Das macht Blockchain

Die Technik hinter Bitcoin & Co.

„Blockchain“ gehört schon seit einiger Zeit zu den angesagtesten Buzzwords in der IT. Wir klären, ob dahinter nur Marketing-Gewäsch steckt oder ob Blockchains tatsächlich in der Lage sein könnten, ganze Industriezweige zu revolutionieren.

Von Hajo Schulz

Die Großen aus der IT-Branche sind dabei: Amazon bietet eine „Blockchain as a Service“, Microsoft hat ein Framework zum Implementieren von Blockchains vorgestellt, von IBM gibt es eine „Blockchain Platform“. Auch aus der Industrie kommen praktisch täglich Ankündigungen von Unternehmen zu dem Thema: Maersk erforscht, wie sich Blockchains in der Schiffslogistik einsetzen lassen, Daimler kooperiert mit der Landesbank Baden-Württemberg, um den Handel mit Anleihen per Blockchain zu automatisieren, der schwedische Staat hat in seiner Verwaltung bereits erste Blockchain-Projekte in Betrieb. Vor allem die Finanzindustrie setzt große Hoffnungen auf die Blockchain-Technik, die im Englischen auch unter dem Namen „Distributed Ledger“, also etwa „verteiltes Kontobuch“ bekannt ist.

Dieser Artikel erklärt, wie eine Blockchain überhaupt funktioniert und wo noch ungelöste Probleme bei ihrem Einsatz lauern. Ein wichtiges Merkmal von Blockchains ist, dass sie sogenannte Smart Contracts ermöglichen, also Verträge, die in Code gegossen sind und sich quasi von selbst erfüllen. Wie das funktioniert, steht im Folgeartikel ab Seite 108.

Was ist die Blockchain?

Technisch ist eine Blockchain zunächst einmal nicht viel mehr als eine verteilte Datenbank, die aus einer Kette von Datenblöcken besteht. „Verteilt“ bedeutet in diesem Zusammenhang, dass die Teilnehmer die Daten in einem Peer-to-peer-Netzwerk (P2P) miteinander austauschen, wobei auf jedem Knoten der komplette Datenbestand vorhanden ist.

Es existieren sowohl öffentliche als auch private Blockchains. Die bekannteste unter den öffentlichen ist die der Krypto-Währung Bitcoin. Auch Ethereum ist eine öffentliche Blockchain, die sich vor allem dadurch einen Namen gemacht hat, dass man dort anders als bei Bitcoin auch Smart Contracts hinterlegen kann. Im Prinzip kann bei öffentlichen Blockchains jeder mitmachen, alle Daten lesen und auch neue Einträge beisteuern. Im geschäftlichen Umfeld sind dagegen eher private Blockchains üblich. Sie existieren nur im Netzwerk und auf Rechnern der beteiligten Organisationen.

Eine der hervorstechendsten Eigenschaften der Blockchain ist ihre Robustheit gegen nachträgliche Änderungen einmal gespeicherter Daten. Deshalb kommt sie als Speichermedium überall da in Frage, wo Daten fortlaufend anfallen und manipulationssicher aufbewahrt werden müssen. Bei den Daten kann es sich um die Ein- und Auszahlungen eines Kontos genauso handeln wie etwa um die Einträge in eine digitale Krankenakte. Die Nutzdaten in der Bitcoin-Blockchain bilden die Transaktionen, also die Überweisungen von Währungsbeträgen zwischen den Teilnehmern.

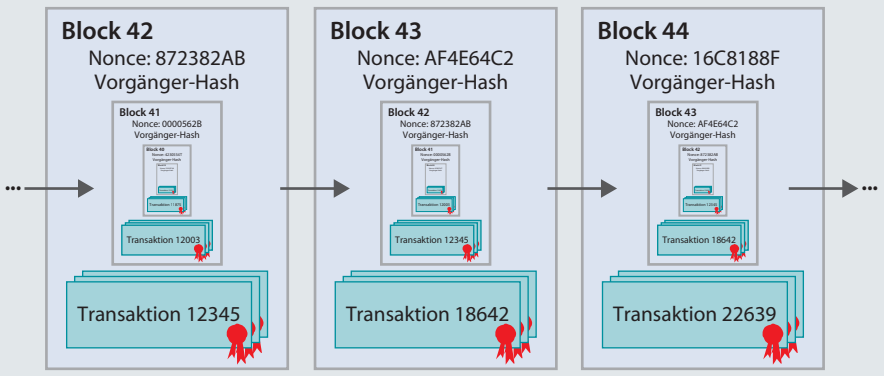
Das kleinste Element einer Blockchain ist immer ein Block. Er besteht neben einem Index und einem Zeitstempel aus mindestens drei Komponenten: den eigentlichen Daten, dem Hash des Vorgängerblocks und einem sogenannten Proof of Work.

