Blockchain-Technologien und ihre Implikationen

Prof. Dr. Peter Roßbach

Teil 1: Was verbirgt sich hinter der Blockchain-Technologie?

Einleitung

In der jüngeren Zeit findet man vermehrt Artikel in Zeitschriften, Internet-Blogs etc., die sich mit dem Thema Blockchain befassen. Demnach nimmt diese recht junge Technologie derzeit rasant an Fahrt auf und hat das Potential, insbesondere im Finanzsektor erhebliche Veränderungen herbeizuführen. Im Vergleich zu den vorherrschen Systemarchitekturen handelt es sich dabei um einen Ansatz, der einen radikalen Konzeptwechsel mit sich bringt.

Um zu verstehen, warum der Blockchain-Technologie ein derartiges Potential zugesprochen wird, muss man zunächst verstanden haben, was sich hinter dem Konzept verbirgt. Gegenstand dieses Beitrags soll es daher sein, die Grundlagen des Blockchain-Konzeptes zu vermitteln. In zwei nachfolgenden Beiträgen sollen dann zum einen die Anwendungsfelder und deren derzeitige Akteure beleuchtet sowie zum anderen ausgewählte Blockchain-Ansätze vorgestellt werden.

Die heutige Situation

Während in etlichen Branchen, wie z.B. im Handel, bereits heute direkte Transaktionen zwischen den Geschäftspartnern stattfinden, ist die Situation auf der Finanzseite davon geprägt, dass Finanzprozesse noch oft über mehrere Intermediäre laufen, bevor beispielweise ein Zahlungs- oder Wertpapierhandelsvorgang abgeschlossen werden kann. Dies gilt insbesondere im internationalen Bereich.

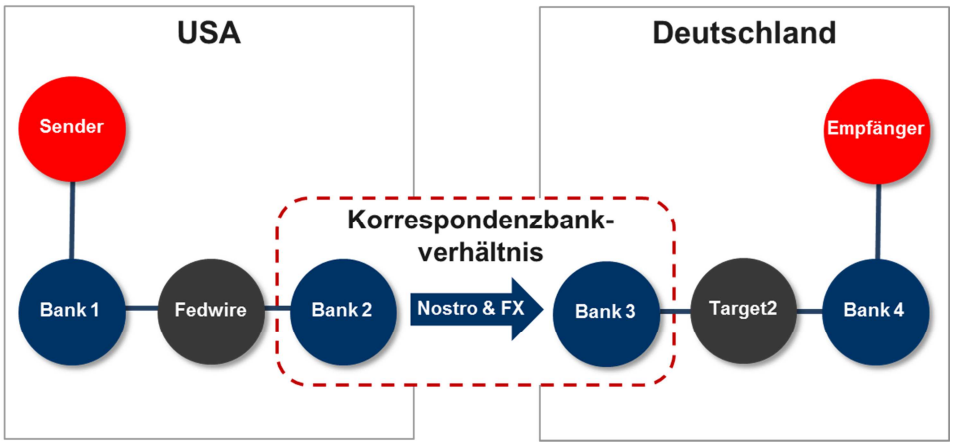

Abbildung 1: Beispiel einer internationalen Zahlungstransaktion

Quelle: In Anlehnung an [1]

Abbildung 1 zeigt ein Beispiel aus dem internationalen Zahlungsverkehr. Im Allgemeinen haben die Länder ihre eigenen Zahlungssysteme mittels derer das Clearing und Settlement der Transaktionen der Banken innerhalb der Länder abgewickelt wird [1]. Ein Spezialfall ist hier die EU, die mit Target2 ein gemeinsames System betreibt. Wenn nun ein Kunde einer kleinen Bank in den USA eine Zahlung an einen Kunden einer kleinen Bank in Deutschland leisten will, so muss die Kundenbank in den USA die Zahlung über das amerikanische Zahlungssystem (wie z.B. Fedwire) an eine amerikanische Bank transferieren, die ein Korrespondenzbankverhältnis zu einer Bank innerhalb des europäischen Zahlungssystems Target2 unterhält. Diese transferiert die Zahlung dann über Target2 an die deutsche Empfängerbank. Bei anderen Finanzprozessen, wie z.B. Im Wertpapierhandel, existieren ähnliche Situationen.

