Blockchain-Technologien und ihre Implikationen

Prof. Dr. Peter Roßbach

Teil 2: Anwendungsbereiche der Blockchain-Technologie

Anwendungskategorien von Blockchain-Technologien

Aufgrund seiner generischen Konzeption ist der Blockchain-Ansatz universell einsetzbar, da die Blockchain im Grunde einen Informationsspeicher darstellt. Entsprechend breit ist das mögliche Anwendungsspektrum. Aufgrund ihrer verteilten und redundanten Konstruktion bietet die Blockchain dabei einen inhärenten Basisschutz vor Manipulation und Ausfall.

Von besonderem Interesse ist die Nutzung zur Verwaltung bzw. Transaktion von Assets (Vermögenswerten), für die in der traditionellen Welt Vertrauensinstanzen, z.B. in Form von Intermediären, notwendig sind (siehe hierzu auch Teil 1). Bei den Assets kann es sich um rein digitale handeln oder solche, die eine digitale Repräsentation eines physischen Objektes sind, z.B. für Dokumente oder Edelsteine. Im Fall der digitalen Repräsentation ist es von Bedeutung, dass sich das physische Objekt durch ein eindeutiges, unveränderbares Merkmal bzw. einer Kombination von diesen charakterisieren lässt.

Die Blockchain kann dabei verschiedene Funktionen erfüllen. Dazu gehört vor allem die Intermediationsfunktion, wenn es um die Vermittlung zwischen verschiedenen Parteien geht. Prinzipiell können die hierzu notwendigen Verträge in der Blockchain abgebildet werden, was vor allem für den Finanzbereich attraktiv ist, da Finanztransaktionen direkt zwischen Geschäftspartnern ermöglicht werden. Insbesondere im Zahlungsverkehr und Wertpapierhandel können mittels der Blockchain-Technologie auch Clearing- und Settlement-Funktionen umgesetzt werden. In den Anwendungsbereichen mit Fokus auf den Finanzsektor findet derzeit ein Schwerpunkt der Entwicklungen statt, da prinzipiell jeder Finanzvertrag in der Blockchain abgebildet werden kann und der Veränderungsdruck im Finanzbereich besonders stark ist.

Desweiteren kann die Blockchain Verzeichnis- und Notariatsfunktionen abbilden. In den vergangenen Jahren sind etliche Anbieter entstanden, die mittels Blockchain-Technologien die Registrierung von Besitz bzw. Eigentum sowie die Bestätigung von Urheberschaften ermöglichen. Anbieter wie Coloredcoins [1] und Factom [2] verwenden die Blockchain als Registratur für digitale und physische Assets, wie Musikstücke, Videos, Dokumente etc. Factom verhandelt z.B. derzeit mit Honduras und Griechenland über eine Anwendung zur Verwaltung von Landrechten [3]. Everledger [4] nutzt die Blockchain, um Luxusgüter wie Diamanten, Schmuck oder Bilder zu verwalten, damit diese z.B. im Fall eines Diebstahls leichter identifiziert werden können.

Einen Auftrieb erhalten die sich mit den Blockchain-Technologien ergebenden Anwendungspotentiale noch durch die Möglichkeit, die Transaktionen in der Blockchain mit Geschäftsregeln oder sonstigem Programmcode anzureichern. Damit können die Anwendungen Autonomie und Dynamik erhalten, so dass Aktionen unter festgelegten Umständen bzw. Ereignissen automatisch ausgeführt werden. So könnte z.B. eine Transaktion erst dann gültig werden, wenn die beteiligten Parteien zugestimmt haben oder eine vorhergehende Transaktion beendet ist. Lighthouse [5] bietet beispielweise ein Crowdfunding-System auf Bitcoin-Basis, bei dem die Zahlungen nur erfolgen, wenn die Mindestsumme erreicht ist, im anderen Fall passiert nichts.

Bei diesen sog. Smart Contracts werden somit Vertragselemente in die Transaktionen eingebaut und dann im Ereignisfall automatisch ausgeführt. Bei Unternehmensanleihen würde dann beispielweise nicht nur der Besitzer in der Blockchain festgehalten, sondern auch die Anweisungen, wann und in welcher Höhe die Kupons auszuzahlen sind [6]. Oder bei einem Automobilkredit könnte die Nutzung des Fahrzeugs im Falle des Zahlungsverzugs automatisch unterbunden werden.

