Schuster, Philipp; Theissen, Erik; Uhrig-Homburg, Marliese

Article

Finanzwirtschaftliche Anwendungen der Blockchain-Technologie

Schmalenbach Journal of Business Research (SBUR)

Provided in Cooperation with:
Schmalenbach-Gesellschaft für Betriebswirtschaft e.V.

Suggested Citation: Schuster, Philipp; Theissen, Erik; Uhrig-Homburg, Marliese (2020) : Finanzwirtschaftliche Anwendungen der Blockchain-Technologie, Schmalenbach Journal of Business Research (SBUR), ISSN 2366-6153, Springer, Heidelberg, Vol. 72, Iss. 2, pp. 125-147,
https://doi.org/10.1007/s41471-020-00090-5

This Version is available at:
https://hdl.handle.net/10419/286426

Schmalenbachs Z betriebswirtsch Forsch (2020) 72:125–147
https://doi.org/10.1007/s41471-020-00090-5

ORIGINALARTIKEL

Finanzwirtschaftliche Anwendungen der Blockchain-Technologie

Philipp Schuster · Erik Theissen · Marliese Uhrig-Homburg

Eingegangen: 21. März 2020 / Angenommen: 26. Mai 2020 / Online publiziert: 19. Juni 2020

Zusammenfassung Die Blockchain-Technologie wurde 2009 als technologische Basis der Kryptowährung Bitcoin erstmals implementiert. Ihr wird das Potential nachgesagt, eine disruptive Technologie zu sein, die zu nachhaltigen Veränderungen in vielen Bereichen des Wirtschaftslebens führen kann. In diesem Beitrag geben wir einen Überblick über die Technologie selbst sowie ihre finanzwirtschaftlichen Anwendungen. Dabei gehen wir insbesondere auf Kryptowährungen, auf das Potential sogenannter Smart Contracts, auf Initial Coin Offerings, die Abwicklung von Wertpapiergeschäften und mögliche Auswirkungen auf die Corporate Governance börsennotierter Unternehmen ein.

Schlüsselwörter Blockchain · Kryptowährungen · Smart Contracts · Wertpapierabwicklung · Initial Coin Offerings · Corporate Governance

Wir bedanken uns bei Fabian Eska für wertvolle Hinweise. Wir danken der Deutschen Forschungsgemeinschaft für die Finanzierung des Projektes [TH 724/7-1 und UH 107/5-1]. Schuster und Uhrig-Homburg danken außerdem der DZ BANK Stiftung für die Finanzierung des Bloomberg Professional Terminals. Das Papier hat von den Kommentaren und Vorschlägen einer anonymen Gutachterin bzw. eines anonymen Gutachters stark profitiert.

P. Schuster · M. Uhrig-Homburg
Lehrstuhl für Financial Engineering und Derivate, Karlsruher Institut für Technologie, Blücherstr. 17, 76185 Karlsruhe, Deutschland

P. Schuster
E-Mail: philipp.schuster@kit.edu

M. Uhrig-Homburg
E-Mail: uhrig@kit.edu

E. Theissen (✉)
Finance Area, Universität Mannheim, L9 1–2, 68131 Mannheim, Deutschland
E-Mail: theissen@uni-mannheim.de

Centre for Financial Research, Köln, Deutschland

JEL Classifications G19 · G29

Applications of Blockchain Technology in Finance

Abstract The blockchain technology was first implemented in 2009 as the basis of the cryptocurrency Bitcoin. The technology is said to be a disruptive technology that has the potential to significantly affect many areas of the economy. In this paper we provide a survey of the blockchain technology and its applications in finance. We focus on cryptocurrencies, smart contracts, initial coin offerings, the clearing and settlement of transactions in financial markets, and implications for the governance of exchange-listed firms.

Keywords Blockchain · Cryptocurrencies · Smart contracts · Settlement of transactions · Initial coin offerings · Corporate governance

1 Einleitung

Weite Teile der Finanzindustrie sind einem tiefgreifenden Wandel unterworfen. Dazu trägt neben regulatorischen Veränderungen in Folge der Finanzkrise insbesondere die Digitalisierung bei, die bestehende Geschäftsprozesse verändert und den Markteintritt neuer Wettbewerber ermöglicht. Bankgeschäfte werden häufig nicht mehr am Schalter, sondern am Smartphone getätigt und die Anlageberatung wird oft von Computeralgorithmen vorgenommen. Der Wertpapierhandel erfolgt weitgehend elektronisch und wird von High-Frequency Tradern dominiert, d. h. von Computerprogrammen, die Handelsentscheidungen in Sekundenbruchteilen treffen und umsetzen. Crowdfunding-Plattformen treten neben traditionelle Formen der Unternehmensfinanzierung. Ein für die Finanzindustrie potentiell bedeutender Aspekt der Digitalisierung ist die Entwicklung der Blockchain-Technologie vor gut einem Jahrzehnt. In einer Publikation der OECD (OECD 2018) werden verschiedene neue Technologien (wie z. B. Big Data, das Internet der Dinge, Künstliche Intelligenz und andere) daraufhin untersucht, inwieweit sie verschiedene Funktionen und Dienstleistungen des Finanzbereichs (wie etwa den Zahlungsverkehr, Geldanlage, Kreditvergabe und andere) beeinflussen. Die einzige neue Technologie, der ein Einfluss auf *alle* Funktionen und Dienstleistungen attestiert wird, ist die Blockchain-Technologie, mit der wir uns in diesem Beitrag beschäftigen.

Die Blockchain-Technologie liegt der Kryptowährung Bitcoin zugrunde, deren Konzept im Jahre 2008 in einem unter Pseudonym verfassten Beitrag (Nakamoto 2008) vorgestellt wurde.[1] Die Grundidee besteht darin, ein dezentrales Zahlungssystem zu entwerfen, das ohne „vertrauenswürdige Dritte", also Finanzinstitutionen wie Zentral- und Geschäftsbanken, auskommt. Seitdem haben Kryptowährungen die traditionellen Währungen zwar nicht verdrängt, sie haben jedoch erheblich an Bedeu-

[1] Die erstmalige Implementierung erfolgte Anfang Januar 2009. Erwähnt sei zudem, dass das Bitcoin-Konzept nicht im „luftleeren Raum" entstand, sondern auf Vorläufern beruhte. Einen Überblick geben Chohan (2017) und Hayes (2019).

tung gewonnen. Die Marktkapitalisierung aller Kryptowährungen beträgt mehrere hundert Milliarden US-Dollar und es gibt Futures und Exchange Traded Funds auf Kryptowährungen. Sogenannte Smart Contracts erlauben unter anderem die Emission von „Tokens“, die zum Beispiel im Rahmen von Initial Coin Offerings (ICOs), einer neuartigen Form der Unternehmensfinanzierung, eingesetzt werden.

Das Anwendungspotential der Blockchain-Technologie erstreckt sich jedoch weit über das Design von Kryptowährungen hinaus. So wird etwa darüber diskutiert, inwieweit sie die Abwicklung von Wertpapiergeschäften revolutionieren könnte. Ebenso wurden weitreichende Auswirkungen auf die Corporate Governance börsennotierter Unternehmen prognostiziert. Daneben sind auch zahlreiche Anwendungen in nicht-finanzwirtschaftlichen Bereichen diskutiert worden, mit denen wir uns in diesem Beitrag jedoch nicht beschäftigen werden.

Allerdings gibt es auch Stimmen, die die Auswirkungen der Blockchain-Technologie als weniger weitreichend ansehen. Die Idee des Bitcoins bestand im Verzicht auf Finanzinstitutionen wie Zentral- oder Geschäftsbanken (Nakamoto 2008). Tatsächlich findet jedoch heute der Großteil der Bitcoin-Transaktionen an Börsen (und damit an Finanzinstitutionen) statt, an denen Bitcoin und andere Kryptowährungen untereinander und gegen traditionelle Währungen gehandelt werden können (vgl. z. B. Brauneis et al 2019), was offensichtlich der Grundidee von Nakamoto (2008) widerspricht. Pirrong (2019) geht noch einen Schritt weiter wenn er (S. 98) schreibt *„... that the initial soaring hopes have been disappointed because the fascination with a shiny new technology blinded too many to underlying economic realities ...“*.

In diesem Beitrag unternehmen wir den Versuch einer kritischen Bestandsaufnahme möglicher finanzwirtschaftlicher Anwendungen der Blockchain-Technologie.[2] Er ist wie folgt gegliedert. Im zweiten Abschnitt beschreiben wir zunächst die technologischen Grundlagen der Blockchain, wobei wir die Bitcoin-Blockchain als Ausgangspunkt verwenden, aber an geeigneter Stelle jeweils alternative Gestaltungsmöglichkeiten diskutieren. Im dritten Abschnitt stellen wir dann die aus unserer Sicht wichtigsten finanzwirtschaftlichen Anwendungen der neuen Technologie dar. Dabei gehen wir insbesondere auf Kryptowährungen, Smart Contracts, Initial Coin Offerings, den Wertpapierhandel und die Corporate Governance börsennotierter Unternehmen ein. Der vierte Abschnitt beschließt den Beitrag mit einem Ausblick.

2 Technologie

Bitcoin und andere Kryptowährungen basieren auf der Blockchain-Technologie – einer Technologie, der, wie oben angedeutet, revolutionäres Potential in Bezug auf ihre möglichen Auswirkungen auf Geschäftsmodelle weltweit zugeschrieben wird. Kurz zusammengefasst ist die Blockchain eine verteilte Open-Source-Datenbank, die auf modernster Kryptografie basiert. Die Blockchain-Technologie zielt darauf ab, Transaktionen zwischen nicht vertrauenswürdigen Akteuren zu ermöglichen und die

[2] Aktuelle, nicht-technisch gehaltene Übersichtsarbeiten zum Potential und den Herausforderungen von Blockchain-Anwendungen im Banken- und Finanzbereich finden sich in Amin (2020), Chen and Bellavitis (2020) und Tapscott and Tapscott (2017).

Notwendigkeit eines vertrauenswürdigen Intermediärs zu beseitigen. Wenn dem so wäre, wären Finanztransaktionen ohne Banken möglich, wir bräuchten keine Makler mehr und auch Ratingagenturen und andere Auskunfteien wären überflüssig. Um zu verstehen, inwieweit die Technologie diese Erwartungen erfüllen kann, erläutern wir nachfolgend die Grundprinzipien der Technologie.[3] Es gibt zwei wesentliche strukturelle Elemente: Erstens eine Methode zum Organisieren und Speichern von Daten und zweitens eine Methode, um das Vertrauen in die Daten zu fördern.

