INFRASTRUKTUR

Keine Kryptowährungen ohne Blockchain-Technologie

Mit der Lancierung von Bitcoin im Jahr 2009 ist auch die Blockchain-Technologie erstmals ins Bewusstsein einer breiteren Öffentlichkeit gerückt. Das Konzept einer Kryptowährung, die sich unabhängig von staatlichen Interventionen und losgelöst vom Diktat der Zentral- oder Geschäftsbanken durchsetzt, wäre allerdings ohne die ihr zugrundeliegende Blockchain-Technologie undenkbar.

DAMIR FILIPOVIC UND ALEXANDER LIPTON

Grundlage der Blockchain-Technologie für ihren praktischen Einsatz sind das exponentielle Wachstum der Rechenleistung von Computern (auch als Moore'sches Gesetz bekannt, das besagt, dass sich die Komplexität integrierter Schaltkreise mit minimalen Komponentenkosten alle zwölf bis 24 Monate verdoppelt) sowie die zunehmende Verfügbarkeit und Reproduzierbarkeit von Informationen in digitaler Form übers Internet.

Zentrale Datenbanken mit gemeinsamen Zugriffsrechten sind schon seit Jahrzehnten bekannt. Ein exemplarisches Beispiel dafür ist Wikipedia. In einer verteilten Datenbank sind darüber hinaus sämtliche Einträge dezentral auf unterschiedlichen Rechnern abgespeichert – und genau auf diesem Prinzip basiert die Bitcoin-Infrastruktur. Dabei werden alle Finanztransaktionen gemeinsam von den Teilnehmern sicher und unveränderbar über ein verteiltes Kontobuch verwaltet. Aus Effizienzgründen werden die entsprechenden Aufzeichnungen gebündelt in Blöcken vorgenommen, woraus sich die Bezeichnung Blockchain ableitet.

Hochkomplexe kryptografische Prozesse

Um Eigentumsverhältnisse ohne eine zentrale Instanz eindeutig festzulegen, kommen kryptografische Methoden zum Einsatz. Über digitale Signaturen authentifizieren die Teilnehmer jede einzelne Transaktion, die wiederum von sogenannten Minern bestätigt wird. Die Bitcoin-Software erzeugt dafür komplexe Kryptorätsel, die von den erwähnten Minern durch den Einsatz eigener Rechnerleistung aufgelöst werden müssen. Als Anreiz erhält der Miner, der das Kryptorätsel löst und damit einen neuen Block in der Kette beglaubigt, einen bestimmten Betrag an neuen Bitcoin – quasi das Äquivalent der Geldschöpfung durch die Zentral- und Geschäftsbanken in den traditionellen Währungen.

Die Bitcoin-Welle hat unzählige Nachahmer auf den Plan gerufen. Inzwischen gibt es zahlreiche Kryptowährungen – ihnen allen gemeinsam ist der Aufbau auf einer Blockchain. Kritiker weisen allerdings auf einige fundamentale Schwachstellen von Kryptowährungen hin. So werden beispielsweise immer wieder ihre beschränkte Skalierbarkeit, die hohe Preisvolatilität oder Regulierungslücken bemängelt. Ein weiterer Schwachpunkt liegt in der geringen Verarbeitungskapazität von Transaktionen. Während etablierte Kreditkartenherausgeber ein Volumen von rund 2000 Transaktionen pro Sekunde verarbeiten, erlaubt das aktuelle Bitcoin-Protokoll lediglich deren sieben und ist damit derzeit wohl kaum massentauglich.

Das Bitcoin-Geldmengenwachstum ist durch die Software vorprogrammiert und absolut begrenzt. Im Vergleich dazu können Geschäftsbanken durch die Kreditvergabe im Rahmen der regulatorischen Vorschriften praktisch unbegrenzt Buchgeld schöpfen. Daher wird der Bitcoin auf absehbare Zeit kaum eine wirtschaftlich relevante Bedeutung gewinnen. Ausserdem führt die Anreizstruktur für das Mining von Bitcoin zu einem absurd hohen Energieverbrauch aufgrund der notwendigen Rechnerleistung für das Lösen der Kryptorätsel.