Varianten der Blockchain-Ansätze

Eine Blockchain kann grundsätzlich im öffentlichen oder im privaten Modus genutzt werden [7]. Eine öffentliche Blockchain ist beispielweise die von Bitcoin. Hier sind alle Transaktionen zu jedem Zeitpunkt von jedermann einsehbar. Jeder kann also jederzeit sehen, welche Transaktionen stattgefunden haben, weiß aber nicht von welchen Personen, da im Bitcoin-System keine Namen, sondern kryptische Adressen verwendet werden. Bei öffentlichen Blockchain-Ansätzen besteht somit unter Umständen ein hoher Anspruch hinsichtlich der Anonymität bestimmter Daten. Für Datenlecks, wie sie in der jüngeren Zeit bei zentralisierten Systemen häufiger vorgekommen sind, beispielsweise bei dem Seitensprung-Portal Ashley Madison, würden hier aufgrund der Verteiltheit und Redundanz der Blockchain vielfältige Angriffspunkte bestehen.

Eine private Blockchain ist dagegen ein geschlossenes System, das als geteiltes System unter mehreren Kooperationspartnern oder rein firmenintern als Alternative zu existierenden Technologien betrieben werden kann. Der Zugriff auf die Blockchain ist hier lediglich auf eine Gruppe Berechtigter limitiert. Aufgrund der oben angesprochenen Datenschutzproblematik wird diese Variante bei vielen Anwendungen im Bankbereich präferiert.

Desweiteren wird unterschieden zwischen einem permissioned und einem permissionless Blockchain-Modus [7]. Im ersteren Fall dürfen nur diejenigen Teilnehmer Transaktionen einstellen, die dazu berechtigt sind, während die Anderen nur lesend auf die Blockchain

zugreifen dürfen. Bei einer permissionless Blockchain bestehen dagegen keine Unterschiede in den Berechtigungen der Teilnehmer.

In Verbindung mit dem öffentlichen bzw. privaten Modus sind damit verschiedene Kombinationen möglich. Bei einer permissioned und privaten Variante könnte ein Bankennetzwerk beispielweise den Regulatoren nur lesend Zugriff in die Blockchain erlauben, damit diese selbstständig an die benötigten Informationen gelangen. Eine permissioned und öffentliche Variante könnte beispielweise für jeden das Urheberrecht für bestimmte Assets, wie z.B. Musikstücke oder Fotos, ausweisen, während die Einträge selbst nur von den voll berechtigten Knoten vorgenommen werden können.

Je nach Kombination bestehen auch Auswirkungen auf die Anforderungen hinsichtlich der Konsensmechanismen (siehe auch Teil 1). In einer privaten Blockchain, bei der alle Teilnehmer untereinander bekannt sind, muss ein Konsensmechanismus nicht die gleiche Komplexität aufweisen, wie in einem System, in dem die Teilnehmer anonym sind und damit nicht klar ist, wem man vertrauen kann und wem nicht [8].

Entwickler von Blockchain-Technologien

Unternehmen, die Blockchain-Technologien nutzen wollen, stehen grundsätzlich vor der Wahl, diese selbst zu entwickeln oder Angebote auf dem Markt zu nutzen. Die Zahl der Anbieter ist dabei in der jüngeren Zeit stark gestiegen. Allein im Finanzbereich sind laut PwC über 300 Start-ups mit der Entwicklung von Blockchain-basierten Technologien aktiv, in die derzeit noch größere Mengen an Risikokapital fließen [9]. Die Schwerpunkte liegen in den Bereichen Zahlungssysteme und Wertpapiergeschäft. Einen Überblick sowie eine Systematik der im Finanzbereich aktiven Start-ups mit Blockchain-Technologien gibt [10].

Während anfangs nahezu ausnahmslos Start-ups Dienste und Produkte anboten, finden sich zunehmend auch etablierte Unternehmen, die Lösungen basierend auf der Blockchain-Technologie für eigene Zwecke oder als Produkte für den Markt entwickeln. Insbesondere die Start-ups haben dabei mit ihren Entwicklungen dafür gesorgt, dass die Blockchain-Technologien mittlerweile einen Reifegrad haben, der sie in der Praxis einsatzfähig macht. Dies nutzen die etablierten Unternehmen, die entweder in Kooperation mit Start-ups oder durch eigene Entwicklungen ebenfalls die Umsetzung und Anwendung der Blockchain-Technologien vorantreiben. Zu den etablierten Unternehmen gehören vor allem Technologieunternehmen und Finanzdienstleistungsunternehmen. So haben beispielsweise IBM und Samsung in Kooperation unter der Bezeichnung ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) ein Blockchain-basiertes System als Verzeichnis sowie zur Kommunikation und Wartung von Geräten im „Internet of Things“ entwickelt [11].