2.1 Organisation und Speicherung von Daten

Eine Blockchain stellt eine Art Kassenbuch dar, das es ermöglicht, Informationen zu erfassen und zu verfolgen, seien es Informationen über Finanztransaktionen wie in Kryptowährungsanwendungen oder Informationen über anderes von Wert. Ein Verständnis der wesentlichen Merkmale dieses Kassenbuchs ist notwendig, um das Potential der Blockchain-Technologie verstehen zu können. Sie sollen daher im Folgenden detaillierter beleuchtet werden. Erstens organisiert die Blockchain Informationen in Form einer stetig wachsenden Liste von zeitgestempelten Datensätzen, zu der wir Daten hinzufügen, nicht aber frühere Daten darin ändern oder löschen können. Dies bedeutet nun nicht, dass das System nicht aktualisiert werden kann. Anstatt jedoch einen bestehenden Eintrag zu überschreiben, wird die Änderung an sich gespeichert, was zu einem neuen separaten zeitgestempelten Eintrag führt. Die Datenstruktur enthält also immer die komplette Historie. Auf den ersten Blick erscheint diese Art der Organisation und Speicherung von Daten umständlich und speicherintensiv, fördert aber, wie wir sehen werden, die Transparenz und die Betrugssicherheit. Technisch bezeichnet man ein Kassenbuch, das nur das Hinzufügen von Daten erlaubt, aber das Ändern oder Löschen von Daten verbietet, als „append-only ledger“. Aus Effizienzgründen werden die Daten zu Blöcken zusammengefasst. Ein Block enthält mehrere Einträge, z. B. mehrere Finanztransaktionen, und durch Anhängen eines neuen Blocks werden dem System neue Informationen hinzugefügt. Jeder Block enthält eine Referenz auf einen vorherigen Block (dessen „Identifikationsnummer“), was zu einer sequentiellen Reihenfolge der Blöcke führt. Somit können wir uns die Datenstruktur als eine Kette von Blöcken vorstellen – eine Metapher, die der Blockchain ihren Namen gab (siehe Abb. 1).

Zweitens ist eine Blockchain ein dezentrales System. Im Gegensatz zu einem klassischen Kassenbuch, das Daten auf einem einzigen System speichert und das von einer zentralen Instanz gepflegt wird, sind die Informationen bei einer Blockchain auf eine große Anzahl von Netzwerkteilnehmern, sogenannte Knoten, verteilt. Diese Knoten – man stelle sich diese als Computer vor – vertrauen sich nicht vollständig. Gleichwohl gelingt es durch einen klugen Mechanismus, dass das Kassenbuch über diese Knoten repliziert wird. Im Ergebnis gibt es auf einer Vielzahl von Computern weltweit identische Kopien der gesamten Transaktionshistorie. Es erscheint intuitiv, dass diese dezentrale Art der Datenorganisation dazu beiträgt, Angriffe zu verhindern und Vertrauen in die Daten zu schaffen. Der Prozess der Datenorganisa-

[3] Eine ausführlichere Einführung in die Blockchain-Technologie im Kontext der Bitcoin-Anwendung findet sich in Berentsen and Schär (2017).

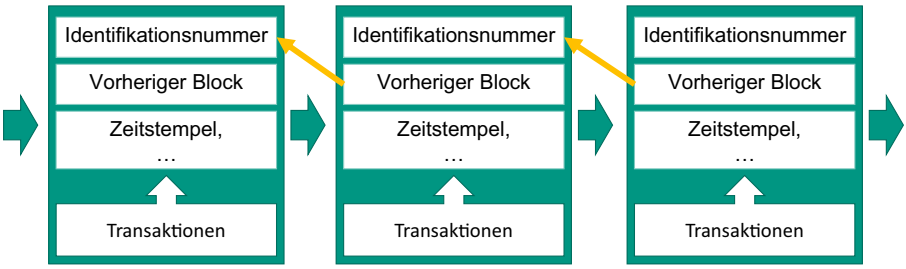

Abb. 1 Aufbau einer Blockchain (Ausschnitt mit drei Blöcken)

tion und der Aktualisierung einer Blockchain kann mit den folgenden vier Schritten zusammengefasst werden:

1. Eine neue Transaktion, die in die Blockchain aufgenommen werden soll, wird eingegeben und dann an jeden Knoten im Netzwerk gesendet. Sie ist nun zwar im Netzwerk verteilt, allerdings noch nicht Teil der Blockchain.
2. Knoten bündeln diese neuen Transaktionen in einem Block und ein durch den sogenannten Konsensmechanismus (s. u.) bestimmter Knoten erhält die Möglichkeit, seinen Block zu übertragen.
3. Andere Knoten bewerten die Gültigkeit aller Transaktionen in diesem Block.
4. Sie akzeptieren validierte Blöcke, indem sie sich in ihrem nächsten Block auf sie beziehen.

Das Ergebnis dieses Prozesses ist ein geordneter Satz von Blöcken, bei dem sich alle Knoten über die Reihenfolge einigen und Kopien der Blockchain vorhalten.

2.2 Vertrauen in die Daten fördern

Natürlich ist die oben beschriebene Datenstruktur nur dann von Wert, wenn ihr vertraut wird. Die spannende Frage ist, wie es möglich ist, das Vertrauen zwischen unzuverlässigen Parteien in einem dezentralen System zu fördern. Mit anderen Worten, wie kann sichergestellt werden, dass alle Parteien jedem einzelnen Block in der Kette vertrauen können? Die Blockchain-Technologie erzeugt ein solches Vertrauen durch zwei wesentliche technische Komponenten, durch asymmetrische Kryptografie und den sogenannten Konsensmechanismus.

2.2.1 Asymmetrische Kryptografie

Asymmetrische Kryptografie dient zunächst dazu, neue Transaktionen, die in die Blockchain aufgenommen werden sollen (vgl. Schritt 1) auf ihre Legitimität hin überprüfbar zu gestalten. Üblicherweise kommt hier ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel zum Einsatz, das über eine Einwegfunktion[4] zueinander in Bezug steht. Hierzu verschlüsselt die Absenderin ihre Transaktion mit ihrem privaten Schlüssel – man spricht auch von signieren – und jeder beliebige

[4] Eine Einwegfunktion lässt sich leicht (d. h. in Polynomialzeit) berechnen, aber nur schwer umkehren.

Netzwerkteilnehmer kann die Transaktion mit dem öffentlichen Schlüssel der Absenderin entschlüsseln und damit verifizieren, dass die Transaktion tatsächlich von der Absenderin stammt. Ziel ist es dabei letztlich, die Authentizität und Integrität der Transaktion zu gewährleisten, also die Transaktion jederzeit ihrer Absenderin zuordenbar zu machen und gleichzeitig sicherzustellen, dass die Transaktion nicht unbemerkt manipuliert wurde. Ehrliche Knoten können hierdurch legitime Transaktionen identifizieren und nur diese im Netzwerk weiterverbreiten. Solche kryptografischen Verfahren wurden nicht spezifisch im Kontext der Blockchain-Technologie entwickelt. Man nutzt sie vielmehr seit einiger Zeit etwa im E-Mail Verkehr, Electronic Banking oder beim Einkaufen im Internet.

2.2.2 Konsensmechanismus

Wie einigt man sich nun in einem dezentralen System auf die durchgeführten Transaktionen? Mit anderen Worten, wie gelangen neue Transaktionsblöcke in die Blockchain (vgl. Schritt 2)? Schließlich ist das Hinzufügen von Blöcken ja die einzig durchführbare Operation und es gibt keine Möglichkeit, bereits existierende Informationen abzuändern oder gar zu löschen. Daher besteht grundsätzlich ein Anreiz, Transaktionen hinzuzufügen, die den Urheber des Blockchain-Eintrags begünstigen. An diesem Punkt kommt die wesentliche Innovation der Blockchain-Technologie ins Spiel, der Konsensmechanismus. Dieser Mechanismus regelt, welcher Knoten seinen Block als nächstes in die Blockchain übertragen darf. Dieser Schritt ist zentral, denn auf der einen Seite soll es keine zentrale Instanz geben, die das Hinzufügen neuer Informationen kontrolliert. Wenn aber jeder beliebige Knoten grundsätzlich neue Informationen anhängen kann, muss man auf der anderen Seite befürchten, dass unehrliche Knoten versuchen, sich dabei ungerechtfertigt zu bereichern. Genau mit diesem Trade-off versucht der Konsensmechanismus umzugehen. Hierzu gibt man zunächst möglichst vielen oder sogar allen Knoten die generelle Möglichkeit, einen neuen Block hinzuzufügen. Damit sich hinreichend viele Knoten an diesem Schritt beteiligen, wird den Knoten, die neue Transaktionen sammeln, prüfen und mit dem Ziel bündeln, den nächsten Block an die bestehende Kette anhängen zu dürfen (die sogenannten Miner), eine Belohnung in Aussicht gestellt. Miner stehen folglich im Wettbewerb zueinander und es gilt, diesen Wettbewerb sinnvoll zu gestalten. So sollten die Knoten einen Anreiz haben, nur Blöcke mit legitimen Transaktionen zu erstellen, die weder zu sich selbst noch zu allen bereits in der Blockchain enthaltenen Transaktionen in Konflikt stehen. Insbesondere sollten also keine Transaktionen Teil des Blockkandidaten sein, die ein und denselben Vermögenswert mehrfach ausgeben (sogenannte Double Spend-Problematik).

Der weitverbreitetste Konsensmechanismus ist der dem Bitcoin-Netzwerk zugrunde liegende Proof-of-Work Mechanismus. Die Kernidee besteht darin, das Erstellen eines Blocks zu verteuern, die Überprüfbarkeit der Korrektheit eines neuen Blockkandidaten aber für alle anderen sehr günstig zu gestalten. Dadurch werden „Falschmeldungen“ teuer und können leicht entlarvt werden.

