April
2018

AWK GROUP
Consulting
Engineering
Project Management

# AWK WISSEN

# So funktioniert die Blockchain

**Angepriesen als die grösste Revolution seit der Erfindung des Internets soll unsere Gesellschaft dank Blockchain komplett neu organisiert werden. Im folgenden Artikel erläutern wir die in Blockchain enthaltene Philosophie und Technologie, und skizzieren einige Anwendungsbeispiele aus verschiedenen Branchen. Dieser erste Eindruck der technischen und ökonomischen Möglichkeiten von Blockchain soll es Ihnen gestatten, die Auswirkungen auf Ihr Unternehmen abzuschätzen.**

Adrian Anderegg, Lukas Möller, Ulrich Sieker

## Hintergrund

Vor rund zehn Jahren wurde Blockchain mit der Erfindung von Bitcoin bekannt. Kernidee dabei ist, durch einen offenliegenden Mechanismus Vertrauen in ein System sich misstrauender Beteiligter zu schaffen. Blockchain ist jedoch weit mehr als Bitcoin.

Der Begriff *Internet of Value* verdeutlicht das Potenzial der Blockchain. Statt Kopien von Daten per E-Mail, Messaging oder Social Media auszutauschen, können durch die Blockchain Werte wie Geld, Rechte, Stimmen oder Verträge transferiert werden.

Erklären lässt sich eine Blockchain als globale, über eine Vielzahl von Rechnern dezentral verteilte Datenbank (*Distributed Ledger*). Beteiligte können Bewegungen aller Art transparent nachvollziehen; eine zentrale Stelle zur Transaktionsabwicklung (Intermediär, *Middleman* oder *Custodian*) wird obsolet.

Folgende Geschäftsmodelle können unterschieden werden:

- **Zentral gesteuerte Wertschöpfung** ist die klassische Form. Unternehmen, allenfalls via Intermediär, bedienen Kunden einzeln und unabhängig voneinander.
- *New* oder *Shared Economy* fördert **dezentrale Modelle** (z. B. Uber oder Airbnb), in denen Unternehmen Marktteilnehmer direkt miteinander verbinden.
- Blockchain ermöglicht vollständig **netzwerkorientierte Organisationen** ohne Intermediär. Für alle Beteiligten verbindliche Partizipations- oder Vergütungsregeln sind in der Blockchain hinterlegt.

Reine Werttransfers (z. B. Geld, Edelsteine, Kunst) lassen sich in der Blockchain zu *Smart Contracts* erweitern, mit denen verbindliche Abkommen abgeschlossen werden. In *Smart Networks* werden Organisationen ohne zentrale Einheit im Konsens aller Beteiligten gesteuert (sog. *Decentralized Autonomous Organisations*).

## Technik

### Grundlagen

In einer Blockchain werden Daten auf allen am jeweiligen Netzwerk angeschlossenen, aktiven Teilnehmern (*Nodes*) gespeichert. Die einzelnen Daten (auch Transaktionen) werden überdies gesammelt und zu einem Block kombiniert. Jeder einzelne Block wird mit seinem Vorgängerblock verkettet (engl. *chain*), so dass eine klare Datenreihenfolge entsteht.

Um die Datenqualität sicherzustellen und die Datenbank trotz dezentraler Datenhaltung synchron zu halten, bedient sich Blockchain einiger technischer Mechanismen:

- **Authentizität**
  In einer öffentlichen, allen Teilnehmern offenstehenden Blockchain verbinden sich

passive Teilnehmer (*Clients*) mit einem oder mehreren aktiven Teilnehmern (*Nodes*). Um Einträge eindeutig einem Teilnehmer zuzuordnen, verfügt jeder *Client* über einen privaten als auch einen daraus generierten öffentlichen Schlüssel. Indem der *Client* die Daten mit seinem privaten Schlüssel signiert, können die übrigen Teilnehmer mit dem öffentlichen Schlüssel jederzeit die Echtheit der Daten überprüfen. Dieses als asymmetrische Kryptographie bekannte Verfahren wird im sicheren Netzwerkverkehr (z. B. SSH, https/SSL) seit Langem eingesetzt.

