliche Strategie, Kapazitäten von kleineren Anlagen zu integrieren. Aufgrund der hohen Anzahl an Erneuerbare-Energien-Anlagen bietet die Blockchain über eine Automatisierung eine schnelle und reibungslose Abwicklung dieser Flexibilitätensbereitstellung. Ob die Blockchain zu den postulierten Zielen beitragen kann und es eine skalierbare Lösung gibt, soll in der Pilotphase des TenneT/Sonnen-Projektes untersucht werden.

Die Wuppertaler Stadtwerke starteten Ende 2017 zusammen mit der Energiehändlerin Axpo einen Blockchain-Handelsplatz für Erneuerbare-Energien-Strom. Hier können KundInnen selbst ihren Stromerzeuger auswählen. Diese wiederum profitieren von einer erhöhten Zahlungsbereitschaft, die besonders dann relevant wird, wenn ab 2020 für viele Windräder die EEG-Förderung ausläuft und die Vermarktungserlöse unter Umständen nicht ausreichen, um die Betriebskosten zu decken (Wuppertaler Stadtwerke 2017). Mit der Blockchain wird verhindert, dass eine Kilowattstunde Strom doppelt verkauft wird. So wird Transparenz in den Verrechnungsdaten geschaffen. Die Aufgabe der Stadtwerke ist es dann lediglich noch, Formalitäten wie die Abrechnung zu erledigen (Flauger 2017).

Grid Singularity, ein Unternehmen aus Österreich, bietet eine Plattform für DApps an, über die NetzbetreiberInnen, EnergieerzeugerInnen, RegulatorInnen und KonsumentInnen miteinander verbunden und so alle Stufen der Wertschöpfungskette bedient werden (Grid Singularity 2017).

Wie die Einbindung von Blockchain-Technologien in Stromnetze und eine dezentrale Energieversorgung aussehen kann, wird in der Studie von PwC (2017) bildlich dargestellt. Auffällig ist eine Zentralisierung im linken Szenario, welches die heutige Situation abbildet. Ebenso ins Auge fällt die Reduktion der Anzahl an beteiligten AkteurInnen durch eine Blockchain-Einbindung (vgl. rechte Seite).

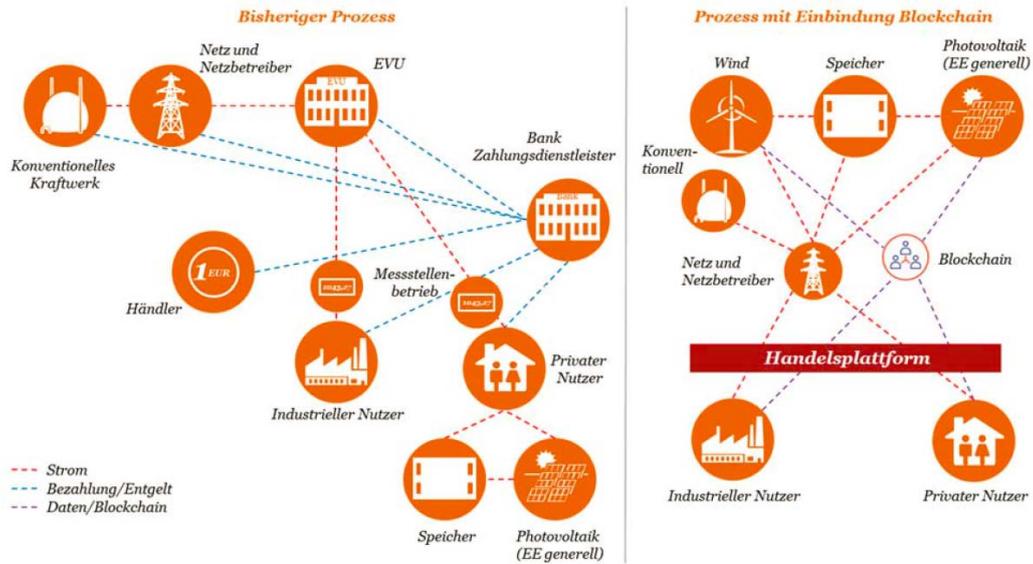


Abbildung 7: Verschiebung der Marktstruktur durch Einführung des dezentralen Transaktionsmodells¹⁶

Slock.it, ein deutsches Start-up, bietet in Zusammenarbeit mit RWE Ladestationen für Elektroautos an, welche automatisch an diesen Ladestationen aufgeladen werden. Dabei kann ein Auto geparkt werden und die/der BesitzerIn einkaufen gehen, während sich das Auto automatisch an einer Station einloggt, auflädt und automatisiert über die Blockchain abrechnet (PwC 2016: 18). Auch das Start-up Motionwerk hat eine App entwickelt, die das Teilen von elektrischen Ladestationen über die Blockchain ermöglicht. Jede/r kann ihre/seine eigene Ladestation registrieren, einen Tarif und Öffnungszeiten festlegen und sie dann mit anderen teilen. Die Blockchain kommt bei der Abrechnung ins Spiel und ermöglicht das Einsehen des auf der Blockchain hinterlegten Zahlungsverlaufs (Kloth 2017a). Bisher gibt es für PrivatbesitzerInnen von Elektroautos, die ihr Fahrzeug mit ihrem Hausstrom aufladen, keine eigenen Tarife. Mithilfe der Blockchain könnten innerhalb des Hausnetzwerks verschiedene Tarife genutzt werden (ebd.; Strom DAO 2017).

Das junge Unternehmen Strom DAO sieht in einem Ausbau von Elektromobilität nicht zwangsläufig eine zusätzliche Netzbelastung. Stattdessen könnten Elektroautos der Fluktuation aus Erneuerbaren sogar ausgleichend entgegenwirken, indem sie vor allem dann geladen werden, wenn viel regionaler Strom aus grünen Quellen zur Verfügung steht. Der Autostromtarif von Strom DAO schafft wirtschaftliche Anreize, indem Prämien von bis zu fünf Cent pro kWh an diejenigen ausgezahlt werden, die ihr Auto zu Zeiten mit einem hohen Angebot an Erneuerbaren Energien laden. Abgewickelt wird dies über die Blockchain.

¹⁶ PwC 2017: 18

4 Chancen und Potenziale

In Kapitel 3.2 bis 3.4 wurden entscheidende Vorteile für die Energiewende in Bezug auf die Anwendung der Blockchain-Technologie bereits erläutert. Darüber hinaus werden im Folgenden weitere wichtige Chancen und Potentiale Blockchain-basierter Technologien im Energiesektor in den Blick genommen.

Blockchain-Anwendungen bieten sowohl Potenzial im Bereich der Prozessanwendungen, in welchen Effizienzverbesserungen erreicht werden können, als auch im Bereich der disruptiven Anwendungsfälle, durch die neue Märkte entstehen (Interview 1). Das Revolutionäre an der Blockchain ist, dass Intermediäre verschiedener Branchen durch die Blockchain überflüssig werden und zugleich im Sinne der schöpferischen Zerstörung (Schumpeter) neue Geschäftsmodelle entstehen können.

4.1 Systemintegrität und Ersetzen von Intermediären

In der Theorie kann jede zentrale Instanz Registereinträge abändern oder die Durchführung von Transaktionen verweigern. In demokratischen Rechtsstaaten mag dieses Problem nicht sehr akut sein – dennoch können zentral abgelegte Daten gehackt werden oder in die Hände undemokratischer Parteien oder Personen gelangen. Eine Software, die alle Personen gleich behandelt und die nur die Kohärenz des Systems interessiert, ist im Gegensatz zu Menschen nicht anfällig für Korruption, Geldhinterziehung oder informelle Absprachen (BlockchainHub 2017, Berentsen und Schär 2017: 43). Zudem ist – zumindest einer libertären Denkschule folgend – fraglich, ob von Eigentum gesprochen werden kann, wenn der Zugriff auf Besitzgüter von der Kooperation einer bestimmten Instanz abhängig ist.

Durch die Blockchain wird die Rolle eines Intermediären nicht etwa vernichtet, sondern durch einen „digital and strictly rule-following middleman“ ersetzt (Drescher 2017: 242). Das Vertrauen gegenüber von Menschen getragenen Organisationen wird nun durch das Vertrauen in eine durch Codes definierte Software ersetzt. Im Energiesektor betrifft dies vor allem Banken, Strom-Börsen, Notariate und MessdienstleisterInnen, aber auch Energieversorger und Netzbetreiber.

Ob und in welchem Umfang durch die Blockchain Arbeitsplätze wegfallen, kann derzeit noch nicht abgesehen werden. Alle Pilotprojekte beinhalten bis dato eine geringe Anzahl von Teilnehmenden und es gibt noch keine Massenanwendungen. Sicherlich gilt, genauso wie beim Streitthema Arbeitsplätze in der Energiewende, dass auch neue Jobs geschaffen werden, die insbesondere auf lokaler Ebene zur regionalen Wertschöpfung beitragen können (Mengelkamp et al. 2017a: 6). Dennoch sollte das Risiko des möglichen Wegfalls von Arbeitsplätzen sehr ernst genommen werden.

