Blockchain-Technologie

Anwendungsbereiche und Betrachtung ausgewählter rechtlicher Aspekte

Seminararbeit von Jonas Häder und Taihao Zhang

Datum: 3. Januar 2020

Darmstadt

TECHNISCHE
UNIVERSITÄT
DARMSTADT

FB Rechts- und
Wirtschaftswissenschaften
FG Bürgerliches Recht und
Unternehmensrecht

Blockchain-Technologie
Anwendungsbereiche und Betrachtung ausgewählter rechtlicher Aspekte

Seminararbeit von Jonas Häder und Taihao Zhang

Datum: 3. Januar 2020

Darmstadt

Erklärung zur Arbeit gem. § 22 Abs. 7 und § 23 Abs. 7 APB TU Darmstadt

Hiermit versichern wir, Jonas Häder und Taihao Zhang, die vorliegende Seminararbeit gemäß § 22 Abs. 7 APB der TU Darmstadt ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
Uns ist bekannt, dass im Falle eines Plagiats (§ 38 Abs. 2 APB) ein Täuschungsversuch vorliegt, der dazu führt, dass die Arbeit mit 5.0 bewertet und damit ein Prüfungsversuch verbraucht wird.
Bei der abgegebenen Arbeit stimmen die schriftliche und die elektronische Fassung gemäß § 23 Abs. 7 APB überein.

Darmstadt, den 3. Januar 2020

(J. Häder)

(T. Zhang)

Urheberschaft

Zwecks der Zuordnung der Abschnitte für die Benotung dieser Seminararbeit vermerken die Autoren die jeweils von ihnen verfassten Abschnitte mit ihren Initialen.

	Autor	Matr.-Nr.	Studiengang	
jh	Jonas Häder	2645515	Wirt.-Inf.	B.Sc.
tz	Taihao Zhang	2884130	Wirt.-Ing./ Bauing.	B.Sc.

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Seminararbeit die Sprachform des generischen Maskulinums angewandt. Es wird an dieser Stelle ausdrücklich darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form geschlechtsunabhängig zu verstehen ist.

Inhaltsverzeichnis

Forschungsfrage[jh, tz]

Nicht selten wird die Blockchain-Technologie als „eine der [...] revolutionärsten Erfindungen“ gepriesen, „gleich dem Internet oder der Elektrizität.“ [1] Sie soll sicher sein, transparent sein, und unveränderlich sein.

Doch ist die Blockchain-Technologie in ihrer Funktionsweise und ihren potentiellen Anwendungen innerhalb Europas noch recht unerforscht.

Im Folgenden soll anhand von ausgewählten Anwendungsbeispielen und Problemstellungen erläutert werden, wie Blockchain-Technologie grundsätzlich funktioniert und wie sie eingesetzt werden kann – oder bereits eingesetzt wird.

Die Arbeit widmet sich der zentralen Fragestellung:

„Wie lässt sich die Blockchain-Technologie in den Markt integrieren?“

[1] Beispielsweise in: Metry, “Blockchain Technology is the Most Significant Invention since the Internet and Electricity”; vergleichbare Zuspitzungen sind u.a. *„Es fühlt sich an wie die frühen Tage des Internets, Web 2.0, Smartphones – alles von Neu an*“ (Sorkin, “Demystifying the Blockchain”)

A. Funktionsweise der Blockchain[jh]

I. Einführung[jh]

Unter dem Begriff Blockchain ist in der Informatik ein Konzept zu verstehen, welches dazu dient verschiedene Datensätze aufzubewahren und deren Integrität im Bereich der Computersystemsicherheit zu gewährleisten.[2]

Jeder Block enthält einen oder mehrere verschlüsselte Datensätze, einen Hashwert, welcher zur Identifikation und Verkettung mit dem nächsten Block dient, und einen Zeitstempel.

Die Blockchain, als Kette aus aneinandergereihten, miteinander verbundenen Datenblöcken, wurde in einem der ersten Anwendungsfälle, Bitcoin, als dezentralisiertes Netzwerk aus einer Vielzahl von Knoten realisiert.[3]

Das dezentralisierte Netzwerk dient dem Zweck, das „Problem der byzantinischen Generäle“ zu lösen, in dem über die verschiedenen, am Netzwerk angeschlossenen Knoten ein Konsensalgorithmus

[2] Burgwinkel, *Blockchain Technology - Einführung für Business- und IT Manager*, S. 5.

[3] Rasinski, *Blockchain-Technologie : Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte*, S. 4–6.

ausgeführt wird.[4]

Unter dem „Problem der byzantinischen Generäle“ ist ein Problem zu verstehen, bei dem sich die verschiedenen Teilnehmer eines Netzwerkes nicht sicher sein können, ob die Informationen die sie erhalten zuverlässig sind oder nicht.

Abstrakt beschreibt das Problem den Fall, dass eine Mehrzahl von Generälen mit ihren Armeen eine Stadt erobern wollen. Dies ist aber nur möglich, wenn sie sich alle auf den selben Schlachtplan einigen, zum selben Moment angreifen. Die Faktoren die dies verhindern können, sind sowohl die Boten, welche falsche Informationen übermitteln können, als auch Generäle, welche Verräter sein können.[5]

Die Parallele zur Blockchain ist, dass falls falsche Informationen versucht eingespeist zu werden, das heißt Blöcke mit Datensätzen an die Blockchain anzuhängen, welche ungültige Informationen enthalten, das Netzwerk dafür sorgen muss, dass alle Knoten die selben, wahren Informationen erhalten. Dies geschieht über den Konsensalgorithmus.

Die genaue Implementierung eines Konsensalgorithmus orientiert sich an der konkreten Problemstellung des Einsatzbereiches.

Da die Blockchain-Technologie weder auf nur eine Weise dargestellt oder implementiert werden kann und sie in der Lage ist komplexe Probleme, wie das „Problem der byzantinischen Generäle“, durch Anwendung verschiedener informationstechnischer, kryptographischer Werkzeuge zu lösen, ergeben sich für sie eine Vielzahl von Anwendungsmöglichkeiten und Anwendungsbereichen.

4 Michèle, “Blockchain Technology”, S. 1–2.
5 Lamport, Shostak und Pease, “The Byzantine Generals Problem”.

II. Kryptographische und mathematische Grundlagen[jh]

Oben genannte kryptographische und mathematische Bestandteile der Blockchain sind Hashfunktionen, um Hashwerte zu bestimmen, und Konsensalgorithmen.

Eine Hashfunktion ist eine mathematische Funktion, deren Zweck es ist eine große Eingabemenge auf eine kleinere Ergebnismenge abzubilden. Da sie in der Blockchain zur Identifikation und Verkettung dient, sollte jeder Hashwert pro Block eindeutig sein. Um das zu erreichen gibt es einige Bedingungen, die eine Hashfunktion erfüllen sollte.

Die Hashfunktion sollte kollisionsfrei sein. Kollisionsfrei bedeutet, dass zwei verschiedene Werte aus der Eingabemenge niemals auf den selben Wert in der Ergebnismenge abgebildet werden. Dies gewährleistet, dass die Hashwerte in den Blöcken eindeutig sind. Des weiteren sollte die Hashfunktion leicht zu berechnen sein, hat man die zu hashenden Daten und die Hashfunktion gegeben. Leicht zu berechnen bedeutet in der Kryptographie, dass es in polynomialer Zeit bestimmbar sein muss.[6]

Der Konsensalgorithmus wird an Hand des Beispiels der Kryptowährung Bitcoin erklärt. Der dort zur Anwendung gebrachte Konsensalgorithmus wird als Proof-of-Work (PoW) bezeichnet. Bei dem PoW Konzept wird einem Rechner oder einem Netzwerk aus Rechnern eine Aufgabe gestellt, ein „mathematisches Puzzle." Aufgabe der Rechner ist es das Puzzle zu lösen und die Lösung

6 Wätjen, *Kryptographie - Grundlagen, Algorithmen, Protokolle*, S. 93–97.

an das Netzwerk zu senden.[7] Diese Puzzle bestehen daraus einen zu hashenden Wert so zu erweitern, dass der daraus folgende Hashwerte einem bestimmten Kriterium unterliegt, geringer als ein bestimmter Wert zu sein. Somit ist das Ergebnis schwer berechenbar, aber leicht nachweisbar.[8]

[7] Rasinski, *Blockchain-Technologie : Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte*, S. 8–9.

[8] Franco, *Understanding Bitcoin - Cryptography, Engineering and Economics*, S. 101–105.

B. Anwendung von Blockchain

I. Anwendung in Kryptowährungen[jh]

Um die Anwendung von Blockchain-Technologie in Kryptowährungen zu veranschaulichen, werden die Anwendungsweise und Anwendungsaspekte der Blockchain-Technologie in drei der größten, mit dem höchsten Marktkapitalisierungswert, Kryptowährungen dargestellt und erläutert. Diese sind Bitcoin, Ethereum und EOS (XRP).[9]

Bitcoin ist zurzeit die größte Kryptowährung und auch zugleich die älteste, erstellt 2009 von Satoshi Nakamoto.[10] Deswegen wird Bitcoin im folgenden als erstes Beispiel behandelt.

