

Vom Außenseiter zum Technologie-Standard

Dezentrale Strukturen der Blockchain-Technologie sorgen für Sicherheit und Vertrauen

Lumir Boureau

1 Einführung

Auch wenn es die Blockchain-Technologie bereits seit einem knappen Jahrzehnt gibt, so kommt sie doch erst in den letzten Jahren zur vollen Entfaltung. Der Grund: Die Technologie war ihrer Zeit voraus und erst allmählich ziehen die Anwendungsbereiche und Einsatzszenarien nach. Hinzu kommt auch, dass die Entscheider mehr Licht ins Dunkle gebracht haben als noch vor fünf Jahren und deshalb die unglaublichen Möglichkeiten dieser Technologie erkennen. So wundert es kaum, dass sich das Blockchain-Prinzip nach und nach in klassischen IT-Prozessen breit macht und speziell bei Prozessen, in denen temporäre Geschäftsbeziehungen ein zentraler Bestandteil sind, immer selbstverständlicher wird.

Was aber wird landläufig unter Blockchain verstanden? Wikipedia¹ definiert eine Blockchain als eine kontinuierlich erweiterbare Liste von Datensätzen (genannt Blöcke), die mittels kryptographischer Verfahren miteinander verkettet sind. Jeder einzelne Block wiederum enthält einen kryptographisch sicheren Streuwert des vorhergehenden Blocks, einen Zeitstempel und Transaktionsdaten.

Aber was macht die Blockchain so besonders, so interessant? Sie reduziert die Abhängigkeit von einem einzelnen Serviceanbieter und ermöglicht stattdessen einen direkten, transparenten und vertrauensvollen Datenaustausch zwischen Business- oder Projektpartnern. Zudem vereinfacht die Blockchain-Technologie die Komplexität von Prozessen und erhöht die Transparenz und Auditierbarkeit von Dokumenten. So wiederum gelingt es der Technologie, ein sicheres Datenübertragungssystem aufzubauen und dadurch eine Vertrauensbasis zwischen verschiedenen Prozessbeteiligten herzustellen – unabhängig davon, ob sich diese kennen oder nicht.

2 Next-Level-Technologie

Durch diese besondere Struktur ist auch automatisch ein wesentlich höheres Sicherheitsniveau gewährleistet – sprich, Cyberkriminelle haben kaum eine Chance, diese Technologie zu unterlaufen.

Wie funktioniert das? Eine Blockchain ist im Grunde nichts anderes als ein verteiltes Register, in dem Daten – seien es statische Aufzeichnungen und/oder dynamische Bewegungsdaten – zunächst nach einem konsensbasierten Mechanismus überprüft und erst dann zur Transaktion freigegeben werden. Dabei verzichtet die Blockchain auf eine zentrale Koordinationsstelle, sondern baut vielmehr auf vier grundlegende Eigenschaften.

1. Dezentrale Validierung

Neue Daten werden in Blöcke gepackt, die erst dann der Blockkette hinzugefügt werden können, wenn ein Konsens über die Gültigkeit der Aktion erreicht ist.

2. Redundanz

Es gibt keinen Single Point of Failure, da mehrere Blockchain Nodes die Daten vorhalten.

3. Unveränderliche Speicherung

Durch die Verkettung von Blöcken werden die gespeicherten Daten unveränderbar und es entsteht eine vollständige Transparenz über die gesamte Transaktion.

¹ Wikipedia <https://de.wikipedia.org/wiki/Blockchain>

4. Verschlüsselung

Digitale Signaturen, die auf kryptografischen Schlüsseln basieren, versetzen die Netzwerkteilnehmer in die Lage zu authentifizieren, welcher Teilnehmer eine Transaktion initiiert, ein Asset besitzt, einen Smart Contract (Vertrag auf Softwarebasis) bereitstellt oder Daten in der Blockchain geschrieben hat.

3 Dimensionen der Blockchain

Die Blockchain-Technologie bietet aufgrund ihrer dezentralen Peer-to-Peer-Struktur maximale Sicherheit, verbesserte Netzwerkflexibilität und reduzierte Transaktionskosten. Besonders gewichtig aber ist, dass sie die Notwendigkeit und Abhängigkeit von Vermittlern reduziert. Damit stellt sie u.a. das etablierte Prinzip von Web-Konzepten auf den Kopf, denn bisher sind die Regeln bei Web-Modellen im Protokoll bewusst einfach gehalten, sodass Anwendungsentwickler die Möglichkeit haben, die Regeln zu legen.



