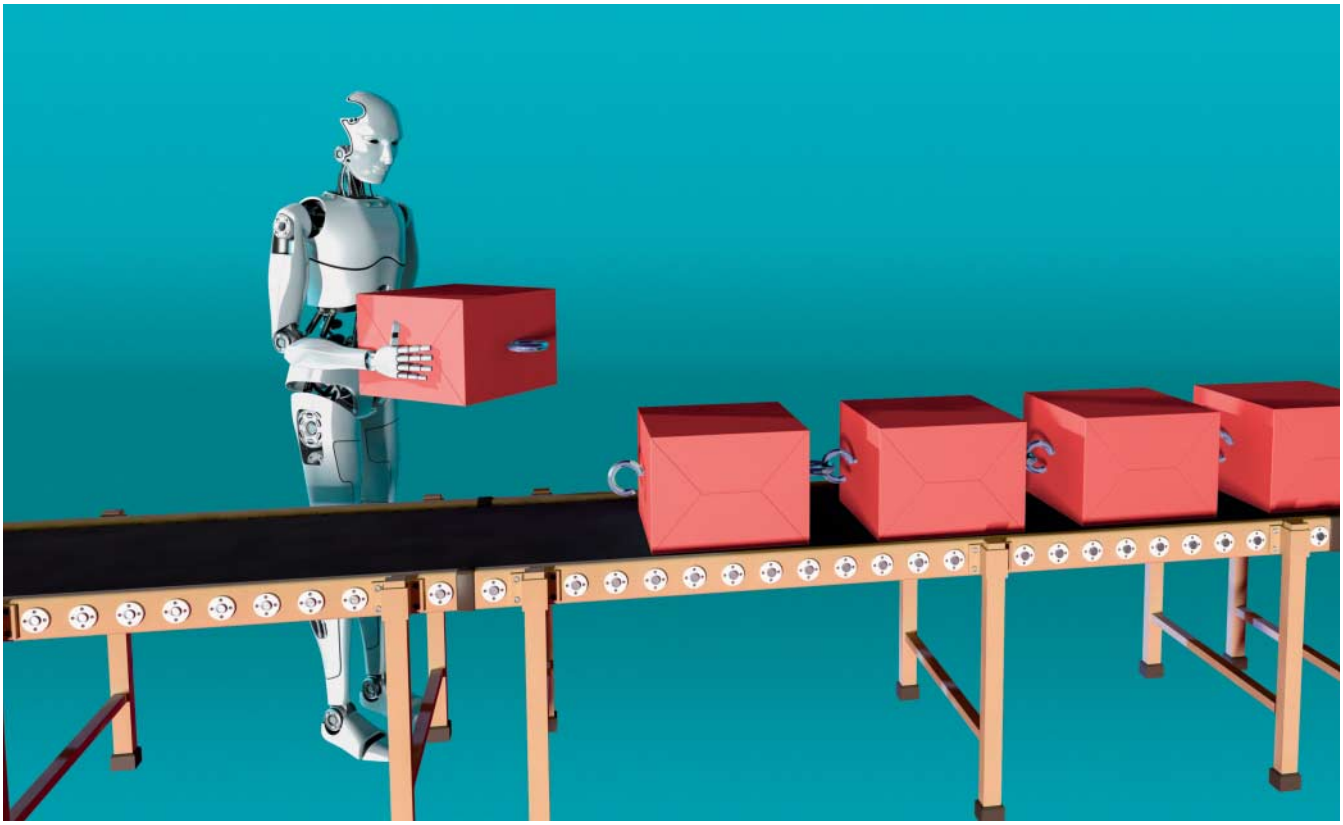

Die Blockchain

Vom Enfant terrible zum Fintech-Star

Immer mehr Startups wollen den weltweiten Zahlungsverkehr vereinfachen, Kundendaten auf Dauer fälschungssicher speichern oder gleich ganze Geschäftsprozesse in Form sogenannter „Smart Contracts“ durch Computer statt von Menschen ausführen lassen. Bei der Umsetzung bauen alle auf das gleiche Fundament: die Blockchain. Eine komplexe Technologie mit großem, aber ungewissem Potenzial.

Von Levin Keller

Stellen Sie sich vor, Ihr Kontostand wäre nicht bei Ihrer Bank gespeichert, sondern bei irgendeinem Fremden auf dessen Rechner. Und nicht nur bei einem Fremden, sondern bei Tausenden Fremden überall auf der Welt. Sie wissen nicht, wer Ihren Kontostand gespeichert hat und ob er versuchen wird, Ihren Kontostand zu verändern oder gleich ganz zu löschen. Trotzdem können Sie sich entspannt zurücklehnen und sich darauf verlassen, dass Ihr Kontostand immer aktuell und korrekt ist und Sie jederzeit über das Geld auf Ihrem Konto verfügen können.