Zu diesem Zweck werden sogenannte Hash-Funktionen eingesetzt. Eine Hash-Funktion bildet eine große Datenmenge (etwa den gesamten Inhalt eines Blocks) auf eine kleine Datenmenge (den Hash-Wert) festgelegter Größe (256 Bit im Falle

der Bitcoin-Blockchain) ab. Die Hash-Funktion ist dabei so gestaltet, dass kleine Veränderungen der Eingangsdaten (etwa das Austauschen eines Buchstaben oder einer Zahl) zu einem völlig anderen Output führen. Die Bitcoin-Blockchain gibt nun einen bestimmten Maximalwert für den Hash-Wert vor, definiert durch die Anzahl führender Nullen. Um diesen Zielwert zu erreichen, wird einem Block eine Zahl (sogenannte Nonce) hinzugefügt. Diese Zahl wird nun durch Ausprobieren so lange verändert, bis der Hash-Wert die Vorgabe erfüllt. Die Zahl der Versuche pro Zeiteinheit, eine zulässige Lösung zu finden, bezeichnet man als Hash-Rate. Der erste Knoten, der eine solche zulässige Lösung findet, darf der Blockchain den Block hinzufügen und erhält eine Belohnung[5] (vgl. Schritt 2). Da die Erfolgsaussichten des Minings mit der eingesetzten Rechenleistung steigen, setzen Miner Hochleistungrechner ein, was zu einem sehr hohen Energieverbrauch führt.[6] Hat ein Miner erfolgreich einen neuen Block an die Blockchain angehängt, können alle anderen Knoten sehr leicht verifizieren, dass die Aufgabe in der Tat gelöst wurde. Dazu müssen sie nur den Block einschließlich der Nonce als Input in die Hash-Funktion eingeben und prüfen, ob der resultierende Hash-Wert die Vorgabe erfüllt. Ebenfalls überprüfbar ist die Validität der in einem Block enthaltenen Transaktionen relativ zur Historie. An dieser Stelle würden double spends, also Mehrfachausgaben desselben Vermögenswertes, unmittelbar erkannt (vgl. Schritt 3). Ungültige Blöcke werden von ehrlichen Knoten einfach ignoriert, wohingegen ein neuer gültiger Blockkandidat Teil der Blockchain wird, indem die Miner bei ihrer nächsten Blockerstellung auf diesen Block referenzieren (vgl. Schritt 4).

Die Verknüpfung, die aus den einzelnen Blöcken eine Kette (eben die Blockchain) macht, wird dadurch erreicht, dass jeder Block den Hashwert des vorherigen Blocks enthält. Würde in irgendeinem Block der Kette eine manipulative Veränderung vorgenommen, so würde das den Hash-Wert dieses Blocks und damit auch die Hash-Werte aller nachfolgenden Blöcke verändern, so dass eine solche Manipulation leicht aufdeckbar wäre. Den Hash-Wert eines Blocks kann man sozusagen als den Fingerabdruck des Blocks interpretieren.

Es kann passieren, dass quasi zeitgleich zwei korrekte neue Blöcke an die Blockchain angehängt werden, so dass gleichzeitig zwei Versionen der Blockchain in Umlauf sind. In diesem Fall muss geregelt werden, welche Version dem aktuellen Zustand entspricht. Konsensregel ist, dass dies die Kette mit der höchsten eingeflossenen Arbeitsleistung ist. In der Regel ist dies die jeweils längste Kette. Je mehr

[5] Die Belohnung setzt sich aus neu geschaffenen Bitcoin-Einheiten und den Transaktionsgebühren im jeweiligen Block zusammen. Die Anzahl der neu geschaffenen Einheiten pro Block betrug zu Beginn 50 Bitcoins. Sie halbiert sich alle vier Jahre. Ab Mai 2020 beträgt sie 6,25 Bitcoins. Durch diesen Mechanismus wird gewährleistet, dass die Zahl der Bitcoins gegen einen festen Wert, nämlich 21 Millionen Bitcoin, konvergiert.

[6] Anfang 2020 überstieg der Energieverbrauch für das Mining den Verbrauch Österreichs, vgl. https://digiconomist.net/bitcoin-energy-consumption (aufgerufen am 22.2.2020). Auf der gleichen Webseite wird dargelegt, dass der Energieverbrauch *einer* Bitcoin-Transaktion dem Energieverbrauch von etwa 300.000 Visa-Transaktionen entspricht (überprüft am 15.5.2020). Auch wenn diese Zahl sicherlich mit Vorsicht zu interpretieren ist, belegt sie doch, dass der Energieverbrauch des Bitcoin-Netzwerks nicht nur absolut, sondern auch relativ zu dem anderer Zahlungssysteme sehr hoch ist.

Blöcke daher auf einen bestimmten Block folgen, desto sicherer ist es, dass das Kollektiv diesen Block als Teil der Blockchain betrachtet.[7]

Letztlich erschwert dieser Proof-of-Work Mechanismus das Erstellen und Hinzufügen neuer Blöcke künstlich, indem zunächst eine geeignete Nonce gefunden werden muss. Die Schwierigkeit dieser probabilistischen Trial-and-Error Aufgabe wird im Bitcoin-Netzwerk so gewählt, dass im Schnitt alle zehn Minuten ein neuer gültiger Block entsteht. Die dabei vom Miner geleistete Arbeit ist namensgebend für den Proof-of-Work Mechanismus.

Im Ergebnis wird über diesen Proof-of-Work Mechanismus geregelt, dass sich das Kollektiv an Netzwerkteilnehmern auf den aktuellen Zustand der Blockchain einigt und den darin enthaltenen Daten vertraut. Das Vertrauen entsteht hier nicht durch einen „vertrauenswürdigen" Intermediär. Vielmehr werden die Kosten für einen erfolgreichen Angriff auf die Daten – die immense Rechenleistung, die hierfür notwendig wäre – prohibitiv hoch gesetzt und gleichzeitig Anreize für ehrliches Verhalten gesetzt. Eine funktionierende Blockchain-Technologie ersetzt sozusagen den „vertrauenswürdigen" Intermediär durch technologisches Vertrauen.

Je nach Ausgestaltungsart (vgl. Abschn. 2.3) der Blockchain sind andere Konsensmechanismen eventuell geeigneter. Eine Alternative zum ressourcenintensiven Proof-of-Work Mechanismus ist beispielsweise das „Proof-of-Stake" Konzept, bei dem die Wahrscheinlichkeit, seinen erstellten Blockkandidaten anhängen zu dürfen, vom Vermögensanteil abhängt, den man an der Blockchain bzw. den darüber erfassten Wertgegenständen hält. Die wesentliche Idee dabei ist, denjenigen Akteuren eine höhere Verantwortung und damit auch Kontrolle zu geben, die ein hohes Interesse am Erfolg der jeweiligen Blockchain haben. In Industrieanwendungen, die in der Regel nicht primär darauf ausgelegt sind, Konsens zwischen unzuverlässigen Parteien herzustellen, kommen weitere Mechanismen in Frage, die auf einer gewissen Anzahl an vertrauenswürdigen Knoten basieren (Proof-of-Authority).

2.3 Ausgestaltungsarten

Die bisher dargestellte Blockchain-Philosophie beruht auf einer vollständig dezentral organisierten Datenstruktur ohne jegliche Zugangsbeschränkungen mit potentiell unehrlichen Teilnehmern. Tatsächlich kann eine Blockchain aber auf sehr unterschiedliche Art und Weise ausgestaltet sein.[8] So lässt sich regeln, wer überhaupt Zugang zu den in der Blockchain gespeicherten Informationen hat. Analog können auch die Schreibrechte geregelt werden. Bei einer öffentlichen (public) Blockchain wie der Bitcoin-Blockchain kann grundsätzlich jeder dem Netzwerk beitreten und auf die gespeicherten Informationen zugreifen. Eine öffentliche Blockchain ist daher in hohem Maße transparent. Bei der Bitcoin-Blockchain kann sich darüber hinaus grundsätzlich jeder als Miner betätigen und damit Änderungen in der Blockchain vornehmen – man spricht daher von einer „public unpermissioned" Blockchain. Hingegen wird in Industrieanwendungen wie etwa Hyperledger oder R3 corda der

[7] Im Bitcoin-Netzwerk erachtet man Blöcke mit fünf oder mehr Nachfolgeblöcken als sichere Bestandteile der Blockchain.

[8] Vgl. hierzu auch die technischen Blockchain-Charakteristika in Labazova et al (2019).

Teilnehmerkreis häufig nur auf bestimmte autorisierte Mitglieder beschränkt. Man spricht dann von einer „private permissioned“ Blockchain.

Eine weitere wichtige Charakterisierung betrifft den Grad der Anonymität, also letztlich die Frage, inwieweit persönliche Daten für die Nutzung der Blockchain erforderlich sind. Einige Kryptowährungen, wie beispielsweise Monero, operieren ohne jegliche Benutzerdaten (anonym), andere Anwendungen erfordern unmittelbar die Angabe von personenbezogenen Daten, etwa der E-Mail Adresse, um an der Blockchain teilnehmen zu können (identifiziert). Standard im Kryptowährungsbereich ist es jedoch, unter Pseudonymen zu arbeiten.

Öffentliche auf dem Proof-of-Work Konzept beruhende Blockchain-Technologien, wie die Bitcoin-Blockchain, sind durch eine geringe Skalierbarkeit und einen hohen Resourcenverbrauch je Transaktion gekennzeichnet. Darüber hinaus sind verschiedene Blockchain-Technologien (etwa Bitcoin und Ethereum) zunächst nicht miteinander kompatibel, so dass direkte Transaktionen zwischen diesen nicht getätigt werden können. Neue technologische Entwicklungen zielen darauf ab, bestehende Restriktionen zu überwinden und der wachsenden Bedeutung der Interoperabilität Rechnung zu tragen.[9] Hier gibt es etwa Konzepte wie „sidechains“ (parallel zur primären Blockchain verlaufende Blockchain), „state channels“ (Transaktionen außerhalb der primären Blockchain) oder die Idee des „sharding“ (Transaktion wird nicht von allen Knoten verarbeitet). Vergleiche hierzu auch Voshmgir (2019).

3 Anwendungsgebiete

Die Hauptinnovation der Blockchain-Technologie ist es, einen Konsens zwischen Agenten herzustellen, die sich nicht vollständig vertrauen – und das ohne einen zentralen vertrauenswürdigen Intermediär wie eine Bank, eine Börse oder einen Makler. Ein einfaches Anwendungsbeispiel liefert ein Gebrauchtwagenkauf: Viele Personen bevorzugen es, einen solchen über einen Händler abzuwickeln und das Auto nicht direkt vom vorherigen Besitzer zu kaufen. Ein Grund hierfür ist das fehlende Vertrauen in den Vorbesitzer. Würden alle das Auto betreffenden „Transaktionen“ wie Unfälle und Reparaturen in einer unveränderlichen Datenbank wie einer Blockchain gespeichert, wäre Vertrauen in den Vorbesitzer nicht mehr notwendig. An die Stelle des Vertrauens in den Autohändler, einen möglicherweise nur schwierig zu überprüfenden Intermediär, würde das Vertrauen in die Blockchain-Technologie rücken.

Die komparativen Vorteile der neuen Technologie lassen sich daher besonders in einem Umfeld realisieren, in dem Agenten, die sich nicht vollständig vertrauen, miteinander Transaktionen abschließen. Im Folgenden werden fünf solcher Anwendungsgebiete vorgestellt.

[9] Streng genommen handelt es sich bei einigen hier diskutierten Anwendungen nicht mehr um Blockchain-Technologien sondern genereller um Distributed-Ledger-Technologien (DLT). Beide Begriffe werden zwar häufig synonym verwendet, der DLT-Begriff ist allerdings breiter und umfasst neben der Datenstruktur in Form einer Blockchain auch Datenstrukturen ohne eine Blockchain in Form eines azyklischen Graphen. Ein Beispiel hierfür ist IOTA.

