Financial Services aktuell

Banken, Fonds, Versicherungen

pwc

Ausgabe 97, November/Dezember 2016

Hype oder Realität – die Blockchain

Studien haben gezeigt, dass Verschwörungen mit mehr als fünf Teilnehmern zum Scheitern verurteilt sind, da zu viele unterschiedliche Interessen aufeinandertreffen und zu viele Mitwisser die Wahrscheinlichkeit des Verrates erhöhen. Daher liegt es nahe, Informationen, von denen man nicht will, dass sie missbräuchlich verwendet werden, mit möglichst vielen Personen zu teilen, sodass es keiner Gruppe möglich ist sie zu manipulieren.

Dies ist die Grundidee von Blockchain, einer der bedeutenden Innovationen unserer Zeit. Die Anwendungsbereiche sind in der Theorie unendlich vielfältig – praktisch umgesetzt sind erst wenige. Dieser Newsletter setzt sich mit der historischen Entwicklung der Blockchain, den aktuellen Anwendungsbereichen sowie möglicher zukünftiger Lösungsansätze auseinander.

Das Mysterium „Blockchain“

Eine Blockchain kann man sich wie eine endlos lange Papierrolle in einer Kassa vorstellen – jede Aktivität erzeugt eine neue Zeile auf dem Papier, wobei keine Zeile gelöscht werden kann ohne die Rolle zu zerstören. In der Blockchain werden die Informationen zusätzlich noch in verschiedenen Kassen identisch mitgeführt, was es faktisch unmöglich macht, die bereits existierenden Informationen zu verändern und somit zu manipulieren.

Die Blockchain ist eine Technologie die es ermöglicht, ein öffentliches Register zu erstellen. In diesem Register sind alle Transaktionen der Teilnehmer gespeichert. Der Name Blockchain ergibt sich aus den zwei Komponenten „Block“ und „Chain“. Eine Gruppe von Transaktionen stellt einen „Block“ dar. Dieser „Block“ wird in der „Chain“ in einer linearen

Auf einen Blick

- Die Blockchain hat bis dato erst vereinzelt Marktreife gezeigt – wo sie zum Einsatz kommt sind die Ergebnisse allerdings beeindruckend und bieten teilweise vollkommen neue Geschäftsfelder.
- Jede internationale Großbank experimentiert mit Blockchain; einige Anwendungsbeispiele sind bereits marktreif und sehr erfolgreich.
- Über eine Milliarde Euro Investments in Blockchain Startups seit 2014.
- Bitcoin hat eine Marktkapitalisierung von über 10 Milliarden USD.
- Banken erwarten potentielle Kosteneinsparungen von mehr als 15 Milliarden USD bis 2022 durch die Blockchain Technologie.

Struktur hinterlegt. Jedes Mal wenn ein neuer „Block“ in die „Chain“ integriert wird, wird eine Referenz zu dem letzten „Block“ in der „Chain“ erstellt.

Die Blockchain ist ein öffentliches Register. Aber wo werden die Daten gespeichert und wie übertragen? Die Blockchain ist eine verteilte Technologie bei der sich die Informationen nicht an einer zentralen Stelle befinden sondern von Teilnehmern, welche das Netzwerk zu Verfügung stellen, verwaltet werden.

