2 Bitcoin, der Disruptor

Die dezentral organisierte Urkryptowährung könnte unser bisheriges Finanzsystem auf den Kopf stellen. Was Bitcoin ist und noch werden kann.

von Pascal Hügli

Der Ursprung von Bitcoin lässt sich auf den 15. September 2008 zurückführen. Es ist dies der Tag, an dem die Investmentbank Lehman Brothers ihren Konkurs bekanntgibt und die Finanzkrise ihren Höhepunkt erreicht. Mit dem Bankrott von Lehman Brothers setzt eine Kaskadenwirkung ein, denn etliche weitere Banken müssen durch ihre Schutzpatrone, die Staaten, gerettet werden. Diese Rettungsaktionen lassen die Verschuldung vieler Staaten vollends aus dem Ruder laufen, weshalb letztlich die Zentralbanken zu deren gewaltigen Staatsanleihen-Ankaufprogrammen übergehen. Noch heute sind die Bilanzen der grossen Zentralbanken deswegen massiv aufgebläht und es scheint wenig realistisch, dass diese Zentralbankliquidität jemals wieder aus dem System abgeführt werden kann.

Sechs Wochen später, am 31. Oktober 2008, erreicht einige hundert Mitglieder einer Mailingliste von Kryptografie-Experten die Nachricht eines gewissen Satoshi Nakamoto. «Seit geraumer Zeit arbeite ich an einem elektronischen Zahlungssystem, das vollständig Peer-to-Peer ist und keiner vertrauenswürdigen Drittpartei bedarf», schreibt der unbekannte Absender. In seiner E-Mail findet sich ein Link zu einem White Paper, das auf eine zwei Monate zuvor registrierte Webseite hochgeladen wurde. Das neunseitige Dokument beschreibt ein Zahlungssystem namens Bitcoin. Dessen spezifisches Alleinstellungsmerkmal: es basiert auf einer Datenbank, die gleichzeitig über unzählige Rechner verteilt ist und immer aufs neue aktualisiert wird.[1] Aufgrund dieser Nonzentralität verfügt das Bitcoin-Netzwerk über keinen zentralen Server und keine Autorität, welche die Buchhaltung sicherstellen und kontrollieren könnte.

Wie funktioniert Bitcoin überhaupt?

Den adressierten Kryptografie-Freaks und Informatikern waren derartige Ideen keinesfalls neu. Bereits vor der Jahrtausendwende gab es verschiedenste solcher Ansätze, die bis dahin jedoch allesamt gescheitert waren. Der Grund: keines der Projekte vermochte die sogenannte «Double-Spending»-Problematik zu lösen, wonach jemand innerhalb des Systems sicherstellen muss, dass Transaktionen nicht doppelt ausgeführt und somit keine Geldeinheiten aus dem Nichts geschaffen werden. Bitcoin setzt dafür auf die einzelnen Netzwerkteilnehmer, genauer gesagt die «Full Nodes». Diese stehen für all jene Netzwerkteilnehmer, die sich eine vollständige Kopie der mit allen anderen «Full Nodes» geteilten Datenbank herunterladen. Aufgrund des Open-Source-Charakters der Bitcoin-Software kann sich jede Person dieses Planeten in das System miteinschalten. Da die «Full Nodes» zu jeder Zeit über den aktuellen Stand der Buchhaltung Bescheid wissen, prüfen sie, dass keine Transaktion doppelt ausgeführt wird.

Doch woran orientieren sie sich? Wie können sie wissen, ob eine Transaktion ausgeführt bzw. deren Geldeinheiten bereits ausgegeben worden sind? Sie gleichen dafür jede neue Transaktion mit der Bitcoin-Datenbank ab. Zudem werden die einzelnen Transaktionen zu einem Block zusammengefasst. Jeder Block wiederum verfügt über einen einzigartigen Hash, eine Art Identifikationsnummer, die jeweils auf den vorangegangenen Block referenziert. Auf diese Weise sind die einzelnen Blöcke über die jeweiligen Identifikationsnummern chronologisch miteinander zu einer Kette verbunden: der Blockchain. Diese Kette führt zurück bis zum Genesis-Block, dem allerersten Block und seinen Ursprungstransaktionen. Erschaffen wird so eine transparente Transaktionshistorie, über die alle Netzwerkteilnehmer verfügen und die niemand verändern kann, ohne Spuren zu hinterlassen. Erfährt ein Block auch nur die kleinste Änderung, zum Beispiel das nachträgliche Anpassen des Inhalts einer einzelnen Transaktion, ändert die Identifikationsnummer dieses Blockes. Mit der Konsequenz, dass dies eine Unstimmigkeit mit der Identifikationsnummer des Folgeblocks schafft.

