Das Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen berichtet über neue Technologien

Blockchains

Die Blockchain-Technologie hat in letzter Zeit viel Aufmerksamkeit erregt, da sie u. a. die technologische Basis für die digitale Währung (bzw. Kryptowährung) Bitcoin bildet. Derzeit gibt es intensive Bemühungen, ihre Vorteile auch für eine zunehmende Zahl anderer Anwendungsbereiche nutzbar zu machen.

Bei einer Blockchain handelt es sich um eine Art von verteilter Datenbank (ein sog. Distributed Ledger), d. h. eine Datenbank, die nicht nur an einem einzigen Ort zentral abgelegt, sondern dezentral auf mehreren Computern in einem Netzwerk vorhanden ist. Die Datenbankeinträge sind dabei kryptografisch gegen Manipulationen geschützt, so dass der Datenbank nur neue Einträge hinzugefügt werden können, sich aber keine Einträge nachträglich modifizieren oder löschen lassen. Die Daten in der Blockchain, wie z. B. die Daten von finanziellen Transaktionen bei Bitcoin, werden in ihrer zeitlichen Reihenfolge zu einzelnen Blöcken zusammengefasst, wobei jeder Block kryptografisch mit dem vorhergehenden Block verknüpft ist, so dass sich eine zusammenhängende Kette von Blöcken ergibt.

Normalerweise ist für die Abwicklung von Transaktionen zwischen zwei Parteien, die sich nicht vollständig gegenseitig vertrauen, eine vertrauenswürdige dritte Partei notwendig, z. B. eine Bank bei finanziellen Transaktionen. Ein wichtiger Grund für das große Interesse an Blockchains ist daher, dass bei solchen Transaktionen prinzipiell keine zentrale Kontrollinstanz mehr erforderlich ist und stattdessen eine Blockchain diese Aufgabe übernehmen kann. Weiterhin bietet der verteilte, dezentralisierte Ansatz von Blockchains eine potenziell hohe Ausfallsicherheit, da bei einem Ausfall eines Netzwerk-Knotens dessen Funktion grundsätzlich durch einen anderen Netzwerk-Knoten übernommen werden kann (Peer-To-Peer-Netzwerk).

Blockchains können im Wesentlichen in Permissionless Blockchains und Permissioned Blockchains unterteilt werden. Bei einer Permissionless Blockchain (häufig auch Public Blockchain genannt) wie Bitcoin gelten keinerlei Einschränkungen für die Netzwerk-Teilnehmer, so dass z. B. prinzipiell jeder den Inhalt der Blockchain zur Kenntnis nehmen und die Blockchain um neue Einträge in Form eines zusätzlichen Blocks erweitern kann. Bei einer Permissioned Blockchain ist der Kreis der Netzwerk-Teilnehmer hingegen eingeschränkt. Dieser Teilnehmerkreis wird üblicherweise durch eine zentrale Instanz kontrolliert, weshalb es sich hierbei nicht um einen vollständig dezentralisierten Ansatz für eine Blockchain handelt.

Blockchains unterscheiden sich außerdem bezüglich des jeweils genutzten Konsensfindungsverfahrens. Dieses Verfahren gewährleistet, dass die Netzwerk-Teilnehmer darin übereinstimmen, in welcher zeitlichen Reihenfolge und um welche neuen Einträge die Blockchain erweitert wird. Ein neuer Block wird der Blockchain daher erst dann hinzugefügt, wenn die Teilnehmer einen Konsens darüber gefunden haben, dass die neuen Einträge unter Berücksichtigung der bereits in der Blockchain enthaltenen Daten auch korrekt sind. Das aktuell am häufigsten genutzte Konsensfindungsverfahren, das auch bei Bitcoin eingesetzt wird, ist Proof of Work. Hierbei konkurrieren die Netzwerk-Teilnehmer untereinander darum, wer einen neuen Block erstellen darf, der dann der Blockchain hinzugefügt wird. Dabei gewinnt derjenige, der als erster nachgewiesen hat, eine bestimmte Menge an Computerressourcen, z. B. Rechenkapazität, für die Lösung einer gewissen Problemstellung aufgewandt zu haben. Permissioned Blockchains besitzen den Vorteil, dass sie nicht unbedingt ein so aufwändiges Konsensfindungsverfahren wie Proof of Work implementieren müssen, weil die Identitäten der Teilnehmer z. B. einer zentralen Instanz bekannt sind und sie deshalb für möglicherweise missbräuchliche Handlungen verantwortlich gemacht werden können.

Praktische Anwendungen von Blockchains sind augenblicklich im Finanzbereich am weitesten fortgeschritten. Beispielsweise sind nach dem Aufkommen von Bitcoin einige weitere Kryptowährungen entstanden. Daneben liegen weitere mögliche Einsatzgebiete für Blockchains im öffentlichen Sektor, wo sie z. B. für notarielle Dienstleistungen oder den Nachweis der Echtheit von Dokumenten Verwendung finden könnten. Außerdem bieten sie die Chance für effizientere Lösungen auf dem Gebiet des Supply Chain Management oder in der Logistik für die Nachverfolgbarkeit des Lagerungszustandes von sensiblen Gütern. Im Energiesektor könnten es Blockchains u. a. erlauben, dass private Haushalte ihren mit Solarzellen erzeugten Strom direkt an andere Haushalte verkaufen und im Gesundheitsbereich könnten sie beispielsweise als Grundlage für eine elektronische Patientenakte genutzt werden. Von Interesse sind auch Online-Dienste auf der Basis von Blockchains, z. B. für soziale Netzwerke wie Facebook. Hierdurch könnte beispielsweise eine Zensur von Informationen überflüssig gemacht werden. Im Bereich der IT-Sicherheit sind Blockchains u. a. zur Erkennung von Angriffen auf Computer bzw. Netzwerke geeignet.

Die Blockchain-Technologie befindet sich insgesamt noch in einem relativ frühen Entwicklungsstadium. So existieren augenblicklich deutlich mehr Visionen und Konzepte für den Einsatz von Blockchains als real existierende, funktionierende Anwendungsbeispiele. Eine wichtige aktuelle Herausforderung stellt der hohe Energieverbrauch des bei Permissionless Blockchains wie Bitcoin häufig eingesetzten Proof-of-Work-Verfahrens dar, der durch den hierfür erforderlichen Rechenaufwand verursacht wird. Eine weitere Herausforderung ist die Skalierbarkeit der Blockchain-Technologie, d. h. in welchem Maße die Technologie bei steigenden Anforderungen, z. B. einer steigenden Anzahl von Transaktionen, mitwachsen kann. Generell könnte sich die Blockchain-Technologie zukünftig auch in anderen Anwendungsfeldern als ähnlich revolutionär erweisen wie im Bereich der digitalen Währungen. Allerdings ist in einigen Anwendungsfällen wahrscheinlich gar keine Blockchain erforderlich, sondern ein Einsatz von herkömmlichen Datenbank-Technologien sinnvoller.

Dr. Klaus Ruhlig