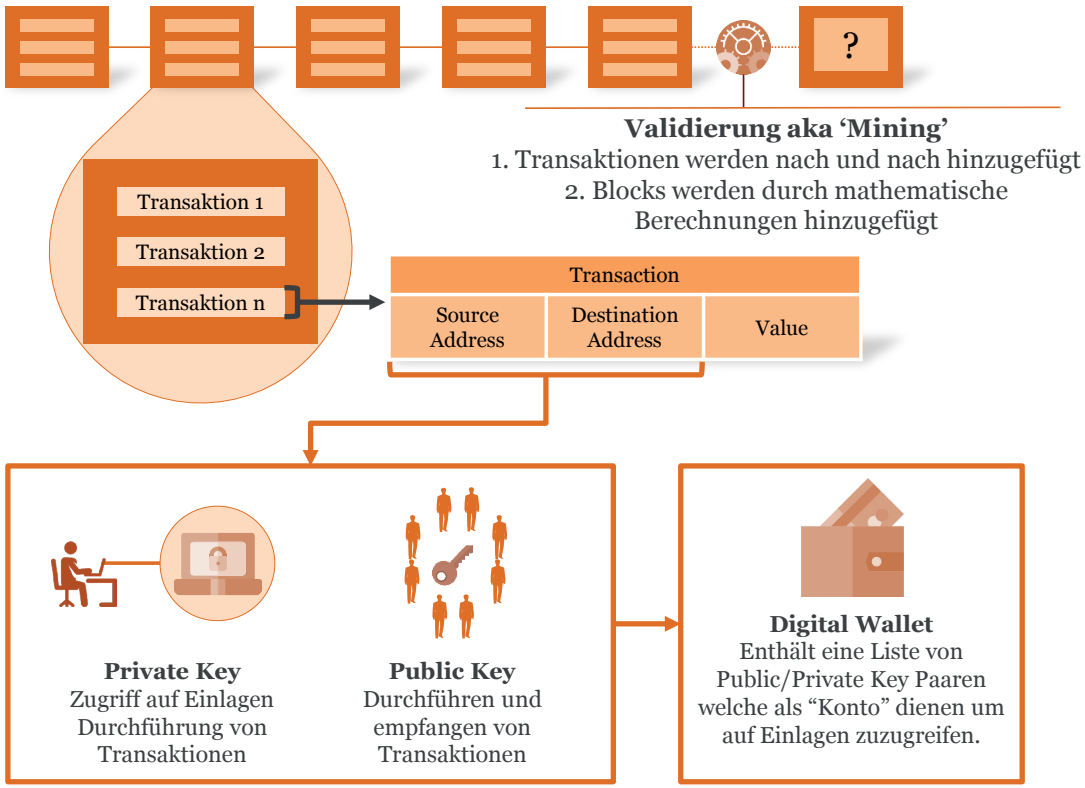
Das bedeutet, dass jeder Teilnehmer (auch Node genannt) des Netzwerkes eine Kopie der kompletten Dokumentation hat. Sobald sich ein neuer Node dem Netzwerk anschließt wird dieser mit dem Netzwerk synchronisiert.
Das bedeutet, dass die Ausfallswahrscheinlichkeit des Netzwerkes lediglich theoretischer Natur ist. Neben den Nodes gibt es auch noch Miners. Diese verfügen über die Hardware um Transaktionen zu sammeln und diese in einen Block zu aggregieren. Ein Block enthält vier Arten von Informationen:

1. Eine Referenz zu dem vorherigen Block
2. Eine Übersicht der enthaltenen Transaktionen
3. Einen Zeitstempel
4. Nachweis über die Erstellung des sicheren Blocks

Blocks benötigen vielfältige unabhängige Validierungen und die Berechnungen dienen dazu, die Sicherheit zu erhöhen und die Manipulierbarkeit zu erschweren. Sobald ein Block in der Blockchain ist, befindet er sich für immer dort.

Der Nachweis zur Erstellung eines Blocks ist eine komplex berechnete Zahl. Durch die Kombination aus all diesen Eigenschaften können die Blocks in einer Chain verknüpft werden und sind zu jedem Zeitpunkt als Gesamtes valide.
Durch die konstante Überprüfung der Blockchain und Transaktionsvalidierung ist das komplette Netzwerk ein sich selbst regulierendes und sicheres System.

Abbildung 1: Blockchain – Ein ständig wachsendes Hauptbuch aller Transaktionen



Miners erhalten für das zu Verfügung stellen der Rechnerkapazitäten (diese wird für die Berechnungen wie oben beschrieben benötigt) z.B. Bitcoins. Mining ist die gebräuchlichste Art wie „neue“ Assets in einer Blockchain generiert werden können und stellt eine Begrenzung der Vermehrung der Netzwerkwährung dar, da die Anzahl der Assets von Beginn an limitiert wird. Am Beginn einer Blockchain ist somit festgelegt wie viele Assets (z.B.: Bitcoins) es maximal in der Blockchain geben wird.

Die Transaktionen innerhalb des Netzwerkes sind somit:

1. Transparent (jeder Teilnehmer hat je nach Ausgestaltung Einsicht auf alle/nur relevante Transaktionen)
2. Unveränderlich (jeder Teilnehmer hat eine Kopie des Registers)
3. Nachvollziehbar (der Fluss kann ab dem Moment der Erstellung verfolgt werden).

