

## Blockchain – ein Thema für die Finanzaufsicht?

Das Ziel der BaFin ist es, für einen stabilen und sicheren Finanzplatz zu sorgen, wobei das Aufsichtsrecht grundsätzlich technologie-neutral ist. Blockchain ist aber nicht bloß eine technologische Weiterentwicklung, sondern berührt auch Geschäfts- und Organisationsprozesse. Dies gilt für einzelne Unternehmen und über die Grenzen von Organisationen hinaus. Durch den Einsatz der Blockchain-Technologie könnten sich Systeme und Prozesse beaufsichtigter Unternehmen tiefgreifend verändern.

### Blockchain – was ist das?

Der 1976 erstmals in einem Patent erwähnte Begriff Blockchain bedeutet fälschungssichere, verteilte Datenstrukturen ohne zentrale Instanz, in denen Transaktionen in der Zeitfolge protokolliert und nachvollziehbar sind. Das ermöglicht kryptografisch gesicherte, dezentrale Transaktionen ohne Intermediäre. Hierbei werden Spieltheorie, Kryptografie und Peer-To-Peer-Technologie miteinander verbunden.

Seit Januar 2009 existiert als Kombination dieser Bereiche das Bitcoin-Netzwerk. Bitcoin zeigt, dass die darunterliegende Blockchain-Technologie erfolgreich eingesetzt werden kann. Hierbei gilt es zwischen Bitcoin und Blockchain zu unterscheiden. Vereinfacht gesagt ist die Blockchain-Technologie ein technologisches Rahmenwerk, und Bitcoin nur der bekannteste Anwendungsfall. Die virtuelle Währung dient zum Bezahlen, der Begriff Bitcoin bezeichnet aber auch das gesamte Netzwerk, das aus allen Bitcoin-Teilnehmern gebildet wird.

Als Bezeichnung kommen Blockchain und Distributed-Ledger-Technologie (DLT) zum Einsatz. Eine einheitliche und akzeptierte Definition oder Abgrenzung dieser Begriffe existiert noch nicht. Derzeit finden bei der Internationalen Standardisierungsorganisa-

tion (ISO TC 307) die ersten Arbeiten statt, um eine solche Abgrenzung und Definition global zu etablieren. In der Praxis werden die Begriffe oftmals synonym verwendet, wobei Blockchain vermehrt verwendet wird.

### Public- und Private-Varianten

Blockchains existieren als Public- und Private-Variante. Bei Public Blockchains, also öffentlichen Netzwerken wie zum Beispiel Bitcoin, steht es jedermann frei, sich zu beteiligen. Bei Private Blockchains, also privaten Netzwerken wie zum Beispiel bei Unternehmenskonsortien, sind Teilnahme und Berechtigungen beschränkt. Um laufende

Transaktionen zu bestätigen, kommen Konsensmechanismen zum Einsatz, bei denen sich die Netzwerkteilnehmer einbringen. Ein verbreitetes Verfahren dafür ist Proof-Of-Work. Hierbei wird eine kryptografische Aufgabe als Arbeitsnachweis der Validierung und Bestätigung von Transaktionen gelöst. Anders als bei Fiatgeld, das die Notenbanken theoretisch unbegrenzt ausgeben können, erfolgt die Schaffung neuer Bitcoins innerhalb des Bitcoin-Netzwerks über ein kryptografisches Verfahren, das man als Mining bezeichnet.

Die Sicherheitsverfahren der Blockchain-Technologie nutzen regelmäßig aktuelle asymmetrische Verschlüsselungstechnologien und Hash-Algorithmen. Hierdurch wird ein unberechtigter Zugriff ausgeschlossen und die Transaktionen lassen sich verhältnismäßig einfach validieren. Bei Public Blockchains sind alle jemals getätigten Transaktionen üblicherweise öffentlich einsehbar und somit nachvollziehbar. Da hierbei die gerade erwähnten Verschlüsselungstechnologien genutzt werden, sind die Informationen nach derzeitigem Wissen unveränderlich.

Bei einigen Blockchain-Netzwerken, wie etwa Ethereum, können auch Smart Contracts zum Einsatz kommen. Diese Smart Contracts sind, stark vereinfacht, programmierte Vereinbarungen, deren Programmcode auf einer Blockchain hinterlegt ist. Ziel ist die Reduktion von Transaktionskosten und eine Erhöhung der Vertragssicherheit, allerdings sind hier noch Fragen wie Rechtssicherheit oder vertragliche Auslegungen ungeklärt.

