Von Bitcoin zum Smart Contract

Anwendungspotenziale der Blockchain-Technologie

In der digitalen Wirtschaft wird die Blockchain-Technologie derzeit häufig als eine der nächsten großen Innovationen bezeichnet. Was zunächst vor allem als Grundlage des virtuellen Zahlungsmittels Bitcoin in Fachkreisen bekannt war, ist neuerdings Geschäftsmodell von Start-up-Unternehmen und Forschungsprojekt von Konzernen. Dieser Beitrag gibt einen ersten Einblick darin, was sich hinter dem Schlagwort „Blockchain“ verbirgt, und wirft einen Blick auf mögliche Anwendungsbereiche.

Bitcoin als Beispiel für die Funktionsweise der Blockchain

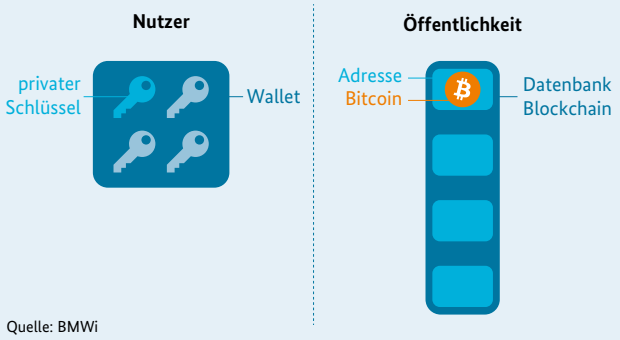
Eine Blockchain ist eine verschlüsselte Datenbank von in Blöcken zusammengefassten Informationen, die auf allen Rechnern eines Blockchain-Netzwerks gleichzeitig gespeichert wird. Ein Verschlüsselungsverfahren sorgt dafür, dass ihr Inhalt leicht ablesbar, aber zugleich schwer manipulierbar ist.

Das erste und in der Öffentlichkeit bekannteste Anwendungsbeispiel für die Blockchain-Technologie ist das seit 2009 bestehende virtuelle Zahlungsmittel Bitcoin, das von mehreren Dienstleistern im Internet sowie vereinzelt auch in physischen Geschäften akzeptiert wird. Für Bitcoin wird ein Blockchain-Netzwerk genutzt, um Zahlungsvorgänge zu dokumentieren und Guthaben zuzuordnen.

Bitcoin basiert auf einem weltweit offenen Netzwerk: Jeder Betreiber eines Computers kann sich dem Bitcoin-Netzwerk anschließen, indem er ein Programm installiert und die dazugehörige Blockchain-Datenbank aus dem Bitcoin-Netzwerk auf seinen Rechner herunterlädt. In der Blockchain des Bitcoin-Netzwerks sind in verschlüsselter Form virtuelle Währungseinheiten, so genannte Bitcoin, verzeichnet und jeweils einer bestimmten Adresse zugeordnet. Bildlich gesprochen gleicht die Adresse einem Schließfach, in dem Bitcoin gelagert werden können, während die Blockchain einem öffentlichen Raum gleicht, in dem die Schließfächer mit Bitcoin untergebracht sind. Zu einer Adresse gehört jeweils ein privater (geheimer) Schlüssel, der Zugang zum Inhalt der Adresse (den Bitcoin) verschafft. Den Schlüssel muss man sich als eine Zeichenfolge vorstellen, die jeweils mit einer dazugehörigen Adresse korrespondiert.