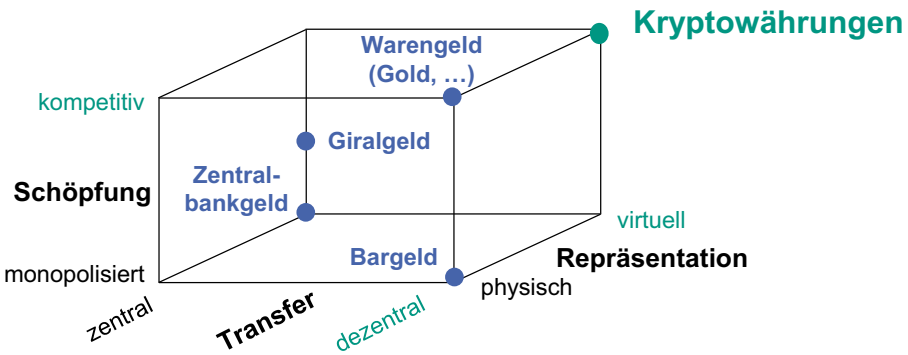

Abb. 2 Dimensionen von Zahlungssystemen nach Berentsen and Schär (2017)

3.1 Kryptowährungen

Nach der klassischen Theorie von Menger (1871) werden Güter, an denen viele zukünftige potentielle Handelspartner Interesse haben, in Tauschgeschäften genutzt, obwohl sie nicht zum unmittelbaren Gebrauchszweck benötigt werden. Werttreiber solcher Güter, die auch als „Geld“ bezeichnet werden, kann also einzig und allein der Glaube daran sein, dass sie zu einem späteren Zeitpunkt oder mit einem anderen Handelspartner wieder zum Tauschen verwendet werden können (sogenannter Liquiditätswert). Kocherlakota (1998) sieht den Hauptzweck von Geld darin, die gegenseitigen Ansprüche der Agenten untereinander festzuhalten. In kleinen Gruppen, man denke beispielsweise an den Austausch von Gefälligkeiten im Freundeskreis, ist dazu kein formales System notwendig. In großen Gesellschaften funktionieren solche informellen Systeme nicht mehr. Geld fungiert hier als eine Art Gedächtnis, das die gegenseitigen Verbindlichkeiten speichert.[10] Zentral in einer solchen als Gedächtnis fungierenden Datenbank ist zum einen, dass die Besitzverhältnisse zu jedem Zeitpunkt eindeutig festgelegt sind. Für ein funktionierendes System ist zum anderen Voraussetzung, dass jede Geldeinheit nur einmal ausgegeben werden kann (Double-Spend-Problematik).

Berentsen und Schär (2017) definieren Währungen oder allgemeiner Zahlungssysteme anhand dreier Dimensionen. Diese betreffen die Regeln, nach denen Geld geschöpft, repräsentiert und übertragen wird (vgl. Abb. 2). Geldschöpfung kann entweder monopolisiert, z. B. durch eine Zentralbank oder kompetitiv wie beispielsweise beim Schürfen von Gold erfolgen. Die Repräsentation kann virtuell wie bei Giralgeld auf dem Bankkonto oder physisch wie bei Bargeld sein. Zuletzt kann der Transfer zwischen verschiedenen Teilnehmern zentral wie beispielsweise bei einer Überweisung über eine Bank bzw. ein angeschlossenes Gironetz oder dezentral wie beim Austausch von Bargeld erfolgen.

Die virtuelle Repräsentation hat gegenüber der physischen erhebliche Effizienzvorteile. Gleichzeitig wird die Abhängigkeit von einer zentralen Instanz aus verschiedenen Gründen (fehlendes Vertrauen, Sicherung des Systems vor Ausfall) negativ

[10] Für eine ausführliche Diskussion siehe z. B. Berentsen and Schär (2017).

gesehen. Die Kombination von virtueller Repräsentation und dezentralem Transfer wäre daher optimal, war aber vor der Entwicklung der Blockchain-Technologie nicht umsetzbar. Kryptowährungen wie Bitcoin oder Ethereum kombinieren aber genau diese aus ökonomischer Sicht wünschenswerten Eigenschaften. Die Frage ist daher, warum sie sich bisher noch nicht auf breiter Basis durchsetzen konnten.[11]

Um diese Frage zu beantworten, betrachten wir die drei zentralen Funktionen von Geldeinheiten (in der Literatur oftmals als „Triade des Geldes“ bezeichnet):

1. Tausch- bzw. Zahlungsmittelfunktion
2. Wertaufbewahrungsfunktion
3. Recheneinheitsfunktion

Damit eine Geldeinheit die Tausch- bzw. Zahlungsmittelfunktion optimal ausfüllen kann, sollte es in einer Ökonomie eine möglichst geringe Anzahl an verschiedenen Währungen geben. Formal wird jeder Agent genau dann eine gegebene Währung akzeptieren, wenn er davon ausgeht, dass ein zukünftiger Tauschpartner die Währung mit einer hohen Wahrscheinlichkeit akzeptiert. Eine neue Währung wird im Allgemeinen zunächst von niemandem akzeptiert. Aufgrund der Abhängigkeit der eigenen Akzeptanz von der Akzeptanz durch andere Marktteilnehmer ist es für eine neue Währung daher sehr schwierig, dieses initiale Gleichgewicht zu verlassen. Dies wird zusätzlich dadurch erschwert, dass klassische Währungen wie Euro und US-Dollar in ihren jeweiligen Ländern gesetzliches Zahlungsmittel sind, d. h. Verkäufer zur Akzeptanz verpflichtet werden. Weitere Gründe, die die Zahlungsmittelfunktion von Kryptowährungen teilweise beeinträchtigen, sind erstens die relativ hohe Komplexität bei der Handhabung und zweitens die zum Teil verhältnismäßig hohen Transaktionskosten.[12] Im Vergleich zu Bargeld und Kreditkarte wirkt sich die typischerweise notwendige Zeit bis zur endgültigen (unumkehrbaren) Bestätigung einer Transaktion ebenfalls negativ auf die Akzeptanz von Kryptowährungen aus.

Die aktuell (noch) sehr hohen Wertschwankungen der meisten Kryptowährungen stehen ihrer Funktion als Wertspeicher entgegen und behindern ihre Funktion als Recheneinheit. Obwohl der Pfad der Geldschöpfung bei den meisten Kryptowährungen im Protokoll festgelegt ist[13] und es daher nicht zu einer inflationären Vergrößerung der Geldmenge kommen kann, führen die Verwendung als Spekulationsobjekt, die ungewisse zukünftige Adaption sowie die Konzentration von großen

[11] Zur Einordnung des derzeitigen Verbreitungsgrades von Kryptowährungen bietet sich ein Vergleich des Bruttoinlandsprodukts (BIP) ausgewählter Währungsräume mit dem über die Bitcoin-Blockchain abgewickelten Transaktionsvolumen (365 Mrd. USD in 2019) an. Dieses entspricht rund 2,7 %, 1,8 % bzw. 0,4 % des BIP der Eurozone, der Vereinigten Staaten bzw. der gesamten Welt (Datenquellen: blockchain.info, Weltbank, Daten für BIP von 2018). Da viele Bitcoin-Transaktionen zu anderen Zwecken als dem Kauf von Gütern und Dienstleistungen abgeschlossen werden, sind die genannten Prozentsätze als Obergrenze anzusehen.

[12] Durchschnittlich zu bezahlende Transaktionskosten schwanken im Zeitverlauf sehr stark und betrugen beispielsweise im Bitcoin-Netzwerk in Zeiten maximaler Nachfrage im Dezember 2017 über 50 USD pro Transaktion (Quelle: https://blockchain.info).

[13] Vgl. etwa die in Fußnote 5 erwähnte Beschränkung des Bitcoin-Umlaufs auf maximal 21 Millionen Bitcoin.

Teilen der Geldmenge bei einigen wenigen Akteuren[14] zu hohen Wertschwankungen. So ist die Volatilität beispielsweise des Bitcoin-USD Wechselkurses in den letzten Jahren zwar etwas zurückgegangen, betrug im Jahr 2019 aber immer noch 70,7 % p. a. Zum Vergleich betrug im gleichen Zeitraum die Volatilität des EUR-USD Wechselkurses nur 5,0 % p. a. Gold, das in einigen Aspekten eine gewisse Ähnlichkeit mit Kryptowährungen aufweist, hatte eine Volatilität von 11,5 % p. a.[15]

Als Reaktion auf die hohen Wertschwankungen wurden sogenannte Stablecoins entwickelt. Die zugrundeliegende Idee ist, dass die Kryptowährung durch einen festen Geldbetrag gedeckt ist. Ein Beispiel hierfür ist die Kryptowährung Tether, bei der jede Tether-Einheit durch 1 USD besichert ist. Auch Libra, die von Facebook geplante Kryptowährung, soll durch einen Währungskorb gedeckt werden.[16] Ein Problem der Stablecoins ist es, dass sie konstruktionsbedingt von einer zentralen Instanz, nämlich dem Unternehmen oder Konsortium, das die Besicherung durchführt, abhängig sind. Dies steht zum einen der Ursprungsidee von Kryptowährungen entgegen, für eine Unabhängigkeit von zentralen Intermediären zu sorgen. Zum anderen führt es möglicherweise zu einer systemischen Relevanz der entsprechenden Akteure und zur Gefahr von Monopolen, die durch die im Zusammenhang mit der Nutzung einer Kryptowährung entstehenden großen Datenmengen noch verschärft wird.

3.2 Smart Contracts

Der Begriff Smart Contracts wird für Verträge verwendet, die an bestimmte Bedingungen geknüpft automatisch vollzogen werden. Im Blockchain-Kontext bezeichnet der Begriff einen in der Blockchain hinterlegten Programmcode, der abhängig von vordefinierten Bedingungen, aber unabhängig vom ursprünglichen Ersteller des Codes, automatisch ausgeführt wird.[17] Smart Contracts erweitern damit die Fähigkeit der Blockchain Informationen zu speichern um die Fähigkeit Berechnungen durchzuführen. Durch die technische Ausgestaltung der Blockchain kann der Programmcode, wenn er einmal abgelegt ist, nicht mehr geändert werden. Er liefert den Vertragsparteien daher die Sicherheit, dass es bei Erfüllung der Bedingungen auch tatsächlich zum vereinbarten Ereignis kommt. Ist das Ereignis eine Zahlung oder die Übertragung eines Vermögensgegenstandes, so wird diese üblicherweise ebenfalls direkt über die Blockchain abgewickelt.