### Erlaubnispflicht je nach Art des Einsatzes

Welche Aspekte sind aus regulatorischer Sicht zu beachten? Das Aufsichtsrecht ist grundsätzlich technologie-neutral und der

*Christoph Kreiterling, Referat Kompetenz IT-Sicherheit, und Stephan Mögelin, Referat Aufsicht über Finanzmarktinfrastrukturen, beide Bundesanstalt für Finanzmarktaufsicht, BaFin, Bonn und Frankfurt am Main*

*Die Blockchain-Technologie wird von der hiesigen Bankenaufsicht als finanztechnologische Innovation identifiziert. Ihr Einsatz in der Praxis kann Systeme und Prozesse beaufsichtigter Unternehmen tiefgreifend verändern. Insofern bedarf ihre Umsetzung in der Finanzdienstleistungsbranche der aufmerksamen aufsichtlichen Begleitung. Mit diesem Tenor verdeutlichen die Autoren, einerseits neue technologische Entwicklungen nicht behindern, andererseits aber auch ihren gesetzlichen Auftrag umsetzen zu wollen. Angefangen von der Vereinfachung und Automatisierung bisher manueller Geschäftsprozesse bis hin zur Reduktion von Betrugsmöglichkeiten registrieren sie zwar viel mögliche Vorteile eines Praxiseinsatzes, sie listen aber auch viele offene Fragen auf, die jeder Anwender sorgfältig prüfen sollte. Risiken können hierbei insbesondere in den Bereichen Technik, Kryptografie, Aufsichtsrecht, Regulatorik und Wirtschaftlichkeit liegen. (Red.)*

Einsatz der Blockchain-Technologie an sich nicht erlaubnispflichtig. Entscheidend für eine mögliche Erlaubnispflicht ist die Art des Einsatzes. Ausschlaggebend ist die Frage, im Rahmen welcher Geschäftstätigkeit die Blockchain-Technologie genutzt wird. Weil die Anwendungsmöglichkeiten für die Blockchain-Technologie vielfältig sind, ist eine pauschale Aussage zur Erlaubnispflicht nicht möglich. Anwendungsschwierigkeiten des Aufsichtsrechts ergeben sich dann, wenn mangels zentraler Instanz dessen Durchsetzung aufgrund fehlender Adressaten erschwert oder unmöglich würde. Grundsätzlich gelten auch beim aufsichtlich relevanten Einsatz der Blockchain-Technologie die entsprechenden Vorgaben wie zum Beispiel die besonderen geldwäscherechtlichen Anforderungen an Legitimitätsprüfungen (Know Your Customer).

**Virtuelle Währungen:** Die Nutzung virtueller Währungen wie Bitcoin als Ersatz für Bar- oder Buchgeld ist keine erlaubnispflichtige Tätigkeit. Der Dienstleister oder Lieferant kann seine Leistungen mit virtuellen Währungseinheiten bezahlen lassen, ohne dass er dadurch Bankgeschäfte oder Finanzdienstleistungen erbringt. Gleiches gilt für den Kunden. Ebenso stellt das Mining von virtuellen Währungseinheiten an sich kein erlaubnispflichtiges Geschäft dar, da der Miner die neu geschaffenen Währungseinheiten nicht selbst emittiert oder platziert. Auch der Verkauf selbst geschürfter oder erworbener virtueller Währungseinheiten oder deren Ankauf sind grundsätzlich nicht erlaubnispflichtig. Treten jedoch weitere Umstände hinzu, kann der gewerbliche Umgang etwa eine Erlaubnispflicht nach dem Kreditwesengesetz auslösen.

**Zahlungsverkehr:** Internationale Zahlungen via Blockchain könnten in nahezu Echtzeit abgewickelt und bestätigt werden und die Transaktionskosten reduzieren. Dieses Verfahren könnte den klassischen Zahlungsverkehr wie auch neue alternative Bezahlfverfahren revolutionieren. Grundsätzlich könnte die Blockchain-Technologie im Zahlungsverkehr zu einer unmittelbaren Interaktion der Teilnehmer führen, die die Rolle bestehender Intermediäre infrage stellt (Disintermediation).

