Wie funktioniert die Blockchain?

Die Blockchain-Technologie gilt als fälschungssicher. Die bekannteste Anwendung ist die Kryptowährung Bitcoin. *Jan Thomas Frecè, Sebastian Höhn*

Die Grundidee hinter der Blockchain ist einfach: Mehrere Parteien führen gemeinsam eine Datenbank und teilen sich die Verantwortung dafür. Bei einer Blockchain gibt es keine zentrale Institution, bei der die Fäden zusammenlaufen. Alle Teilnehmenden halten gleichgestellte Kopien der Blockchain. Neue Einträge werden in alle Kopien übernommen, sobald Konsens über den jeweils aktuellen Stand hergestellt wird. Für die Verteilung der Daten und die Herstellung des Konsenses werden je nach Art der Blockchain unterschiedliche Methoden eingesetzt. Als prominentes Beispiel basiert die Kryptowährung Bitcoin – sprich deren Transaktionsdatenbank – auf dieser Technologie.

Für die Speicherung in der Blockchain werden die Daten in Blöcken zusammengefasst, wo beliebige Daten abgelegt werden können. Löschen ist hingegen nicht möglich. Anschliessend werden die Blöcke miteinander kryptologisch verkettet, sodass es nachweisbar ist, falls einer fehlt oder verändert wurde. Wie bei einer fortlaufenden Rechnungsnummer kann so die Vollständigkeit der in der Blockchain gespeicherten Daten erkannt werden. Soll ein neuer Datenblock hinzugefügt werden, so muss eine vorher festgelegte Anzahl der Teilnehmer dessen Richtigkeit elektronisch bestätigen. Jeder neue Block bestätigt alle früheren Blöcke an Transaktionen, sodass Manipulationen erkennbar sind.

Veränderungen fallen auf

Für eine öffentlich betriebene Blockchain ist der Aufwand für das Einfügen eines neuen Blocks mit einem hohen Rechenaufwand verbunden. So wird bei Bitcoin häufig der hohe Stromverbrauch bemängelt. Der Grund ist der «Proof of Work» (POW). Dieser verhindert, dass Angreifer massenweise manipulierte Blöcke in die Blockchain schreiben. Ist der Teilnehmerkreis hingegen bekannt, werden effizientere Verfahren für den Konsens eingesetzt, und der Ressourcenverbrauch kann deutlich reduziert werden.

In einer Blockchain gelten Daten als «unveränderbar». Was bedeutet dies? Die in der Blockchain gespeicherten Daten können wie alle digital gespeicherten Dokumente verändert werden. Veränderungen an den Daten werden durch den Einsatz von digitaler Signatur, Verschlüsselung und Redundanz jedoch erkannt. Zudem kann jeder Teilnehmer, der die korrekten Daten vorlegt, auch beweisen, dass diese korrekt sind.

Wie muss man sich «Datenkonsens» vorstellen? Anders als bei einer zentralen Datenbank, die voraussetzt, dass man der Stelle vertraut, die sie führt, werden bei einer Blockchain neue Daten nur dann hinzugefügt, wenn eine vorab definierte Anzahl von Teilnehmern diese (vollautomatisiert) geprüft und mittels kryptografischer Verfahren bestätigt hat. Dadurch ist Vertrauen in einzelne Teilnehmer nicht notwendig; einzelne betrügerische Teilnehmer können die Korrektheit der Daten nicht gefährden.

Ein spannendes Forschungsfeld sind sogenannte Smart Contracts: Dies sind im Kontext der Blockchain ausführbare Computerprogramme, die dynamische Verträge repräsentieren. Mit den Mechanismen der Blockchain lassen sich die Unveränderbarkeit des Computerprogramms sowie die Unveränderbarkeit der Ausführungsumgebung sicherstellen. Dadurch lassen sich zum Beispiel sichere, vollautomatische Lösungen für Zahlungsverkehr oder Warennachverfolgung umsetzen, die eine grosse Anzahl von unterschiedlichen Kunden und Lieferanten massgeschneidert integrieren können.

Jan Thomas Frecè
Dr. des., wissenschaftlicher Mitarbeiter, E-Government-Institut, Berner Fachhochschule, Bern

Sebastian Höhn
Dr. rer. nat., Dozent, E-Government-Institut, Berner Fachhochschule, Bern