

KRYPTOTECHNOLOGIEN IN DER PRAXIS

Blockchains im Testlauf



Blockchains tauchen immer häufiger in allen Bereichen auf. Unternehmen erhoffen sich dadurch Transparenz, Effizienz und Sicherheit. Ob die Technik das auch einhalten kann, muss sich erst noch zeigen. ■ NICOLAI SCHWARZ

Viele Unternehmen experimentieren derzeit mit Blockchains. Die Initiativen gehen quer durch alle Branchen, von der Lebensmittelindustrie über Energieunternehmen hin zum Finanzsektor. Blockchains stecken zwar zweifelsohne noch in den Kinderschuhen, aber die Unternehmen erhoffen sich auf Dauer einige Vorteile. Die Technologie ist recht komplex und, je nachdem, wie tief Sie in die Technik und Mathematik einsteigen möchten und welche Vorerfahrungen Sie haben, auch schwer verständlich.

Prinzip einer Blockchain

Eine Blockchain ist eine dezentralisierte Datenbank. Oft wird sie mit einem Kassenbuch verglichen. Dort können verschiedene Daten bzw. Transaktionen gespeichert werden. Nicht nur für Geld, das von Nutzer A an Nutzer B überwiesen wird, sondern zum Beispiel auch, wer welche Ware an wen geliefert hat oder wer wieviel Strom erzeugt oder verbraucht hat. Alle Daten werden der Reihe nach in der Blockchain abgespeichert, wodurch diese auch immer länger wird. Das Kassenbuch bzw. die Blockchain

liegt aber nicht zentral auf dem Server einer Bank, sondern ist dezentral im Netz verteilt – auf den Rechnern der Nutzer, die an der Blockchain teilnehmen. Neue Transaktionen werden zusammengefasst und als neue Blöcke der Blockchain angehängt. Diese werden in den Kassenbüchern jedes einzelnen Nutzers eingetragen. Die Blöcke selbst werden kryptografisch miteinander verknüpft (siehe Infografik). Dafür werden Hashwerte erzeugt. Damit lassen sich lange Zeichenketten auf kurze Zeichenketten abbilden. Ein oft genutztes

Verfahren ist SHA256 (für: *Secure Hash Algorithm*). Aus dem Satz „The quick brown fox jumps over the lazy dog.“ ergibt sich der SHA256-Wert: EF537F25C895BFA-782526529A9B63D97AA631564D5D789C2B-765448C8635FB6C. Das Ergebnis ist hierbei immer 64 Zeichen (bzw. 256 Bit) lang. Ändert sich auch nur ein Zeichen in der ursprünglichen Zeichenkette, ergibt sich ein völlig anderer Hashwert. Für die Blockchain werden verschiedene Hashwerte genutzt. Zunächst werden Hashwerte aus den Transaktionen bzw. Informationen innerhalb eines neuen Blocks erzeugt. Diese werden zusammen mit dem Hash des vorherigen Blocks im Header des aktuellen Blocks zusammengefasst. Aus allen Daten im Header wird ein weiterer Hashwert gebildet, der in den nächsten Block einfließt. Auf diese Weise sind alle Blöcke kryptografisch miteinander verknüpft. Die Blöcke bilden eine Kette, daher also der Name: Blockchain.

