Die Blockchain ermöglicht, digitale Einträge fälschungssicher und unveränderbar zu speichern.

Digitales „Kassabuch“

Die Blockchain-Technologie ermöglicht es, mit Vertragspartnern gesicherte Transaktionen zu tätigen oder verbindliche Vereinbarungen zu treffen, ohne dass eine Bank, ein Vermittler oder Notar nötig ist.

Die einen sehen es als eine neue Stufe der digitalen Revolution, die unsere Wirtschaft, ja, unser gesamtes soziales Zusammenleben ändern wird, die anderen befürchten eine Blase, die in sich zusammenbrechen wird. Wenn es um Blockchain geht, ist meist auch das Thema Bitcoin mit dabei. Im allgemeinen Verständnis ist Blockchain noch immer weitgehend gleichgesetzt mit Bitcoin, oder anderen Krypto-Währungen, denen die Blockchain-Technologie zugrunde liegt. Doch zunehmend redet man über Anwendungen im Bereich „Smart Contracts“ (automatische Verträge) oder „Supply Chain“ (Lieferketten).

Die Blockchain ist vereinfacht ausgedrückt ein digitales Kassabuch mit beliebig vielen Kopien. Dieses Kassabuch hat einige wichtige Eigenschaften: Sobald ein Eintrag erfolgt ist und bestätigt wurde, ist dieser unveränderlich gespeichert und in jeder Kopie verfügbar. Die Beweisbarkeit des Eintrags ist gesichert, weil dieser Eintrag nicht nur an einer Stelle, sondern an vielen Stellen gespeichert wird. Jede Änderung des Eintrags ist sofort erkennbar, weil alle Einträge durch spezielle Prüfsummen gesichert werden. Die Quelle des Eintrags und die Rechtmäßigkeit des Eintrags ist nachvollziehbar und beweisbar, weil die Einträge über digitale Signaturen identifiziert sind.

Die analoge Entsprechung zur Blockchain ist ein Kassabuch (oder Protokoll), das von Notaren nach klar definierten Regeln parallel geführt wird, unter dem Gesichtspunkt, dass immer alle Kopien inhaltlich identisch, also konsolidiert sein müssen. Anders als bei der klassischen Notariatsregelung kann „jeder“ die Einträge „jederzeit“ überprüfen und es fallen statt der Notariatsgebühren nur marginale Kosten an, die sich aus der Speicherung in der Blockchain ergeben.

Technologie. Die Blockchain ist eine Kette von Datenblöcken, die miteinander so verknüpft sind, dass jeder nachträgliche Eingriff sofort erkennbar und lokalisierbar wird – und damit in der Praxis unmöglich ist. Die Blockchain ist erst durch die moderne Kryptografie möglich geworden, die sich seit der Mitte des 20. Jahrhunderts entwickelt hat. Die wichtigsten Durchbrüche waren die Erfindung moderner symmetrischer Verschlüsselung und der Hashing-Algorithmen. Ohne diese Entwicklungen wären auch viele Errungenschaften nicht möglich, die Grundlagen unserer neuen digitalen Welt sind. Die moderne Kryptografie erlaubt uns sichere Internet-Kommunikation, digitale Signaturen, Verteilung und Speicherung von vertraulichen Informationen, Identifizierung von Perso-

FOTO: IPOPBA/STOCK.ADOBE.COM

Die Blockchaintechnologie ist durch Bitcoin bekannt geworden.

nen, Fahrzeugen, Geräten und Dokumenten und den Aufbau von Vertrauen zwischen einander unbekannten Stellen, etwa Webshops und Nutzern des Webshops. Und es ist erst durch die moderne Kryptografie ist es möglich, selbst Kontrolle über seine Geheimnisse zu übernehmen – vorausgesetzt, Kryptografie wird richtig verwendet, was seitens Entwickler und Anwender oft genug unzureichend geschieht. Bis zu Bitcoin war Kryptografie eine Sache für Mathematiker und Sicherheitsexperten. Durch Bitcoin ist Kryptografie ins Rampenlicht getreten und hat plötzlich Millionen interessiert. Die kryptografischen Grundlagen, die die Blockchain prägen, werden jedoch bereits schon länger in vielen Bereichen verwendet – vom Zentralen Melderegister bis zur Sicherung von amtlichen Dokumenten vor Verfälschung, oder zur Feststellung der Identität im Internet, über Bürgerkarte und Handysignatur.

Misstrauen. Am Beginn der bekanntesten Blockchain, der Bitcoin-Blockchain, stand das Misstrauen gegen das zentralisierte Bankensystem, das der Willkür der Mächtigen ausgesetzt ist: Der Wert des Geldes ist abhängig von den Entscheidungen der Zentralbanken. Bitcoin versprach ein Geldsystem, das dezentral funktioniert und dessen Wert aus sich selbst heraus entsteht. Ähnliche Motivationen trieben andere Blockchain-Entwicklungen an: Statt einer zentralen Instanz, die Herrschaft über die Transaktionen besitzt, sollten diejenigen, die die Transaktionen durchführen, Kontrolle über die Prozesse besitzen.

