

Das Potential der Blockchain

Preprint des Originals aus der Rhein-Neckar-Zeitung, Heidelberg, vom 7.02.2021

https://www.rnz.de/zeitjung_artikel,-informatik-das-potenzial-der-blockchain-_arid,623413.html

Von Caspar Oesterreich

Heidelberg. Professor Dr. Klaus-Georg Deck, Jahrgang 1966, ist seit 1999 Professor für Wirtschaftsinformatik an der DHBW Mosbach. Seine Lehrgebiete umfassen Algorithmen, Künstliche Intelligenz und Maschinelles Lernen. Nach Studium von Mathematik sowie Philosophie und Promotion in Genetischer Epidemiologie war er mehrere Jahre bei der SAP AG in der Basistechnologie-Entwicklung tätig.

Neben seiner Lehr- und Forschungstätigkeit an der Dualen Hochschule ist er Lehrbeauftragter in Philosophie an der Uni Heidelberg und arbeitet zudem als Data Scientist in einem Schweizer Finanzunternehmen. In Bezug auf das Thema Blockchain hat Deck etwa untersucht, wie man ein Rating-System Blockchain-basiert implementieren und somit die im Rahmen der Finanzkrise etwas in Verruf geratenen Rating-Agenturen durch ein veritableres System ersetzen beziehungsweise ergänzen kann.

Die Idee der Blockchain ist simpel, die Informatik dahinter kompliziert. Wie erklären Sie diese relativ neue Technologie einem Laien?

Eng verwandt mit dem Begriff der Blockchain ist ein etwas allgemeinerer, nämlich die "Distributed Ledger Technologie" (DLT), die auf einer fälschungssicheren, verteilten Datenverwaltung basiert. Dahinter steckt die Idee, Daten – etwa einer Finanztransaktion – nicht an einer zentralen Stelle, sondern zugleich bei allen Beteiligten zu hinterlegen, die untereinander direkt verbunden sind. Da die Entscheidung über die Annahme einer Transaktion nicht bei einer einzigen Stelle liegt, sorgt ein Algorithmus dafür, dass bei allen Teilnehmern die gleiche Information vorliegt. Dieser Konsensmechanismus entspricht einem erweiterten Wahlentscheid, wobei für die Ausübung des Stimmrechts ein besonderer Leistungsnachweis durch Lösung eines künstlich erzeugten Rechenrätsels erbracht werden muss – "proof of work" genannt. Jener Aspekt der gleichberechtigten Beteiligung aller Teilnehmer, der an die Prinzipien einer Basisdemokratie erinnert, ist zum Verständnis dieser Technologie besser geeignet als der Begriff Blockchain selbst. Dieser hat natürlich seine Berechtigung: Die Datenstruktur, mit der die Informationen an jedem einzelnen Knoten verwaltet werden, entspricht einer verketteten Liste von Informations-Blöcken – daher der Name –, wobei jeder einzelne Block die Unverfälschbarkeit seiner Daten und die seiner Vorgänger-Blöcke garantiert.

Haben Sie ein anschauliches Beispiel dafür?

Die Distributed Ledger Technologie lässt sich mit der Situation in einem Verein vergleichen, bei dem es keinen Vorstand gibt. Ob als nächstes ein Kühlschrank oder eine Kaffeemaschine angeschafft werden soll, entscheiden einzig und allein die Mitglieder. Damit die Organisation einer Abstimmung überschaubar bleibt, sind nur diejenigen Mitglieder stimmberechtigt, die mindestens zehn Arbeitsstunden für den Verein erbracht haben, und als zusätzlicher Anreiz wird jede Stimme mit den Arbeitsstunden gewichtet: Wer mehr geleistet hat, darf mehr mitbestimmen.

Was fasziniert Sie an der Blockchain-Technologie als Forschungsthema?