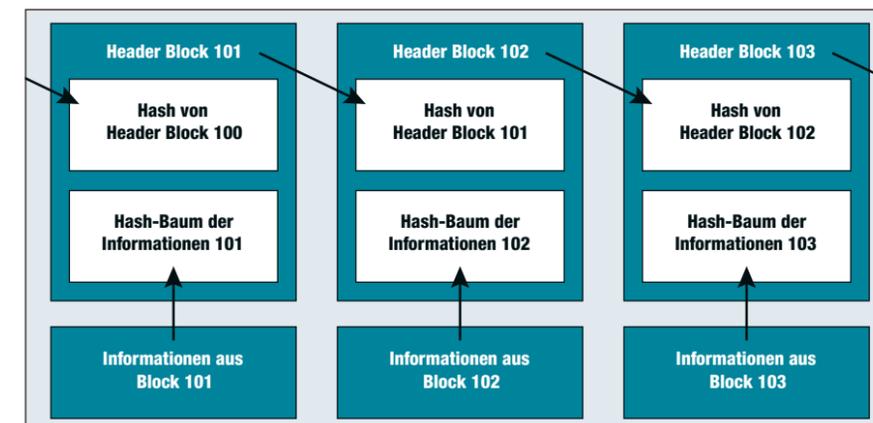
Das Prinzip sorgt für Sicherheit. Es kommen neue Blöcke hinzu, aber alte Blöcke bleiben unverändert in der Blockchain gespeichert. Sie können nicht einfach einen einzelnen Block austauschen, weil dann der Hashwert im folgenden Block nicht mehr stimmt. Wer einen Block manipulieren wollte, müsste ab diesem Block auch den Rest der Kette ändern. Da aber andere Nutzer die Blockchain auch gespeichert haben, können sie Unterschiede leicht feststellen.

Die Blockchain dient also dazu, Transaktionen lückenlos und unveränderbar dezentral zu speichern. Die Inhalte der Blöcke in der Bitcoin-Blockchain können Sie im Netz nachlesen, zum Beispiel auf blockchain.com. Dort sehen Sie auch, welcher Miner den Block erzeugt hat. Die Transaktionen selbst können Sie ebenfalls nachschlagen. Allerdings sehen Sie nur, welche Adresse an welche Adresse überwiesen hat. Die Adressen sind hier nur Zeichenfolgen. Sie können die Zeichenfolgen erst einmal keiner realen Person zuordnen – solange es nicht andere Hinweise gibt, welche Person sich hinter der Zeichenfolge verbirgt.

Konsensverfahren

Nun stellt sich die Frage, wie neue Transaktionen genau hinzugefügt werden. Schließlich ist es wenig sinnvoll, wenn jeder Nutzer einfach neue Daten einfügen dürfte. Dann könnte nämlich jeder beliebige Transaktionen erfinden. Bei einer Bank oder Paypal prüft eine zentrale Stelle die Rechtmäßigkeit der Transaktionen. Aber wie funktioniert das bei einer dezentralen Blockchain? Die Nutzer müssen sich irgendwie einigen,

Das Grundprinzip einer Blockchain



Jeder Block einer Blockchain enthält eine Reihe von Informationen. Von diesen werden die Hashwerte ermittelt und in einem Hash-Baum im Header des Blocks abgelegt. Zusätzlich enthält der Header den Hashwert des letzten Blocks. Aus dem Header wird nun wiederum ein eigener Hashwert berechnet, der Teil des nächsten Blocks wird. Dadurch sind die einzelnen Blöcke miteinander verknüpft und bilden eine Kette.

Blöcke	Transaktionen	Miner	Cost
552333	7 minutes	368	SECOIN
552332	17 minutes	583	Unknown
552331	19 minutes	290	Unknown
552330	35 minutes	363	Bitcoin.com
552329	37 minutes	1804	Unknown

Auf blockchain.com können Sie sich alle Blöcke der Bitcoin-Blockchain im Detail ansehen.

wer einen neuen Block hinzufügen darf. Das geschieht über ein Konsensverfahren. Hier gibt es mehrere Möglichkeiten. Das populärste Verfahren nennt sich *Proof of Work* und kommt zum Beispiel bei Bitcoins zum Zuge. Hier konkurrieren die Nutzer der Blockchain miteinander, wer den nächsten Block hinzufügen darf. Dazu muss eine komplexe Rechenaufgabe gelöst werden. Genau genommen werden einfach der Reihe nach verschiedene Zahlen durchprobiert, bis die aktuelle Aufgabe gelöst wurde (siehe Infokasten). Der Schnellste darf seinen Block hinzufügen. Das Verfahren kostet Zeit und eine Menge Strom, weil die so genannten Miner ggf. die gleichen Rechnungen durchführen.