Während die Technologieunternehmen den Fokus mehr auf die Entwicklung verkaufsfähiger Produkte haben, geht es bei den Finanzdienstleistungsunternehmen derzeit vor allem um die Entwicklung von Lösungen, die zu einer Verbesserung der eigenen IT und Prozesse im Hinblick auf Kosten, Zeit und Fehleranfälligkeit führen. Viele der Finanzdienstleistungsunternehmen führen zurzeit eigene Projekte durch (Übersichten finden sich in [12] und [13]), es existieren aber auch Kooperationsprojekte, die aufgrund des Infrastrukturcharakters der Blockchain-Technologien besonders interessant sind.

Die wohl wichtigste gemeinsame Initiative ist das 2014 gegründete Start-up R3 CEV, in dem sich mittlerweile 42 der weltweit größten Banken engagieren [14]. Darunter befinden sich die UBS, Credit Suisse, HSBC, Goldman Sachs, J.P. Morgan, Commerzbank und die Deutsche Bank. Die genauen Inhalte der Aktivitäten von R3 CEV sind unbekannt. Angekündigt ist eine Blockchain-basierte Finanzfabrik mit einem verteilten Ledger auf einer Open-Source-Basis [15]. Dies beinhaltet dann die entsprechenden Protokolle für den Zahlungsverkehr, Wertpapierhandel etc. Die Partnerbanken kontrollieren bereits jetzt direkt oder indirekt den größten Teil des internationalen Finanzverkehrs. Wenn diese Gruppe einen gemeinsamen Standard entwickelt, hat er auch große Chancen, sich weltweit durchzusetzen. Erste Ergebnisse der Entwicklungen sollen 2016 in Betrieb genommen werden.

Auch die Euro Banking Association (EBA) steht den Blockchain-Technologien positiv gegenüber. So empfahl sie den Banken Mitte Mai 2015 in einer Veröffentlichung, sich genauer mit dem Thema Blockchain zu beschäftigen, da diese das Potenzial zu Kosteneinsparungen, geringeren operativen Risiken und Innovationen hätte [16]. In der nahen Zukunft sieht die EBA die größten Chancen dabei vor allem in Blockchain-basierten Technologien, die sich auf den Austausch von digitalen Repräsentationen physischer Assets, wie Aktien, Bonds, Währungen etc., fokussieren und die damit verbundene Dienstleistungen bereitstellen, wie z.B. dem Währungstausch bei internationalen Bezahlvorgängen.

Kategorien von Blockchain-Technologien

Die Entwicklungen und Angebote im Bereich der Blockchain-Technologien lassen sich in drei Segmente unterteilen, die als Schichten übereinander liegen: "Anwendungen", "Middleware und Services" sowie "Infrastruktur und Basisprotokolle" (vgl. Abbildung 1) [10].

Im Segment "Infrastruktur- und Basisprotokolle" finden Entwicklungen von Blockchain-Varianten und den dazu gehörenden Protokollen, wie z.B. den Konsensprotokollen, statt. Diese bilden die konzeptuellen und technischen Grundlagen, um Blockchain-basierte Anwendungen zu erzeugen. Hierzu gehören beispielsweise die Blockchain- und Konsens-Konzepte von Bitcoin und Ripple, die sich in ihrer Funktionsweise maßgeblich unterschieden (siehe auch Teil 3).

Abbildung 1: Kategorisierung von Blockchain-Technologien
Quelle: In Anlehnung an [10]

Viele der derzeitigen Blockchain-basierten Anwendungen nutzen die Blockchain von Bitcoin. Diese wurde von vornherein als offenes System konstruiert und kann somit nicht nur reine Bitcoin-Transaktionen aufnehmen. Diesen Umstand machen sich viele der Anbieter zunutze und verwenden die öffentliche Bitcoin-Blockchain als Speichermedium für die Transaktionen bzw. die Verwaltung von Assets. Andere Anbieter nutzen wiederum das Blockchain-Konzept von Bitcoin, um daraus eigene Adaptionen abzuleiten und damit separate und gegebenenfalls private Blockchains zu betreiben. Ein Beispiel dafür ist Multichain [17].