Die Blockchain von Bitcoin ist wie folgt aufgebaut: Es gibt einen Ursprungsknoten, von welchem aus neue Knoten in chronologischer Reihenfolge angehängt und verkettet werden. Würde man jeweils den vorherigen Knoten beginnend vom neusten Knoten folgen, so würde man schließlich am Ursprungsknoten ankommen. So entsteht eine fortwährende Kette an Datensätze, welche jegliche

9 CoinLore, *Cryptocurrency List*.

10 Furneaux, *Investigating Cryptocurrencies - Understanding, Extracting, and Analyzing Blockchain Evidence*, S. xxiii.

Transaktionen über Bitcoin festhält.

Unterschiede der Blockchain zur allgemeinen Funktionsweise (siehe *Einführung*, S. 2) sind, dass als dezentralisiertes peer-to-peer Netzwerk „forking“ auftreten kann und die genaue Implementierung des Konsensalgorithmus PoW. Forking tritt auf, wenn zwei Knoten des Netzwerkes auf unterschiedliche Lösungen kommen, diese aber gleichzeitig versuchen ihren Block an die Blockchain anzuhängen. Lösung des Problems ist bei Bitcoin immer die längere Kette als richtige Kette anzusehen. Wenn zwei Knoten ihre Blöcke gleichzeitig senden, so werden zuerst beide Blöcke angehängt. Der nächste gesendete Block entscheidet sich dann, an welchen der beiden Blöcke er seinen neuen Block anhängt. Somit ist eine der beiden Ketten länger und wird als korrekte angesehen.[11]

Ethereum, die zurzeit zweitgrößte Kryptowährung, ist auch eine Blockchain, unterscheidet sich aber in Form und Funktion stark von Bitcoin, da sie noch weitere Funktionen ausführt als eine Kryptowährung zu sein. Neben der die Transaktionen enthaltende Blockchain, gibt es auch einen „World State“, welcher sich mit jedem, aus mehreren Transaktionen bestehenden, Block ändert. Der World State enthält alle Objekte in Konten in Ethereum als Objekte. Ethereum ist als dezentralisiertes Netzwerk zu verstehen, welches das ausführen von dezentralen Programmen erlaubt und die Kryptowährung als Zahlungsmittel für das benutzen dieser Funktion verwendet.[12] Es lassen sich mit Ethereum auch „Smart Contracts“ ausführen, welche wesentlich Protokolle sind, die die Bedingungen von Verträgen überprüfen und einhalten.[13]

Anhand von EOS, zurzeit siebtgrößte Kryptowährung, soll ein

11 Tomov, “Bitcoin: Evolution of Blockchain Technology”.

12 Kindler, *Towards a Toolchain for Exploiting Smart Contracts on the Ethereum Blockchain*, S. 10–26.

13 Ebd., S. 1–2.

weiterer Konsensalgorithmus dargestellt werden, Proof-of-Stake (PoS).[14] Im Proof-of-Stake werden statt dem lösen von Aufgaben, von den Nutzern verlange ein Teil ihres Vermögens zu setzen. Teilnehmer werden nach einem bestimmten Verfahren ausgewählt und müssen entscheiden, ob ein neu hinzugefügter Block gültig ist. Sollte während des Auswahlverfahrens festgestellt worden sein, dass der Teilnehmer die Richtigkeit der Blockchain manipulieren wollte, so wird sein gesetzter Anteil ihm weggenommen, ansonsten wird er entlohnt. Vorteil gegenüber des PoW ist es, dass es nicht zu einem Wettbewerb kommt, wer die meisten Blöcke bestätigt und somit verhindert wird, dass durch Besitz des Großteils des Netzwerkes mutwilliges manipulieren möglich ist.[15]

1. Risiken von Kryptowährungen[jh]

Als neuartige Technologie birgt Blockchain Risiken, auf welche sich der Markt vor der Regulierung, und gegebenenfalls der Einführung, vorbereiten muss. Je nach Etabliertheitsgrad des Feldes, in dem innovative Blockchain Anwendungen eingesetzt werden, können Fehleinschätzungen gravierende Folgen haben. Da Kryptowährungen für den Finanzmarkt und den Geldmarkt geschaffen worden sind, gibt es dementsprechend Risiken die zu beachten sind.

Im Jahr 2018 haben sich die Regierungschefs und Finanzminister der G20 Länder getroffen und verschiedene Risiken von Kryptowährungen besprochen, welche sich alle auf den Finanzmarkt beziehen und den Finanzmarkt negativ beeinflussen könnten.

14 Stergiou, *EOS Cryptocurrency Initial Coin Offering: A case study : How the EOS cryptocurrency raised more than $4.4 billion in its 2017 ICO*, S. 67.

15 Maung Maung Thin u. a., “Formal Analysis of a Proof-of-Stake Blockchain”.

Dazu gehören der Schutz von Anlegern und Verbrauchern, das Verhindern von Terrorismusfinanzierung und Geldwäsche, sowie Steuerhinterziehung. Für diese Punkte wurde entschieden, dass weitere Regulierungen stattfinden werden.[16]

In verschiedenen Regionen gibt es bereits Regulierungen oder Pläne für Regulierungen. Innerhalb Deutschlands und der EU wurden Pläne und Regulierungen innerhalb eines Reports dargestellt. (siehe *Blockchain als regulierte Technologie*, S. 26) China, Indonesien und Indien haben sich dafür entschieden verschiedene Aktivitäten im Bereich der Krypto-Assets zu verbieten. In China sind Kryptowährungen und auch Initial Coin Offerings gänzlich verboten.[17] Die Teilnehmer haben sich geteilt in Länder die offen für einen Krypto-Asset-Markt sind (Australien, Deutschland, Frankreich, Italien, Japan, USA, Brasilien, EU, Großbritannien, Kanada, Mexiko, Russland, Saudi Arabien, Südkorea, Türkei) und welche die es nicht sind. (China, Indien, Indonesien)

Argentinien und Südafrika haben sich nur für Meldungen verdächtiger Transaktionen im Bezug auf Krypto-Assets bereiterklärt.

Für Krypto-Asset-Märkte wurden weitere Klassifizierungen von Risiken gefunden. Diese sind Marktliquiditätsrisiken, Volatilitätsrisiken, Leverage-Risiken und technische und operationelle Risiken. Marktliquiditätsrisiken zeigen das Problem auf, dass es nicht immer möglich sein wird die eigenen Krypto-Assets zu liquidieren und deswegen das Kapital gegebenenfalls nicht verwendet werden kann.

Volatilitätsrisiken beschreiben den Fakt, dass die Preise von verschiedenen Kryptowährungen extrem stark geschwankt sind und

16 Read, “Positionierung der G20 zu globalen Risiken durch Krypto-Assets”, S. 896.

17 Ebd., S. 899.

Krypto-Assets daher keine sichere Anlagequelle sind.

Sollten diese dem Volatilitätsrisiko ausgesetzten Kryptowährungen mit Fremdkapital finanziert werden, so entstehen Leverage-Risiken. Dies kommt vom Leverage-Effekt aus dem Finanzwesen, durch welchen sich anhand von unterschiedlichen Zinssätzen von Fremdkapital und Eigenkapital die Gesamtrentabilität einer Investition erhöhen kann, wenn sich der Anteil an Fremdkapital erhöht. Da dies aber eine Hebelwirkung darstellt ist es auch dementsprechend möglich, die Rentabilität zu senken, besonders anfällig bei hoher Volatilität.

Technische und operationelle Risiken sind auf den Aspekt der digitalen Sicherheit bezogen. Die Plattformen, welche Krypto-Assets kaufen, verkaufen und verwalten sind anfällig für Betrug und Hackerangriffe, wodurch Verluste bei Marktteilnehmern entstehen können.[18]

Als eines der ersten Treffen der G20 Länder in denen Krypto-Asset-Märkte und ihre Risiken einen großen Teil der Themen eingenommen haben, hat sich gezeigt, dass viele Risiken aus bekannten Themenfeldern sich auf Krypto-Assets übertragen lassen, technische und operationelle Risiken und Volatilitätsrisiken, sowie das Risiko von Steuerhinterziehung.

Aus dem Treffen lässt sich schlussfolgern, dass durch die verschiedenen Wege mit denen Krypto-Asset-Märke behandelt werden ein global standardisierter Handel aller Nationen mit Krypto-Assets nicht stattfinden wird.

Teilnehmer die bereits Regulierung eingeführt habe, welche keinem Verbot entsprechen und Teilnehmer die in den Regulierungs-

[18] Read, “Positionierung der G20 zu globalen Risiken durch Krypto-Assets”, S. 899.

vorbereitungen sind, sind geographisch nicht auf eine Region konzentriert, weshalb ein internationaler Handel mit vielen Teilnehmern dennoch möglich sein wird.

II. Anwendung außerhalb von Kryptowährungen tz

Es ist nicht von der Hand zu weisen, dass die Blockchain-Technologie erstmals ins Leben gerufen wurde, um die Kryptowährung Bitcoin zu realisieren.[19]

Dennoch birgt die Blockchain-Technologie einige unschätzbare Eigenschaften, wie zum Beispiel die Unveränderlichbarkeit der Transaktionen, oder dass keine Intermediäre erforderlich sind, denen gegenüber die Nutzer Vertrauen aufbringen müssen.

