

Kartenmanagement-Glossar

Bitcoin

Von Ewald Judt ■ Bitcoin ist der Versuch, Geld zu schaffen, das von keiner Regierung, keiner Notenbank und keiner Geschäftsbank abhängig ist. Heute gibt es Geld als Münzgeld, Papiergeld und als Buchgeld, das unter der Kontrolle von Notenbanken (ent)steht. Als Währung ist es das vom Staat autorisierte/anerkannte Geld, das im jeweiligen Wirtschaftsraum allgemein als gesetzliches Zahlungsmittel akzeptiert wird. Erfolgreiche Währungen existieren lange. Kommt es aber zu einer Währungskrise, die zu einer raschen Abwertung einer Währung führt, leidet das Vertrauen in sie. In einer derartigen Situation kommt es oft zu Ersatzwährungen; das können andere (vertrauenswürdiger) Währungen sein, Kurantmünzen (meist aus Gold), deren Wert durch das Metall gedeckt ist, aus dem sie besteht, oder Notgeld, das von Dritten emittiert wird und nicht vom Staat autorisiert/anerkannt ist. Sie existieren in Krisenzeiten neben der offiziellen Währung.

Netzgeld ohne durchschlagenden Erfolg

Mit dem Aufkommen des Netzeitalters wurde ergänzend zu Münz-, Papier- und Buchgeld die Idee des Netzgeldes entwickelt. Netzgeld sind elektronische Zahlungseinheiten meist mit eigener Bezeichnung, die auf Rechnern aller Art gespeichert werden können, allerdings keine gesetzlichen Zahlungsmittel sind. Von jedem Rechner kann das Netzgeld zu anderen Rechnern des Netzes transferiert und dort wieder gespeichert werden, ohne dass Bargeld oder Buchgeld bewegt wird. Das Netzgeld und seine Bewegungen werden durch kryptografische Verfahren geschützt. Es ähnelt dem

Ersatzgeld, wenngleich es im Gegensatz zu ihm mit Buch- oder Bargeld erworben wird und beim Rücktausch wieder zum gesetzlichen Zahlungsmittel wird.

Die ab den siebziger Jahren des vorigen Jahrhunderts geschaffenen Netzgeld-Realisierungen haben aber alle nicht zu dem Erfolg geführt, den die Proponenten erwarteten. Ein Beispiel für ein derart gescheitertes digitales Geld ist e-Cash, das nach einigen Jahren ohne die hochgesteckten Ziele zu erreichen wieder eingestellt wurde.

Weiterentwicklung des digitalen Geldes

Wie Netzgeld können auch Bitcoin-Einheiten („Bitcoins“) transferiert werden. Bitcoin ist aber vom System her eine Weiterentwicklung des digitalen Geldes zu einer digitalen Währung, die selbst Geld schöpft. Der große Unterschied zu Ersatzgeld/Netzgeld ist somit, dass es nicht von einem Dritten (wie Unternehmen oder Gemeinden) emittiert oder aus Buchgeld gewechselt wird, sondern in einem „Miningprozess“ (wie beim Schürfen des Goldes für die Goldmünzen) gewonnen wird.

Das Konzept dazu basiert auf einem 2008 veröffentlichten White Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“, als dessen Autor Satoshi Nakamoto fungiert. Satoshi Nakamoto dürfte allerdings das Pseudonym für eine ganze Gruppe sein, welche die Bitcoin-Software entwickelte.

Die Geldschöpfung, das „Mining“, kann theoretisch durch alle Netzwerkteilnehmer

erfolgen. Sie erfolgt durch die Lösung hochkomplexer mathematischer Formeln, wozu große Rechnerleistung benötigt wird. Mit der Zeit und zunehmender Anzahl von Bitcoin-Einheiten wird es immer schwerer, neue Einheiten zu „schürfen“. Mittlerweile wird – es sind schon über zwölf Millionen Bitcoin-Einheiten im Umlauf – bereits eine so große Rechnerleistung (mit hohem Stromverbrauch) benötigt, dass nicht mehr allzu viele Rechner dazu in der Lage (und die Stromkosten vielfach schon zu hoch) sind.