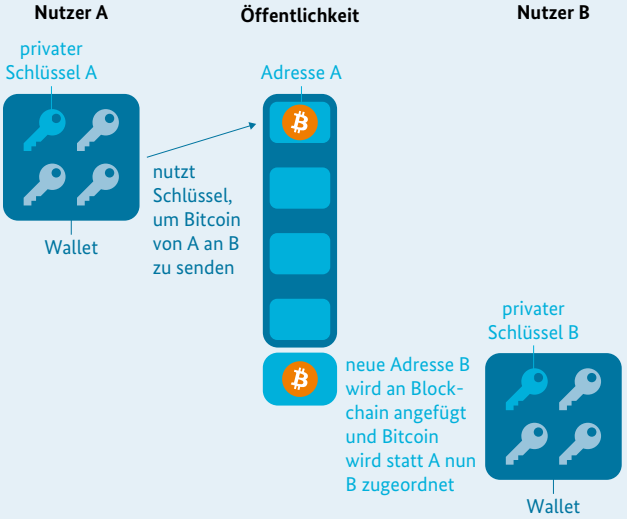
Nutzer der Bitcoin-Blockchain können ihre privaten Schlüssel in einem so genannten „Wallet“ speichern. Im Unterschied zu einer physischen Geldbörse ist diese digitale Geldbörse ein Software-Programm, das nicht Bitcoin selbst (das Geld) enthält, sondern die privaten Schlüssel, die es ermöglichen, an bestimmten Adressen der Blockchain (den Schließfächern) über Bitcoin zu verfügen.

Abbildung 1: Bitcoin und privater Schlüssel



Quelle: BMWi

Abbildung 2: Bitcoin-Transaktion



Quelle: BMWi

Wer Bitcoin erwerben will, kann mit seinem Computer eine (zunächst leere und nicht auf der Blockchain verzeichnete) Adresse generieren. Er muss dann einen Geschäftspartner finden, der ihm bereits auf der Blockchain verzeichnete Bitcoin überträgt. Das ist beispielsweise in Bitcoin-Börsen im Internet möglich. Der Veräußerer muss seinen privaten Schlüssel zu einer Adresse auf der Blockchain dazu verwenden, um die dieser Adresse zugeordneten Bitcoin der Adresse des Empfängers zuzuordnen. Der private Schlüssel legitimiert den Veräußerer gleichsam, über in dem passenden Schließfach abgelegte Bitcoin zu verfügen und sie in das Schließfach des Empfängers zu transferieren. Diese neue Zuordnung von Bitcoin wird an das Blockchain-Netzwerk gemeldet. Die Blockchain-Datenbank wird danach von einem Netzwerk-Rechner in einem rechenintensiven Verfahren um einen zusätzlichen verschlüsselten Informationsblock erweitert, der die Neuzuordnung der verkauften Bitcoin an die Adresse des Zahlungsempfängers enthält. Damit wird die Transaktion bestätigt. Die erweiterte Blockchain wird dann von den übrigen Teilnehmern des Netzwerks nach und nach übernommen.

Bisher hält sich die Akzeptanz von Bitcoin – besonders außerhalb des Internet – in Grenzen. Ob Bitcoin sich etablieren kann, ist noch ungewiss. Spektakuläre Fälle von Passwort-Diebstählen haben die Sicherheit von Bitcoin im alltäglichen Gebrauch in Frage gestellt. Zudem ist die Leistungsfähigkeit des Bitcoin-Netzwerks begrenzt; die Bestätigung einer Transaktion dauert rund zehn Minuten. Für zeitkritische Anwendungen, etwa am Finanzmarkt, dürfte Bitcoin deshalb wenig attraktiv sein.

Die grundlegende Eigenschaft der Blockchain-Technologie – die in einem dezentralen Netzwerk in einer Blockchain-Datenbank abgelegten Informationen sind kaum manipulierbar und für jedermann leicht lesbar – macht diese über Bitcoin hinaus aber auch für eine Fülle weiterer Einsatzzwecke interessant.

Neue Anwendungen für die Blockchain-Technologie

Die bisher bekannten Anwendungen, die allerdings meist noch nicht über die Erprobungsphase hinausgekommen sind, lassen sich nach zwei Zielrichtungen unterscheiden:

- Nutzung der Blockchain zur sicheren Dokumentation (Notariatsfunktion)
- Nutzung der Blockchain zur selbständigen Ausführung vertraglicher Vereinbarungen (Smart Contracts)

Dabei wird teilweise die bestehende Bitcoin-Blockchain, teilweise eine neue Blockchain verwendet, die – wie Bitcoin – öffentlich oder auch privat, also mit begrenztem Teilnehmerkreis, ausgestaltet sein kann. Große Technologie-Unternehmen wie Microsoft oder IBM bieten mittlerweile Umgebungen zur Erprobung von Blockchain-Anwendungen an. Technologie- und besonders Finanzunternehmen arbeiten an einer Standardisierung und Weiterentwicklung der Blockchain-Technologie.