- **Integrität**
  Jeder *Node* verfügt über eine gleichberechtigte Datenkopie. Um eine nachträgliche Veränderung gespeicherter Daten zu verhindern, wird der *Hash*-Wert[1] des vorherigen Blocks in den aktuellen integriert. Damit ist die Unveränderbarkeit der Daten gewährleistet (vgl. Abbildung 1).

- **Synchronität**
  Alle *Nodes* in der Blockchain sind gleichberechtigt und können neue Blöcke anhängen. Um eine eindeutige Abfolge der Blöcke sicherzustellen, bedienen sich Blockchain-Implementationen unterschiedlicher **Konsens-Algorithmen**. In öffentlichen Blockchains werden oft Implementationen des *Proof-of-Work*-Mechanismus eingesetzt. Andere Blockchains nutzen den *Proof-of-Stake*-Mechanismus oder Kombinationen verschiedener Algorithmen.

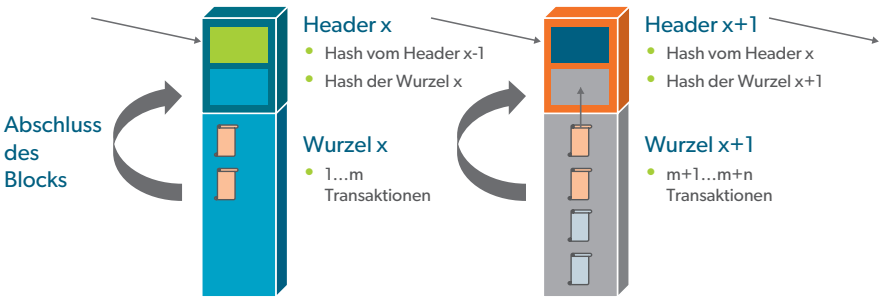


*Abb. 1: Aufbau eines Blocks zur Wahrung der Integrität*

Das Grundprinzip der Algorithmen ist jeweils identisch und wiederholt sich für jeden Block (vgl. Abbildung 2):

1. Jeder *Node* kann eine neue Transaktion an das Netzwerk übermitteln.

2. Zum Abschluss eines Blocks wird im Netzwerk entschieden, welcher *Node* den nächsten Block definiert. Dieser Vorgang hängt vom eingesetzten Konsens-Algorithmus ab und heisst im *Proof-of-Work*-Mechanismus *Mining:* Die *Nodes* müssen eine Zufallszahl errechnen, die bestimmte Bedingungen erfüllt. Bei anderen Algorithmen entscheidet das Zufallsprinzip oder der Block wird von einer zentralen Autorität festgelegt.

3. Der ausgewählte *Node* hängt den neuen Block an die bestehende Kette an und verteilt sie an die übrigen *Nodes*.

Der eingesetzte Konsens-Algorithmus regelt das Sicherheitsniveau und die Verarbeitungsgeschwindigkeit neuer Blöcke. Der für Bitcoin eingesetzte *Proof-of-Work*- Mechanismus hat viele Nachteile und führt zu hohem Stromverbrauch und langen Verarbeitungszeiten. Andere Algorithmen eignen sich nur für Blockchains mit eingeschränktem Zugriff (*private* oder *permissioned* Blockchain). Wie mit reduziertem Aufwand ein ähnliches Sicherheitsniveau erreicht wird, beschäftigt aktuell die Forschung.

## Smart Contracts

*Smart Contracts* sind eine Weiterentwicklung von Blockchain. Dabei werden neben Werten auch kleine Applikationen in der Blockchain gespeichert (vgl. Abbildung 3).