Wie aber werden neue Blöcke an die bestehende Kette angefügt? Hier kommen die sogenannten Miner ins Spiel, was man mit «Schürfern» übersetzen kann. Im gegenseitigen Wettbewerb versucht ein jeder Miner, unter Verwendung von Rechenleistung schnellstmöglich einen neuen Block zu erstellen. Ungefähr alle zehn Minuten gelingt es einem Miner, einen Block zu erstellen, dessen Gesamtinhalt den Anforderungen des Bitcoin-Algorithmus entspricht.[2] Als Belohnung locken neue Bitcoins.[3] Ein vereinfachendes Bild mag an dieser Stelle helfen: Derjenige Miner, der bei einer zehnziffrigen Zahl zuerst für jede Ziffer eine Sechs gewürfelt hat, gewinnt, vorausgesetzt, der Block umfasst nur

«Den Europäern, allen voran den Schweizern, scheinen Bitcoin und Kryptowährungen wenig revolutionär zu sein, weshalb sie vor allem als Spekulationsobjekte abgetan werden.»

Pascal Hügli

Pascal Hügli, zvg.

«Dass selbst die begründende Kraft hinter Bitcoin unbekannt ist und keine zentrale Machtposition innehat, unterstreicht die Integrität und das Wertversprechen dieser Idee.»

Pascal Hügli

noch nicht ausgeführte Transaktionen. Die Miner kontrollieren ihre Ergebnisse gegenseitig und sorgen so dafür, dass stets bloss gültige Blöcke in die Blockchain integriert werden. Während sich das Finden eines gültigen Blockes als hochkompetitiv und schwierig darstellt, ist der anschliessende Prozess der Verifikation trivial.

No Rulers, no Leader: «In Code We Trust»

Es ist dieses ausgeklügelte, softwareprogrammierte Anreizsystem, das den Bitcoin von seinen Vorgängeransätzen abhebt. Wie die vorangegangenen Versuche gezeigt haben, kann ein nonzentralistisches Computernetzwerk für «Peer-to-Peer»-Werttransfer ohne ein solches Anreizsystem kaum funktionieren. Denn der Softwarecode ist nicht in Stein gemeisselt und kann theoretisch geändert und somit sabotiert werden – so auch der Bitcoin-Programmiercode. Da sich das Bitcoin-Ökosystem allerdings aus Miners, Nutzern, Entwicklern und Unternehmern zusammensetzt, die sich in ihren Interessen entgegenstehen, lassen sich Änderungen innerhalb des Systems nur schwer realisieren – vor allem dann, wenn sie mehreren Interessen zuwiderlaufen. Wann immer eine Gruppe den Bitcoin-Quellcode in eine Richtung vorentwickeln möchte, können andere Gruppierungen mit einem Fork[4], also einer Abspaltung vom Ursprungscode, liebäugeln. Diese divergierenden Interessen werden zwar von einigen als Bremsklotz wahrgenommen, die eine Systemreform fast verunmöglichen. Man kann darin aber auch ein Feature sehen und nicht einen Bug, denn die Nonzentralität verspricht Beständigkeit und Resilienz.

Das durchaus menschliche Bedürfnis nach Ordnung führt oft zu einer Sehnsucht nach einer alles überspannenden Autorität, nach einem wohlmeinenden Diktator, der Konflikte löst, indem er ein Machtwort spricht. Doch eine solche Autorität gibt es bei Bitcoin nicht. Zwar hat das Bitcoin-Ökosystem durchaus seine Galionsfiguren und Vordenker, diese sind aber über alle Haupt- und Interessengruppen verteilt. Am ehesten ein starkes Gewicht würde wohl eine Aussage des Schöpfers Satoshi Nakamoto haben. Doch dieser hat sich seit dem April 2011 nicht mehr zu Wort gemeldet. Es weiss auch niemand, wer hinter dieser Person steckt, denn der Name ist bloss ein Pseudonym.[5] Um seine wahre Identität zu verschleiern, verwendete Nakamoto mindestens drei E-Mail-Adressen, die allesamt derart aufwendig verschlüsselt waren, dass niemand die Mühe auf sich nahm, die dahinterstehende Person oder Gruppe ausfindig zu machen. Das Bitcoin-System schuf sich so seinen eigenen Schöpfungsmythos und dieser widerspiegelt letztlich das Hauptanliegen: Nonzentralität. Dass selbst die begründende Kraft hinter Bitcoin unbekannt ist und keine zentrale Machtposition innehat, unterstreicht die Integrität und das Wertversprechen dieser Idee und ist zudem äusserst raffiniert. Denn gerade in den Anfängen des Bitcoins hätte das System über die Manipulation oder Eliminierung des Begründers arg erschüttert oder gar zerstört werden können. Fehlt die neuralgische Zentralstelle, ist das viel schwieriger.

