

13.07.2016 | BLOCKCHAIN

Die Verkettung der Welt

Eine unscheinbare Innovation lockt Investoren in Scharen: Die Blockchain ist radikal offen, kaum zu manipulieren - und könnte bald Wirtschaft und Gesellschaft gehörig aufmischen.

von Stefan Mey





© ISTOCK / COFOTOISME (AUSSCHNITT)

Es sei die größte Erfindung einer ganzen Generation, sagt der US-amerikanische Berater Don Tapscott. Die Auswirkungen auf die Gesellschaft: so groß wie beim World Wide Web.

Zehn Prozent des weltweiten Bruttoinlandsprodukts würden im Jahr 2027 mit dieser Technologie abgewickelt. Das schätzten unlängst Experten am World Economic Forum.



Die großen globalen Bankinstitute sind bereits aktiv geworden. Mit im Boot beim neuen New Yorker Joint Venture R3Cev: die Deutsche Bank, UBS und Goldman Sachs.

Die Blockchain hat einen Hype verursacht wie selten eine Technologie zuvor.

Fast eine halbe Milliarde US-Dollar haben Kapitalgeber im vergangenen Jahr in Blockchain-Start-ups gesteckt. Nur an der breiten Öffentlichkeit ist die Blockchain bislang weitgehend spurlos vorübergegangen.

Dabei dürften die meisten zumindest indirekt davon gehört haben. Die Blockchain ist eng verwoben mit einer Technologie, die ebenfalls bereits als Revolution gepriesen wurde, bislang aber eher als Kuriosum der Netzwelt gilt: Bitcoins, die digitale Währung, die ohne jegliche staatliche Kontrolle auskommt und allein aus der Selbstorganisation heraus entsteht. Dank der Blockchain könnten Bitcoins nun doch den einst versprochenen Durchbruch erleben, wenn auch anders als gedacht. Die Blockchain – das ist die große Zweckentfremdung der Bitcoins.

Wie das funktionieren könnte, zeigt der Konstanzer Informatikprofessor Bela Gipp. Durchschnittlich alle fünf Minuten schicken er und sein Team einen Bruchteil eines Bitcoins von A nach B. Doch um Geld geht es ihnen nicht, sondern um die Infrastruktur, die die Digitalwährung zur Verfügung stellt. Bei ihrem Projekt OriginStamp erforschen die Konstanzer Wissenschaftler, wie man Dateien einen Zeitstempel verpassen kann, der sich nicht manipulieren lässt und absolut vertrauenswürdig ist. Ein Fotograf in Krisenregionen könnte damit beispielsweise den Entstehungszeitpunkt seiner Bilder genau dokumentieren.



Eine Datenbank, die allen gehört

Die Blockchain ist womöglich das ideale Werkzeug dafür, meinen die Konstanzer. Denn erfunden wurde sie einst als Antwort auf ein ganz ähnliches Problem. Angenommen, Frau Müller will an Frau Schmidt ein digitales Geldstück überweisen. Wie kann man sicherstellen, dass ihr das Geldstück tatsächlich gehört, und vor allem, dass sie es nicht schon längst ausgegeben hat? Die 2008 veröffentlichte Lösung des Bitcoin-Entwicklers bestand darin, alle nötigen Informationen in einer einzigen riesigen Datenbank öffentlich abzulegen. Eine Datenbank, die niemandem gehört – und damit allen zugleich.

Diese Sammlung aktualisiert sich permanent selbst, sie ist dezentral, das heißt, sie liegt auf allen beteiligten Rechnern. Und sie ist völlig transparent, denn sie enthält Informationen über alle jemals getätigten Transaktionen. Trotzdem ist sie anonym, da bei entsprechenden Vorsichtsmaßnahmen keiner weiß, wer sich hinter den digitalen Bitcoin-Brieftaschen verbirgt. Mit Hilfe der Datenbank lässt sich jeder Bitcoin lückenlos zurückverfolgen. Taucht eine digitale Geldeinheit hingegen ohne Vorgeschichte plötzlich auf, weiß man, dass Betrug im Spiel ist. Diese Erfindung und ihre Implementierung gelten inzwischen als die eigentliche Innovation des unter dem Pseudonym Satoshi Nakamoto bekannten Bitcoin-Entwicklers.

Wenn Frau Müller den Überweisungsauftrag erteilt, prüfen einige der Rechner in der Bitcoin-"Crowd" anhand der abgespeicherten Daten, ob die Transaktion legitim ist. Ist alles okay, wird ihre Überweisung zusammen mit allen anderen Bitcoin-Überweisungen der letzten zehn Minuten zusammengefasst und in Form



eines einzelnen, digitalen "Blocks" gespeichert. Und der wird dann an die Liste der bisherigen Bitcoin-Blöcke gehängt, eine Blockkette entsteht – auf Englisch "Blockchain".