4.2 Transparenz

Blockchains gewähren, sofern sie als öffentliche und nicht als private Blockchains ausgestaltet sind, eine hohe Transparenz. Physische Geldeinheiten wie Münzen oder Scheine haben einen hohen Anonymitätsgrad und es gibt meistens keine Aufzeichnungen über ihren aktuellen Verbleib (Berentsen und Schär 2017: 39). Virtuelle Geldeinheiten können dieses Problem lösen, sehen sich aber im Gegenzug mit einem „double-spending“-Problem konfrontiert. Digitale Daten können ohne großen Aufwand kopiert werden. Dieses Kopieren ist das digitale Äquivalent zum Drucken

von Falschgeld. In P2P-Systemen kann dies problematisch werden, etwa wenn es Informationsasymmetrien gibt und jemand sein Eigentum mehr als einmal an eine andere Person überträgt (Drescher 2017: 51f.).

Im Blockchain-System hingegen kann diese Problematik nicht auftreten. Will eine Person Geldeinheiten gleichzeitig an zwei verschiedene Nodes verschicken, werden beide Nachrichten zunächst simultan im Netz verbreitet. Da sich die beiden Nachrichten widersprechen, kann am Ende nur eine Transaktion in einen Block integriert und an die Kette gehängt werden (Berentsen und Schär 2017: 57f.). Auch wenn die hohe Transparenz gelegentlich als der Technologie hinderlich bezeichnet wird (schließlich kann es Daten geben, die nicht öffentlich zugänglich sein sollten), so ist zumindest die Möglichkeit der Offenlegung zuvor auch bewusst geheim gehaltener Daten eine interessante Neuerung.

Auf welche Weise und in welchem Umfang Transparenz eingehalten wird, wird sicherlich von der jeweiligen Ausgestaltung und der Art der Daten in den entsprechenden Branchen abhängen. Dennoch könnten sich hier Chancen beispielsweise für zivilgesellschaftliche Organisationen auftun, die soziale oder ökologische Kriterien wirtschaftlicher Aktivitäten in den Blick nehmen. Auf der anderen Seite ist jedoch auch zu beachten, dass im Darknet viele Geschäfte über die Blockchain abgewickelt werden. Hier zeigt sie sich eher als Unterstützerin der Intransparenz.

Im Energiesektor kann durch Herkunftsnachweise von Grünstrom gesichert werden, dass dieser auch wirklich zu 100 % aus erneuerbaren Energiequellen kommt oder einen bestimmten Anteil an Investitionen in Neuanlagen sicherstellt. Bisher ist es Unternehmen möglich, ihren produzierten Kohlestrom mithilfe von Zertifikaten „grünzuwaschen“. Die Blockchain bietet auch hier Transparenzvorteile, sodass VerbraucherInnen sich sicher sein können, dass es sich bei ihrem Strom um „echten“ Ökostrom handelt (Sieverding und Schneidewindt 2016: 3). Wird die Blockchain in der Energieversorgung eingesetzt, sind entsprechende digitale Messgeräte (Smart Meter) eine wesentliche Voraussetzung (vgl. Kapitel 1.1). Diese können VerbraucherInnen helfen, ihren Stromverbrauch und die entstehenden Kosten nachzuverfolgen (Wiedmaier 2017: 49)¹⁷. Je weniger Intermediäre an einer Transaktion beteiligt sind, desto weniger Schnittstellen zwischen Personen oder Institutionen gibt es, an denen Nachrichten verloren gehen oder verfälscht werden können.

4.3 Effizienzsteigerungen und Kostensenkungspotenziale

Die Blockchain kann Effizienzmaßnahmen ermöglichen und damit Kostensenkungspotentiale realisieren. Sie ist nie offline, über sie können Transaktionen 24 Stunden am Tag und sieben Tage die Woche abgewickelt werden (Drescher 2017: 193). Durch Automatisierung können z. B. Personalkosten eingespart werden. Um derzeit Geld von einem Land in ein anderes zu transferieren, werden bis zu fünf Mittelspersonen beteiligt, von denen jede für die Durchführung ihres Arbeitsschritts Zeit braucht und dafür außerdem meistens eine Gebühr verlangt (Drescher 2017: 21). Ebenso entfallen durch Einsatz der Blockchain Gebühren und Gewinnaufschläge für Unternehmen, die bisher als Intermediäre tätig waren und künftig keine Rolle mehr spielen werden (PwC 2016: 34). Je nach Branche entfallen Kosten für Ablese- und Abrechnungsverfahren, Mahnverfahren

¹⁷ Risiken und Chancen des sogenannten „Roll-outs“ von Smart Metern können überblicksartig in Mielke/Zimmermann et al. (2016: 22-29) nachgelesen werden.

ren, Inkassoverfahren, einen über Banken abgewickelten Zahlungsverkehr, Vertragsschließung oder Zertifizierungen (ebd.; Sieverding und Schneidewindt 2016: 2).

Für Unternehmen der Energiebranche lassen sich vielfältige Einsatzmöglichkeiten der Blockchain und damit auch vielfältige Einsparpotenziale finden. Die Blockchain hat das Potential, ein effizientes Datenmanagement-System zu sein, über das Transaktionen einfach abgewickelt werden können. Prozesskosten können eingespart und interne Verrechnungsprozesse einfach abgebildet werden (Interview 2). Eine Finanzierung kann etwa über Initial Coin Offerings durchgeführt werden, sodass geringe bis keine Kapitalkosten entstehen.

StromerzeugerInnen können in regionalen Energiegenossenschaften ihren Strom direkt an EndverbraucherInnen vermarkten und durch eine erhöhte Zahlungsbereitschaft für regionale Produkte gegebenenfalls höhere Margen erzielen (Wuppertaler Stadtwerke 2017), was insbesondere in Anbetracht auslaufender EEG-Förderung relevant werden kann. Auch kleinere ErzeugerInnen können ihren Strom profitabel verkaufen, da über die Blockchain auch geringe Mengen an Strom gehandelt werden können (Mengelkamp 2017a: 3). Lokaler Stromhandel über die Blockchain führt in Microgrids dazu, dass der generierte Profit in der Community bleibt, regionale Wertschöpfung erlaubt und etwa in zusätzliche erneuerbare Stromerzeugung reinvestiert werden kann (ebd.: 2).

Die Auswirkungen der Kostensenkungspotenziale auf die Verbrauchenden im Energiemarkt lässt sich noch nicht genau abschätzen. Derzeitige Abschätzungen besagen, dass es sich nicht um signifikante Summen handeln wird, aber durchaus Einsparpotenzial existiert (Sieverding und Schneidewindt 2016: 2). Da sich der Strompreis für Haushalte zum Großteil aus Steuern und Abgaben zusammensetzt (ca. 54 %), bleiben in der ökonomischen Sphäre noch die beiden Hebel Netzentgelte (ca. 24 %) und Einkauf und Vertrieb (ca. 21 %) (dena 2016: 25).

Zwar könnte möglicherweise durch dezentrale Microgrids, in denen Haushalte untereinander mit Strom handeln, der Bedarf an teuren Übertragungsnetzen leicht verringert werden. Gleichzeitig entstehen jedoch zusätzliche Kosten für den Ausbau vieler dezentraler Anlagen, Verteilnetze und Speichertechnologien – sowie zusätzliche Stromkosten.

Wie groß das Sparpotenzial im Bereich Einkauf und Vertrieb ist, wird davon abhängen, wie hoch die Gewinnmargen der Blockchain-Anbieter sein werden. Zwar handelt es sich bei der Blockchain um eine open-source-Technologie, jedoch gibt es keine dezentralen Benutzeroberflächen. Zumindest in den nächsten Jahren werden StromkundInnen auf die Expertise vermittelnder Unternehmen angewiesen sein, die Abrechnungen und Formalien für sie erledigen.

Nichtsdestotrotz kann eine zunehmende Dezentralisierung auch mit einer weiter zunehmenden Unabhängigkeit der Prosumer von marktdominierenden Energiekonzernen einhergehen. Mehr Wettbewerb auf dem Energiemarkt kann dann zu Preissenkungen führen. Durch Automatisierung mithilfe von Blockchain-Anwendungen würde es zudem einfacher werden, den individuellen Konsum zu steuern und den Stromverbrauch an variable Preise anzupassen, wodurch Kostensenkungen erzielt werden können (Wiedmaier 2017: 50). Hierbei liegt das wesentliche Kostensenkungspotential im verstärkten Einsatz Erneuerbarer Energien, die zu Grenzkosten nahe Null Strom erzeugen können. Zu obiger Diskussion sei einschränkend zu erwähnen, dass Einsparpotenziale nur dann relevant werden können, wenn die IT-Infrastruktur mit digitalen und smarten Geräten bereits besteht und mit einem minimalen Kostenaufwand genutzt werden kann (dena 2016: 23).