Beispiele dafür wären öffentliche Register wie das Grundbuch, oder Prozesse, in denen es viele Beteiligte gibt, die kein Vertrauen ineinander haben, etwa in der verteilten Energieerzeugung bei privaten Einspeisungen in das Energienetz. Beispiele sind vertragsartige Übereinkünfte, die zwischen belie-

FOTO: THAUT IMAGES/STOCK.ADOBE.COM

Digitale Verträge bauen auf der Blockchain-Technologie auf.

bigen Beteiligten geschehen und die auf einen Intermediär verzichten wollen und können. In der ersten Begeisterung sah man die Blockchain als Lösung für jedes nur erdenkliche Problem. Inzwischen haben sich Kriterien entwickelt, die bei der Entscheidung helfen, ob eine Blockchain für ein bestimmtes Problem eine geeignete Lösung bieten kann.

Die erste Welle des Hype ist verebbt. Die Projekte werden realistischer und unterliegen einer „natürlichen" Selektion. Anhand der Kriterien, die allgemein anerkannt sind, lassen sich auch für Entscheider die Argumente für oder gegen eine Blockchain im jeweiligen Anwendungsfall besser abschätzen. Wir werden in Zukunft die Blockchain als eine Technologie unter vielen verwenden, ein Teil des Werkzeugkastens für digitale Anwendungen. Weiters ist zu hoffen, dass durch die Blockchain generell das Verständnis für Kryptographie steigt, denn es gibt eine Reihe von Einsatzbereichen der Kryptographie, die mit Blockchain weniger zu tun haben. Wir werden in Zukunft eine Reihe von Anwendungen der Blockchain erleben, die uns sinnvoll bereichern, aber auch andere Anwendungsformen kryptographischer Methoden, die mit Blockchain nichts zu tun haben.

Beispiele für den Blockchain-Einsatz. Berühmt und berüchtigt wurde die Blockchain durch die Bitcoin, die als Hilfsmittel für anonyme Zahlungen außerhalb des klassischen Finanzsystems ambivalente Wirkungen hat (siehe „Kryptowährungen – Verschleierte Geldflüsse" in Öffentliche Sicherheit 1-2/19). Die Blockchain wird jedoch auch für Lösungen in ganz anderen Bereichen eingesetzt, etwa in der Kontrolle und Dokumentation der Kühlkette: Frische Lebensmittel, empfindliche Medikamente, bestimmte Chemikalien benötigen eine zuverlässige Einhaltung

FOTO: THODONAL/STOCK.ADOBE.COM

der Kühlkette. Blockchain ist hier für das Monitoring gut geeignet. Für die Kühlkette gibt es meist unterschiedliche Verantwortliche in zeitlicher Abfolge. Die Abstimmung und Kommunikation ist nicht einheitlich, oft gibt es auch keine zentrale Instanz, die sich um den gesamten Verteilungsweg kümmert. Hier hilft Blockchain: Temperatursensoren in den Produktverpackungen senden über energiesparende Funktechnologien den Temperaturverlauf, der in einer Blockchain gespeichert wird. Eine Kontrolle ist jederzeit auch für Dritte möglich, Manipulationen und nachträgliche Löschungen von Daten sind nicht möglich.

Ein weiteres Beispiel wäre die Protokollierung von umfangreichen Begutachtungs- und Bewilligungsverfahren. Wenn Dokumente zwischen verschiedenen Stellen versendet werden, unterschiedliche oder gegnerische Seiten miteinander kommunizieren müssen und ein größerer Kreis von Beteiligten, vielleicht sogar die Öffentlichkeit, über den Status und Verlauf informiert werden soll, dabei aber jede Veränderung zeitlich wie inhaltlich nachvollziehbar sein muss, ist eine Blockchain eine geeignete Möglichkeit. Dabei würden die ursprünglichen Dokumente in Form von Hashes gesichert werden, sowie jede Änderung entweder selbst in die Blockchain geschrieben werden, oder Hashes der Änderungen. Links zu den jeweiligen Dokumenten können mit eingeschlossen werden, der Zugriff kann außerhalb der Blockchain geregelt werden.

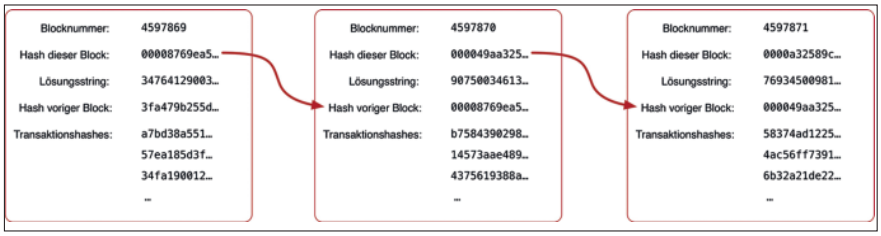
Die Blockchain ist nicht geeignet für ein sehr hohes Datenvolumen, einen eingegrenzten Benutzerkreis und rasche Transaktionen.

