

Autoren:

Matthias Niklowitz, Matthias.Niklowitz@swisscom.com

Johs Höhener, Johannes.Hoehener@swisscom.com

11.02.2016

Grundlagen der Blockchain-Technologie

Sachverhalt

Die Blockchain-Technologie gilt bei Grossbanken und Börsenbetreibern als möglicher Game-Changer mit grossen Konsequenzen für die IT und die Geschäftsmodelle. Banken wie Goldman Sachs und Bank of America haben dazu je rund 20 Patente eingereicht, weil sie sich durch eine rasche Einführung proprietärer Anwendungsfälle einen grossen kompetitiven Vorteil (Kosten und Dauer der Prozesse) versprechen. Die Phase der ersten Proof-of-Concepts und Versuche ist Ende 2015 durch eine Phase erster kleiner produktiver Applikationen abgelöst worden. Für das laufende Jahr haben Banken und Börsenbetreiber kommerzielle Starts von wichtigen Applikationen auf der Basis von Blockchain-Technologien angekündigt. Im vorliegenden Report beschreiben wir kurz die Funktionsweise, die populärsten Anwendungsmöglichkeiten und erläutern das Potenzial.

Konsequenz

Die Weiterentwicklungen bei Blockchain-Technologien erfolgen sehr schnell und von der breiten Öffentlichkeit weitgehend unbemerkt. Banken kommen deshalb nicht umhin:

- > Den Aufbau interner Expertise auf Stufe GL und IT voranzutreiben;
- > Sich mit möglichen Partner-Banken zum Thema und den relevanten Entwicklungen regelmässig auszutauschen und Kooperationen zu diskutieren;
- > Rasch ein, zwei erste Leuchtturm-Projekte vorzubereiten, auch um erste Erfahrungen zu sammeln;
- > Und bei der Entwicklung der eigenen längerfristigen Business-Strategie immer auch die Umstellungen bzw. Implikationen der Blockchain-Technologie berücksichtigen.

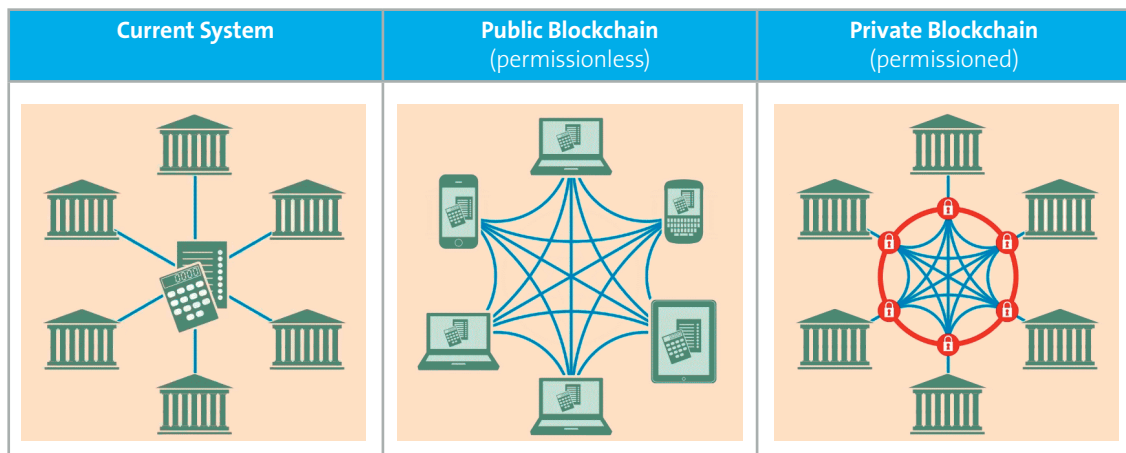
Fragen und Antworten zum Thema Blockchain

Die Blockchain-Technologie hat es auf die Titelseiten und in die Wirtschaftsressorts der Massenmedien gebracht. Auch am World Economic Forum in Davos dominierte das Thema in vielen Diskussionen und Panels Executives von Banken.

Die Blockchain-Technologie könnte die Finanzwelt in den kommenden 10 bis 20 Jahre ebenso nachhaltig umwälzen wie das IP-Protokoll in den 1990er Jahren, der den Weg zu den modernen Internet-Anwendungen, wie wir sie heute kennen, freigemacht hatte. Ein Indiz, wie ernst Banken diese Entwicklung nehmen, ist die Tatsache, dass sowohl Goldman Sachs als auch Bank of America ihre eigenen Entwicklungen mit jeweils mehr als 20 Patentanträgen zu schützen versuchen. Das US-Patentbüro veröffentlicht bewilligte Patente 18 Monate nach Einreichung. Diese beiden Banken hatten demnach ihre Anträge bereits im Sommer 2014 eingereicht.

Allerdings gibt es in den Diskussionen immer wieder offene Fragen zur Funktionsweise und zu den konkreten Auswirkungen. Die folgenden Fragen und Antworten sind als ein einfaches Tool konzipiert, mit dem man Strategie-Diskussionen zu diesem Thema sicher führen kann.

