Lara Bolesch / Andreas Mitschele

Revolution oder Evolution? Funktionsweise, Herausforderungen und Potenziale der **Blockchain-Technologie**

Selten hat eine neue Technologie die Finanzindustrie mehr in ihren Bann gezogen als aktuell die Blockchain beziehungsweise Distributed Ledger Technologie (DLT). Viele Beteiligte erwarten einen Paradigmenwechsel durch das neue Konzept und so wurden in den vergangenen drei Jahren bereits über 1,4 Mrd. US-Dollar in seine Entwicklung investiert.[1)] Einige technische und rechtliche Aspekte haben jedoch Zweifel an einer baldigen Omnipräsenz der Technologie aufkommen lassen, weshalb sich nach anfänglicher Euphorie stellenweise auch Ernüchterung breitmacht.

Bedeutung von Blockchain beziehungsweise Distributed Ledger?

Allgemein gesprochen stellt die Blockchain (Blockkette) ein digitales, chronologisch aktualisiertes, verteiltes und kryptografisch verschlüsseltes Verzeichnis aller Datenübermittlungen eines Systems dar.[2)] Unter einem „Distributed Ledger" versteht man eine verteilte Datenbank, bei der alle Teilnehmer zusammenarbeiten, um einen Konsens über die Validität der geteilten Daten zu erzielen. Da die Blockchain-Technologie diese Eigenschaft aufweist, kann der Begriff grundsätzlich synonym verwendet werden. Umgekehrt verwendet aber nicht jeder Distributed Ledger unbedingt eine Blockkette.[3)]

Dezentrale Datenbank mit Konsensmechanismus: Vereinfacht lässt sich die Blockchain als eine auf einer Vielzahl von Rechnern im Netzwerk gespiegelte Datenbank beschreiben, bei der eingehende Datensätze in Blöcke verpackt und kryptografisch signiert werden. Die Authentizität der einzelnen Datenbankeinträge wird durch einen aus dem Netzwerk hergestellten Konsensmechanismus sichergestellt. Sämtliche Einträge werden dabei in der Datenbank öffentlich, dauerhaft und unabänderlich erfasst, wie beispielsweise im Bitcoin-System[4)]. Hierdurch können die Rechner im Netzwerk jederzeit historische Einträge prüfen, zum Beispiel im Anwendungsfall Bitcoin, ob ein bestimmter Geldbetrag bereits ausgegeben worden ist.[5)]

Im Grunde kann in einer solchen Datenbank jegliche Art von digitalen Eigentumsrechten verbrieft werden, worin sich auch das gewaltige Potenzial der Technologie begründet. Da die dezentrale Organisation einen Intermediär überflüssig macht, könnte die Blockchain zukünftig auch in vielen Anwendungsbereichen außerhalb der Finanzindustrie ihre disruptive Wirkung entfalten.[6)]

Lara Bolesch, Tullius Walden Bank AG, Stuttgart, und Prof. Dr. Andreas Mitschele, Studiengangsleiter BWL-Bank, Wissenschaftlicher Leiter Master in Business Management Finance, Duale Hochschule Baden-Württemberg, Stuttgart

Was ist Blockchain? Welche Bedeutung wird diese Technologie für die Finanzwirtschaft und andere Bereiche des Wirtschaftslebens haben? Und wie schnell wird sie Fuß fassen? Diese Fragen bewegen seit Monaten nicht nur eine kleine Gruppe von Fachleuten, sondern längst die breite Öffentlichkeit. Die Autoren stellen zunächst vereinfacht die technische Funktionsweise der Blockchain am Beispiel des Bitcoin-Systems dar und systematisieren verschiedene Ausgestaltungsvarianten. Nach einem Überblick potenzieller Anwendungsfelder der Technologie diskutieren sie aktuelle Herausforderungen bei der Umsetzung. Abschließend erläutern sie anhand des entstehenden „Internet der Dinge", dass die Blockchain in diesem Bereich aus ihrer Sicht im Grunde keine Revolution darstellt, sondern lediglich den nächsten evolutionären Schritt zur Weiterentwicklung der bisherigen Web-Infrastruktur hin zu einem „Internet der Werte". (Red.)