Dadurch, dass jeder Block einen Hash seines Vorgängers enthält, sind die Blöcke untereinander verknüpft und schützen einander vor Manipulationen oder zufälligen Änderungen etwa durch Speicher- oder Übertragungsfehler: Würden sich die in einem Block gespeicherten Daten nachträglich ändern, wäre sein Hash ein anderer, was im nächsten Block sofort auffallen würde. Aber nicht nur das: Der Vorgänger-Hash ist ja Teil des Blocks und fließt deshalb in die Berechnung des eigenen Hash-Wertes ein, der wiederum im nächsten Block gespeichert ist. Wollte man also die Daten in einem bereits bestehenden Block ändern, müsste man die gesamte Kette ab diesem Punkt neu berechnen. Das ist zwar theoretisch möglich, aber umso aufwendiger und damit für potenzielle Betrüger unattraktiver, je weiter die zu manipulierenden Daten in der Historie der Blockchain zurückliegen.

Um derartige Manipulationen noch schwieriger und ab einem bestimmten Punkt schlicht unmöglich zu machen, kommt bei den meisten Blockchain-Implementierungen der Proof of Work ins Spiel: Hierbei handelt es sich um eine Zahl, die schwer zu berechnen, aber leicht

Das Blockchain-Prinzip

Jeder Eintrag einer Blockchain enthält außer den eigentlichen Daten einen Hash seines Vorgängerblocks. Einmal gespeicherte Daten ließen sich nur ändern, wenn man auch alle nachfolgenden Blocks neu berechnen würde. Dass das passiert, verhindern Verfahren wie „Proof of Work“, die die dazu nötige Rechenleistung in astronomische Höhen treiben.



nachzuprüfen ist. Realisiert wird das, indem man von dem Hash eines gültigen Blocks fordert, dass er einer bestimmten Regel gehorcht, beispielsweise nicht größer als eine festgelegte Obergrenze ist. Um einen neuen Block zu berechnen, muss ein Programm die Zahl, die den Proof of Work darstellt, so lange ändern und immer wieder einen neuen Hash berechnen, bis die Bedingung erfüllt ist. Solange der verwendete Hash-Algorithmus nicht kompromittiert ist, gibt es keinen anderen Weg, zu einem gültigen Block zu kommen, als das Durchprobieren immer wieder neuer Werte für diese Zahl. Im Bitcoin-Jargon wird die Zahl übrigens Nonce genannt – auch wenn diese Bezeichnung, die sich von „Number used once“ ableitet, in der Kryptografie eigentlich für eine Zufallszahl steht, die in bestimmten Protokollen als eine Art Einmalkennwort verwendet wird.

Durch Anpassen der Regel für gültige Blöcke kann man steuern, wie aufwendig die Hash-Berechnung werden soll. In der Bitcoin-Blockchain wird beispielsweise die Obergrenze für die Gültigkeit eines Hashes regelmäßig so angepasst, dass die Mitgliedergemeinschaft im Schnitt alle zehn Minuten einen neuen gültigen Block findet. Die Ethereum-Blockchain soll pro Minute um vier Blöcke wachsen. Der dort verwendete Hash-Algorithmus benötigt nicht nur Rechenleistung, sondern auch einige Gigabyte Speicher. Dadurch soll verhindert werden, dass sich gültige Blöcke mit Spezialhardware wie ASICs berechnen lassen – eine größere Investition in solche Hardware könnte die Mehrheit der Rechenleistung des gesamten Verbundes unter die Kontrolle einiger weniger Teilnehmer bringen und so die Stabilität der Blockchain gefährden.