Die Folge ist, dass derartige Prozesse langsam, teuer und fehleranfällig sind. Jeder im Prozess beteiligte Intermediär betreibt ein eigenes System und der Prozess wandert von System zu System. Die Architektur der einzelnen Systeme folgt einem zentralisierten Ansatz, d.h. es handelt sich um jeweils geschlossene Systeme, die die Verwaltung und Abwicklung von Transaktionen vornehmen (siehe Abbildung 2). Dazu führt jedes System ein eigenes Buch, in dem die Konten- und/oder Transaktionsinformationen gespeichert werden. Dieses Buch soll im Folgenden als Ledger bezeichnet werden.

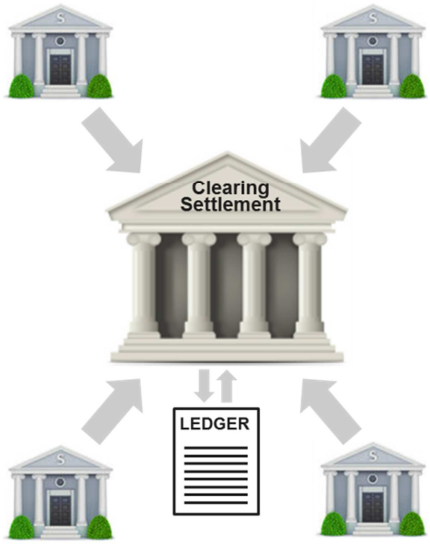

Abbildung 2: Der traditionelle zentralisierte Ansatz
Quelle: In Anlehnung an [2]

Um die Funktionsfähigkeit eines einzelnen Systems zu gewährleisten, müssen hohe Aufwendungen betrieben werden. Neben der Sicherstellung der Korrektheit der Funktionalität müssen die Systeme vor allem auch gegen Manipulation, Einbruch und Ausfall abgesichert werden. Ein solches zentrales System stellt somit immer einen Single Point of Failure dar, der ein entsprechendes operatives Risiko mit sich bringt. Sind an einem

Finanzprozess dann auch noch mehrere dieser Systeme beteiligt, so führt dies zu einer Kumulation von Kosten und Risiken.

Angesichts dieser Ineffizienzen in den Finanzprozessen wäre es eine Idealvorstellung, wenn man direkte Finanztransaktionen zwischen den Geschäftspartnern betreiben könnte. Mit den traditionellen, zentralisierten Systemarchitekturen würde dies aber ein weltweit zentrales System bedingen. Weltweit agierende Finanzdienstleister, wie Paypal, arbeiten bereits nach diesem Prinzip, jedoch ist man damit an einen Anbieter gebunden. Im Hinblick auf ein weltweit bankenübergreifend betriebenes System dürften etliche politische Hürden bestehen, die von der Frage hinsichtlich des Betreibers bis hin zu den Autonomie- und Sicherheitsbedürfnissen der einzelnen Länder reichen. Ein solches System beinhaltet aufgrund seiner zentralisierten Architektur zudem immer noch die Problematik eines Single Point of Failure, so dass ein immenser Verwaltungsapparat notwendig wäre.

Ein verteilter Ansatz als Alternative

Basierend auf den technologischen Entwicklungen der vergangenen Jahre bietet sich ein verteilter Ansatz als Alternative an. Hierbei wird ein Netz aus unterschiedlichen Teilnehmern (im Folgenden als Knoten bezeichnet) betrieben, bei dem jeder Knoten die gleichen Rechte hat. Man bezeichnet einen solchen Netzansatz auch als Peer-to-Peer-Netz. Die Knoten können von Ländern oder Banken oder sonstigen Unternehmen betrieben werden. Um die gleichen Rechte zu wahren, dürfen keine ungleichen Machtverhältnisse bestehen. Dies kann gewährleistet werden, indem alle Knoten die gleichen Informationen besitzen und das Recht haben, neue Informationen dem Netz hinzuzufügen.