Eine weitere Eigenschaft der Blockchain liegt darin, dass sie robust gegenüber Ausfällen von einzelnen Netzwerkknoten ist. Fällt also ein der Blockchain angehöriger Rechner einem Hacker-Angriff zum Opfer, dann hat dies keine Auswirkungen auf die fortbestehende Funktionalität des dezentralen Netzwerkes als Ganzes.[20]

Diese grundlegenden Eigenschaften der Blockchain erlauben es ihr, in den verschiedensten Bereichen zur Anwendung zu kommen – beispielsweise stets dann, wenn eine Dezentralisierung des Einflusses, den eine einzelne Person sonst haben würde, von hoher Notwendigkeit ist.

Im diesem Abschnitt werden verschiedene Anwendungsbereiche außerhalb von Kryptowährungen aufgeführt und in einfacher Weise deren Vor- und Nachteile, sowie gegebenenfalls deren Realisierbarkeit diskutiert.

19 Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”.

20 Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology”, S. 3.

1. Blockchain-Technologie in der Medizin[jh]

Im Bereich der Medizin gibt es verschiedene Probleme, die nicht optimal gelöst werden. Für diese Probleme gibt es Ansätze und Ideen, wie man diese mit Hilfe von Blockchain-Technologie lösen kann oder wie sie bereits gelöst werden. Eines dieser Probleme ist die Verbreitung gefälschter Arzneimittel, um Kosten bei der Produktion zu sparen oder in für das Unternehmen unqualifizierte Märkte einzutreten. Da das verbreiten und verabreichen von gefälschten Arzneimittel große gesundheitliche Risiken mit sich trägt, gibt es bereits Prozesse um dies zu verhindern, trotzdem werden solche Arzneimittel weiterhin in signifikantem Maße hergestellt und verbreitet. Vorgestellt wurde ein Ansatz, mit welchem die Rückverfolgbarkeit solcher Arzneimittel garantiert werden soll.[21]
Das in der ”2019 11th International Conference on Communication Systems and Networks”vorgestellte Konzept zur Sicherung der Rückverfolgbarkeit gefälschter Arzneimittel stellt eine Ansatz vor, in welchem zur Rückverfolgbarkeit relevante Daten anhand einer bitcoinähnlichen Blockchain zugänglich gemacht und gespeichert werden. Arzneimittelproduzenten werden bei dem Hinzufügen von Blöcken anhand eines spezifischen QR-Codes (Quick Response Code) und ihrem Public-Key, welcher zur Zugriffsverifikation und Signatur der Daten verwendet wird, identifiziert. Die Daten werden verschlüsselt gespeichert. Zur Bildung der Blockchain werden pro Block der Hashwert des vorherigen Blocks gespeichert, gleich der Bitcoin Blockchain.
Zugang zur Blockchain sollen nur legitime Hersteller von Arzneimitteln erhalten, dementsprechend wäre dieser Ansatz der

[21] Kumar und Tripathi, “Traceability of counterfeit medicine supply chain through Blockchain”, S. 568.

Blockchain kein dezentralisierter, sondern müsste von einer Zertifizierungsstelle überprüft, instand gehalten und verifiziert werden müssen.

Arzneimittelhersteller müssen Informationen wie Name, Herstellungsort, Herstellungszeit, Zutaten, wie man die Arzneimittel verwendet und Nebeneffekte der Einnahme angeben. Damit diese Daten dann auch in der Blockchain angezeigt werden, müssen sie als Hersteller und der Herstellungsprozess von der Zertifizierungsstelle verifiziert werden. Dieser Prozess könnte über Smart Contracts ablaufen, welche überprüfen, ob alle nötigen Faktoren vorhanden sind.

Auf der anderen Seiten können legitimierte Nutzer wie Privatpatienten und Krankenhäuser mit Hilfe der öffentlich bereitgestellten Public-Keys auf jeweilige Informationen zugreifen.[22]

Durch eine einheitliche Zertifizierungsstelle ist dieses System nicht dezentralisiert. International gibt es bereits implementierte Systeme, die ein dezentralisiertes Gesundheitssystem fördern und ermöglichen.

In Estland wird eine Blockchain verwendet, um die medizinischen Akten von Patienten in Echtzeit für Ärzte und Krankenhäuser verfügbar zu machen. Die Integrität und Sicherheit der Daten wird von dort zuständigen Instanzen gewährleistet. Durch den Austausch dieser Daten in Echtzeit wird die Diagnose und Behandlung von Patienten beschleunigt, da keine weiteren Maßnahmen für die Beschaffung der Daten nötig ist.[23]

Ein dezentralisierter Austausch von medizinischen Patientenakten und Zugriff auf medizinische Patientenakten kann die Dauer

22 Kumar und Tripathi, “Traceability of counterfeit medicine supply chain through Blockchain”, S. 569.

23 Novikov u. a., “Blockchain and Smart Contracts in a Decentralized Health Infrastructure”, S. 699.

einer Behandlung und die Verzögerung bis zum Beginn der Behandlung signifikant verringern. Zudem würde ein Verlust von Daten eines Knoten, eines Krankenhauses oder eines Arztes, durch Umweltkatastrophen, Stromausfälle oder Hackerangriffen keinen kompletten Verlust der Daten über einen Patienten bedeuten, da diese dezentral gespeichert sind. Bei einer anonymisierten Datenspeicherung können solche Daten auch für Forschungszwecke verwendet werden, ohne sie speziell für eine Studie erneut erheben zu müssen.

Innerhalb Deutschlands kann sich somit die Verwendung einer dezentralisierten Blockchain als sinnvoll erweisen. Jedoch zählen in Deutschland die medizinischen Patientenakten nach § 9 Abs. 1 DSGVO zu den „besonderen Kategorien personenbezogener Daten“ und unterliegen somit verschiedenen gesetzlichen Richtlinien. Sie dürfen nach § 9 Abs. 2 Buchstabe h DSGVO zwar verarbeitet werden, jedoch könnte bei einer dezentralisierten Datenbank das Problem auftreten, dass die Daten ungewollt an Dritte freigegeben, die nach § 9 Abs. 3 DSGVO nicht der Geheimhaltungspflicht entsprechen, da jeder Teilnehmer die gesamte Blockchain speichern muss, damit ihre Integrität gewährleistet wird.

Die Vorteile der Erweiterung der medizinischen Infrastruktur mit Hilfe einer dezentralisieren Blockchain sind auf kurze Frist ersichtlich, jedoch könnte sich in Deutschland durch die Regulierungen eine standardisierte Einführung dieser Technologie als nicht tragbare Herausforderung herausstellen. Zudem könnten die Daten zwar nach neusten Sicherheitsstandard verschlüsselt werden, sodass selbst bei Zugriff von ungewollten Dritten auf Datensätze innerhalb der Blockchain kein Schaden entsteht und

die DSGVO nicht verletzt wird, jedoch würde sich mit Hilfe von Quantencomputern in Zukunft eine heutzutage sichere Verschlüsselung entschlüsseln lassen.[24]

2. Blockchain-Technologie im Energiesektor[jh]

Blockchain im Energiesektor lässt sich aus zwei Richtungen betrachten, als Technologie die Energie verbraucht und als Technologie die Energie spart. Blockchain-Technologie verbraucht besonders bei Kryptowährungen durch Konsensalgorithmen wie PoW hohe Mengen an Energie.

Um den hohen Verbrauch von Energie durch Blockchain-Technologie in der Zukunft entgegenzuwirken gibt es verschiedene Möglichkeiten um die Blockchain-Technologie in den Energiesektor einzubauen, um effizientere Verwaltung und Verteilung von Stromnetzen zu erlauben, aber auch dem Verbraucher mehr Information darüber zu vermitteln, wie der Strom produziert, gespeichert und verteilt wird.

Zur Verteilung der Energie innerhalb des Stromnetzes gibt es Ansätze die mit Hinblick auf den Klimaschutz vorteilhaft sein können. Einer der Hauptbestandteile von Blockchain-Technologie sind dezentralisierte Netzwerkstrukturen. Um dies auf den Energiesektor anzuwenden kann man ein Peer-to-Peer Netzwerk aus Verbrauchern erstellen, mit dem Zweck den Strom so zu verteilen, dass er der direkten Nachfrage angepasst wird. Kauft ein Teilnehmer Strom in Mengen und verbraucht diesen nicht komplett, so könnte er diesen innerhalb des Netzwerkes weiterverkaufen. Produziert ein Haushalt seinen eigenen Strom so könnte

[24] Mosca, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”, S. 39.

es jeglichen Überschuss weiterverkaufen.

Die Blockchain-Technologie findet ihren Einsatz darin, indem sie eine Blockchain als Plattform anbietet, über die verschiedene Smart Contracts regeln, welcher Strom versendet wird und welcher Strom angenommen wird. Dies beinhaltet Attribute des Stroms, sodass zum Beispiel nur Strom aus erneuerbaren Energien innerhalb des Netzwerkes weitergeleitet und in das Netzwerk eingespeist wird oder nur lokal, innerhalb des Landes, produzierter Strom.

