Bundesministerium
für Wirtschaft
und Energie

Smart Data

Die Blockchain-Technologie

Problemstellung

Bei Transaktionen im Internet, sei es ein Einkauf, eine Überweisung, ein Grundstücksverkauf oder ein Vorgang bei einem Versicherer, sind die manipulationssichere Übertragung und Speicherung von Daten oder Geld von zentraler Bedeutung, insbesondere um Betrug zu vermeiden. Daher ist eine vertrauenswürdige Lösung notwendig, mit der die jeweilige Transaktion transparent nachvollzogen werden kann. Klassischerweise erfolgt dies über die Dokumentation des Austauschs, z. B. im Falle von Geld, bei einer Mittlerinstanz wie einer beteiligten Bank. Doch jede zwischengeschaltete Instanz birgt das Risiko, manipuliert zu werden. Aus diesem Grund werden alternative vertrauenswürdige und vor allem manipulationssichere Speicher benötigt.

Lösungsansatz

Die Blockchain ist eine Art dezentrale Datenbank oder digitales manipulationssicheres Register: In ihr werden, für alle beteiligten Parteien nachvollziehbar, alle Details einer Transaktion gespeichert. Eine Mittlerinstanz ist dabei nicht mehr erforderlich. Der Begriff „Blockchain“ (englisch „chain“ = Kette) basiert darauf, dass die relevanten Informationen in Bezug auf die Transaktion in Blöcken wie bei einer Kette aneinanderhängen. Erst die Gesamtinformation aus mehreren Blöcken, also die gesamte Kette, bildet die Blockchain.

Die Blockchain-Technologie

Das Ziel der Blockchain-Technologie ist die Realisierung eines manipulationssicheren Speichers im Internet, der keine zentrale vertrauenswürdige Stelle benötigt. Dazu wird die Blockchain auf allen am Blockchain-Netzwerk beteiligten Computern gespeichert: Jeder Knoten innerhalb des Netzwerks enthält dabei eine vollständige Kopie der Blockchain. Wie Perlen an einer Kette reiht sich so Datenblock an Datenblock und die Blockchain entsteht. Die Teilnehmer des Netzwerks können die gespeicherten Daten, beispielsweise Transaktionen, einsehen.

Um Manipulationen zu vermeiden, sind im Protokoll des Blockchain-Netzwerks verschiedene Sicherheitsmechanismen eingebaut. So wird die Rechtmäßigkeit jeder Transaktion im Vorhinein geprüft. Bei einer Überweisung von Bitcoins etwa wird automatisch anhand der in der Bitcoin-Blockchain gespeicherten Daten überprüft, ob der Sender überhaupt über den entsprechenden Betrag verfügt. Eine Transaktion wird bestätigt, indem die Mehrheit der Rechner im Netzwerk ihr zustimmt. Die Manipulation einer Blockchain ist dadurch mit einem enormen Aufwand verbunden. Jeder Block enthält nämlich neben den eigentlichen Daten Informationen zur Verifikation des Vorgängerblocks. Soll ein Block in der Blockchain manipuliert werden, müssen daher auch alle nachfolgenden Blöcke neu erzeugt werden. Da der dafür benötigte Rechenaufwand in der Regel nur durch die Mehrheit des Netzwerkes, nicht aber durch einzelne Teilnehmer realisierbar ist, entsteht Manipulationssicherheit.

Anwendungsbereiche

Durch den Wegfall einer zentralen vertrauenswürdigen Stelle sind potenzielle Anwendungsbereiche für Blockchains breit gefächert. Sie sind bereits in verschiedenen Branchen zum Hoffnungsträger geworden, beispielsweise bei Versicherungen, bei Banken, bei Fintech-Start-ups, in der Industrie oder im Bereich der öffentlichen Hand. Prominenz hat die Blockchain als Technologie hinter Bitcoin, der bekanntesten Kryptowährung (digitales Zahlungsmittel), erlangt. Weiterhin gibt es derzeit Ansätze, durch Blockchains Grundbücher auf neue, digitale Füße zu stellen, den Aktienhandel zu revolutionieren und durch sogenannte Smart Contracts Lieferketten abzusichern. Grundsätzlich ist die Blockchain-Technologie einsatzfähig und wird im Rahmen von Bitcoin bereits erfolgreich genutzt. In weiteren Bereichen wird sie sich noch bewähren müssen. Ob beim Aktienhandel, in der Verwaltung oder im Versicherungswesen: Die Blockchain überzeugt durch eine hohe Manipulationssicherheit und durch die dezentrale Speicherung der Informationen, durch die sie auch beim Ausfall eines Knotens intakt bleibt. Ob sie ihre großen Versprechen halten kann, wird der Praxistest zeigen – ebenso wie ihre Akzeptanz in der Bevölkerung.

Im Rahmen des Technologieprogramms „Smart Data – Innovationen aus Daten“ spielt die Übertragung von Daten im Internet eine zentrale Rolle. Ein spezielles Identitätsmanagement-Verfahren, das durch die Blockchain-Technologie ermöglicht wird, ist die französische Standardisierungsinitiative ISÆN (Individual perSonal data Auditable addrEss Number). Die Smart-Data-Begleitforschung hat dieses Verfahren analysiert. Die betreffende Studie ist online abrufbar unter http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/smartdata_studie_isaen.html.

Über Smart Data – Innovationen aus Daten

Mit dem Technologieprogramm „Smart Data – Innovationen aus Daten“ fördert das BMWi von 2014 bis 2018 insgesamt 16 Leuchtturmprojekte, die den zukünftigen Markt von Big-Data-Technologien für die deutsche Wirtschaft erschließen sollen. „Smart Data“ ist Teil der Hightech-Strategie und der Digitalen Agenda der Bundesregierung. Weitere Informationen zum Smart-Data-Technologieprogramm erhalten Sie unter www.smart-data-programm.de.

Stand
August 2017

Redaktion
Loesch*Hund*Liepold Kommunikation GmbH

Bild
Quelle: monsitj/fotolia