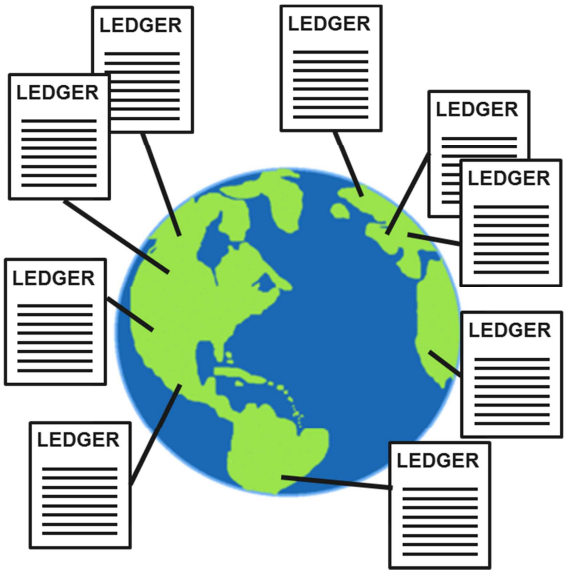

Abbildung 3: Der verteilte Ansatz

Die gleichen Informationen zu besitzen, bedeutet im gegebenen Kontext, dass jeder Knoten eine Kopie des kompletten Ledgers besitzt (siehe Abbildung 3). In diesem Fall bestünde ein

Basisschutz des Netzes vor Manipulationen, da diese auf der Mehrzahl der Knoten durchgeführt werden müssten, um wirksam zu sein. Die Funktionsfähigkeit des Netzes selbst bliebe auch dann erhalten, wenn einzelne Knoten oder Knotensegmente ausfallen würden. Gleiches gilt für das Hinzufügen und Entfernen von Knoten. Die durch die Verteilung des Ledgers bewirkte vollständige Redundanz ist somit ein Mittel gegen einseitige Macht, Manipulation und Ausfall, womit allein durch die Architektur des Systems bereits Schutzmechanismen existieren, die in den zentralisierten Ansätzen aufwendig bereitgestellt werden müssen.

Die personenbezogenen Daten im Ledger können zudem anonymisiert sein, um nicht auf die einzelnen Geschäftspartner schließen zu können. Diese Informationen wären dann allein dem jeweiligen Urheber einer Transaktion vorbehalten. Aus dem Ledger ginge dann hervor, was Gegenstand der Transaktion war, aber nicht, wer daran beteiligt war.

In einem verteilten Ansatz wie dem hier dargestellten, existiert somit keine zentrale Instanz mehr. Damit kann auch deren Intermediärsfunktion, für die Korrektheit der Vorgänge zu sorgen, nicht mehr in Anspruch genommen werden.

Das Double-Spending-Problem

Derartige Systemansätze scheiterten im Finanzbereich in der Vergangenheit immer an dem sog. Double-Spending-Problem. Dieses ergibt sich aus dem Umstand, dass man sein Geld nicht mehrfach ausgeben bzw. seine Wertpapiere nicht mehrfach verkaufen kann. Hat man beispielsweise nur noch 100 Euro auf seinem Konto, sollte es nicht möglich sein, diese in zwei oder mehrere Transaktionen mehrfach zu verwenden.

In der traditionellen Welt werden derartige Betrugsversuche durch die Intermediäre, hier den Betreiber des Zahlungssystems, erkannt und verhindert. In einem verteilten Netzwerk ohne einen derartigen Intermediär besteht dieser Schutzmechanismus jedoch nicht. Hinzu kommt, dass digitale Einheiten leicht vervielfältigt werden können. Es wird somit ein Mechanismus benötigt, der verhindert, dass man dasselbe Geld an jemanden transferieren kann, wenn man es zuvor schon an jemanden anderen transferiert hat.

In einem Peer-to-Peer-Netz stehen neu auftretende Informationen nicht zum exakt gleichen Zeitpunkt allen Knoten zur Verfügung, sondern müssen sich immer erst im Netz verteilen, da sie an einer Stelle, also einem Knoten, dem Netz zugefügt werden und sich dann von dort aus auf die anderen Knoten verbreiten müssen (siehe Abbildung 4). Dies benötigt Zeit.

