Möglichkeiten und Grenzen der neuen Blockchain-Technologie

Mehr Hype oder doch Revolution für Finanzprozesse?

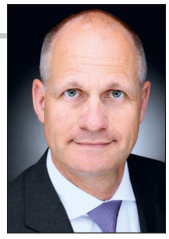
Dr. Axel Sauerland

Transaktionen wie Überweisungen, Kauf- oder Leasing-Verträge können mittels Blockchain schnell, sicher und transparent digitalisiert abgewickelt werden. Die Technologie ersetzt bisherige zentrale Instanzen und Intermediäre. Welche Eigenschaften, Einsatzgebiete und welchen Nutzen kennzeichnen Blockchains in der Finanzindustrie? Werden sie die Banken verdrängen? Der Beitrag beschreibt Sicherheitsaspekte, Möglichkeiten, aber auch Grenzen für den technologischen Einsatz.

In einer Titelgeschichte erklärte „The Economist“ Ende 2015 Blockchain zur „Vertrauensmaschine“; das World Economic Forum legte im Jahr 2016 eine umfangreiche Studie zum Potenzial der „Distributed Ledger Technologie“ für die Finanzwelt vor, gemeint ist damit Blockchain. Forschungsinstitute und Konferenzen haben das Thema auf ihren Agenden ganz nach oben gesetzt, Fintechs und Start-ups experimentieren damit, Banken gründen Finanzkonsortien, um Industriestandards zu setzen.

Selbst technologieaffinen Interessierten wird der Begriff Blockchain oft mit einem Verweis auf die virtuelle Währung Bitcoin nahegebracht – das ist richtig und auch falsch. Richtig ist, dass es seit der Einführung von Bitcoins im Jahr 2008 möglich ist, Überweisungen ohne zentrale Abwicklungsstellen wie Banken oder Online-Bezahlsysteme durchzuführen. In diesem Falle werden nur Datensätze zwischen den Nutzern in der Blockchain – dies am besten übersetzt mit „Kontokette“ – ausgetauscht. Falsch ist es allerdings, die Technologie lediglich auf den Einsatz von Kryptowährungen zu beschränken. Vielmehr sind vielfältige Anwendungen bei Finanztransaktionen denkbar, zum Beispiel neue Smart Contracts ohne Intermediäre, Echtheitszertifikate entlang von Lieferketten und vieles mehr. Blockchain ist immer dann in Betracht zu ziehen, wenn drei Dinge zusammenkommen: Mehrere Parteien mit einem Objekt, kein bedingungsloses Vertrauen zwischen den Parteien sowie der Wunsch nach digitalisiertem Ablauf.

DER AUTOR:



Dr. Axel Sauerland, Düsseldorf,

verantwortet als Leasing Industry Leader in der Beratungssparte von IBM Global Business Services das Marktsegment Absatzfinanzierer.

E-Mail: axel.sauerland@de.ibm.com

Komponenten und Arbeitsweise

Das Prinzip von Blockchain erlaubt eine schnelle, sichere und transparente Durchführung von Transaktionen; zentrale Instanzen wie bisher[1] können dadurch entfallen. Blockchain besteht – vereinfacht dargestellt – aus nachfolgenden, näher beschriebenen Komponenten.

Es gibt ein geteiltes Register, das heißt, ein verteiltes und gemeinsames Bestandsführungssystem – oder Kassenbuch –, deren Kopien auf den Rechnern der teilnehmenden Parteien liegen. Teilnehmer sind die Nutzer oder Parteien, die an einer auf Blockchain basierenden Lösung angeschlossen sind und den jeweiligen Regeln folgen, insbesondere dem Consensus-Prinzip. Alle Teilnehmer akzeptieren demnach im Netzwerk verifizierte Transaktionen (Consensus).

Eine Transaktion kann ein Geschäftsvorfall in Form einer Überweisung von Person A zu Person B, ein Kaufvertrag, eine notarielle Beurkundung, eine Geschäftsregel und so weiter sein. Diese Information wird in eine Datei geschrieben, dem (neuen) Block. Blocks werden durch einen sogenannten Hash (Prüfsumme) ausgezeichnet, zusammen mit dem Hash des vorangegangenen Blocks (Transaktionshistorie) verknüpft und in die Kette (englisch: chain) angehängt.