Was versteht man unter Blockchain?



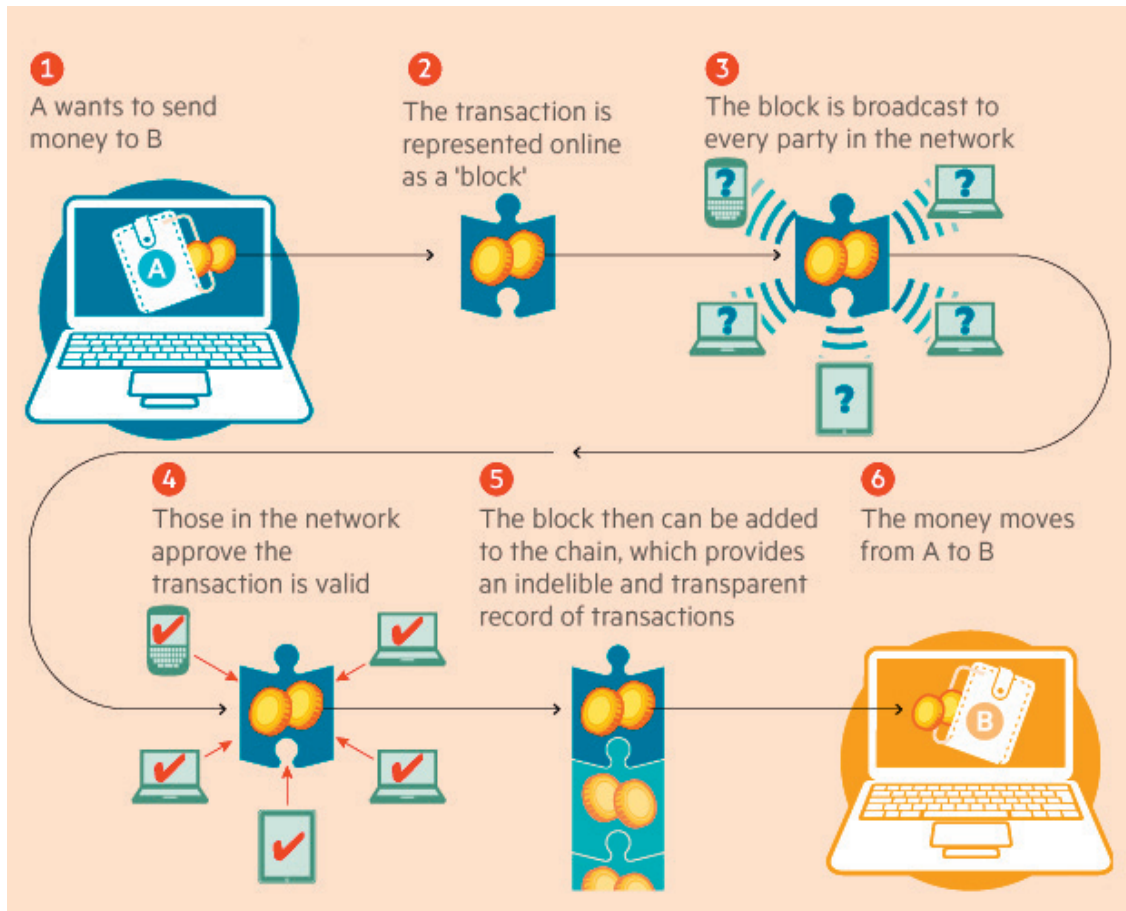
Grafik 1: Vergleich von unterschiedlichen Interbanken-Netztypen
(Quelle: Models of Blockchain Organization esp. for financial transactions (c) Financial Times)

Die Blockchain (wörtlich: «Block-Kette») ist eine dezentral verwaltete Datenbank. In ihr werden Geldeinheiten, Finanzanlagen (Aktien, Bonds, Derivate), Besitzrechte (z.B. Autoregister, Grundbucheinträge) oder Grundrechte (Immobilien) dezentral verwaltet.

Zentral sind drei Prinzipien, mit denen verhindert wird, dass dezentral verwaltete Assets zwei- oder mehrfach verwendet werden können:

- > **Dezentral:** Die nach oben offen konzipierten Datenbanken, bei der jeweils die Transaktionen einzeln nachgeführt werden, sind auf Servern dezentral verteilt. Die Datenbanken sind untereinander via Internet und ein eigenes Blockchain-Protokoll verbunden.
- > **Verschlüsselung:** Besitzer von Geldeinheiten, Anlagen oder Rechten haben ein eigenes digitales Wallet mit einem privaten digitalen Key. Der Public Key ist auf der Blockchain. Transaktionen können nur in Zusammenwirken von privatem und öffentlichem Key vorgenommen werden, wenn alle Bedingungen (Besitzrechte, Verfügbarkeit von Geld usw.) geklärt sind.
- > **Konsens-Prinzip:** Eine 51-Prozent-Mehrheit der dezentralen Datenbanken ist für den Abschluss einer Transaktion zwingend erforderlich.