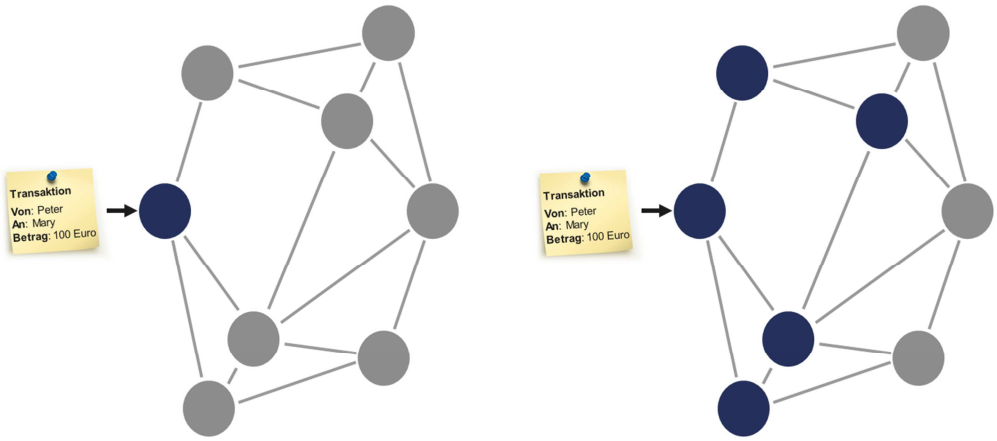

Abbildung 4: Transaktionseingang und -verteilung

Wenn nun ein Knoten eine Transaktion mit einem Asset in eine Richtung schickt und eine andere Transaktion mit dem gleichen Asset in eine andere Richtung, so bestünde ein Double-Spending-Problem, das das Netz in einen inkonsistenten Zustand bringt, da die Knoten unterschiedliche bzw. widersprüchliche Informationen haben (siehe Abbildung 5).

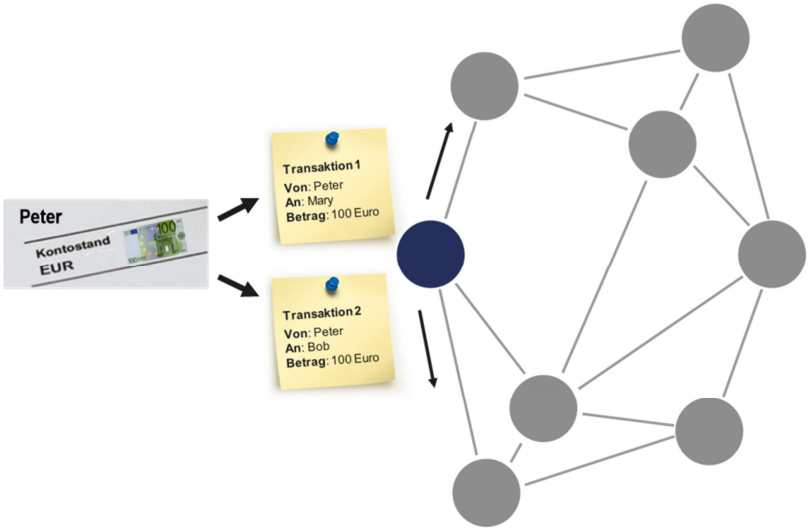

Abbildung 5: Double Spending

Lösungsansatz durch Bitcoin

Die Lösung dieses Double-Spending-Problem war lange Zeit ein Hindernis für die Umsetzung Verteilungs-basierter Ansätze im Finanzbereich. Mit der Erfindung von Bitcoin im Jahre 2008 wurde schließlich erstmals ein allgemeiner Ansatz geschaffen, mittels dessen das Problem gelöst werden konnte [3]. Auch wenn Bitcoin primär als digitale Währung wahrgenommen wird, kann diese ohne eine zentrale Vertrauensinstanz nicht funktionieren, wenn sie keinen Schutz vor Double Spending bietet.

