COT Legal // Steinfeld Recht

Claudia Otto
Rechtsanwältin
Bockenheimer Landstraße 2-4
60306 Frankfurt am Main
Telefon: +49 69 667 748 360
Telefax: +49 69 667 748 450
Mail: claudia.otto@cot.legal
Web: https://cot.legal

Mirjam Hannah Steinfeld, Mag. iur., CFE
Rechtsanwältin und
Fachanwältin für Strafrecht
Voelckerstraße 21
60322 Frankfurt am Main
Telefon: 069 24 74 199 30
Telefax: 069 24 74 199 32
Mail: kanzlei@steinfeld-recht.de
Web: www.steinfeld-recht.de

Gemeinsame Stellungnahme vom 18. März 2021

in Vorbereitung der

Sachverständigenanhörung zum

1) Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren" (BT-Drucksache 19/26925)

   sowie

2) Antrag der Fraktion der FDP „Einen innovationsfreundlichen Rechtsrahmen für Kryptoassets schaffen – Digitale Wertpapiere aller Art ermöglichen" (BT-Drucksache 19/26025)

am 22. März 2021

A. Zum Regierungsentwurf

Diese Stellungnahme ergänzt die Stellungnahme zum Referentenentwurf vom 13. September 2020. Die Stellungnahme zum Referentenentwurf ist als **Anlage** beigefügt. Ihr Schwerpunkt liegt auf der Darstellung und Begegnung von Gefahren, die aus der besonderen Machtstellung des registerführenden Emittenten herrühren können. Die Verlagerung der Problematik in eine Rechtsverordnung[1] schafft nicht den erforderlichen Schutz vor Missbrauch. Insbesondere gilt es weiterhin, die auf Seite 7 der Stellungnahme zum Referentenentwurf aufgezeigte Regelungslücke in § 7 eWpG-E zu schließen.

Folgende weitere Vorschläge erscheinen sinnvoll und diskussionswürdig:

I. Entsprechende Anwendung der sachenrechtlichen Vorschriften

Nach § 2 Abs. 3 eWpG-E gilt ein elektronisches Wertpapier, eine unkörperliche, digital gespeicherte Information, als körperlicher Gegenstand. Diese Regelung wirkt unnatürlich im Gesamtgefüge einer einheitlichen Rechtsordnung, auch wenn der Sinn und Zweck gut nachvollziehbar ist. Möglicherweise kann der Widerspruch aufgelöst werden durch eine Verfeinerung des Wortlauts in Orientierung an § 90a BGB, etwa:

> *Ein elektronisches Wertpapier ist keine Sache. Auf das elektronische Wertpapier sind die für Sachen geltenden Vorschriften entsprechend anzuwenden, soweit nicht etwas anderes bestimmt ist.*

II. Der Registerbegriff dürfte mehr Erläuterung brauchen

Der Begriff „Register" im Sinne des Gesetzesentwurfs ist nicht legaldefiniert. Der Gesetzesentwurf unterscheidet lediglich nach zentralem Register und Kryptowertpapierregister (vgl. § 4 Abs. 1 eWpG-E). Beim Studium anderer Stellungnahmen entsteht der Eindruck, dass hier möglicherweise unterschiedliche Vorstellungen vor allem im Hinblick auf das Kryptowertpapierregister vorherrschen und diese Divergenzen auch in Zukunft die Rechtsanwendung maßgeblich beeinflussen können. Die Begründung zu § 7 Abs. 1 (S. 46) verwirrt zusätzlich mit dem Verweis auf „branchenübliche ‚best practices'". Eine Kryptowertpapierregisterführung ist sogar im Blockchain-Netzwerk Bitcoin denkbar. Die §§ 17, 18 eWpG-E stehen dem nicht entgegen.

Grundsätzlich wird eine Legaldefinition für nicht erforderlich und nur bedingt möglich gehalten, weil ein digitales Register viele verschiedene Formen und Gestaltungen annehmen kann. Insofern besteht kein Änderungsbedarf am Gesetzesentwurf selbst. Sinnvolle Hinweise, z.B. welche technischen Implementierungen derzeit möglich sind, könnten in die Gesetzesbegründung aufgenommen werden. Praktikabler erscheint jedoch eine praxis- und risikoorientierte Konkretisierung nach dem Vorbild der MaRisk durch die BaFin auf Grundlage des § 25a KWG.

Eine konkrete Ausgestaltung dieser Anforderungen bedürfte einer tiefergehenden Prüfung.

---

[1] Vgl. Begründung des Regierungsentwurfs, S. 46.

III. Anforderungen an das Kryptowertpapierregister an den Gesetzgeberwillen anpassen

§ 16 Abs. 1 eWpG-E verlangt ein fälschungssicheres Aufzeichnungssystem, in dem Daten gegen unbefugte Löschung sowie nachträgliche Veränderung geschützt gespeichert werden. Das gibt es jedoch nicht in dieser Absolutheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Abschlussbericht zum Projekt 374 vom 29. April 2020 festgehalten:

> *Es existieren so gut wie keine Angebote mit formalen Sicherheitsnachweisen, die wesentliche Teile des Angebots betreffen. Formale Sicherheitsnachweise existieren zwar für die eingesetzten kryptographischen Bausteine wie Verschlüsselungsverfahren oder Signaturfunktionen, viele Blockchain-Angebote versprechen jedoch weit darüber hinausgehende Sicherheitseigenschaften, wie* ***Unveränderlichkeit*** *oder Resistenz gegen Sybil-Angriffe.* ***Für diese Aussagen bestehen in der Regel keine formalen Nachweise oder wissenschaftliche Untersuchungen****.*[2]

Das Problem sind aber weniger die gesetzlichen Anforderungen als der verbreitete Irrglaube, die Blockchain als bekanntester Unterfall der Distributed-Ledger-Technologie (DLT) sei unveränderlich und damit fälschungssicher sowie gegen Löschung und nachträgliche Änderung geschützt. Der Fall von „The DAO" in 2016 hat bewiesen, dass unter bestimmten Umständen unerwünschte Blockchain-Eintragungen rückgängig gemacht werden können („Rollback").[3] Nachvollziehbar ist daher die relativierende Gesetzesbegründung[4], „*fälschungssicher*" soll verstanden werden als „*vor dem Hintergrund des Stands der Technik gegen Fälschungen gesichert*". Der Wortlaut des § 16 Abs. 1 eWpG-E sollte diesem Gesetzgeberwillen angepasst werden:

> *Ein Kryptowertpapierregister muss auf einem ~~fälschungssicheren~~ gegen Fälschungen gesicherten Aufzeichnungssystem geführt werden, in dem Daten in der Zeitfolge protokolliert und gegen unbefugte Löschung sowie nachträgliche Veränderung geschützt gespeichert werden.*

Damit können die Mindestanforderung gehalten und Bezug zur Realität hergestellt werden. Denn die „Sicherung gegen Fälschungen" kann nun ein realistisches Niveau haben und ist daher relativ im Gegensatz zum absoluten „fälschungssicher".

Hilfreich wäre noch eine Erläuterung in der Gesetzesbegründung, welchen Fälschungsbegriff der Gesetzgeber hier zugrunde legt. Denn eine Urkundenfälschung nach § 267 Abs. 1 StGB umfasst auch die Herstellung einer unechten Urkunde. Vor der Herstellung eines „unechten elektronischen Wertpapiers", also eines solchen, bei dem der angegebene Emittent nicht der Emittent ist, schützt eine Blockchain oder vergleichbare Technologie gerade nicht.

---

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html, S. 35 f.
[3] Erläuterung des "Rollbacks" in einfachen Worten: „*to roll back the transactions miners adopt new rules invalidating some valid blocks thus the belonging transactions are also invalid so we cancel these transactions and we go back to the past the previous state. to do so we need a fork. what's happend in the hardfork in case of the Dao is : we forked the chain at the block 1920000 invalidating all the blocks coming after look at the picture below.*",
https://ethereum.stackexchange.com/questions/9535/how-does-a-hard-fork-rollback-transactions.
[4] S. 58.

