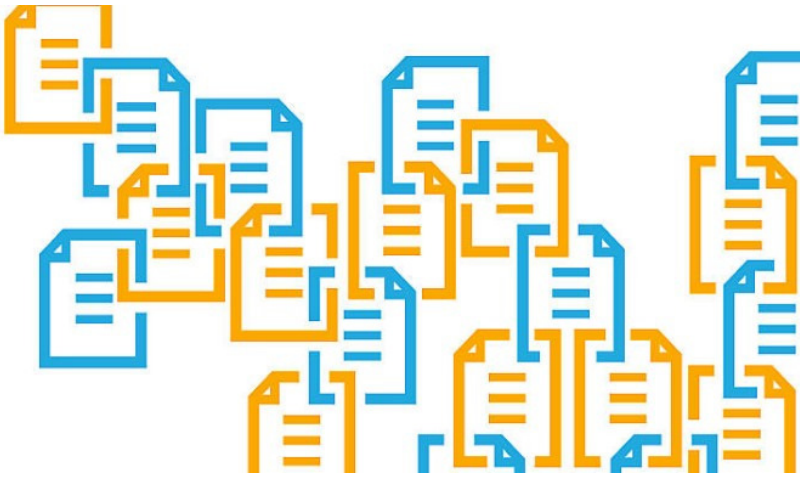
Frankfurter Allgemeine | 29.11.2020 - Aktualisiert: 30.11.2020, 10:57 Uhr
https://www.faz.net/-ikh-a60de

Zukunft der Computer

Bitcoin – Blockchain – Boom

Der jüngste Kursanstieg der Kryptowährung lenkt den Blick auf eine Technologie, die gewaltiges Potential hat: Es geht um sichere Lieferketten, den digitalen Euro und mehr. Ein Gastbeitrag.

Von WOLFGANG PRINZ



© F.A.Z.

Neue Hoffnung für die Blockchain: Kommt diesmal der Durchbruch?

Als sich der Bitcoin vor wenigen Jahren innerhalb kurzer Zeit von 300 auf mehr als 17.000 Euro verteuerte, wurde ihm und anderen Kryptowährungen, aber auch der darunterliegenden Blockchain-Technologie eine große Zukunft vorhergesagt: Dies werde einmal den Zahlungsverkehr revolutionieren und womöglich Notare oder Grundbuchämter ersetzen. Mit sogenannten „Smart Contracts“ sollten „Dezentralisierte Autonome Organisationen“ (DAO) geschaffen werden, die nach vorgeschriebenen und von Vertragspartnern abgestimmten Regeln transparent und nicht korrumpierbar Finanztransaktionen durchführen. Ende 2017 war das gewesen.

Die Ernüchterung folgte rasch. Der Wert dieser Anlagen verminderte sich, zahlreiche Projekte scheiterten. Aktuell steigt indes nicht nur der Bitcoin-Kurs wieder, sondern hat die Blockchain in Forschungsinitiativen, Umsetzungsprojekten und vielen Strategiepapieren einen festen Platz erobert.

Denn nach wie vor wecken wichtige Eigenschaften dieser Technologie großes Interesse: Erstens sind Transaktionen, die in einer Blockchain gespeichert wurden, nachträglich nicht mehr manipulierbar. Dabei muss es sich nicht ausschließlich um Finanztransaktionen von Kryptowährungen handeln, dort können auch Dokumente oder Produktionsdaten gesichert werden.

Zweitens wird die Verwaltung der Blockchain-Inhalte nicht von einer einzelnen Instanz

durchgeführt, sondern von einem Netzwerk miteinander kooperierender Knoten. Alle Knoten verfügen über die nach einem Konsensverfahren abgestimmten Transaktionen. Damit ist nicht mehr ein einzelner Intermediär wie eine Bank, ein Treuhänder oder ein Plattformanbieter für eine Dienstleistung zuständig und verantwortlich dafür, die Daten zu verwalten und ihre Unverfälschtheit sicherzustellen – sondern alle an dem Netzwerk beteiligten Partner. Entsprechend entfällt die Abhängigkeit von einem Anbieter. Das Blockchain-Konzept setzt auf ein dezentral betriebenes Ökosystem anstelle eines zentral betriebenen Plattformmodells.

Vertrauen müssen sich die Partner nicht

Drittens ist es schließlich mit dieser Technologie möglich, einfache Prozessschritte mittels „Smart Contracts“ zu automatisieren. Smart Contracts, die auch Chain-Code genannt werden, sind kleine Programme, die wie die Daten in einer Blockchain nicht manipulierbar sind. Damit lassen sich Regelwerke oder abgeschlossene Verträge automatisieren. Das Verfahren garantiert, dass kein Partner nachträglich einmal getroffene Regelungen wie zum Beispiel Provisionsanteile oder Zahlungsbedingungen im Programmcode ändern kann, die an eine digital überprüfbare Bedingung wie das Eintreffen einer Lieferung gebunden sind.

