Blockchain: Rechtliche Hürden für „Smart Contracts"

Von Markus Kaulartz und Jörn Heckmann

Bildquelle: flickr/portal/gda

Blockchainbasierte Plattformen machen sogenannte selbstausführende Verträge möglich, bei denen die Bedingungen für die Ausführung zuvor programmiert wurden. Durch solche „Smart Contracts" wachsen IT und Recht zusammen. Denn die Programmcodes können schon deshalb keine alleinige Rechtswirkung entfalten, weil sie fehlerhaft oder manipuliert sein und Fälle eintreten können, die vom Willen mindestens eines der Vertragspartner abweichen. Red.

Betrachtet man die (noch sehr kurze) Geschichte der Blockchain-Technologie, so lassen sich Kryptowährungen wie Bitcoin als „Blockchain-1.0-Epoche" einordnen. Doch diese Epoche wird vermutlich nur von sehr kurzer Dauer sein. So schicken sich die Anhänger der Blockchain-Technologie zurzeit an, die blockchainbasierten Plattformen um die Möglichkeit einer komplexen Bedingungsprüfung vor Ausführung einer Transaktion zu erweitern. Sie legten damit den Grundstein für eine „Blockchain 2.0", welche erstmals die Ausführung sogenannter Smart Contracts ermöglicht.

„Selbst ausführende Verträge"

Solche Smart Contracts gelten als „the next big thing" im Bereich der blockchainbasierten Anwendungen. Sie sind keine Verträge im Rechtssinne, sondern automatisieren den Leistungsaustausch.

Nach dem Siegeszug der Kryptowährung Bitcoin ermöglicht eine technische Weiterentwicklung der blockchainbasierten Plattformen erstmals die Schaffung sogenannter „selbstausführender Verträge". Hierzu werden Transaktionen (zum Beispiel die Überweisung eines Betrags in einer Kryptowährung) vom Eintritt zuvor programmierter Bedingungen abhängig gemacht – dem Smart Contract. Die Ausführung erfolgt dabei auf den an einem P2P-Netzwerk beteiligten Rechner, ohne dass es zentraler, kontrollierender Intermediäre wie Treuhänder oder Banken bedürfte.

Auch einer menschlichen Instanz zur Überwachung der Smart Contracts bedarf es nicht. Dabei ist es keine zwingende Voraussetzung für das Vorliegen eines Smart Contract, dass dieser smart in jenem Sinne ist, wie der Begriff im Kontext von Industrie 4.0 für eine wie auch immer geartete „Intelligenz" oder „A.I. – Artificial Intelligence" gebraucht wird.

Zu den Autoren

Dr. Markus Kaulartz, Rechtsanwalt, CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, München, **Dr. Jörn Heckmann**, Rechtsanwalt, CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB, Hamburg

Nur für digital abbildbare Leistungen

Die Idee von Smart Contracts ist nicht neu. Sie wurden vielmehr bereits Ende der neunziger Jahre vom US-amerikanischen Juristen Nick Szabo diskutiert. Seine Vision: Ein Leasinggeber lässt einen Computer vor jeder Verwendung des Leasinggegenstands überprüfen, ob dieser die Leasingrate beglichen hat. Übertragen auf ein Autoleasing könnte beispielsweise der Boardcomputer die entsprechenden Abfragen vornehmen und gegebenenfalls die Zündung blockieren. Allerdings erschienen die damals verfügbaren Technologien zur wirtschaftlichen Umsetzung von Smart Contracts noch nicht fortgeschritten genug. Dies änderte sich erst mit dem Siegeszug blockchainbasierter Technologien, welche auf Grundlage vorgenommener Erweiterungen auch die Abbildung von Smart Contracts ermöglichen.

Es liegt in der Natur der Sache, dass der Smart Contract keine Leistungen aus der realen Welt durchführen kann (zum Beispiel die Reparatur eines Autos). Die durchzuführende Leistung muss vielmehr digital abbildbar sein, wie etwa die Bezahlung von (Krypto-)Geld, der Austausch digitaler Güter oder die Änderung eines blockchaingestützten Grundbuches. Weiter ist die Bedingungsprüfung von Smart Contracts

auf digital prüfbare Ereignisse beschränkt. Auch hier ist zwischen solchen Ereignissen zu unterscheiden, die durch Transaktionen in einer Blockchain abbildbar sind, und solchen, die in der realen Welt eintreten.