IV. § 4 Abs. 11 eWpG-E: Der Begriff „Aufzeichnungssystem" ist wenig verständlich

Der Begriff des Aufzeichnungssystems wird im Regierungsentwurf unter § 4 Abs. 11 eWpG-E bestimmt. Hiernach handelt es sich um

> *ein[en] dezentrale[n] Zusammenschluss, in dem die Kontrollrechte zwischen den das jeweilige System betreibenden Einheiten nach einem im Vorhinein festgelegten Muster verteilt sind.*

Erkennbar ist, dass sowohl technische als auch organisatorische Aspekte von Relevanz sein sollen. Das ist grundsätzlich richtig. Es stellt sich jedoch die Frage, ob die Begriffsdefinition nicht klarer und damit besser verständlich gefasst werden kann. Ein Vorschlag wäre:

> *Ein Aufzeichnungssystem ist ein auf Grundlage eines Protokolls zusammenwirkendes Rechnernetzwerk, in dem die Netzwerkbeteiligten gemeinsam Daten verarbeiten.*

B. Zum Antrag (Drucksache 19/26025)

Der Antrag ist missverständlich und verliert sich dem Anschein nach zwischen den im Rahmen des Digital Finance Package vorgeschlagenen Regelungen der Europäischen Kommission.

So ist anzumerken, dass der noch in einem frühen Entwicklungsstadium befindliche Entwurf einer „Markets in Crypto-assets"-Verordnung (MiCAR) ausweislich ihres Art. 2 Abs. 2 lit. a) gerade keine Finanzinstrumente und damit in Verbindung stehende Geschäfte und Personen behandelt. Die MiCAR soll, gleich einem Auffangregelwerk, diejenigen „Kryptowerte" erfassen, die nicht anderweitig geregelt sind oder werden.[5] Art. 4 Abs. 1 Nr. 15 MiFID II („Finanzinstrument") soll um die Klarstellung ergänzt werden,[6] dass Finanzinstrumente auch „mithilfe" der DLT emittiert werden können. So sollen bestehende Regelungslücken geschlossen werden.

Es fehlen Anhaltspunkte, dass die schrittweise Schließung von Regelungslücken eine lähmende Überregulierung darstellt. Wie daneben die unter Bedingungen stehende Ermöglichung der Begebung von Wertpapieren in elektronischer Form „Blockchain-Projekte" in der Realwirtschaft unwirtschaftlich machen soll, bleibt unklar.

I. Zum Beschlussantrag I

1. Zusammenfassung

Die Antragsteller:innen begrüßen den sich noch im frühen Entwicklungsstadium befindlichen Entwurf der MiCAR, halten ihn aber für ebenso hinderlich für die Etablierung von Blockchain-Projekten in der Realwirtschaft. Technologieneutralität im Kontrast zum DLT-Bezug der MiCAR

[5] So bspw. von der Markets in Financial Instruments Directive (Richtlinie 2014/65/EU, MiFID II).
[6] Gemäß Art. 6 des Vorschlags einer Änderungsrichtlinie (2020/0268 (COD).

schreiben die Antragsteller:innen groß. Dennoch brauche es dringend eine Blockchain-fördernde Gesetzgebung.

Die Antragsteller:innen vermuten, dass es an Deutschland liegt, dass „*bisher kaum Initiativen aus der Blockchain-Strategie in tatsächliche Gesetzgebung umgesetzt*" wurden. So brauche der deutsche Gesetzgeber zu lange, um elektronische Wertpapiere einzuführen, deren Zulassungserfordernisse nicht über denen der MiCAR-Vorgaben liegen sollen. Die Bundesregierung soll daher (auch) dafür sorgen, dass die MiCAR-Verordnung mehr im Sinne der Dienstleister ausfällt. Die Antragsteller:innen sehen in der Wartezeit einen Rückschritt für die Nutzung der Blockchain-Technologie. Die Möglichkeiten der Digitalisierung würden vor allem deshalb beschnitten, weil der Entwurf des eWpG keine elektronischen Aktien vorsieht. Seine Regelungen zum sog. Kryptowertpapierregister würden zu der Dezentralität und Kernidee der meisten Blockchain-Anwendungen in Widerspruch stehen. Startups würden nicht zuletzt durch hohe Bürokratie- und Kostenhürden am Markteintritt gehindert werden.

Im Hinblick auf sog. Stablecoins würden hohe Hindernisse geschaffen werden, sogar ein Verbot wird seitens der Antragsteller:innen gefürchtet. Stablecoins seien schließlich an staatliche Währungen oder andere Vermögenswerte gebunden und hätten dadurch voraussichtlich eine geringere Volatilität, wobei sie v.a. Ländern mit instabilen Währungen oder weniger entwickeltem Bankenmarkt potentiell Zugang zu sichererem Zahlungsverkehr via die Blockchain-Technologie geben würden. Milliarden Menschen würden Stablecoins einen Zugang zu einem günstigeren und schnelleren internationalen Zahlungsverkehr bieten – die MiCAR stünde dem nach Ansicht der Antragsteller:innen entgegen.

2. Stellungnahme

Der Beschlussantrag zu I verwirrt durch seine Widersprüchlichkeit. Er überrascht im Hinblick auf die Annahme, dass der technische Fortschritt und seine Nutzung ihre Grenzen in technologieneutralen Gesetzen finden. Im Antrag vom 11. September 2018 (Drucksache 19/4217) wurde z.B. eine „*rasante Wachstumsphase*" bei sog. ICO (Initial Coin Offerings), einer DLT-basierten Finanzierungsform, festgestellt. Hier wurde allerdings die BaFin als wenig kompetent und innovationshinderlich bezeichnet. Der Antrag fand keine Zustimmung (Drucksache 19/10013).

Mit Verwunderung nimmt man die Heraushebung der Bedeutung von sog. Stablecoins wahr. Der Antrag scheint festzustellen, dass es sich bei dem Euro um eine instabile Währung handelt und Deutschland sowie europäische Länder einen nur wenig entwickelten Bankenmarkt und wenig bis keinen Zugang zu sicherem Zahlungsverkehr vorweisen können, weshalb der Stablecoin die vermeintliche Rettung sei. Allerdings wird dieser erkennbar missverstanden. Selbst infrastrukturärmere afrikanische Länder wie Kenia brauchen keine Blockchain-Stablecoins, weil sie ein wesentlich effizienteres Geldtransfersystem (M-PESA) etabliert und über Ländergrenzen hinaus ausgedehnt haben.[7] M-PESA ist sogar ein taugliches Vorbild für den digitalen Euro.

[7] *Muchoki*, M-PESA's Impact on the Kenyan Economy, Ri-nova 2018, frei abrufbar unter: https://rechtinnovativ.online/ri-nova-01-2018-muchoki-mpesas-impact-on-kenyan-economy. Siehe dazu auch die weiterführenden Beiträge von *Gitiri* und *Bruckhuisen* im Sonderheft Ri-nova 2018 (https://rechtinnovativ.online/ri-nova-01-2018).

Die Grundlagen der Forderungen im Antrag stehen nicht im Einklang mit der Realität. Die Antragsteller:innen schreiben der deutschen und europäischen „Krypto-Branche" größere Bedeutung und Marktrelevanz zu als ihr tatsächlich zukommt. Das BSI hat in seinem Abschlussbericht zum Projekt 374 vom 29. April 2020[8] folgende Feststellungen getroffen:

> *Auffallend ist hier insbesondere, dass über ein Viertel aller Blockchain-Angebote aus den USA stammt, während Deutschland nur mit knapp 3% vertreten ist.[...] Auffallend ist außerdem, dass ein signifikanter Teil der Produkte nicht von einer Firma hergestellt und vertrieben wird, sondern von Privatpersonen oder einer Community.*[9]

Die Antragsteller:innen – wie auch die Europäische Kommission – berücksichtigen nicht, dass deutsche und europäische Startups, i.e. Firmen, offenbar eine geringere Rolle spielen, als etwa Privatpersonen oder über Ländergrenzen hinweg zusammenwirkende Privatpersonen in einer Community[10]. Startups werden häufig als relevant wahrgenommen, weil sie sich als relevant darstellen oder (von sog. Experten) darstellen lassen. Das BSI hat dazu festgestellt:

> *[...] über ein Drittel aller Anwendungen sind bisher nicht über das Stadium einer Marketingwebseite hinausgekommen. Mit einem durchschnittlichen Reifegrad von 2,38 sind Blockchain-Anwendungen die am wenigsten entwickelte Art von Blockchain-Angeboten auf dem Markt. Es entsteht insgesamt der Eindruck, dass es bisher noch so gut wie keine im Einsatz befindlichen Anwendungen für die Blockchain-Technologie gibt.*[11]

Das BSI fasst in seinem Abschlussbericht in deutlichen Worten u.a. zusammen:[12]