Des Weiteren können Geschäftsregeln (Smart Contracts) zu einer Blockchain-Lösung gehören. Die Hinterlegung von Vereinbarungen oder Verträgen erfolgt in Form eines Programmcodes. Dieser wird, in Abhängigkeit von definierten Ereignissen, automatisch ausgeführt. Die Verkettung eines Blocks in die gesamte

1) Das könnte manchen klassischen Akteur in der Finanzindustrie zukünftig ersetzen, ebenso die durch Disruption entstandenen neuen Vermittler wie Uber oder Airbnb, wenn Personenbeförderungen oder Unterkünfte nur noch über Blockchain vermittelt werden.

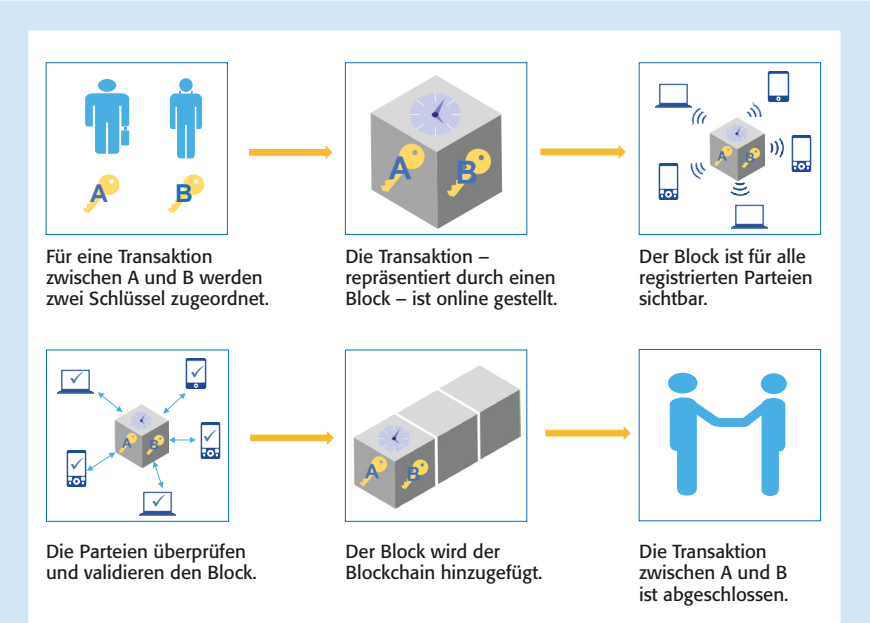
Blockchain kann nur dann stattfinden, wenn die Mehrheit der teilnehmenden Rechner die Richtigkeit der Transaktion in dem Block bestätigt. Somit herrscht ein hohes Maß an Zuverlässigkeit und Sicherheit. Ein Hacker müsste für eine Manipulation eines Blockes alle vorhergehenden Blöcke manipulieren, und zwar auf mindestens 50 Prozent der Rechner der registrierten Teilnehmer. Nach heutigem Stand der Technik ist dies unmöglich.

Allerdings bleibt bei dieser Technologie nichts geheim. Jede Transaktion kann von den Teilnehmern der Blockchain eingesehen werden, zumindest in ihrem Programmcode. Eine Vertraulichkeit in der Blockchain hingegen gewährleistet die asymmetrische Verschlüsselung mittels privatem und öffentlichem Schlüssel. Anonymität ist dadurch gegeben, dass jede Transaktion durch einen privaten – geheimen – Schlüssel signiert wird.

Der öffentliche Schlüssel fungiert als Empfangsadresse und ist die Kennung, analog einer Kontonummer, mit der ein Teilnehmer für andere sichtbar ist. Der öffentliche Schlüssel (Public Key) stimmt kryptografisch jeweils mit dem privaten Schlüssel (Private Key) überein. Um die Vertraulichkeit zu erhöhen, gibt es inzwischen Blockchain-Implementierungen, die für jede Transaktion ein neues Schlüsselpaar nutzen. Eine Transaktion kann somit wie in Abbildung 1 dargestellt aussehen.