Zu der Frage, ob Blockchain-Technologien ein Erfolgsfaktor für die Energiewende werden können, gibt es keine eindeutige Antwort, aber immerhin ein paar Indizien. Im System einiger Kryptowährungen (zum Beispiel SolarCoin) werden Prosumer für die Installation von Erneuerbaren-Energien-Anlagen in der jeweiligen Währung entlohnt. Dies kann es zunehmend attraktiver machen, eine PV-Anlage zu installieren (Wiedmaier 2017: 49). Die Blockchain-Technologie kann dabei helfen, den

Ausbau dezentraler Energiesysteme zu fördern (Interview 1). Einige AutorInnen sehen in dieser Dezentralisierung auch ein nicht unwesentliches Demokratisierungspotential, da Dezentralisierungsprozesse zur Beteiligung und individuellen Teilhabe der VerbraucherInnen am Energiemarkt einladen (z. B. Rifkin 2015).

5 Risiken und Schwachstellen

In Kapitel 1 wurde bereits auf die Gefahr der Entsolidarisierung von Wohlhabenden im Rahmen von Smart Grids – insbesondere wenn wirklich eine volle Autarkie angestrebt wird – hingewiesen. Darüber hinaus werden im Folgenden weitere entscheidende Risiken und Schwachstellen blockchain-basierter Technologien im Energiesektor in den Blick genommen.

5.1 Energieintensität

In den letzten Wochen des Jahres 2017 bekam der Vorwurf, Kryptowährungen wie Bitcoin seien "Stromfresser" (Frankfurter Rundschau 2017) und „bedrohen die globale Energiewende“ (Spiegel Online 2017a), eine breite mediale Aufmerksamkeit. Im Zuge eines "Bitcoin-Hypes" (Süddeutsche Zeitung 2017), ausgelöst durch einen rasanten Preisanstieg der digitalen Währung, wurde der Energieverbrauch des Miner-Netzwerks genauer unter die Lupe genommen.

Der Ökonom Alex de Vries, der auf seiner Seite Digiconomist.net verschiedene Szenarien modelliert und schon vor Jahren den immensen Stromverbrauch Bitcoins und später Ethereum's anprangerte, schätzt die gesamte jährliche Energienachfrage des Bitcoin-Rechnernetzwerks auf 32,68 TWh – das ist mehr, als Länder wie Bahrain oder Irland in einem Jahr an Strom nutzen. Eine vierköpfige Familie aus Deutschland nutzt im Jahr etwa 0,000004 TWh Strom (Pannewick und Herbst 2017). Bricht man den Gesamtverbrauch von Bitcoin auf eine Transaktion herunter, liegt der Stromverbrauch bei 235 KWh, was genug wäre, um eine Energiesparlampe über 20.000 Stunden leuchten zu lassen. Der Rechenaufwand, der für den Kauf einer Tasse Tee aufgebracht werden muss, steht in einem klaren Missverhältnis zu den 2,00 Euro, die für das Heißgetränk mit Bitcoins bezahlt werden. Den Berechnungen von de Vries liegen die Annahmen zugrunde, dass Miner etwa 60 % ihrer Einnahmen für Energiekosten ausgeben und unterschiedlich leistungsstarke Hardware benutzen.

Während Marc Bevand die Berechnungen von de Vries kritisiert und als Gesamtstromverbrauch für Bitcoin eine Zahl zwischen 4,12 und 4,73 TWh pro Jahr errechnete, verweisen Medienportale wie ARD oder Spiegel Online auf die Berechnungen des Digiconomist.

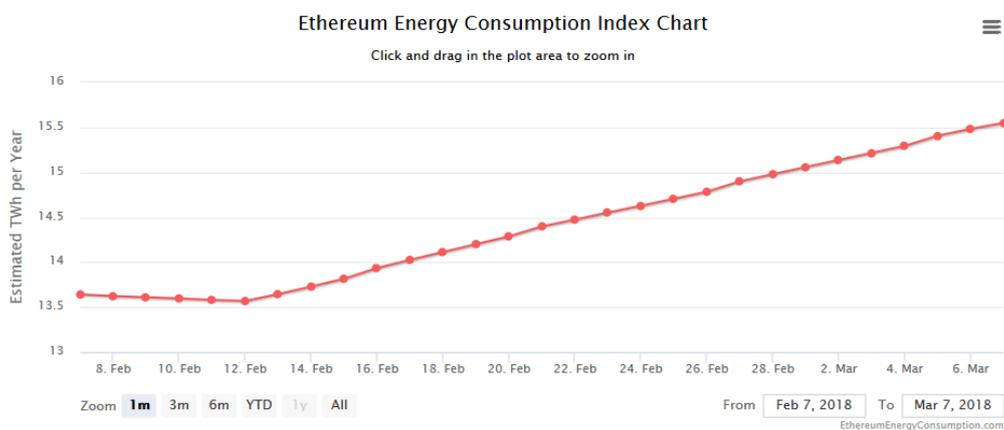


Abbildung 8: Anstieg des Stromverbrauchs von Bitcoin von Anfang Februar bis Anfang März 2018¹⁸

¹⁸ <https://cloud.highcharts.com/embed/ywoqita/> (abgerufen am 12.12.2017)

Dieser hat auch für Ethereum Berechnungen durchgeführt. Ethereum ist zwar weder als gesamtes Netzwerk noch pro Transaktion so energieintensiv wie Bitcoin, es verbraucht aber immer noch ein Vielfaches an Strom beispielsweise einer VISA-Transaktion. Pro Transaktion wird demnach etwa ein Viertel des Bitcoin-Energieverbrauchs fällig.

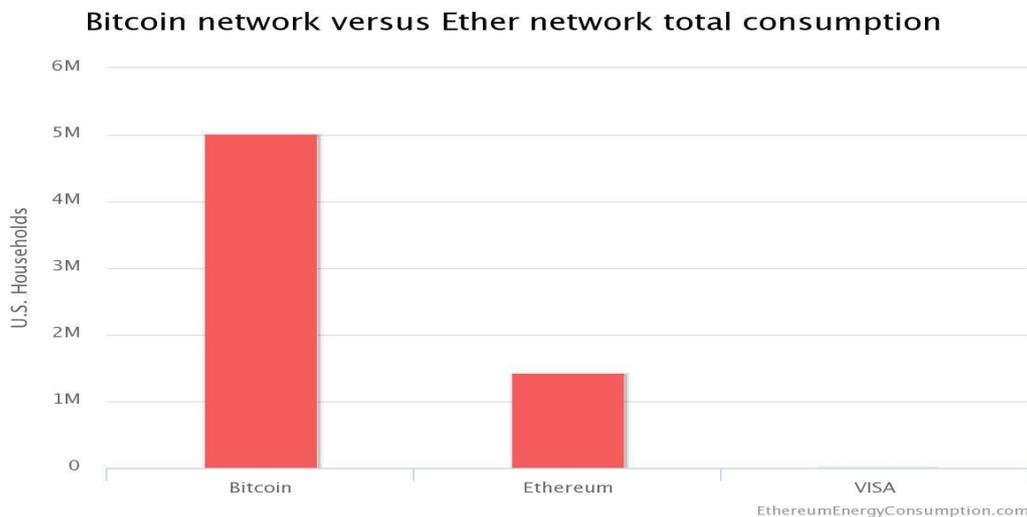


Abbildung 9: Gesamter Stromverbrauch des Bitcoin-, Ethereum- und VISA- Netzwerks pro Jahr in Relation zum Stromverbrauch eines durchschnittlichen US-Haushalts (der Betrieb von Banken wird bei der Untersuchung des VISA Netzwerks nicht berücksichtigt)¹⁹

Je nachdem, in welchem Land Coins geschürft werden, fällt eine erhebliche Menge an CO₂ an. Ein Mining Standort in der Mongolei, der seinen Strom von einem Kohlekraftwerk bezieht, setzt bis zu 13.000 kg CO₂ pro geschürftem Bitcoin frei. Das können bis zu 40.000 kg CO₂ pro Stunde sein (Malmo 2017a). Im deutschen Strommix würde ein Gesamtstromverbrauch von etwa 30 TWh eine Freisetzung von über 15 Tonnen CO₂ bedeuten. Um dieselbe Menge an CO₂ mit einem Mittelklassewagen auszustoßen, müsste man über 2,1 Millionen Mal die Erde umrunden (Pannewick und Herbst 2017).

Problematisch ist, dass der Wechselkurs einer Kryptowährung und die Menge an Elektrizität, die aufgebracht wird, um Tokens zu minen, proportional zueinander sind (Malmo 2017a). Je höher der Wechselkurs ist, desto eher lohnt es sich für Personen, dem Netzwerk beizutreten und im Mining-Wettkampf zu partizipieren. Durch ein vergrößertes Netzwerk steigt auch der gesamte Energieverbrauch.

Letztendlich lässt sich der gesamte Stromverbrauch nicht auf die Megawattstunde genau berechnen. Er ist abhängig von der Effizienz der verwendeten Hardware. Die Klimaschädlichkeit wiederum ist abhängig von der regionalen Verfügbarkeit von grünem oder braunem Strom. Zudem gibt es, ganz im Sinne eines dezentralen und demokratischen Netzwerks, kein Register, in dem aufgeführt wird, wie viele Nodes mit welcher Rechenleistung zum System beitragen (Malmo 2017a). Die Berechnungen von de Vries sind also nicht absolut exakt, aber es steht außer Frage, dass die derzeitige Energieintensität der Bitcoin- und Ethereum-Netzwerke nicht mit einer emissionsarmen

¹⁹ <https://digiconomist.net/ethereum-energy-consumption> (abgerufen am 12.12.2017)

Zukunft vereinbar ist – schon gar nicht, wenn zukünftig nicht 350.000²⁰, sondern Millionen von Transaktionen pro Tag über verschiedene Blockchains abgewickelt werden.