Transaktionen in der Blockchain werden von Usern durchgeführt welche die Blockchain nutzen. Dazu später mehr.

Aktuelle Anwendungsbereiche

Die wohl bekannteste Anwendung der Blockchain stellt heute „Bitcoins“ dar. Eine von Satoshi Nakamoto im Jahre 2008 erdachte Krypto-Währung (synthetisch erzeugte Währung) deren Wert sich aus den für ihre Erzeugung und Aufrechterhaltung notwendigen Kosten errechnet. Der Preis der Währung ergibt sich – klassisch marktwirtschaftlich – aus dem Zusammenspiel von Angebot und Nachfrage. Während sich der Wert auf Basis klar definierter Algorithmen entwickelt, unterliegt der Preis deutlichen spekulativen Schwankungen, was in der breiten Öffentlichkeit den Eindruck von Unsicherheit erzeugt.

Transaktionen in der Blockchain stellen Übertragungen von Besitzrechten an virtuellen Gütern (z.B.: Bitcoins) zwischen zwei Parteien dar. Der aktuelle Kontostand kann über ein „Wallet“ eingesehen werden. Ein Wallet ist wie ein virtuelles Bankkonto in dem angezeigt wird was/wie viel der Benutzer besitzt. Zum Beispiel in der Bitcoin Blockchain wird der Wert als Bitcoin angegeben. In anderen Blockchains kann ein anderes Asset verwendet und auch in einem Wallet dargestellt werden.

Um ein Wallet anlegen zu können braucht der Benutzer ein „Crypto Key Pair“. Dieses besteht aus einem Public und eine Private Key. Ein solcher Key sind kryptographisch generierte hashes (im Wesentlichen lange Nummern-/Buchstabenkombinationen). Wie die Bezeichnungen schon verraten, ist ein Public Key öffentlich einsehbar, wohingegen ein Private Key nur dem Nutzer bekannt ist. Der öffentliche Key dient sozusagen als Kontonummer für Transaktionen von Dritten und der Autorisierung von Transaktionen. Public und Private Key sind mathematisch miteinander verbunden. Durch die Erstellung eines Wallets wird der Private Key des Users generiert. Ein Wallet ist nur mithilfe des Private Keys einsehbar. Sollte also ein Nutzer diesen verlieren, ist sein Guthaben unwiederbringlich verloren.

Beispiel: Vergleich Grundbucheintragung heute vs. Grundbucheintragung in einer Blockchain Welt

Grundbucheintragung heute

Ihr Nachbar entscheidet sich sein Haus zu verkaufen. Er inseriert das Haus und findet einen Käufer, der das Haus kaufen möchte. Der Verkäufer sucht einen Rechtsanwalt auf, welcher einen Vertrag aufsetzt. Danach wird ein Notar hinzugezogen, der ein Treuhandkonto bei einer Bank öffnet. Der Käufer überweist das Geld auf das Treuhandkonto, damit Ihr Nachbar sicher sein kann, dass das Geld vorhanden ist. Das Haus wechselt den Besitzer – die Grundbucheintragung findet statt. Sobald Ihr Nachbar das Haus an den Käufer überschrieben hat wird das Geld am Treuhandkonto vom Notar freigegeben und auf das Konto ihres Nachbarn überwiesen. Der Besitzer ist nun offiziell der Käufer.

Grundbucheintragung in einer Blockchain Welt

Nehmen wir an das Grundbuch hat als Basis eine Blockchain (so wie es gerade in Schweden und Honduras erprobt wird). Ihr Nachbar hat in diesem Fall auch einen Käufer gefunden. Ein für Hausverkäufe standardisierter Smart Contract (der z.B. von staatlicher Stelle herausgegeben wird) wird von beiden Parteien als geeignet angesehen. Im selben Moment, in dem beide Parteien dem Vertrag zustimmen, wird automatisiert und in Echtzeit überprüft ob eine Kontodeckung besteht und - sollte dies der Fall sein - das Geld sofort an Ihren Nachbarn transferiert. Der Eintrag im Grundbuch wurde im selben Moment vollautomatisiert angepasst. Ihr Nachbar hat sich die Kosten für einen Anwalt, einen Notar und ein Treuhandkonto gespart.