**Wertpapiermärkte- und Nachhandelssegment:** Beim Post-Trade werden die Tätigkeiten des Nachhandelssegments umgesetzt, die im Anschluss an ein Handels-

geschäft mit einem Wertpapier oder Finanzinstrument erfolgen. Darunter fallen unter anderem das Clearing und Settlement. Die gesetzlichen Bestimmungen und Anforderungen sehen für bestimmte Finanzinstrumente im Bereich Clearing (zum Beispiel OTC-Derivate) den Einsatz einer zugelassenen zentralen Gegenpartei vor. Ebenso ist im Bereich Settlement (Abwicklung eines Wertpapiergeschäfts) der Einsatz eines zugelassenen Zentralverwahrers vorgesehen.

### Viele rechtliche Fragen

Ob sich die gesetzlichen Anforderungen mit dem Einsatz von Blockchain-Technologie umsetzen lassen, ist noch fraglich. Die zentrale Funktion der Finanzmarktinfrastrukturen und die Zulassungspflicht als juristische Person stehen im Widerspruch zur Dezentralität der Blockchain-Technologie. Darüber hinaus besteht mangels konkreter Anwendungsfälle bisher keine aufsichtliche Bewertung. Die aufsichtlichen Vorgaben sind jedoch auch hier grundsätzlich technologieneutral.

Beim Einsatz der Blockchain-Technologie ist die Zusammenarbeit von verschiedenen Systemen und Techniken entscheidend. Blockchain-Lösungen müssen grundsätzlich interoperabel sein: einerseits innerhalb eines Blockchain-Systems gegenüber den IT-Systemen der Teilnehmer, andererseits systemübergreifend gegenüber anderen Marktteilnehmern. Insbesondere in den Bereichen Clearing und Settlement bestehen oft direkte beziehungsweise indirekte Anbindungen an die Zahlungssysteme der Zentralbanken, die hier zu berücksichtigen sind. In den aufsichtsrechtlichen Fokus fallen Blockchain-Lösungen auch, wenn zum Beispiel Wertpapiere per Token zur Abbildung in einer Blockchain übertragen werden.

### Auswirkungen auf Geschäftsprozesse

Welche Herausforderungen sind bei Blockchain erkennbar? Die Innovation Blockchain hat das Potenzial, einige bankfachliche Geschäftsprozesse zu ändern. So erfordern etwa bislang unterschiedliche Betriebsabläufe einer Bank die Abstimmung getrennter Bücher. Die Blockchain-Technologie könnte diesen Prozess durch eine einheitliche Datenhaltung und Datenstruktur vereinfachen. Risiken können hierbei insbesondere in den Bereichen

Technik, Kryptografie, Aufsichtsrecht, Regulatorik, Wirtschaftlichkeit und operationale Einbettung bestehen.

Diese Risiken können dann etwa bei technischen Umstrukturierungen auftreten, da das einmal festgelegte Protokoll bei der komplexen Technik nur schwierig zu ändern ist, da Änderungen mit den Netzwerkpartnern durchgeführt werden. Fragen der Skalierbarkeit und Transaktionsvolumina stellen ein weiteres Risiko dar. Blockchains haben regelmäßig einen wachsenden Speicherbedarf und es besteht Abhängigkeit von den eingesetzten kryptografischen Verfahren. So könnten bei einer technischen Umstrukturierung, etwa durch Weiterentwicklungen der kryptografischen Standards, Inkompatibilitäten mit bestehenden Implementierungen festzustellen sein. Jedoch scheinen sich für manche Beschränkungen Lösungen abzuzeichnen. Die weitere Entwicklung wird zeigen, inwiefern solche Herausforderungen zukünftig bewältigt werden können.

Grundsätzlich funktionieren Blockchains ohne die Grenzen von Nationalstaaten. Das beste Beispiel dafür ist Bitcoin, wo die Teilnehmer des Netzwerks weltweit verteilt sind. So könnten sich etwa zwei Transaktionsbeteiligte in unterschiedlichen Jurisdiktionen befinden. Dies könnte bei sich widersprechenden rechtlichen Regelungen zur Frage führen, welches Regelwerk im Zweifel anzuwenden ist. Daneben ist bislang richterlich beziehungsweise juristisch ungeklärt, welchen Stellenwert eine Blockchain-Transaktion oder Smart Contracts haben. Allerdings gilt auch bei Einsatz von Blockchains der bestehende regulatorische Rahmen der BaFin, wenn die Beteiligten dem deutschen Aufsichtsrecht unterliegen.