Hacker gegen das Finanzsystem

Klingt utopisch? Ist aber bereits Realität. Möglich macht dies die sogenannte Blockchain, ein dezentrales Datenspeicher- und Kontrollsystem, das unter anderem die technische Grundlage für Kryptowährungen wie Bitcoin ist.

Bekannt ist die Blockchain seit etwa einem Jahrzehnt. Als Reaktion auf die globale Finanzkrise veröffentlichten IT-Aktivisten unter dem Pseudonym „Satoshi Nakamoto“ im Jahr 2008 das Konzept eines alternativen Geldsystems, das nicht mehr zentral, sondern von den Beteiligten selbst verwaltet werden sollte.

Ziel war nicht nur die Schaffung der neuen Währung Bitcoin, sondern auch der Aufbau einer technischen Infrastruktur, um die neuen digitalen Geldeinheiten sicher zwischen Netzwerkteilnehmern transferieren zu können. Dies gelang den Aktivisten durch eine geschickte Kombination von bereits bekannten Konzepten wie asymmetrischer Verschlüsselung, Peer-to-Peer-Networking und Proof of Work (PoW).

Was die Blockchain unter anderem so besonders macht, ist die Tatsache, dass nichts, was jemals in einer solchen „Datenblock-Kette“ (Blockchain) gespeichert wurde, nachträglich gelöscht werden kann. Das gewährleistet ein aufwendiger dezentraler Algorithmus. Tausende von verteilten Computern weltweit berechnen hochkomplexe mathematische Prüfsummen, die die Daten in der Blockchain versiegeln.

Diese mathematischen Aufgaben sind so schwierig, dass nur alle Rechner gemeinsam in der Lage sind, die nötigen Prüfsummen zu erzeugen. Dass einzelne Personen Prüfsummen berechnen können, die eine nachträgliche Veränderung der Datenbank zulassen würden, ist ausgeschlossen.

Im Fall von Kryptowährungen wie Bitcoin werden die hoch spezialisierten Rechner von den sogenannten Minern betrieben. Sie verarbeiten die Bitcoin-Transaktionen, indem sie neue Datenblöcke an die Kette anhängen. Dafür müssen sie aber zunächst Hash-Werte errechnen, was nur durch wildes Ausprobieren geht und Teil der „Arbeit“ im Proof-of-Work-Prozess ist. Für jeden neuen Block dauert der Vorgang etwa zehn Minuten. Wer als Erstes auf das Ergebnis kommt, darf den neuen Datenblock, der zurzeit etwa 2000 Transaktionen bündelt, an die Blockchain anhängen und wird dafür mit frischen Bitcoins entlohnt.

Mit dieser Entlohnung wird bei Bitcoin nicht nur ein Anreiz geschaffen, Rechenleistung zu investieren, um das Fortschreiben und die Integrität der Blockchain zu garantieren – sie dient auch zur Geldschöpfung des banken- und staatenlosen Kryptogelds. Das Bitcoin-System sieht allerdings nur eine maximale Geldmenge von 21 Millionen Bitcoins vor, weshalb die Höhe der Belohnung mit der Zeit abnimmt.

Miner für Bitcoin kann im Prinzip jeder werden – wie auch für viele der anderen Kryptowährungen, die inzwischen wie Pilze aus dem Boden schießen und jeweils ihre eigenen Blockchains betreiben. Dazu muss man nicht einmal eigene Hardware besitzen, sondern kann auch Rechenleistung gegen Gebühr bei Mining-Dienstleistern anmieten.

Das Blockchain-Konzept lässt sich aber nicht nur für Kryptowährungen nutzen. Denn grundsätzlich können in Blockchains sehr viele Anwendungen abgebildet werden – vorausgesetzt, die gewünschten Funktionen lassen sich durch mathematische Regeln beschreiben und durch maschinenlesbaren Code steuern.

Bezahlkanal

In der Bitcoin-Blockchain ist die Komplexität der Skriptsprache und damit der mögliche Funktionsumfang allerdings absichtlich sehr begrenzt: Ein einfaches System ist schlicht besser auf Fehler zu überprüfen. Dennoch lassen sich auch damit interessante Dinge anstellen – zum Beispiel Payment Channel betreiben.

Ein solcher Payment Channel kann Anbietern von Online-Medien beispielsweise helfen, Kleinstbeträge für den Konsum von digitalen Inhalten einzunehmen, ohne dass diese von den oft sehr viel höheren Gebühren traditioneller Zahlungsdienstleister gleich wieder geschluckt werden.