Ein *Smart Contract* wird einmalig erstellt und unveränderbar auf der Blockchain abgelegt. Die durch eine Transaktion angestossene Applikation wird auf allen *Nodes* gleichzeitig ausgeführt. Ein Trigger zur Ausführung der Applikation kann von einem privaten Konto oder einem anderen *Smart Contract* stammen. Für die Ausführung der Applikation ist keine Infrastruktur nötig; die Rechenleistung übernehmen die *Nodes* der Blockchain. So spricht man bei Ethereum von der *Ethereum Virtual*

[1] Eine kryptographische *Hash*-Funktion (auch Streuwertfunktion) bildet einen beliebigen Eingabewert auf einen Zielwert mit fester Länge ab. Die Funktionen sind stets Einwegfunktionen und somit irreversibel: Der Eingabewert ist aus einem gegebenen Zielwert nicht berechenbar. Zudem bilden kollisionsresistente Funktionen niemals zwei Eingabewerte auf denselben Zielwert ab.

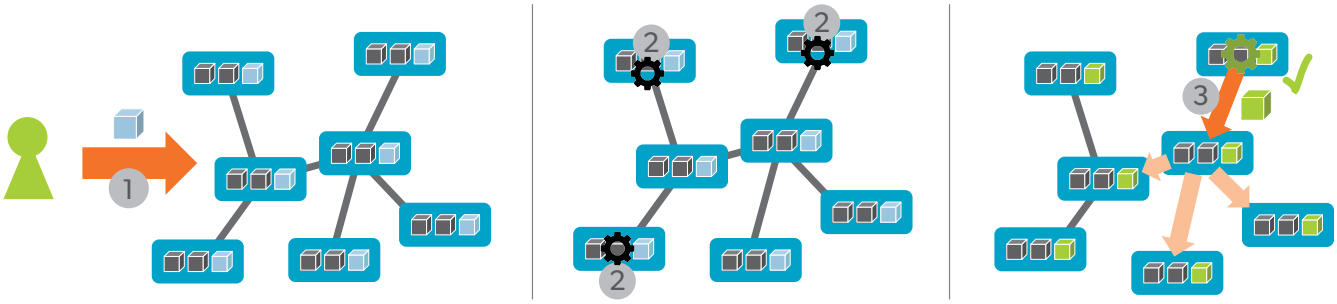


*Abb. 2: Algorithmus zur Konsensfindung über die Regelkonformität neuer Transaktionen*

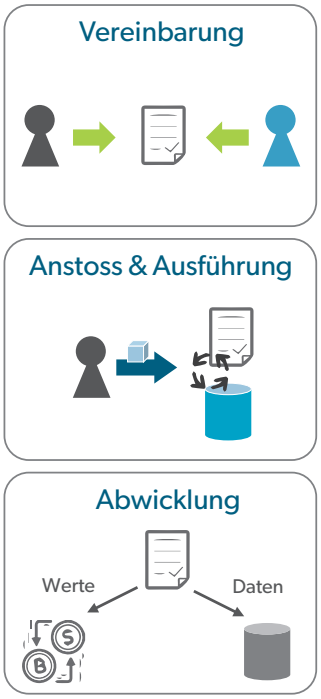


*Abb. 3: Smart Contracts*

*Machine* (EVM), welche die *Smart Contracts* ausführt. Für die Ausführung des Codes wird eine Gebühr verlangt, deren Höhe von der Komplexität der Applikation abhängt und unter den ausführenden *Nodes* aufgeteilt wird.

Mit einem *Smart Contract* kann beispielsweise eine Eigentumsübertragung fix an einen Zahlungseingang gekoppelt werden. Der manuelle Eingriff eines Mittelsmanns entfällt.

### Rechtemanagement auf der Blockchain

Unterschieden werden zwei Implementierungen. Welche Art der Blockchain eingesetzt wird, entscheidet der Anwendungsfall.