Das Problem der Energieintensität ist den ProgrammiererInnen und EntwicklerInnen durchaus bewusst. Das Umstellen der proof-of-work- auf die proof-of-stake-Konsensmethode würde den Stromverbrauch drastisch verringern. Er würde dadurch sehr gering (Digiconomist 2017). Allerdings erfüllt die proof-of-stake-Methode nicht die gleichen Sicherheitsanforderungen (vgl. Kapitel 2.2). Kombinationen von proof-of-work und proof-of-stake können perspektivisch die Vorteile beider Methoden erfüllen und den Energieverbrauch senken. So arbeitet Ethereum derzeit an „Casper“, einer dieser Kombinationen, welche auf komplexen mathematischen Eigenschaften beruht. Auch wenn die Implementierung von Casper relativ einfach wäre, ist es bislang noch nicht tauglich für eine breite Anwendung, denn „Casper remains imperfect“ (Buterin und Griffith 2017: 9).

Die oben genannten Kritikpunkte an den beiden Systemen Bitcoin und Ethereum sind repräsentativ für fast alle Blockchain-Systeme. Es gibt einzelne Unternehmen, die Side Chains benutzen, welche aus nur wenigen Rechnern bestehen und in regelmäßigen Abständen einen Abgleich zur großen Ethereum-Blockchain durchführen, wodurch der Stromverbrauch gesenkt wird (Interview 1). Solange es einen Link zur Haupt-Blockchain gibt, erfüllt eine **Side Chain** die notwendigen Sicherheitsanforderungen. Mithilfe von **Relay Chains** können verschiedene Blockchains miteinander verknüpft werden, sodass zum Beispiel die Nutzung einer Ethereum DApp mit Bitcoins bezahlt werden kann (BTC Relay 2017). Hierbei wird mit einzelnen Informationen aus einem Block und nicht mehr gesamten Blöcken gearbeitet, wodurch das Volumen und der damit einhergehende Stromverbrauch gesenkt werden.

Offensichtlich ist jedenfalls, dass die Blockchain nur bei einer entsprechenden Weiterentwicklung eine konstruktive Rolle im Rahmen einer globalen Energiewende spielen kann.

5.2 Unveränderlichkeit /Trägheit und kritische Größe für Sicherheit

Zwar werden Blockchain-Technologien oft als revolutionär und disruptiv bezeichnet, jedoch gelingt die Integration von Fortschritten ins System zumindest bei öffentlichen Blockchains meist nur sehr langsam. Private Blockchains können täglich modifiziert werden, da die EntwicklerInnen sämtliche Entscheidungen alleine und beliebig treffen können. Bei öffentlichen Blockchains gibt es jedoch keine feste Prozedur, nach der Änderungen an wesentlichen Eigenschaften vorgenommen werden können, sobald sich eine Blockchain erst einmal in Anwendung befindet. Wenn es durch Fehler im Code Sicherheitslücken gibt, stellt dies aufgrund der Unveränderlichkeit der Blockchain eine große Herausforderung dar (Drescher 2017: 208).

Auch eine Ausweitung der Anwendungsmöglichkeiten oder das Aufkommen neuer Technologien kann eine Anpassung wünschenswert machen (Berentsen und Schär 2017: 72). Derzeit können Verbesserungsvorschläge durch alle Personen im Netzwerk vorgebracht werden, welche dann öffentlich in Foren oder über Mailing-Listen diskutiert werden. Wenn für einen Vorschlag kein eindeutiger Konsens erreicht wird, kann eine explizite Abstimmung durchgeführt werden, bei der Anträge mit einer Zustimmung von 55 %, 75 % oder 95 % angenommen werden (ebd.: 73). Das Stimmrecht bemisst sich auf Grundlage der Allokation der Rechenleistung.

²⁰ Für die aktuelle Anzahl an Transaktionen pro Tag der Bitcoin Blockchain vgl. Blockchain.info, <https://blockchain.info/de/charts/n-transactions> (abgerufen am 14.12.2017).

Diese Form der Entscheidungsfindung ist zeitintensiv und es ist fraglich, ob alle Miner über die erforderliche Expertise verfügen, zukünftige Entwicklungen zu antizipieren und im Interesse des Netzwerks abzustimmen. Kritisiert wird außerdem, dass der Entscheidungsprozess von nur einer einzigen Anspruchsgruppe, den Minern, dominiert wird. Andere Stakeholder wie KonsumentInnen und HändlerInnen haben kein Abstimmungsrecht, obwohl sie ein Interesse am Fortbestand des Netzwerks haben. Sie können sich jedoch aktiv an Diskussionen beteiligen und den Entwicklungsprozess gegebenenfalls so beeinflussen. Letztendlich haben jedoch auch Miner, die bei Abstimmungen Vorteile für sich bewirken könnten, Interesse an einer hohen Glaubwürdigkeit ihrer Währung (ebd.: 76).

In kleinen Netzwerken ist die Wahrscheinlichkeit höher, dass schnell ein Konsens erreicht wird, da weniger Nodes in Diskussionen um mögliche Änderungen einbezogen werden müssen. Andererseits ist essentiell, dass das Netzwerk eine kritische Größe erreicht und hält. In einem System von 10 Nodes können leicht die Hälfte dieser gehackt werden. Ein System muss so groß sein, dass 51 %-Attacken unmöglich sind²¹ (Drescher 2017: 209). Obwohl Bitcoin eines der größeren Netzwerke ist, wird es selbst dort als kritisch betrachtet, dass die Zahl der Nodes zwischen 2013 und 2015 von 15.500 auf 5.500 Nodes sank (Berentsen und Schär 2017: 102). Wer mehr Kapital hat, kann regelmäßiger in neue Hardware investieren, wodurch kleinere und ineffizientere Miner vom Markt gedrängt werden. Bildet sich ein oligopolistischer Markt heraus, kann eine kleine Gruppe von Minern ihre Macht missbrauchen und das Weiterleiten von Informationen unterlassen oder andere Nodes bewusst diskriminieren (Drescher 2017: 208).

5.3 Skalierbarkeit und Sicherheit

Viele der täglich über eine Blockchain durchgeführten Transaktionen sind Finanztransaktionen, welche im Vergleich zu bisherigen Überweisungen relativ schnell abgewickelt werden können. Auch wenn das Geld schneller am Zielort ankommt, können jedoch nur sieben Transaktionen pro Sekunde über Bitcoin initiiert werden, während es über 50.000 über VISA sind (PwC 2016: 11). Für die meisten Anwendungen im Energiesektor sind bestehende Blockchain-Typen ebenfalls zu langsam (Hesse 2017a). Das Ziel Ethereums ist es, innerhalb von zwei Jahren eine Millionen Transaktionen pro Sekunde möglich zu machen, also zu skalieren (ebd.). Ob dies realistisch ist, können jedoch selbst die EntwicklerInnen nicht einschätzen. Viele Unternehmen, die derzeit mit Blockchain-Anwendungen experimentieren, arbeiten entweder über die Ethereum-Blockchain oder haben ein eigenes Netzwerk aufgebaut. Dieses besteht zumeist aus einer Handvoll von Nodes, weshalb selbst bei erfolgreicher Anwendung oft nicht auf ein Funktionieren im vielschichtigen und umfangreichen Kerngeschäft geschlossen werden kann.

Die nächsten zwei bis drei Jahre sollen als Testfeld dienen, um die Technologie zu verstehen und mögliche Kinderkrankheiten zu identifizieren. Viele der Unternehmen wissen noch nicht, ob die Blockchain die erwünschten Erfolge bringt und ob die Technologie nur unterstützend am Rande oder zentral zum Einsatz kommt. Fest steht aber, dass ProgrammiererInnen weltweit an Prototypen arbeiten, die die Skalierbarkeit erhöhen, die Sicherheit gewährleisten und Auswirkungen auf ökologische sowie soziale Bedingungen berücksichtigen sollen.

²¹ Angriffe können auch von Minern durchgeführt werden, die über weniger als 51 % der Rechenleistung verfügen. Allerdings ist die Wahrscheinlichkeit gering, dass eine solche Manipulation gelingt. Und selbst bei einem erfolgreichen Eingriff sind die Möglichkeiten der angreifenden Miner beschränkt: Es können im schlimmsten Fall Transaktionen umgekehrt oder es kann verhindert werden, dass bestimmte Transaktionen der Blockchain hinzugefügt werden (Berentsen und Schär 2017: 235).

Die Blockchain ist ebenfalls ungeeignet, eine große Masse an Daten zu speichern. Transaktionsdaten werden möglichst schlank gehalten, um die Verbreitung von Nachrichten nicht durch zu große Mengen an Informationen zu verlangsamen. Im Beispiel eines dezentralen P2P-Stromhandels bedeutet dies, dass nur Transaktionsdaten auf der Blockchain gespeichert werden und nicht etwa individuelle und mehrmals täglich erfasste Verbrauchsdaten oder Erzeugungsdaten.

