Dirk Fox

Bitcoin

Der Name des im Jahr 2008 unter dem Pseudonym Satoshi Nakamoto veröffentlichten digitalen Zahlungssystems Bitcoin [2] ist eigentlich irreführend – „digitale Münzen" gibt es in Bitcoin nämlich nicht. Zumindest technisch gesehen ist Bitcoin kein digitales Geld wie beispielsweise DigiCash [1]. Technisch ähnelt Bitcoin eher einem großen, öffentlichen Haushaltsbuch: In einer immer länger werdenden Liste (*Blockchain*) werden Transaktionen (*Blocks*) aneinandergereiht, deren Höhe in „Bitcoin"-Einheiten bemessen wird. Damit stellen die Teilnehmer sich gegenseitig gewissermaßen „Schuldscheine" aus, in denen sie sich zur Zahlung virtueller „Bitcoin" an andere Teilnehmer verpflichten. Neue Transaktionen werden von dem transferierenden Teilnehmer mit einem Zeitstempel versehen, digital unterschrieben und publiziert. Durch unabhängige Teilnehmer der Bitcoin Community (den *Minern*) wird jeder neue Block geprüft und im Erfolgsfall über einen kryptographischen Hashwert fest mit dem bis dato letzten Eintrag der Liste verknüpft.

Die Transaktionsliste ist per *Peer-to-Peer*-Netzwerk redundant über das Internet verteilt und jedem Teilnehmer zugänglich – eine zentrale Verwaltungsinstanz (wie z. B. eine Bank) ist überflüssig. Die Teilnehmer melden sich unter einem (oder mehreren) Pseudonym(en) an; ihre geheimen kryptografischen Schlüssel, mit denen sie die Gültigkeit einer Transaktion zu ihren Gunsten nachweisen und über ihr Guthaben weiter verfügen können, sind in einem lokalen oder von einem Dienstleister verwalteten *Wallet* gespeichert (das man nicht verlieren oder löschen sollte).

Double Spending (das mehrfache Ausgeben einer digitalen Münze), ein zentrales Problem bei elektronischen Währungen, gibt es bei Bitcoin im eigentlichen Sinne nicht. Denn in diesem „Überweisungs-Logbuch" sind keine Konto-Überziehungen erlaubt: Transferieren darf man nur Bitcoins, die man besitzt. Um Betrug zu verhindern, überprüfen die Bitcoin-Miner jede Transaktion, indem sie aus der Transaktionskette die „Kontostände" der Beteiligten berechnen und Zahlungsfähigkeit und Signatur überprüfen.

Damit ermöglicht Bitcoin aber auch die Erstellung von Profilen über das Zahlungsverhalten einzelner Teilnehmer, mit denen in Einzelfällen z. B. eine Korrelation mit Kaufvorgängen und sogar die Identifikation eines Teilnehmers möglich sein kann – anonym ist Bitcoin daher, anders als vielerorts behauptet, nicht (DigiCash und Bargeld hingegen sehr wohl).

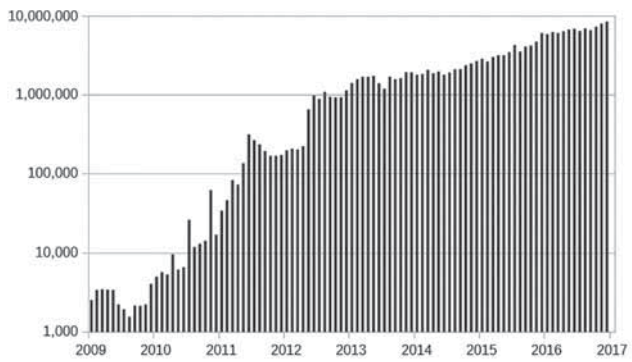
Das Bitcoin-Protokoll „bereinigt" die Transaktionsliste um nicht bestätigte Transaktionen oder (wegen möglicher kurzzeitiger Abweichungen der dezentral geführten Listen voneinander) entstandene Verzweigungen (*Forks*). Daher ist auch erst nach einer Weile (wenige Minuten bis ggf. Stunden) sicher, dass eine Transaktion auch tatsächlich in die maßgebliche Version der *Blockchain* aufgenommen wurde. Ein Transaktionsempfänger sollte also bis zur Konsolidierung der *Blockchain* warten, bevor er sich auf den Zahlungseingang verlässt. Für schnelle Transaktionen ist Bitcoin daher eher ungeeignet.

Welcher Zweig tatsächlich weitergeführt wird, entscheidet letztlich die Mehrheit der an der Überprüfung beteiligten Systeme. Stirbt ein längerer *Fork* ab, müssen dort angehängte, verwaiste Transaktionen wieder an die eigentliche *Blockchain* angehängt werden.

Wie aber wird aus einer solchen Transaktionsliste ein Zahlungssystem? Dafür müssen neue Bitcoins „geschöpft" werden – und einen Tauschwert darstellen. Die Schöpfung von Bitcoins ist raffiniert mit der Prüfung der *Blockchain* verknüpft: wer sich als Miner an Transaktionsprüfungen beteiligt, darf sich selbst mit jedem erfolgreich angefügten Block einen kleinen Bitcoin-Obolus gutschreiben. Damit füllen sich die Konten der Teilnehmer, die dafür (indirekt) mit der investierten Rechenleistung zahlen.

Den eigentlichen Wert erhalten Bitcoin über die Bereitschaft von Teilnehmern, Bitcoin gegen etwas anderes einzutauschen – z. B. gegen „echtes" Geld. Teilnehmende Bitcoin-Börsen bieten solche Tauschvorgänge an. Damit Bitcoin keine inflationäre Entwertung erfahren, wenn es immer mehr davon gibt, wächst der (Rechen-)Aufwand zum Schöpfen neuer Bitcoin im Laufe der Zeit; so werden Bitcoin nach und nach für die Teilnehmer „teurer". Außerdem ist die Maximalzahl der schöpfbaren Bitcoin durch einen stetig schrumpfenden Miner-Obolus auf 21 Millionen begrenzt. Letztlich aber basiert Bitcoin auf dem Vertrauen der Teilnehmer in die kryptografischen Verfahren und die Vertrauenswürdigkeit der Transaktionsprüfung durch die Bitcoin-Community.

Abb. 1 | Bitcoin-Transaktionen pro Monat



Tatsächlich scheint das am 03.01.2009 mit 50 Bitcoin gestartete System zu funktionieren: Bis Dezember 2016 stieg die Zahl der monatlichen Bitcoin-Transaktionen auf knapp 10 Millionen (Abb. 1); der Bitcoin-Wechselkurs verzehnfachte sich seit Januar 2015 auf z. Zt. rund 2.500 USD.

Literatur

[1] Chaum, David: *Blind signatures for untraceable payments*. Advances in Cryptology, Proceedings of Crypto. Springer, 1983, S. 199–203.

[2] Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. bitcoin.org, Oktober 2008.