- Auf ein ***public* Blockchain**-Netzwerk hat jeder Zugriff. Bekannteste Beispiele sind Ethereum, Lisk oder rootstock. Auch Bitcoin und andere, reine *Smart Currencies* sind öffentlich zugänglich, werden jedoch nur für Transaktionen in den jeweiligen Währungen genutzt. Die Benutzung der Applikation lässt sich über die Implementierung eines Zugriffsmechanismus (sog. ***permissioned* Blockchain**) auf ausgewählte Benutzer und/oder Funktionen einschränken.

- Ein eigenes, ***private* Blockchain**-Netzwerk dürfen nur bekannte und berechtigte Beteiligte einsehen und beschreiben, z. B. im Interbankenhandel mit Ripple. Eine *private* Blockchain ist somit immer *permissioned*, wobei die Teilnehmer gleichberechtigt sind oder unterschiedliche Berechtigungen erhalten. Aufgesetzt werden kann eine *private* Blockchain mit (Open-Source-)Software; am verbreitetsten sind Hyperledger Fabric oder Ethereum als private Installation.

### Anwendungen

Die Blockchain-Technologie mit ihrer verteilten Datenstruktur und der automatisierten Sicherstellung der Authentizität von Information ermöglicht neben Kryptowährungen viele interessante Anwendungen ohne zentrale Autorität. Ausserdem eignet sich die Blockchain zum Teilen und Bearbeiten von Daten zwischen unabhängigen oder sogar konkurrierenden Unternehmen. Von der erzielten Effizienzsteigerung profitieren alle an der Blockchain beteiligten Unternehmen und letztlich der gesamte Markt. Ferner können hochverfügbare, öffentlich erreichbare Applikationen ohne eigenes IT-System publiziert werden.

Im Folgenden verdeutlichen wir das Potenzial der Blockchain an einigen Beispielen aus unterschiedlichen Branchen.

### Nachvollziehbarkeit in der Lieferkette

Erfolgsfaktoren einer effizienten Lieferkette sind Transparenz und das Sicherstellen der vollständigen Rückverfolgbarkeit von Materialien. Eine unveränderbare Blockchain ist prädestiniert für die Aufzeichnung und Validierung von Informationen zu Gütern, während diese vom Lieferanten zum Hersteller und vom Gross- über den Detailhandel schliesslich zum Endkunden gelangen.

Nach wie vor gibt es im *Supply Chain Management* diverse Medienbrüche. Bei der Übergabe von Gütern zwischen zwei Parteien oder bei Statusänderungen von Verträgen und Lieferungen ist oftmals kein durchgängiger, transparenter Datenfluss vorhanden. Mit