Weitere Anwendungsbereiche

Stellen Sie sich einen Geldschein vor. Der Geldschein bekommt bei seiner Erstellung eine Seriennummer durch welche ersichtlich ist, in welcher Druckerei der Schein gedruckt worden ist. Der Schein zirkuliert und verschleißt, bis er schlussendlich wieder bei einer Nationalbank landet und ausgetauscht wird. Der Nationalbank ist bewusst, wo dieser Schein produziert worden ist, aber ansonsten ist ihr der Weg des Geldes zumindest teilweise nicht bekannt. In einer Blockchain Welt weiß die „Nationalbank*“ jederzeit wo sich der „Schein“ befindet. Eine Spur durch jede einzelne Transaktion wird gelegt. Aber in einer Blockchain ist nicht nur der „Nationalbank“ bewusst wo sich das Geld befindet, sondern auch jedem einzelnen Teilnehmer des Netzwerkes. Jeder, der sich dem Netzwerk anschließt, hat eine Kopie aller Transaktionen, die innerhalb dessen getätigt worden sind.

Hier stellt sich natürlich die Frage warum irgendjemand möchte, dass jede einzelne Geldbewegung jeder anderen Person zugänglich und somit einsehbar ist. Dies wird durch eine andere Eigenschaft der Blockchain umgangen: Grundsätzlich ist jeder Teilnehmer anonym. Wir erreichen sozusagen einen Status, in dem nicht bekannt ist wer welches Geld besitzt, sondern nur wie sich das Geld bewegt. Aber auch die Blockchain verspricht keine 100%ige Sicherheit. Kein System oder Modell kann das. Das Versprechen der Blockchain ist allerdings die Sicherheit im Vergleich zu heutigen Systemen zu erhöhen.

Mehrwert für Endverbraucher

Den größten Mehrwert einer Blockchain ist, dass das Netzwerk als Treuhänder fungiert. Dadurch, dass jeder Teilnehmer eine Kopie sämtlicher Transaktionen hat, muss kein Dritter bestätigen, dass diese Transaktion stattgefunden hat (siehe Grundbuchbeispiel). Ausgaben für etwaige Treuhandfunktionen lassen sich auf ein Minimum reduzieren.

Der Einsatz von Public/Private Keys macht die Verwendung von Blockchain-basierten Anwendungen sicher. Mithilfe eines Layer, der auf der Blockchain aufbaut, können standardisierte Smart-Contracts erstellt werden, die automatisiert Aufgaben durchführen, für die bis heute manuelle Eingriffe notwendig sind. Smart Contracts stellen ein Regelwerk dar, welches auf Basis der Blockchain bei definierten und eintretenden Ereignissen Funktionen auslöst.

Mehrwert für Financial Services

Der erste Einsatz der Technologie und momentan die wichtigste marktreife Anwendungsmöglichkeit sind peer-to-peer Transaktionsplattformen wie zum Beispiel Bitcoin, Ripple oder SETL. Auch NASDAQ hat Blockchain-basierte Anwendungen in ihrem Portfolio. NASDAQ Linq ermöglicht ihren Kunden einen fast komplett automatisierten und in Echtzeit durchgeführten Handel von unterschiedlichen Finanzprodukten.

Momentan befinden wir uns in dem Stadium, in dem Smart Contracts mehr und mehr Aufmerksamkeit auf sich ziehen. Am bekanntesten ist wohl das R3Consortium bestehend aus 50 der größten Banken weltweit. Diese Institutionen haben mit der R3 Corda ein standardisiertes Hauptbuch speziell für Financial Services bereitgestellt, welches sehr stark der Blockchain ähnelt. Auf deren Basis können verschiedenste, untereinander kompatible Anwendungen entwickelt werden. Die Besonderheit von R3 Corda ist, dass die Daten nur an die involvierten Parteien (z.B. zwei Banken, Nationalbank/EZB und Aufsicht) anstatt an alle Netzwerkteilnehmer weitergegeben werden. Im Sommer 2016 haben außerdem Santander, UBS, BNY Mellon, ICAP und Deutsche Bank die USC (Utility Settlement Coins) angekündigt um in Zukunft Währungstransaktionen und das Clearing schneller und billiger durchführen zu können.