Ein komplexerer Anwendungsfall liegt beim Fahrzeug-Leasing vor. Die bisherige Prozesskette Hersteller, Händler, Absatzfinanzierer, Kunde ist bei den unterstützenden Informationssystemen stark fragmentiert. Der Einsatz von Blockchain generiert eine schnelle, sichere und automatisierte Weitergabe der Services im Geschäftsnetzwerk[2]. Das Kraftfahrtbundesamt erteilt und veröffentlicht die Typgenehmigung für das neue Fahrzeug mit einem Smart Contract. Der Hersteller ergänzt innerhalb einer Instanz den

Abbildung 1: Ablauf einer Transaktion



Quelle: Dr. Axel Sauerland, IBM Corporation

Smart Contract mit der Fahrzeug-Identifizierungsnummer (FIN/VIN), Marke, Modell und weiteren Informationen. Diese Ergänzung ist für alle teilnehmenden Parteien sichtbar und wird lediglich von den sogenannten Validating Peers, die für den Consensus zuständig sind, bestätigt. Anschließend wird der Vertrag zur Leasing-Gesellschaft transferiert. Der Leasing-Nehmer steigt dann ebenfalls in diesen Smart Contract ein, dieser wird um verkaufs- und finanzierungsrelevante Details ergänzt. Fahrzeugrücknahme und die Verwertung der Fahrzeuge dürfen dann nur die vorab im Smart Contract zugelassenen Anbieter durchführen (siehe Abbildung 2, Seite 110).

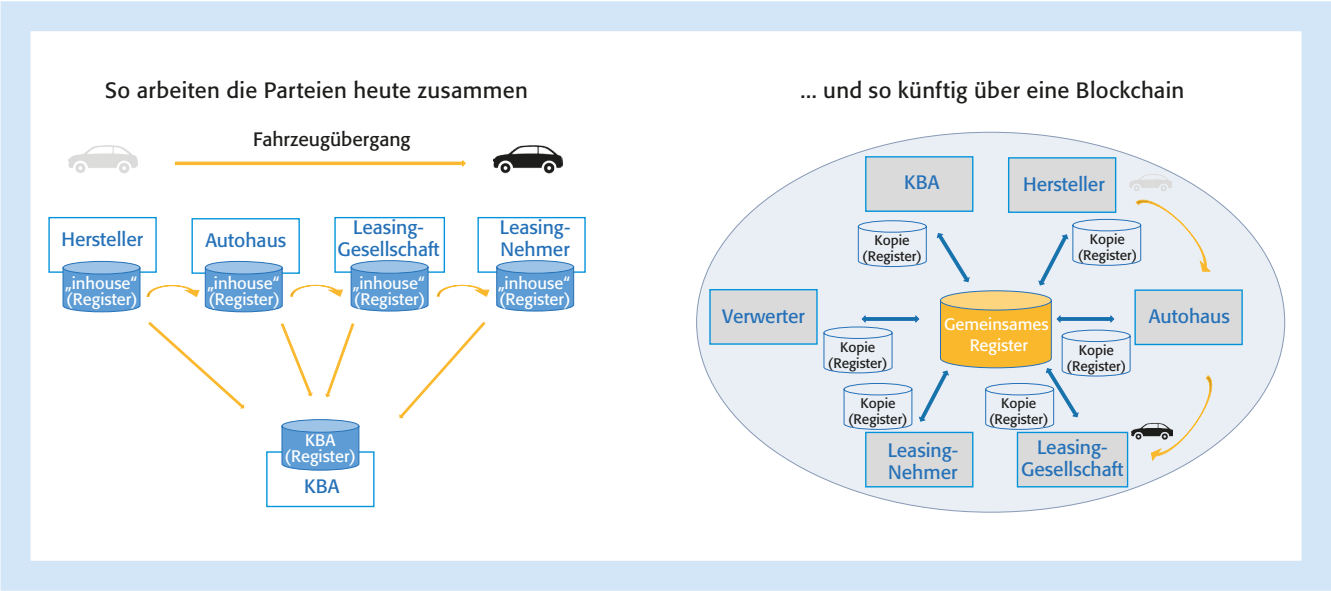
Voraussetzungen und Nutzen

Die vorhergehenden Beispiele zeigen folgende Anforderungen an einen Anwendungsfall, der zum Einsatz einer Blockchain führt: Es muss eine Interessengemeinschaft bestehen, zunächst auch von kleiner Teilnehmerzahl aufgebaut, die wichtige Referenzdaten teilen will und darauf eine konsolidierte und konsistente Ansicht nahezu in Echtzeit wünscht. Die übertragenen Daten können Finanzgüter sein, aber auch andere Informationen wie Stimmrechte, Dividendenbenachrichtigungen und so weiter. Denkbar sind auch Grundbucheinträge zur Ablösung eines bisherigen papierbasierten staatlichen Grundbuches, (finanzielle) Nutzungsbedingungen zwischen Künstler und Fans innerhalb einer globalen Musikrechte-Datenbank, das Regelwerk zwischen Versicherungsnehmer und Versicherung einschließlich der Registrierung und Begleichung von Schadensfällen, sogar ein auf Blockchain basierendes Wahlsystem.