- ***Es existieren so gut wie keine Angebote mit formalen Sicherheitsnachweisen, die wesentliche Teile des Angebots betreffen.*** *Formale Sicherheitsnachweise existieren zwar für die eingesetzten kryptographischen Bausteine wie Verschlüsselungsverfahren oder Signaturfunktionen, viele Blockchain-Angebote versprechen jedoch weit darüber hinausgehende Sicherheitseigenschaften, wie Unveränderlichkeit oder Resistenz gegen Sybil-Angriffe. Für diese Aussagen bestehen in der Regel keine formalen Nachweise oder wissenschaftliche Untersuchungen.*

- ***Blockchain-Anwendungen spielen auf dem Markt kaum eine Rolle.*** *Fast 80% aller untersuchten Anwendungen haben eine kleine oder sehr kleine Marktrelevanz.*

- ***Existierende Angebote wurden bisher kaum öffentlichen Sicherheitsanalysen oder „Penetration Tests" unterzogen.*** *Obwohl das Hauptverkaufsargument der meisten Blockchain-Angebote die Sicherheit ist, wurden nur in wenigen Einzelfällen von den Herstellern der Produkte unabhängige Sicherheitsuntersuchungen in Auftrag gegeben und deren Ergebnisse veröffentlicht.*

---

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html.
[9] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html, S. 19 f.
[10] ISv vier oder mehr Personen, welche sich zur Bearbeitung eines DLT-Projektes zusammengeschlossen haben, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html, S. 12.
[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html, S. 35.
[12] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Studie-374.html, S. 35 f.

- ***Zahlungsverkehr und Spiele sind die Hauptanwendungsfelder von existierenden Blockchain-Anwendungen.*** *Der größte Teil der untersuchten Blockchain-Anwendungen (ca. 20%) ist für den Einsatz im Finanzsektor gedacht, bei dem zweitgrößten Teil handelt es sich um Spiele, die ihre Spieldaten in der Blockchain verwalten. Insbesondere die Anwendungsfelder Verwaltung, IoT, Identitätsmanagement, Gesundheit und Energie, welche häufig als Hauptverkaufsargument für Blockchain-Technologie genannt werden, werden bisher kaum von existierenden Blockchain-Anwendungen abgedeckt. Ein signifikanter Teil der Anwendungen (ca. 22%) ist keinem der klassischen Anwendungsfelder zuzuordnen.*

Der Antrag beinhaltet im Ergebnis Vor- und Darstellungen, die entzaubert sind. Spezialgesetze sowie ihre Chancen und Risiken bedürfen daher einer eingehenden Prüfung.

II. Zum Beschlussantrag zu II

Die angeführten Maßgaben sind nicht zielführend.

1. Handwerkliche Mängel der vorgeschlagenen MiCAR

Ungeachtet des Umstands, dass das vorgeschlagene Auffangregelwerk MiCAR ausdrücklich keine Finanzinstrumente regeln soll und die gewünschten Begriffsschärfungen in die Beratungen zur Änderung der MiFID II gehören, sei auf Folgendes hingewiesen:

Das größte Problem der vorgeschlagenen MiCAR und Begleitregelwerke im Rahmen der Digital Finance Strategy ist die sie durchziehende Begriffsungenauigkeit. Insoweit ist den Antragsteller:innen ausdrücklich beizupflichten. Exemplarisch kann man dies am Begriff der „Distributed-Ledger-Technologie" aufzeigen, „legaldefiniert" z.B. in Art. 3 Nr. 1 MiCAR-E:

> *„Distributed-Ledger-Technologie" oder „DLT" [ist] eine Technologie, die die verteilte Aufzeichnung verschlüsselter Daten unterstützt;*

Dem durchschnittlichen Richter dürfte der Unterschied zu einer Rundmail[13] an passwortgeschützte E-Mailpostfächer nicht wirklich klar sein. Die Definition ist auch technisch gesehen viel zu eng, denn Daten in „einer Blockchain" als bekanntester Fall von DLT sind in der Regel nicht verschlüsselt. So sind z.B. die Daten in der Bitcoin- bzw. Ethereum-Blockchain mangels Verschlüsselung für jedermann leicht einsehbar. Beliebte, Ethereum-basierte Kryptowerte würden daher von der MiCAR nicht erfasst. Das Auffangregelwerk ist im Ergebnis keines, weil die wichtigsten DLT-Netzwerke durch das Raster fallen.

Der auf Vorstehendem basierende Begriff „Kryptowert" in Art. 3 Nr. 2 MiCAR-E ist nicht schärfer gefasst:

[13] Gemeint ist eine E-Mail an eine Vielzahl von Empfängern.

> *„Kryptowert" [ist] eine digitale Darstellung von Werten oder Rechten, die unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden können;*

Damit wird auch die fotografierte und per Rundmail versandte Fotografie einer Euro-Münze zum Kryptowert.

Die Bundesregierung sollte darauf hinweisen, dass der Entwurf der MiCAR sowie sämtliche Begleitregelwerke mit denselben Legaldefinitionen gravierende Mängel aufweisen und das Ziel hoher Regelungsdichte nicht zu erfüllen vermögen.

2. „Markteintrittsbarriere" oder notwendige Gefahrenkontrolle?

Deutsche und Europäische „Blockchain-Startups" haben nur wenig Marktrelevanz, wie das BSI in seinem Abschlussbericht eindrucksvoll festgestellt hat. Zu oft liegen Worte und Fakten weit auseinander. Keine der von der Europäischen Kommission vorgeschlagenen Maßnahmen berücksichtigt den vom BSI bestätigten Umstand, dass vor allem Privatpersonen und aus Privatpersonen bestehende, über diverse Länder dieser Welt ausgedehnte, Communities die „Crypto-Szene" bestimmen. Sie schaffen statistisch gesehen (quantitativ) mehr Gefahren als Unternehmen mit Erlaubnis der BaFin.

Der hohe Anteil von Privatpersonen ist aber kein Grund, an Blockchain-Startups geringe Anforderungen zu stellen. Die allein dem Einsatz von DLT immanente Schaffung (qualitativ) hoher (Verlust-)Gefahren[14] ist mit niedrigen Marktzugangsschwellen nicht zu vereinbaren.

3. Stablecoins begründen die finanzielle Abhängigkeit des Nutzers

In Bezug auf sog. Stablecoins ist richtigzustellen, dass diese nicht nur Vorteile, sondern auch Nachteile haben. Diese werden u.a. auf der Website der Stablecoin-Plattform Ethereum klar benannt:

- *Centralized – someone must issue the tokens.*
- *Requires auditing to ensure company has suffficient reserves.*[15]

Das bedeutet, dass es einen Emittenten gibt, welcher die Kontrolle inne hat und diese über die Existenz und Benutzbarkeit „seiner" Stablecoins behält. Eine Transaktion in Verbindung mit Stablecoins kann, ausweislich des realen Fallbeispiels des USD Coin (USDC) aus dem Sommer 2020,[16] vom Emittenten unterbunden und damit beeinflusst werden.

Die Missbrauchsgefahr ist hoch. In totalitären Staaten kann ein Stablecoin dazu dienen, die Bürger dem Herrscherwillen zu unterwerfen – schließlich kann er die Liquidität des Einzelnen oder von Personengruppen unmittelbar oder mittelbar beeinflussen. Eine vergleichbare Einflussnahme-

[14] Siehe dazu die Stellungnahme vom 13. September 2020, Anlage.
[15] https://ethereum.org/de/stablecoins/.
[16] Mehr dazu unter: https://cot.legal/stablecoins-gefahren-des-programmierbaren-geldes.

möglichkeit kommt nicht einmal der Europäischen Zentralbank und Bundesbank, geschweige denn den sonstigen Banken zu.

Doch auch die Verlustgefahr ist extrem hoch, weil Existenz und Benutzbarkeit eines Stablecoins von der Existenz und den Mitteln des Emittenten abhängen. Nicht zuletzt ist die Verwendung von Stablecoins in einem Netzwerk wie Ethereum abhängig von Transaktionsgebühren in einer anderen sog. Kryptowährung, die erheblichen Schwankungen unterliegen kann. Dies hat die jüngere Vergangenheit gezeigt. Ein Grund: Das hohe Aufkommen von Transaktionen im Zusammenhang mit sog. DeFi (Decentralized Finance) Angeboten.

Ein Stablecoin ist aufgrund der Abhängigkeit des Nutzers vom Emittenten mehr Gefahr als Chance. Daher sind Schwellenwerte und die Möglichkeit des Verbots sogar notwendige Instrumente der Regulierung und des Schutzes von Demokratie, Frieden, Finanzstabilität, Finanzmärkten und natürlich Verbrauchern.