Die Blockchain-Technologie ist in vielerlei Hinsicht faszinierend und innovativ: Basierend auf relativ einfachen Konzepten der Informatik wie Internet, Vernetzung, Verschlüsselung ermöglicht sie zahlreiche Anwendungen in der Finanzwirtschaft, der Öffentlichen Verwaltung, der Industrie, im Dienstleistungsbereich, aber auch im privaten und gesellschaftlichen Leben. Zum einen interessieren uns an der DHBW die unmittelbaren Anwendungen in den angesprochenen Bereichen, die viele

Abläufe in den Unternehmen und Institutionen unterstützen, vereinfachen und beschleunigen, aber auch zu teilweise völlig neuartigen Geschäftsmodellen führen und etablierte Strukturen in Frage stellen. Darüber hinaus, und das macht gerade auch eine Hochschule aus, blicken wir über den Tellerrand hinaus und beschäftigen uns kritisch mit diesen Veränderungen. Jede Technologie verändert nicht nur die Welt, in der wir leben und die wir gestalten, sondern auch die Gesellschaft, und nicht zuletzt uns als wahrnehmende, handelnde und denkende Wesen selbst.

Bekannt ist der Begriff Blockchain durch die Kryptowährung Bitcoin. In welchen anderen Bereichen kann man sie außerdem anwenden?

Kryptowährungen wie Bitcoin stellen die prominentesten Anwendungen von Distributed Ledger Technologien dar. Darüber hinaus gibt es viele Anwendungsmöglichkeiten, etwa wenn es im juristischen und staatlichen Umfeld um die Authentizität von Daten geht, wie bei der Registerführung wie zum Beispiel Grundbuch oder Standesamt, oder bei Wahlen oder Umfragen. Man denke hier an den Vorwurf des Wahlbetrugs bei den Präsidentschaftswahlen in den USA. Im Gesundheitswesen geht es zum Beispiel um die Dokumentation von Gesundheitsdaten, Zahlungsströme, Arzneimittelsicherheit. In der Energiewirtschaft wären die Beispiele Automatisierung von Abrechnungen, Stabilisierung des Verteilnetzes zu nennen. In Industrie und Handel geht es unter anderem um die Rückverfolgbarkeit von Liefer- und Produktionsketten, Automatisierung von Routineprozessen.

Besonders hervorzuheben sind die sogenannten Smart Contracts. Was hat es mit denen auf sich?

Der Smart Contract wendet die ihm einprogrammierten Regeln an und "handelt" daher quasi eigenständig: Ein Kunde bucht zum Beispiel auf einer solchen Plattform einen gewünschten Mietwagen und akzeptiert damit die im System hinterlegten Nutzungsbedingungen und Vertragskonditionen wie Pauschalmietpreis, Kilometer-Mietpreis oder Zeitdauer. Die gesamte Abwicklung wie die Authentifizierung, Führerscheinkontrolle, Schlüsselausgabe, Fahrzeugrückgabe, Abrechnung, Fahrzeugzustand, Kostenabrechnung finden automatisiert und ohne persönlichen Kontakt statt. Ein solches Verfahren ist deutlich zeit- und kostensparender als der herkömmliche Prozess, bei dem Mitarbeiter des Autoverleihs zahlreiche einfache Routinetätigkeiten ausführen.

Steht dahinter immer dieselbe Blockchain, oder gibt es verschiedene?

In einem so innovativen Feld gibt es mittlerweile zahlreiche Produkte, wie etwa Ethereum und die dazu gehörenden Kryptowährung Ether, die nach Bitcoin die zweitgrößte Marktkapitalisierung besitzt. Mittlerweile gibt es einige Tausend Kryptowährungen mit einer Marktkapitalisierung von insgesamt mehreren 100 Milliarden US-Dollar. Nicht alle Blockchains verfügen über eine eigene Währung, so etwa Hyperledger Fabrics, ein Produkt, das von vielen Industrieunternehmen gefördert wird, aber zugleich auch Privatpersonen offen steht. Grundsätzlich wird unterschieden zwischen öffentlichen, allen zugänglichen, und zulassungsbeschränkten privaten oder konsortialen Blockchain-Systemen, die in der Regel von Unternehmen betrieben werden und deren Teilnehmerkreis von vornherein eingeschränkt wird. Denn die wenigsten Unternehmen wollen mit völlig Unbekannten Geschäfte machen.

Wie sicher sind Blockchains, schließlich speichern sie viele persönliche Daten, Überweisungen und "Kontostände"?