Ein Beispiel für eine Anwendung ist eine Versicherung gegen extreme Ereignisse. Wird solch ein Kontrakt auf herkömmliche Weise mit einem Versicherungsunterneh-

[14] Beispielsweise halten im Bitcoin-Netzwerk etwas mehr als 100 Adressen insgesamt über 15 % des umlaufenden Vermögens, über 21 Millionen Adressen – und damit etwa 73 % aller Adressen mit positivem Guthaben – halten insgeamt nur 0,18 % des umlaufenden Vermögens (Daten vom Februar 2020, https://bitinfocharts.com).

[15] Die Volatilitäten weiterer Wechselkurspaare im selben Zeitraum sind CHF-USD mit 5,6 % p. a., GBP-USD mit 8,3 % p. a. und JPY-USD mit ebenfalls 5,6 % p. a. Berechnet mit Daten aus Bloomberg, Refinitiv und https://blockchain.info.

[16] Für eine ausführliche Diskussion des Libra-Konzepts und der sich dadurch ergebenden regulatorischen Probleme und systemischen Risiken vgl. Schmeling (2019).

[17] Vgl. auch Narayanan et al (2016) und Berentsen und Schär (2017).

men als zentralem Intermediär implementiert, dauert die Bearbeitung von Ansprüchen oftmals verhältnismäßig lange. Aufgrund komplexer Auszahlungsbedingungen und schwierig zu verstehender Vertragstexte besteht beim Versicherungsnehmer eine gewisse Unsicherheit über die tatsächliche Auszahlung. Im Unterschied dazu führt die Abwicklung über einen Smart Contract zu transparenten Bedingungen, die an messbare Ereignisse wie z. B. Windgeschwindigkeiten oder Erdbebenstärken geknüpft werden können und bei Erfüllung zu einer sofortigen Auszahlung führen. Die Effizienz bei der Abwicklung wird auch dadurch ermöglicht, dass durch den der Blockchain inhärenten Konsensmechanismus sehr schnell ein Konsens über den „wahren" Zustand der Welt erreicht werden kann. Die Bereitstellung des Versicherungsschutzes kann durch ein Versicherungsunternehmen oder direkt durch die Versichertengemeinschaft und gegebenenfalls weitere Investoren erfolgen. Die Implementierung als Smart Contract bietet damit durch den Abbau von Eintrittsbarrieren auch die Möglichkeit, entsprechende Risiken noch effizienter zu verteilen.[18]

Eine der zentralen Herausforderungen bei der Erstellung von Smart Contracts in einer Blockchain ist die Einbindung externer Informationen wie beispielsweise Wetterdaten oder auch Wertpapierpreise. Schnittstellen, die solche Informationen sammeln, verifizieren und für die Blockchain nutzbar machen, werden Oracles genannt. Da sie von externen Zuständen abhängig sind und dementsprechend nicht durch die kryptografischen Mechanismen der Blockchain abgesichert werden können, stellen sie in vielen Fällen einen zentralen Angriffspunkt und damit ein gewisses Sicherheitsrisiko dar.

Einfache Smart Contracts wie beispielsweise die Knüpfung einer Zahlung an komplexe Bedingungen oder an die Lieferung eines Krypto-Assets lassen sich auch in der Bitcoin-Blockchain abbilden. Da die Bitcoin-Skriptsprache allerdings keine Schleifen zulässt, können viele Arten von Berechnungen damit nicht durchgeführt werden – formal ausgedrückt: die Sprache ist nicht turing-vollständig. Sollen komplexere Smart Contracts auf einer öffentlichen Blockchain ausgeführt werden, kann dazu beispielsweise Ethereum verwendet werden. Die zugehörige Programmiersprache erlaubt die Programmierung sogenannter Distributed Apps, ist turing-vollständig und bietet Tools zur Standardisierung von Verträgen wie beispielsweise die Herausgabe eigener Krypto-Wertmünzen (sogenannte Tokens).

Um entscheiden zu können, welche Art von Verträgen sinnvoll über Smart Contracts abgebildet werden können, diskutieren wir Stärken und Schwächen dieser Vertragsform. Smart Contracts sind verlässlich und vollständig transparent. Da es sich um maschinenlesbaren Code handelt, lassen sie im Unterschied zu üblichen Vertragsformen keinerlei Spielraum bei der Interpretation. Sie bieten ein hohes Sicherheitsniveau, da Vertragsbedingungen im Nachhinein nicht verändert werden können und üblicherweise kryptografisch verschlüsselt werden. Durch den Wegfall von bürokratischen Strukturen und die Unabhängigkeit von Drittparteien führen sie in vielen Anwendungsfällen zu einer Zeit- und Kostenersparnis. Einschränkend ist zu beachten, dass sämtliche Vertragsinformationen in der Blockchain vorhanden oder über Oracles eingebunden werden müssen. Die Unabänderlichkeit des Codes macht nachträgliche Upgrades, selbst wenn alle Parteien einverstanden sind, un-

[18] Vgl. auch https://www.skalex.io für weitere Anwendungsbeispiele.

möglich. Demzufolge lassen sich auch Fehler im Code nicht ohne weiteres, d. h. in den meisten Fällen nur durch eine Hard Fork, beheben.[19] Dieses Problem wird noch dadurch erschwert, dass das Testen von Smart Contracts teilweise schwierig ist, da eine Interaktion mit anderen Smart Contracts oder externen Services bestehen kann. Interessanterweise hat eine Untersuchung von Nikolić et al (2018) ergeben, dass etwa 3 % von knapp einer Million analysierten Smart Contracts auf der Ethereum-Blockchain Schwachstellen aufweisen.[20]

Die Abwicklung einer Transaktion über einen Smart Contract hängt eng mit der Vollständigkeit des zugrunde liegenden Vertrages zusammen. Erstens erfordert die Implementierung über einen Smart Contract, dass alle zukünftig möglichen Zustände, in denen eine Aktion erforderlich ist, bereits im Vorhinein erfasst und im Programmcode berücksichtigt werden. Dies gilt auch, wenn die jeweiligen Eintrittswahrscheinlichkeiten nur sehr gering sind. Es ist daher nicht ohne weiteres möglich, für bestimmte Situationen die Vorgehensweise bewusst offen zu lassen und nur im Bedarfsfall eine Einigung mit dem Vertragspartner zu erzielen. Solche unvollständigen Verträge sind aber in vielen Situationen, vor allem wenn die Anzahl der zukünftigen Zustände hoch ist und die Formulierung eines vollständigen Vertrages damit sehr teuer wäre, gebräuchlich und auch optimal (vgl. z. B. Hart und Moore 1999 sowie Segal 1999). Ein typisches Beispiel für einen unvollständigen Vertrag, der sich nicht sinnvoll über einen Smart Contract abbilden lässt, ist ein Arbeitsvertrag, da weder der Arbeitsinhalt noch die Arbeitsbedingungen ex ante exakt festgelegt werden können (vgl. Cartier 1994).

Zweitens führt die Abwicklung von Transaktionen über eine gemeinsame Blockchain dazu, dass zukünftige Zustände, die ansonsten für bestimmte Akteure nicht nachprüfbar wären, über den dezentralen Konsensmechanismus nachvollziehbar werden und direkt als Bedingungen in Smart Contracts verwendet werden können. So lässt sich beispielsweise der Verkaufserfolg eines Endprodukts auch für den vorgeschalteten Zwischenhändler nachvollziehen. Dadurch erweitern sich die Möglichkeiten, vollständige Verträge abzuschließen. Durch die breite Informationsbasis werden Eintrittsbarrieren reduziert und Wettbewerb wird gefördert. Allerdings kann die erweiterte Verfügbarkeit von Informationen, die für das Erreichen des dezentralen Konsenses für jeden Teilnehmer zugänglich sein müssen, zu neuen Möglichkeiten der geheimen Absprache zwischen Wettbewerbern führen. Cong and He (2019) analysieren diesen Trade-Off und finden, dass der resultierende ökonomische Gesamteffekt – auch abhängig von regulatorischen Gegebenheiten – sowohl positiv als auch negativ sein kann.

[19] Eine Hard Fork entsteht durch eine Änderung im Konsensprotokoll, die nicht kompatibel mit dem alten Protokoll ist, wodurch es zu einer Aufspaltung der Blockchain kommt. Demgegenüber führt eine Soft Fork nicht zu einer Aufspaltung, da die nach neuem Protokoll erstellten Blöcke trotzdem noch dem alten Protokoll genügen. Eine Hard Fork gab es bei Ethereum um einen „Diebstahl" von Tokens, der durch einen Fehler im Code möglich wurde, rückgängig zu machen (vgl. Securities and Exchange Commission 2017).

[20] Die Autoren suchen mit einem automatisierten Analysetool nach Sicherheitslücken, die dazu führen, dass Mittel auf unbestimmte Zeit gesperrt sind, an beliebige Nutzer weitergeleitet werden können oder der Smart Contract von jedermann beendet werden kann.

3.3 Initial Coin Offerings

In einem Initial Coin Offering (ICO) verkauft ein Unternehmen, in den meisten Fällen ein Internet-Startup, Tokens, d. h. Wertmünzen. Diese können entweder Zahlungsansprüche gegenüber dem Unternehmen verbriefen, die an Gewinn oder Umsatz des Unternehmens gekoppelt sein können (Security Tokens) oder zur Nutzung der zukünftigen Dienstleistung des Unternehmens berechtigen (Utility Tokens). Auch bei Utility Tokens steht in vielen Fällen die Hoffnung auf einen späteren Weiterverkauf mit Gewinn im Mittelpunkt. ICOs sind daher typischerweise eine Mischform aus Wertpapieremission und Vorabverkauf eines Produktes (siehe Abb. 3). Dies führt dazu, dass sie nur sehr schwer zu bewerten sind. Bestehende Gesetze und Vorschriften aus den Bereichen Investoren- und Konsumentenschutz passen nicht zum neuen Konzept und die unklaren Zuständigkeiten erschweren das Erarbeiten neuer Regulierungsvorschriften.