Ein anderes Verfahren nennt sich *Proof of Stake*. Hier wird mit einem gewichteten Zufall ermittelt, welcher Teilnehmer im Netzwerk den nächsten Block erzeugen darf.

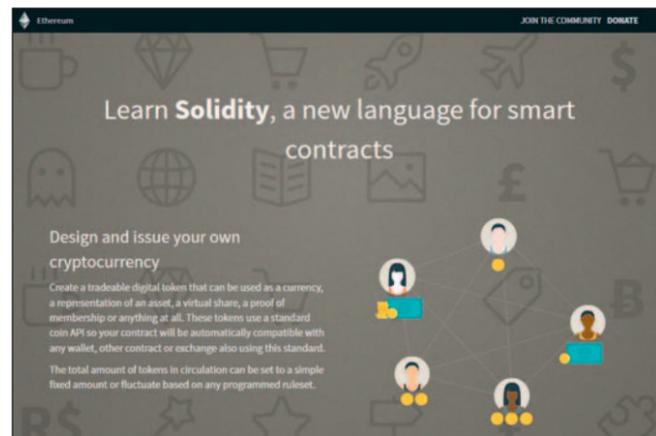
So werden etwa Teilnehmer bevorzugt, die schon länger teilnehmen. Bei diesem Verfahren können neue Blocks sehr schnell erzeugt werden. Es gibt aber auch weitere Verfahren wie *Proof of Capacity*, *Proof of Burn* und *Proof of Activity*.

Blockchain ist also nicht gleich Blockchain. Neben verschiedenen Konsensverfahren können auch unterschiedliche Hashfunktionen zum Einsatz kommen. Ebenso muss eine Blockchain nicht unbedingt öffentlich sein. Bei *Permissioned Blockchains* wird beschränkt, wer darauf zugreifen bzw. Inhalte lesen und hinzufügen darf. Bei solchen Blockchains haben eine oder mehrere Parteien die Kontrolle über das System.

Smart Contracts

Im Zusammenhang mit Blockchains ist manchmal auch von Smart Contracts die Rede. Das sind Computerprogramme, die

nach dem Prinzip Wenn-Dann ablaufen. Ein einfaches Beispiel wäre: Wenn Datum A erreicht ist, dann überweise die Miete in Höhe von B an Person C. Oder Sie wenden das Prinzip auf Crowdfunding an: Aktuell können Unterstützer zum Beispiel auf Kickstarter ein Projekt mit einer bestimmten Summe unterstützen. Wird das Finanzierungsziel erreicht, zieht Kickstarter die einzelnen Geldbeträge ein und überweist den Betrag an den Leiter des Projektes. Wenn Sie das Schema als Smart Contract umsetzen, fiele Kickstarter als Mittelsmann weg. Unterstützer könnten ihr Interesse direkt beim Projekt anmelden. Zu einem gegebenen Zeitpunkt ist die gewünschte Zielsumme entweder erreicht oder auch nicht – und dementsprechend überweist das Programm selbstständig die einzelnen Summen an das Projekt oder eben nicht. Die Befürworter der Technologie sehen einige Vorteile in dem System. Zunächst einmal fällt der Mittelsmann weg, was die Kosten senkt. Außerdem kann das Programm die Bedingungen sofort auswerten; alles läuft also schneller ab. Und da die Smart Contracts in der Regel mit Blockchains kombiniert werden, können alle Beteiligten den Code und die Transaktionen selbst prüfen, so dass es transparenter und sicherer ist. Aber die Smart Contracts haben auch ein paar Nachteile. Wenn ein Smart Contract beispielsweise einen Fehler beinhaltet, bleibt dieser für immer bestehen. Denn in der Blockchain werden alte Daten ja absichtlich nicht verändert. Sie müssten hier im Smart Contract die Möglichkeit vorsehen, zu einem neuen, korrigierten Smart Contract wechseln zu können. Außerdem können Sie nicht ohne weiteres mit einem Smart Contract interagieren. Sie benötigen die interne, digitale Währung des jeweiligen Systems. Das wird häufig Ether sein, die Währung von Ethereum.