Der Umstand, dass jeweils nur einem Miner Bitcoin für das erfolgreiche Lösen eines Kryptorätsels zugeteilt werden, führt letztlich zu Übertinvestitionen in die Rechnerkapazität und damit zu einer wachsenden Konzentration auf immer weniger, dafür grössere Pools von Minern (vgl. Grafik links). Diese haben ihre Mining-Farmen vorzugsweise in Gegenden mit geringen Stromkosten angesiedelt, zum Beispiel in China oder Russland.

Die vier grössten Pools produzieren gegenwärtig mehr als die Hälfte aller Bitcoin. In letzter Konsequenz verliert der Bitcoin damit seinen Status als dezentrale Währung.

In der Grauzone der Legalität

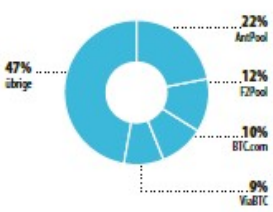
Obwohl oder gerade weil Bitcoin keinen realen Gegenwert besitzen, hat sich der Marktpreis eines Bitcoins innerhalb der letzten fünf Jahre von unter 20 auf mehr als 4000 $ entwickelt (vgl. Grafik). Die Preisentwicklung ist extrem volatil, was vermuten lässt, dass die meisten Teilnehmer Bitcoin zu Spekulationszwecken handeln.

Zahlungen in Bitcoin sind grundsätzlich anonym, was die Durchsetzung des Geldwäschereigesetzes erschwert. Bitcoin wird von Kritikern auch regelmässig mit illegalen Geschäften in Verbindung gebracht. Ausserdem steht der Verdacht im Raum, dass Bitcoin in bestimmten Ländern zur Umgehung von Kapitalverkehrskontrollen benutzt werden.

Mit dem Utility Settlement Coin (USC) entwickelt ein Bankenkonsortium unter der Federführung der UBS seit 2015 eine valable Alternative zum Bitcoin – allerdings wird der USC einer kleinen Gruppe von Grossbanken vorbehalten bleiben. Zweck des USC ist es, Interbanktransaktionen direkt und ohne Umwege über die Zentralbanken durchzuführen. Damit sollen Kosten gespart und die Effizienz gesteigert werden. Der USC ist an eine staatliche Währung gekoppelt und hat damit im Gegensatz zum Bitcoin einen unmittelbaren und stabilen Gegenwert in Einheiten von Zentralbankgeld. Die Transaktionen werden wiederum auf einer Blockchain festgehalten, sie werden jedoch – im Unterschied zu Bitcoin – von vertrauenswürdigen Notaren durch digitale Unterschrift beglaubigt.

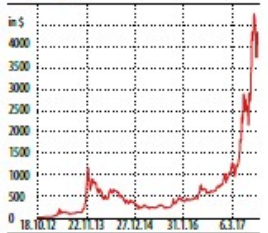
Allen Unkenrufen zum Trotz: Die Blockchain-Technologie wird die Finanzindustrie revolutionieren, sofern ein verbindlicher Rechtsrahmen geschaffen und durchgesetzt wird. Insofern ist die Bitcoin-Entwicklung ein Meilenstein auf dem Weg der fortschreitenden Digitalisierung, die nicht mehr aufzuhalten ist.

Pools von Minern



Quelle: blockchain.info / cash. now_br

Marktpreis eines Bitcoins



Quelle: blockchain.info / cash. now

DAMIR FILIPOVIC

Damir Filipović ist Finanzprofessor am Swiss Finance Institute und hält den Swissquote-Lehrstuhl für Quantitative Finance an der EPFL.

ALEXANDER LIPTON

Alexander Lipton, Gründer und CEO von Stronghold Labs, derzeitiger Visiting Professor an der EPFL. Er war Gastredner am 12. Annual Meeting des SFI.