Aus diesen Eigenschaften lassen sich wiederum unmittelbar Kriterien ableiten, nach denen Anwendungsfälle bewertet werden können: Die Blockchain-Technologie ist dann sinnvoll, wenn Daten manipulationssicher und nachvollziehbar in einem Partnernetzwerk verwaltet werden müssen. Ein solches Partnernetzwerk kann aus den Unternehmern einer Wertschöpfungskette bestehen, die darüber Liefer- und Produktionsdaten austauschen, oder aus Unternehmen einer Branche, die beispielsweise Mobilität anbieten und über eine Blockchain Tickets und anteilige Dienste abrechnen.

Gegenseitig vertrauen müssen sich die Partner dank dieser Technik übrigens nicht notwendigerweise. Und kein Intermediär und keine zentrale Plattform braucht die Funktion einer Clearingstelle zu übernehmen.

Der Blockchain-Ansatz stellt im Bereich der Unternehmen infolgedessen eine neue Kooperations-Technologie dar. Ein Treiber dieser Entwicklung ist die in den vergangenen Jahren entstandene Vielfalt. Der Betrieb des Bitcoin-Netzwerks ist wegen seines auf der Lösung eines Kryptorätsels beruhenden Konsensverfahrens (der sogenannte Proof of Work) sehr rechenintensiv. Da mit der Lösung des Rätsels und dem damit erworbenen Recht, einen neuen Block mit Transaktionen an die Blockchain anzufügen, auch eine finanzielle Belohnung in Form von neu geschaffenen Bitcoins verbunden ist, entstand ein Wettlauf um immer leistungsfähigere Rechnerknoten. Das hatte seinerseits einen steigenden Energieverbrauch zur Folge. Neuere Blockchain-Ansätze zielen hingegen darauf ab, mittels alternativer Konsensverfahren oder Netzwerkstrukturen ohne aufwendige Rechnerkapazitäten auszukommen. Solche neuen Lösungen werden oft als Distributed Ledger Technology (DLT) bezeichnet.

Zeugnisse und Gesundheits-Zertifikate

Diese Entwicklungen bilden die Grundlage für aktuelle Lösungsangebote, die schon auf der Blockchain oder auf der DLT beruhen und die unterschiedlichsten Branchen adressieren. Die naheliegendste Lösung ist die sichere Prüfung von digitalen Urkunden und Zeugnissen im Ausbildungsbereich.

Da Bewerbungsprozesse in vielen Fällen digital erfolgen, werden auch Zeugnisse in digitalisierter Form eingereicht. Diese sind jedoch nicht nur problemlos fälschbar, es existieren auch Anbieter, die etwa Doktortitel gegen Gebühr verkaufen. Um sicherzugehen, müssten daher Personalabteilungen die Zeugnis-Originale und deren Herkunft prüfen. Dies unterbleibt allerdings oft, weil es Aufwand und Kosten verursacht.

Werden jedoch die digitalen Zeugnisse und Urkunden in einer „Zeugnis-Blockchain" registriert, lässt sich schnell und sicher prüfen, ob ein vorgelegtes digitales Zeugnis dem Original entspricht – und wer es wann und mit welcher Gültigkeit ausgestellt hat. Start-ups wie TrustCerts oder das von der Fraunhofer Gesellschaft gegründete digicerts.de-Netzwerk bieten so etwas an.

Deutschlandweit haben sich zudem verschiedene Anbieter und Nutzer im gerade von Kanzleramtschef Helge Braun ausgezeichneten „Netzwerk Digitale Nachweise" zusammengeschlossen, um über gemeinsame Standards digitale Zeugnisse zu fördern. Dazu gehören neben akademischen Institutionen auch Industrie- und Handelskammern (IHKs) oder die Bundesdruckerei. So hat die IHK München im Sommer ihren Absolventen ein digitales Zeugnis ausgehändigt, das über eine Blockchain nachprüfbar ist. Ganz aktuell basiert die Lösung der vom Digital Health Germany e.V. koordinierten Initiative zum digitalen Corona-Gesundheitszertifikat ebenfalls auf Blockchain-Technologie.

Personalisierte Tickets

Von der Verwaltung digitaler Zeugnisse ist der Schritt nicht weit zu Zertifikaten und Herkunftsnachweisen, speziell im Lebensmittelbereich. Beispiele dafür sind das vom Bundesforschungsministerium geförderte Projekt zu sicheren Lebensmittelketten (SiLKe), die von IBM mit Food Trust schon kommerziell angebotene Lösung für Herkunfts- und Lieferkettennachweise oder die Lösung des Anbieters Arxum für Lieferketten in der Automobilindustrie.