Ignorieren auf eigene Gefahr

Das Erscheinen des Bitcoin-White-Papers unmittelbar nach dem Ausbruch der globalen Finanzkrise 2008 ist wohl kaum als blosser Zufall zu bewerten. Nakamoto wies 2009 darauf hin[6], dass Zentral- sowie Geschäftsbanken ihre hohe Stellung und das Vertrauen, das ihnen im Laufe der Zeit zugekommen ist, immer wieder missbraucht hätten. Bitcoin dagegen bietet seinem Besitzer die Möglichkeit, der endgültige Herr über sein eigenes Geld zu sein. Wer über die entsprechenden Privatschlüssel[7] auf seine Bitcoins zugreifen kann, wird dies immer tun können, auch ohne die Einwilligung Dritter. Einmal abgewickelte Bitcoin-Transaktionen können durch niemanden mehr rückgängig gemacht werden. Wer seine Bitcoins selber hält, muss zudem nicht befürchten, dass diese im Hintergrund durch eine Drittpartei verliehen werden. Letztlich gibt es bei Bitcoin auch keine Zentralbank, die das Angebot an Bitcoin manipulieren kann.

Bitcoin und damit die breitere Kryptowelt sind daher in ihren Ursprüngen ein Versuch, eine mögliche Alternative oder gar Antwort auf die eben beschriebenen Entwicklungen und Probleme

unseres Finanzsystems zu bieten, und können als eine Art der Geld- oder Finanzreform gesehen werden. Diese «Reform» unterscheidet sich allerdings von anderen politisch motivierten, zentral orchestrierten Unterfangen wie Konventionalgeldern, Vollgeld oder globalen UNO-Finanzreformen. Denn Bitcoin wurde von keiner Partei lanciert, stieg ausserhalb der bestehenden Finanzstrukturen auf und erlangte seine zunehmende Bedeutung auf spontane Art und Weise durch den Zuspruch und die Wertschätzung einzelner Individuen. War bisher für komplexere Finanzangelegenheiten ein Bankkonto unerlässlich, braucht es das mit Kryptowährungen nicht mehr: ihr Potenzial, die eingesessenen, zentralisierten Vertrauensstrukturen unseres Finanzsystems aufzubrechen, ist gross.

Weit mehr als ein Spekulationsobjekt

Den Europäern, allen voran den Schweizern, scheinen Bitcoin und Kryptowährungen wenig revolutionär zu sein, weshalb sie vor allem als Spekulationsobjekte abgetan werden. Wir sind hierzulande derart «overbanked», dass uns deren Nutzen kaum einzuleuchten scheint. Schliesslich verfügen wir über mehrere Bankkonten und Kreditkarten, Twint, ein funktionierendes Bankensystem sowie einen verlässlichen Schweizer Franken. Fast niemand gehört hierzulande zu den weltweit zwei Milliarden erwachsenen Menschen, die als «unbanked» gelten und nicht einmal über ein einfaches Giro- oder Sparkonto, geschweige denn einen Zugang zu einem elektronischen Zahlungssystem wie Visa oder Mastercard verfügen. Doch auch die Verhältnisse in der Schweiz sind nicht für die Ewigkeit gemacht. Gerade weil wir uns finanziell stabile Verhältnisse und funktionelles Geld gewöhnt sind, sollten wir zur Vorsicht und Umsicht angehalten sein. Staatliche Papiergeldwährungen und deren elektronisches Derivat, das Buchgeld, waren in der Geschichte der Menschheit nicht immer Geld und werden es wohl auch nicht immer sein.