Die Lösung im Bitcoin-Konzept ist ein Mechanismus, der als Blockchain bezeichnet wird [4]. Diese realisiert ein Transaktionsbuch, in dem alle Bitcoin-Transaktionen verzeichnet sind, die

jemals stattgefunden haben. Es handelt sich dabei um einen kollektiven, öffentlichen Ledger, der allen Teilnehmern des Systems zur Einsicht steht, aber von niemandem kontrolliert wird. Der Ledger wird dabei nicht zentral gespeichert, sondern bei den Teilnehmern des Bitcoin-Systems als lokale Kopie.

Mit Bitcoin konnten Personen, die sich nicht gegenseitig vertrauen oder kennen müssen, zum ersten Mal ein digitales Asset auf sichere Weise austauschen, ohne eine neutrale zentrale Instanz als Intermediär zu benötigen [3]. Dies entspricht genau dem oben dargestellten Prinzip der Verteilung. Angestoßen durch diese Entwicklung sind dann im Laufe der Zeit weitere Blockchain-basierte Ansätze entwickelt worden, die eine Lösung des Double-Spending-Problems bereitstellen und somit als Grundlage für verteilte Systeme verwendet werden können.

Voraussetzungen

Für die Funktions- und Praxisfähigkeit eines derartigen Systems müssen drei Grundvoraussetzungen erfüllt sein: Korrektheit, Einigkeit und Anwendbarkeit [5].

Korrektheit meint hier, dass die in das System aufgenommenen Transaktionen gültige Transaktionen sind. Dazu muss ein Mechanismus existieren, der dafür sorgt, dass eine Transaktion sich nicht auf ein frei erfundenes Asset oder das Asset eines Anderen beziehen kann. So können beim Bitcoin-System beispielsweise keine Bitcoins transferiert werden, die gar nicht existieren und jeder kann nur das transferieren, was er auch hat. Dafür sorgen entsprechende Technologien der Kryptografie, auf die hier nicht weiter eingegangen wird [6].

Einigkeit bedeutet, dass alle Netzknoten über die gleichen Informationen verfügen und es nicht unterschiedliche bzw. widersprüchliche Informationsstände gibt. Dies muss nicht exakt zu jedem Zeitpunkt gelten, was auch gar nicht möglich wäre. Es müssen aber die Informationen, auf die die Netzknoten sich geeinigt haben, bei allen gleich und nachträglich unveränderbar sein. Die Konsequenz davon ist, dass der Grundsatz gelten muss: "Was einmal im Ledger steht, kann nicht mehr verändert werden." Es darf damit nicht möglich sein, Informationen aus dem Ledger nachträglich zu verändern oder zu löschen.

Anwendbarkeit meint schließlich, dass der Zeitbedarf vom Eingang einer Transaktion bis zum Zeitpunkt der Einigkeit über diese Transaktion (und damit deren Bestätigung) in einem zeitlichen Rahmen liegen muss, der den Anforderungen der Praxis an das Netz entspricht. Ein Zeitraum von Tagen oder länger wäre keine brauchbare Lösung.

Um sicherzustellen, dass ein Double Spending nicht möglich ist, muss ein zweiter Grundsatz eingeführt werden: „Die erste Transaktion eines Assets, die im Ledger aufgenommen wird, ist die einzig Gültige!“. Die Transaktion muss dabei korrekt im obigen Sinne sein.

Notwendigkeit eines Konsens-Mechanismus

Es stellt sich somit die Frage, wie die Aufnahme von Transaktionen in die verteilten Ledger unter den gegebenen Anforderungen gestaltet werden kann. Intuitiv bietet es sich zunächst an, den zeitlichen Eingang der Transaktion in den jeweiligen Knoten als Maß für die Reihenfolge zu nehmen [7]. Das Problem ist hier jedoch, dass die Verteilungsmechanismen im Netz bedingen, dass die Knoten die Transaktionen zu unterschiedlichen Zeitpunkten erhalten. Damit können unterschiedliche Reihenfolgen entstehen, wie das Beispiel des Double Spendings in Abbildung 5 zeigt, und die Knoten hätten unterschiedliche Informationen hinsichtlich des oben formulierten zweiten Grundsatzes. Alternativ könnte der Zeitstempel des Eingangs der Transaktion in das Netz verwendet werden. Dies beinhaltet jedoch die Problematik, dass Zeitstempel manipulierbar sind, womit eine Transaktion z.B. im Rahmen eines Betrugsversuchs vordatiert werden könnte. Eine rein zeitbasierte Ordnung ist somit nicht funktionsfähig.