Die Blockchain-Technologie ermöglicht in diesen Fällen, innerhalb eines Netzwerks unterschiedlichster Partner den gemeinsamen Lieferkettenprozess und die dabei entstehenden Daten und Transaktionen nachvollziehbar und sicher zu digitalisieren. Die Beispiele illustrieren, dass die Technologie sinnvoll angewendet werden kann, wenn zu verhindern ist, dass Partner oder einzelne Beteiligte mit der Fälschung von Daten einen Wettbewerbsvorteil erzielen können.

In der Unterhaltungsbranche betrifft dies den Verkauf gefälschter Tickets oder die Unterbindung eines Schwarzmarkts mittels personalisierter Tickets. Die Tickets in einer Blockchain zu registrieren sichert die Originalität und macht den Eigentümerwechsel nachvollziehbar, wie dies etwa die Unternehmung TicketHash anbietet.

Hinter vielen Ansätzen verbirgt sich schlussendlich die Idee, digitale oder reale Gegenstände oder Eigentumswerte (Assets) als sogenannte Token in einer Blockchain zu repräsentieren. Token sind ein eineindeutiges digitales Abbild dieser Assets, und jeder Eigentumswechsel kann durch eine Transaktion des Tokens in der Blockchain dokumentiert und nachvollzogen werden. Token erlauben folglich die einfache Abbildung eines Eigentumswechsels.

Im Energiebereich wurde dies als einer der ersten Anwendungsfälle im lokalen Stromhandel in New York demonstriert. Gegenwärtig beschäftigt sich eine ganze Reihe von Vorhaben wie das von Siemens koordinierte Projekt Pebbles damit, auf einer Blockchain basierende

Lösungen für den lokalen Stromhandel zu entwickeln und zu erproben.

Dezentrale digitale Identitäten

Wird dieser Token-Ansatz erweitert, kann eine Blockchain auch den sogenannten digitalen Zwilling oder Schatten beispielsweise einer Maschine verwalten. Dieser digitale Schatten protokolliert den Lebenslauf einer Maschine oder eines Produkts und kann zusätzliche Dienste anbieten. Interessant daran ist, dass zum Beispiel Maschinenbauer auf diese Weise neue Dienste anbieten können zur verbrauchsgesteuerten Abrechnung oder Versicherung, ohne auf einen Plattformanbieter angewiesen zu sein.

Seit ungefähr zwei Jahren rückt mit der Verwaltung und Prüfung von digitalen Identitäten überdies ein neues Anwendungsgebiet in den Vordergrund. In vielen Fällen wird eine digitale Identität bestimmt durch eine E-Mail-Adresse, einen Google-Account oder einen Facebook-Account, mit dem sich Nutzer auch in anderen Diensten anmelden. Dies ist einerseits anwenderfreundlich, bedeutet aber auch, Daten über die Nutzung von Drittdiensten den Plattformen zugänglich zu machen, die diese Identität bereitstellen.

Aus diesem Grund gibt es Bestrebungen, digitale Identitäten dezentral und selbstbestimmt über eine Blockchain zu vergeben und überprüfbar zu machen, wie es etwa das im Jahr 2016 gegründete Sovrin-Netzwerk zum Ziel hat. Das World Wide Web Consortium (W3C) publizierte seinerseits im Jahr 2019 den ersten Entwurf und im August 2020 die erste Empfehlung für einen dezentralen Identitätsstandard, der das Format und die Prüfung digitaler Identitäten vereinheitlichen und damit für Interoperabilität zwischen Anwendungen sorgen soll.

Darüber hinaus ermöglicht der Standard die selektive Weitergabe von Identitätsinformationen. So kann bei der Freigabe des Geburtsdatums für eine Altersprüfung festgelegt werden, ob entweder das genaue Geburtsdatum, das Alter oder auch nur die Tatsache freigegeben wird, dass jemand ein Mindestalter erreicht hat. Ziel dabei ist die weitestgehende Selbstbestimmung der Nutzer über ihre Identitätsinformationen.

Dieser Standard geht zugleich darüber hinaus. Über das Konzept der Verifiable Credentials (VC) bietet er Institutionen die Möglichkeit, einer Person eine bestimmte Eigenschaft, Referenz oder einen Ausweis auszustellen. Dies kann im öffentlichen Bereich von einem Ausweis für die Stadtbücherei bis hin zu einem Führerschein reichen und im unternehmerischen Umfeld ein Betriebsausweis sein. Dieser könnte gleichzeitig als digital überprüfbare Berechtigung genutzt werden, um eine Maschine zu bedienen, sie zu warten oder bestimmte Dokumente zu signieren. Die Tatsache, dass mit diesem Standard Anwendungen übergreifend Identitäten geprüft werden können, hat schon dazu geführt, dass Unternehmungen wie Spherity, Blockchain-Helix oder der main-incubator entsprechende Lösungen anbieten.