Ethereum ist eine bekannte dezentrale Plattform, mit der sich Smart Contracts umsetzen lassen.

Mining von Bitcoins

Wie funktionieren die Rechenaufgaben, die Bitcoin-Miner lösen müssen?

Die richtige Anzahl von Nullen

Zusätzlich zu den Informationen über die Transaktionen enthält ein Bitcoin-Block einen so genannten *Nonce*. Das ist ein 32-Bit-Feld, das verschiedene Werte annehmen kann. Eine kleine Änderung an diesem Wert erzeugt einen komplett anderen Hashwert des Blocks. Die Aufgabe an die Miner besteht darin, einen Wert für den *Nonce* zu finden, so dass der erzeugte Hashwert mit einer bestimmten Anzahl von Nullen beginnt. Während sich der Hashwert zwar schnell berechnen lässt, funktioniert die umgekehrte Richtung nicht annähernd so schnell. Die Miner probieren daher alle möglichen *Nonces* der Reihe nach durch, bis einer die Voraussetzung erfüllt. Das kostet Rechenleistung. Mit einem einfachen PC zu Hause können Sie da nicht mithalten. Sie könnten zwar zufällig die richtige Zahl raten – aber da stehen Ihre Chancen im Lotto besser. Die Anzahl an Nullen wird regelmäßig angepasst, damit nur ein Block etwa alle zehn Minuten erstellt wird.

Ether war lange Zeit die zweite, bekannte Kryptowährung hinter Bitcoin. Im Bereich der Kryptowährungen rangiert Ether aktuell auf Platz 3, mit einer Marktkapitalisierung von rund 10,4 Milliarden Euro (Platz 2 belegt derzeit Ripple). Während Bitcoins allerdings von Anfang an als reine Kryptowährung konzipiert war, hat Ethereum einen ganz anderen Ansatz. Grundsätzlich ist es ein verteiltes System im Bereich der Finanztechnologie, das die Vorteile der Block-

chain mit den Smart Contracts verknüpft. Weil Ethereum so flexibel ist, bauen viele Blockchain-Ideen auch darauf auf.

Digitale Abstimmungen

Im Bereich E-Voting gibt es zahlreiche Tools, die auf die Blockchain setzen. Ende November wurde zum Beispiel berichtet, dass die südkoreanische Regierung die Entwicklung eines Blockchain-Wahlsystems plant. Die ersten Tests für das System sollten noch in 2018 beginnen. In Amerika konnten letzten November Wahlberechtigte aus West Virginia, die im Ausland lebten, bei den Midterms, den Zwischenwahlen zum US-Kongress, per App abstimmen. Auch hier basierte die Technologie auf Blockchains. In der Schweiz wurden bereits verschiedene Systeme zum E-Voting in verschiedenen Kantonen getestet. Im Sommer kam in der Stadt Zug ein weiteres System auf Blockchain-Basis dazu: Einwohner, die sich eine E-ID (digitale Identität) bei der Stadtverwaltung besorgt hatten, konnten über eine App am Testlauf teilnehmen und verschiedene Fragen mit Ja und Nein beantworten, etwa ob sie das Feuerwerk beim Zuger Seefest gut finden oder nicht. Der Abschlussbericht zieht eine positive Bilanz, auch wenn die 72 Teilnehmer sicher noch ausbaufähig sind.