Schließlich sollten die Transaktionen den Anspruch erheben, dass sie einerseits lückenlos zurückverfolgt werden können – inklusive Eigentums- und Statusübergänge – und somit eine Historiendokumentation im Sinne eines Prüfpfades (Audit Trail) bieten. Andererseits müssen sie unveränderbar sein (Manipulationssicherheit). Schlussendlich sollte nur ein Ort über Eigentum oder Trans-

2) Im Detail siehe https://www.youtube.com

Abbildung 2: Neue Formen der Zusammenarbeit



Quelle: IBM Corporation

aktionsabschluss (Shared Ledger) bestimmen können, damit eine Finalität im Sinne einer Bestandskraft vorliegt.

Der Nutzen einer Blockchain lässt sich an folgenden Eigenschaften darstellen:

- Resistenz: Cyberangriffe, Missbrauch und Manipulationen sind weitestgehend ausgeschlossen. Allerdings gilt dies nur bei bestehenden und etablierten Blockchains wie die für Bitcoin. Wird eine völlig neue Blockchain aufgesetzt, ist naturgemäß diese Eigenschaft für die Netzwerkarchitektur mit ihren Knoten noch nicht hergestellt.
- Effizienz: Transaktionszeiten für die Übertragung von Werten werden drastisch reduziert. Zum Beispiel kann die Abwicklung von Transaktionen im Wertpapierhandel von Tagen auf Echtzeit reduziert werden.
- Stabilität: Gemeinsame Prozesse und Bestandsführung erhöhen das Vertrauen.
- Kostenersparnis: Der größte Vorteil stellt sich in der Reduktion der Transaktionskosten dar. Bisher regulierende oder kontrollierende Instanzen oder Intermediäre wie Banken, Clearingstellen, Anwälte und Notare, Zwischenhändler, Broker et cetera entfallen. Das Netzwerk kontrolliert die Gültigkeit von Geschäften selbst, also Geldtransaktionen oder Verträge, die in den Blocks hinterlegt sind.

Das größte Potenzial der Blockchain liegt dennoch in der Generierung neuartiger Verträge, die sogenannten Smart Contracts. In den Transaktionsdaten einer Blockchain lassen sich vertragliche Vereinbarungen im Sinne einer Wenn-Dann-Logik hinterlegen. Sobald die Blockchain mehrheitlich registriert, dass bestimme vertragliche Bedingungen erfüllt sind, werden automatisch vorher definierte Aktivitäten ausgelöst. Herkömmliche zwischengeschaltete Instanzen und Intermediäre, die üblicherweise Vertrauen zwischen den Parteien herstellen, werden damit überflüssig. Beispielsweise wird beim Autokauf der digitale Autoschlüssel erst dann freigeschaltet, wenn der vorab definierte Anzahlungspreis beim Verkäufer eingegangen ist – und wiederum gesperrt, wenn eine Ratenzahlung ausbleibt.

Sicherlich ist die physische Größe einer Blockchain beachtenswert, muss allerdings auch handhabbar bleiben. Die der Bitcoin hat Stand Anfang 2017 eine Größe von circa 120 Gigabyte[3] erreicht, was dem Dateninhalt von gut zwei Blu-Ray-Discs entspricht, und verteilt sich auf etwa 5700 Knoten[4]. Trotzdem gibt es schon generelle Überlegungen, wie das Wachstum einer Blockchain gebremst werden kann. Neben dem Abschneiden oder Ausdünnen einer Blockchain (Pruning) wird die Entwicklung von Sidechains diskutiert. Eine Sidechain wird nur für eine bestimmte Anwendung erstellt und existiert zunächst autark. Die Transaktionen, die über diesen Zweck hinausgehen, werden über eine Schnittstelle in die eigentliche Blockchain transferiert.