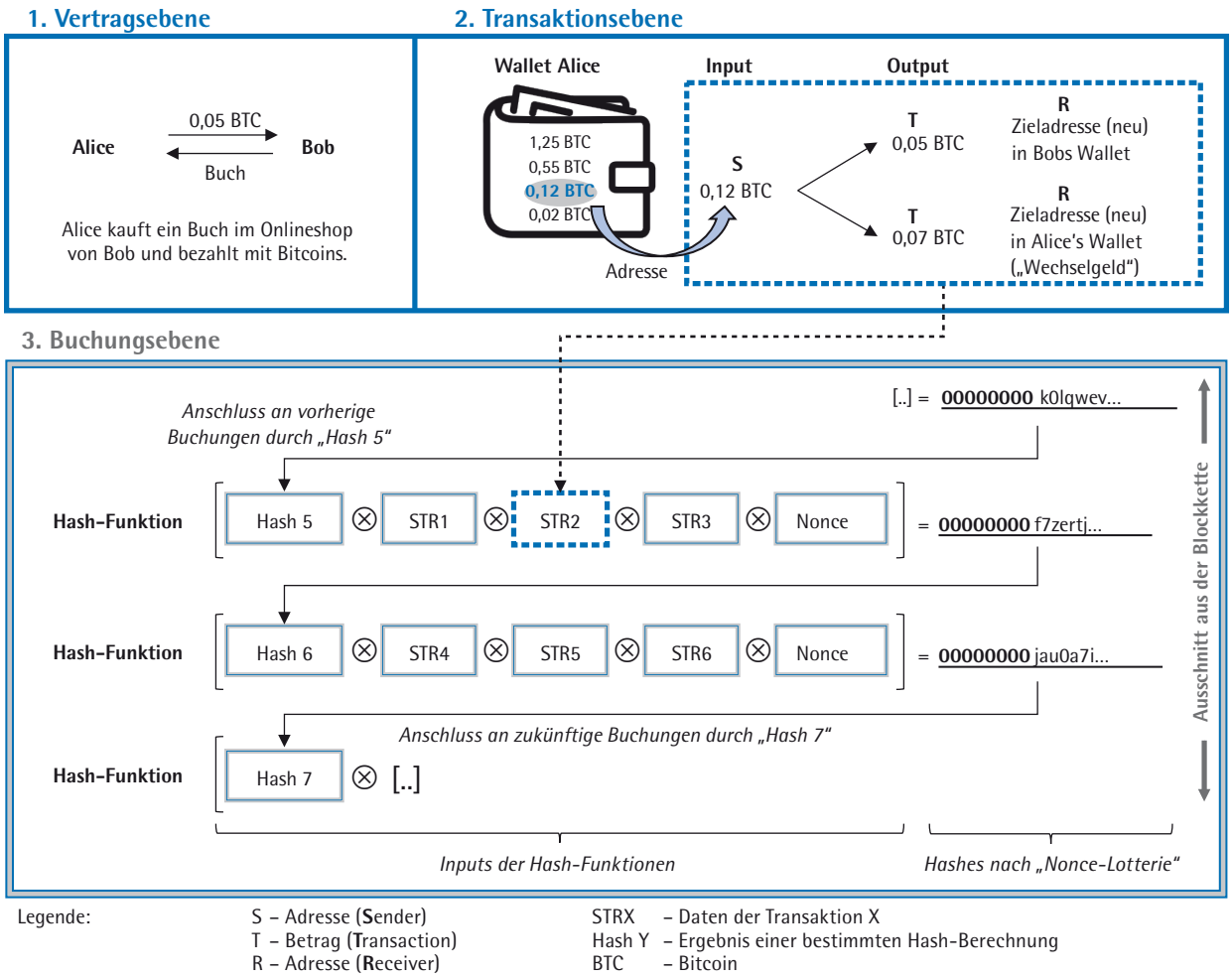
Bitcoin: Anfang 2009 als Open-Source-Projekt veröffentlicht

Wie alles begann – Bitcoin: Die Blockchain-Technologie geht zurück auf ein Arbeitspapier, das im November 2008 anonym über eine Mailingliste veröffentlicht wurde.[7)] Der bis heute unbekannte Autor oder die Autorengruppe mit dem Pseudonym „Satoshi Nakamoto" beschreibt darin das elektronische Zahlungssystem Bitcoin, das Peer-to-Peer über das Internet organisiert ist und ohne zentralen Intermediär auskommt. Das auf der Funktionsbeschreibung basierende Bitcoin-Basissystem wurde dann Anfang 2009 als Open-Source-Projekt veröffentlicht, wodurch die virtuelle Währung ins Leben gerufen wurde.