Als wirtschaftliches Risiko gilt insbesondere, dass beim Einsatz der Blockchain-Technologie einmal ausgeführte Transaktionen grundsätzlich nicht rückgängig gemacht werden können, da sie kryptografisch abgesichert wurden. Obwohl sich Transaktionsbeteiligte nicht persönlich bekannt sein müssen, können sie sich darauf verlassen, dass eine einmal durchgeführte Transaktion Bestand hat und somit irreversibel in der Blockchain verzeichnet ist. Die Frage, ob das eigene Geschäftsmodell überhaupt mit den Ansätzen der Blockchain-Technologie kompatibel ist und die Frage der Finalität von Blockchain-Transaktionen können ebenfalls Risiken darstellen. Auch Fra-

## Zeitschrift für das gesamte Kreditwesen



### Verlag und Redaktion:

Verlag Fritz Knapp GmbH  
Aschaffburger Str. 19, 60599 Frankfurt,  
Postfach 70 03 62, 60553 Frankfurt.

Telefon: (0 69) 97 08 33 - 0, Telefax: (0 69) 7 07 84 00  
E-Mail: red.zfgk@kreditwesen.de  
Internet: www.kreditwesen.de

**Herausgeber:** Klaus-Friedrich Otto

**Chefredaktion:** Dr. Berthold Morschhäuser (Mo),  
Philipp Otto (P.O.)

**Redaktion:** Swantje Benkelberg (sb), Daniel  
Rohrig (dro), Hanna Thielemann (Volontärin, ht),  
Philipp Hafner (Volontär, ph), Frankfurt am Main

**Redaktionssekretariat und Layout:** Anja Oehrl

Die mit Namen versehenen Beiträge geben nicht immer die Meinung der Redaktion wieder. Bei unverlangt eingesandten Manuskripten ist anzugeben, ob dieser oder ein ähnlicher Beitrag bereits einer anderen Zeitschrift angeboten worden ist. Beiträge werden nur zur Alleinveröffentlichung angenommen.

Die Zeitschrift und alle in ihr enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig.

**Manuskripte:** Mit der Annahme eines Manuskripts zur Veröffentlichung erwirbt der Verlag vom Autor das ausschließliche Verlagsrecht sowie das Recht zur Einspeicherung in eine Datenbank und zur weiteren Vervielfältigung zu gewerblichen Zwecken in jedem technisch möglichen Verfahren. Die vollständige Fassung der Redaktionsrichtlinien finden Sie unter [www.kreditwesen.de](http://www.kreditwesen.de).

**Verlags- und Anzeigenleitung:** Uwe Cappel,  
Frankfurt am Main, Aschaffburger Str. 19.

**Anzeigenverkauf:** Hans-Peter Schmitt,  
Tel. (0 69) 97 08 33-43, Frankfurt am Main,  
Aschaffburger Str. 19.

Zurzeit ist die Anzeigenpreisliste Nr. 59 vom 1.1.2017 gültig.

**Zitierweise:** KREDITWESEN

**Erscheinungsweise:** am 1. und 15. jeden Monats.

**Bezugsbedingungen:** Abonnementspreise inkl. MwSt. und Versandkosten: jährlich € 593,15, bei Abonnements-Teilzahlung: 1/2-jährlich € 304,75, 1/4-jährlich € 155,45. Ausland: jährlich € 615,47. Preis des Einzelheftes € 24,00 (zuzügl. Versandkosten).

**Verbundabonnement** mit der Zeitschrift »bank und markt«: € 904,29, bei Abonnements-Teilzahlung: 1/2-jährlich € 474,77, 1/4-jährlich € 248,99. Ausland: jährlich € 931,65.

Studenten: 50% Ermäßigung (auf Grundpreis).

Der Bezugszeitraum gilt jeweils für ein Jahr. Er verlängert sich automatisch um ein weiteres Jahr, wenn nicht einen Monat vor Ablauf dieses Zeitraumes eine schriftliche Abbestellung vorliegt. Bestellungen direkt an den Verlag oder an den Buchhandel.

Probeheftanforderungen bitte unter  
Tel.: (0 69) 97 08 33-25.

Bei Nichterscheinen ohne Verschulden des Verlags oder infolge höherer Gewalt entfallen alle Ansprüche.