Um von den Vorteilen der Transparenz und der Manipulationssicherheit profitieren zu können, müssen Lösungen in Form von Regeln, Geräten und Geschäftsmodellen gefunden werden, die den Übergang von Daten eines bestimmten Geräts auf die Blockchain sicher machen. Selbst angenommen es besteht kein Zweifel an der Sicherheit und Unveränderbarkeit der Daten, sobald diese auf der Blockchain sind, so gibt es die Gefahr, dass Informationen unmittelbar davor, bei ihrem „entry point“ manipuliert werden. Um dieses sogenannte „Oracle-Problem“ zu lösen, arbeiten einige Unternehmen an sicheren Lösungen, im Energiebereich zum Beispiel an Zählerdaten-Validierung an der Schnittstelle zwischen Smart Metern und der Blockchain (Interview 1). Es müssen sichere Geräte für Übergabepunkte entwickelt werden, was insbesondere in Anbetracht der sich in den Kinderschuhen befindenden Blockchain-Technologie eine große Herausforderung darstellt.

6 Zusammenfassung der Chancen und Potenziale, Risiken und Schwachpunkte

| Chancen und Potenziale – allgemein | Risiken und Schwachpunkte – allgemein |
|--|---|
| <ul style="list-style-type: none"> - Ersetzen der Intermediäre - Einsparung von Intermediärskosten (Personal, Mahnverfahren, etc.) - nicht korrumpierbar - Informationssymmetrie - kein initiales Vertrauen zwischen Vertragsparteien notwendig - Transparenz & Rückverfolgbarkeit - Unveränderlichkeit von Daten und Verträgen - Entscheidungen werden auf Basis von Daten getroffen - Zahlungsausfallrisiken werden gesenkt - Automatisierung von Prozessen - Demokratisierungspotential - resistent gegenüber Hacker-Angriffen - neue Geschäftsmodelle entstehen - Unternehmen benötigen weniger Startkapital - Umgehen des double-spending-Problems - dauernde Verfügbarkeit | <ul style="list-style-type: none"> - mangelhafte Geschwindigkeit und Skalierbarkeit - zunehmende Zentralisierung durch Mining-Pools - oligopolistische Mining-Märkte - kritische Größe muss erreicht werden - enorme Energieintensität - kaum eingängige Benutzeroberflächen - Akzeptanz fraglich, da Funktionsweise abstrakt - Machtkonzentration durch wenige EntwicklerInnen - regulatorischer Rahmen unklar - private Blockchains verletzen ursprüngliche Attribute - Wegfall von Arbeitsplätzen? - Balancierung von Transparenz und Anonymität - AnsprechpartnerInnen fallen weg - schwer zu identifizierende Sicherheitslücken - Trägheit und langsame Entscheidungsfindung - Oracle-Problem (Manipulation vor dem „entry point“) - ungeeignet für die Speicherung einer Vielzahl von Daten - geringe Partizipationsmöglichkeiten für Personen ohne Internetzugang oder Smartphone - „Unbarmherzigkeit“, da durch feste Regeln keine Ausnahmen gemacht werden können - Datenmissbrauch bei privaten Blockchains (360° Bilder von KundInnen) - langsame Integration von Fortschritten |
| Chancen und Potenziale – Energiesektor | Risiken und Schwachpunkte – Energiesektor |
| <ul style="list-style-type: none"> - transparentes Verbrauchsverhalten - Effizienzreize - bessere Ressourcenauslastung - sinkende Stromkosten, preisdifferenzierte Modelle | <ul style="list-style-type: none"> - erhöhter Energieverbrauch durch mehr smarte Geräte - enorme Energieintensität der Technologie - Kosten für Bereitstellung digitaler Infrastruktur - Vertrauen in Blockchain-Dienstleister zunächst nötig |

| | |
|---|---|
| <ul style="list-style-type: none">- Anreize, Erneuerbare-Energien-Anlagen zu installieren- regionale Stromversorgung stärkt Akzeptanz ggü. Energiewende und fördert Gemeinschaft- Demokratisierung im Energiesystem- Marktmachtverringering- Stromhandel mit geringen Mengen lukrativ- Enabler für Demand Side Management- Sicherung Herkunftsnachweise Grünstromzertifikate- Förderung der Sektorenkopplung- Bezahlssysteme über Kryptowährungen- Konkurrenz zu zentralisierten P2P-Netzwerken- möglicherweise verringerter Übertragungsnetzausbaubedarf | <ul style="list-style-type: none">- Transaktionsgeschwindigkeit zu gering- Machtkonzentration durch private Blockchains- sich verändernde Rollen mit neuen Aufgaben- oft geringe IT-Expertise bei Marktteilnehmenden- Entsolidarisierung bzgl. Netzkosten |
|---|---|

Abbildung 10: Chancen und Potentiale, Risiken und Schwachpunkte der Blockchain²²

²² Quelle: Eigene Darstellung

7 Fazit und Ausblick

Die Blockchain wird mit einer hohen Wahrscheinlichkeit Prozesse und Geschäftsmodelle verändern, offen ist, in welchem Ausmaß. Sie ändert auch die Akteursrollen, was wir beispielhaft in der Energiewirtschaft sehen können: KonsumentInnen werden zu Prosumern. Die Rollen von Verteil- und Übertragungsnetzbetreibern verändern sich. Energieunternehmen werden künftig verstärkt Dienstleistungen anbieten (z. B. Blockchain as a Service, BaaS). Die Digitalisierung verschafft VerbraucherInnen eine neue Möglichkeit zur Partizipation. Und Start-ups bieten völlig neue Chancen im P2P-Handel an.

Für die Energiewirtschaft kann die Anwendung von Blockchain-Technologien interessant sein. Dies sollte in den Zielsetzungen der Bundesregierung zur Digitalisierung der Energiewirtschaft berücksichtigt werden. Die Politik sollte Rahmenbedingungen schaffen, welche die in dieser Studie dargelegten Chancen und Potentiale der Blockchain heben hilft und zugleich die Risiken und Schwachpunkte in angemessener Weise adressiert. Es ist dann an den Unternehmen, diese Balance zwischen Potentialen und Risiken umzusetzen und an der Zivilgesellschaft als Frühwarnsystem für verbleibende Risiken zu fungieren. Sie kann im Diskurs mit Wirtschaft und Politik wichtige Hinweise geben.

Zentral für einen erfolversprechenden Einsatz im Rahmen der Energiewende ist, dass die Technologieentwicklung das Problem der Energieintensität in den Griff bekommt. Außerdem muss die Versorgungssicherheit im Energiesystem auf gleichem Niveau erhalten bleiben, auch wenn sich Verantwortlichkeiten ändern (Sieverding und Schneidewindt 2016: 4). Kostensenkungspotenziale sollten vor allem den VerbraucherInnen zu Gute kommen. Auch muss sichergestellt werden, dass es sich bei der Blockchain um eine partizipative Technologie handelt, von der auch technische Laien profitieren können. Von überzogenen Hoffnungen in die Blockchain mit Bezug zum Energiesektor raten wir zumindest kurzfristig ab, da sie mit den Worten Wiedmaiers (2017) zunächst mehr als „complementary technology, not a substitute“ anzusehen ist (S. 54). Die Blockchain kann die Energietransformation beschleunigen, jedoch keine nachhaltige Energiepolitik ersetzen.

Ein Knackpunkt, der weniger mit den technologischen Grenzen zu tun hat als mit den durch die Blockchain entstehenden Organisationsstrukturen, ist der mangelhafte Regulierungsrahmen. Wer wird in einem dezentralen System ohne hierarchische Struktur verantwortlich gemacht, wenn es zu Komplikationen oder Betrug kommt? Dass Rechtssicherheit durch den Konsens der Mehrheit geschaffen wird, ist nach Auffassung von Scholtka und Martin (2017) „für Juristen zunächst eine schwer nachvollziehbare und ungenügende Prüfungsgrundlage, erscheint hier eine eindeutige Zuordnung von Verantwortlichkeiten doch zumindest fraglich“ (S. 114). Eventuell könnten Versicherungslösungen eine Rolle spielen, im Zuge derer die Versicherungsprämie auf alle AkteurInnen umgelegt wird. Es muss also gelöst werden, wie die Blockchain-Technologie in das bestehende Regelwerk integriert werden kann. Hierbei muss auch die Frage gestellt werden, wie sich Smart Contracts mit rechtsgültigen Verträgen kombinieren lassen.

Als das Internet entwickelt wurde, hat nur eine geringe Anzahl von EnthusiastInnen an eine Durchsetzung der Technologie geglaubt. Wahrscheinlich hätten selbst sie sich nicht vorstellen können, was innerhalb von 30 Jahren alles möglich geworden ist. Es ist durchaus denkbar, dass es sich in Bezug auf die Blockchain-Technologie ähnlich verhalten könnte. Wir sehen bereits jetzt erste Erfolge in der Anwendung. Eigenschaften wie Dezentralität, Kryptographie und konsensbasierte Entscheidungsfindung bieten klare Vorteile zu anderen etablierten Technologien.