Digitaler Strommarktplatz

Auch in der Energiewirtschaft gibt es viele Ideen auf Basis der Blockchain. Zum Beispiel die Peer-2-Peer-Plattform *Eblox*. Das System ermöglicht den personalisierten Vertrieb von Strom zwischen regionalen Produzenten erneuerbarer Energien und potenziellen Konsumenten. Die Blockchain erfasst alle nötigen Informationen rund um Produktion, Verbrauch und die vertraglichen Beziehungen zwischen den Teilnehmern der Plattform. So können Sie genau verfolgen, wo Ihr Strom erzeugt wurde. Die Wuppertaler Stadtwerke nutzen *Eblox* seit Januar 2018 für ihren digitalen Strommarktplatz *Tal.Markt* (www-talmarkt.de). Kunden stellen sich darüber einen individuellen Strom-Mix aus erneuerbaren Energien zusammen. Betreiber von Solar-, Biomasse-, Wasser- oder Windkraftanlagen können ihren Strom an regionale Abnehmer verkaufen. Im ersten Quartal 2019 soll das Projekt bundesweit ausgerollt werden.

Diamanten verfolgen mit Tracr

Das Unternehmen De Beers ist der größte Diamantenproduzent und -händler der Welt mit Sitz in Luxemburg und liefert etwa ein Drittel der Weltproduktion von Roh-

Weitere Blockchains

Egal, welches Themengebiet Sie sich herauspicken: Sie können sicher sein, dass irgendwer gerade an einer innovativen Blockchain-Idee in diesem Bereich arbeitet.

■ **Smart Dubai:** Schon Anfang 2017 hat Dubai seinen ambitionierten Plan angekündigt, bis 2020 die erste Smart City zu sein, die in allen Bereichen von Blockchains unterstützt wird. → smartdubai.ae

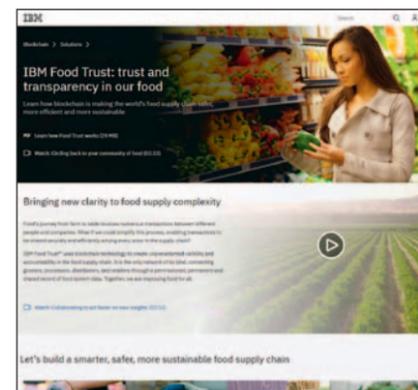
■ **E-Government:** Estland gilt als Pionier in Sachen Digitalisierung und E-Government und hat auch für die Zukunft große Pläne. Zum Beispiel in den Bereichen Gesundheit, Verkehr, Cyber Security und Real-Time Economy. → e-estonia.com

■ **Charity:** Die Plattform GiveTrack nutzt die Blockchain, um Spendern transparent und in Echtzeit zu zeigen, wo ihre Spengelder hinfließen. → givetrack.org

■ **Kartenspiele:** Eine ganze Reihe neuer Trading Card Games baut auf Blockchains und Smart Contracts auf. Darunter Darkwinds, Spell of Genesis, EtherMage und Volition. Die Blockchain hält fest, wer welche Karte besitzt, getauscht oder auch verändert hat. → volitionccg.com



Volition: ein Print-on-demand, digitales Blockchain-basiertes Sammelkartenspiel



IBMs Food Trust verspricht mehr Transparenz bei der Lieferkette von Nahrungsmitteln.

diamanten. Ein Problem sind hier immer wieder Blut- bzw. Konfliktdiamanten, also Diamanten, mit deren Erlös gewalttätige Konflikte finanziert werden. Auch De Beers steht deswegen in der Kritik. Das Unternehmen hat sich mit anderen Firmen aus der Diamantbranche zusammengetan, um *Tracr* zu entwickeln. Diese Blockchain-Plattform gibt jedem Diamanten eine einzigartige ID, bei der auch Eigenschaften wie Gewicht, Farbe und Klarheit gespeichert werden. Die Lieferwege der Diamanten werden in der Blockchain festgehalten. Im Mai 2018 hat das Unternehmen die Wege von 100 Diamanten von der Mine bis zum Händler darüber aufgezeichnet. Kunden haben so die Möglichkeit, den Weg einzelner Diamanten genau zu verfolgen, um sicher zu gehen, dass es sich nicht um Blutdiamanten handelt.