Ob eine Blockchain intakt ist, kann jeder Teilnehmer mit überschaubarem Aufwand nachprüfen: Er muss dazu nur den Hash jedes Blocks neu berechnen, mit dem Vorgänger-Hash im nächsten Block vergleichen und prüfen, ob die Nonce die Gültigkeitsbedingung erfüllt.

Goldgräber

Das Fortbestehen einer öffentlichen Blockchain hängt davon ab, dass sich stets genug Teilnehmer finden, die neue Blöcke berechnen. Das wirft die Frage auf, wieso überhaupt jemand einer Blockchain seine Rechenleistung zur Verfügung stellen sollte.

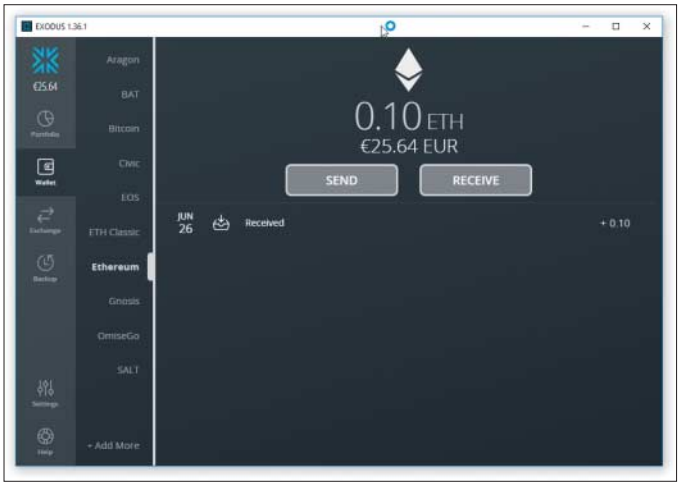
Beantworten lässt sich das ganz gut am Beispiel Bitcoin. Einige Erklärungen zur grundsätzlichen Funktionsweise von Krypto-Währungen sind dazu aber unerlässlich: Wer ein Bitcoin-Guthaben besitzt, kann einem anderen Nutzer einen bestimmten Betrag zukommen lassen, indem er eine kryptografisch abgesicherte Nachricht an das System schickt, die den Auftrag für eine entsprechende Überweisung enthält. Das P2P-Netzwerk verteilt diese Aufträge an alle Teilnehmer, die sich zum Berechnen neuer Blöcke angemeldet haben. Um einen neuen Block zu berechnen, wählt der Teilnehmer aus den bis dahin bei ihm aufgelaufenen Aufträgen diejenigen aus, die er verarbeiten will, verpackt sie in eine spezielle Datenstruktur, fügt den Hash des letzten ihm bekannten Blocks und eine Nonce hinzu und beginnt mit der Hash-Berechnung. Hat er nach wiederholtem Austausch der Nonce schließlich einen gültigen Block gefunden, sendet er ihn über das P2P-Netzwerk an alle anderen Teilnehmer. Durch das Anhängen des Blocks an die Blockchain werden die in ihm enthaltenen Aufträge zu gültigen Transaktionen.

Die Frage, warum sich jemand bereit erklären sollte, Blöcke zu berechnen, beantworten praktisch alle öffentlichen Blockchains damit, dass sie mit einem geldwerten Gut verknüpft sind, also irgendeiner Form digitalen Geldes. Wer einen neuen gültigen Block findet, wird dafür mit einem festgelegten Betrag dieser Währung belohnt. Im Bitcoin-System ist das so gelöst, dass derjenige, der einen neuen Block berechnet, eine Transaktion in den Block einbauen darf, die ihm aus dem Nichts eine bestimmte Summe an Bitcoins überweist. Durch diesen Prozess entstehen neue digitale Münzen, weshalb er auch Mining, also Bergbau genannt wird.