Der Bitcoin-Wechselkurs (BTC) hat sich seitdem äußerst volatil entwickelt und stand Anfang November 2016 bei zirka 725 US-Dollar.[8)] Dies impliziert eine Marktkapitalisierung von knapp 12 Milliarden US-Dollar und macht die Währung damit auch attraktiv für Hacker. Hauptziel bisher erfolgreicher Attacken waren Bitcoin-Börsen wie Mt. Gox oder aktuell Bitfinex.[9)] Derartige Angriffe können mit einem klassischen Banküberfall verglichen werden, bei dem Kundenbargeld aus dem Banktresor entwendet wird. Die Blockchain als technische Basis von Bitcoin konnte allerdings bis heute noch nicht kompromittiert werden. Insofern kann Bitcoin – trotz aller berechtigten Vorbehalte[10)] – als „Proof-of-Concept" der Blockchain-Technologie angesehen werden. Das technische Verfahren wird in der Abbildung 1 vereinfacht anhand einer Bitcoin-Transaktion erläutert.

Zur besseren Übersichtlichkeit des Beispiels wird das Bitcoin-Zahlungssystem in ver-

Abbildung 1: Funktionsweise der Bitcoin-Blockchain in verschiedenen Ebenen



schiedenen Ebenen betrachtet. Auf Vertragsebene kauft die Privatperson Alice im Onlineshop des Händlers Bob ein Buch zum Preis von 0,05 Bitcoin (zirka 36 USD). Auf der Transaktionsebene befinden sich im digitalen Wallet von Alice mehrere Bitcoin-Beträge (insgesamt 1,94 BTC), die jeweils mit einem Geldschein vergleichbar sind. Jeder dieser Beträge kann mit Hilfe seiner eindeutigen und öffentlich bekannten Adresse (sogenannter öffentlicher Schlüssel) jederzeit und von jedem Netzwerkteilnehmer überprüft und einer vergangenen Bitcoin-Transaktion zugeordnet werden.

Um die Zahlung empfangen zu können, übermittelt Bob seine Überweisungsdaten in Form einer neuen Bitcoin-Zieladresse an Alice. Für die Bezahlung des Einkaufs wird vom System die bestehende Bitcoin-Adresse mit 0,12 BTC aus dem Wallet von Alice als „spent" markiert und in zwei Teilbeträge zerlegt: 0,05 BTC als Zahlungsbetrag an Bobs genannte Zieladresse und 0,07 BTC als Wechselgeld für Alice an eine neue Zieladresse in ihrem eigenen Wallet (Abbildung 1).

Vertrauen in die Technologie – unabänderliche Transaktionsverbuchung

Zur Übertragung der Bitcoins muss Alice zunächst noch beweisen, dass ihr der in ihrem Wallet hinterlegte Betrag von 0,12 BTC tatsächlich gehört. Hier kommt das aus der Kryptographie bekannte Public-Key-Verfahren zum Einsatz (siehe Infobox 1). Zu jedem öffentlich bekannten Schlüssel (Adresse) eines Bitcoin-Betrags (hier: 0,12 BTC) existiert ein sogenannter privater Schlüssel, der nur dem rechtmäßigen Eigentümer bekannt ist. Das Wallet von Alice signiert die beabsichtigte Transaktion mit diesem privaten Schlüssel und sendet sie an das gesamte Netzwerk. Obwohl der private Schlüssel aus dieser Nachricht nicht extrahierbar ist, können die teilnehmenden Rechner mithilfe des korrespondierenden öffentlichen Schlüssels die Eigentumsverhältnisse fälschungssicher verifizieren und anschließend das Netzwerk hierüber informieren.

Bemerkenswert an dieser Vorgehensweise ist, dass zur rechtmäßigen Übertragung der Bitcoins keine zentrale Institution als Vertrauensgeber notwendig ist. Das Bitcoin-System basiert auf dem Vertrauen der Teilnehmer in die Sicherheit des zugrunde liegenden Public-Key-Verfahrens. Zudem wird angenommen, dass durch den freien Zugang und die Verbreitung des Systems eine Manipulation sehr unwahrscheinlich ist.