In einer Blockchain wie Bitcoin sind alle Speicherungen öffentlich einsehbar und nachvollziehbar, also auch die einzelnen Zahlungstransaktionen. Die Beteiligten einer solchen Transaktion, also Zahlungspflichtiger und Zahlungsempfänger, sind zwar nicht im Klartext erkennbar, sie hinterlassen jedoch im System eine digitale Spur: Es können zu ein und demselben Anwender gehörende Buchungen identi-

fiziert werden, ebenso lassen sich die Vorgängertransaktionen nachverfolgen, und damit rekonstruieren, woher das Geld stammt. Auch wenn dabei verschlüsselte Namen, also Pseudonyme verwendet werden, lässt sich mit mancher Zusatzinformation in dem ein oder anderen Fall auf die wahre Identität der Akteure schließen. Es gibt Kryptowährungen, etwa Monero, die auf starke Anonymität setzen, die Transaktionsfolge bewusst verschleiern, und daher häufig für den Zahlungsverkehr im Darknet eingesetzt werden. Aus Gründen des Speicherplatzes und der Performance, aber auch aufgrund des Datenschutzes werden nicht unbedingt alle Informationen eines Geschäftsvorfalles in der Blockchain abgelegt, sondern extern mit besonderen Verschlüsselungsverfahren verwaltet. Auch wenn die Blockchain starke kryptografische Verfahren benutzt, beziehen sich diese zunächst nur darauf, dass niemand die verwalteten Daten verändern kann. Die weiteren Anforderungen des Datenschutzes, wie etwa der Schutz personenbezogener Daten vor unberechtigtem Lesezugriff, sind durch die Entwickler und Betreiber des Systems eigens sicherzustellen. Dies gilt aber grundsätzlich für jedes, auch konventionelle IT-System.

Als Satoshi Nakamoto 2009 mit Bitcoin die erste Blockchain veröffentlichte, wurde die Technologie gehyped. Dann flachte die Begeisterung etwas ab. Welche Bedeutung werden Blockchains in den nächsten zehn, 50 oder 100 Jahren haben, wie werden sie unseren Alltag verändern?

Es ist nicht ungewöhnlich, dass bei technologischen Innovationen die öffentliche Aufmerksamkeit und die mit ihnen verbundenen Erwartungen in einer ersten Phase zu stark ausgeprägt scheinen und danach abflachen. Natürlich kann ich nicht hellsehen, doch ich gehe davon aus, dass die Blockchain-Technologie eine wesentliche Komponente in der digitalen Transformation leisten wird. Nicht einzig und allein, sondern gerade zusammen mit anderen Schlüsselthemen wie Big Data und Künstliche Intelligenz. Der Einfluss dieser Technologie auf die gesellschaftlichen Strukturen und auf unser Selbstverständnis wird zunehmen.

Gibt es auch Kritik an der Blockchain-Technologie?

Kritische Stimmen gibt es viele. Die datenschutzrechtlichen Bedenken wurde ja bereits genannt. Hinzu kommt der enorme Energieverbrauch des in Bitcoin realisierten Konsensmechanismus (mehrere hundert Kilowattstunden pro Transaktion). Kritisiert wird auch, dass Bitcoin für viele mehr ein Spekulationsobjekt darstellt und weniger ein Zahlungsmittel. Es gibt rechtliche und steuerliche Unklarheiten sowie geldwirtschaftliche Bedenken, weil die Kontrollfunktion des Staates über die Geldmenge beeinträchtigt wird. Diese Stimmen sind sicher nicht unberechtigt, ganz im Gegenteil: Sie fordern auf, die adressierten Probleme zu thematisieren und das Finden von Lösungen als Herausforderung zu begreifen. Kritiken sind immer auch ein Signal dafür, dass es sich um eine ernst zu nehmende Technologie mit Potential handelt. Man muss aber auch umgekehrt zulassen, dass die Blockchain-Technologie selbst als Kritik verstanden werden kann, nämlich als unmittelbare Reaktion auf die Finanzkrise und das sie mitverursachende Versagen institutioneller und staatlicher Organe.