Ein Block würde Transaktionsdaten über Form und Menge erhalten. Das heißt, dass über die im Block gespeicherten Daten erkenntlich gemacht wird, wo der Strom herkommt und wie er produziert wurde und welche Menge an welchen Teilnehmer des Netzwerkes weitergeleitet wurde, damit würde eine komplette Transaktionshistorie entstehen mit der man auch im Nachhinein Herkunft und Verwendung des Stroms überprüfen kann.[25]

Eine effizientere Nutzung und Verteilung könnte das Problem der steigenden Energiekosten durch innovativere und breitere Anwendung von Blockchain-Technologie verringern und den Energiesektor digitalisieren. Somit würden Ersparnisse gemacht werden, ohne weitere Energie zu produzieren, abgesehen von Haushalten, welche ihre eigene Nachfrage decken.

[25] Naveed UL, “Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges and Solutions”, S. 1–3.

3. Blockchain zur Verbesserung des Domain Name Service[tz]

Begriffserläuterung

Beim Domain Name Service (DNS) handelt es sich um ein System, das dazu dient, eine Vielzahl von IP-Adressen den entsprechenden Domain-Namen zuzuordnen. Diesem Vorgang wird eine hohe Wichtigkeit zugeschrieben, weil erst die Domain-Namen eine für den Menschen aufgreifbare Form besitzen – sie sind im allgemeinen Sprachgebrauch als *Webadressen* bekannt. Im Gegensatz dazu haben die IP-Adressen eine rein numerische Form inne, die für den Menschen nur schwierig zu verinnerlichen ist.
Um sicherzustellen, dass diese Zuordnung fehlerfrei vonstatten geht, ist es unter anderem unverzichtbar, dass alle teilhabenden Personen im Einklang darüber sind, welche Domain-Namen bereits vergeben sind, und welche noch zum Erwerb zur Verfügung stünden. Darüber hinaus ist es erforderlich, dass der Nutzer – unabhängig davon, welcher DNS-Server tatsächlich angefragt wird – davon ausgehen kann, stets die identische Antwort zu seiner spezifischen Anfrage zu erhalten.[26]
Wesentliche Komponenten des DNS sind unter anderem die Besitztumsverhältnisse der Domain-Namen; diese müssen auf ständiger Basis gespeichert werden und bei einem Kauf eines Domain-Namen entsprechend transferiert werden. Daran anknüpfend sind außerdem die DNS-Einträge[27] zu speichern. Wie diese Informationseinheiten in einer Blockchain realisiert werden können soll im

[26] Benshoof u. a., “Distributed Decentralized Domain Name Service”, S. 1280.
[27] Bei den sogenannten DNS-Einträgen handelt es sich um die tatsächlichen Datenbankeinträgen, bei denen aus den einzelnen Zeilen die Zuordnung von Domain-Namen zu IP-Adressen hervorgeht.

Folgenden diskutiert werden. Es stellt sich heraus, dass die mit der Blockchain-Technologie grundlegend einhergehenden Eigenschaften wie Dezentralisiertheit und die Gleichheit der Inhalte bei allen Teilnehmern hierbei stark zu Nutzen kommen können.

Kritik am bestehenden DNS

Der bestehende DNS weist verschiedene Schwachstellen auf, unter anderem die Verletzlichkeit gegenüber DDoS-Angriffen,[28] sowie das Problem des DNS-Spoofing;[29] insbesondere aber wird kritisiert, dass der DNS recht zentral gesteuert wird und aufgrunddessen dem Einfluss und auch der Zensur von örtlichen Behörden unterliegt.[30] Es wird der Vorschlag unterbreitet, die Informationen auf eine dezentrale Weise zu speichern und somit zu gewährleisten, dass der Einfluss von Regierungen lediglich geringfügige Maße annimmt.[31]

Ferner wird jedoch darauf hingewiesen, dass der vorgeschlagene *Distributed Decentralized DNS* (D^3NS) keineswegs den bestehenden DNS gänzlich ersetzen kann, denn dieser ist bereits zu weit verbreitet und in seiner jetzigen Form ein integraler Bestandteil des Internets wie wir es heute kennen.[32]

---

28 Bei *Denial of Service Angriffen* (DoS) handelt es sich um einen Versuch, einen Internetdienst zu überlasten und auf diese Weise herbeizuführen, dass er nicht mehr verfügbar ist. Zusätzlich wird bei ***Distributed** DoS Angriffen* (DDoS) diese Unzahl an Anfragen von verschiedenen (virtuellen) Standorten aus durchgeführt, sodass der Angriff schwieriger aufzuhalten oder gar zurückzuverfolgen ist.

29 DNS-Spoofing beschreibt eine Methode, bei der der Angreifer dem DNS korrumpierte Informationen hinzufügt, sodass bestimmte Domain-Namen zu ungewollten IP-Adressen aufgelöst werden; dem Angreifer gelingt es auf diese Weise, dass der Datenverkehr bei ihm passiert und er Information abfangen kann, die nicht für ihn bestimmt waren.

30 Wiefling, Iacono und Sandbrink, "Anwendung der Blockchain außerhalb von Geldwährungen".

31 Benshoof u. a., "Distributed Decentralized Domain Name Service", S. 1279.

32 Ebd., S. 1279.

Im Gegensatz dazu sehen die Autoren jener Arbeit ab, dass D^{3}NS mit dem bestehenden DNS abwärtskompatibel sein wird und es in der Theorie möglich wäre, D^{3}NS schrittweise in den bestehenden DNS zu integrieren. Somit kommt man dem Ziel näher, dass Unternehmen einen tatsächlichen Anreiz haben, D^{3}NS umzusetzen.[33]

Einsatz der Blockchain-Technologie beim D^{3}NS

Zunächst lässt sich feststellen, dass klare Parallelen zwischen den Charakteristiken der Bitcoin-Blockchain und der Blockchain, die beim D^{3}NS zum Einsatz kommen soll, existieren.
So werden in der Bitcoin-Blockchain eine Reihe an Transaktionen gespeichert, die fortlaufend weitergeführt werden. Die in einem vorgegebenen Zeitraum enstandenen Transaktionen werden dann zu einem Block zusammengeführt.[34] Dabei ist maßgebend, dass ein neuer Block nicht ohne den zuvor als gültig erklärten Block zustandekommen kann.
Für die Weiterführung der Bitcoin-Blockchain durch die Miner, die die neuen Blöcke validieren, wird eine Belohnung in Form eines recht hohen Betrages an Bitcoin ausgeschüttet.[35]
Die beim D^{3}NS vorgeschlagene Blockchain soll auf ähnliche Weise verlaufen. Statt der Transaktionshistorie wird die Blockchain dazu genutzt, Besitztumsverhältnisse von Domain-Namen abzuspeichern. Zusätzlich können Einträge auch eine Übertragung des Besitzes eines Domain-Namen verzeichnen. Im Einklang mit der

33 Benshoof u. a., “Distributed Decentralized Domain Name Service”, S. 1279.

34 Bei der Bitcoin-Blockchain beispielsweise beträgt dieser Zeitraum zehn Minuten. Das beim Proof-of-Work zu lösende mathematische Problem wird in seinem Schwierigkeitsgrad alle 2016 Blöcke erhöht, sodass die benötigte Dauer von zehn Minuten kontinuierlich eingehalten wird. (ebd.)

35 Hein, Wellbrock und Hein, *Rechtliche Herausforderungen von Blockchain-Anwendungen*, S. 10.

Bitcoin-Blockchain wird auch hier für das erfolgreiche Minen eines neuen Blocks eine Belohnung ausgeschrieben. Spezifischer besteht der Anreiz zum Minen darin, dass man das Anrecht auf einen neuen, noch nicht vergebenen Domain-Namen erhält.[36]

Stellungnahme

Grundsätzlich ist das von *Benshoof (2016)* vorgestellte Konzept als sehr zielführend und sinnvoll zu erachten, da es die adressierten Problematiken des bestehenden DNS sehr konzis behandelt und die vorgeschlagenen Lösungen, insbesondere die Blockchain-Technologie als Bestandteil des D^{3}NS zu integrieren, ebenfalls plausibel und realisierbar sind.

Tatsächlich jedoch besteht eine Schwierigkeit darin, dass die Weitergabe von Domain-Namen eng mit privaten und öffentlichen Schlüsseln verbunden ist. Dies führt unweigerlich dazu, dass ein gegebener Domain-Name bei Verlust des privaten Schlüssels des vorherigen Besitzers nicht weitergegeben werden kann an einen neuen Besitzer.[37]

Dieser Zusammenhang kann in der Praxis eventuell zu Problem führen. Denn einige Domain-Namen besäßen eine hohe Begehrtheit, sodass eine Vielzahl von Personen nach dem Ableben des vorherigen Besitzers ein Interessen daran hegten, jene Domain-Namen zu erwerben. Die Tatsache, dass dies unter dem D^{3}NS System nicht möglich wäre, stellt in dem Fall eine immense Hürde dar.

