

Blockchain – Spekulationsobjekt oder mehr?

BLOCKCHAIN Spekulationsobjekte oder Medienhype? Alle sprechen darüber, doch wie funktioniert die Technologie konkret? Ist sie disruptiv? Was bedeutet denn «Initial Coin Offering» und bietet die Technologie wirklich so bahnbrechende Möglichkeiten, wie viele behaupten? Wir klären auf.

VON BRAD RICHARDS UND PETRA ASPRION

Eine Blockchain ist im Grunde nichts anders als ein Transaktionsregister, das mittels kryptographischer Techniken quasi fälschungssicher realisiert wird. Sie ist die Basis eines verteilten Systems, das ohne eine zentrale Instanz zuverlässig Transaktionen zwischen allen Teilnehmenden ermöglicht. Die Teilnehmenden können mittels einer Software ein sogenanntes «Wallet» (Portemonnaie) erstellen. Dieses Wallet beinhaltet – statt Dollars oder Euro – Einheiten einer digitalen Währung und dient dazu, Überweisungen zu initiieren oder zu empfangen. Zwischenzeitlich gibt es hunderte verschiedener solcher Währungen, unter den bekanntesten sind Bitcoin, Ethereum und Monero.

Der Wert einer digitalen Währung wird durch ihren Tauschwert bestimmt: Wie viel kann man für eine Währungseinheit erhalten? Dies ist bei digitalen Assets und traditionellen Währungen ähnlich: Momentan sind Schweizer Franken begehrt, venezolanische Bolívar weniger. Die meisten analogen Währungen werden von Nationalbanken verschiedener Länder verwaltet, während digitale Währungen verteilt im Internet existieren und (in den meisten Fällen) nicht zentral betrieben werden. Nicht wenige Regierungen misstrauen dieser Situation und fühlen sich bedroht – dies insbesondere in Ländern, die eine sehr restriktive Geldpolitik verfolgen oder deren Währungen wenig Vertrauen geniessen.

Transaktionen werden jeweils von einem Sender initiiert. Dieser wählt einen Betrag für eine bestimmte Empfängerin und sendet diese Informationen an das Netzwerk. Bestimmte Netzwerkknoten,

sogenannte «Miner», prüfen die Transaktion und fügen sie der Blockchain hinzu. Da die Blockchain von jedem Netzwerkteilnehmenden gelesen werden kann, sind die Transaktionen öffentlich und können, mit einigem Aufwand zwar, auf die einzelnen Akteure zurückverfolgt werden.

WEITERE ANWENDUNGEN VON BLOCKCHAINS

Blockchain ist ein Konzept, das sich sehr gut für digitale Transaktionen eignet. Es gibt zahlreiche potenzielle Einsatzbereiche wie zum Beispiel die elektronische Stimmabgabe (E-Voting). Um eine ehrliche Wahl zu gewährleisten, muss nachvollziehbar sein, wer seine Stimme abgegeben hat und sichergestellt werden, dass jede Person nur einmal abgestimmt hat. Wenn jede gültige Stimme in einer Blockchain eingetragen wäre, könnte dies genutzt werden, um die Stimmabgabe zu kontrollieren und zu archivieren. Der eigentliche Inhalt des Votums kann durch eine zusätzliche Verschlüsselung geschützt werden.

Jeder Bereich, in dem eine Art Hauptbuch und Konten verwendet werden, ist grundsätzlich auch ein mögliches Einsatzgebiet für Blockchains: etwa die Dokumentierung der Produktionsschritte eines industriellen Herstellungsprozesses, die Wartungsprotokolle einer Maschine und natürlich auch die traditionelle Buchhaltung, wo rückwirkende Änderungen ausgeschlossen werden müssen.

FÄLSCHUNGSSICHERHEIT UND ÖFFENTLICHKEIT

Blockchains gelten als fälschungssicher. Konkret bedeutet dies, dass rückwirkende

Änderungen zu abgeschlossenen Transaktionen praktisch unmöglich sind, weil die Konsistenz der Blockchain über einen sogenannten Konsensus-Prozess über alle beteiligten Netzwerkknoten abläuft. Jeder beteiligte Rechner hat eine vollständige Kopie der Blockchain: Ein Fälschungsversuch wird deshalb bemerkt und verworfen; es regiert die Mehrheit.

Es ist auch möglich, eine private Blockchain zu definieren. Damit können nicht für die Öffentlichkeit gedachte, vertrauliche Informationen verwaltet werden. Ein Beispiel sind Transaktionen in einer Lieferkette, etwa zwischen einem Unternehmen und seinen Lieferanten. Eine solche Blockchain wird dann jedoch nicht von Millionen Rechnern im Internet verwaltet, sondern nur von den verfügbaren Rechnern innerhalb des Unternehmens und denjenigen seiner Partnerunternehmen. Dies reduziert die Fälschungssicherheit und verlangt deshalb eine Vertrauensbeziehung zwischen den Teilnehmenden.