4. Innovationsoffene Regulierung von Kryptoassets

Die bestehende, weitgehend technologieneutrale Rechtslage vermag viele technologische Neuerungen zu erfassen. Insbesondere erfasst sie auch sog. Blockchain-Angebote. Das Problem ist jedoch die Begriffsunschärfe und die Verbreitung von Mythen, die Anbieter noch heute für sich nutzbar machen. Sie schaffen Verwirrung und legen den Grundstein für falsche Subsumtion oder neue, unscharfe Rechtsbegriffe. Es ist insofern begrüßenswert, klar(stellend)e Regelungen zu formulieren, um die Rechtsanwendung zu erleichtern. Die neuen Regelungen sollen dabei nicht im Widerspruch zur Rechtslage stehen, sondern v.a. spezifischen Gefahren begegnen.

Es braucht daher keine besondere Förderung der sog. Blockchain-Technologie. Die Antragsteller:innen widersprechen sich hier im Hinblick auf die Forderung von Technologieneutralität (vgl. Beschlussantrag zu I, S. 2, 1. Absatz). Wie das BSI herausgearbeitet hat, ist der Glaube an ihre Bedeutung größer als ihre (ggf. zu erwartende) Bedeutung selbst.

Den Antragsteller:innen ist jedoch zu danken, weil sie (wenn auch nicht unbedingt intendiert) die unzureichende Regelungsdichte in der geplanten MiCAR und Begleitregelwerken aufgezeigt haben. Denn tatsächlich sind diese ungewollt „innovationsoffener" als gedacht.

III. Zum Beschlussantrag zu III

Die Anregungen sind nicht zielführend.

1. Elektronische Aktien passen nicht in das eWpG und zur Corporate Governance

a) Systemwidrigkeit des eWpG im Verhältnis zum AktG

Der Sinn und Zweck des eWpG-E ist mit dem Wunsch der Antragsteller:innen, die elektronische Aktie mitzuregeln, nicht vereinbar:

Im Gegensatz zur ausweislich § 1 eWpG-E einzig erfassten Inhaberschuldverschreibung nach § 793 BGB, einem sog. konstitutiven Wertpapier, hat die Verbriefung (d.h. Erstellung einer Urkunde) im Aktienrecht rein deklaratorische, mithin keine konstitutive Bedeutung. Das heißt, die Entstehung der Mitgliedschaft in einer Aktiengesellschaft (AG) hat nur zwei zwingende Voraussetzungen:

1. die Übernahmeerklärung des Aktienzeichners und
2. die Eintragung der Gründung oder Kapitalerhöhung in das Handelsregister.

Die Verbriefung der Mitgliedschaft mit ihren Rechten und Pflichten erfolgt hiernach als dritter, aber rein fakultativer Akt. Eine gesetzliche Vorgabe zur Ausgabe einer Aktienurkunde gibt es nicht. Sie ist für die Entstehung der Mitgliedschaft nicht wesentlich, sondern dient v.a. einer erhöhten Verkehrsfähigkeit der Aktie.

Die (verzichtbare) Aktienurkunde hat nicht nur im Gesetz, sondern auch praktisch längst an Funktion verloren: Die Übertragung von Aktien erfolgt heute v.a. auf dem elektronischen Weg im Rahmen der Abwicklung des Effektenhandels (Effektengiroverkehr). Die „Tokenisierung" der Aktie ist vor dem Hintergrund der geringen Reife, Sicherheit, Verbreitung und hohen Kosten sowie Risiken von DLT mehr Bürde als Nutzen.

Gewissermaßen ist genau dies ein Fall der Blockchain, die ein zu lösendes Problem noch sucht. Die elektronische Aktie auf Blockchain-Basis ist keine Lösung, sie schafft Probleme.

b) Eine elektronische Aktie iSd eWpG-E ist überflüssig und war nie gewollt

Ein Vorteil elektronischer Inhaberaktien ist nicht erkennbar, v.a. weil die Ausgabe von Inhaberaktien nach § 10 Abs. 1 S. 2 AktG aus Transparenzgründen per se beschränkt ist. Ein Register zur Führung elektronischer Namensaktien erscheint unter Verweis auf das Aktienregister in § 67 AktG überflüssig. Für die Registerführung braucht es offenkundig keine Distributed-Ledger-Technologie.

Vielmehr dürfte in einer elektronischen Inhaberaktie nach dem Vorbild des eWpG-E ein sog. Wertrecht (vgl. „Kryptowert") liegen. Der (deutsche) Gesetzgeber hat sich im Zuge der Novellierung des Aktiengesetzes bewusst gegen reine Wertrechte entschieden:

> *Der geänderte § 10 Abs. 5 AktG geht darüber hinaus, indem er die Möglichkeit eröffnet, auch den Anspruch der einzelnen Aktionäre auf Ausstellung einer Mehrfachurkunde über ihren jeweiligen Anteil auszuschliessen.*
> *Damit wird nicht der Schritt zum Wertrecht unter Abkehr vom Wertpapier vollzogen, denn der Ausschluß der Verbriefung betrifft lediglich den jeweiligen Anteil der einzelnen Aktionäre. Von einer etwaigen einschränkenden Satzungsbestimmung unberührt bleibt dagegen die Ausstellung und Hinterlegung einer die Gesamtheit der Mitgliedschaftsrechte verkörpernden Globalurkunde.*[17]

[17] BT-Drucksache 13/10038, S. 25.

c) Elektronische Aktien auf DLT-Basis sind schwer vereinbar mit allgemeinen Grundsätzen

DLT-Netzwerke wie Bitcoin oder Ethereum sind nicht gerade bekannt für einen moderaten Energieverbrauch.[18] Vor dem Hintergrund der sog. Corporate Social Responsibility (CSR) wirkt sich die Nutzung solcher Technologien wahrscheinlich sogar nachteilig auf eine Aktiengesellschaft aus:

Nach dem CSR-Richtlinie-Umsetzungsgesetz vom 11. April 2017, basierend auf der Richtlinie 2014/95/EU vom 22. Oktober 2014, haben Kapitalgesellschaften im Sinne des § 289b HGB ihren Lagebericht um eine nichtfinanzielle Erklärung zu erweitern. Diese nichtfinanzielle Erklärung beinhaltet nach § 289c Abs. 2 Nr. 1 HGB mindestens Aspekte der Umweltbelange, wobei sich die Angaben beispielsweise auf Treibhausgasemissionen, (...), die Nutzung von erneuerbaren und nicht erneuerbaren Energien (...) beziehen können. Die Nutzung einer energieintensiven Technologie zwecks Verbriefung von Aktien, die keiner Verbriefung bedürfen, dürfte schwer erklärbar sein.

Daneben sind nach § 289c Abs. 2 Nr. 3 HGB Aspekte der Achtung der Menschenrechte in die nichtfinanzielle Erklärung aufzunehmen, wobei sich die Angaben beispielsweise auf die Vermeidung von Menschenrechtsverletzungen beziehen können. Zudem trifft jedes Leitungsorgan die Legalitätspflicht,[19] wonach es dafür Sorge zu tragen hat, dass das „Unternehmen so organisiert und beaufsichtigt wird, dass keine Gesetzesverstöße erfolgen. Eine entsprechende Kontrolle ist bei gemeinsam mit zahlreichen Dritten genutzten DLT-Netzwerken unmöglich. So wurden in der Bitcoin-Blockchain bereits Links auf Seiten mit KiPo-Material sowie Nacktbilder gespeichert.[20] Wer eine vollständige Kopie der Bitcoin-Blockchain vorhält, hält Kopien hiervon auf eigenen Rechnern vor. Und wird dies kaum erklären können.