**Bankverbindung:** Landesbank Hessen-Thüringen Girozentrale, Frankfurt am Main, IBAN: DE73 5005 0000 0010 5550 01, BIC: HELADEF3333

**Druck:** Druck- und Verlagshaus Zarbock GmbH & Co. KG, Sontraer Straße 6,  
60386 Frankfurt am Main.

ISSN 0341-4019

gen der Haftung sind insbesondere beim Einsatz von Public Blockchains vielfach noch unbeantwortet.

### Viele Vorteile

Wie könnte sich Blockchain zukünftig entwickeln? Die BaFin hat die Blockchain-Technologie als finanztechnologische Innovation identifiziert, die umfangreiche Änderungen in der Finanzdienstleistungsbranche auslösen könnte. Daher verfolgt die BaFin die weitere Entwicklung aufmerksam. Nach derzeitiger Einschätzung liegt bei den Unternehmen, die die BaFin beaufsichtigt, das Wertschöpfungspotenzial von Blockchains zukünftig in den folgenden Bereichen, wobei diese Aufzählung weder vollständig noch abschließend ist:

– Vereinfachung und Automatisierung bisher manueller Geschäftsprozesse.

– Optimierung von bestehenden Prozessabläufen und Produkten (zum Beispiel durch Echtzeitabwicklung, Skalierbarkeit und Transparenz)

– Effizienzsteigerung durch nahezu Echtzeitüberwachung der Finanzmarktteilnehmer untereinander.

– Reduktion des Ausfallrisikos von Gegenparteien, da Verträge in einem sichereren und automatisierten Umfeld ausgeführt werden und auch Zeiten für mögliche Folge- oder Anschlusstransaktionen sinken könnten.

– Reduktion von Betrugsmöglichkeiten.

### Offene Fragen

Welche grundlegenden Fragen sind vor dem Einsatz von Blockchains zu beantworten? Auch beim Einsatz der Blockchain-Technologie gelten die zentralen Schutzziele der IT-Sicherheit (vergleiche unter anderem MaRisk AT 7.2): Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit. Daneben könnten die folgenden Fragen als Anregung beim möglichen Einsatz von Blockchains dienen:

– Stellt die Blockchain-Verschlüsselung einen ausreichend hohen Schutz für den eigenen Schutzbedarf der Daten dar?

– Ist ein Perimeterschutz oder ein physische Trennung der Daten nötig?

– Unterliegen die Transaktionen der Geheimhaltung?

– Wird eine zentrale Instanz oder Stelle benötigt, um Konflikte zu lösen?

– Ist es erforderlich, dass nur eine zentrale Instanz Transaktionen validieren kann?

– Ist die nachträgliche Änderbarkeit von Daten erforderlich?

– Handelt es sich um ein Netzwerk mit einer kleinen Anzahl von Teilnehmern?

– Wird den anderen Teilnehmern des Netzwerkes ein akzeptabel hohes Maß an Vertrauen entgegengebracht?

– Wird bei den Transaktionen eine große Menge an Daten gespeichert?

– Sind die Transaktionsvolumina hoch in Bezug auf die absolute Anzahl von Transaktionen oder auch bezogen auf die Anzahl pro Zeiteinheit?

– Wird über das Netzwerk hinaus eine große Zahl von Schnittstellen zu anderen Netzen oder Altsystemen benötigt, um Daten auszutauschen?

Diese Fragen dienen als Anregung. Sie ersetzen keineswegs eine individuelle Analyse, die vor dem Einsatz jeglicher Technologie steht.

### Aufmerksame aufsichtliche Begleitung

Welchen Regulierungsansatz verfolgt die BaFin bei der Blockchain-Technologie? Die BaFin wird auch bei der Blockchain-Technologie ihren gesetzlichen Auftrag umsetzen. Da es sich um eine noch recht neue Technologie handelt, bei der sich aufsichtlich relevante „Use Cases“ gerade erst entwickeln, wird die BaFin diese Entwicklungen aufmerksam verfolgen und aufsichtlich begleiten. Dabei wird die BaFin ihren Ansatz der Proportionalität des Aufsichtshandelns und der Technologieneutralität auch hier weiter umsetzen. Ziel der BaFin ist es dabei einerseits, Innovationen nicht unnötig zu behindern, andererseits aber auch die Integrität des Finanzplatzes und ein Level Playing Field zu gewährleisten. Daher geht die BaFin auch beim Einsatz der Blockchain-Technologie nach dem bewährten Grundsatz „gleiches Geschäft, gleiches Risiko, gleiche Regulierung“ vor.