Ein ICO dient zur (erstmaligen) Kapitalaufnahme durch ein (Startup-) Unternehmen auf Basis der Blockchain-Technologie. Häufig existiert zum Zeitpunkt des ICO noch kein Produkt bzw. keine Dienstleistung, sondern nur ein sogenanntes „White Paper", das die grundsätzliche Produktidee und ihre Ausgestaltung beschreibt. Die neu emittierten Wertmünzen werden ohne Börsen oder andere Intermediäre verkauft, wobei die Bezahlung meistens in Kryptowährungen erfolgt. Die Abwicklung eines ICO erfolgt typischerweise über eine Blockchain mit Hilfe von Smart Contracts. Wichtig ist aber, dass die Investoren durch den Kauf der Wertmünzen keine unmittelbare rechtliche Beziehung zum Unternehmen eingehen.[21]

Das Volumen der durch Unternehmen neu emittierten Wertmünzen ist 2018 auf 21,6 Mrd. USD gestiegen, mehr als eine Verdreifachung im Vergleich zu 2017 und eine Steigerung um mehr als den Faktor 80 gegenüber 2016. Im Jahr 2019 kam es mit nur noch 3,3 Mrd. USD dann zu einem starken Einbruch in den Volumina.[22] ICOs stehen in Konkurrenz zu klassischer Venture Capital Finanzierung und Crowdfunding bzw. ergänzen diese in Form von hybriden Modellen (vgl. strategy& et al 2018). Trotz der zeitweise sehr hohen Volumina werden ICOs in der öffentlichen Wahrnehmung vor allem mit Skandalen in Verbindung gebracht – und tatsächlich gab es eine Vielzahl von Fällen, in denen Investoren durch ICOs ihr gesamtes Investment verloren haben. Besonders in Verruf geraten sind ICOs, die von Prominenten beworben werden, so dass die US-Aufsichtsbehörde SEC explizit vor dieser Art von ICO warnt. Da ICOs oftmals über mehrere Runden strukturiert sind und der Preis der Tokens im Verlauf ansteigt, bergen sie auch immer die Gefahr von Ponzi Schemes. Einige Regulatoren reagieren auf die Skandale mit einem kompletten Verbot von ICOs (beispielsweise China). Die meisten westlichen Länder versuchen demgegenüber mit Einzelfallprüfungen und teilweise relativ strikten Regulierungen Investoren zu schützen, ohne ICOs komplett zu verbieten. Unter anderem als Reaktion auf die Skandale haben sich neben klassischen ICOs mittlerweile Initial Exchange Offerings (IEOs) als eine weniger dezentrale Weiterentwicklung etabliert. Hierbei

[21] Darstellung teilweise in Anlehnung an Hahn and Wons (2018), die auch eine ausführliche Diskussion zu Umsetzung und Ablauf von ICOs liefern.

[22] Datenquelle: https://www.coinschedule.com/stats.html.

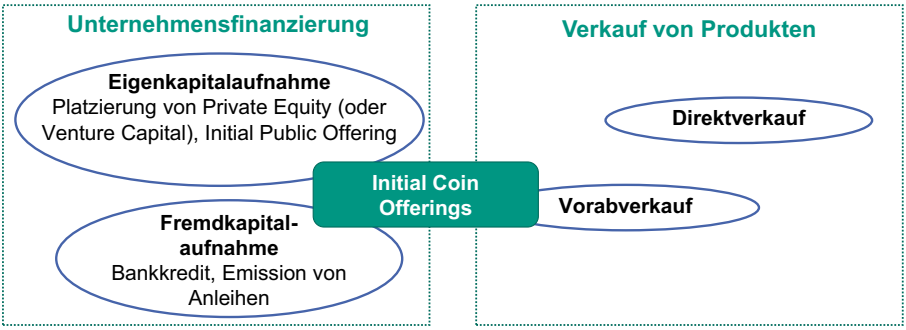

Abb. 3 Einordnung von Initial Coin Offerings (ICOs)

nimmt eine Kryptobörse die Rolle eines Intermediärs ein, führt ein erstes Screening des Unternehmens durch und wickelt den Verkauf der Wertmünzen anschließend ab.

Um besser verstehen zu können, wie ICOs reguliert werden sollten und in welchen Situationen sie eingesetzt werden können, betrachten wir zwei Kanäle, über die ICOs ökonomischen Wert schaffen. Erstens helfen sie bei der Plattformbildung (vgl. hierzu Li und Mann 2018). Bei vielen Plattformanwendungen steigt der Nutzen aller Teilnehmer mit Anzahl und Aktivitäten anderer Nutzer durch Netzwerkeffekte, so dass sich ein Beitritt nur bei einer hinreichend großen Anzahl weiterer Nutzer lohnt.[23] Durch den Kauf der (Utility) Tokens senden Investoren ein Signal, dass sie an der durch das Startup entwickelten Plattform teilnehmen werden. Dadurch wird das Risiko für andere Teilnehmer gemindert, dass ihr Nutzen aufgrund zu weniger weiterer Teilnehmer negativ ist. ICOs lösen damit das zugrundeliegende Koordinationsproblem. Findet ein ICO über mehrere Runden statt, ist ein Anstieg des Token-Preises damit anreizkompatibel und dadurch gerechtfertigt, dass das Projekt durch die bestehenden Engagements früherer ICO-Runden einen höheren Wert besitzt. Ein zweiter Kanal, über den ICOs Wert schaffen, ist der sogenannte Wisdom-of-the-Crowd Effekt. Im Unterschied zu einem klassischen Initial Public Offering (IPO), in dem Investmentbanken für die Aggregation vorhandener Informationen und die Bewertung des Unternehmens zuständig sind, erfolgt der Bewertungsprozess für ICOs dezentral und wird stark von „Online Analysten“ und frühen Investoren getrieben (vgl. auch Lee et al 2019). Durch die Empfehlungen und Investitionsentscheidungen dieser Gruppen verbunden mit der Möglichkeit, ICOs über mehrere Runden durchzuführen, können weniger gut informierte Teilnehmer das Investitionsverhalten der Experten beobachten und dazu beitragen, die kritische Masse an Teilnehmern zu erreichen.

Beide Effekte hängen eng mit der dualen Rolle von ICOs als Nutzungsrecht und Wertanlage zusammen. Ein hohes Interesse an den Tokens signalisiert eine hohe Nutzung, die über Netzwerkeffekte zu einer Rückkopplung auf den Wert der Anteile

[23] Beispiele für ICOs von Startups mit Plattformcharakter sind Ethereum (Smart Contracts), Filecoin (dezentrales Teilen von Speicherkapazitäten) und Unikrn (Wetten auf E-Sports).

führt. Ein höherer Wert führt wiederum zu mehr Aufmerksamkeit und dadurch zu einer höheren Adaption der Plattform.[24]

3.4 Wertpapierabwicklung

Wertpapiere werden an Börsen oder außerbörslichen Plattformen gehandelt. Mit dem Abschluss einer Transaktion ist der Handelsvorgang jedoch nicht abgeschlossen. Die gegenseitigen Lieferverpflichtungen müssen festgestellt werden (Clearing) und die Wertpapiere müssen vom Verkäufer an den Käufer sowie der Kaufpreis vom Käufer an den Verkäufer übertragen werden (Abwicklung oder Settlement). Derzeit erfolgt die endgültige Erfüllung einer Transaktion erst zwei Werktage nach dem Handelstag. Sie erfolgt unter Einschaltung einer Reihe spezialisierter Institutionen wie Broker, Clearinghäuser und Zentralverwahrer (Wertpapiersammelbanken, Central Securities Depositories). Dabei ist der Markt fragmentiert in dem Sinne, dass es mehrere, parallel operierende Systeme (sogenannte „Silos“) gibt wie etwa bei der Deutschen Börse, wo Eurex Clearing das Clearing und Clearstream das Settlement durchführen. Diese Fragmentierung wiederum erfordert die Existenz von Schnittstellen zwischen den Systemen. Diese Architektur macht die Abwicklung von Wertpapiertransaktionen im Allgemeinen und die Abwicklung von systemübergreifenden Transaktionen im Besonderen komplex und teuer.

Eine Blockchain kann man als ein Verfahren beschreiben, mit dem das Eigentum und die Übertragung des Eigentums an nichtmateriellen Vermögensgegenständen dokumentiert werden kann, indem ein Konsens über durchgeführte Transaktionen hergestellt wird. Insofern sollte eine Blockchain grundsätzlich geeignet sein, um Wertpapiertransaktionen abzuwickeln.[25] Allerdings sind die Anforderungen an eine Blockchain in dieser Anwendung andere als etwa bei Kryptowährungen, da Wertpapiertransaktionen regulatorischen und steuerlichen Regeln sowie Datenschutzanforderungen unterliegen, die eingehalten werden müssen (vgl. etwa Seretakis 2017). Das schließt insbesondere eine vollständig anonyme Systemarchitektur aus.

Es sind verschiedene Ausgestaltungsformen denkbar.[26] So könnte etwa die Infrastruktur innerhalb eines Silos auf eine Blockchain übertragen werden. Weit fortgeschritten bei der Implemetierung eines solchen Ansatzes ist die australische Börse. Geplant ist dort eine private Blockchain mit Zugriffsrechten für zugelassene Teilnehmer und Drittparteien mit berechtigtem Interesse (etwa Regulatoren).[27] Bei einer solchen Lösung würden die Geschäftsprozesse und Intermediäre im Wesentlichen unverändert bleiben. Auch die derzeit existierende Fragmentierung würde erhalten bleiben wenn es nicht gelingt, gemeinsame Standards zu entwickeln und zu implementieren.

Als Extremlösung, die die potentiellen Vorteile eines Blockchain-gestützten Wertpapierhandels umfassend nutzt, kann man sich ein System vorstellen, in dem alle

[24] Vgl. auch Cong et al (2019) und Sockin und Xiong (2018).

[25] Wir beschäftigen uns hier nur mit dem Sekundärmarkt. Für eine Diskussion Blockchain-basierter Emissionen auf dem Primärmarkt vgl. Kaal und Evans (2019).

[26] Pinna und Ruttenberg (2016) geben einen Überblick über verschiedene Gestaltungsmöglichkeiten.

[27] Vgl. https://www.asx.com.au/services/chess-replacement.htm. Zugegriffen: 18.6.2020.

Schritte – die Transaktion selbst, das Clearing und das Settlement – durch Einträge in einer Blockchain vorgenommen werden, was einen weitgehenden Verzicht auf Intermediäre bedeuten würde. Im Folgenden diskutieren wir wesentliche Aspekte einer solchen Lösung.

Der vollständig Blockchain-gestützte Wertpapierhandel hat eine Reihe potentieller Vorteile. Der Wertpapierbesitz ließe sich leicht nachverfolgen.[28] Das ermöglicht es auch, durch entsprechend ausgestaltete Smart Contracts Vorgänge wie die Zins- und Dividendenzahlung zu automatisieren. Die Abwicklung wäre deutlich effizienter als im traditionellen Abwicklungssystem. Die bisherige Abwicklung zwei Börsentage nach dem Handelstag könnte durch eine deutlich schnellere Abwicklung oder sogar durch Echtzeit-Abwicklung ersetzt werden. Durch die simultane Ausführung von Wertpapierlieferung und Bezahlung könnten Abwicklungsrisiken reduziert oder sogar eliminiert werden. Eine zentrale Gegenpartei wäre dann nicht mehr nötig.[29] Das ist insofern potentiell bedeutsam, als eine zentrale Gegenpartei Abwicklungsrisiken kumuliert und somit zu einem „Single point of failure" im System werden kann.