Auch der weitere Aspekt der Vermeidung und Bekämpfung von Korruption sowie Bestechung (§ 289c Abs. 2 Nr. 5 HGB) lässt sich nur schwer mit der gemeinsam mit zahlreichen Dritten erfolgenden DLT-Nutzung vereinbaren. Es ist einer Aktiengesellschaft mangels umfassender Kontrolle und Überschaubarkeit kaum möglich, brauchbare oder gar wahrheitsgemäße Angaben über fremde DLT-Inhalte zu machen. Entsprechendes gilt für Geldwäsche und Terrorismusfinanzierung, wofür sog. Kryptowährungen auf Basis von DLT ebenfalls genutzt werden.[21] Der europäische Gesetzgeber hat sich deshalb zu einer Erweiterung des Anwendungsbereiches der Geldwäschevorschriften veranlasst gesehen.[22]

Vor diesem Hintergrund dürfte Aktienzeichnern kaum vermittelbar sein, dass sie Zugang zu einem nicht umweltfreundlichen, nicht kontrollierbaren und möglicherweise illegal genutzten DLT-Netzwerk benötigen, um ihre Legitimation und die Verkehrsfähigkeit ihrer Aktie(n) zu erhalten. Wenig sinnvoll erscheint daneben die Schaffung und Unterhaltung eines eigenen DLT-

---

[18] *Sedlmeir et al.*: The Energy Consumption of Blockchain Technology, Bus Inf Syst Eng 599 (603 f.) (2020), https://link.springer.com/article/10.1007/s12599-020-00656-x.
[19] LG München I, Urt. v. 10.12.2013 – 5 HK O 1387/10 („Neubürger-Urteil").
[20] *Matzutt et al.*, A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, S. 2, https://www.comsys.rwth-aachen.de/fileadmin/papers/2018/2018_matzutt_bitcoin-contents_preproceedings-version.pdf.
[21] Erwägungsgrund 8 der Richtlinie (EU) 2018/843.
[22] *Steinfeld*, A Legislator's (Hyper)Activity The EU and the case of money laundering, Ri-nova, 2019, 27 (27f.).

Netzwerks. Die Kosten dürften den Nutzen erheblich übersteigen. Die Attraktivität und praktische Bedeutung der elektronischen Aktie dürfte also sehr gering sein.

2. Der registerführende Emittent darf nur mit Erlaubnis operieren

Die dem registerführenden Emittenten zukommende Machtstellung und die ihr immanente hohe Missbrauchsgefahr wurden bereits in der Stellungnahme vom 13. September 2020[23] dargestellt. Gerade diese Machtstellung bedarf eines qualifizierten Gegengewichts wie der BaFin, weshalb die Erlaubnispflicht notwendig und richtig ist. Anstatt wie von den Antragsteller:innen gefordert, gehören die Anforderungen an den registerführenden Emittenten erhöht.

3. Relevante Startups sollen die hohen Anforderungen finanzieren können

Wie bereits ausgeführt, stellen Startups per se keine bemerkenswerte Größe im Bereich der Blockchain-Anwendungen dar. Der Ansatz, hohe Risiken schaffenden Startups einen leichteren Marktzugang durch geringere regulatorische Anforderungen zu gewähren, geht fehl. Vielmehr sollte überlegt werden, ob und wie man ggf. bessere Rahmenbedingungen für die finanzielle Ausstattung und Ausbildung der wenigen relevanten Startups sowie ihrer Verantwortlichen schaffen kann, damit sie die hohen regulatorischen Anforderungen erfüllen können.

4. Das Verhältnis von eWpG und MiCAR entspricht dem von Äpfeln und Birnen

Den Antragsteller:innen ist insoweit beizupflichten, dass das geplante eWpG und die geplante MiCAR nicht in Konflikt geraten sollten. Da das eWpG-E übertragbare Wertpapiere behandelt, mithin Finanzinstrumente im Sinne der MiFID II, steht es per se nicht im Konflikt mit der vorgeschlagenen MiCAR. Denn diese soll nach ihrem Art. 2 Abs. 2 lit. a) gerade keine solchen Kryptowerte regeln, die Finanzinstrumente im Sinne der (geänderten) MiFID II sind.

Insofern können die Zulassungserfordernisse des eWpG-E nicht über die der geplanten MiCAR hinausgehen. Zumindest lässt der Antrag nicht erkennen, wo genau ein kritischer Konflikt aufzutreten droht.

[23] Anlage.

Anlage

COT Legal // Steinfeld Recht

Claudia Otto
Rechtsanwältin
Bockenheimer Landstraße 2-4
60306 Frankfurt am Main
Telefon: +49 69 667 748 360
Telefax: +49 69 667 748 450
Mail: claudia.otto@cot.legal
Web: https://cot.legal

Mirjam Hannah Steinfeld, Mag. iur., CFE
Rechtsanwältin und
Fachanwältin für Strafrecht
Voelckerstraße 21
60322 Frankfurt am Main
Telefon: 069 24 74 199 30
Telefax: 069 24 74 199 32
Mail: kanzlei@steinfeld-recht.de
Web: www.steinfeld-recht.de

Gemeinsame Stellungnahme

zum

Entwurf eines Gesetzes für ein Gesetz zur Einführung von elektronischen Wertpapieren
im Rahmen der Anhörung der Verbände und interessierten Kreise

GZ: VII B 5 - WK 6100/20/10001 :004

DOK: 2020/0779342

vom 13. September 2020

I. Einleitung

Wir begrüßen den Referentenentwurf des Bundesministeriums der Finanzen sowie des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Einführung von elektronischen Wertpapieren. Er ist gut durchdacht und begegnet bekannten Gefahren für Anlegerinnen und Anleger[1] sowie Finanzmarkt mit den richtigen Schutzmaßnahmen.

Wir gehen aufgrund öffentlicher Informationen davon aus, dass z.B. die Grundfragen zur Sachfiktion in § 2 Abs. 3 eWpG-E, zum Begriff der Inhaberschaft sowie zu Übergangs- und Kollisionsregelungen von anderen versierten Kommentatoren umfassend adressiert werden. Wir möchten uns daher in dieser Stellungnahme auf die Gefahren herrührend aus der Doppelrolle des registerführenden Emittenten in § 16 Abs. 2 S. 3 eWpG-E beschränken. Diese lassen bei genauerer Betrachtung erkennen, dass der Referentenentwurf keinesfalls von innovations- und wettbewerbsbeschränkendem Charakter ist. Allerdings erscheint uns der Hinweis wichtig, die im Folgenden dargestellten Gefahren zum Anlass zu nehmen, die Doppelrolle in der für angemessen erachteten Art und Weise konkret und angemessen zu regulieren.

II. Fokus dieser Stellungnahme: die Doppelrolle Emittent/registerführende Stelle

Die Doppelrolle des registerführenden Emittenten, also des Emittenten zugleich in der Rolle der registerführenden Stelle, ist ausschließlich in § 16 Abs. 2 S. 3 eWpG-E geregelt. Auch ohne weitere klarstellende Bezugnahme auf die Pflichten der registerführenden Stelle im eWpG-E sowie das Erlaubniserfordernis nach dem neuen KWG ist klar, dass den Emittenten diese Vorschriften betreffen. Nicht erfasst ist jedoch die in der Doppelrolle angelegte, erhöhte Einflussnahmemöglichkeit des Emittenten. Dies gilt insbesondere vor dem Hintergrund der sich etablierenden DeFi-Systeme. DeFi ist eine Kurzform von Decentralized Finance, in dem klassische Finanzdienstleistungen und Bankgeschäfte unter Verwendung sog. Smart Contracts (teil-)automatisiert erfolgen. Smart Contracts sind Computerprogramme, die Register mit bestimmten Funktionen darstellen. Smart Contracts können in verschachtelter oder kaskadenförmiger Art und Weise interagieren.

1. Der Fall „Sushi"

a. Was ist passiert?

Ende August 2020 gab es Bewegung im Bereich DeFi. Basierend auf der bekannten Blockchain-Plattform *Ethereum* tauchte das sog. *SushiSwap*-Projekt auf. Es umfasste allerdings kein essbares, aber ein für viele Menschen finanziell sehr schmackhaftes Angebot: das sinngemäße Geldverdienen im Schlaf. Binnen weniger Tage wurden mehrere Millionen US-Dollar „elektronisch gebunden". Die *SushiSwap*-Community kritisierte, dass fast 50 Prozent der Anteile an *SushiSwap* in einer Hand lagen; nämlich in der Hand des Schöpfers, des unbekannten „Chef Nomi". Am 5. September 2020 tauschte „Chef Nomi" sämtliche seiner SUSHI-Token gegen Ether (ETH) ein – im Wert von 10 Millionen US-Dollar. Der Preis des SUSHI-Token halbierte sich und sinkt seitdem

[1] Nachstehende Personenbezeichnungen sollen, soweit sich Abweichendes nicht aus dem Text ergibt, alle Geschlechter meinen.

weiter ab. Binnen zwei Wochen verloren also Involvierte ihr Vermögen in nicht unwesentlichem Umfang. Zwei Wochen, in denen einflussreiche Kryptobörsen wie *Binance* erheblich zu den Verlusten beitrugen und Verantwortlichkeit durch ihre Geschäftsführung von sich wiesen:

Quelle: Twitter

Auf den erkennbar ausgelösten Aufruhr in der Community hin wies „Chef Nomi" einen Betrug, einen sog. Exit-Scam, von sich. Er hätte den ETH „verdient" für seine Leistungen:[2]