Um diesem Problem entgegenzutreten, müssten Maßnahmen getroffen werden, die eine Übertragung des Besitzes auch nach Ver-

[36] Benshoof u. a., “Distributed Decentralized Domain Name Service”, S. 1281.

[37] Ebd., S. 1285.

lust des privaten Schlüssels möglich machen würden. Gleichzeitig jedoch darf nicht die Integrität des Systems gefährdet werden – solche Maßnahmen müssten dagegen abgesichert sein, ausgenutzt zu werden. Es müsste sichergestellt werden, dass sie nur bei tatsächlicher Nicht-Erreichbarkeit des privaten Schlüssels (zum Beispiel nach Tod des Besitzers) zum Tragen kommen würden.
Abschließend sei angemerkt, dass das Konzept des D^3NS insgesamt gute Aussichten für die Zukunft birgt, und lediglich einigen Feinschliffen bedürfe.

4. Blockchain-Einsatz bei der Produktion und dem Transport von Lebensmitteln[tz]

Ausgangslage

Bei der Produktion und dem Transport von Lebensmitteln gibt es sehr hohe und strenge Anforderungen an äußerliche Einflüsse, die es zu kontrollieren gilt. So ist es bei Gemüse, Obst, und Fleischwaren zumeist der Fall, dass sie nicht allzu hohen Temperaturen ausgesetzt werden dürfen, da sonst die Gefahr besteht, dass sie zu rapide verderben ehe sie in die Hände des Endverbrauchers gelangen. Um diesen Anforderungen nachzukommen, und darüber hinaus eine persistente und bis an den Anfang der Produktionskette reichende Zurückverfolgung eines Produktes zu

ermöglichen, gibt es in der Literatur bereits detaillierte Konzepte, die einer höheren Sicherheit in der Lebensmittelproduktion dienen sollen.[38,39,40]

Geeignetheit der Blockchain

Die zu transportierenden Lebensmittel werden mit RFID-Chips[41] ausgestattet, um die Gesamtheit des Produktionsweges zurückverfolgbar abzuspeichern. Auf diese Weise wird garantiert, dass zu jedem Zeitpunkt einsehbar ist, welche Herkunft das Produkt hat, und ob es tatsächlich den gesamten Transportweg über in einer angemessenen Temperatur gekühlt wurde.[42]
Die Eigenschaften der Blockchain sind hierbei von erheblichem Vorteil, da sie ermöglicht, dass alle Teilnehmer stets die identischen Informationen über ein Produkt einsehen können, und es gleichzeitig keinem Teilnehmer möglich ist, unwahre Informationen zu verbreiten.

Stellungnahme

Das Konzept ist grundlegend als sehr positiv zu bewerten, da es der Bevölkerung einen gewissen grad an Zusicherung zukommen lässt, dass die von ihnen erworbenen Lebensmittel auf legitime

38 Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology" in Wiefling, Iacono und Sandbrink, "Anwendung der Blockchain außerhalb von Geldwährungen"
39 Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things".
40 Tse u. a., "Blockchain application in food supply information security".
41 **R**adio **F**requency **ID**entification beschreibt eine Technologie, bei der ein kleiner Chip am zu identifizierenden Objekt (Produkt, Tier, Person, etc...) installiert wird. Der Chip entsendet elektromagnetische Wellen, welche als primitiven Daten aufgefasst werden können. Die Kodierung auf diesem Chip kann anschließend mit eigens dafür geeigneten Geräten ausgelesen oder auch verändert werden.
42 Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things".

Weise produziert, ausgeschöpft, und transportiert wurden, bis hin zum Supermarkt, wo es erworben wird.
Jedoch bringt eine tatsächliche Einführung einer solchen Technologie einige Schwierigkeiten mit sich – so bedürfe es beispielsweise der nahtlosen Teilnahme aller an der Produktionskette beteiligten Personen. Für den Fall, dass auch nur eine Partei ausbleibt, stellt das eine Sicherheitslücke da, da es keine Auskunft darüber gibt, wie die Lebensmittel in jenem Schritt gehandhabt wurden, und ob deren Unversehrtheit noch weiterhin garantiert werden kann. Je nach Höhe der Kosten bei der Ersteinführung einer solchen Technologie ist also nicht zwangsläufig von allen Teilnehmern zu erwarten, dass sie an diesem Prozess partizipieren. Eine weitere Hürde stellt dar, dass die Mehrkosten eventuell auf den Endverbraucher umgeschlagen werden könnten, was wiederum dazu führt, dass Personen, die nicht sonderlich avers den Risiken der Lebensmittelproduktion gegenüber eingestellt sind, schlichtweg nicht diese besagten Produkte kaufen – sie würden die herkömmlichen Produkten erwerben in dem Gedanken, dass es „gut genug“ sei. Für eine tatsächliche Umsetzung dieses Konzeptes gilt es also, die Kosten zu senken und die grundlegende Technologie somit mehr Produzenten und Abnehmern zugänglich zu machen.

III. Blockchain in europäischen Märkten[jh]

1. Blockchain als Regulierungstechnologie[jh]

Basierend auf dem Problem der byzantinischen Generäle (siehe *Einführung*, S. 2) lässt sich die Blockchain-Technologie einsetzen, um Abläufe zu regulieren an denen mehrere Instanzen teilnehmen, welche entweder nicht überwacht werden können oder nicht vertraut werden können.[43]

Solche Abläufe finden finden beim regulieren und überwachen von Märkten statt. Veröffentlicht wurden Ansätze zur Verwendung der Blockchain-Technologie bei diesem Anwendungsfall innerhalb des Reports „BLOCKCHAIN FOR GOVERNMENT AND PUBLIC SERVICES“, des EUBlockchainforum[44], von ConsenSys AG, im Auftrag der europäischen Kommission. Ansätze innerhalb des Reports werden im folgenden erläutert und besprochen.

Für das überwachen von Marktteilnehmern wird von diesen verlangt, regelmäßig Berichte innerhalb des Gesetzesrahmens an zuständige Behörden zu übermitteln, zum Beispiel über einen Jahresabschluss nach § 242 Abs. 1 Satz 1 HGB. Dies setzt ein korrektes Datenerhebungsverfahren innerhalb des Unternehmens voraus und erzeugt eine zeitliche Verzögerung der Daten zwischen dem Zeitpunkt des Erhebens des Marktteilnehmers und dem des Erhaltens der Daten der regulatorischen Instanz. Regulatorische Instanzen sind nicht in der Lage die absolute Korrektheit der von den Teilnehmern erhobenen Daten nachzuweisen, somit eröffnen sich Möglichkeiten des Steuerbetrugs.

Um Blockchain-Technologie zur Unterstützung der im Ablauf des

43 Michèle, “Blockchains as a Regulatable Technology”.
44 *Reports*, S. 16–17.

Überwachens eines Markts vorkommenden Prozesse zu verwenden, bietet sich die Möglichkeit einer Blockchain ähnlich der Blockchain Bitcoins oder ähnlich der Blockchain Ethereums.
Ähnlich der Blockchain Bitcoins würde sich eine Blockchain anbieten, um eine gemeinsame Blockchain zwischen Marktteilnehmer und Marktregulierungsinstanz zu bilden, welche dem Austausch von Daten dient. Diese Daten würden Transaktionsdaten und Buchführungsdaten enthalten.
Somit könnte die Marktregulierungsinstanz in Echtzeit Einsicht über Transaktionen erhalten, welche steuerlich relevant sind und zu bezahlende so wie zu erhaltende Steuern exakter bestimmen. Durch ein automatisiertes Auslesen der Blockchain auf der Marktregulierungsinstanzenseite und einem automatischen einfügen in die Blockchain der Marktteilnehmerseite, wäre es durch die Eigenschaft der Blockchain nicht-kooperative Teilnehmer zusammenarbeiten zu lassen, möglich Steuerbetrug zu minimieren.
Über einen Ansatz einer Ethereum-ähnlichen Blockchain könnten mit Hilfe von Smart Contracts Steuereinzahlungen und Steuerauszahlungen zwischen Marktregulierungsinstanz und Marktteilnehmer komplett automatisiert stattfinden.

2. Blockchain als regulierte Technologie[jh]

Blockchain-Technologie unterliegt europaweit in den Märkten durch seine Neuartigkeit noch nicht vielen Regulierungen. Um Blockchain-Technologie und Kryptowährungen stabil mit dem Markt interagieren zu lassen hat das Bundesministerium für Wirtschaft und Energie eine Strategie entwickelt, in welcher ein rechtlicher Rahmen vorgestellt wird um Krypto-Assets in den Markt

aufzunehmen.[45]

Krypto-Assets ist eine andere Bezeichnung für Kryptowährungen. Gründe des Unterscheidens zwischen Währung und Asset sind, dass diese meist nicht als übliche Währung angesehen und dementsprechend nicht akzeptiert werden und der Wert der Währung sich bis jetzt stetig stark verändert hat.[46]

Die Strategie der Bundesregierung hat als Ziel bis Ende 2021 das Vorhandensein und verwenden von Blockchain-Technologie in Deutschland und Europa zu erweitern. Geplant ist es, Regulierungen für elektronische Wertpapiere einzuführen, sowie für ausgewählte Krypto-Tokens, Anteile von Krypto-Assets auf einer Blockchain, das öffentliche Angebot zu regulieren. Innovationsprojekte sollen gefördert werden, Investitionen ermöglicht, neue Anwendungsfelder getestet und das allgemeine Wissen über Blockchain-Technologie soll verbreitet werden.