Der im Wallet von Alice hinterlegte private Schlüssel sichert ihr also durch das kryptografische Verfahren das Eigentum am Bitcoin-Betrag von 0,12 BTC. Wenn eine an-

dere Person, zum Beispiel ein Hacker, Kenntnis dieses Schlüssels erlangen sollte, kann er den Betrag ungehindert entwenden. Der Hacker ist dann vergleichbar mit einem Taschendieb, der einen Geldschein aus einem Portemonnaie stiehlt. Im Vergleich zum Bargeldklau besteht bei einem Bitcoin-Raub allerdings deutlich weniger Hoffnung auf eine Überführung des Täters. Wenngleich die Bitcoin-Adressen (öffentliche Schlüssel) sowie alle Transaktionen öffentlich bekannt sind, so verläuft eine Transaktion dennoch grundsätzlich anonym ab. Die verwendeten öffentlichen Bitcoin-Adressen können einem bestimmten Sender/Empfänger nämlich nicht zugeordnet werden.[11] Um nachträgliche Manipulationen an der beschriebenen Transaktion zwischen Alice und Bob auszuschließen, wird diese im abschließenden Schritt dauerhaft und unabänderlich mit der bereits bestehenden Kette von Transaktionsblöcken (Blockchain) verknüpft (Abbildung 1, Buchungsebene).

Aufwendige Lotterie als Proof-of-Work

Hierfür sammeln die ans Bitcoin-Netzwerk angeschlossenen Rechner (sogenannte „Miner") die im aktuellen Zeitintervall aufgelaufenen Transaktionen in einem neuen Block. Anhand eines speziellen Hash-Algorithmus (siehe Infobox 2) verdichten die Miner den Hash-Wert des vorhergehenden Transaktionsblocks, alle aktuellen Transaktionen[12] und eine sogenannte „Nonce" (Zufallszahl) in einem neuen Hash-Wert. Eine minimale Änderung an dieser in die Hash-Funktion eingehenden Zeichenkette führt zu einem vollkommen unterschiedlichen Hash-Wert. Dadurch, dass immer der Hash-Wert des vorhergehenden Blocks in die Berechnung eines neuen Blocks eingeht, wird dieser mit den bisherigen Transaktionsblöcken verknüpft und es entsteht eine „Blockkette" mit praktisch unabänderlichen historischen Transaktionsdaten. Wenn ein Angreifer eine bestimmte Transaktion manipulieren wollte, müsste er alle dem Manipulationszeitpunkt zeitlich nachgelagerten Blöcke neu berechnen.

Der für eine Neuberechnung aufzubringende Zeit- beziehungsweise Rechenaufwand wird durch folgende besondere Vorgabe des Bitcoin-Systems jedoch massiv erhöht: Unter den Minern, die neue Transaktionsblöcke an die Blockchain anhängen, wird ein mit einer Lotterie vergleichbarer Wettbewerb veranstaltet. Das System generiert dazu quasi eine „Gewinnzahl", indem der Hash-Wert des neuesten Blocks eine bestimmte Anzahl führender Nullen ausweisen muss. Die Miner-PCs variieren die Nonce bei der Hash-Berechnung solange, bis sie einen entsprechenden Output gefunden haben (Abbildung 1).

Aufgrund der mathematischen Beschaffenheit des verwendeten Hash-Algorithmus (SHA-256, siehe Infobox 2) existiert keine Möglichkeit, einen entsprechenden Output effizient zu berechnen. Alle beteiligten Rechner müssen also große Mengen an Rechenleistung investieren, um eine passende Nonce zu finden. Desto mehr Rechenleistung ein einzelner Miner (oder ein Verbund von Minern) investiert, desto höher ist dabei die Wahrscheinlichkeit, einen Treffer zu landen beziehungsweise die „Gewinnzahl" zu erraten. In Parallele zu einer klassischen Lotterie ist ein höherer Input an Rechenleistung also mit dem Erwerb einer entsprechend höheren Anzahl an Gewinnlosen vergleichbar.[13] Die Miner sind deswegen motiviert, Rechenleistung

Infobox 1: Public-Key-Verfahren

Es handelt sich hierbei um ein asymmetrisches Verschlüsselungsverfahren, das beispielsweise zur sicheren E-Mail-Kommunikation verwendet wird. Benötigt werden dabei ein privater und ein öffentlicher Schlüssel, die als Paar in einem mathematischen Zusammenhang stehen. Der Sender verschlüsselt seine Nachricht mit dem öffentlichen Schlüssel des Empfängers. Nur Letzterer kann die Nachricht dann beim Empfang mithilfe seines privaten Schlüssels dechiffrieren.

Das Verfahren eignet sich ebenfalls zur digitalen Signierung von Nachrichten. Hierzu „unterschreibt" der Sender seine Nachricht mit seinem privaten Schlüssel, der nur ihm bekannt sein darf. Jeder Empfänger kann daraufhin mithilfe des öffentlich bekannten Schlüssels des Senders eindeutig nachvollziehen, dass die Nachricht tatsächlich vom Sender signiert wurde.