Da das Bitcoin-System so ausgelegt ist, dass die Gesamtzahl des jemals in Umlauf befindlichen digitalen Geldes beschränkt ist, wird die Belohnung, die Miner für das Errechnen eines neuen Blocks bekommen, im Lauf der Zeit immer kleiner. Damit sich das Schürfen trotzdem lohnt – es hält schließlich den Betrieb der Blockchain aufrecht –, können Auftraggeber von Transaktionen dem Miner, der sie in die Blockchain einträgt, eine Transaktionsgebühr zukommen lassen. Tatsächlich haben Bitcoin-Aufträge, die keine solche Gebühr ausloben, mittlerweile kaum noch eine Chance, in endlicher Zeit ausgeführt zu werden.

In einer öffentlichen Blockchain wie dem Bitcoin-Netzwerk kann im Prinzip jeder zum Miner werden und damit der Kette neue Blöcke hinzufügen. Die Teilnehmer kennen sich untereinander nicht, es herrscht auch kein Vertrauensverhältnis. Dass Manipulationen trotzdem praktisch unmöglich sind, stellt ein zweistufiges Verfahren sicher: Dafür, dass die Transaktionen prinzipiell gültig sind, sorgt in einem ersten Schritt die Pflicht, Aufträge kryptografisch zu signieren. Trotzdem kann es theoretisch passieren, dass ein Teilnehmer einen Block berechnet, in dem eine Transaktion steckt, die ein bestimmtes Guthaben von User A an User B überträgt, und gleichzeitig ein zweiter Miner einen Block erzeugt, dessen Transaktionen dasselbe Guthaben an User C überweist.

Solche Kollisionen räumt das Netzwerk folgendermaßen aus dem Weg: Sobald ein Miner einen gültigen Block errechnet hat, schickt er ihn per Broadcast an alle anderen Mitglieder des P2P-Netzes. Wer so einen Block empfängt, prüft zunächst dessen Gültigkeit. Ist der Block



Wer nur ein Krypto-Guthaben verwalten und Überweisungen tätigen will, benötigt keinen kompletten Blockchain-Client. Eine sogenannte Wallet-Anwendung wie das hier gezeigte Exodus genügt.

in Ordnung, hängt der Empfänger ihn an seine lokale Kopie der Blockchain an, löscht die enthaltenen Transaktionen aus seiner Liste der zu verarbeitenden Aufträge und beginnt, aus den verbleibenden Einträgen einen neuen Block zu berechnen. Trudeln mehrere von anderen Minern berechnete, als gültig in Frage kommende Blöcke gleichzeitig ein, muss man zwei Fälle unterscheiden: Im ersten besitzen alle denselben, bereits als gültig erkannten Vorgängerblock. Mit welchem es dann weitergeht, kann der Empfänger nach eigenem Gutdünken entscheiden; meist nimmt er den ersten.

Dasselbe gilt, wenn die empfangenen Blöcke zwar unterschiedliche Vorgänger besitzen, aber alle dieselbe Distanz zum letzten gemeinsamen Vorgänger aufweisen. Dann ist ein sogenannter Fork passiert: Die Blockchain hat sich in mehrere Zweige aufgeteilt. Früher oder später wird aber einer der Äste länger als die anderen werden. Dann werden die kürzeren Zweige aus der Blockchain entfernt und die darin enthaltenen Transaktionen verworfen. Auch die Belohnung für die Miner, die an diesem Ast gerechnet haben, ist perdu. Auf diese Weise setzt sich früher oder später der Zweig durch, in den die meiste Rechenleistung eingeflossen ist: Man geht davon aus, dass hinter ihm auch die Mehrheit der Teilnehmer steckt. Auf diese Weise wird ausgeschlossen, dass einige wenige betrügerische Miner die gesamte Blockchain auf Dauer beeinflussen können.

Längere Forks treten in der Bitcoin-Blockchain nur sehr selten auf. Die meisten Teilnehmer gehen deshalb davon aus, dass eine Transaktion sicher bestehen wird, wenn sie in einem Block steckt, der mindestens sechs Nachfolger besitzt. Spätestens dann werden beispielsweise Bargeldbeträge ausgezahlt oder per Bitcoin bezahlte Bestellungen abgewickelt. Dass etwa ein Wirt, der eine Zahlung in Bitcoin entgegennimmt, auf dem Deckel sitzen bleibt, weil die dazugehörige Transaktion in einem letztendlich verworfenen Zweig der Blockchain gelandet ist, passiert trotzdem äußerst selten: Wird der Auftrag von der Mehrheit der Miner als legitim erkannt, kommt er ja im Normalfall in allen Zweigen an. Er landet im Zweifel nur in einem anderen Block.