Blockchain und Industrie 4.0

Eine weitere Bedeutung wird die Blockchain-Technologie bei der vierten industriellen Revolution bekommen. Nach der Mechanisierung durch die Einführung der Dampfmaschine, der arbeitsteiligen Massenproduktion durch Elektrifizierung und der Automatisierung durch Einsatz von Computertechnik wird die durchgängig

3) Abgerufen unter: https://bitinfocharts.com
4) Abgerufen unter https://bitnodes.21.co.

digitalisierte Industrie, Stichwort Industrie 4.0 oder Internet of Things, einen weiteren Produktivitätsschub und neue Geschäftsmodelle hervorbringen. Ein Beispiel ist der 3-D-Druck von Objekten. Neben interessanten Fragestellungen für das Leasing dieser Objekte – beispielsweise der Zuordnung des geistigen Eigentums an dem Objekt zum Designer, zu dem Programmierer der Daten, zur Druckgesellschaft beziehungsweise allen gemeinsam – müssen die Informationen über den Herstellungsprozess von einer übergeordneten Instanz überwacht werden. So könnten die für den 3-D-Druck notwendigen Daten über eine „Blockchain-as-a-service" verschlüsselt ausgetauscht werden, sie wären damit eben nicht mehr veränderbar, würden aber trotzdem allen am Prozess Beteiligten zur Verfügung gestellt werden.

Aktuell überwiegen noch die Vorbehalte über die Einsatzmöglichkeiten dieser neuen Technologie. Skepsis bestand allerdings ebenso vor gut 30 Jahren bei der Vorstellung eines damals unbekannten Netzwerkprotokolls, des TCP/IP-Standards, welches heute die Grundlage des weltumspannenden Internets und damit auch von Industrie 4.0 ist.

Zukunft und Grenzen

Blockchains werden die bisherigen Banken als Intermediäre nicht verdrängen. Ganz im Gegenteil: Diese bilden Konsortien wie das Start-up R3[5], um die Technologie selbst zu nutzen und in ihrem eigenen Sinne weiterzuentwickeln, beispielsweise in einem Produkt zur Verwaltung von Finanzverträgen. Das im Dezember 2015 von der Linux-Foundation gegründete Hyperledger-Projekt wiederum verfolgt den Anspruch, Blockchain-Technologie durch Identifizierung und Umsetzung wichtiger branchenübergreifender Funktionalitäten zu einem offenen Standard für verteilte Register weiterzuentwickeln.

Die Initiative wächst, von 17 Gründungsmitgliedern ist die Gemeinschaft auf mehr als 100 Mitglieder – Stand Ende 2016 – angestiegen. Diese Innovatoren, Branchenexperten und Infrastrukturanbieter wirken gemeinsam daran, geschäftliche Transaktionen auf Basis von Blockchain weiterzuentwickeln. Auf der offenen Plattform IBM-Blockchain Ecosystem können beispielsweise Organisationen gemeinsam oder komplementär an technischen wie auch geschäftlichen Themen rund um die Hyperledger Fabric arbeiten und diverse Technologien nutzen.

Allein: Es gibt zurzeit nicht die eine verwendbare Blockchain als „Vertrauensmaschine"[6] und schon gar nicht wird es eine weltumspannende Blockchain geben. Vielmehr existieren aktuell unterschiedliche und nicht kompatible Technologieansätze, die noch nicht als ausgereift bezeichnet werden können und meist auf Unternehmen zugeschnitten sind.

Weitere zukunftsweisende Technologien

Zudem müssen grundsätzliche Fragen des Datenschutzes, der Governance und Compliance für die Finanzbranche angegangen werden, was die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bereits erkannt hat.[7] Auf die Studie des World Economic Forum[8] zurückkommend ist Blockchain demnach geeignet, die Finanzwelt nachhaltig zu transformieren, wird aber nicht die einzige revolutionäre Technologie bleiben. Sie bewegt sich vielmehr in bester Gesellschaft mit weiteren Zukunftsthemen wie Cognitive Banking, Quantum Computing und Robotics. ◄

5) R3CEV LLP.
6) Siehe http://www.economist.com. Abgerufen am 6.1.2017.
7) Siehe https://www.bafin.de. Abgerufen am 6.1.2017.
8) Die Studie ist abrufbar unter https://www.weforum.org/reports. Abgerufen am 6.1.2017.