Der Grund dafür ist, dass das Bitcoin-„Mining“ von der Konzeption her bewusst immer schwieriger wird. Längstens ab 21 Millionen Bitcoin-Einheiten und spätestens 2033 wird demzufolge kein weiteres „Mining“ mehr möglich sein. Diese Überlegungen der Entwickler sind vom Goldstandard inspiriert und sollen Bitcoin vor Inflation schützen.

Die Gefahr einer deflationären Entwicklung der Bitcoin-Einheiten, die aufgrund Geldmangels ständig an Wert gewinnen, und damit vorwiegend zur (spekulativen) Wertaufbewahrung und kaum mehr zum Geldtransfer herangezogen werden, wird in der Konzeption negiert.

Da heute von „normalen“ Nutzern in der Regel keine Bitcoin-Einheiten mehr generiert werden können, müssen sie, wenn sie mit Bitcoin-Einheiten im Internet bezahlen beziehungsweise Bitcoin-Überweisungen durchführen wollen, Bitcoin-Einheiten anschaffen. Dies ist über Online-Anbieter möglich. Hier gibt es einerseits Online-Börsen (Bitcoin Exchanges) bei denen – wie an der richtigen Börse – Käufer einen Höchst- und Verkäufer einen Mindestpreis festlegen, ab dem

die Transaktion stattfinden kann. Die Bitcoin-Einheiten sind vom Verkäufer an der Online-Börse zu deponieren und werden auf den Rechner des Käufers übermittelt. Der Gegenwert der Transaktion ist vom Käufer in Buchgeld zu zahlen und wird dem Verkäufer in Buchgeld überwiesen. Andererseits gibt es Wechselstuben (Fixed Rate Shops), wo gegen Buchgeld zu einem angegebenen Kurs Bitcoin-Einheiten angeschafft werden können, die dann auf den Rechner des Käufers übertragen werden.

Peer-to-Peer-Version des Netzgeldes

Was den Geldtransfer betrifft, so ist Bitcoin eine reine „Peer-to-Peer“-Version des Netzgelds. In der realen Welt ist das Zahlungsmittel somit nicht vertreten. Es erlaubt den Übertrag von Bitcoin-Einheiten von einem Rechner auf einen anderen Rechner ohne dass eine dritte Partei (Bank) in die Transaktion involviert ist.

Bitcoin-Transaktionen können nur zwischen den Teilnehmern am Netzwerk durchgeführt werden. Das sind hauptsächlich Geldtransfers für alle möglichen im Internet angebotenen Waren und Dienstleistungen. Zum Geldtransfer müssen die Teilnehmer auf ihrem Rechner ein Bitcoin-Programm starten, mit dessen Hilfe sie die Transaktionen ausführen.

Sowohl die Speicherung von Bitcoin-Einheiten als auch deren Erhalt oder Weitergabe sind durch starke Verschlüsselung vor Verlust und Diebstahl geschützt. Darüber hinaus wird jede Transaktion von Bitcoin-Einheiten zwischen den Netzwerkteilnehmern in einer im Bitcoin-Netzwerk verteilten Datenbank signiert aufgezeichnet.

Inwieweit Bitcoin im Gegensatz zu diversen anderen Vorgängern bei Netzgeld zu einem Erfolg führen wird, hängt davon ab, ob es gelingt, Bitcoin-Einheiten außerhalb von Nischen zu etablieren. Es

liegt hier das klassische Problem eines zweiseitigen Marktes vor, wo es notwendig ist, viele Nutzer sowohl auf der Käuferseite als auch auf der Verkäuferseite zu haben, die Zahlungen mit Bitcoin-Einheiten leisten beziehungsweise annehmen. Derzeit halten sich wohl deshalb die Transaktionen – verglichen mit denen konventioneller Zahlungsmittel im Internet – in einem engen Rahmen, weshalb Bitcoin-Einheiten heute vorwiegend zur

(spekulativen) Wertanlage genutzt werden. Dies wahrscheinlich allerdings nur so lange, wie das Vertrauen in Bitcoin generell und in eine Wertsteigerung vorhanden ist sowie die Sicherheit gewährleistet ist. Offen ist auch noch, ob und wie Bitcoin (und auch andere mögliche Alternativwährungen) einer gesetzlichen Regelung zugeführt werden.

Dr. Ewald Judt ist Honorarprofessor an der Wirtschaftsuniversität Wien, ewald.judt@wu.ac.at