Die Blockchain als Notar

Im Bitcoin-System ist Kernfunktion der Blockchain, alle Transaktionen und damit die Zuordnung der Bitcoin manipulationssicher zu dokumentieren. Außer Zahlungstransaktionen lassen sich allerdings über kryptographische Verfahren auch beliebige andere Informationen (z. B. Nachrichten oder Bilder) in eine Blockchain einbinden.

Die Blockchain dient damit gleichsam als Notariat, um eine Information manipulationssicher abzulegen.

Nachfolgend zwei Anwendungsbeispiele:

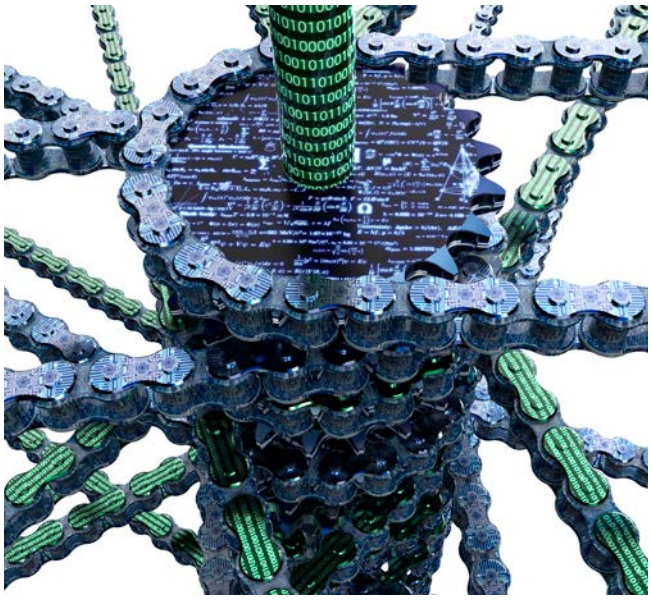
- Ein Konsortium von Großbanken und anderen Finanzdienstleistern kündigte im August 2016 an, im institutionellen Zahlungsverkehr eine so genannte Utility Settlement Coin (USC) auf Basis der Blockchain-Technologie einsetzen zu wollen. Die USC soll es ermöglichen, Wertpapiertransaktionen unter Umgehung von Abwicklungsdienstleistern zu verrechnen. Auf diese Weise hoffen die Teilnehmer, etwa bei der Hinterlegung von Sicherheiten bei Zentralbanken erhebliche Zeitersparnis zu erzielen. Die Blockchain dient hier der Dokumentation von Zahlungstransaktionen; anders als Bitcoin soll die USC aber kein eigenes Zahlungsmittel sein, sondern lediglich Verrechnungsvereinbarungen zwischen bestehenden Vermögenswerten, etwa Wertpapieren, beweissicher dokumentieren.

- Das britische Unternehmen Everledger will zentrale Eigenschaften (z. B. Identifikationsnummern) von Diamanten erfassen und diese sowie die Eigentümerhistorie eines Steins in die Bitcoin-Blockchain einspeisen. Dabei soll der Umstand genutzt werden, dass wesentliche Eigenschaften eines Diamanten nicht oder nur unter starkem Wertverlust verändert werden können. Die von Everledger erfassten und durch die Blockchain gleichsam beglaubigten Informationen sollen dazu beitragen, die Transaktionshistorie eines bestimmten Steins offenzulegen, so dass beispielsweise gestohlene Steine beim Verkauf am Markt erkannt werden können.

Grundsätzlich kommt der Einsatz einer Blockchain überall in Betracht, wo Vertrauen auf die Echtheit von Informationen wichtig ist. Außer im Wertpapierhandel könnte auch für Grundstücke oder Kunstgegenstände eine Blockchain eine kostengünstige und schnelle Alternative zu einem zentralen Register sein oder – etwa in Staaten, in denen kein zentrales Grundbuch existiert – überhaupt erst eine verlässliche Dokumentation der Eigentumszuordnung schaffen.