Ein Hash ist eine spezielle Form einer Prüfsumme, die wie ein Fingerabdruck funktioniert: Es lassen sich damit Daten identifizieren, ohne dass man aus einem Hash die Originaldaten herauslesen kann. Ein Hash ist eine mathematische Einwegfunktion, die „kollisionsfrei“ und hochgradig zufällig ist. Kollisionsfrei bedeutet, dass die Wahrscheinlichkeit, dass zwei unterschiedliche Texte den gleichen Hashwert haben, extrem niedrig ist. Außerdem erzeugen selbst minimale Veränderungen im Ausgangstext komplett unterschiedliche Hashwerte.

Michael Werzowa

Zum Autor:
Michael Werzowa, Experte für Netzwerk- und Datensicherheit, Vorstand der IoT Austria – The Austrian Internet of Things Network (www.iot-austria.at)

BLOCKCHAIN-TECHNOLOGIE



Die Blöcke einer Blockchain enthalten Nutzdaten, die durch die Blockchain vor Veränderung geschützt werden sollen und den Hash des vorhergehenden Blocks sowie einen Hash über die Nutzdaten + vorheriger Hash + Lösungszahl aus dem „Proof of Work“.

Öffentliche Sicherheit	SHA512: 5013EE6B5166148599758A13CF856D3DA90F7C6CC25AFAA2F71E76C2991F013C8777660031EEF70E1BBF56C1EA31CB8AEB616A644E36DFA6F84A5DCE2E797874
ÖffentlicheSicherheit	SHA512: 557329F3FAED06AEDBC5D3F754F8A8C464D50D19DE5C49B04908E634544853DA28837877840E54C4ADF985ED402D8E550211A2EC343713DFF34CFD922A808FFF
A	SHA512: 21B4F4BD9E64ED355C3EB676A28EBEDAF6D8F17BDC365995B3190971530440805 16BD083BFCCE66121A3072646994C8430CC382B8DC543E84880183BF856CFF5

Hashes sind immer gleich lang, unabhängig vom Umfang des Ausgangsmaterials. Ein SHA512 hat 512bit. Die Hashwerte sind „zufällig“ und nicht rückführbar, aber wiederholbar.

Blockchain-Aufbau

Die Nutzdaten in einer Blockchain können verschiedener Art sein: Transaktionen, Bilder, Texte, Tondokumente – oft werden in Blockchains aber nicht die Daten selbst gespeichert, da diese zu umfangreich sein können, sondern nur Hashes der Daten, die unveränderbar geschützt sein sollen. Wenn ein Block abgeschlossen wird, werden alle Daten in diesem Block fixiert: Es wird ein Hash über die Nutzdaten und den Hash des vorigen Blocks gebildet, dieser wird in den neuen Block hineingeschrieben: Dadurch wird die Verkettung hergestellt. Bei Blockchains nach dem Prinzip „Proof of Work“ ist für den neuen Hash eine Aufgabe zu lösen, beispielsweis eine Lösungszahl zu suchen, die in den Hash miteinbezogen wird und mit deren Hilfe der berechnete Hash am Anfang beispielsweise vier Nullen erhält. Diese Zahl zu finden ist sehr aufwendig, da die entstehenden Hashes „zufällig“ sind.

Hashwerte

Funktionell betrachtet ist ein Hash eine Prüfsumme: Sie kann aus gegebenen Ausgangsdaten relativ einfach berechnet werden, somit jederzeit überprüft werden. Dennoch ist das Ergebnis nicht rückführbar. Hashwerte haben einige wichtige Eigenschaften, um ihren Nutzen zu erfüllen: Sie verteilen sich gleichmäßig und ungeordnet über den gesamten Zahlenraum des jeweiligen Hashes (SHA256: ca. 1,158 x 10^{77} – unser gesamtes Sonnensystem hat nur rund 1,192 x 10^{57} Atome, das uns bekannte Universum hat etwa 10^{78} bis 10^{82} Atome). Dadurch ist es heute praktisch unmöglich, einen Ausgangstext zu erzeugen, der zu einem bestimmten vorgegebenen Hash passt. Ein Hash kann über beliebig kleine oder große Datenmengen gebildet werden, er ist immer gleich groß, siehe Darstellung Hash SHA512. Jede noch so kleine Änderung in den Ausgangsdaten führt zu einem völlig neuen Hash, der keine Ähnlichkeit mit dem vorigen Hash zeigt.

GRAFIKEN: MICHAEL WERZOWA