DIGITALE ASSETS UND INITIAL COIN OFFERINGS

Eines der ersten, wohl das bekannteste und aktuell erfolgreichste digitale Asset ist Bitcoin. Heute gibt es tausende weiterer solcher Assets. Eine Blockchain, ein bisschen Werbung und schon hat man eine digitale Währung lanciert. Die meisten sind vergleichsweise wertlos – niemand will echte Waren gegen eine spekulative Währung eintauschen. Dennoch, wohl ein Dutzend der digitalen Währungen ist ernst zu nehmen.

Wegen des ausserordentlichen Interesses an digitalen Assets haben einige Unternehmen eine neue Möglichkeit entwickelt,



Das Potenzial der Blockchain scheint unbegrenzt – ihr konkreter praktischer Nutzen teilweise noch ungeklärt.

Bild: iStock / ikachan999

um zu Investorengeld zu kommen: das «Initial Coin Offering», abgekürzt ICO. Das Unternehmen initiiert eine eigene digitale Währung und verspricht, dass diese zukünftig gegen Firmenleistungen eingetauscht werden kann. Investoren kaufen sie in der Hoffnung auf Erfolg des Unternehmens und anschliessender Wertsteigerung der so lancierten digitalen Währung. Der Initiator erhält somit eine sofortige Finanzierung gegen zukünftig versprochener Leistungen. Für die Investoren ist dies nichts anderes als eine Wette auf Unternehmenserfolg. Diese Methode ähnelt letztlich stark dem sogenannten Crowdfunding. Langsam aber sicher wecken diese ICOs das Interesse der Aufsichtsbehörde, nachdem einige unseriöse ICO-Initianten Investorengeld angenommen haben, nur um sich danach wieder aufzulösen.

SMART CONTRACTS UND ANDERE ERWEITERUNGEN

Transaktionen können auch dynamische Inhalte haben: Wenn schon digital, warum nicht gleich ein Programmcode? Ethereum, eine der digitalen Währungen, hat sich auf diesem Gebiet spezialisiert. Das System realisiert sogenannte «Smart Contracts», also Programmcode, der von einem Blockchain-System dezentral ausgeführt wird. So kann man eine Abmachung, also einen Vertrag, digitalisieren und unwiderruflich als Teil der Ethereum-Blockchain veröffentlichen.

Allerdings ist Vorsicht geboten, denn Fehler in diesen Smart Contracts sind genauso unwiderruflich wie jede andere Transaktion – so sind angeblich bereits hunderte Millionen Dollar einfach so verpufft. Dennoch eignen sich Smart Contracts für zahlreiche Anwendungen, etwa für Finanzgeschäfte, Versicherungen oder Hypotheken.

Die Anonymität der Anwender wird oft in Zusammenhang mit digitalen Transaktionssystemen hervorgehoben. Bitcoin und die anderen digitalen Assets sind nicht automatisch anonym: Wenn eine Adresse einem Nutzer zugeordnet werden kann, können dessen Transaktionen öffentlich nachvollzogen werden. Da Anonymität für viele Zwecke wünschenswert ist, haben manche digitalen Währungen (z.B. Monero) eine echte Anonymität integriert: Nur die Teilnehmenden an einer Transaktion können Details sehen und verifizieren; somit ist diese Information nicht öffentlich zugänglich.

FAZIT

Blockchains basieren auf einer innovativen und vielversprechenden Technologie. Man kann zwar klar von einem Hype sprechen, dennoch zeichnen sich viele interessante Anwendungsfelder ab, wovon digitale Währungen nur eines ist. Wie bei allen neuen Technologien ist eine gewisse Bodenhaftung angesagt. Die Nutzung von Blockchains per se ist nicht disruptiv. Für den

Einsatz von Blockchains müssen sinnvolle Anwendungsgebiete identifiziert und auf ihr wirtschaftliches Potenzial geprüft werden – dahingehend, ob und wo diese neuen Technologien wirklich etwas beitragen können.

DIE AUTOREN



Prof. Dr. Brad Richards doktorierte an der University of Texas. Nach Projektarbeiten bei der University of Aberdeen und der EPFL wurde er als Professor in den Bereichen Künstliche Intelligenz und Software Engineering an die Fachhochschule Furtwangen berufen. Im Jahr 2001 gründete er zusammen mit seiner Frau eine eigene Softwarefirma. 2009 nahm er eine Professur an der FHNW an, wo er technische Vorlesungen hält.



Prof. Dr. Petra Maria Asprion, Leiterin Kompetenzzentrum Cyber Security & Resilience, Hochschule für Wirtschaft, Fachhochschule Nordwestschweiz FHNW.