Chiu und Koeppl (2019) entwickeln ein theoretisches Modell einer auf dem Proof-of-Work Verfahren beruhenden public unpermissioned Blockchain, die Wertpapierlieferung und Zahlung simultan ausführt. Die Abwicklungsgeschwindigkeit wird variabel gestaltet, indem die Marktteilnehmer eine Gebühr zahlen können, die ihre Transaktion für die Miner attraktiver macht, so dass sie schneller ausgeführt wird. Das Gebührenaufkommen wiederum ist erforderlich, um Anreize für die Miner zu schaffen. Daraus wiederum ergibt sich die Konsequenz, dass die Kapazität der Blockchain begrenzt sein muss – nur wenn es zu Engpässen kommt, werden nämlich Marktteilnehmer bereit sein, eine Gebühr für schnellere Ausführung zu zahlen. Chiu und Koeppl (2019) vermuten, dass eine Koordination der Marktteilnehmer auf ein solches Blockchain-Design schwer zu erreichen sein wird und sehen hier (S. 1750) einen potentiellen Bedarf für regulatorische Eingriffe.

Neben den oben bereits erwähnten Herausforderungen bei der Systemgestaltung – die Beachtung regulatorischer, steuerlicher und datenschutzrechtlicher Anforderungen – ist blockchain-gestützter Wertpapierhandel auch mit potentiellen Risiken und Nachteilen verbunden. Die Effizienzgewinne wären maximal, wenn es nur ein System gäbe. Ein solches System wäre dann aber ein Monopol mit den daraus resultierenden Problemen (ähnlich Benos et al 2017).[30] Ein Übergang zu Echtzeit-

[28] Mit der Möglichkeit, dass Marktteilnehmer in einer für andere Händler anonymen Blockchain durch die Verwendung mehrerer Konten ihre Wertpapierbestände und Transaktionen verschleiern, beschäftigen sich Malinova und Park (2017).

[29] Wenn zwei Parteien Wertpapiere miteinander handeln, trägt der Käufer ein Lieferrisiko und die Verkäuferin ein Zahlungsrisiko. Wenn eine sogenannte zentrale Gegenpartei existiert, wird der Vertrag zwischen dem Käufer und der Verkäuferin durch zwei neue Verträge ersetzt (sogenannte Novation); ein Vertrag zwischen Käufer und zentraler Gegenpartei und ein Vertrag zwischen zentraler Gegenpartei und Verkäuferin. Die zentrale Gegenpartei übernimmt dadurch das gesamte Abwicklungsrisiko und sichert sich selbst wiederum ab, indem sie von den Beteiligten Sicherheitsleistungen verlangt.

[30] An dieser Stelle ist ein Blick in die USA interessant. Dort gibt es zwar zahlreiche Handelsplattformen, das Clearing und Settlement erfolgt aber einheitlich über die Depository Trust & Clearing Corporation (DTCC), deren Besitzer ihre Nutzer sind. Es erscheint allerdings wenig wahrscheinlich, dass eine solche Lösung in Europa ohne regulatorische Eingriffe umsetzbar ist.

Abwicklung würde ebenfalls neue Probleme schaffen. Erstens würde die Zahl der abzuwickelnden Transaktionen dramatisch ansteigen. Derzeit findet nämlich nach Ende eines Handelstages ein sogenanntes Netting statt, bei dem für jeden Clearing-Teilnehmer[31] die Netto-Lieferverpflichtungen und Lieferansprüche aus den Transaktionen eines Tages ermittelt werden. Nur für diese Nettoforderungen findet dann das Settlement statt. Bei Echtzeit-Abwicklung ist ein solches Netting nicht möglich, so dass jede Transaktion „brutto" abgewickelt werden muss. Zweitens ist es bei Echtzeit-Abwicklung nicht mehr möglich, innerhalb eines Tages Leerverkäufe zu tätigen und diese bis zum Ende des Tages glattzustellen. Diese Möglichkeit ist insbesondere für Market-Maker wichtig. Bei Echtzeit-Abwicklung müssten sie statt dessen entweder hohe Wertpapierbestände halten oder durch entsprechende Wertpapierleihgeschäfte jederzeit die Lieferfähigkeit für die Echtzeit-Abwicklung sicherstellen. Dies könnte die Marktliquidität negativ beeinflussen.

Zusätzliche Probleme können sich bei Transaktionen mit derivativen Finanzinstrumenten ergeben. Bei solchen Transaktionen müssen die Marktteilnehmer regelmässig Sicherheitsleistungen (Margins) erbringen. Durch diese Sicherheiten werden bereits entstandene Verluste aus bestehenden Positionen sowie zukünftige Verlustrisiken abgedeckt. Preisveränderungen ziehen Veränderungen der Höhe der erforderlichen Sicherheiten nach sich. Ist ein Marktteilnehmer nicht in der Lage, einer erhöhten Sicherheitsanforderung (einem sogenannten Margin Call) nachzukommen, so wird seine Position zwangsweise glattgestellt. Durch Smart Contracts lassen sich diese Vorgänge automatisiert und in Echtzeit abwickeln. Das hat Vorteile durch die Reduzierung von Gegenparteirisiken, aber auch Nachteile, da die Marktteilnehmer permanent Liquidität für mögliche Margin Calls bereithalten müssen. Im Extremfall – nämlich dann, wenn es zu zwangsweisen Glattstellungen kommt – können adverse Preiseffekte auftreten.

Die vorstehenden Ausführungen zeigen, dass die „revolutionäre" Lösung eines komplett Blockchain-gestützten Handels zahlreiche Probleme mit sich bringt. Das macht es wahrscheinlich, dass in absehbarer Zeit eher „evolutionäre" Lösungen, bei denen nur die Infrastruktur innerhalb bestehender Institutionen auf eine Blockchain übertragen wird, realisiert werden.

3.5 Corporate Governance

Yermack (2017) diskutiert Auswirkungen der Blockchain-Technologie auf die Corporate Governance.[32] Dabei geht seine Argumentation davon aus, dass der Wertpapierhandel vollständig Blockchain-gestützt erfolgt. Wie oben erwähnt lässt sich in diesem Fall der Wertpapierbesitz leicht nachverfolgen. Dies erlaubt es den Emittenten, schnell und kostengünstig mit ihren Aktionären zu kommunizieren. Lafarre

[31] Als Clearing-Teilnehmer bezeichnet man diejenigen Marktteilnehmer, die Mitglieder des Clearinghauses sind und damit direkt an der Abwicklung teilnehmen. Andere Marktteilnehmer, insbesondere alle Privatanleger, nehmen nur indirekt über ihren Broker oder mit diesem verbundene Unternehmen an der Abwicklung teil.

[32] Einen Schritt weiter geht Kaal (2019), der das Konzept einer Blockchain-gestützten Unternehmensorganisation ohne die Notwendigkeit von Prinzipal-Agent-Beziehungen (sogenannte decentralized autonomous organization, DAO) diskutiert. Darauf wird in diesem Beitrag jedoch nicht näher eingegangen.

und Van der Elst (2018) argumentieren, dass die Blockchain-Technologie die Funktion der Hauptversammlung verbessern kann, indem die Kosten der Abstimmungen durch Aktionäre reduziert und die Funktion der Hauptversammlung als Aktionärsforum gestärkt wird.

Wie ebenfalls bereits im vorhergehenden Abschnitt erwähnt, wird Blockchain-gestützter Wertpapierhandel aufgrund der rechtlichen Rahmenbedingungen nicht anonym sein. Es ist daher davon auszugehen, dass zumindest die Aufsichtsbehörden die Identität der Anteilseigner kennen. Dadurch könnte Insiderhandel leichter aufgedeckt werden und die heimliche Akkumulation von Positionen unter Umgehung aufsichtsrechtlicher Meldepflichten würde erschwert. Die Information der Marktteilnehmer über meldepflichtige Wertpapiertransaktionen von Unternehmensinsidern (Directors Dealings) könnte in Echtzeit erfolgen, was die Insiderhandelsgewinne reduzieren und die Informationseffizienz des Marktes erhöhen sollte (vgl. zu letztgenanntem Punkt Betzer et al 2015). Das Umdatieren von Aktienoptionen für Manager (sogenantes Backdating, s. z. B. Lie 2005) würde ebenfalls erschwert, sofern auch die Optionen Blockchain-basiert sind.

Yermack (2017) prognostiziert, dass es vor allem weniger entwickelte Volkswirtschaften sein könnten, die als erste Blockchain-basierten Wertpapierhandel einführen und die resultierenden Governance-Vorteile nutzen. Seine Prognose basiert unter anderem auf der Beobachtung, dass in diesen Ländern die bestehenden Institutionen wenig vertrauenswürdig sind, was die potentiellen Vorteile einer Blockchain-Lösung im Vergleich zu den existierenden institutionellen Rahmenbedingungen erhöht.

4 Ausblick

Zwei zentrale Probleme der gängigen öffentlichen Blockchain-Implementierungen, wie sie auch Bitcoin verwendet, sind der hohe Ressourcenverbrauch und die geringe Skalierbarkeit. Der hohe Ressourcenverbrauch hat mit den im System gesetzten Anreizen und dem Proof-of-Work Konsensmechanismus zu tun. Durch die Vergütung für jeden neu geminten Block kommt es zu einem Gleichgewicht, bei dem die Miner so lange Anreize haben, neue Rechenleistung in Betrieb zu nehmen, bis die Grenzkosten dem Grenzerlös entsprechen. Ein hoher Bitcoin-Preis führt daher dazu, dass auch die Grenzkosten in Form von Elektrizitätsausgaben hoch sind und der Stromverbrauch des Bitcoin-Netzwerks mittlerweile dem Stromverbrauch ganzer Länder entspricht.[33]

Das zweite Problem, die geringe Skalierbarkeit, hängt mit der im Protokoll festgelegten maximalen Blockgröße und der Zeit zwischen zwei Blöcken zusammen. Bei Bitcoin entsteht im Durchschnitt alle 10 Minuten ein neuer Block, der eine maximale Größe von einem Megabyte hat. Dies führt dazu, dass rund 7 Transaktionen

[33] In diesem Kontext sei allerdings nochmals auf das in Fußnote 5 erwähnte „Bitcoin Halving“ verwiesen. In regelmäßigen Abständen wird die Zahl der Bitcoins, die ein erfolgreicher Miner erhält, halbiert. Das wiederum hat Auswirkungen auf den Grenzerlös des Minings (der sich allerdings um weniger als die Hälfte reduzieren wird, da mit einem Rückgang der Intensität des Minings die Wahrscheinlichkeit, mit gegebenem Energieeinsatz erfolgreich einen Block zu minen, steigen wird) und dadurch auch auf den Energieeinsatz und Energieverbrauch.

pro Sekunde durchgeführt werden können. Wenn man das mit den Erfordernissen von typischen Zahlungssystemen wie z. B. Visa vergleicht, liegen diese um mehrere Größenordnungen darüber. Es gibt verschiedene Ansätze, dieses Problem zu lösen. So kann zum einen die Zeit zwischen zwei Blöcken herabgesetzt (vgl. die Kryptowährung Litecoin mit 2,5 Minuten zwischen zwei Blöcken) oder das Größenlimit pro Block erhöht werden (vgl. die Kryptowährung Bitcoin Cash mit derzeit 32 Megabyte pro Block). Beide Möglichkeiten haben allerdings zur Folge, dass die Größe und damit das Speichererfordernis der auf jedem einzelnen Knoten redundant vorgehaltenen Blockchain noch stärker wächst.