Die Herausforderung für einen möglichen Angreifer besteht bei diesem Verfahren darin, dass er den zur Entschlüsselung oder Signierung notwendigen privaten Schlüssel aus dem öffentlich bekannten Schlüssel einer Person mit bekannten Mitteln nicht in vertretbarer Zeit herleiten kann. Daher gilt das Verfahren als sehr sicher.

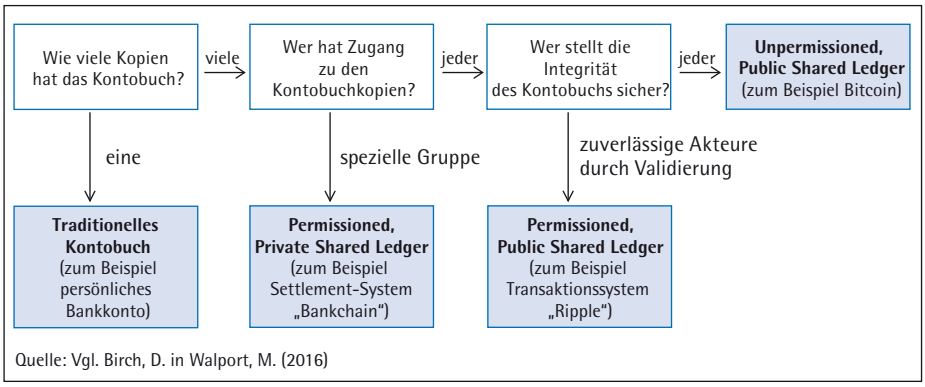
Infobox 2: Secure Hash Algorithm 256 (SHA-256)

Grundsätzlich bildet eine Hash-Funktion eine Zeichenkette beliebiger Länge auf eine Zeichenfolge mit fest definierter Länge ab, die Hash-Wert genannt wird. Beim SHA-256 (Bitcoin) ist dieser Wert immer 64 Zeichen lang. Ein solches Verfahren ist beispielsweise bei der Übertragung von Dateien über das Internet hilfreich. Bei identischen Hash-Werten einer Datei vor und nach Übertragung kann dabei mit sehr hoher Wahrscheinlichkeit von einer verlustfreien Übermittlung ausgegangen werden.

Bei kryptografischen Hash-Algorithmen, wie dem SHA-256, sollte es nicht gelingen, zwei Eingangszeichenketten zu finden, die denselben Hash-Wert erzeugen. Diese Eigenschaft macht sich das Bitcoin-System zunutze, indem es einen Wettlauf der Miner-PCs veranstaltet, um einen Hash-Wert des aktuellen Transaktionsblocks mit bestimmten Eigenschaften zu ermitteln. Es gibt hierzu kein effizientes Suchverfahren, da bereits minimale Änderungen den Hash-Wert vollständig und nicht vorhersehbar verändern. Beispielsweise ergeben sich mittels SHA-256 folgende 64 Zeichen langen Hash-Werte aus den beiden nahezu identischen Zeichenketten:

Das ist ein Test. ⇨1d94336663002167a47c61f4fd9296d67b1db74c60dc7e9b658ced82c3132f0d
Das ist ein Test! ⇨89af4993d822a136b16a5efe49895e99b0c7200b0c61975ad083b07f14b13951

Abbildung 2: Klassifizierung von Kontenbüchern



Quelle: Vgl. Birch, D. in Walport, M. (2016)

in dieses Verfahren einzubringen, da eine erfolgreiche Suche derzeit mit 12,5 BTC (aktuell zirka 9000 US-Dollar) belohnt wird. Dieses Verfahren wird „Proof of Work" genannt.

Sobald ein Miner eine passende Nonce, respektive „Gewinnzahl", gefunden hat, sendet er den Block an alle Teilnehmer. Diese validieren den Block nochmals und drücken ihre Akzeptanz dadurch aus, dass sie zur Bearbeitung des nächsten Blocks übergehen. Wenn sich die Mehrheit der Teilnehmer den nächsten Datensätzen widmet, gilt der Block als valide und die darin enthaltene Transaktion zwischen Alice und Bob ist unwiderruflich bestätigt.[14] Es kann hierbei vorkommen, dass sich zwei unterschiedliche Blockchain-Zweige bilden. Das demokratische Verfahren der Bitcoin sorgt jedoch dafür, dass sich dabei der Zweig durchsetzt, der von der Mehrheit der Rechner weiterverwendet wird.[15]

Automatische Anpassung an den technischen Fortschritt

Auf jedem Rechner, der dem Bitcoin-System angeschlossen ist, wird stets eine aktuelle Version der Blockchain gespeichert. Dieser Verbund von tausenden Rechnern bringt gemeinsam eine immense Rechenleistung auf, die das Bitcoin-System am Laufen hält. Um dem technischen Fortschritt und der einhergehenden ständigen Zunahme der Rechengeschwindigkeit Rechnung zu tragen, wurde das System vom Urheber so konzipiert, dass der Schwierigkeitsgrad der oben beschriebenen „Lotterie" regelmäßig und automatisiert an die Gesamtperformance des Rechnernetzes angepasst wird. Dadurch soll der Abstand zwischen neu generierten Blöcken dauerhaft zirka zehn Minuten betragen.

