MARTIN FRIES

Finanzausschuss des Deutschen Bundestages

An die Vorsitzende
Frau Bettina Stark-Watzinger MdB
Platz der Republik 1
11011 Berlin

Stellungnahme

zu Rahmenbedingungen für die Distributed-Ledger-Technologie im Finanzmarkt

Zum Antrag der FDP-Fraktion im Deutschen Bundestag und ihrer Abgeordneten vom 11. September 2018 (BT-Drucks. 19/4217) möchte ich einige Überlegungen beisteuern, die sich vorrangig auf die im Antrag unter Ziffer III. 7. und 8. geforderten Maßnahmen beziehen.

1. Rechtsgültigkeit von Smart Contracts

Die rechtswissenschaftliche Literatur ist sich weitgehend einig darüber, dass es sich bei den in jüngster Zeit vieldiskutierten *smart contracts* nicht um Verträge im klassischen Sinne, sondern um Programmcode handelt, der dazu dient, vertragliche Pflichten automatisiert zu erfüllen oder Gütertransaktionen automatisch zu vollziehen.

> *Kaulartz/Heckmann*, CR 2016, 618 (621)
> *Finck*, in: Fries/Paal (Hrsg.), Smart Contracts, 2019, S. 1 (4 ff.)

Wer sich in ein solches Transaktionsprogramm einklinkt, kann damit zwar in den Grenzen des Vertragsrechts und namentlich des AGB-Rechts einen Vertrag schließen. Ein solcher Vertragsschluss ist aber im Kern nichts Anderes als ein Online-Kauf mit Einzugsermächtigung für den Kaufpreis oder ein eBay-Gebot mit einem bedingten Handlungsauftrag für den automatischen Bietagenten. Regelungsbedarf für das deutsche Recht sehe ich an dieser Stelle nicht. Selbst diejenigen ausländischen Rechtsordnungen, die in den vergangenen Jahren Blockchain-Gesetze erlassen haben – siehe etwa die Arizona Revised Statutes, § 44-7061 (E) No. 2) sowie die

MARTIN.FRIES@JURA.UNI-MUENCHEN.DE

Tennessee Senate Bill 1662, § 47-10-201(2) – beschränken sich mit Blick auf *smart contracts* im Wesentlichen auf deskriptive Definitionen, die das bisher geltende Recht nicht entscheidend verändern.

Finck, Blockchain Regulation and Governance in Europe, 2019, S. 161 ff.
Fries, in: Brägelmann/Kaulartz (Hrsg.), Rechtshandbuch Smart Contracts, 2019, im Erscheinen

2. Sicherheitslücken bei Smart Contracts

Weil der Programmcode eines *smart contract* nicht notwendig mit dem vertraglichen Pflichtenprogramm übereinstimmt, kann es dazu kommen, dass der Code eine im Vertrag nicht vorgesehene Transaktion ausführt oder aber eine Transaktion nicht ausführt, die nach dem Vertrag eigentlich statthaft wäre. Ebenso können Dritte Lücken im Code zum unrechtmäßigen Zugriff auf Token oder andere Vermögenswerte nutzen. Solche Transaktionen geschehen im Sinne des § 812 Abs. 1 S. 1 BGB ohne Rechtsgrund und lassen sich daher auf dem Rechtsweg wieder rückgängig machen. Gleichwohl trägt natürlich der Betroffene, dessen Vermögenswert unrechtmäßig verschoben wurde, die Anspruchs- und Beweislast für seinen Bereicherungsanspruch wie auch das Risiko, dass die bereicherte Person unauffindbar oder insolvent ist.

Fries, AnwBl 2018, 86 (88 f.)
Heckelmann, NJW 2018, 504 (506)

Nun werden sich Fehler im vertragsausführenden Code nie ganz verhindern lassen. Umso mehr lohnt sich allerdings eine Investition in die Programmqualität von *smart contracts*. Nach meiner Wahrnehmung ist die Blockchain-Community für dieses Thema seit dem Hack der Investmentplattform *The DAO* 2016 durchaus sensibilisiert. Im Bereich des Finanzmarkts könnten gleichwohl Prüfkompetenzen der BaFin für weiter gesteigerte Sorgfalt auf Seiten der Programmgestalter sorgen. Die BaFin müsste hierfür ihre bereits bestehenden Kompetenzen im Bereich der Distributed-Ledger-Technologie ausbauen, was allerdings mit Blick auf die prognostizierte Bedeutung der Blockchain-Technologie ohnehin sinnvoll erscheint. Auch bei einer aktiveren Rolle der BaFin müsste freilich die Letztverantwortung für den Code und seine Fehler beim Emittenten bleiben.