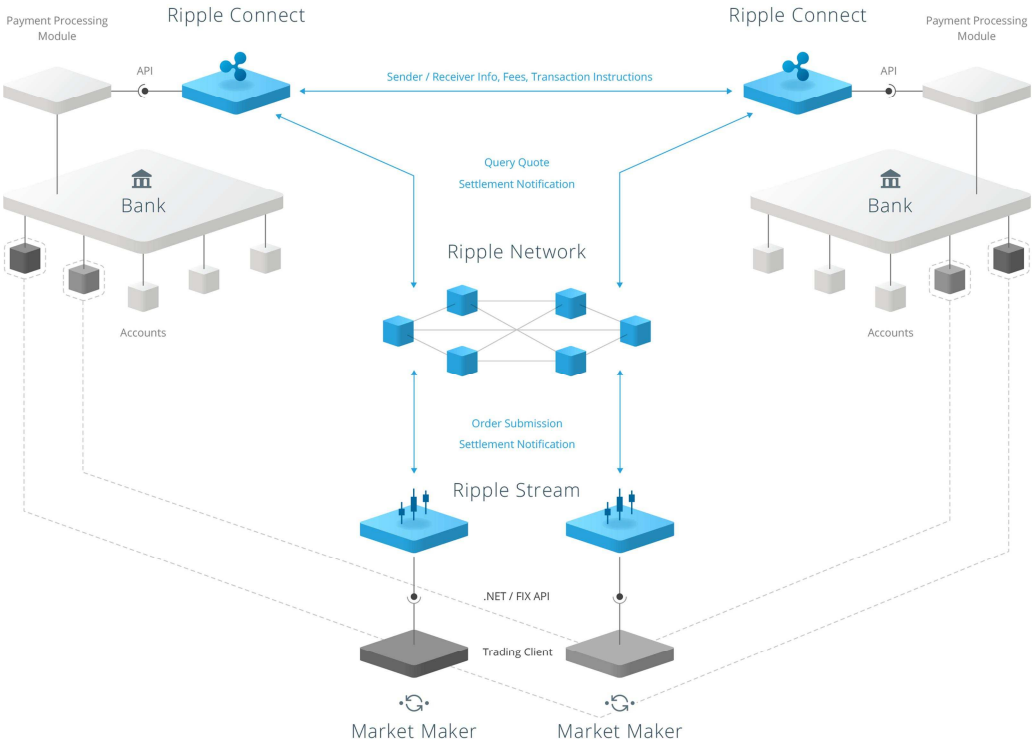

Abbildung 2: Architektur von Ripple, Quelle: [18]

Ein anderes Konzept verfolgt die Firma Ripple, die sowohl Infrastruktur und Protokolle als auch die zum Zugriff darauf notwendigen APIs (Application Programming Interfaces) und darauf aufbauende Dienste zur Verfügung stellt (vgl. Abbildung 2). Das Ripple-Kernsystem (Ripple Network) besteht aus einem Peer-to-Peer-Netzwerk von Servern, die den als Blockchain organisierten Ledger verwalten und sich über den Ripple Protocol Consensus Algorithm abstimmen [19, 20]. Ripple Connect stellt Module bereit, mittels derer die Finanzdienstleistungsunternehmen den Zugang zum Ripple Network erhalten, um Transaktionen über das Netz auszuführen. Über Ripple Stream werden weitere Dienstleister angebunden, die als Market Maker z.B. für den Währungstausch bei internationalen Transaktionen sorgen. Derzeit ist das System fokussiert auf Finanztransaktionen im Zahlungsverkehr und Wertpapierbereich. Ein wichtiger Kunde in Deutschland ist die Fidor-Bank. Ripple bietet damit nicht nur Infrastruktur, sondern auch darüber hinausgehende Leistungen.

Im Segment "Middleware und Services" werden Lösungen angeboten, mit denen aufbauend auf das entsprechende Blockchain-Konzept Anwendungen erstellt und ausgeführt werden können. Hierzu gehören die Anbieter von Entwicklungs- und Ablaufplattformen sowie von APIs, die vereinfachte bzw. auf bestimmte Anwendungsbereiche spezialisierte Schnittstellen zum Zugriff auf die Infrastrukturebene bieten. Daneben finden sich hier auch Service-Anbieter, die Dienstleistungen für spezielle Anwendungsbereiche zur Verfügung stellen und beispielsweise im Bereich der Wertpapierabwicklung Clearing- und Settlement-Funktionen mit Schnittstellen in die traditionelle Welt (z.B. Digital Asset Holdings [21]) oder mit automatisierten Finanzkontrakten (z.B. Clearmatics [22]) anbieten.

Ein bemerkenswerter Vertreter bei den Entwicklungs- und Ablaufplattformen ist Ethereum [23]. Es handelt sich hierbei um ein Crowdfunding-finanziertes Open-Source-Projekt, das eine Blockchain-Plattform mit einer eingebetteten Programmiersprache bietet. Ethereum nutzt dabei eine eigene Blockchain mit einem eigens entwickelten Konsensprotokoll. Damit können Teile von Ethereum auch dem Infrastruktur- und Basisprotokollsegment zugeordnet werden. Auf Basis der integrierten Programmiersprache kann eine Vielzahl an möglichen Anwendungen entwickelt werden [24]. Im Vordergrund stehen dabei Lösungen mit Smart Contracts sowie dezentrale Anwendungen. Einige der derzeit in der Entwicklung befindlichen Anwendungen setzen auf Ethereum auf, wie z.B. das zuvor genannte ADEPT.