Wie funktionieren Transaktionen via Blockchain?



Grafik 2: Ablauf einer Zahlungs-Transaktion via Blockchain (Quelle: Financial Times)









Eine Transaktion (oben am Beispiel eines Geld-Transfers) wird bei der Blockchain ausgelöst, indem ein Käufer einem Verkäufer mithilfe des eigenen digitalen Wallet eine Geldsumme oder ein anderes Besitzrecht überweist. Mit dem Auslösen der Transaktion wird ein Prozess gestartet, bei dem überprüft wird, ob der Sender das Geld bzw. die Assets in seinem digitalen Wallet/Depot/Konto hat. Dann werden die Assets dem Empfänger gut geschrieben. In einem dritten Schritt wird das allen anderen dezentralen Datenbanken «mitgeteilt» (das ist der Grund, warum solche Transaktionen zwischen 10 Sekunden und einigen Minuten dauern). In einem vierten Schritt (hinter den Kulissen) tauschen sich die dezentralen Datenbanken jeweils über den neuesten Stand aus – ein weiterer «Block», der einige tausend Transaktionen umfasst, ist dann «vollgeschrieben» (Schritt fünf). Der sechste Schritt bildet den Abschluss der Transaktion. Prinzipiell funktionieren eine Aktien-Transaktion oder eine Immobilien-Transaktion genau mit den gleichen Schritten.

Das Onboarding bei Blockchain-basierten Applikationen (wie beispielsweise einem P2P-Payment-System) erfolgt via digitaler Konto-Eröffnung. Ein User legt sich – unter Benutzung der entsprechenden App, ein neues Wallet/Konto/Depot an. Je nach Bank und Regulierung sind weitere Schritte erforderlich, analog dem heutigen Stand des digitalen/ nicht digitalen Onboardings.

Das oben skizzierte Prinzip der Transaktionen hat folgende positive Aspekte:

- Die dezentral vorgenommenen und gespeicherten Transaktionen machen das System sehr robust in Hinsicht auf Fälschungen/Manipulationen.
- Alle Transaktionen lassen sich einzeln nachverfolgen. Aus Sicht der Regulation ist das sehr erwünscht (AML usw.).
- Teure zentrale Instanzen sind nicht mehr erforderlich. Das hat positive Effekte auf die Gesamtkosten (Opex-Schätzungen e-foresight: minus 10 bis minus 50 Prozent; Autonomous Research rechnet mit einem Einsparpotenzial von 30 Prozent bei den Kosten für Clearing und Settlement im globalen Aktienhandel).

Was sind die populärsten Blockchain basierten Anwendungsmöglichkeiten?

Use Cases	Beschreibung	Status
 BC as a Service	Bitpay provides Bitcoin payment processing and local currency payouts to over 65,000 businesses worldwide, are now using Microsoft Azure Blockchain as a service offer.	Offering
 Luxury Goods	Immutable ledger for diamond ownership & related transaction history verification using the bitcoin blockchain and Eris as a platform for provenance and combating insurance fraud	Pilot
 Nasdaq	Nasdaq's blockchain technology offers efficient fully electronic services that facilitate the issuance, transfer, and management of private company securities.	Pilot
 Land title registry	A proof of concept for land title registry. The land registry tool will use bitcoin's distributed ledger, the blockchain, to prevent the counterfeiting, forgery and corruption surrounding land titles in the developing world	Pilot
 Identity	A mobile ID using the bitcoin blockchain. ID can be verified easily in e-commerce, for credit card payments, banks and insurance incidents. It prevents fraud and is highly secure.	Proof-of-Concept
 Finance Industry	Consensus based protocol designed specifically for existing financial institutions, supplementing existing processes & directly supporting fiat currencies. Lead use cases are international payments & inter financial institution settlement.	Proof-of-Concept
 Health-care	A platform that decentralizes healthcare data stored on bitcoin blockchain gives patient's full control over their healthcare information while ensuring secure access and storage.	Concept
 IoT platform	IoT platform ADEPT serves as a ledger of existence for billions of devices that autonomously broadcast transactions between peers, it serves as a bridge between many devices at low cost.	Concept

Grafik 3: Use-Cases von Blockchain-Applikationen

Die obenstehende Grafik zeigt acht aktuelle populäre Use-Cases für Blockchain-Anwendungen auf. Die Anwendungen variieren nach dem Reifegrad. Weitere neue Anwendungen, die hier nicht aufgeführt sind, stehen kurz vor dem kommerziellen Start (beispielsweise die globale Asset-Handelsplattform von Lykke) bzw. im fortgeschrittenen Pilot-Stadium (das seit November 2015 in der Pilotphase befindliche Mobile Banking/Payment der tunesischen Post basierend auf einer Plattform von Monet.net). In Honduras testet die Firma Digital Asset Holding ein Grundbuchregister auf Blockchain-Basis. Nicht erwähnt ist oben die bisher mit Abstand grösste Anwendung: Die (umstrittene) Kryptowährung Bitcoin läuft bereits seit Anfang 2009.