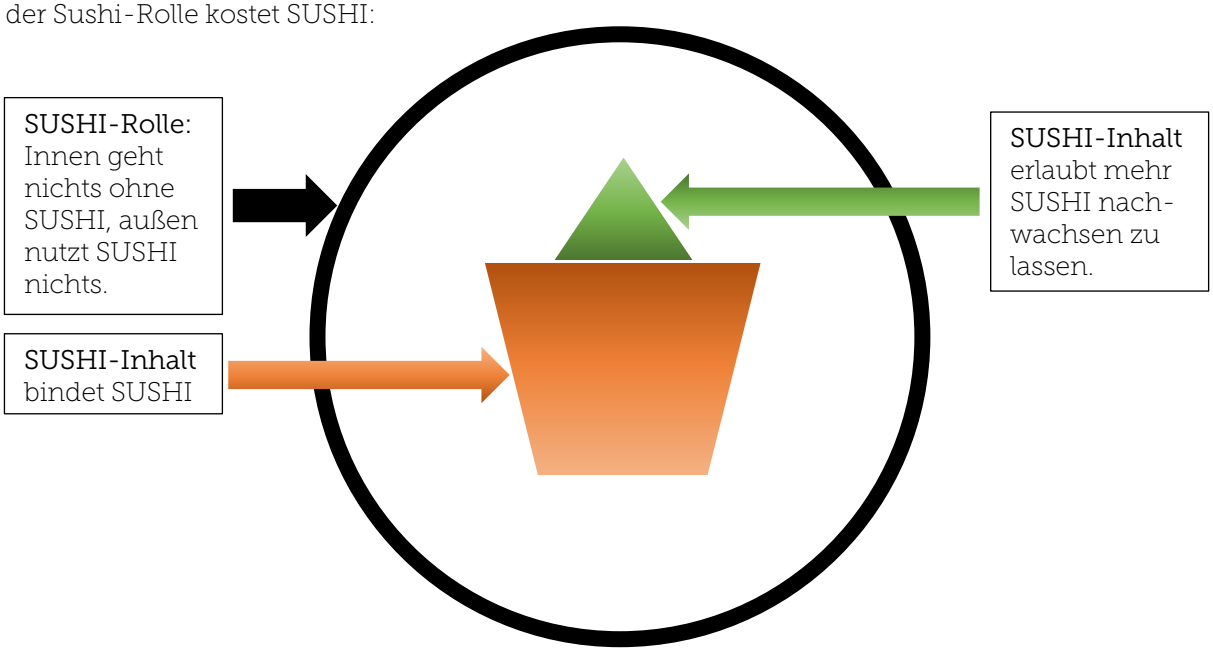
Quelle: Twitter

Hiernach übertrug er – angeblich – seine Kontrollbefugnisse über *SushiSwap* auf einen anderen Unbekannten. Es ist nicht zu erwarten, dass der Verlust des SUSHI-Token durch Kursänderungen rückgängig gemacht wird.

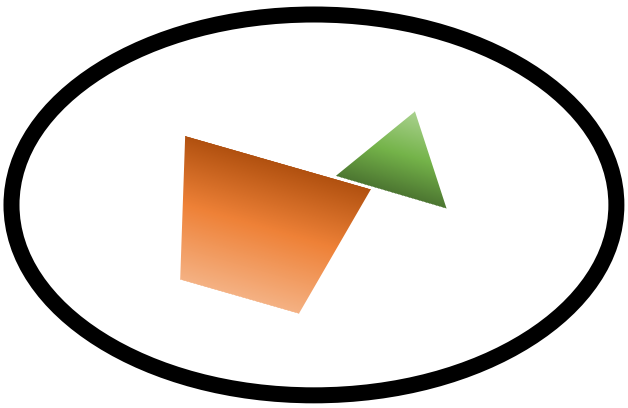
[2] Näheres im Artikel „Something fishy" vom 6. September 2020 unter https://cot.legal/something-fishy.

b. SUSHI-Token und *SushiSwap* leicht erklärt

Der SUSHI-Token erfüllt viele Zwecke, ist jedoch dem Ether (ETH) als sog. Kryptowährung ähnlicher als einem Wertpapier. Der SUSHI-Token kann als Registerwährung verstanden werden, die in mehreren Unterregistern zur Anwendung kommt. Gewissermaßen kann man sagen: alles in der Sushi-Rolle kostet SUSHI:



Die Sushi-Rolle ist die grafische Darstellung von *SushiSwap* und kann als Hauptregister verstanden werden. *SushiSwap*-Rolleninhalte brauchen SUSHI und stellen deshalb jeweils für sich zweckspezifische (Unter-)Register dar. Die einen (Unter-)Register dienen dem Binden von SUSHI, etwa zum Zwecke der Beteiligung an einem Unterprojekt. Andere (Unter-)Register dienen z.B. dazu, SUSHI samenähnlich einzusetzen und wie eine Pflanze „anzubauen". Im Falle *SushiSwap* hat, vereinfacht dargestellt, „Chef Nomi" durch Abstoßen von knapp 50% Inhalt der Außenrolle die Konsistenz der Rolle insgesamt beeinträchtigt:



Verständlich also, dass der Wert des SUSHI um gut 50% gefallen ist. *SushiSwap* ist durch den Ausstieg des Entwicklers insgesamt „aus der Form" geraten. Daher steht der Vorwurf des Exit-Scam im Raum.

c. Wie passt *SushiSwap* in das Gefüge des Referentenentwurfs?

SushiSwap mitsamt seinen (Unter-)Registern wurde von „Chef Nomi" erschaffen. Er erschuf den SUSHI-Token. Auch die in den einzelnen (Unter-)Registern zum Tragen kommenden Spezial-Token wurden von „Chef Nomi" kreiert. Die Spezial-Token dürften ihrem Sinn und Zweck nach entweder Schuldverschreibungen im Sinne des eWpG-E oder auch zukünftig zu regelnde elektronische Aktien bzw. Investmentanteile darstellen. „Chef Nomi" allein war in der Lage, das ganze System *SushiSwap* und die Anleger-Community mit einer egoistischen Entscheidung ins Chaos zu stürzen. Aus diesem Grund ist der Fall „Sushi" von großer Bedeutung für die Gesetzgebung zum elektronischen Wertpapier.

SushiSwap ist ein „Abkömmling" von *Uniswap*, einer *Ethereum*-basierten sog. Decentralized Swap Exchange. *Uniswap* ist, weniger spektakulär formuliert, ein Protokoll, welches es erlaubt, ERC-20-Token tauschen zu können. Dabei kann jeder ERC-20-Token tauschbar gemacht werden – hierfür muss lediglich ein Smart Contract, ein sog. (Liquidity) Pool angelegt werden. Jeder dieser Smart Contracts ist dann eine xToken-Tauschbörse für sich. Der Wert der jeweiligen xToken bestimmt sich dann anhand einer einfachen Gleichung: xToken und daneben ETH müssen mit demselben US-Dollar-Wert „hinterlegt" werden. Will ein Dritter xToken erwerben, „zahlt" er ihren Gegenwert in ETH ein. Das Verhältnis von xToken zu ETH verändert sich: weniger xToken stehen mehr ETH gegenüber – der Wert der xToken, die knapper geworden sind, steigt also. Statt Tauschens kann dem xToken auch nur Liquidität beigesteuert werden, mit denen die Beitragenden dann sog. Liquidity Provider Fees verdienen können. Der Beitragende erhält im Gegenzug xPool-Token, die ebenso ERC-20-Token sind. Diese Pool-Token sind wiederum tausch- und einsetzbar in anderen Smart Contracts. Gleichzeitig stellen sie einen Anteil an den gepoolten xToken und den anfallenden Tauschgebühren dar.

SushiSwap ist allerdings kein *Uniswap*-Smart Contract, sondern ein sog. Fork, eine *Ethereum*-basierte Abspaltung von *UniSwap*. Dabei interagiert eine Mehrheit von Smart Contracts: miteinander, nebeneinander, nacheinander. Die einzelnen Smart Contracts und auch ihre Spezial-Token – neben dem SUSHI-Token – erfüllen verschiedene (Pool-)Zwecke. Sie eint das gemeinsame *SushiSwap*-Protokoll (des „Hauptregisters"), welches die zweckgerichtete Registrierung der Token in den jeweiligen Smart Contracts („Unterregistern") reglementiert. Zwecke können hier sein:[3]

- Stimmrechtszuweisung und -ausübung,
- Einnahmen generieren und umwandeln,
- Finanzierung,
- Dividenden verdienen.