IT-Schnittstellen mit Manipulationsrisiko

Um Ereignisse der realen Welt erfassen zu können, sehen Smart Contracts dazu IT-Schnittstellen vor (Oracles genannt), welche es dem Smart Contract ermöglichen, mit der realen Welt zu interagieren. Den über das Oracle gelieferten Input kann der Smart Contract sodann verarbeiten und beispielsweise die Bezahlung einer Ware in Abhängigkeit zu einem Versandstatus veranlassen.

Die Entwicklung derartiger Schnittstellen steht noch ganz am Anfang. Hierbei werden neben der Frage der Standardisierung auch Fragen der IT-Sicherheit und der Manipulationssicherheit eine große Rolle spielen, zumal gerade diese IT-Schnittstellen prädestiniert für eine Manipulation des Smart Contracts von außen sind. Ein denkbares Angriffsszenario: Ein Hacker übermittelt über ein Oracle an eine Vielzahl von Smart Contracts wahrheitswidrig die Information, dass eine Bestellung versendet worden ist.

Reduzierung von Risiken und Transaktionskosten

Diesen Nachteilen stehen die Vorteile solcher „smarten" Verträge" gegenüber, welche insbesondere in der Reduzierung der Risiken und Transaktionskosten der Vertragsausführung zu sehen sind. Grund ist, dass der Eintritt der Bedingungen nicht manipuliert werden kann und Leistung und Gegenleistung damit garantiert sind. Durch eine angestrebte höhere Standardisierung sollen überdies durch Inkompatibilitäten hervorgerufene Kosten verringert werden. All dies soll Geschäftsfelder etwa im Mikrotransaktionsbereich ermöglichen und erleichtern.

Einer der Vorteile, auf den auch die öffentliche Verwaltung aufmerksam geworden ist, liegt zudem in der Möglichkeit, die Blockchain öffentlich les- oder beschreibbar auszugestalten. Hierdurch könnten Geldströme nachverfolgt, Berechtigungen überprüft oder authentifizierte Geschäfte durchgeführt werden. Die Stärke liegt in der Dokumentation, der Authentizität und der Irreversibilität von Transaktionen.

Natürlich konnten diese Herausforderungen auch mit herkömmlicher Technik gelöst werden. Durch den Einsatz von Smart Contracts soll dies aber effizienter und vertrauensvoller möglich sein. Smart Contracts sollten daher nicht dort zum Einsatz kommen, wo sich technische Implementierungen bereits bewährt haben und praktisch störungsfrei laufen. Vielmehr sollte sich der Einsatz auf jene Bereiche konzentrieren, die bislang nur umständlich und mit großen Reibungsverlusten bedient werden konnten. Es sollten also nicht Probleme für Smart Contracts geschaffen, sondern Smart Contracts sollten als Lösung für bestehende Probleme erwogen werden.

Erste praktische Anwendungen

Dies vorangestellt verwundert es nicht, dass Fintechs und Banken bereits damit begonnen haben, erste praktische Erfahrungen mit Smart Contracts zu sammeln. So gibt es erste Überlegungen, Börsengeschäfte ganz ohne Bank, Börsenmakler und zentrale Handelsplattform abzuwickeln. Der mitunter aussichtsreichste Anwendungsfall liegt vielleicht im Derivatehandel: Bereits Ende 2015 wurde das erste Papier auf der blockchaingestützten Handelsplattform Nasdaq Linq gehandelt.

Da der Einsatz von Smart Contracts die Gegenleistung garantiert, ist kein Vertrauen in den anonymen Vertragspartner vonnöten. Mit Blick auf mögliche Datenschutz- und Sicherheitsbedenken ist es noch nicht einmal zwingend erforderlich, auf eine öffentliche Blockchain (zum Beispiel bei Bitcoins) zu setzen. Diskutiert wird vielmehr auch der Einsatz privater Blockchains, die etwa aus einem Netzwerk teilnehmender Banken bestehen könnten. Schließlich testen auch Versicherungskonzerne Smart Contracts. Ein erstes Anwendungsbeispiel ist die Abbildung von Naturkatastrophen-Swaps und -Anleihen auf Grundlage von Smart Contracts. Hierzu kann beispielsweise der Bedingungseintritt „Unwetter" unter Berücksichtigung externer Wetterdaten, welche mittels eines Oracles an den Smart Contracts übergegeben werden, überprüft werden. Es steht zu erwarten, dass die noch sehr junge Branche der Insurtech-Start-ups mit ähnlichen Ideen folgen wird.