Die Blockchain könnte bei solchen Anwendungen in die Sphäre bisher staatlich geregelter Tätigkeit (z. B. Grundbuchamt) eindringen oder etablierte Intermediäre (z. B. Abwicklungsdienstleister im Finanzmarktbereich) verdrängen. Aus heutiger Sicht wird wohl noch einige Zeit vergehen, bis es möglicherweise zu solchen Verdrängungseffek-

ten kommt. Zudem hat das Blockchain-System Grenzen, die weiterhin Geschäftsfelder für Intermediäre ermöglichen dürften. So muss ein öffentliches Blockchain-Netzwerk sehr groß sein, um das nötige Vertrauen in die gegenseitige Kontrolle der Teilnehmer sicherzustellen. Dies dürfte in der Regel zu Lasten der Kapazität und Transaktionsgeschwindigkeit gehen. Die Bitcoin-Blockchain hat zudem den Nachteil, dass alle Transaktionen öffentlich sind und mögliche Fehler oder Lücken vielleicht nicht schnell genug von einer zentralen Instanz behoben werden können. Diese Lücken können Hackern Angriffspotenzial bieten. Vertrauenswürdige Intermediäre könnten diesen Nachteilen abhelfen, indem sie schnellere und vertrauliche eigene Blockchains zwischen ausgewählten Teilnehmern anbieten.



Smart Contracts

Als Smart Contracts werden Computerprogramme bezeichnet, die vertragliche Vereinbarungen selbständig ausführen. Auch Smart Contracts sind Informationen, die in einer Blockchain weitgehend manipulationssicher abgelegt werden können. So wird etwa im BMWi-Projekt SAMPL (Secure Additive Manufacturing Platform) im Förderschwerpunkt Digitale Technologien in der Wirtschaft (PAiCE) die Blockchain als Möglichkeit zur Absicherung von Lizenz- und Urheberinformationen für 3D-Druckverfahren erprobt, damit 3D-Modelle von räumlich entfernten 3D-Druckern nur entsprechend der Vereinbarung mit dem Urheber genutzt werden können.

Neue Anbieter, wie beispielsweise das Unternehmen Ethereum, das eine eigene Blockchain betreibt, streben darüber hinaus an, selbsterfüllende Verträge (self-fulfilling contracts) mittels eines Blockchain-Netzwerks umzusetzen. Grundsätzlich muss dabei zunächst eine Vereinbarung in Programmiersprache (Code) gefasst werden, wobei für das Eintreten bestimmter Bedingungen (z. B. Lieferung einer Ware) bestimmte Folgen (z. B. Zahlung) definiert werden. Die Blockchain erfüllt dabei die Aufgabe, durch Feststellung des Bedingungseintritts automatisch die Folge auszulösen und die im Vertrag vereinbarten Leistungen abzuwickeln. Die Blockchain-Technologie übernimmt damit die Funktion eines Sicherungsmechanismus bei der Erfüllung gegenseitiger Verträge. Sie kann dadurch die Vertragserfüllung erleichtern und löst vor allem das Vertrauensproblem, das entsteht, wenn Leistungen der Vertragsparteien nicht simultan erfolgen und eine Partei einseitig in Vorleistung treten müsste.

Einige Anwendungsbeispiele:

- Das Versicherungsunternehmen Allianz hat im Juni 2016 bekannt gegeben, in einem Pilotprojekt den Einsatz der Blockchain-Technologie bei so genannten Katastrophen-Swaps eingesetzt zu haben. Gegenstand des Projekts seien Verträge, mit denen das Risiko einer Katastrophe (z. B. Hurrikan) gegen Zahlung auf eine andere Partei übertragen wird. Die Blockchain-Technologie sei genutzt worden, um bei einem vordefinierten Ereignis automatisch die vertraglich vorgesehenen Folgen auszulösen.

- Das Brooklyn Microgrid, ein Projekt in New York, nutzt die von Ethereum betriebene Blockchain, um ein lokales Stromnetz zu verwalten. Stromverbraucher, die z. B. über eine Solaranlage auf dem Dach auch selbst Strom erzeugen, können über Smart Contracts überschüssigen Strom direkt an andere Kunden abgeben oder von anderen Produzenten beziehen.