Konkret umgesetzt werden soll damit, dass Wertpapiere sich auch in rein elektronischer Form über eine Blockchain speichern lassen sollen, ohne ihre Gültigkeit zu verlieren. Bislang war eine Ausgabe in Papierform Zwang.[47]

Über die Regulierung eines öffentlichen Angebotes ausgewählter Krypto-Tokens wurde beschlossen, dass die Regulierungen europaweit gelten sollen, aber erst auf nationale Regulierung gesetzt wird. Innerhalb dieser Regulierung soll ein hohes Anlegerschutzniveau von Krypto-Tokens erreicht werden. Genauere Angaben darüber, welche Krypto-Tokens ausgewählt werden sollen für die Regulierungen wurden nicht gemacht.

45 *Blockchain-Strategie*.

46 Hu, Rache und Fabozzi, *Modelling Crypto Asset Price Dynamics, Optimal Crypto Portfolio, and Crypto Option Valuation*, S. 1.

47 *Blockchain-Strategie der Bundesregierung*, S. 5–6.

Entgegengesetzt den Anlegern sollen für Handelsplattformen und Krypto-Verwahrer, Anbieter von Dienstleistungen wie dem verwahren von Krypto-Assets, Rechtssicherheit geschaffen werden. Die Einhaltung von Regulierungen von Geldwäsche und Terrorismusfinanzierung mit Hilfe von Krypto-Assets sollen zur Pflicht gemacht werden, die Unternehmer sollen dementsprechend die Möglichkeit bekommen das Recht der Bundesanstalt für Finanzdienstleistungsaufsicht zum Umtauschen von Krypto-Assets in gesetzliche Währung erhalten zu können.[48]

Mit Hilfe von praxisnahen Untersuchungen und Tests sollen für die Blockchain-Technologie neue Anwendungsmöglichkeiten entdeckt und getestet werden und bestehende optimiert werden. Ein gemeinsamer Faktor aller Anwendungsmöglichkeiten ist der hohe Energieverbrauch, der durch das abspeichern großer Datenmengen und einem entsprechend komplexen Konsensalgorithmus entsteht.

Um Innovation auch durch nicht-staatliche Projekte zu fördern, muss ein rechtlicher Rahmen für Investitionstätigkeiten geschaffen werden. Dabei soll der Rahmen technologieneutral betrachtet werden, das heißt die jeweiligen Ausprägungen der Technologie müssen sich vorhandenen Regelungen anpassen, wie der Datenschutz-Grundverordnung (DSGVO). Der Rahmen soll nicht der Technologie angepasst werden.

Zudem es soll besprochen werden, inwiefern sich Blockchain-Technologie einsetzen lässt um eine Beweisführung durchzuführen anhand der Irreversibilität und dem Nachweis der Unveränderbarkeit der Daten. Relevant wäre dies für Urheberrechte und vor Gericht.

48 *Blockchain-Strategie der Bundesregierung*, S. 6–7.

Um auch für neue Unternehmen den Einstieg und die Möglichkeit der Investition in und mit Blockchain-Technologie zu ermöglichen, sollen Standards eingeführt werden. Standards um europaweit, und gegebenenfalls auch international, die selben Schnittstellen für Blockchain-Technologie anwenden zu können. Smart Contracts sollen damit standardisiert ausführbar sein und diese sollen auch offiziell zertifiziert werden.[49]

3. Stellungnahme[jh]

Mit der vorgestellten Strategie bietet die Bundesregierung einen umfassenden, über viele Anwendungsbereiche greifenden, Rahmen an, um die Blockchain-Technologie in den Markt zu integrieren. Trotz dessen wird nur ein sehr unkonkretes Programm geboten, verschiedene Dinge werden nicht weiter erläutert. Die Auswahl der Krypto-Tokens blieb aus und die Gebiete in denen Realtests durchgeführt werden sollen sind nicht näher beschrieben. Aus der Strategie ist zu erkennen, dass unabhängig der konkreten Umsetzung die Blockchain-Technologie in Deutschland und der europäischen Union nicht ohne Regulationen verwendbar sein wird. Die komplette Umsetzung der Strategie ist zurzeit für das Jahr 2021 angesetzt, weshalb eine Prognose bezüglich des Erfolgs auf Grund der unkonkreten Daten nicht präzise möglich ist. Durch den Regulierungscharakter der Strategie lässt sich darauf schließen, dass die Blockchain-Technologie ihre Anwendungsbereiche in Deutschland und der europäischen Union größtenteils im legalen Raum finden wird.

Meine Hypothese lautet daher, dass es deshalb entweder durch eine Überregulierung dazu kommen wird, dass die Blockchain-

[49] *Blockchain-Strategie der Bundesregierung*, S. 8–16.

Technologie nicht, oder nur in Nischenfällen verwendet wird, oder in mäßigem Maße auf dem Markt Verwendung finden wird, aber sich kaum in illegalen Einsatzbereichen finden lässt, obwohl sie unter anderem dafür bekannt ist dort häufig eingesetzt zu werden, durch fehlende Intermediäre bei der Datenübertragung.

C. Rechtliche Aspekte tz

I. Datenschutzrechtliche Herausforderungen der Blockchain tz

Grundlegende und oft als wichtigste erachtete Merkmale der Blockchain sind die (nachträgliche) Unveränderbarkeit der enthaltenen Daten (engl. *Immutability*), die dezentrale und verteilte Registerführung (engl. *Distributed Ledger*), sowie der Aspekt, dass von Seiten der Nutzer ausgehend keiner zentralen Partei blindes Vertrauen entgegengebracht werden muss (engl. *Trustlessness*), und schlussendlich auch die Transparenz[50] der Blockchain.[51,52]

1. Vorhandenheit von *personenbezogenen* Daten tz

Unverzichtbar für die Anwendbarkeit der im Mai 2018 in Kraft getretenen Datenschutz-Grundverordnung der Europäischen Union (DSGVO) ist an erster Stelle die Vorhandenheit von sogenannten

50 Vgl. Art. 5 Abs. 1 lit. a DSGVO
51 Böhme und Pesch, "Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie", S. 473.
52 Marnau, "Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung", S. 1026.

personenbezogenen Daten.[53,54,55]

Als personenbezogen bezeichnet man Daten, die eine natürliche Person identifizieren, oder die unter Zuhilfenahme von zusätzlichen Mitteln für eine solche Identifizierung genutzt werden können.[56] In erster Linie handelt es sich um Daten wie Name oder Geburtsdatum einer Person. Doch auch die im Rahmen der Blockchain-Nutzung verwendeten pseudonymisierten Kennzeichnungen der Nutzer werden in diesem Sinne als personenkennzeichnendes Merkmal aufgefasst, denn Dritte können beispielsweise Ansprüche geltend machen, aus denen Mittel hervorgehen würden, die anschließend eine solche Identifizierung ermöglichen.[57]

Außerdem sind auch die Informationen zu Transaktionen als personenbezogene Daten zu verstehen. Ganz gleich, ob ein öffentliches Blockchain-Netzwerk vorliegt oder ein privates mit Zulassungsbeschränkung.[58,59]

2. Veranwortliche Stelle[tz]

Bei der herkömmlichen Datenverarbeitung wird die Grundidee verfolgt, dass Daten zentral von einem Unternehmen, einer natürlichen oder juristischen Person, oder einer anderweitig vergleichbarer Einrichtung verwaltet, verarbeitet, und insgesamt gehandhabt werden.[60]

53 Quiel, "Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO", S. 567.
54 Hein, Wellbrock und Hein, *Rechtliche Herausforderungen von Blockchain-Anwendungen*, S. 21ff.
55 Böhme und Pesch, "Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie", S. 478.
56 Vgl. Art. 4 DSGVO
57 Quiel, "Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO", S. 568.
58 Ebd., S. 568.
59 Böhme und Pesch, "Datenschutz trotz öffentlicher Blockchain?", S. 94.
60 Vgl. Art. 4 Nr. 7 DSGVO, sowie Erwägungsgrd. 79 DSGVO

Auf diese Weise gehandhabte Daten unterliegen dem ständigen Risiko, dass sie durch die verantwortliche Person zwecktentfremdet werden können, oder anderweitig in die Hände von Dritten gelangen können. Für die Nutzung solcher Dienste geht also vom Endnutzer ein gewisses Vertrauen aus, dass seine Daten sorgfältig und vernünftig aufbewahrt, und auch geschützt werden.
Bei der Blockchain-Technologie gestaltet sich diese Situation insofern anders, dass die in der Blockchain enthaltenen Daten aufgrund der Struktur der Blockchain einer dezentralen Kontrolle unterliegen und somit grundsätzlich jedermann zugänglich sind.[61] Eine zentrale Stelle, die die Daten verwaltet und in dem Sinne auch als endgültigen, letztlich Verantwortlichen zu bezeichnen ist, gibt es in dem Fall nicht.