Von einigen Anlegern werden Bitcoin und andere Kryptowährungen gar als Schutz oder finanztechnisch gesprochen als «Hedge» betrachtet. Ob diese Ansicht gerechtfertigt ist, wird sich erst noch zeigen müssen. Bitcoin-Kritiker weisen mit Recht darauf hin, dass die Kryptowährung bislang nur das ungewöhnliche Marktumfeld seit der letzten Finanzkrise kennt. So haben Zentralbanken in den letzten zehn Jahren – also exakt während der bisherigen Lebenszeit von Bitcoin – mit ihrer ultraexpansiven Geldpolitik für eine regelrechte Blase bei den Vermögenswerten gesorgt. Die Marktvolatilität wurde in den Keller gedrückt, die Risikoeinpreisung auf den Finanzmärkten ist de facto eliminiert. Berechtigte Fragen kommen daher auf: Wie wird sich der Bitcoin-Preis in einer Rezession verhalten, wie nach einem möglichen Crash an den Finanzmärkten? Das weiss niemand, doch vielleicht mausert sich Bitcoin zu einer Alternative zu unserer heutigen Finanzwelt, verkörpert er in seinem Ursprung doch die Antithese dazu.

Von diesem anfänglichen institutionskritischen Geist, der in Zentralbanken und Geschäftsbanken die Horte alles Bösen sieht, ist heute nicht mehr allzu viel übrig. Ironischerweise sind mittlerweile auch jene Interessen und Kreise miteingebunden, gegen die das Kryptophänomen in seinen Anfängen angetreten ist. Zentralbanken, der Internationale Währungsfonds IMF und weitere Institutionen machen sich Gedanken über mögliche Digitalwährungen. Eine klare Unterscheidung zwischen Digital- und Kryptowährungen ist aber vonnöten, denn es gibt einen entscheidenden Unterschied: Kryptowährungen wie Bitcoin entziehen sich jeglicher Kontrolle durch eine Zentralinstanz und funktionieren eher wie digitales Bargeld. Eine Digitalwährung dagegen, wie ein durch die Schweizer Nationalbank herausgegebener «Schweizer E-Franken», kann durch die Zentraleinheit beliebig gesteuert, einfacher besteuert und notfalls manipuliert werden. Kryptoenthusiasten ist diese Differenzierung deshalb so wichtig, weil sie befürchten, dass der derzeitige Rummel um Kryptowährungen als innovatives Trittbrett für die immer häufiger geforderte Bargeldabschaffung und Digitalwährungseinführung missbraucht wird. Schliesslich soll Geld auch im Internetzeitalter ein Stück geprägte Freiheit bleiben. ‹

Lesen Sie auch:
Das Mining von Bitcoin frisst viel Strom. Das lässt sich ändern, meint Benjamin Walter auf: schweizermonat.ch

[1] Die Bitcoin-Blockchain wird alle zehn Minuten aktualisiert. So ist das im Quellcode festgeschrieben.
[2] Die Miner versuchen einen exakten Nonce-Eintrag zu finden, ein Prozess, der gemeinhin als «das Lösen eines komplexen mathematischen Problems» beschrieben wird. Tatsächlich geht es aber nur um eine simple Aufgabe, die nur ein Computer lösen kann. Auf der Suche nach der Lösung stellt der Computer milliardenfach Berechnungen an, bis endlich irgendwo im Netzwerk eine qualifizierte Antwort gefunden wird.
[3] Zurzeit erhält jeder Miner 12,5 neue Bitcoins für das Erschaffen eines neuen Blocks. Diese Anzahl verringert sich alle vier Jahre um die Hälfte, bis im Jahr 2140 alle 21 Millionen Bitcoins geschaffen worden sind.
[4] Dabei handelt es sich um eine Aufspaltung der Blockchain in eine neue und eine alte Version.
[5] Trotz einigen Theorien konnte bis heute niemand einen Beweis für die wahre Identität von Satoshi Nakamoto erbringen.
[6] p2pfoundation.ning.com/forum/topics/bitcoin-open-source
[7] Der Privatschlüssel verschafft einem Zugriff auf die auf der Blockchain verwaltete Information. Er fungiert wie ein gewöhnliches Passwort. Jeder «Private Key» verfügt über einen korrespondierenden «Public Key». Diese Adresse lässt sich mit einer E-Mail- oder besser mit einer Kontonummer vergleichen und dient dem Empfangen, Versenden und Aufbewahren der auf der Blockchain verwalteten Information.

Pascal Hügli
ist Redaktor des Punkt-Magazins. Er beschäftigt sich schon seit längerem mit Krypto-Assets und hält dazu auch Vorträge.