Zum Segment "Anwendungen" gehören schließlich Blockchain-basierte Technologien, die von Privatpersonen und Firmen i.S. eines Endverbrauchers genutzt werden können. Hierzu zählen Zahlungs-, Verzeichnis-, Notariats-, Investment-, Brokerage-, Informationsdienste etc.

Fazit

Die Entwicklung im Bereich der Blockchain-Technologien und -Anwendungen ist derzeit in vollem Gang. Nachdem sich zu Beginn vor allem Start-ups in diesem Bereich engagiert haben, erkennen zunehmend auch etablierte Unternehmen das Potential dieser Technologie und beginnen mit Investitionen und Projekten. Die Potentiale und der Reifegrad der Technologie sowie die Anzahl der Projekte sind ein Hinweise darauf, dass Blockchain-basierte Systeme eine wichtige Bedeutung in der Zukunft erlangen können.

Sollten sich die Blockchain-Technologien durchsetzen, hätte dies vor allem auf die Bankenlandschaft massive Auswirkungen. Neben disruptiven Veränderungen der Infrastrukturen in sowie zwischen den Banken, wären vor allem auch viele der Intermediäre, die heute noch für die Ausführung der Finanzprozesse notwendig sind, in ihrer Existenz bedroht. Ähnliche Beispiele hat es bereits mehrfach im Zuge der Entwicklung der digitalen Technologien in anderen Bereichen gegeben.

Ob und vor allem wann sich die Blockchain-Technologien durchsetzen werden, lässt sich derzeit noch nicht beurteilen. Einerseits fehlt noch die Killerapplikation, die der Blockchain-Technologie zum Durchbruch verhilft, und andererseits sind noch einige Fragen offen. Insbesondere aufgrund der Verteiltheit bestehen neue Ansprüche an Sicherheits- und Notfallkonzepte. Auf die Sicherheit der Protokolle alleine zu vertrauen, kann kein gangbarer Weg sein, da nie ausgeschlossen werden kann, dass im Laufe der Zeit Schwachstellen gefunden werden oder diese durch die Entwicklung neuer Technologien entstehen, wie z.B. den Quantencomputern im Kryptobereich. Im Finanzbereich werden zudem die Reaktionen der Gesetzgeber und Regulatoren eine wichtige Rolle spielen.

Literatur

[1] http://coloredcoins.org

[2] http://factom.org

[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] http://www.everledger.io

[5] http://www.vinumeris.com

[6] Seibel, K. (2015): Blockchain ist die Revolution des Geldverkehrs, http://www.welt.de/147906848

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

[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] Wild, J.; Arnold, M.; Stafford, P. (2015): Das Rennen um die Blockchain, http://www.capital.de/investment/das-rennen-um-die-blockchain.html

[10] Mougayar, W. (2015): Update to the Global Landscape of Blockchain Companies in Financial Services, http://startupmanagement.org/2015/12/08/update-to-the-global-landscape-of-blockchain-companies-in-financial-services

[11] IBM (2015): Empowering the edge, http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03662usen/GBE03662USEN.PDF

[12] Goel, A. (2015): Bank-Wise Analysis of Blockchain Activity, http://letstalkpayments.com/bank-wise-analysis-of-blockchain-activity

[13] Goel, A. (2015): Financial Institutions: Blockchain Activity Analysis, http://letstalkpayments.com/financial-institutions-blockchain-activity-analysis

[14] http://r3cev.com/newsroom

[15] Eyers, J. (2015): R3 CEV says global bank blockchain should be operating within a year, http://www.smh.com.au/business/banking-and-finance/r3-cev-says-global-bank-blockchain-should-be-operating-within-a-year-20151206-glgyvv.html

[16] 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

[17] Greenspan, G. (2015): MultiChain Private Blockchain, http://www.multichain.com/white-paper

[18] http://ripple.com/technology

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

[20] Cohen, D.; Schwartz, D.; Britto, A. (2015): The Ripple Ledger Consensus Process, http://ripple.com/knowledge_center/the-ripple-ledger-consensus-process

[21] http://digitalasset.com

[22] http://clearmatics.com

[23] http://www.ethereum.org

[24] Karapetsas, L. (2015): A Next-Generation Smart Contract and Decentralized Application Platform, http://github.com/ethereum/wiki/wiki/White-Paper