IBM Food Trust

In der Lebensmittelindustrie ist es ebenso wichtig, die genauen Lieferwege zu kennen. Wenn heute kontaminierte Lebens-

mittel gefunden werden, kann es Tage oder Wochen dauern, um den Weg zurückzuverfolgen und die Ursache eines lebensmittelbedingten Krankheitsausbruchs zu bestimmen. Der *IBM Food Trust* ist eine Blockchain-basierte Cloud-Plattform, mit der Lebensmittel in der gesamten Lieferkette verfolgt werden können. Auch hier ist es das Ziel, bessere Rückverfolgbarkeit, Transparenz und Effizienz zu bieten. Da alle Lieferungen in der Blockchain festgehalten werden, dauert es nur ein paar Sekunden, bis der Ursprungsort ermittelt ist. Die Basis bildet hier eine Permissioned Blockchain, so dass nur die einzelnen Teilnehmer an der Lieferkette Daten eintragen dürfen.

Als erstes großes Unternehmen nutzt Walmart das System. Ab dem 31. Januar 2019 sollen alle Lieferanten von Blattgemüse das System nutzen, ab 2020 soll es auf andere Lieferanten ausgeweitet werden. Neben Walmart hat IBM auch weitere Partner gefunden. So will der französische multinationale Einzelhändler Carrefour (mit mehr als 12.000 Geschäften) den *IBM Food Trust* zunächst für einige seiner Private-Label-Produkte einsetzen; mit der Absicht, ihn 2022 auf alle seine Marken zu erweitern.

Offene Fragen

Die Vorteile, die Blockchains in Aussicht stellen, sind zu begrüßen: Alles soll transparenter, dezentraler, sicherer werden. Doch noch befinden sich die meisten Projekte in der Startphase, und es bleiben eine Menge Fragen offen. Dazu gehört an erster Stelle, wie sich die neue Technologie einem Otto Normalnutzer erklären lässt? Blockchains und Kryptotechnologien sind nicht einfach zu verstehen. Noch dazu ist Blockchain nicht gleich Blockchain. Wie aber soll

ein normaler Nutzer einschätzen können, ob die Blockchain-Technologie tatsächlich sicherer ist als andere Lösungen? So wurden laut Wikipedia bis Ende 2017 bereits 980.000 Bitcoins gestohlen. Das passt erst einmal nicht zu der als sicher beworbenen Blockchain. Tatsächlich ist die Blockchain selbst bisher noch nicht erfolgreich angegriffen worden. Aber rundherum gibt es jede Menge Websites, Apps und andere Technologien, die angreifbar sind. Da also bereits einige Bitcoin-Systeme gehackt wurden: Wie sicher sind E-Voting-Systeme? Falls irgendjemand Rückschlüsse von einer ID auf einen konkreten Bürger ziehen könnte, wären all seine Abstimmungen nicht mehr geheim, weil man anhand der Blockchain all seine getroffenen Wahlen nachvollziehen könnte.

Auch bei den Lieferwegen ergeben sich Fragen. So ist es noch nachvollziehbar, den Weg eines Bitcoins per Blockchain zu verfolgen. Aber wie sicher funktioniert das bei physischen Gütern? Ein Diamant hat noch ein paar Eigenschaften, die sich überprüfen lassen. Aber wie stellt man sicher, dass Blattgemüse nicht ausgetauscht wurde? Und warum muss es überhaupt eine Blockchain sein? Wenn es darum geht, die Lieferwege festzuhalten und ohnehin nur eine begrenzte Anzahl von Lieferanten Zugriff auf das System hat, würde auch eine traditionelle Datenbank mit entsprechend angepassten Rechten reichen. Dazu kommt, dass viele Unternehmen ihre Blockchain-Ideen zwar mit Websites, White Papers und üblichen Hype-Begriffen bewerben. Aber konkrete Informationen über die genutzte Technik werden eher selten geboten oder sind gut versteckt. Es fehlt zu oft die angepriesene Transparenz. ■