Es muss folglich ein Verteilungsmechanismus gefunden werden, bei dem sich die Knoten auf die aufzunehmenden Transaktionen einigen. Ein solcher Mechanismus wird in der Literatur als Consensus bezeichnet. Als Consensus wird hier eine gemeinsame Einigung mehrerer Parteien, die sich gegenseitig nicht zwangsläufig vertrauen müssen, auf einen gemeinsamen Ledger verstanden [8].

Um einen solchen Prozess effizient zu gestalten, macht es keinen Sinn, ihn für jede einzelne Transaktion durchzuführen, da dies viel zu aufwändig wäre. Aus diesem Grund werden die eingehenden Transaktionen von den Knoten über einen bestimmten Zeitraum gesammelt (bei Bitcoin z.B. über ungefähr 10 Minuten) und dann als Gruppe in den Einigungsprozess eingebracht (siehe Abbildung 6). Diese Gruppe an Transaktionen bildet die Kandidaten für die Erstellung eines Blocks von Transaktionen, der dem Ledger hinzugefügt wird. Neue Transaktionen sind also nicht automatisch Bestandteil des Ledgers. Stattdessen werden sie zunächst in einer Art temporärem Speicher gesammelt, im Rahmen eines Konsensprozesses zu einem Block geschnürt und dann dem Ledger angehängt.

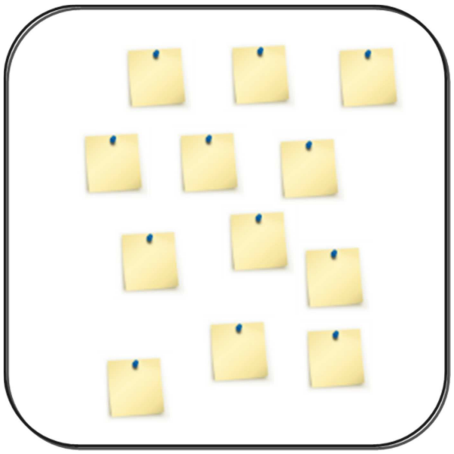

Abbildung 6: Zusammenfassung von Transaktionen zu einem Block

Die Blockchain

Die Blockbildung hat noch einen weiteren Vorteil. So wäre ein sequentiell geschriebener Ledger prinzipiell zu jedem Zeitpunkt an jeder Stelle rückwirkend manipulierbar. Man müsste nur auf die Transaktion an der entsprechenden Stelle zugreifen und deren Daten verändern. Wenn die Transaktionen jedoch in Blöcken abgespeichert sind, so kann man diese Blöcke vor Manipulationen absichern, indem man in jeden Block als digitalen Fingerabdruck ein kryptografisches Abbild des vorhergehenden Blocks einbaut (siehe Abbildung 7).