Hoppen, „TheDAO-Hack" und der letzte Flug Otto Lilienthals am 09.08.1896, CR-online-Blog v. 21. Juni 2016
Möslein, ZBB 2018, 208 (209 ff.)

3. Einführung einer Blockchain-Form

Die meisten Rechtsordnungen kennen für rechtserhebliche Erklärungen und Verträge inzwischen neben der klassischen Schriftform auch eine elektronische Form. In Deutschland knüpft § 126a BGB diese Form an eine qualifizierte elektronische Signatur. Nun haben mehrere US-amerikanische Bundesstaaten vor kurzem eine Blockchain-Form geschaffen und der elektronischen Form gleichgestellt, vgl. Arizona Revised Statutes § 44-7061(A) und (B), Tennessee Senate Bill 1662, § 47-10-202(a) und (b), Vermont Statutes, Title 12, § 1913.

Der Erlass einer ähnlichen Vorschrift in Deutschland wäre im Moment allerdings nicht sinnvoll, weil die heute verbreiteten Distributed-Ledger-Technologien im Unterschied zur qualifizierten elektronischen Signatur nicht unbedingt eine Aussage zur Identität der Netzwerkteilnehmer einfordern. Demgegenüber erscheint es durchaus erwägenswert, eine Verbriefung von Wertpapieren nicht nur auf Papier, sondern auch in einem *distributed ledger* zu ermöglichen.

Kaulartz/Matzke, NJW 2018, 3278 (3281 ff.)

4. Blockchain und Datenschutzrecht

Ohne Frage gibt es erhebliche Spannungen zwischen dem in Europa soeben erst weitgehend harmonisierten Datenschutzrecht und der Blockchain-Technologie. Im Kern geht es darum, dass die europäische Datenschutz-Grundverordnung (DSGVO) in Art. 17 Abs. 1 ein Recht auf Vergessenwerden statuiert, während Distributed-Ledger-Technologien im Grundsatz ein lückenloses Gedächtnis haben. Die DSGVO gilt zwar wie auch das Bundesdatenschutzgesetz nur für *personenbezogene* Daten, ein solcher Personenbezug ist allerdings bei Finanztransaktionen regelmäßig herstellbar. Das Dilemma lässt sich nur auflösen, wenn man entweder das geltende Datenschutzrecht lockert oder die Blockchain-Technologie entsprechend anpasst.

Bei Art. 17 DSGVO handelt es sich um eine junge Norm mit durchaus rationalem Telos, die eine ewige Datenspeicherung gegen den Willen der Betroffenen ganz bewusst verhindern möchte. Insofern sind Lösungsansätze für das Dilemma weniger in einer DSGVO-Novelle, sondern eher bei einer Anpassung der Blockchain-Technologie zu suchen. Am ehesten möglich erscheint dabei eine Entkopplung des Personenbezugs von den im *distributed ledger* gespeicherten Daten, alternativ ggf. auch eine Zentralisierung der Blockchain-Verwaltung mit zusätzlichen Kompetenzen der verantwortlichen Stelle.

Schrey/Thalhofer, NJW 2017, 1431 (1433 ff.)
Martini/Weinzierl, NVwZ 2017, 1251 (1252 ff.)
Pesch, in: Fries/Paal (Hrsg.) Smart Contracts, 2019, S. 13 (18 ff.)

Es erscheint gegenwärtig offen, ob es gelingen wird, die Distributed-Ledger-Technologie datenschutzkonform weiterzuentwickeln, ohne dass sie ihre wesentlichen Vorteile, namentlich den Verzicht auf Intermediäre und die hohe Fälschungssicherheit, einbüßt. Sollte dieser Versuch scheitern, wäre immerhin nicht jegliche Nutzung von Blockchain-Anwendungen ausgeschlossen, denn außerhalb des Finanzmarkts gibt es im B2B-Bereich eine Vielzahl von Projekten, die vorrangig nicht mit personenbezogenen, sondern mit objektbezogenen Daten arbeiten und daher dem Anwendungsbereich von DSGVO und BDSG von vornherein nicht unterfallen.

Martin Fries ist Privatdozent an der Juristischen Fakultät der Ludwig-Maximilians-Universität München. https://twitter.com/mrtnfrs, https://www.youtube.com/jurapodcast/.

MARTIN.FRIES@JURA.UNI-MUENCHEN.DE