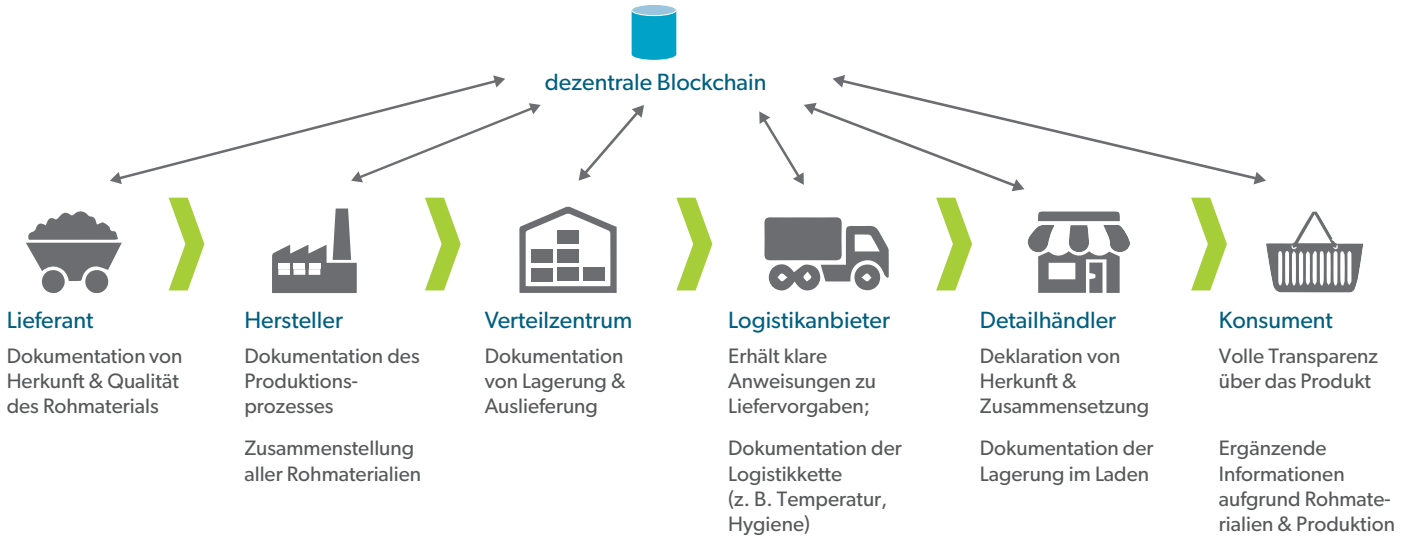


*Abb. 4: Nachvollziehbarkeit in der Lieferkette*

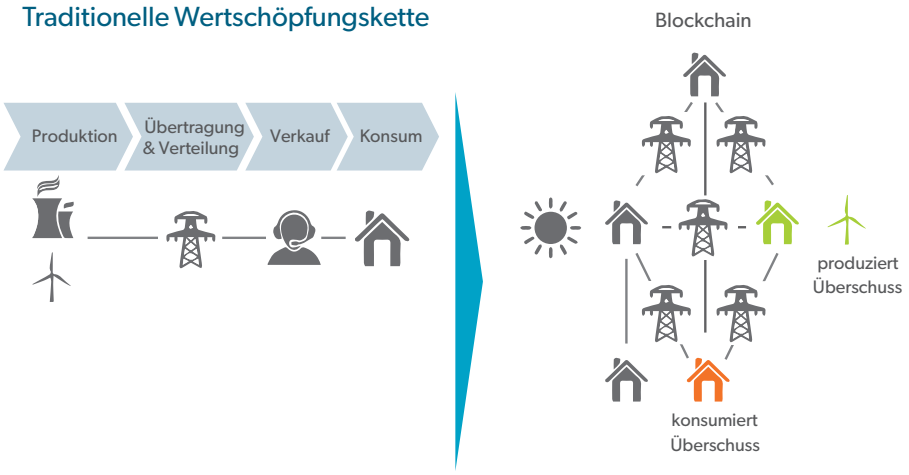


*Abb. 5: Energiehandel ohne Intermediär*

einer *permissioned* Blockchain als verteilten, für das gesamte Ökosystem zugänglichen Plattform, können Statusinformationen sowie Vertrags- und Lieferdokumente aufgezeichnet, eingesehen und geprüft werden. Statt Rohmaterialien, Komponenten oder das Endprodukt an jedem Punkt der Lieferkette manuell auf Echtheit und Vertragskonformität zu prüfen, stehen dazu relevante Informationen stets digitalisiert in der Blockchain zur Verfügung (vgl. Abbildung 4 auf Seite 3).

### Von der digitalen Identität zur e-Residency

Auch im öffentlichen Sektor gibt es prädestinierte Anwendungsfälle. Angedacht sind Anwendungen zur grenzüberschreitenden Identifikation von Staatsbürgerschaften, Systeme für Wahlen und Abstimmungen bis hin zu Grundbucheinträgen und Eigentumsübertragungen. Ziel dabei ist, die aufwändigen Prozesse effizienter zu gestalten, die Betrugsrisiken zu minimieren und das Vertrauen in den öffentlichen Sektor zu stärken.