Konsens

Das Proof-of-Work-Konzept ist nicht ohne Probleme; der größte Kritikpunkt dürfte der Ressourcenverbrauch sein: Unzählige Miner verheizen Rechenleistung und damit elektrische Energie, um Hashes von Blöcken zu berechnen, die letztendlich nicht in der Blockchain landen und verworfen werden. Andere Blockchain-Implementierungen verwenden deswegen alternative Verfahren, um zwischen den Teilnehmern eine Einigung über den nächsten gültigen Block zu erzielen.

Ein relativ weit verbreiteter sogenannter Konsens-Algorithmus heißt Proof of Stake (Beweis der Beteiligung). Wo er zum Einsatz kommt, müssen Teilnehmer, die neue Blöcke berechnen und bestätigen wollen, eine Einlage in Form der mit der Blockchain verbundenen Digitalwährung leisten. Die Wahrscheinlichkeit, zufällig als nächster „Validator“ ausgewählt zu werden, steigt mit der Höhe dieser Sicherheitsleistung. Ein Problem beim Proof-of-Stake-Verfahren besteht darin, dass einzelne Teilnehmer oder kleine Gruppen durch eine hohe Einlage viel Macht erlangen und Blöcke zu ihren Gunsten manipulieren könnten. Um das zu verhindern, sehen manche Proof-of-Stake-Implementierungen nicht nur Belohnungen für das Berechnen neuer gültiger Blöcke vor, sondern bestrafen Teilnehmer per Abzug von der Einlage, wenn sie Blöcke eines Fork berechnen, der schließlich verworfen wird.

In Blockchain-Projekten mit beschränktem Zugang und einem gewissen Maß an Vertrauen zwischen den Teilnehmern kommen weitere Konsens-Algorithmen mit noch weniger Overhead in Betracht. Bei deren Auswahl kann man sich zunutze machen, dass – anders als bei öffentlichen, unbeschränkten Blockchain-Netzen – an privaten Blockchains immer nur eine begrenzte Zahl aktiver Nutzer teilnimmt.

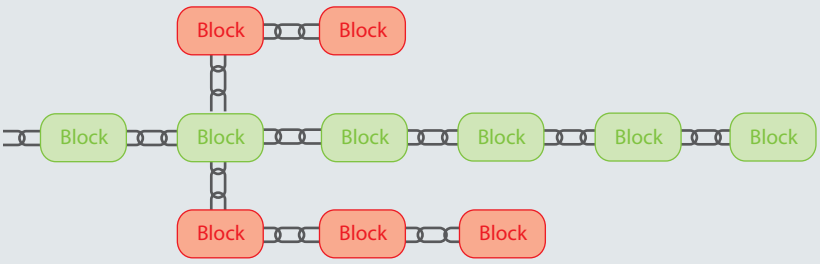
Eines der in der Praxis verwendeten Verfahren heißt „Practical Byzantine Fault Tolerance“ (PBFT), übersetzt „praktische Toleranz gegen byzantinische Fehler“. Der Name stammt von einer Legende, der zufolge im Jahr 1453 das osmanische Heer Konstantinopel belagerte. Die Generäle, die die einzelnen Armeen befehligten, konnten nur über Boten miteinander kommunizieren, um sich darüber abzustimmen, ob die Stadt an einem bestimmten Tag anzugreifen sei. Um erfolgreich zu sein, mussten sich an einer Attacke möglichst viele Armeen beteiligen. Unter den Generälen gab es aber Verräter, sodass sich keiner sicher sein konnte, welchen eintreffenden Nachrichten er vertrauen konnte. Betrachtet man das Problem mathematisch, kommt man zu dem Ergebnis, dass eine verlässliche Einigung auf einen Angriff immer dann möglich ist, wenn weniger als ein Drittel der Generäle sie sabotieren.