Viele, wenn nicht gar sämtliche Geschäfte im Rahmen *SushiSwap*s dürften bekannte und bereits geregelte Bankgeschäfte oder Finanzdienstleistungen darstellen. „Chef Nomi" wäre, nach unserer Auffassung, als „registerführender Emittent" im Sinne des eWpG-E anzusehen.

[3] The *SushiSwap*-Project, 26. August 2020, https://medium.com/sushiswap/the-sushiswap-project-c4049ea9941e; Erläuterungen unter https://cot.legal/something-fishy.

d. Kryptowährungen als Mittel automatisierter, algorithmenbasierter Registerführung

Der Fall „Sushi" ist nicht nur ein Beispiel für die Manipulierbarkeit der Preise sog. Kryptowährungen: Er ist vor allem auch ein warnendes Beispiel für die Einflussmöglichkeiten des registerführenden Emittenten auf die von ihm begebenen und registrierten Wertpapiere. Denn all seine (Unter-)Register setzen auf der von ihm geschaffenen Kryptowährung (des Hauptregisters) auf, um *„die Verwaltung und Fortschreibung des Registers automatisiert und algorithmenbasiert erfolgen"*[4] zu lassen. Sie bilden also eine wirtschaftliche Einheit.

Der Fall „Sushi" zeigt zudem, welche Gefahren sich ergeben können, wenn diese Einflussmöglichkeiten bei einer Einzelperson liegen, die technisch versiert ist. Wenn eine Einzelperson in der Lage ist, umfassende Schäden zulasten der Anleger und des Vertrauens in die Funktionsfähigkeit der Finanzmärkte auszulösen, darf die Rechtsform, Größe oder Neuheit des registerführenden Emittenten keinen Einfluss auf die regulatorischen Anforderungen haben.

2. Sich aus dem Beispielsfall ergebender Anpassungsbedarf

Der Referentenentwurf geht davon aus, dass durch die Dezentralität des Kryptowertpapierregisters ein Machtmissbrauch ausgeschlossen ist. Tatsächlich sagt das Merkmal der Dezentralität nichts über die tatsächlichen Machtverhältnisse im Einzelfall aus. Diese können auf der „untersten" (Register-)Ebene wie *Ethereum* andere sein als auf einer der höheren, individuell ausgestaltbaren (Unterregister-)Ebenen. Dort kann die absolute Mehrheit, wie im Fall „Sushi", in der Hand einer einzigen Person liegen. „Chef Nomis" (Entscheidungs-)Macht lag nicht nur in einer sondern auch auf der Hand: Er hat *SushiSwap* programmiert. Er hat *SushiSwap* zu seinem eigenen Vorteil programmiert. Wer wie er versteht, mehrere Register miteinander zu verknüpfen, um hieraus persönlichen Vorteil zu ziehen, sollte nicht nur eine Nebenbemerkung im Gesetz bleiben.

Ein registerführender Emittent sollte seine ausnutzbare zentrale Machtstellung nicht durch Untätigkeit erlangen, sondern erst auf Nachweis des Erfüllens und Prüfung spezifischer Zuverlässigkeitsvoraussetzungen durch die Aufsichtsbehörde im Rahmen der §§ 32 ff. KWG. Interessenkonflikte müssen von vornherein hindernd sein: Wer seine eigenen oder fremden Interesse über die ihm anvertrauten Interessen anderer stellen könnte, darf gar nicht erst in diese Vertrauensposition gelangen. Zwar erfolgt die Registerführung automatisiert und dezentral, jedoch bleibt die Entscheidungsmacht über das Wie stets beim programmierenden Erschaffer – in diesem Fall dem registerführenden Emittenten. Er ist in der Lage, sich sämtliche Kontrollbefugnisse vorzubehalten und diese bei Bedarf *automatisiert und algorithmenbasiert* auszuüben.

Eine derartige einseitige Machtverteilung, zumal in Kombination mit einem einseitigen Wissensvorsprung und diametralen pekuniären Interessen vieler Personen, ist dem deutschen Recht unbekannt. So ist es die Maxime des deutschen (Zivil)Rechts, für ein „level playing field" zu sorgen, wo denjenigen, der über mehr Macht und/oder mehr Wissen verfügt, auch mehr Verantwortung und mehr Pflichten treffen. Genau dieses „level playing field" wird durch den bisherigen Referentenentwurf in Bezug auf den registerführenden Emittenten noch nicht umfassend geschaffen.

[4] Referentenentwurf, Seite 57.

III. Umsetzungsvorschläge

Nachstehende Vorschläge könnten als Grundlage für die weiteren gesetzgeberischen Entscheidungen dienen. Sie sind nicht abschließend und dienen der Veranschaulichung des Vorstehenden. Die Vorschläge wurden im partiell übernommenen, einschlägigen Entwurfstext farblich hervorgehoben.

1. eWpG

Nach dem Referentenentwurf hat *„die registerführende Stelle den Schutz der Datenintegrität vor einer Manipulation durch Dritte zu gewährleisten (Hacking, Angriff auf die Integrität des Wertpapierregisters). Hierzu hat sie ein dem Stand der Technik entsprechendes IT-Sicherheitssystem zu nutzten. Sämtliche Anforderungen an die IT-Sicherheit werden durch Einzelbestimmungen im Verordnungswege konkretisiert."*[5]

Nachfolgende Ergänzungen sollen diejenigen Fälle erfassen, in denen kein technisch bedingter Datenverlust und keine unbefugte Datenveränderung, i.e. Manipulation Dritter, zum Tragen kommt. Weil das Kryptowertpapierregister in den hier adressierten Fällen technisch einwandfrei und wie vom registerführenden Emittenten vorbestimmt funktioniert, greifen § 7 Abs. 2 und 3 eWpG-E nicht. Hinzu kommt, dass emittentenseitig technisch vorbehaltbare Einwirkungsmöglichkeiten auf den Wert von Kryptowertpapieren nicht zwingend zu einer falschen Rechtslage im Sinne des § 7 Abs. 2 eWpG-E führen, sondern lediglich zu für Berechtigte nicht zu erwartenden Wertverlusten. Der Emittent soll im Ergebnis nicht in der Lage sein, sich ohne Weiteres von seiner Schuld zu befreien bzw. sich auf Kosten anderer zu bereichern.

Wir schlagen vor

a) in § 4 eWpG-E die Begriffe „registerführender Emittent" und „sonstiges Register" zu ergänzen;
b) in § 7 eWpG-E einen Haftungstatbestand zu ergänzen, der die missbräuchliche Ausnutzung der automatisierten, algorithmenbasierten Registerführung durch den registerführenden Emittenten selbst erfasst. Weil Dritte unter Umständen zu einem solchen „exploit" fähig sein können, soll der registerführende Emittent sich exkulpieren dürfen. Frei von Haftung soll er jedoch nicht sein. Seine Haftung richtet sich nur nach § 7 Abs. 3 eWpG-E;
c) in § 16 eWpG-E den Begriff des Kryptowertpapierregisters an die Entwicklungen im Bereich sog. Decentralized Finance (DeFi) anzupassen, v.a. ihre Register-in-Register-Gestaltung zu erfassen sowie von Interessenkonflikten betroffene Personen von der Registerführung auszuschließen;
d) in § 17 eWpG-E weitere Registerangaben zur Transparenz von technischen sowie personellen Interdependenzen vorzusehen;
e) in § 21 eWpG-E den Emittenten in die Missbrauchsprävention einzubinden und den registerführenden Emittenten für die aktive Vermeidung von schadensauslösenden Kaskadeneffekten in die Verantwortung zu nehmen.

[5] Referentenentwurf, Seite 48.

Vorstehende Regelungsvorschläge könnten wie folgt umgesetzt werden:

§ 4 Begriffsbestimmungen

(8) Registerführender Emittent ist der Emittent, der nach § 16 Absatz 2 Satz 3 zugleich registerführende Stelle eines Kryptowertpapierregisters nach § 16 ist.

(9) Sonstiges Register ist ein Register, das nach § 16 Absatz 1 Satz 2 und 3 der Führung eines Kryptowertpapierregister dienen kann, ohne selbst für die Eintragung von Kryptowertpapieren bestimmt zu sein.

§ 7 Registerführung; Schadenersatz

(5) Der registerführende Emittent ist zum Ersatz des Schadens verpflichtet, der Berechtigten infolge einer missbräuchlichen Ausnutzung der automatisierten, algorithmenbasierten Registerführung entsteht, es sei denn, er hat den Schaden nicht zu vertreten. Seine Haftung bestimmt sich in diesem Fall nach Absatz 3.