(Quelle: Fotolia_1176848952_Tierney)

Im Blockchain-Modell dagegen sind die Regeln direkt im Protokoll eingebaut, sodass die Daten unveränderbar, aber für alle nutzbar sind. So können etwa Smart-Contract-Entwickler mächtige Algorithmen direkt in das Protokoll schreiben, ähnlich wie bei einer zentralen Steuerung, nur, dass das Matching direkt auf der Blockchain passiert.

4 Blockchain – Entwicklungsland Deutschland

Doch trotz dieses Potenzials steckt die Blockchain in Deutschland noch in den Kinderschuhen. Das zeigt nicht zuletzt eine aktuelle Untersuchung des Bitkom². Laut Umfrage birgt die Blockchain-Technologie ähnlich wie die künstliche Intelligenz (KI) und das Internet of Things (IoT) enormes Potenzial: 15 Prozent aller vom Bitkom befragten Unternehmen gehen sogar davon aus, dass Blockchain die Gesellschaft und Wirtschaft ebenso stark verändern wird wie ehemals das Internet; fragt man die IT-Experten von Unternehmen mit mehr als 500 Mitarbeitern, teilen sogar 36 Prozent diese Einschätzung.

In der Bitkom-Umfrage gibt jedes zehnte Unternehmen an, dass die deutsche Wirtschaft verglichen mit anderen Ländern bei der Blockchain derzeit abgeschlagen sei, rund jedes zweite (46 Prozent) Unternehmen ordnet Deutschland sogar als Nachzügler ein. Etwa 40 Prozent sehen Deutschland im Mittelfeld – aber keines der befragten Unternehmen empfindet Deutschland als führend oder gar der Spitzengruppe zugehörig.

Unabhängig davon lässt sich grundsätzlich festhalten, dass die Blockchain-Technologie in der Wirklichkeit ankommt – auch wenn sich dabei die Grenzen ihrer Einsatzmöglichkeiten abzeichnen: Es wird

² Bitkom-Umfrage: <https://www.bitkom.org/Presse/Presseinformation/Deutsche-Wirtschaft-zoegert-bei-der-Blockchain>

immer klarer, dass diese Technologie nicht für einen massenhaften Einsatz geeignet ist, sondern dass sie vielmehr für ganz spezielle Anforderungsprofile Lösungen bietet – beispielsweise für Kryptowährungen. Auch wenn die Kryptowährungen sehr gehypt wurden und die Erwartungen überzogen waren, so ist dieser inzwischen abklingende Hype-Zyklus doch sehr typisch für neue Technologien und deren Markteinführung. Für die Glaubwürdigkeit und den Nutzen der Blockchain-Technologie hat dies jedoch keine negativen Folgen.

5 Wo die Reise hingeht

Eine Blockchain ist eine unveränderliche, verteilte Datenbankstruktur, die Transaktionen mit einem oder mehreren Parteien vereinfacht und gleichzeitig sicherer gestaltet, ohne dass eine Validierung durch Dritte erforderlich ist. Durch das Dezentralisierungskonzept hat keine der einzelnen Parteien den gesamten Transaktionssatz, und es entsteht eine sichere Plattform, die automatisch das Vertrauen aller genießt. Basierend auf diesem Prinzip, lassen sich revolutionäre neue Anwendungen entwickeln, die unser Zusammenleben nachhaltig prägen werden. Bitcoin & Co. sind nur der Anfang.

Problematisch bleibt bei aller Euphorie allerdings, dass der Proof-of-Work-basierende Konsensmechanismus die Blockchain-Technologie energieaufwendig macht und der Rechenzentrumsbedarf enorm ist. Insbesondere vor dem Hintergrund, dass die Kryptominer in Indien oder China arbeiten – in Ländern, in denen Energie nichts kostet –, sollten sich Unternehmen, die auf Blockchain setzen, des energetischen Aufwands bewusst sein. Deshalb ist es wichtig, diese Kontroverse nicht zu übergehen, sondern bei der Blockchain-Diskussion durchaus die Vorteile der Datendezentralisierung sowie deren Unabhängigkeit zu thematisieren. Dann kann und wird sich die Blockchain-Technologie weiterentwickeln und vielleicht noch weitere Optionen für die Zukunft eröffnen.

Fachbeitrag zum Buch: Köhler-Schute, Christiana (Hg.): Blockchains und Distributed-Ledger-Technologien in Unternehmen, Grundlagen, Konzepte und Praxisbeispiele, juristische Aspekte, Berlin: KS-Energy-Verlag, 2019 (ISBN: 978-3-945622-09-4)

Mit freundlicher Genehmigung: KS-Energy-Verlag, Berlin 2019