Der PBFT-Algorithmus verwendet replizierte Zustandsautomaten, die über Änderungen ihres Status per Nachrichtenaustausch abstimmen. Benutzt wird er zum Beispiel im Hyperledger Fabric, einem Blockchain-Framework, das die Linux Foundation pflegt und Interessierten zum Implementieren eigener Blockchain-Anwendungen zur Verfügung stellt. Glaubt man den Erfindern, erzeugt der PBFT-Algorithmus nur minimalen Overhead bei der Kommunikation der Netzwerkknoten untereinander.

Zwei in der Finanzindustrie gern eingesetzte Varianten des PBFT-Algorithmus

Verzweigungen beschnitten

In der Bitcoin-Blockchain werden neue Blöcke asynchron und von vielen Teilnehmern parallel berechnet. Finden mehrere Miner gleichzeitig einen Block, kann ein sogenannter Fork passieren: Die Blockchain teilt sich in mehrere Äste auf. Über kurz oder lang wird sich aber ein Zweig als der längste durchsetzen. Kürzere werden dann verworfen. Ein Angreifer müsste mehr Rechenleistung als alle ehrlichen Miner zusammen haben, um mit einer manipulierten Kette die echte zu überholen.



Normale PC-Technik kann beim Bitcoin-Mining nicht mehr mithalten. Professionelle Miner benutzen ASIC-Rechner wie den hier gezeigten „Antminer S9“ von Bitmain.

hören auf die Namen Ripple und Stellar. Sie ermöglichen prinzipiell unendlich viele Netzknoten, setzen aber voraus, dass jeder Teilnehmer ausgewählten Partnern voll vertraut und die so gebildeten Gruppen einander überlappen. Die beiden Algorithmen unterscheiden sich in der Art und Weise, wie die Abstimmungen der Knoten über den nächsten validen Block stattfinden. Ihnen ist gemein, dass sie viele Transaktionen in kürzester Zeit verarbeiten können und diese schnell final in die Blockchain übernehmen.

Probleme

Die ideale Blockchain weist eine niedrige Latenz auf, lässt neue Blöcke schnell final werden, verarbeitet viele Transaktionen in kurzer Zeit und skaliert gut auf viele Teilnehmer. Diese Anforderungen schließen einander aber teilweise aus: Konsensmodelle, die zu schnellen Entscheidungen führen, sind in der Regel nur für eine beschränkte Teilnehmerzahl geeignet und lassen sich nicht auf Netze mit potenziell unendlich vielen Knoten übertragen. Konsensmodelle, die versuchen, die genannten Anforderungen unter einen Hut zu bringen, funktionieren nur dann, wenn die Teilnehmer zumindest ausgewählten Partnern voll vertrauen.

Bevor sich Blockchains auf breiter Front im geschäftlichen Umfeld durchsetzen, sind aber noch andere Probleme zu lösen. So funktioniert eine Blockchain nur, wenn jeder P2P-Knoten stets die komplette Datenbank vorhält. Es gibt keine Löschung von Daten, die Blockchain wächst also ständig. Das mag für ein paar Jahre gut gehen und auch gewollt sein, auf längere Sicht kann der Overhead obsolet gewordener Daten aber zum Bremsklotz werden. Zudem wird es im Lauf der Zeit immer schwieriger, die Integrität der Blockchain zu verifizieren, weil man dazu ja von Anfang an Block für Block die Hashes nachrechnen muss.

Wer heute ein Blockchain-Projekt aufsetzen will, sieht sich einer breiten Auswahl von Dienstleistern und Frameworks gegenüber. Das ist im Prinzip zu begrüßen, bedeutet aber auch, dass man sich relativ früh für eine Implementierung entscheiden muss. Sollte sich herausstellen, dass man aufs falsche Pferd gesetzt hat, ist ein nachträglicher Umstieg so gut wie unmöglich, denn es fehlt an allgemein anerkannten Standards.