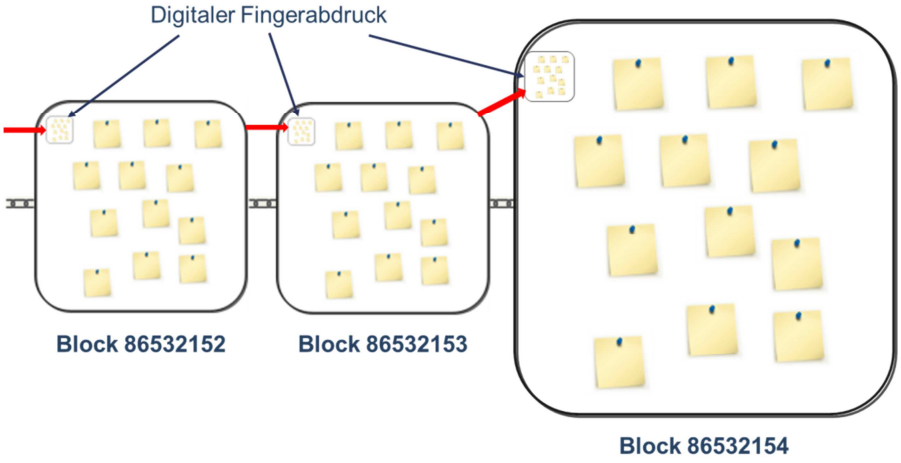

Abbildung 7: Die Blockchain

Auf diese Weise werden die Blöcke in einer Kette verbunden, bei der das kryptografisches Abbild jedes nachfolgenden Blocks von dem des vorhergehenden Blocks und damit von allen vorhergehenden Blöcken abhängt. Da die Manipulation eines Blocks zu einem anderen kryptografischen Abbild führen würde, wäre eine Manipulation somit nur noch möglich, wenn ausgehend vom dem Block, der die zu manipulierende Transaktion enthält, auch alle nachfolgenden Blöcke manipuliert würden. Dies müsste zudem geschehen, bevor der nächste Block entsteht und die Manipulation müsste an der Mehrzahl der Knoten stattfinden. Wenn darüber hinaus die Erzeugung eines Blockes sehr aufwändig ist (wie bei

Bitcoin) oder die Zusammenarbeit mehrerer Knoten erfordert (wie bei anderen Blockchain-Ansätzen), besteht eine extrem große Hürde für die Durchführung etwaiger Manipulationen.

Die Blockchain repräsentiert somit einen Ledger, in dem die Informationen in Form von kryptografisch verketteten Blöcken organisiert sind. Durch die Verbindung des Block-Prinzips mit Methoden der Kryptografie kann der Ledger in einem verteilten Ansatz verwendet werden, ohne die Notwendigkeit einer zentralen Instanz bzw. des gegenseitigen Vertrauens der Beteiligten. Die Sicherheitsmechanismen im Hinblick auf Manipulation und Ausfall sind dabei bereits inhärent in den Konzepten und Protokollen enthalten und müssen nicht wie bei den zentralisierten Ansätzen mit großem Aufwand hinzugefügt werden.

Blockchain-Technologien eröffnen die Möglichkeiten, Transaktionsprozesse schneller, billiger, weniger fehleranfällig und nachvollziehbarer zu gestalten. Dies ist insbesondere für den Finanzsektor von Bedeutung. Entsprechend erwartet die European Banking Authority (EBA), dass die Blockchain-Technologien von den Banken zunächst für die weitere Automatisierung der existierenden Prozesse genutzt werden, auf längere Sicht aber auch Raum für Innovationen bieten [9].

In diesem Beitrag wurde die grundsätzliche Funktionsweise des Blockchain-Ansatzes dargestellt. In den vergangenen Jahren sind daraus verschiedene Varianten abgeleitet worden, die sich u.a. in der Netzarchitektur, den verwendeten Consensus-Mechanismen sowie in den Anwendungsbereichen unterschieden. Einen Überblick gibt [10]. Ausgewählten Ansätzen wird sich ein späterer Beitrag widmen.

Literatur

[1] McCune, E. (2014): There Is No Such Thing As An International Wire, http://paymentsviews.com/2014/05/15/there-is-no-such-thing-as-an-international-wire

[2] Santander (2015): The Fintech 2.0 Paper: rebooting financial services, http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

[3] The Economist (2015): The great chain of being sure about things, Oct 31st 2015, http://www.economist.com/news/briefing/21677228-technology-behind-bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable

[4] Nakamoto, S. (2008): Bitcoin: A Peer-to-Peer Electronic Cash System, http://bitcoin.org/bitcoin.pdf

[5] Schwartz, D.; Youngs, N.; Britto, A. (2014): The Ripple Protocol Consensus Algorithm, http://ripple.com/files/ripple_consensus_whitepaper.pdf

[6] Bergmann, C. (2013): Kryptografie des Bitcoins für Anfänger, http://bitcoinblog.de/2013/12/22/kryptografie-des-bitcoins-fuer-anfaenger

[7] Poelstra, A. (2015): On Stake and Consensus, http://download.wpsoftware.net/bitcoin/pos.pdf

[8] Swanson, T. (2015): Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[9] Euro Banking Association (2015): Cryptotechnologies, a major IT innovation and catalyst for change, http://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf

[10] BitFury Group (2015): Public versus Private Blockchains, Part 1 and 2, http://bitfury.com/white-papers-research