Letztendlich sollte die Blockchain nicht um jeden Preis oder aus „Peer Pressure“ (dena 2016: 32) zur Anwendung kommen. Es mag Bereiche geben, in denen bestehende Lösungen schneller, so-

zialer, ökologischer und schließlich insgesamt sinnvoller sind. In welchen Einsatzmöglichkeiten welcher Branchen Blockchains einen Mehrwert bieten können, wird sich zeigen. Es kann sinnvoll sein, sich am Forschungs- und Entwicklungsprozess früh zu beteiligen, um technologische Verbesserungen nicht zu verschlafen. Es könnte auch für die Bundesregierung eine Chance sein, Verwaltungsprozesse auf die Blockchain zu verlagern, wie es Schweden, die Schweiz und Estland bereits tun. Hier könnten weitere Potenziale erkannt und genutzt werden (Blockchain Bundesverband 2017b).

Es ist jedoch auch nicht auszuschließen, dass sich der Wirbel um Blockchains als haltlos erweist und dass nach dem „Peak of Inflated Expectations“ die Phase des „Trough of Disillusionment“ folgt (vgl. Gartner 2016). Ebenso kann sich am Ende eine dezentrale Technologie durchsetzen, die im Sinne eines funktionalen Äquivalents viele, aber nicht alle der Eigenschaften der Blockchain aufweist und auch nicht mehr unter diesem Namen firmiert. Entscheidend sollten letztlich neben der ökonomischen Tragfähigkeit der soziale und ökologische Nutzen der Anwendungen sein. Hierauf sollten deshalb Wirtschaft, Politik und Zivilgesellschaft ihr Augenmerk legen und die neuesten Entwicklungen im Kontext der in dieser Studie diskutierten – und möglicherweise neuer zu Tage tretender – Chancen und Risiken stets neu bewerten und adressieren.

Referenzen

Quellen

Amelang, Sören (2017): The Digitalisation of the Energiewende. Digitalisation Ignites New Phase in Energy Transition, [online]

www.cleanenergywire.org/dossiers/digitalisation-energiewende (abgerufen am 26.10.2017).

BaFin (2016): „Distributed Ledger - Die Technologie hinter den Distributed Ledger: Die Technologie hinter den virtuellen Währungen am Beispiel der Blockchain“. [online]

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2016/fa_bj_1602_blockchain.html (abgerufen am 23.02.2018).

BDEW (2017): Was bedeutet die Digitalisierung für die Energiewirtschaft?, [online]

www.bdew.de/energie/digitalisierung/was-bedeutet-der-trend-der-digitalisierung-fuer-die-energiewirtschaft/ (abgerufen am 20.12.2017).

Berentsen, Aleksander und Schär, Fabian (2017): Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung. Books on Demand, Norderstedt.

Bevand, Marc (2017): Electricity Consumption of Bitcoin: a Market-Based and Technical Analysis, [online]

<http://blog.zorinaq.com/bitcoin-electricity-consumption/> (abgerufen am 12.12.2017).

Bitcoin Generator (2017): Ethereum generieren - verdienen - oder kaufen, [online]

<http://bitcoin-generator.de/ethereum-kaufen-mining-investieren> (abgerufen am 24.10.2017).

Bitcoinchain Homepage (2017): [online] <https://bitcoinchain.com/> (abgerufen am 11.12.2017).

Blockchain Bundesverband (2017b): Kernforderungen Blockchain Bundesverband e.V. (i.Gr.), [online]

<https://drive.google.com/file/d/0B4RX0v7k6Ttu4WGtZMVJoa0NIXzA/view> (abgerufen am 26.10.2017).

Blockchain Bundesverband (2017c): Blockchain. Chancen und Herausforderungen einer neuen digitalen Infrastruktur für Deutschland, [online]

http://bundesblock.de/wp-content/uploads/2017/10/bundesblock_positionspapier_v1.1.pdf (abgerufen am 20.12.2017).

Blockchain Bundesverband Homepage (2017a): [online] <http://bundesblock.de/> (abgerufen am 27.10.2017).

Blockchain.info Homepage (2017): [online] <https://blockchain.info/de/charts> (abgerufen am 14.12.2017).

BlockchainHub Homepage: [online] <https://blockchainhub.net/> (abgerufen am 16.11.2017).

BMBF (Bundesministerium für Bildung und Forschung) (2017): Kopernikus-Projekt P2X, [online]

<https://www.kopernikus-projekte.de/projekte/power-to-x> (abgerufen am 12.12.2017).

Brooklyn Microgrid Homepage: [online] <https://www.brooklyn.energy/> (abgerufen am 30.10.2017).

BTC Relay Homepage (2017): [online] <http://btcrelay.org/> (abgerufen am 13.12.2017).

Bundesministerium für Wirtschaft und Energie (2017a): Die Digitalisierung der Energiewende, [online] <https://www.bmwi.de/Redaktion/DE/Artikel/Energie/digitalisierung-der-energiewende.html> (abgerufen am 24.10.2017).

Bundesministerium für Wirtschaft und Energie (2017b): Erneuerbare Energien, [online] <https://www.bmwi.de/Redaktion/DE/Dossier/erneuerbare-energien.html> (abgerufen am 20.12.2017).

Bundesnetzagentur (2016): 3.Quartalsbericht 2015 zu Netz- und Systemsicherheitsmaßnahmen. Viertes Quartal 2015 sowie Gesamtjahresbetrachtung 2015. Bonn. https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/Publikationen/Berichte/2016/Quartalsbericht_Q4_2015.pdf?__blob=publicationFile&v=1 (abgerufen am 09.12.2017).

Bundesnetzagentur (2017): Moderne Messeinrichtungen und intelligente Messsysteme, [online] https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Verbraucher/NetzanschlussUndMessung/SmartMetering/SmartMeter_node.html (abgerufen am 25.10.2017).

Buterin, Vitalik (2014): DAOs, DACs, DAs and More: An Incomplete Terminology Guide, [online] <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/> (abgerufen am 27.10.2017).

Buterin, Vitalik und Griffith, Virgil (2017): Casper the Friendly Finality Gadget, [online] http://517shangke.com/static/file/4236615_qq_com_1505925043620719.pdf (abgerufen am 12.12.2017).

Cao, Shuyan, Yanan Cao, Xiaoyu Wang, Yangjiao Lu (2017): A Review of Researches on Blockchain. *WHICEB 2017 Proceedings* 57.

Chuen, David LEE Kuo und Deng, Robert H. (2017): Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1. Cryptocurrency, FinTech, InsurTech and Regulation, Nikki Levy (Hrsg.), Elsevier, London.

Dena (Deutsche Energie Agentur) (2017): Demand Side Management. Stromnachfrage gezielt steuern, [online] <https://www.dena.de/themen-projekte/energiesysteme/flexibilitaet-und-speicher/demand-side-management/> (abgerufen am 12.12.2017).

Dena (Deutsche Energie-Agentur) (2016): Blockchain in der Energiewende. Eine Umfrage unter Führungskräften der deutschen Energiewirtschaft. Berlin.

Die Zeit (2017): China. Kontrolle über alles. [online] www.zeit.de/politik/ausland/2015-07/china-plangesellschaft-xi-jinping (abgerufen am 01.01.2018).

Digiconomist (2018a): Bitcoin Energy Consumption Index, [online] <https://digiconomist.net/bitcoin-energy-consumption> (abgerufen am 08.03.2018).

Digiconomist (2018b): Ethereum Energy Consumption Index, [online] <https://digiconomist.net/ethereum-energy-consumption> (abgerufen am 08.03.2018).

Don Tapscott (2016): Wie die Blockchain Geld und die Geschäftswelt verändert, [Video] https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business?language=de#t-35401 (abgerufen am 26.10.2017).

Drescher, Daniel (2017): Blockchain Basics. A Non-Technical Introduction in 25 Steps. Apress. Frankfurt am Main.