Es ist wichtig zu erwähnen, dass Smart Contracts nicht unbedingt die Blockchain verwenden müssen. Nichtsdestotrotz scheint die Kombination aus Blockchain und Smart Contracts die aktuell attraktivste zu sein. Vorreiter auf dem Gebiet der Smart Contracts ist momentan die unabhängige Plattform Ethereum. Während der letzten Monate sind einige Schwachstellen innerhalb des Ethereum-Netzwerkes bekannt geworden, sowohl Angriffe von außen als auch Manipulationen innerhalb des Netzwerkes. Die These dass eine kommerzielle Verwendung noch nicht möglich ist wurde somit mehrfach bestätigt.

Trotz der aktuellen Schwierigkeiten kann festgehalten werden, dass so gut wie jede internationale Großbank derzeit Piloten und Tests im Bereich Blockchain/Smart Contracts durchführt.

Wie geht PwC mit dem Thema um?
Innerhalb des PwC Netzwerkes wurden mehrere Teams weltweit aufgebaut, die sich mit den potentiellen Anwendungen der Blockchain Technologie beschäftigen.

Wir bieten eine breite Palette an verschiedensten Dienstleistungen in Zusammenhang mit Technologie und der Blockchain im Speziellen an, die auf Ihre spezifische Situation eingehen:

1. Analyse Ihrer bestehenden Geschäftsmodelle und Prüfung auf potentiellen Einsatz einer Blockchain in bestimmten Bereichen Ihrer Organisation.
2. Mithilfe unserer Denovo Lösung (globale Referenzliste mit diversen Startups aus dem Technologiebereich) bieten wir eine gesamtheitliche Analyse des Blockchain Marktes, die Ihnen mögliche Übernahme/-Kooperationspartner aufzeigen kann.
3. Erstellung von Markteintrittsstrategien, Definition der Zielgruppe und Entwicklung verschiedenster Preismodelle.
4. Überprüfung wie der Einsatz von Blockchain Technologie Ihr operationales Risiko beeinträchtigen kann und welche regulatorischen Probleme entstehen können.
5. Entwicklung eines ganzheitlichen Geschäftsmodells mit Organisationsdefinition, Wirkungsanalyse, Geschäftsprozesserstellung und funktioneller / technischer Architektur.
6. Unterstützung während der Entwicklung und Einführung Ihrer Blockchain Lösung.

Gerne unterstützen Sie unsere Experten auf diesem spannenden Weg!

Zu den Autoren

Günther Seyer
Senior Manager, Technology Consulting
guenther.seyer@at.pwc.com

Günther Seyer ist Senior Manager bei PwC im Team Financial Services Consulting. Vor seiner Zeit bei PwC war er bei einer internationalen Bankengruppe und anderen Beratungsunternehmen tätig. Er ist auf den Bereich Strategie und IT Effectiveness spezialisiert.

Simon Samy El-Dib
Senior Manager, Technology Consulting
simon.samy.el.dib@at.pwc.com

Ihre Ansprechpartner

Dieter Harreither
Partner
Technology Consulting
+43 1 501 88-1110
dieter.harreither@at.pwc.com

Günther Seyer
Senior Manager
Technology Consulting
+43 1 501 88-5118
guenther.seyer@at.pwc.com

Simon Samy El-Dib
Senior Manager
Technology Consulting
+43 1 501 88-1173
simon.samy.el.dib@at.pwc.com

PwC Wien
Erdbergstraße 200, 1030 Wien
www.pwc.at

In der nächsten Ausgabe

Besteuerung von Bonuszahlungen für Bankenmanager – ein Länderüberblick

Bis Ende Dezember 2013 waren die Mitgliedstaaten der Europäischen Union verpflichtet, die Richtlinie 2013/36/EU in nationales Recht umzusetzen. Ziel dieser Richtlinie war es, die Bonuszahlungen an Bankenmanager zu begrenzen und so deren Risikobereitschaft einzudämmen.
Die nächste Ausgabe unseres Newsletter Financial Services aktuell gibt einen Überblick über die Unterschiede bei der Besteuerung der Vergütungen und Gehälter in ausgewählten Mitgliedstaaten.

Medieninhaber und Herausgeber: PwC Österreich GmbH Wirtschaftsprüfungsgesellschaft, Erdbergstraße 200, 1030 Wien

Für den Inhalt verantwortlich: StB Mag. Thomas Strobach, thomas.strobach@at.pwc.com

Für Änderungen der Zustellung verantwortlich: Tatjana Wallner, tatjana.wallner@at.pwc.com, Tel.: +43 1 501 88-3308, Fax: +43 1 501 88-73308