Resistent, effizient, stabil und nicht zensierbar

Der Konstanzer Bela Gipp sieht darin vier Vorteile: "Erstens ist das System sehr betrugsresistent, da eine Art 'Kopfgeld' auf erfolgreiche Manipulationen der Technologie ausgesetzt ist." Wer es schafft, das System zu manipulieren, könnte Millionen an Bitcoins auf das eigene Konto überweisen. Dann würde aber deren Wert sehr schnell in Richtung null sinken, da jeder versuchen würde, seine eigenen Coins schnellstmöglich zu verkaufen. Man könne daher davon ausgehen, dass, solange Bitcoins einen signifikanten Wert haben, die Blockchain nicht manipuliert werden kann.

Zweitens existiert mit der Blockchain eine hoch effiziente, öffentliche Infrastruktur, derer sich jeder bedienen kann. Drittens ist sie ein geniales, selbst organisiertes System, das dafür sorgt, dass viele Beteiligte ein Interesse an der Stabilität und Integrität des Netzwerks haben: Privatpersonen, die Bitcoins als Wertanlage halten, Unternehmen, die Transaktionen via Bitcoin abwickeln, und Investoren, die ihre komplexen Geschäftsmodelle auf der Blockchain aufbauen.

Viertens ist sie nicht zensierbar, da sie auf tausenden Rechnern weltweit verteilt liegt: "Kein Staatsanwalt kann einfach so mit der Polizei vorbeikommen, einen Server abholen, Informationen aus dem Netz nehmen und zukünftige Transaktionen verhindern." Die Kehrseite davon ist natürlich, dass sich diese



Infrastruktur auch gut für kriminelle Geschäfte und Geldwäsche eignet. Geldflüsse von Bitcoins können nicht mehr blockiert werden und sind in aller Regel den tatsächlichen Personen nicht zuzuordnen. Kein Wunder, dass sich die digitale Währung bislang vor allem auf den halblegalen Marktplätzen im Netz, dem Darkweb, etabliert hat.



© ISTOCK / PETROVICH9 (AUSSCHNITT)

Offene Daten | Die Transparenz der Blockchain macht ihre große Stärke aus. Wenn jeder alles einsehen kann, sind Manipulationen praktisch ausgeschlossen.



Doch das Potenzial der Bitcoins, so zeigt sich jetzt, liegt offenbar ohnehin woanders. Wer die Blockchain für andere Zwecke einsetzen möchte, muss nur ein paar Tricks anwenden. Man kann einen Bitcoin oder einen Bruchteil davon mit einem ganz anderen Gut verknüpfen, beispielsweise einem Wertpapier. Wird eine Coin-Einheit über die Blockchain von Nutzer A zu Nutzer B geschoben, wird auch der Transfer dieses Wertpapiers öffentlich dokumentiert.

Smart contracts und andere schlaue Lösungen

Zudem ist es möglich, auf Basis der Blockchain "schlaue Verträge" zu basteln. An eine Blockchain-Transaktion lassen sich Informationen anhängen, das ist in etwa so, als würde man eine Fünfeuronote weitergeben, auf der man zuvor per Hand etwas vermerkt hat. Auf diese Art lassen sich Schnipsel mit Programmiercode einbauen, die eine Wenn-dann-Bedingung definieren – das Grundprinzip eines Vertrags. Es kann etwa Folgendes vermerkt werden: Wird eine klar definierte Dienstleistung erbracht, was dann von der Blockchain-Crowd verifiziert wird, fließt automatisch ein bestimmter Betrag von einem Treuhandkonto X an Bitcoin-Konto Y. Diese Smart Contracts, wie sie in der Tech-Sprache heißen, sind "schlau", weil sie sich selbst vollziehen. Ein Dienstleister muss nicht mehr auf seine Bezahlung warten oder sie gar mit Hilfe eines Anwalts einklagen.

Im Kern geht es bei Blockchain-Szenarien stets darum, Transaktionen abgewickeln zu können, ohne dass sich die Partner vertrauen müssen, meint Gipp: "Dadurch macht die Blockchain zwischengeschaltete Instanzen, die üblicherweise Vertrauen



zwischen Partnern sicherstellen, wie zum Beispiel Banken oder Notare, überflüssig. Anstatt zentraler Instanzen übernimmt die dezentrale Blockchain-Crowd diese Funktion."