- Energieagentur NRW (2017): Power-to-X, [online] www.energieagentur.nrw/tool/sektorenkopplung/information/power-to-x.php (abgerufen am 12.12.2017).
- Enkhardt, Sandra (2017): Tennet und Sonnen starten Blockchain-Projekt zur Netzstabilisierung. *pv magazine*, [online] www.pv-magazine.de/2017/11/02/tennet-und-sonnen-starten-blockchain-projekt-zur-netzstabilisierung/ (abgerufen am 11.12.2017).
- enviaM (2017): Digitalisierung in der Energiewirtschaft, [online] www.enviam-gruppe.de/energiezukunft-ostdeutschland/energie-fakten/digitalisierung-in-der-energiewirtschaft (abgerufen am 20.12.2017).
- FAZ (2017): Supermarkt in Jordanien : Wo Flüchtlinge mit einem Augenblick bezahlen, [online] www.faz.net/aktuell/finanzen/digital-bezahlen/jordanien-iris-scan-und-blockchain-bei-fluechtlingen-15306863.html (abgerufen am 14.12.2017).
- Finanzen.net (2018a): Bitcoin - Euro, [online] www.finanzen.net/devisen/bitcoin-euro/chart (abgerufen am 08.03.2018).
- Finanzen.net (2018b): Ether - Euro, [online] www.finanzen.net/devisen/ethereum-euro-kurs (abgerufen am 08.03.2018).
- Finley, Klingt (2016): A \$50 Million Hack Just Showed That the DAO Was All Too Human, [online] www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ (abgerufen am 09.12.2017).
- Flauger, Jürgen (2017): Wuppertaler Stadtwerke. "Ökostrom direkt vom Erzeuger", [online] www.handelsblatt.com/unternehmen/energie/wuppertaler-stadtwerke-oekostrom-direkt-vom-erzeuger/20599886.html (abgerufen am 11.12.2017).
- Wille, Joachim (2017): Stromfresser Bitcoin. Frankfurter Rundschau, [online] www.fr.de/wirtschaft/bitcoin-stromfresser-bitcoin-a-1399284 (abgerufen am 12.12.2017).
- Gabler Wirtschaftslexikon (2017): Prinzipal-Agent-Theorie, [online] <http://wirtschaftslexikon.gabler.de/Archiv/924/prinzipal-agent-theorie-v9.html> (abgerufen am 12.12.2017).
- Gartner (2016): Gartner's 2016 Hype Cycle for Emerging Technologies Identifies Three Key Trends That Organizations Must Track to Gain Competitive Advantage, [online] www.gartner.com/newsroom/id/3412017 (abgerufen am 14.12.2017).
- Graichen, Patrick und Zuber, Fabian (2017): Regionale Grünstromvermarktung. In: Energiewende und Dezentralität. Zu den Grundlagen einer politisierten Debatte. Agora Energiewende, Berlin.
- Grid Singularity Homepage (2017): [online] <http://gridsingularity.com/#/0/1> (abgerufen am 11.12.2017).
- Hertig, Alyssa (o.J.): What Is a DAO?, [online] www.coindesk.com/information/what-is-a-dao-ethereum/ (abgerufen am 27.10.2017).
- Hesse, Ewald (2017a): Rettet die Blockchain-Revolution für die Energiewende. Hintergrundgespräch. Interview vom 12.01.2017 von Stiftung Neue Verantwortung, [online] www.stiftung-nv.de/de/veranstaltung/blockchain-revolution-f%C3%BCr-die-energie-wende-hintergrundgespr%C3%A4ch-ewald-hesse (abgerufen am 08.12.2017).
- Hesse, Ewald (2017b): Ewald Hesse, Geschäftsführer bei Grid Singularity, am 10. Industriekongress, [Video] www.youtube.com/watch?v=0Y7UU12JR8I (abgerufen am 08.12.2017).

Kaulartz, Markus (2016): Die Blockchain Technologie. Hintergründe zur Distributed Ledger Technology und zu Blockchains. *Computer und Recht*, 32 (7), S. 474-480.

Kessler, Scott (2017): LO3 Energy's Brooklyn Microgrid Challenges Energy Markets. Interview with The Green Revolution Show, [Video] www.youtube.com/watch?v=A_4XR5E8C5k (abgerufen am 11.12.2017).

King, Sunny und Nadal, Scott (2012): Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper*. Online verfügbar unter: peerco.in/assets/paper/peercoin-paper.pdf (abgerufen am 06.03.18).

Kloth, Carsten (2017a): Mit der Blockchain über die Grenze. Bizz Energy, [online] http://bizz-energy.com/mit_der_blockchain_ueber_die_grenze (abgerufen am 16.11.2017).

Kloth, Carsten (2017b): Strom DAO - Blockchain-Start-up erlaubt Blick in die Energie-Zukunft. Bizz Energy, [online] http://bizzenergytoday.com/blockchain_startup_blick_energiezukunft (abgerufen am 16.11.2017).

Krauskopf, Sascha (2017): Energieversorger tasten sich an künstliche Intelligenz heran. *e21.digital*, 55/17. Energate Verlag, Essen.

Livingston, David (2017): A Blockchain-Based Energy Future?, [online] <http://carnegieendowment.org/2017/08/31/blockchain-based-energy-future-pub-72973> (abgerufen am 26.10.2017).

Lund, Peter D. et al: Review of energy system flexibility measures to enable high levels of variable renewable electricity. In: *Renewable and Sustainable Energy Reviews* 45, 785–807, 2015.

Malmö, Christopher (2017a): One Bitcoin Transaction Now Uses as Much Energy as Your House in a Week, [online] https://motherboard.vice.com/en_us/article/ywbbpm/bitcoin-mining-electricity-consumption-ethereum-energy-climate-change (abgerufen am 16.11.2017).

Malmö, Christopher (2017b): Ethereum Is Already Using a Small Country's Worth of Electricity, [online] https://motherboard.vice.com/en_us/article/d3zn9a/ethereum-mining-transaction-electricity-consumption-bitcoin (abgerufen am 16.11.2017).

Mengelkamp, Esther, Johannes Gärtner, Kerstin Rock, Scott Kessler, Lawrence Orsini, Christof Weinhardt (2017a): Designing Microgrid Energy Markets. A Case Study: The Brooklyn Microgrid. In: *Applied Energy*.

Mengelkamp, Esther, Benedikt Notheisen, Carolin Beer, David Dauer, Christof Weinhardt (2017b): A Blockchain-Based Smart grid: Towards Sustainable Local Energy Markets. In: *Computer Science - Research and Development*.

Mielke, Jahel, Hendrik Zimmermann, Verena Wolf, Hannah Vermaßen, Nane Retzlaff, Jan Burck und Christoph Bals (2016a): Governance und Geschäftsmodelle für die Transformation: 11 Thesen zur Energiewende. Online verfügbar unter: www.germanwatch.org/de/12815 (abgerufen am 14.12.2017).

Mielke, Jahel, Hendrik Zimmermann, Hannah Vermaßen, Nane Retzlaff, Jan Burck (2016b): Grüner Investitionsschub in Europa: Zwölf Empfehlungen für Green Growth und eine erfolgreiche Energiewende. Online verfügbar unter: www.germanwatch.org/de/13120 (abgerufen am 14.12.2017).

Next Kraftwerke (2016): Flexibilitätsoptionen – Perspektiven für die Energiewende, [online] www.next-kraftwerke.de/energie-blog/flexibilitatsoptionen (abgerufen am 20.12.2017).

- Next Kraftwerke (2017): Was bedeutet Merit-Order?, [online] www.next-kraftwerke.de/wissen/strommarkt/merit-order (abgerufen am 13.12.2017).
- Pannewick, Julia und Herbst, Julian (ARD Börse) (2017): Umweltsünder Bitcoin. So dreckig wie zwei Jahre Berlin, [online] <https://boerse.ard.de/boersenwissen/boersenwissen-fuer-fortgeschrittene/umweltsuender-bitcoin102.html> (abgerufen am 09.12.2017).
- Peters, Peter und Mohr, Niko (2015): Digitalisierung im Energiemarkt: Neue Chancen, neue Herausforderungen. In: *Energiewirtschaftliche Tagesfragen*, 65 (12), S. 8-12.
- PwC (PricewaterhouseCoopers) (2016): Blockchain - Chance für Energieverbraucher? Kurzstudie für die Verbraucherzentrale NRW, Düsseldorf.
- Quartz (2016): Fake news of a fatal car crash wiped out \$4 billion in ethereum's market value yesterday, [online] <https://qz.com/1014559/vitalik-buterin-dead-a-hoax-on-4chan-crashed-ethereums-price/> (abgerufen am 30.10.2017).
- Rifkin, Jeremy (2015): A Smart Green Digital Europe. Herausgeber: The Foundation on Economic Trends, [online] www.qualityoflifeobserver.com/sites/default/files/smart-green-third-industrial-revolution-digital.pdf (abgerufen am 26.10.2017).
- Ropenus, Stephanie (2017a): Regionale Verteilung von Erzeugung und Verbrauch. In: *Energiewende und Dezentralität. Zu den Grundlagen einer politisierten Debatte*. Agora Energiewende, Berlin.
- Ropenus, Stephanie (2017b): Smart Grids und Smart Market. In: *Energiewende und Dezentralität. Zu den Grundlagen einer politisierten Debatte*. Agora Energiewende, Berlin.
- Scholtka, Boris und Martin, Jule (2017): Blockchain - Ein neues Modell für den Strommarkt der Zukunft? *Recht der Energiewirtschaft*, 17 (3), S. 113-119.
- Sieverding, Udo und Schneidewindt, Holger (2016): Blockchain in der Energiewirtschaft. Schöne neue (digitale) Energiewelt für Verbraucher_innen und Prosumer? In: *WISO direkt*. 30/2016. Herausgeber: Friedrich-Ebert-Stiftung.
- Simmchen, Christoph (2017): Blockchain (R)Evolution. Verwendungsmöglichkeiten und Risiken. *MMR 2017* (3), S. 162 - 165.
- Spanheimer, Robert (2017): Energiepolitik. Der Energiewende digital zum Durchbruch verhelfen, [online] <https://digitalwahl.de/bitkom/org/Digitalwahl/Positionen-Was-zu-tun-ist/Positionen/Energiepolitik.html> (abgerufen am 26.10.2017).
- Spiegel Online (2017a): Stromverbrauch für Kryptogeld. Warum der Bitcoin-Boom die globale Energiewende bedroht, [online] www.spiegel.de/wirtschaft/unternehmen/bitcoin-stromverbrauch-bedroht-globale-energiewende-a-1182234.html (abgerufen am 12.12.2017).
- Spiegel Online (2017b): Vor fünf Jahren 1000 Dollar investiert = heute 2.000.000 Dollar, [online] www.spiegel.de/wirtschaft/unternehmen/bitcoin-warum-die-kryptowaehrung-rekorde-feiert-a-1180769.html (abgerufen am 17.12.2017).
- Statista (2017a): Volumen der weltweiten Venture Capital-Investitionen in Blockchain-Technologien von 2012 bis zum 3. Quartal 2016 (in Millionen US-Dollar), [online] <https://de.statista.com/statistik/daten/studie/654326/umfrage/venture-capital-investitionen-in-blockchain-technologien-weltweit/> (abgerufen am 24.10.2017).
- Statista (2017b): Anzahl der sich im Umlauf befindlichen Bitcoins (BTC) von März 2016 bis November 2017 (in Millionen), [online]

<https://de.statista.com/statistik/daten/studie/283301/umfrage/gesamtzahl-der-bitcoins-in-umlauf/> (abgerufen am 09.12.2017).