Das Bitcoin-System funktioniert vor allem aufgrund zweier zentraler Faktoren bisher reibungslos: Zum einen besteht keine Möglichkeit zur Doppelausgabe, da die Struktur der Blockketten statisch ist und bei jeder Bitcoin-Adresse abgeglichen wird, ob sie bereits Input einer anderen Transaktion war. Zum anderen stellt die Belohnung aus dem Proof-of-Work-Prozess einen Anreiz für alle Beteiligten dar, ehrlich zu handeln. Indem die erfolgreichen Miner mit Bitcoins vergütet werden, würde ein Betrug letztendlich deren eigenes Vermögen schmälern.

Im Gegensatz zu einem klassischen Kontobuch, wie zum Beispiel dem persönlichen Bankkonto, existieren bei einem Distributed Ledger (oder noch allgemeiner „Shared Ledger") mehrere Kopien des Kontobuchs. Abhängig von den Zugangsmöglichkeiten unterscheidet man in „permissioned" und „unpermissioned" Ledgers (siehe Abbildung 2). Letztere stellen die Basis von Kryptowährungen wie Bitcoin dar. Derartige Kontobücher haben keinen Besitzer und ermöglichen es somit jedem Nutzer, Transaktionen in das System einzubringen. Sie sind dadurch gegen Zensur geschützt. Weitere Einsatzmöglichkeiten ergeben sich beispielsweise in Bereichen, die im öffentlichen Interesse stehen (zum Beispiel Immobiliengrundbücher).

Permissioned (private shared) Ledgers unterliegen dagegen einem kontrollierten Zugang, der nur ausgewählten Nutzern offensteht (zum Beispiel staatlichen Institutionen oder Banken). Die Validierung der Daten obliegt ebendiesen Nutzern, die sich über den sogenannten Proof-of-Stake-Mechanismus (Beteiligungsnachweis) legitimieren müssen.[16] Dadurch ist die Datenbank deutlich schneller als eine offene Blockchain, aber auch einfacher manipulierbar. In der Variante „permissioned, public shared" ist das Kontobuch öffentlich, aber nur dessen Besitzer oder ausgewählte zuverlässige Akteure können Transaktionen validieren (Abbildung 2)[17].

Vielversprechendes Potenzial durch Smart Contracts

Satoshi Nakamoto trat 2008 mit dem provokativen Ziel an, Intermediäre überflüssig zu machen und somit deren Macht über Transaktionsgebühren nachhaltig zu brechen. Insofern zeichnet sich in allen Bereichen, in denen bisher noch zentrale Institutionen notwendig sind, enormes Kosteneinsparpotenzial ab. Unternehmen aller Branchen können durch die Blockchain interne und externe Prozesse weiter automatisieren und standardisieren.

Die dezentrale Blockchain-Buchhaltung hat zudem einen innovativen Vorteil: Es können Regeln für einzelne Transaktionen hinterlegt werden, die bei Eintreten bestimmter Szenarien automatisch ausgelöst werden. Solche in einer Blockchain organisierten Verträge werden als „Smart Contracts" bezeichnet. Technisch handelt es sich um eine Software-Anwendung, die das Verhalten von Vertragspartnern überwachen und im Vertrag hinterlegte Bedingungen bei Vorliegen eines entsprechenden Trigger-Events automatisiert auslösen kann. Beispielsweise ist es somit denkbar, Kredite online auf einer Blockchain abzuschließen und gleichzeitig individuelle Bedingungen von einem solchen „smarten" Vertrag verwalten zu lassen. Wenngleich konkrete Praxisanwendungen derzeit noch rar sind – das Potenzial ist erheblich.[18]

Technische und rechtliche Herausforderungen

Bei der Anwendung neuer Technologien in Banken kommt dem Urteil der Aufsicht eine besondere Bedeutung zu. Diese wiederum hält sich hierzu derzeit noch recht bedeckt. Auch in der öffentlichen Meinung wird die Blockchain – nicht zuletzt aufgrund negativer Wahrnehmung der Bitcoin – recht kritisch gesehen.