Diverse Wirtschaftszweige tüfteln bereits an Einsatzszenarien. Am größten ist die Euphorie paradoxerweise in der Bankbranche, die in den frühen Anarchovisionen des Bitcoins überflüssig gemacht werden sollte. Bankmanager träumen davon, veraltete Strukturen zu ersetzen, die die Finanzwirtschaft seit Langem in ihrer Entwicklung lähmen. Transaktionen von Geld oder Wertpapieren dauern deswegen so lang, weil stets eine Vielzahl an Zwischeninstanzen die Abwicklung begleitet und vollzieht. Um diese Instanzen (mit ihren Arbeitsplätzen) ersetzen zu können, haben sich die großen globalen Bankinstitute zu einer gemeinsamen Blockchain-Initiative zusammengeschlossen. Das New Yorker Joint Venture R3Cev soll unter Beteiligung der Big Player der Finanzindustrie eine maßgeschneiderte Blockchain-Lösung entwickeln.

Zu viel Offenheit und Transparenz scheint den Finanzinstituten allerdings doch Unbehagen zu bereiten. Statt auf die radikal öffentliche Bitcoin-Blockchain setzt das Joint Venture auf ein eigenes, geschlossenes Modell, auf das nur die beteiligten Banken Zugriff haben.

Rechteverwaltung an die Kette gelegt

Aufbruchstimmung gibt es auch in der Musikindustrie. Die krankt seit Jahren daran, dass es keinen globalen Überblick gibt, wer in welchen Ländern welche Rechte an Musiktiteln hält. Das Start-up Ujo will deswegen eine Musikrechte-



Blockchain aufbauen: Musiker stellen ihren Song ein. Dabei definieren sie klar, wer die Rechte daran hält und was verschiedene Nutzungsformen kosten. Wird das Nutzungsrecht an einem Song erworben und der entsprechende Geldbetrag per Blockchain überwiesen, fließt das Geld automatisch und beinahe in Echtzeit an die vorher definierten Rechteinhaber.

Und dann gibt es viele andere Ideen: Das US-Start-up SmartContract.com will Notare und Juristen überflüssig machen und bietet schon fertig formulierte "schlaue" Blockchain-Verträge an, die mit wenigen Klicks geschlossen werden können. Everledger verpasst Diamanten per Blockchain ein individuelles Profil, um Fälschungen zu erschweren. Und das sächsische Start-up Slock.it will mit einem Minicomputer "smarte" Haushaltsgeräte, Autos oder Fahrräder an die Blockchain anschließen und so über das Prinzip der Sharing Economy verleihbar machen. So soll ein wirkliches "Internet der Dinge" entstehen.

Es kursieren sogar Konzepte für Politik und Verwaltung: Das US-Start-up Followmyvote ermöglicht Blockchain-Wahlen, bei denen jeder nachvollziehen kann, ob seine Stimme tatsächlich gezählt wurde. Und eine Visionärin aus Schweden will mit ihrem Projekt Bitnation Ausweispapiere erstellen; die Identität der Teilnehmer wird dann über die Blockchain protokolliert. Anders als die bisherigen nationalen Dokumente sollen sie über die "Weltbürger"-Blockchain jedem zugänglich sein.



Was setzt sich durch?

Das immense Potenzial zeige sich immer dort, wo plötzlich direkte Transaktionen möglich werden, sagt Gipp; da hier die Blockchain einen zentralen Akteur ersetzt, der zuvor Kontrolle über Daten hatte, eine Provision kassierte oder gar zensierend eingriff. Doch nicht überall, wo Blockchain draufsteht, kommen diese Vorteile auch zum Tragen. Zweifel des Konstanzer Professors wecken vor allem jene Konzepte, die nicht die Bitcoin-Blockchain zweckentfremden, sondern eigene Varianten davon basteln. Das bietet ihnen zwar mitunter mehr Gestaltungsmöglichkeiten. Sie verfügen aber nicht über die große "Crowd", die das Bitcoin-Blockchain-System so manipulationssicher und unzensierbar macht.

Und natürlich sei Technologie nicht der einzige entscheidende Faktor. Ein weiteres Projekt, an dem Bela Gipp zurzeit arbeitet, ist eine mobile App für Leute, die ihr Smartphone als so genannte Dashcam einsetzen. Dabei wird das Gerät hinter der Windschutzscheibe platziert, um beim Fahren die Umgebung vor dem Auto zu filmen und im Falle eines Falles die Unschuld des Fahrers beweisen zu können. Die Funktion der App: Sobald das Smartphone eine starke Erschütterung registriert, wird für die Videosequenz der letzten zwei Minuten ein eindeutiger, digitaler Fingerabdruck erstellt und über OriginStamp in die Blockchain eingeschrieben.

Damit kann der Fahrer beweisen, dass die jeweilige Filmsequenz die "echte" ist und nicht manipuliert wurde – technologisch ist das eine zwingende Logik. Ob aber auch Gerichte diese Methode als Beweis akzeptieren? Das sei offen, merkt



Gipp an. Wie eigentlich bei allen Blockchain-Szenarien: "Es ist nicht nur eine technologische Frage, ob sich eine Lösung durchsetzt, schöne Technologie hin oder her."

Stefan Mey

Der Autor ist Technologie-Journalist in Berlin.