Statista (2017c): Anzahl der Altcoins weltweit in ausgewählten Monaten von Dezember 2015 bis September 2016, [online] <https://de.statista.com/statistik/daten/studie/660486/umfrage/anzahl-der-altcoins-weltweit/> (abgerufen am 21.12.2017).

Stiftung Neue Verantwortung (2017): Rettet die Blockchain-Revolution für die Energiewende. Hintergrundgespräch mit Ewald Hesse, [online] www.stiftung-nv.de/de/veranstaltung/blockchain-revolution-f%C3%BCr-die-energiewende-hintergrundgespr%C3%A4ch-ewald-hesse (abgerufen am 26.10.2017).

Süddeutsche Zeitung (2017): Das große Glücksspiel mit dem Bitcoin-Hype, [online] www.sueddeutsche.de/wirtschaft/digitalwaehrung-das-grosse-gluecksspiel-mit-dem-bitcoin-hype-1.3773966 (abgerufen am 12.12.2017).

Tapscott, Don (2016): How Blockchains Could Shape the World. Interview by McKinsey & Company. [online] www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world (abgerufen am 07.12.2017).

Tapscott, Don und Tapscott, Alex (2016): Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin Publishing Group.

TenneT (2017): Europaweit erstes Blockchain-Projekt zur Stabilisierung des Stromnetzes startet: TenneT und sonnen erwarten Ergebnisse 2018, [online] www.tennet.eu/de/news/news/europaweit-erstes-blockchain-projekt-zur-stabilisierung-des-stromnetzes-startet-tennet-und-sonnen-e/ (abgerufen am 11.12.2017).

TenneT (2017): Europe's First Blockchain Project to Stabilize the Power Grid Launches: TenneT and SonnenExpect Results in 2018, [online] www.tennet.eu/news/detail/europes-first-blockchain-project-to-stabilize-the-power-grid-launches-tennet-and-sonnen-expect-res/ (abgerufen am 16.11.2017).

Ujo Music Homepage (2017): [online] <https://ujomusic.com/> (abgerufen am 14.12.2017).

Umweltbundesamt (2017a): Erneuerbare Energien in Zahlen, [online] www.umweltbundesamt.de/themen/klima-energie/erneuerbare-energien/erneuerbare-energien-in-zahlen#textpart-1 (abgerufen am 01.11.2017).

Umweltbundesamt (2017b): Kraft-Wärme-Kopplung (KWK), [online] www.umweltbundesamt.de/daten/energie/kraft-waerme-kopplung-kwk (abgerufen am 13.12.2017).

Voshmgir, Shermin (2016): Blockchains, Smart Contracts und das Dezentrale Web. Herausgeber: Hammel, Christian/Technologiestiftung Berlin.

Vranken, Harald (2017): Sustainability of Bitcoin and Blockchains. In: *Current Opinion in Environmental Sustainability*, 28, 1-9.

Wiedmaier, Maximilian (2017): The Role of Blockchain Technology and Energy Coalitions in reducing Energy Grid Variability, Masterarbeit im Fach Business Information Management an der Rotterdam School of Management (RSM).

Wilson, Kageni (2017): A layman's guide to blockchains, cryptocurrencies and why they matter, [online] <https://medium.com/@wilsonkageni/understanding-blockchains-cryptocurrencies-why-they-matter-41da50429c43> (abgerufen am 22.10.2017).

Wuppertaler Stadtwerke (2017): Wuppertaler Stadtwerke starten ersten Blockchain-Handelsplatz für Ökostrom, [online] www.wsw-online.de/unternehmen/presse-medien/presseinformationen/pressemeldung/meldung/wuppertaler-stadtwerke-starten-ersten-blockchain-handelsplatz-fuer-oekostrom/ (abgerufen am 11.12.2017).

Zimmermann, Hendrik und Mielke, Jahel (Germanwatch) (2014): Hindernisse für die Energiewende. Online verfügbar unter: www.germanwatch.org/de/download/9555.pdf (abgerufen am 14.12.2017).

Zimmermann, Hendrik und Wolf, Verena (2016): Sechs Thesen zur Digitalisierung der Energiewende: Chancen, Risiken und Entwicklungen. Online verfügbar unter: www.germanwatch.org/de/download/15649.pdf (abgerufen am 14.12.2017).

Interviews

Interview 1:

- Hasberg, Kirsten. Interview am 06.11.2017 in der Factory, Berlin.

Interview 2:

- Burger, Christoph. Interview am 24.11.2017 in der European School of Management and Technology, Berlin.

Sie fanden diese Publikation interessant?

Wir stellen unsere Veröffentlichungen zum Selbstkostenpreis zur Verfügung, zum Teil auch unentgeltlich. Für unsere weitere Arbeit sind wir jedoch auf Spenden und Mitgliedsbeiträge angewiesen.

Spendenkonto: BIC/Swift: BFSWDE33BER, IBAN: DE33 1002 0500 0003 212300

Spenden per SMS: Stichwort „Weitblick“ an 8 11 90 senden und 5 Euro spenden.

Mitgliedschaft: Werden Sie Fördermitglied (Mindestbeitrag 60 Euro/Jahr) oder stimmberechtigtes Mitglied (ab 150 Euro/Jahr, Studierende ab 120 Euro/Jahr) bei Germanwatch. Weitere Informationen und das Anmeldeformular finden Sie auf unserer Website unter:

www.germanwatch.org/de/mitglied-werden

Wir schicken Ihnen das Anmeldeformular auf Anfrage auch gern postalisch zu:
Telefon: 0228/604920, E-Mail: info@germanwatch.org

Germanwatch

„Hinsehen, Analysieren, Einmischen“ – unter diesem Motto engagiert sich Germanwatch für globale Gerechtigkeit und den Erhalt der Lebensgrundlagen und konzentriert sich dabei auf die Politik und Wirtschaft des Nordens mit ihren weltweiten Auswirkungen. Die Lage der besonders benachteiligten Menschen im Süden bildet den Ausgangspunkt unseres Einsatzes für eine nachhaltige Entwicklung.

Unsere Arbeitsschwerpunkte sind Klimaschutz & Anpassung, Welternährung, Unternehmensverantwortung, Bildung für Nachhaltige Entwicklung sowie Finanzierung für Klima & Entwicklung/Ernährung. Zentrale Elemente unserer Arbeitsweise sind der gezielte Dialog mit Politik und Wirtschaft, wissenschaftsbasierte Analysen, Bildungs- und Öffentlichkeitsarbeit sowie Kampagnen.

Germanwatch finanziert sich aus Mitgliedsbeiträgen, Spenden und Zuschüssen der Stiftung Zukunftsfähigkeit sowie aus Projektmitteln öffentlicher und privater Zuschussgeber.

Möchten Sie die Arbeit von Germanwatch unterstützen? Wir sind hierfür auf Spenden und Beiträge von Mitgliedern und Förderern angewiesen. Spenden und Mitgliedsbeiträge sind steuerlich absetzbar.

Bankverbindung / Spendenkonto:

Bank für Sozialwirtschaft AG,
IBAN: DE33 1002 0500 0003 2123 00,
BIC/Swift: BFSWDE33BER

Weitere Informationen erhalten Sie unter **www.germanwatch.org** oder bei einem unserer beiden Büros:

Germanwatch – Büro Bonn

Dr. Werner-Schuster-Haus
Kaiserstr. 201, D-53113 Bonn
Telefon +49 (0)228 / 60492-0, Fax -19

Germanwatch – Büro Berlin

Stresemannstr. 72, D-10963 Berlin
Telefon +49 (0)30 / 2888 356-0, Fax -1

E-Mail: info@germanwatch.org

Internet: www.germanwatch.org



Hinsehen. Analysieren. Einmischen.

Für globale Gerechtigkeit und den Erhalt der Lebensgrundlagen.