Heutzutage wird eine Transaktion mit einem handschriftlich unterzeichneten Stück Papier vollzogen. Ob die Handelsware dem Geschäftspartner jedoch tatsächlich gehört, ist beispielsweise für den Käufer eines Gemäldes oder Fahrzeugs nur schwer nachvollziehbar. Das bestehende hohe finanzielle Risiko kann einzig über den kostspieligen und zeitintensiven Einbezug einer zentralen, vertrauenswürdigen Stelle reduziert werden. In einer Blockchain lässt sich dieses zentrale Vertrauen dezentralisiert abbilden.

### Sichere Transaktionen ohne Intermediär

Diskutiert wird die Blockchain-Technologie häufig in Verbindung mit Kryptowährungen. Statt über eine zentrale Clearingstelle werden Transaktionen direkt unter den Netzwerkteilnehmern bestätigt und abgewickelt. Diverse Ideen drängen auf den Markt, die in ähnlicher Weise versprechen, Prozesse zwischen Endverbrauchern effizienter zu gestalten.

Im Energiehandel beispielsweise können Privathaushalte Überschüsse an selbst produziertem Strom direkt anderen Privatkonsumenten verkaufen. Den Preis pro Energieeinheit und weitere Bedingungen vereinbaren die beiden Haushalte individuell und halten sie in einem *Smart Contract* fest. Treffen die Bedingungen ein, wird der Vertrag automatisch terminiert und die Transaktion vom konsumierenden zum produzierenden Haushalt ohne Intermediär ausgeführt (vgl. Abbildung 5).

Die Musikindustrie birgt ebenfalls Potenzial für Blockchain-Anwendungen. So schmälern die zahlreichen Mittelsmänner zwischen Künstler und Konsumenten den Umsatz des Künstlers. In einer Blockchain kann die Abgeltung für den vorübergehenden Konsum des geistigen Eigentums mithilfe von *Smart Contracts* direkt vom Konsumenten zum Künstler erfolgen. Insbesondere im Zusammenhang mit Musikstreaming bietet die Blockchain interessante Alternativen, um den Austausch von geistigem Eigentum transparent und effizient zu gestalten.

### Zum Schluss

Blockchain als interessantes technisches Hilfsmittel hält sowohl Chancen als auch Risiken bereit. Jedes Unternehmen sollte überlegen, welche Elemente seiner Wertschöpfung durch Blockchain unterstützt werden können respektive davon bedroht sind. Dazu ist jetzt der richtige Zeitpunkt! Setzen Sie sich mit den technischen Grundlagen der Blockchain auseinander. Nur mit ausreichend Technologieverständnis lassen sich die Auswirkungen auf Ihr Geschäftsmodell abschätzen.

Gerne beraten wir Sie bei einer ersten Wirkungsanalyse oder bei Verständnisworkshops zum Thema Blockchain und *Smart Contracts*. Ebenso unterstützen wir Sie bei der Evaluation der richtigen Technologie, bei Überlegungen zur Integration in Ihre IT-Architektur oder bei Informationssicherheits- und Businesskontinuitätsfragen.

## Ihr Kontakt

**Adrian Anderegg**

MSc ETH MTEC
Bereichsleiter Banken & Versicherungen

## Über die AWK GROUP AG

**AWK ist eines der grössten unabhängigen Schweizer Beratungsunternehmen für Informationstechnologie und Digitalisierung.**

**Wir sind schweizweit tätig mit Standorten in Zürich, Bern, Basel und Lausanne.**

**Unsere Dienstleistungen umfassen Consulting, Engineering und Projektmanagement.**

AWK GROUP AG
Leutschenbachstrasse 45, CH-8050 Zürich
T +41 58 411 95 00, www.awk.ch

Zürich • Bern • Basel • Lausanne