Denn der Payment Channel auf der Bitcoin-Blockchain ermöglicht die Bündelung vieler kleiner Transaktionen zwischen zwei oder auch mehreren Vertragspartnern zu einer Transaktion. In die Blockchain eingetragen werden müssen nach der Laufzeit des Channel nur die erste und die finale Transaktion, was Speicherplatz und Kosten spart.

So ein Payment Channel kann im Prinzip jahrelang offen gehalten werden und erzeugt dann während der Nutzung keine Kosten für weitere Zahlungen. Bislang funktionieren solche Payment Channel, wie sie etwa das Startup SatoshiPay anbietet, zwar nur in eine Richtung (Kunde bezahlt), in Zukunft sollen sie jedoch Geldflüsse in beide Richtungen ermöglichen und müssten dann nie geschlossen werden.

Payment Channel sind aber nicht nur zum Bezahlen von Medieninhalten geeignet. Im Prinzip kann man damit alle digitalen Ressourcen bezahlen, die heute im Internet von Interesse sind.

Das Startup „21“ aus den USA beispielsweise fokussiert sich auf den Bereich der API-Abfragen: Zahlreiche Programme und auch Webseiten hängen davon ab, Daten von Drittanbietern abzurufen. Zwar sind viele der APIs gratis erreichbar – bei anderen muss man vor einer Nutzung aber erst ein Konto anlegen, Zahlungsinformationen hinterlegen und unter Umständen auch ein monatliches Fixum entrichten, obwohl man die API vielleicht nur selten nutzt.

Bei „21“ entfällt dies alles, da man bei der API-Abfrage direkt eine Mikro-Transaktion in einem Payment Channel autorisiert, was die Gegenstelle wiederum dezentral verifiziert und die Ressourcen dann freigibt. Die Server tauschen also nicht nur die Information aus, sondern bezahlen sich dabei auch noch automatisch gegenseitig.

Schlaue Verträge

Mutiger als die Bitcoin-Macher sind die Entwickler im Ethereum-Projekt gewesen, das ebenfalls eine große öffentliche Blockchain betreibt. Die Ethereum-Ent-

Bild: Bitmain

Moderne Geldruckmaschine: Mit ASIC-Chip-Rechnern wie diesem „Antminer S9“ von Bitmain werden heute Kryptowährungen geschürft und Blockchains betrieben. Kostenpunkt: rund 2000 Euro.

wickler wählten einen sehr radikalen Ansatz und bauten in ihre Blockchain, die seit 2015 im Live-Betrieb ist, eine vollwertige Programmiersprache ein, die auch die Abbildung komplexer Vertragsmodalitäten in Form sogenannter „Smart Contracts“ erlaubt.

Ziel solcher Smart Contracts ist meist die Automatisierung von Geschäftsprozessen, die sich in der Regel bereits gut digital abbilden lassen, die aber trotzdem oft noch ein hohes Maß an händischem Aufwand erfordern.

Zum Beispiels will das deutsche Startup „Slock.it“ die Ethereum-Blockchain nutzen, um Wohnungsschlüssel-Übergaben bei Buchungen über die Vermietungsplattform Airbnb obsolet zu machen. Dazu wird die zu vermietende Wohnung zunächst mit einem IoT-fähigen Schloss ausgestattet.

Dieses „intelligente Schloss“ wird dann von einem Smart Contract in der Blockchain gesteuert. Zahlt ein Mieter die Kaution und den Mietpreis in den Smart Contract ein, kann er die Wohnung anschließend kontaktlos über ein Ethereum-Wallet auf dem Handy öffnen.

Nach dem Aufenthalt verlässt der Gast die Wohnung und erhält, wenn alles in Ordnung ist, automatisch die Kaution aus dem Smart Contract zurück.

Ähnliche Konzeptideen gibt es auch für die Nutzung von Stellplätzen in Parkhäusern, das Entsperren von Elektroauto-Ladestationen, Carsharing, Mitfahrgelegenheiten und vieles mehr. Abgerechnet wird in der jeweiligen Kryptowährung – bei Ethereum etwa ist das der sogenannte „Ether“.

Einsparpotenzial

Smart Contracts lassen sich im Prinzip für alle vertraglichen Vereinbarungen zwischen zwei oder mehreren Parteien nutzen, solange sich die Vertragsbedingungen in Form maschinenlesbarer Anweisungen beschreiben lassen. Die Blockchain garantiert als verteilt gespeichertes Transaktionsregister dann nicht nur, dass die von den Vertragspartnern fixierten Klauseln dauerhaft fälschungssicher hinterlegt sind, sondern auch, dass die Vertragsklauseln bei Eintreten der Vereinbarung sofort automatisch ausgeführt werden. Die Einbindung sogenannter „vertrauenswürdiger dritter Instanzen“ (Notar, Treuhänder) ist in vielen Fällen nicht mehr nötig.