Andere Ausgestaltungsarten von Distributed-Ledger-Technologien (DLT) führen nicht zu so hohem Ressourcenverbrauch und sind skalierbarer. Ein Beispiel hierfür ist die Kryptowährung IOTA, die auf eine Kettenstruktur wie sie der Blockchain-Technologie zugrunde liegt, verzichtet. Bei dieser Kryptowährung muss jeder, der eine Transaktion ausführen möchte, andere Transaktionen bestätigen. Diese sind in einem gerichteten azyklischen Graphen abgelegt und die Kernidee ist, dass sie um so sicherer sind, je höher der Anteil der Transaktionen ist, die später auf ihnen aufbauen. Der zugrundeliegende Konsensmechanismus ist aber deutlich komplexer und ein Konsens im noch kleinen Netzwerk aktuell nicht ohne zentralen Koordinator zu erreichen.

Kryptowährungen haben wünschenswerte Eigenschaften (insbesondere die Kombination aus dezentralem Transfer und virtueller Repräsentation), die mit keinem anderen bekannten Zahlungssystem erreichbar sind. Trotzdem ist nach unserer Einschätzung in naher Zukunft nicht mit einer breiten Adaption von „echten“ Kryptowährungen zu rechnen. Hauptgrund hierfür ist der Effizienzverlust, der sich durch eine zusätzliche Währung mit einem von dem der Hauptwährung (dem gesetzlichen Zahlungsmittel) abweichenden Wert ergeben würde. Diesen Nachteil haben Stablecoins (zu denen auch die von Facebook initiierte Kryptowährung Libra gehört) nicht. Allerdings sind Stablecoins durch ein Portfolio von Assets in traditioneller Währung (etwa Staatsanleihen) gesichert und erkennen insofern quasi eine traditionelle Hauptwährung als Benchmark an. Die Adaption von Stablecoins wäre daher ein weit weniger revolutionärer Schritt als die einer „echten“ Kryptowährung.

Die Blockchain-Technologie wird ihre Stärken vor allem über Smart Contracts ausspielen. Diese erlauben es, basierend auf einem breit abgestützten Konsens und abhängig von in der Blockchain hinterlegten und damit nun beobachtbaren Zuständen, detaillierte Regelungen zu treffen. Sie erweitern damit die Möglichkeiten, Verträge abzuschließen. Initial Coin Offerings ermöglichen es kleineren Investoren schon in einer sehr frühen Phase am Unternehmenserfolg zu partizipieren, so von ihrem Expertenwissen zu profitieren und andere zur Nachahmung anzuregen. Ein weiterer Vorteil ist die im Vergleich zu anderen frühen Beteiligungsformen deutlich bessere Handelbarkeit von Kryptomünzen über Kryptobörsen. Ihre duale Rolle als Nutzungsrecht und Wertanlage hilft Plattformbetreibern dabei, die zugrundeliegenden Netzwerkeffekte auszunutzen. Die Wertpapierabwicklung wird, wie erläutert, schon aus regulatorischen Gründen nicht auf eine anonyme Blockchain übertragen werden können. Auch erscheint die Implementierung eines vollständig Blockchain-basierten Wertpapierhandels derzeit wenig realistisch und dürfte ohne regulatorische Eingriffe auch kaum umsetzbar sein. Die in Abschn. 3.5 diskutierten Auswirkun-

gen auf die Corporate Governance börsennotierter Unternehmen beruhen in weiten Teilen auf einem solchen vollständig Blockchain-basierten Wertpapierhandel, so dass auch hier in absehbarer Zeit nicht mit revolutionären Veränderungen gerechnet werden sollte. Dagegen wird es zu Effizienzgewinnen durch Blockchain-basierte Prozesse innerhalb der derzeitigen institutionellen Rahmenbedingungen kommen. Ähnliches gilt im Übrigen auch in anderen, in diesem Beitrag nicht näher diskutierten Anwendungsfeldern wie etwa der Emission von Schuldscheindarlehen.[34]

Zusammenfassend lässt sich sagen, dass der disruptive Charakter der Technologie neben den diskutierten möglicherweise ganz neue Anwendungen entstehen lässt, deren Entwicklung aber mehr Zeit benötigt als eine evolutionäre Verbesserung bestehender Prozesse. Aus diesem Grund ist es gut möglich, dass sich auch 10 Jahre nach Entwicklung der Technologie noch Anwendungen herauskristallisieren, die ein hohes Potential haben, das Wirtschaftsleben zukünftig fundamental zu verändern.

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Funding Open Access funding provided by Projekt DEAL.

Literatur

Amin, A.D. 2020. Blockchain technology in banking and finance sector: Its effects and challenges. *Purakala* 31(13):349–358.

Benos, E., R. Garratt, und P. Gurrola-Perez. 2017. *The economics of distributed ledger technology for securities settlement*. Bank of England staff working paper, Bd. 670

Berentsen, A., und F. Schär. 2017. *Bitcoin, Blockchain und Kryptoassets*. Norderstedt: Books on Demand.

Betzer, A., J. Gider, D. Metzger, und E. Theissen. 2015. Stealth trading and trade reporting by corporate insiders. *Review of Finance* 19:865–905.

Brauneis, A., R. Mestel, R. Riordan, und E. Theissen. 2019. *Bitcoin exchange rates: How integrated are markets?* working paper.

Cartier, K. 1994. The transaction costs and benefits of the incomplete employment contract. *Cambridge Journal of Economics* 18:181–196.

Chen, Y., und C. Bellavitis. 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights* 13:e151.

[34] Siehe für ein Beispiel etwa https://innovationsblog.dzbank.de/2019/05/23/blockchain-plattform-mit-finledger-schuldscheindarlehen-digital-abgewickeln/. Zugegriffen: 18.6.2020

Chiu, J., und T. Koeppl. 2019. Blockchain-based settlement for asset trading. *Review of Financial Studies* 32:1716–1753.
Chohan, U. 2017. *A history of bitcoin*. working paper.
Cong, L.W., und Z. He. 2019. Blockchain disruption and smart contracts. *The Review of Financial Studies* 32:1754–1797.
Cong, L.W., Y. Li, und N. Wang. 2019. *Tokenomics: Dynamic adoption and valuation*. working paper.
Hahn, C., und A. Wons. 2018. *Initial Coin Offering (ICO) – Unternehmensfinanzierung auf Basis der Blockchain-Technologie*. Wiesbaden: Gabler.
Hart, O., und J. Moore. 1999. Foundations of incomplete contracts. *Review of Economic Studies* 66:115–138.
Hayes, A. 2019. The socio-technological lives of bitcoin. *Theory Culture & Society* 36:49–72.
Kaal, W. 2019. *Blockchain-based corporate governance*. working paper.
Kaal, W., und S. Evans. 2019. Blockchain-based securities offerings. *UC Davis Business Law Journal* 20:89–109.
Kocherlakota, N.R. 1998. Money is memory. *Journal of Economic Theory* 81:232–251.
Labazova, O., T. Dehling, und A. Sunyaev. 2019. *From hype to reality: A taxonomy of blockchain application*. Proceedings of the 52nd Hawaii International Conference on System Sciences., 4555–4564.
Lafarre, A., und C. Van der Elst. 2018. *Blockchain technology for corporate governance and shareholder activism*. European Corporate Governance Institute working paper, Bd. 390/2018
Lee, J., T. Li, und D. Shin. 2019. *The wisdom of crowds in fintech: Evidence from initial coin offerings*. working paper.
Li, J., und W. Mann. 2018. *Initial coin offerings and platform building*. working paper.
Lie, E. 2005. On the timing of CEO stock option awards. *Management Science* 51(5):802–812.
Malinova, K., und A. Park. 2017. *Market design with Blockchain technology*. working paper.
Menger, C. 1871. *Grundsätze der Volkswirthschaftslehre*. Wien: Braumüller.
Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Zugegriffen: 18.6.2020.
Narayanan, A., J. Bonneau, E. Felten, A. Miller, und S. Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: A comprehensive introduction*. Princeton: Princeton Univers. Press.
Nikolić, I., A. Kolluri, I. Sergey, P. Saxena, und A. Hobor. 2018. *Finding the greedy, prodigal, and suicidal contracts at scale*. Proceedings of the 34th Annual Computer Security Applications Conference., 653–663.
OECD. 2018. *Financial markets, insurance and private pensions: Digitalisation and finance*. working paper.
Pinna, A., und W. Ruttenberg. 2016. Distributed ledger technologies in securities post-trading. ECB occasional paper 172. https://ssrn.com/abstract=2770340. Zugegriffen: 16.6.2020.
Pirrong, C. 2019. Will blockchain be a big deal? Reasons for caution. *Journal of Applied Corporate Finance* 31(4):98–104.
Schmeling, M. 2019. *What is Libra? Understanding Facebook's currency*. working paper.
Securities and Exchange Commission. 2017. Report of investigation pursuant to section 21(a) of the securities exchange act of 1934: the DAO. wwwBitcoinOrg. https://www.sec.gov/litigation/investreport/34-81207.pdf. Zugegriffen: 18.6.2020.
Segal, I. 1999. Complexity and renegotiation: A foundation for incomplete contracts. *Review of Economic Studies* 66:57–82.
Seretakis, A. 2017. *Blockchain, securities markets and central banking*. working paper.
Sockin, M., und W. Xiong. 2018. *A model of cryptocurrencies*. working paper.
strategy&, PwC, und Crypto Valley. 2018. *Initial coin offerings – eine strategische perspektive. Juni 2018 Edition*
Tapscott, A., und D. Tapscott. 2017. How blockchain is changing finance. *Harvard Business Review* 1(9):2–5.
Voshmgir, S. 2019. *Token economy: How blockchains and smart contracts revolutionize the economy*. Berlin: BlockchainHub.
Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21(1):7–31.