Das „Code is law"-Dogma ist ein Irrtum

Auch die juristische Perspektive spielt eine wichtige Rolle. Zunächst muss ein großer Irrtum beseitigt werden: Smart Contract-Anhänger frohlocken bei dem Gedanken, dass zukünftig einzig der Programmcode Rechtswirkung entfalten könnte. Es bräuchte dann – so die Hoffnung mancher Entwickler – weder Anwälte noch Gerichtsvollzieher zur Erstellung und Durchsetzung der Smart Contracts. Die rechtliche Beziehung – so die weitere Vorstellung mancher Entwickler – ergäbe sich einzig und alleine aus dem Code – „Code is Law". Eine Vision, welche der amerikanische Jurist Laurence Lessig bereits 1999 in seinem Buch „Code and Other Laws of Cyberspace", vorstellte.

Diese Hoffnung hat mit der rechtlichen Wirklichkeit jedoch wenig gemein: Das „Code is Law"-Dogma steht im Konflikt damit, dass das deutsche Recht teilweise zwingend und damit nicht dispositiv ist. Es versteht sich, dass ein Smart Contract diese vom Gesetzgeber gezogene Grenze nicht überschreiten kann – ebenso wenig wie ein Vertrag auf Papier. Oder anders gewendet: Der „Code" ist nicht das einzige „Law". Es gelten zusätzlich alle vom Gesetzgeber als zwingend angesehenen, nicht dispositiven Gesetze. Diesen können sich die Vertragsparteien auch nicht durch wie auch immer geartete Erklärungen im

Programmcode verschließen. So wird ein Vertrag etwa nicht allein nach seinem Wortlaut (beziehungsweise im Falle eines Smart Contracts nach seinem Programmcode) beurteilt. Vielmehr sieht das Bürgerliche Gesetzbuch vor, dass sich der Inhalt eines Vertrags in jedem Einzelfall nach dem Willen der Vertragsparteien bestimmt. Hierzu sind auch die Begleitumstände des Vertragsschlusses bei der Auslegung des Vertrags heranzuziehen. Was sich für die Anhänger des „Code is Law"-Dogmas auf den ersten Blick wie ein Anachronismus längst vergangener Zeiten anhört, entpuppt sich schnell als Segen, etwa wenn der Smart Contract fehlerhaft programmiert wurde. In diesen Fällen nämlich gilt das von den Vertragsparteien Gewollte und nicht das von den Vertragsparteien in Code Abgebildete.

Dass ein solcher fehlerhafter Smart Contract nicht lediglich eine theoretische Möglichkeit ist, hat die Kontroverse um den sogenannten The-DAO-Hack eindrucksvoll gezeigt: Bei The DAO handelt es sich um eine autonome Organisation (Decentralized Autonomous Organization – DAO), welche gegründet wurde, indem „Anleger" auf Grundlage eines Smart Contracts digitale Anteile erwerben konnten. Diese wurden als Smart Assets in der Blockchain hinterlegt, ähnlich einem Investmentfonds. Im Gegenzug erhielt der Anleger Stimmrechte über die Verwendung der Investitionen. The DAO umfasste zusätzlich eine sogenannte Split-Funktion, die es Investoren erlauben sollte, aus der Gesellschaft auszuscheiden und ihr Kapital in eine Art Tochtergesellschaft abzuziehen. Durch eine wiederholte Ausführung dieser Funktion gelang es allerdings einem Unbekannten, etwa 40 bis 60 Millionen Dollar auf eine Tochtergesellschaft zu transferieren. Dieser Transfer war möglich, da der Smart Contract dem Angreifer durch die wiederholte Ausführung der Split-Funktion fälschlicherweise Zugriff auf Anlagevermögen anderer Anteilseigner ermöglichte.