Die Wirtschaft geht von erheblichen Einsparungen aus, würde man traditionelle Vertragswerke künftig durch Smart Contracts ersetzen. Das Interesse zieht sich durch nahezu alle Branchen, von der Finanzindustrie über den Energiemarkt bis hin zur Schiffslogistik.

Aber nicht nur Unternehmen, auch Kunden hätten Vorteile. Autoversicherer beispielsweise könnten in einer Blockchain hinterlegte Smart Contracts nutzen, um Prämienkonditionen automatisch an die tatsächliche Jahresfahrleistung anzupassen, statt Pi-mal-Daumen-Stufen zu verwenden, die oft Differenzen von mehreren tausend Kilometern aufweisen.

Das Wirtschafts- und IT-Beratungsunternehmen Capgemini rechnete zuletzt vor, dass allein durch das Abschaffen papierbasierter Gutachten und Dokumentationsprozesse, die bislang das Privatkunden-Geschäft von Banken prägen, in den USA und der EU zwischen drei und zehn Milliarden Euro an Verwaltungskosten eingespart werden könnten. Würde man das Geld auf Kunden umlegen, ergäben sich „Einsparpotenziale von durchschnittlich 430 bis 860 Euro, beziehungsweise 11 bis 22 Prozent für Hypotheken- und Kontoführungsgebühren“, heißt in einer Studie von Capgemini. Wobei in der Finanzbranche häufig nicht direkt von Blockchain-Anwendungen, sondern meist von sogenannten „Distributed-Ledger-Technologien“ (DLT) die Rede ist, also „verteilten Kontobüchern“.

Graue Theorie und Wolkenschlösser

Vieles ist mit Smart Contracts möglich: die Beglaubigung von Vertragsunterschriften, Eintragungen in Grundbücher und Handelsregister, Einträge in Geburtsurkunden oder der Handel auf Wertpapierbörsen. Egal was man in die Blockchain schreibt: Man könnte sich immer sicher sein, dass der Eintrag weder nachträglich verändert noch jemals gelöscht wird.

Wäre da nicht ein kleiner Haken: Viele dieser Ideen sind weit von einer funktionierenden Implementierung und insbesondere noch weit vom Massenmarkt entfernt. Nicht nur deshalb warnen viele Kritiker vor einer übertriebenen Zuversicht beim Thema Blockchain.

Startups in Deutschland mit Blockchain-Schwerpunkt

Ascribe, Berlin	Digital Rights Management auf Blockchains
BigchainDB, Berlin	Großdatenbank mit eigener Blockchain
Bitbond, Berlin	Peer-2-Peer-Kredite mit Bitcoin
Bitwala, Berlin	Rechnungen mit Bitcoin bezahlen
EthCore, Berlin	eigener Ethereum-Client (jetzt Parity)
Genesis Mining, München	großer Cloud-Mining-Betreiber
Pey, Hannover	Bitcoin-Ökosystem-Enabler
SatoshiPay, Berlin/London	Mikrozahlungen per Payment Channel
Slock.it, Mittweida	Smart Contracts auf Ethereum

Auch bedeutet nicht alles, was machbar ist, zwangsläufig einen wirtschaftlichen Vorteil. Im Fall des erwähnten Airbnb-Beispiels etwa muss zunächst das entsprechende Schloss entwickelt und eingebaut werden. Den erforderlichen Rund-um-die-Uhr-Internetzugang gibt es ebenfalls nicht umsonst.

Hinzu kommen konzeptionelle Fragen. Beispielsweise gibt es bei heutigen Verträgen oft Grauzonen, die man nicht so ohne Weiteres in Source Code übersetzen kann. Was ist zum Beispiel, wenn jemand eine Berufsunfähigkeitsversicherung per Blockchain abgeschlossen hat und dann tatsächlich berufsunfähig wird?

Wer prüft die Erkrankung und wer speist diese Information in den Smart Contract ein? Und wie kann die Versicherung einen Vertrag rückgängig machen, sollte ein Versicherter falsche Angaben zu Vorerkrankungen gemacht haben? Es werden noch große Anstrengungen und auch intensive Anpassungen der heutigen Strukturen und Gesetze notwendig sein, um Blockchains so in den Massenmarkt zu bringen, dass sie schließlich von allen genutzt werden können.

Ob es jemals dazu kommt, kann heute keiner sagen. Aber mit Bitcoin, Ethereum & Co. ist bereits ein erster großer Schritt gelungen. *(pmz@ct.de)* c't

Levin Keller ist Mathematiker, Unternehmer, Vorstandsmitglied im Bundesverband Bitcoin e. V. und Geschäftsführer von Hardfork, das Smart-Contract-Prototypen und Software-Tools für Blockchain-Applikationen entwickelt.