Dabei könnte ein ausgefeiltes Blockchain-basiertes System allein aufgrund des transparenten Aufbaus für die Aufsichtsbehör-

den eine willkommene Neuerung darstellen. Als Teilnehmer oder Verwalter des Systems könnten sie alle Informationen und Transaktionen innerhalb des Systems einsehen und überwachen.

Technisch hat die Blockchain noch einige Schwächen, beispielsweise ist sie bisher nicht ausreichend skalierbar. Große Datenbanken oder ganze Handelssysteme würden daher derzeit noch an ihre Grenzen stoßen. Daher wird in diesem Bereich intensiv geforscht. Für Banken stellt sich neben der maximal bearbeitbaren Datenmenge auch die Frage, wie offen ein solches System sein soll. Hierbei sind Lösungen gesucht, die den offenen und demokratischen Charakter der Blockchain mit dem Sicherheitsanspruch von Kreditinstituten verbinden wie beispielsweise in der aktuellen Initiative zur Utility Settlement Coin (USC).[19]

Die Blockchain als Baustein im Internet der Dinge

In Deutschland gibt es derzeit rund 40 Millionen Haushalte.[20] In nahezu jedem Haushalt sollte zumindest ein Kühlschrank, ein Haustürschloss, ein Stromanschluss und eine Heizung vorhanden sein. All diese Alltagsgegenstände sollen zukünftig durch das „Internet der Dinge" miteinander verbunden und „smart" gemacht werden.

Beispielsweise könnte ein Kühlschrank seinen Bestand an Lebensmitteln kontrollieren und bei Bedarf automatisch nachbestellen oder eine Klingelanlage jederzeit Statusänderungen übermitteln. Damit die Menschen die Kommunikation der Geräte untereinander untereinander und mit Dritten überhaupt zulassen, müssen sie dem übermittelnden System beziehungsweise Netzwerk vertrauen. Angesichts andauernder Diskussionen und Skandale im Zusammenhang mit Datenschutz sowie Häufungen von Hackerangriffen auf renommierte Institutionen sind allerdings viele Menschen zurückhaltend gegenüber derartigen Innovationen geworden. Nach Ansicht von Experten könnte die dezentrale Blockchain-Technologie eine Lösung für dieses Problem darstellen. Wie dargestellt, erfordert sie kein Vertrauen unter den handelnden Personen, sondern lediglich Vertrauen in die Zuverlässigkeit der Technologie.

Konkret könnte dies wie folgt ablaufen: Ein neuer Nutzer erhält zunächst eine digitale Identität in einem Blockchain-basierten System. Nun kann er alle seine Geräte (zum Beispiel Mobiltelefon, Fernseher, Toaster) mit seiner digitalen Identität über die Blockchain authentifizieren und seiner Person fälschungssicher zuordnen. Eigentums- und Nutzungsverhältnisse realer Güter könnten so transparent und effizient verwaltet werden.

Ein Kühlschrank kann nun autorisiert werden, bei Unterschreiten eines gewissen Füllstands den regulären Wocheneinkauf selbsttätig nachzubestellen. Elektrogeräte könnten ihre eigene Wartung im Servicecenter des Herstellers im Namen ihres Eigentümers veranlassen. Es zeichnen sich unzählige Möglichkeiten ab, wie ein solches dezentrales System im Internet der Dinge wirken kann.

Revolution? – Evolution!

Ohne Frage kann die Blockchain-Technologie in vielen Bereichen disruptiv wirken und stellt insofern eine revolutionäre Neuerung dar. Im entstehenden Internet der Dinge kann sie allerdings auch als evolutionäre Weiterentwicklung der bisherigen (ebenfalls dezentralen) technischen Architektur des Internets gesehen werden.

Die Zahl der verbundenen Geräte im Internet der Dinge steigt sehr stark an. Dadurch erhöht sich auch der Bedarf an Rechenleistung enorm. Die Blockchain-Technologie bietet sich hier als ideale Lösung an. Indem jedes ans Internet angeschlossene Gerät dem System freie Rechenleistung und Bandbreite sowie Speicherplatz zur Verfügung stellt, könnte mithilfe einer Blockchain eine gewaltige Menge an Ressourcen genutzt werden. Zudem werden deutlich schnellere und günstigere Transaktionen, auch mit sehr geringen Beträgen, ermöglicht.[21] Die Blockchain kann also ein wichtiger Baustein sein, um Authentifizierung, Zahlungen und Ressourcen-Allokation im Internet der Dinge zu realisieren.