Es ist offensichtlich, dass das selbstpostulierte „Code is Law"-Dogma im Falle des The-DAO-Hacks zu untragbaren Ergebnissen führen würde. Dies erkannten auch die Gründer und ließen die Community darüber abstimmen, ob die Plattform so umprogrammiert werden soll, dass die Ausnutzung der Programmlücke rückgängig gemacht wird (sogenannter hard fork). Wenig überraschend fand dieser Vorschlag große Zustimmung. Die Befürworter rechtfertigten dieses Vorgehen unter anderem mit dem Hinweis, dass The DAO einen Status erreicht hatte, welcher sich mit „too big to fail" umschreiben lässt. Im Anschluss kommentierte einer der Mitgründer dieses Ergebnis mit: „Wir haben gerade unseren obersten Gerichtshof gefunden – die Community".

Mag dieses Ergebnis auch gerecht klingen: Rechtstaatlich legitimiert war dieses Vorgehen nicht. Kritiker weisen daher zu Recht darauf hin, dass durch das gewählte Vorgehen und die Durchbrechung der Gewaltenteilung letztlich das Vertrauen in Smart Contracts generell unterminiert wird. Dies könnte das Lehrgeld sein, das die Community dieser neuen Technologie aufbringen musste.

Mit rechtlichen Gegebenheiten harmonisieren

Die weitere Entwicklung von Smart Contracts steht somit nicht nur vor technischen Herausforderungen, sondern hängt auch von einer Lösung der damit im Zusammenhang stehenden rechtlichen Fragen ab. Nur so lässt sich verhindern, dass einem Missbrauch von fehlerhaften Smart Contracts zukünftig Tür und Tor geöffnet wird.

Es zeigt sich dabei, dass das Recht bereits jetzt genügend Instrumentarien bereithält, um die rechtlichen Herausforderungen von neuen Technologien wie Smart Contracts zu meistern. Teilweise bedarf es aber noch einer Harmonisierung der Smart Contracts mit den rechtlichen Gegebenheiten: So erweist sich der Automatismus der tatsächlichen Leistungserbringung durch den Smart Contract dort als Schwäche, wo er vom tatsächlichen Willen mindestens einer Vertragspartei abweicht.

Schiedsstellen programmieren

Für jene Fälle kann es im Einzelfall sinnvoll sein, im Algorithmus den Zugang für eine Art Schiedsstelle zu ermöglichen, auch wenn dies manchen Vorzügen der Blockchain zuwiderläuft. Als Schiedsstelle kommt jede Person oder Institution in Betracht, auf die sich die Parteien im Vorfeld als neutralen Dritten verständigen. Das Intervenieren einer Schiedsstelle könnte darin bestehen, dass diese etwa über die Richtigkeit von Informationen aus dritter Quelle (zum Beispiel den Börsenkurs zu einem bestimmten Zeitpunkt) oder über Programmierfehler entscheidet, die dem rechtlichen Vertrag widersprechen. Am Ende könnte der Schiedsstelle dann die Möglichkeit eröffnet sein, die Vertragsdurchführung und damit den Vermögensfluss zu steuern und bei Bedarf rückabzuwickeln. Da der Smart Contract nur ausführen kann, was in seinem Programmcode steht, gilt auch hier, dass der Zugang der Schiedsstelle sowie die Möglichkeiten der Schiedsstelle zuvor einprogrammiert werden müssten. Hier werden also bereits die Schranken der Schiedsstelle festgelegt.

Offene rechtliche Fragen

Juristen müssen offene Fragen im Bereich des Daten- und Verbraucherschutzrechts, des Wettbewerbs- und Kartellrechts sowie Fragen der Haftung für (fehlerhaft programmierte) Smart Contracts im Blick zu behalten. Entwickler sind ganz grundsätzlich gut beraten, mit Anwälten zusammenzuarbeiten, um Lücken des Smart Contracts im Vergleich zum anwendbaren Recht zu schließen. Überdies ist sicherzustellen, dass auf Smart Contracts gestützte Rechtsbeziehungen unter Umständen auch rückabgewickelt werden und Gewährleistungsrechten zugänglich sein müssen. Dies führt zu einer spannenden Verschmelzung der Disziplinen Technik und Recht.