Die Politik fördert die Blockchain-Technologie nicht nur in verschiedenen Forschungsprojekten, sondern auch in Umsetzungsinitiativen. Beispiele dafür sind das Blockchain-Grundgutachten des Verkehrsministeriums, das Bundesamt für Migration und Flüchtlinge (Bamf) mit der Entwicklung einer auf Blockchain basierenden Lösung für die behördenübergreifende Zusammenarbeit im Asylprozess, die Planungen des Wirtschaftsministeriums für eine weiterführende Studie über die Potentiale der Blockchain-Technologie oder des Umweltbundesamtes für eine Studie zum CO2-Zertifikate-Handel auf Blockchain-Basis.

In der Praxis erprobt der Automobilhersteller Ford mit der Stadt Köln neue Modelle zur Verringerung des Schadstoffausstoßes von Hybridfahrzeugen, die so gesteuert werden, dass sie in ausgewiesenen Stadtbezirken elektrisch fahren. Kontrolliert wird dies mittels GPS und der Protokollierung der Fahrzeugdaten in einer Blockchain, die zusätzlich über „Smart Contracts“ Anreize in Form von grünen Meilen an die Fuhrparkbetreiber verteilt, welche wiederum für andere Dienstleistungen eingetauscht werden können sollen.

Das Bundesfinanzministerium und das Justizministerium haben derweil ein Eckpunktepapier für ein Gesetz zur Einführung von elektronischen Wertpapieren vorgestellt. Nordrhein-Westfalen hat die Gründung eines Europäischen Blockchain-Instituts auf den Weg gebracht, das Blockchain-Netzwerk „govchain nrw“ aufgebaut und ein „Blockchain-Reallabor“ im Rheinischen Revier initiiert.

Mehrere Gründe für den digitalen Euro

Wichtigen Schub wird die Technologie nicht zuletzt durch die aktuellen Pläne der Europäischen Zentralbank erhalten für einen digitalen Euro. Wird diese Lösung für den allgemeinen Gebrauch bereitgestellt, begegneten die Euro-Notenbanker damit nicht nur Facebooks Libra-Plänen, sondern schafften zudem die Grundlage für einen programmierbaren Euro, mit dem Zahlungen nicht nur auf einfache Art und Weise automatisierbar werden, sondern auch winzige Beträge kostengünstig transferiert werden könnten. Diese Micro-Payments ermöglichen es, kleinste Dienstleistungen wirtschaftlich abzurechnen – zum Beispiel das kurze induktive Nachladen eines Akkus an der Ampel, die Bereitstellung einzelner Artikel einer Zeitung, die Freigabe von Datenpunkten eines Sensors oder die Zuschaltung von intelligenten Maschinenfunktionen abhängig vom Werkstück in der Industrie 4.0.

Diese Möglichkeiten schafften die Grundlage für neue Geschäftsmodelle, da sie Hersteller dazu befähigten, ihre Produkte mit digitalen Diensten anzureichern, die als Smart Contracts die Dienstleistung und die Gegenleistung (Bezahlung) sicher und nachvollziehbar integrieren. Plattformanbieter, die bislang diese Dienste anbieten, entfallen sowohl aus der Wertschöpfungskette als auch als (unerwünschter) Datensammler.

Der jüngste Kursanstieg des Bitcoins zeigt schließlich, welchen Effekt die Aufnahme einer Kryptowährung in normale Zahlungsprozesse haben kann. Nach dem „Bitcoin Halving“ im Mai, also der Halbierung der Anzahl der Bitcoins, die mit jedem neuen Block in Umlauf gebracht wurde, blieb der Kurs noch nahezu unverändert – obwohl viele Vorhersagen einen anschließenden Kursanstieg beinhalteten. Weil nun aber der Bitcoin von Paypal in Zahlungsprozessen genutzt werden kann, wird es nicht nur einfacher, diese Kryptowährung zu kaufen, es steigt auch die Nachfrage und damit der Preis.

All diese Beispiele zeigen, dass und wie die Blockchain-Technologie sich ausbreitet. Natürlich ist auch in Zukunft viel Forschungsarbeit und Entwicklungsarbeit zu leisten. Zugleich ist zu erwarten, dass Komponenten der Blockchain-Technologie Bestandteile von Alltagsgeräten und Smartphones werden, um Daten und Fakten zu sichern, Identitäten zu prüfen oder Bezahlvorgänge durchzuführen und abzusichern.

*Der Informatiker **Wolfgang Prinz** ist Professor an der RWTH Aachen und stellvertretender Leiter des Fraunhofer-Instituts für Angewandte Informationstechnik (FIT).*

Quelle: F.A.Z.