§ 16 Kryptowertpapierregister

(1) Ein Kryptowertpapierregister muss auf einem dezentralen, fälschungssicheren Aufzeichnungssystem geführt werden, in dem Daten in der Zeitfolge protokolliert und gegen unbefugte Löschung sowie nachträgliche Veränderung geschützt gespeichert werden. Ein Kryptowertpapierregister kann Teil eines weiteren Kryptowertpapierregisters sein. Ist das übergeordnete Register ein Sonstiges Register, so gilt es ebenfalls als Kryptowertpapierregister, wenn es mit dem Kryptowertpapierregister eine wirtschaftliche Einheit bildet.

(2) Registerführende Stelle ist, wer vom Emittenten gegenüber dem Inhaber als solche benannt wird. Ein Wechsel der registerführenden Stelle durch den Emittenten ist ohne Zustimmung des Inhabers oder des Berechtigten zulässig, es sei denn, in den Emissionsbedingungen ist etwas Abweichendes geregelt. Unterbleibt eine Benennung nach Satz 1, gilt der Emittent als registerführende Stelle („registerführender Emittent"). Im Falle verbundener Kryptowertpapierregister nach Absatz 1 und Vorliegen eines Ausschlussgrundes nach Absatz 3 muss der Emittent eine andere registerführende Stelle benennen.

(3) Registerführender Emittent kann nicht sein, wer

1. bereits ein übergeordnetes Kryptowertpapierregister im Sinne des Absatzes 1 führt,

2. gesetzlicher Vertreter der registerführenden Stelle eines übergeordneten Kryptowertpapierregisters im Sinne des Absatzes 1 ist,

3. gesetzlicher Vertreter einer anderen Kapitalgesellschaft ist, deren Aufsichtsrat ein Vorstandsmitglied der registerführenden Stelle eines übergeordneten Kryptowertpapierregisters im Sinne des Absatz 1 angehört, oder

4. in den letzten zwei Jahren Vorstandsmitglied derselben börsennotierten registerführenden Stelle des übergeordneten Kryptowertpapierregisters im Sinne des Absatz 1 war, es sei denn, seine Wahl erfolgt auf Vorschlag von Aktionären, die mehr als 25 Prozent der Stimmrechte an der Gesellschaft halten.

§ 17 Registerangaben

(1) Die registerführende Stelle hat sicherzustellen, dass das Kryptowertpapierregister folgende Angaben über das eingetragene Wertpapier enthält:

1. den wesentlichen Inhalt des Rechts einschließlich einer eindeutigen Kennnummer und der Kennzeichnung als Wertpapier,

2. eine Kennzeichnung, ob es sich um eine Einzel- oder Sammeleintragung handelt,

3. eine Kennzeichnung, ob ein übergeordnetes Kryptowertpapierregister nach § 16 Absatz 1 besteht,

4. die registerführende Stelle des übergeordneten Kryptowertpapierregisters nach § 16 Absatz 2 Satz 3,

5. den Emittenten,

6. den Hinweis auf die abrufbare Darstellung der technischen Berechtigungen des registerführenden Emittenten,

7. den Inhaber,

8. Verfügungshindernisse,

9. Rechte Dritter und

10. Angaben zum Mischbestand nach § 9 Absatz 3.

Die Bezeichnung des Inhabers muss durch Zuordnung einer eindeutigen Kennung erfolgen.

(2) Die registerführende Stelle hat sicherzustellen, dass die Angaben nach Absatz 1 Satz 1 in einer Weise verknüpft sind, dass sie nur zusammen abgerufen werden können.

§ 21 Pflichten des Emittenten

(3) Der registerführende Emittent trifft die erforderlichen technischen und organisatorischen Maßnahmen, um missbräuchlicher Ausnutzung der automatisierten, algorithmenbasierten Führung eines Kryptowertpapierregisters nach § 16 Absatz 1 vorzubeugen. Er hat insbesondere sicherzustellen, dass Änderungen an einem anderen Kryptowertpapierregister nach § 16 Absatz 1 Satz 3 nicht automatisiert und algorithmenbasiert zu Änderungen an dem Kryptowertpapierregister oder den Kryptowertpapieren führen.

2. KWG

„Aus Gründen des Anlegerschutzes, der Marktintegrität, der Transaktionssicherheit sowie der Funktionsfähigkeit der Märkte sollen die Stellen, die ein Kryptowertpapierregister führen, unter die Aufsicht der Bundesanstalt für Finanzdienstleistungsaufsicht gestellt werden. Hierzu wird die Kryptowertpapier-Registerführung als Finanzdienstleistung ausgestaltet. Die registerführenden Stellen für Kryptowertpapierregister unterliegen daher im Grundsatz der für Finanzdienstleistungsinstitute geltenden Vorgaben nach dem KWG. Allerdings sieht § 2 Absatz 7b KWG für Kryptowertpapierregisterführer weitreichende Ausnahmen vom Anwendungsbereich des KWG vor."[6]

Ausnahmen sollten nur dann Geltung finden, wenn keine Kryptowertpapierregisterführung in der Rolle des registerführenden Emittenten erfolgt. Erst recht dürfen die strengen Anforderungen des KWG nicht abgeschwächt werden, wenn der Kryptowertpapierregisterführung ein von einer natürlichen oder juristischen Person kontrolliertes DeFi-System zugrunde liegt, also eine von ihm kontrollierte Verknüpfung und Verschachtelung mehrerer (Kryptowertpapier-)Register.

„Zu berücksichtigen sind außerdem Haftungsfragen", erkennt der Referentenentwurf zutreffend.[7] Im Fall „Sushi" beträgt der Verlust aktuell 98,5%, legt man den Allzeithöchstwert von 168,91 US-Dollar am Starttag, den 28. August 2020 an. Bei 101.423.735 Token im Umlauf betrug der Gesamthöchstwert damit 17.131.483.078,85 US-Dollar. Der Gesamtverlust beträgt bei dieser vereinfachten Rechnung 16.874.510.823,67 US-Dollar. 730.000,00 EUR Anfangskapital braucht man nicht in US-Dollar umzurechnen, um zu wissen, dass dieser Betrag selbst in einem kurzen Zeitraum von zwei Wochen nicht mehr als einen Tropfen auf den heißen Stein darstellt. Hier sollte überlegt werden, wie den hohen Risiken und binnen weniger Tage möglicherweise eintretenden Verlusten Rechnung getragen werden kann.

Nicht zuletzt bedarf es unserer Ansicht nach der Einführung weiterer aufsichtsrechtlicher Sicherungsmechanismen, die am besten bereits im Vorfeld der Erlaubnisprüfung durch die BaFin greifen:

[6] Referentenentwurf, Seite 48.
[7] Referentenentwurf, Seite 77.

a) So ist an die erforderliche Vorlage eines technischen, für jedermann verständlich geschriebenen Gutachtens zu denken, in der eine unabhängige Stelle Missbrauchsmöglichkeiten „im Code" ausschließt (siehe unseren Vorschlag zum möglicherweise neuen § 17 Nr. 6 eWpG-E).

b) Transparenz sollte geschaffen werden, gegenüber der Aufsichtsbehörde und den (potentiellen) Inhabern von Kryptowertpapieren, inwiefern der registerführende Emittent theoretische und tatsächliche Eingriffsmöglichkeiten innehat (siehe vorstehenden Buchstaben a und auch unseren Vorschlag zum möglicherweise neuen § 17 Nr. 6 eWpG-E).

c) Die vorstehend dargestellte enge Verzahnung von Kryptowerten i.S.d. § 1 Abs. 11 S. 4 KWG und Wertpapieren sollte sich im KWG und Begleitvorschriften wiederspiegeln. Technische und wirtschaftliche Zusammenhänge müssen dargelegt bzw. von der Aufsichtsbehörde ermittelt werden. Interessenkonflikte müssen ausgeschlossen sein.

d) Es muss sichergestellt werden, dass registerführende Stellen und insbesondere registerführende Emittenten keine Erlaubnis nach § 32 Abs. 1 KWG erhalten, wenn eine Erlaubnis in Bezug auf die Führung eines übergeordneten Kryptowertpapierregisters nicht erteilt wurde.

e) Diese Sicherungsmechanismen müssen nicht zuletzt über den Tellerrand gedacht werden, wie das obige Beispiel der Kryptobörse *Binance* zeigt. Ein Vertrauen in Kryptofinanzmärkte kann nicht entstehen, wenn anerkannte Kryptobörsen sinngemäß Schrotttoken anbieten können.