- Im Ethereum-Netzwerk wurde im April 2016 ein Smart Contract-Projekt namens The DAO („Decentralized Autonomous Organization“) durchgeführt, das ähnlich wie ein Investmentfonds Geld in andere Projekte investieren soll. Medienberichten zufolge wurde allerdings durch Ausnutzung einer Lücke im Code von The DAO im Juli 2016 ein Betrag von mehr als 50 Millionen US-Dollar abgezweigt und konnte nur durch manuellen Eingriff der Entwicklergemeinschaft von Ethereum teilweise zurückgeholt werden.

Das letzte Beispiel verdeutlicht, dass der Einsatz von Smart Contracts in einer öffentlichen Blockchain auch erhebliche Risiken birgt: Sind die Vertragsbedingungen unvollständig oder fehlerhaft, ist die Lücke für jedermann erkennbar und das System angreifbar.

Wahrscheinlich werden selbsterfüllende Verträge daher zunächst eher in privaten, von einer zentralen Instanz administrierten Blockchain-Anwendungen Verbreitung finden, etwa in von Finanzdienstleistern verwalteten Netzwerken für Zahlungsverkehr, Wertpapierhandel oder Risikotransfer. Perspektivisch denkbar sind allerdings auch selbsterfüllende Verträge, mit denen Ferienwohnungen oder Mietwagen verwaltet werden. In einem künftigen „Internet der Dinge", in dem jeder Gegenstand über ein Netzwerk kommuniziert, könnte Smart Contracts eine wichtige Steuerungsfunktion zukommen.

Regulatorische Herausforderungen

Eine weitere Verbreitung Blockchain-basierter Anwendungen in der Wirtschaft würde voraussetzen, dass die Rechtsordnung den Einsatz der Blockchain hinreichend anerkennt. Grundsätzlich lässt zwar die Vertragsfreiheit genügend Spielraum zur Vereinbarung und Nutzung neuer Technologien bei der Vertragserfüllung, wenn die Beteiligten das wollen. Soweit die Blockchain aber Funktionen gesetzlich verankerter Sicherungs- und Schutzmechanismen übernehmen soll (Beispiel: Notariatsfunktion), setzt dies eine Anerkennung durch die Rechtsordnung voraus. Der Gesetzgeber stünde dann vor der Frage, ob er eine auf dezentralisiertem Vertrauen und kryptographischen Methoden basierende Lösung anerkennen will. Grundsätzlich dürfte es dabei sinnvoll sein, unabhängig von der Technologie ein Geschäftsmodell mit gleichem Risiko auch denselben Regeln zu unterwerfen. In der Welt der selbsterfüllenden Verträge stellen sich aber noch viel weiter gehende rechtliche Fragen, zum Beispiel: Wie ist das Verhältnis zwischen in der Blockchain abgelegtem Code und dem Zivilrecht? Wie kann gewährleistet werden, dass die Grenzen der Vertragsfreiheit, etwa das Verbot der Sittenwidrigkeit, und die Grundsätze richterlicher Auslegung beachtet werden? Welches Recht kommt bei internationalen Transaktionen zur Anwendung? Ebenso wie die Entwicklung von Smart Contracts dürfte auch ihre juristische Einbettung noch einige Zeit in Anspruch nehmen.

Fazit

Während die Zukunft des Zahlungsmittels Bitcoin ungewiss ist, zeigen sich für die zugrunde liegende Technologie Blockchain verschiedene weitere Anwendungsmöglichkeiten. Ob sich die jeweiligen Anwendungen durchsetzen, dürfte entscheidend davon abhängen, wem die Nutzer mehr Vertrauen schenken – einem dezentralen Blockchain-Netzwerk oder etablierten Intermediären, wie etwa Finanzmarktunternehmen. In jedem Fall bietet die neue Technologie bestehenden Intermediären, aber auch neuen Marktteilnehmern, die Gelegenheit, Geschäftsmodelle in einer Blockchain-basierten Umgebung zu entwickeln. Aus juristischer Perspektive dürfte die Einbindung der Blockchain-Technologie in das bestehende Rechtssystem eine spannende Herausforderung darstellen.

Kontakt: Dr. Malte Rosenberg
Referat: Geld, Kredit, Finanzmärkte