3. Stellungnahme[tz]

Wie sich bereits zeigt, ist es schwierig, Datenschutzrecht direkt auf die Blockchain-Technologie anzuwenden, da eine Vielzahl von herkömmlichen Begriffen im Datenschutzrecht kein direktes Pendant in der Realität der Blockchain besitzen. Um dennoch einen Datenschutz zu gewähren, ist es folglich nötig, dass speziell für die Blockchain konkrete Gesetze entworfen werden, die sich konkret mit dieser Technologie und ihren Eigenheiten auseinandersetzt. Dabei darf jedoch nicht zu stark in die freien Rechte der Blockchain-Nutzer eingegriffen werden, da die Blockchain sonst beginnen würde, ihren ursprünglichen Reiz zu verlieren. Die neuen Regelungen müssten demnach sicherstellen, dass Begriffe wie *verantwortliche Stelle* und *personenbezogene Daten* unmissverständlich definiert

[61] Böhme und Pesch, “Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie”, S. 478.

werden – gleichzeitig sei darauf zu achten, dass die Pseudonymität der Nutzer nicht verletzt werde, sowie die Nicht-Notwendigkeit eines Intermediärs weiterhin erhalten bleibt.
Nur unter diesen Voraussetzungen ist es möglich, dass die Blockchain auch weiterhin (speziell in der Europäischen Union) ihren Platz hat, und es Unternehmen und Forschern weiterhin möglich ist, verschiedenste Innovationen mithilfe der Blockchain zu realisieren.

II. Blockchain-bezogene Kriminalität am Beispiel der Kinderpornographie[tz]

Die grundlegende Natur der Blockchain ermöglicht es Nutzern, neben der Transaktion von Geldbeträgen ihr auch andere Inhalte beizufügen. Diese können beispielsweise einfacher Text, oder auch Links zu Bildern sein.[62] Bei diesen Links handelt es sich mitunter auch um solche, die auf Seiten, die illegale Pornographie darstellen, verweisen – auch Kinderpornographie ist hierbei enthalten.[63] Eine wesentliche Problematik besteht darin, dass jeder Nutzer der Blockchain lokal eine Kopie der gesamten Transaktionshistorie, und somit auch dieser rechtswidrigen Inhalte, speichert;[64,65] ob nun die alleinige Verwendung der Blockchain in dem Fall eine Straftat, namentlich den Besitz von Kinderpornographie i. S. d. § 184b Abs. 3 StGB, konstituiere, soll im Nachfolgenden diskutiert werden.

Da der Nutzer sich nicht bei jedem der Inhalte der Blockchain sicher sein kann, ob bei den jeweiligen Daten tatsächlich Kinderpornographie enthalten ist, werde die Annahme getroffen, dass ein solcher Fall vorliege.

Es ist eine Unterscheidung vorzunehmen zwischen dem lediglichen Zugang zu solchen Links, sowie dem *eigentlichen* Besitz der dort abrufbaren Kinderpornographie. Für den Tatbestand des Besitzes reicht es nicht aus, den Zugang zu diesem, von einem Dritten bereitgestellten, Link zu haben, da der Nutzer und die

62 Matzutt u. a., "Thwarting Unwanted Blockchain Content Insertion", S. 1.
63 Wieduwilt, "Kinderpornographie in der Blockchain gefunden".
64 Matzutt u. a., "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", S. 1.
65 Böhme und Pesch, "Datenschutz trotz öffentlicher Blockchain?", S. 94.

pornographischen Schriften nicht in einem tatsächlichen Herrschaftsverhalten stünden.[66,67] Ferner setzt dieser Straftatbestand das Tatbestandsmerkmal des Vorsatzes gem. § 15 StGB voraus,[68] was selbst ein Wissen und Wollen der Tatbestandsverwirklichung wiederum voraussetzt.

So ist beispielsweise eine gutgläubige Person, die unwissend eine mit böswilligen Dateien kontaminierte E-Mail öffnet, dadurch nicht im Besitz der durch die Email erhaltenen Dateien.[69] In diesem Zusammenhang lässt sich eine deutliche Parallele zu den in Blockchain enthaltenen Links zu Kinderpornografie ziehen – denn bei Personen, die diese Technologie lediglich zur Transaktion von Geldern verwenden, ist mit hinreichender Plausibilität davon auszugehen, dass sie keinen Vorsatz verfolgen, Besitztum an jener Kinderpornographie zu erlangen. Auch befindet sich nicht zwangsläufig jeder Nutzer von einem technischen Standpunkt aus betrachtet überhaupt in der Lage, diese Inhalte dann tatsächlich aus der Blockchain zu beziehen.

Sämtliche Inhalte der Blockchain im Einzelnen kennen zu müssen, sowie sich derer Legalität sicher sein zu müssen darf also keineswegs Voraussetzung für die Nutzung einer öffentlichen Blockchain sein. Denn im umgekehrten Fall müsste jeder Nutzer stets die strafrechtliche Verfolgung befürchten, sodass die Blockchain nur noch in sehr begrenztem Maße Anwendung finden würde.[70]

66 Hein, Wellbrock und Hein, *Rechtliche Herausforderungen von Blockchain-Anwendungen*, S. 16.
67 Matzutt u. a., "Thwarting Unwanted Blockchain Content Insertion", S. 3.
68 Laufhütte und Roggenbuck, "Dreizehnter Abschnitt: Straftaten gegen die sexuelle Selbstbestimmung", StGB, § 184a Rn. 10.
69 Ebd., StGB, § 184b Rn. 8.
70 Hein, Wellbrock und Hein, *Rechtliche Herausforderungen von Blockchain-Anwendungen*, S. 17.

Stellungnahme

Die Speicherung von (rechtswidrigen) Inhalten in der Blockchain und die theoretische Zugänglichmachung dieser Inhalte stellt einen neuartigen Sachverhalt dar, der sich fortlaufend und mit einer schnelleren Geschwindigkeit weiterentwickelt als der Gesetzgeber mithalten kann. Des Weiteren bedarf es für das Vorliegen einer Straftat in jedem Fall einem Vorsatz, sei es für den Besitz oder der Verbreitung solcher Inhalte. Fest steht, dass in den überwiegend meisten Fällen der Blockchain-Nutzung nicht von einem derartigen Vorsatz auszugehen ist. Vielmehr verfolgen Nutzer das Ziel, finanziellen Wert zu schöpfen.

Hierbei sei natürlich nicht außer Acht gelassen, dass es durchaus Individuen gibt, die das Ziel verfolgen, sich auf diese Weise einen Zugang zu den illegalen Inhalten zu verschaffen. Schließlich gelangten die Inhalte durch gleichgesinnte Nutzer überhaupt erst in das Netzwerk. Es kann also nicht jedem Nutzer ohne weitere Prüfung seine Unschuldigkeit zugesprochen werden. Das andere Ultimatum, dass jedem Nutzer allein durch die Verwendung der Blockchain bedingt der Besitz von illegalen Inhalten unterstellt wird, ist jedoch ebenfalls nicht vertretbar.

Um diesem Dilemma entgegenzutreten, ist es sicherlich angebrachter, an der Quelle zu agieren und überhaupt das Zustandekommen kinderpornographischer Inhalte zu unterbinden. Vom durchschnittlichen Blockchain-Nutzer hingegen ist nicht zu erwarten, dass er auf regelmäßiger Basis die Inhalte der Blockchain untersucht, oder sich derer Rechtmäßigkeit vergewissert.

D. Fazit tz

Die Autoren kommen zu dem Schluss, dass die in dieser Arbeit behandelte Blockchain-Technologie eine noch verhältnismäßig neuartige Technologie darstellt, deren aktueller Stand der Forschung sich mit jedem Tag um große Mengen voranbewegt.
Ihr Etabliertheitsgrad fluktuiert je nach Einsatzbereich, und somit auch die damit einhergehenden rechtlichen Regelungen. Die dargestellten Ergebnisse lassen eine folgende Beantwortung der Forschungsfrage **„Wie lässt sich die Blockchain-Technologie in den Markt integrieren“** zu.
Zum einen gibt es selektierte Bereiche der Industrie, in denen dem Bereich der Forschung und Entwicklung eine höhere Wichtigkeit zukommt als bei anderen Bereichen. Oftmals ist das im Technologiesektor der Fall, oder auch bei Start-Ups, deren Erfolg oder Misserfolg gänzlich von innovativen Geschäftsideen abhängig ist. In solchen Betrieben liegt die Vermutung nahe, dass sie sehr offen gegenüber der Integration und Nutzung von Blockchain-Technologie sind. Sie können sich auf hervorragende Weise die Unveränderlichbarkeit und Unempfindlichkeit der Blockchain zu Nutzen machen.
Auf der anderen Seite jedoch gibt es speziell im Banken- und Finanzwesen viele Unternehmen, die sehr stringenten rechtlichen

Regelungen unterliegen. Für jene Unternehmen ist es eventuell nicht auf Anhieb möglich, die Blockchain-Technologie auf eine Art umzusetzen, wie sie sich eventuell wünschten. In ähnlicher Weise spielt die Frage des Datenschutzes eine wichtige Rolle, speziell in der Europäischen Union ist die Datenschutz-Grundverordnung nahezu unmöglich wegzudenken.