Aus ökologischer Sicht sind Blockchains, die zur Konsensfindung Proof of Work verwenden, eine Katastrophe: Experten schätzen, dass das Bitcoin-Netzwerk derzeit insgesamt mindestens ein Gigawatt mit dem Berechnen von Hashes verheizt – das ist etwa die Leistung eines handelsüblichen Kernkraftwerks. Bei durchschnittlich sechs Blöcken pro Stunde verbraucht das Berechnen eines einzigen Blocks also rund 167 MWh. In Deutschland würden dafür rund 48.700 Euro an Stromkosten anfallen. Miner erhalten für einen neuen Block gegenwärtig 12,5 Bitcoins als Belohnung; in Echtgeld entsprach das bei Redaktionsschluss für diesen Artikel knapp 60.000 Euro. Ein deutscher Miner macht also mit einem gefundenen Block immer noch über 10.000 Euro Gewinn. Dieses große Los zu ziehen ist aber äußerst unwahrscheinlich. Um den Gewinn zu maximieren, betreiben professionelle Miner ihre Mining-Farmen in Gegenden, wo Strom besonders günstig ist, etwa in China, Russland oder Island.

Zusätzlich zum Stromverbrauch muss man in die Ökobilanz auch einbeziehen, dass beim Bitcoin-Mining mit normalen Prozessoren oder Grafikkarten mittlerweile kein Blumentopf mehr zu gewinnen ist. Spezialhardware, die das Berechnen von Hashes mit ASICs erledigt, ist deutlich schneller. Erfahrungsgemäß überholt aber die nächste Generation an Mining-Hardware jeweils aktuelle Geräte innerhalb weniger Monate und macht sie dadurch zu Elektronikschrott.

Was geht

Allen Problemen zum Trotz setzen zahlreiche Unternehmen auf die Blockchain. Vor allem die Finanzindustrie erwartet, dass sich damit Geschäfte rationalisieren lassen: Wo das Vertrauen zwischen Geschäftspartnern durch Technik garantiert werden kann, braucht es keine Notare oder Treuhänder mehr, die darüber wachen, dass alle Beteiligten ihren Pflichten nachkommen. Eine passive Blockchain, die als reiner Datenspeicher fungiert, reicht dazu allerdings nicht aus. Zusätzlich braucht es Smart Contracts, also Programmcode, der manipulationssicher in der Blockchain gespeichert ist und garantiert ausgeführt wird, sobald bestimmte Ereignisse eintreten. Details zu Smart Contracts liefert der nachfolgende Artikel.

Eine weitere Branche, die große Hoffnungen auf die Blockchain setzt, ist die Logistik-Industrie. Hier geht es vor allem darum, lückenlos und verzögerungsarm nachzuvollziehen, wo sich eine Sendung gerade befindet und welchen Weg sie genommen hat.

Echten Zusatznutzen auch für Verbraucher könnten Blockchains in der Nahrungsindustrie bringen: Sie sind das ideale Speichermedium, um den Weg von Lebensmitteln vom Erzeuger bis zum Einzelhändler nachzuvollziehen. Dass sich jeder Landwirt und jeder Hersteller an so einem System beteiligt, ist aber noch Zukunftsmusik. Mit Nestlé hat immerhin ein Branchenriese damit begonnen, die Herkunft der Zutaten für seine Produkte per Blockchain zu verfolgen.

Viel mehr als erste Pilotprojekte stecken hinter den genannten Beispielen gegenwärtig aber noch nicht. Sie sollen den Nutzen und die Probleme beim Einsatz von Blockchains ausloten. Ob sich die erhofften Vorteile in der Praxis erreichen lassen, steht in den Sternen. Die Marktforscher von Gartner sehen die Blockchain-Technik denn auch in ihrem diesjährigen „Hype Cycle“ am Übergang zwischen dem „Gipfel der überzogenen Erwartungen“ und dem „Trog der Enttäuschungen“ und schätzen, dass noch fünf bis zehn Jahre ins Land gehen, bevor sie das „Plateau der Produktivität“ erreicht.

Das von manchem Anbieter versprochene Allheilmittel, mit dem sich jedes Unternehmen modernisieren lässt, ist die Blockchain jedenfalls nicht. Wie bei jedem Marketing-Hype muss man schon genauer hinsehen, hinter welchen Ankündigungen tatsächlich eine Revolution steckt und wo einfach nur ein Buzzword verwendet wird, um Modernität zu suggerieren. *(hos@ct.de)* c't