Fußnoten

1) Vgl. World Economic Forum: The future of financial infrastructure, August 2016.
2) Vgl. Sorin, M. et al.: Israel: A Hotspot for Blockchain Innovation, S. 6, Februar 2016.
3) Vgl. Van de Velde et al.: Blockchain in Capital Markets, S. 5, Februar 2016.
4) Alle historischen Bitcoin-Transaktionen umfassen derzeit zirka 90 GB und sind beispielsweise unter der Adresse https://blockexplorer.com/ abrufbar, bis zurück zur ersten Transaktion am 3. 1. 2009.
5) Dieses Problem wird als „Double Spending" bezeichnet. Bei klassischen Zahlungssystemen stellt ein Intermediär beziehungsweise eine zentrale Autorität sicher, dass ein Geldbetrag nicht doppelt verwendet wird.
6) Vgl. Beck, R. und Milkau, U.: Blockchain: „Die Rolle der Banken wird technisch und prozessual anders aussehen", Redaktionsgespräch, Zeitschrift für das gesamte Kreditwesen, 12-2016, S. 576–581, Juni 2016.
7) Dieses Arbeitspapier ist beispielsweise unter https://bitcoin.org/bitcoin.pdf verfügbar.
8) Am 4. 12. 2013 kostete ein Bitcoin 1 238,97 USD an der Börse Mt. Gox (Quelle: https://www.coindesk.com/).
9) Mt. Gox war die größte Bitcoin-Börse mit Sitz in Tokio. Im Februar 2014 teilte die Firma mit, dass durch einen Hackerangriff Bitcoins im Wert von etwa 480 Mio. USD aus dem Kundenbestand abhandengekommen seien. In der Folge stellte die Börse den Betrieb ein. Am 2. 8. 2016 wurde beim zweitgrößten Bitcoin-Diebstahl bei der Börse Bitfinex ein Gegenwert von über 60 Mio. USD entwendet.
10) Vgl. beispielsweise Hafke, C.: Einige rechtliche Aspekte zum Comeback von Bitcoins, Zeitschrift für das gesamte Kreditwesen, 18-2014, S. 910-912, September 2014 sowie Brennan, C. und Lunn, W.: Blockchain – The Trust Disrupter, Credit Suisse Connections Series, August 2016.
11) Im Falle eines Diebstahls gilt dies auch für gestohlene private Schlüssel. Es ist allerdings nicht ausgeschlossen, dass durch gezielte Analyse der öffentlich verfügbaren Transaktionen doch Rückschlüsse auf einzelne Kontrahenten gezogen werden können.
12) Um Speicherplatz zu sparen, werden im Bitcoin-System die Transaktionsdaten des aktuellen Blocks ebenfalls in einen Hash-Wert (sog. Merkle Root) verdichtet, vgl. Nakamoto (2008).
13) Professionelle Miner verwenden zudem spezielle Rechner, die für die benötigten Rechenoperationen optimiert sind.
14) Zur Sicherheit wird aktuell dennoch empfohlen zu warten, bis sechs weitere Blöcke an die Kette angehängt worden sind (zirka 60 Minuten).
15) Aus diesem Umstand heraus resultiert das Risiko einer sogenannten „51%-Attacke", wenn ein Miner oder ein Zusammenschluss von Minern mehr als die Hälfte der insgesamt verfügbaren Rechenleistung kontrolliert.
16) Diese Berechtigung wird von der Institution erteilt, die das jeweilige System kontrolliert.
17) Vgl. Walport, M.: Distributed Ledger Technology: beyond block chain, UK Government Office for Science, 2016.
18) Das zeigt sich in zahlreichen Initiativen außerhalb der Finanzindustrie, zum Beispiel von IBM (http://www.ibm.com/blockchain/) oder vom RWE-Konzern, der diese Technologie für das Laden von Elektroautos verwenden möchte.
19) Ein Konsortium, u.a. mit UBS und Deutsche Bank, hat am 24. 8. 2016 die Blockchain-basierte „Utility Settlement Coin (USC)" zur Prozessvereinfachung bei Clearing und Settlement vorgestellt. Dabei soll eine direkte Anbindung an Zentralbankgeld erfolgen.
20) Vgl. Statistisches Bundesamt: „Bevölkerung und Erwerbstätigkeit", Wiesbaden, 2016.
21) Vgl. IBM Institute for Business Value: „Device Democracy: Saving the Future of the Internet of Things".