Bis die Blockchain-Technologie sowohl in der Breite als auch in der Tiefe vermehrt Anwendung findet, sowie die durchschnittliche Person über ihre grobe Funktionsweise, Risiken, und Anwendungsbereiche aufgeklärt ist, ist es unweigerlich noch ein weiter Weg. Dieser Weg jedoch wird kontinuierlich geebnet und zugänglicher gemacht, sodass die Autoren zuversichtlich sind, dass schon in der nahen Zukunft die Blockchain ein integraler Bestandteil des Alltags werden könnte.

Sogleich die Blockchain-Technologie als „revolutionärste Erfindung gleich der Elektrizität“[71] bezeichnet wird, so gibt es auch Stimmen am anderen Ende des Spektrums, die hinterfragen, ob Blockchain nicht „eine Lösung auf der Suche nach einem Problem“[72] sei.

Dass solche Kritik seine Daseinsberechtigung hat, ist offenkundig. Jedoch sind Lösungen ohne Probleme nicht gleich verwerflich, besagte Probleme könnten vielleicht schon sehr bald emergieren. Abschließend sei angemerkt, dass die Autoren für die Zukunft der Blockchain mehr neue und spannende Anwendungsbereiche sehen, als sie Probleme mit sich bringen würde.

71 (siehe *Forschungsfrage*$^{jh,\,tz}$, S. 1)

72 Skinner, “Blockchain: A Solution Looking for a Problem?”

Literatur

Benshoof, B., A. Rosen, A. G. Bourgeois und R. W. Harrison (Mai 2016). “Distributed Decentralized Domain Name Service”. In: *2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*. IEEE. DOI: 10.1109/ipdpsw.2016.109.

Blockchain-Strategie (2019). URL: https://www.bundesregierung.de/breg-de/themen/digital-made-in-de/blockchain-strategie-1546662 (besucht am 01. 12. 2019).

Blockchain-Strategie der Bundesregierung (2019). URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=10 (besucht am 01. 12. 2019).

Böhme, R. und P. Pesch (2017a). “Datenschutz trotz öffentlicher Blockchain?” In: *Datenschutz und Datensicherheit - DuD* 41.2, S. 93–98. DOI: 10.1007/s11623-017-0735-x.

– (2017b). “Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie”. In: *Datenschutz und Datensicherheit - DuD* 41.8, S. 473–481. DOI: 10.1007/s11623-017-0815-y.

Burgwinkel, D. (2016). *Blockchain Technology - Einführung für Business- und IT Manager*. 1. Aufl. Berlin: De Gruyter.

CoinLore (2019). *Cryptocurrency List*. URL: https://www.coinlore.com/all_coins (besucht am 24. 11. 2019).

Franco, P. (2014). *Understanding Bitcoin - Cryptography, Engineering and Economics*. 1. Aufl. New York: John Wiley & Sons.

Furneaux, N. (2018). *Investigating Cryptocurrencies - Understanding, Extracting, and Analyzing Blockchain Evidence*. New York: Wiley.

Hein, C., W. Wellbrock und C. Hein (2019). *Rechtliche Herausforderungen von Blockchain-Anwendungen*. 1. Aufl. Wiesbaden: SpringerGabler. DOI: 10.1007/978-3-658-24931-1.

Hu, Y., S. T. Rache und F. J. Fabozzi (2019). *Modelling Crypto Asset Price Dynamics, Optimal Crypto Portfolio, and Crypto Option Valuation*. arXiv: 1908.05419 [q-fin.RM].

Kindler, S. (2019). *Towards a Toolchain for Exploiting Smart Contracts on the Ethereum Blockchain*. URL: http://nbn-resolving.de/urn:nbn:de:bsz:943-opus-5392 (besucht am 26. 11. 2019).

Kumar, R. und R. Tripathi (2019). "Traceability of counterfeit medicine supply chain through Blockchain". In: *2019 11th International Conference on Communication Systems Networks (COMSNETS)*, S. 568–570. DOI: 10.1109/COMSNETS.2019.8711418.

Lamport, L., R. Shostak und M. Pease (1982). "The Byzantine Generals Problem". In: *ACM Transactions on Programming Languages and Systems*, S. 382–401. URL: https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/.

Laufhütte, H. W. und E. Roggenbuck (2009). “Dreizehnter Abschnitt: Straftaten gegen die sexuelle Selbstbestimmung”. In: *Strafgesetzbuch Leipziger Kommentar*. Hrsg. von H. W. Laufhütte, R. Rissing-van Saan und K. Tiedemann. 12., neu bearbeitete Auflage. Bd. 6. Berlin: De Gruyter Rechtswissenschaften Verlags-GmbH.

Marnau, N. (2017). “Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung”. de. In: DOI: 10.18420/IN2017_105.

Matzutt, R., M. Henze, J. H. Ziegeldorf, J. Hiller und K. Wehrle (Apr. 2018a). “Thwarting Unwanted Blockchain Content Insertion”. In: *2018 IEEE International Conference on Cloud Engineering (IC2E)*. IEEE. DOI: 10.1109/ic2e.2018.00070.

Matzutt, R., J. Hiller, M. Henze, J. H. Ziegeldorf, D. Müllmann, O. Hohlfeld und K. Wehrle (2018b). “A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin”. In: *Proceedings of the 22nd International Conference on Financial Cryptography and Data Security*. Springer.

Maung Maung Thin, W. Y., N. Dong, G. Bai und J. S. Dong (2018). “Formal Analysis of a Proof-of-Stake Blockchain”. In: *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, S. 197–200. DOI: 10.1109/ICECCS2018.2018.00031.

Michèle, F. (2018a). “Blockchain Technology”. In: *Blockchain Regulation and Governance in Europe*. Cambridge University Press, S. 1–33. DOI: 10.1017/9781108609708.001.

– (2018b). “Blockchains as a Regulatable Technology”. In: *Blockchain Regulation and Governance in Europe*. Cambridge University Press, S. 34–65. DOI: 10.1017/9781108609708.002.

Mosca, M. (2018). “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” In: *IEEE Security Privacy* 16.5, S. 38–41. DOI: 10.1109/MSP.2018.3761723.

Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. In.

Naveed UL Chau, D. (2019). “Blockchain Technologies for Smart Energy Systems: Fundamentals, Challenges and Solutions”. In: *IEEE Industrial Electronics Magazine*.

Novikov, S. P., O. D. Kazakov, N. A. Kulagina und N. Y. Azarenko (2018). “Blockchain and Smart Contracts in a Decentralized Health Infrastructure”. In: *2018 IEEE International Conference ”Quality Management, Transport and Information Security, Information Technologies”(IT QM IS)*, S. 697–703. DOI: 10.1109/ITMQIS.2018.8524970.

Quiel, P. (Aug. 2018). “Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO”. In: *Datenschutz und Datensicherheit - DuD* 42.9, S. 566–573. DOI: 10.1007/s11623-018-1000-7.

Rasinski, A. (2018). *Blockchain-Technologie : Analyse ausgewählter Anwendungsfälle und Bewertung rechtlicher Aspekte*. Universität Ulm. DOI: 10.18725/OPARU-6891.

Read, O. (2018). “Positionierung der G20 zu globalen Risiken durch Krypto-Assets”. In.

Reports (2018). URL: https://www.eublockchainforum.eu/reports.

Stergiou, D. (2019). *EOS Cryptocurrency Initial Coin Offering: A case study : How the EOS cryptocurrency raised more than $4.4 billion in its 2017 ICO*.

Tian, F. (Juni 2016). “An agri-food supply chain traceability system for China based on RFID & blockchain technology”. In: *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*. IEEE. DOI: 10.1109/icsssm.2016.7538424.

– (Juni 2017). “A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things”. In: *2017 International Conference on Service Systems and Service Management*. IEEE. DOI: 10.1109/icsssm.2017.7996119.

Tomov, Y. K. (2019). “Bitcoin: Evolution of Blockchain Technology”. In: *2019 IEEE XXVIII International Scientific Conference Electronics (ET)*.

Tse, D., B. Zhang, Y. Yang, C. Cheng und H. Mu (Dez. 2017). “Blockchain application in food supply information security”. In: *2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE. DOI: 10.1109/ieem.2017.8290114.

Wieduwilt, H. (23. März 2018). “Kinderpornographie in der Blockchain gefunden”. In: *Frankfurter Allgemeine Zeitung*. URL: https://www.faz.net/aktuell/wirtschaft/diginomics/kinderpornographie-in-blockchain-gefunden-15507813.html (besucht am 18. 11. 2019).

Wiefling, S., L. L. Iacono und F. Sandbrink (Aug. 2017). “Anwendung der Blockchain außerhalb von Geldwährungen”. In: *Datenschutz und Datensicherheit - DuD* 41.8, S. 482–486. DOI: 10.1007/s11623-017-0816-x.

Wätjen, D. (2018). *Kryptographie - Grundlagen, Algorithmen, Protokolle*. 3. Aufl. Berlin Heidelberg New York: Springer-Verlag.