Bitcoin ist der Beginn einer Alternative zum staatlichen Geld

Dem Euro ein Schnippchen schlagen, ohne sich selbst ein Bein zu stellen – geht das?
Über die Chancen und Risiken einer digitalen Währung, die gerade den Kinderschuhen entwächst | *Von Gerold Lechner*

Die von Zentralbanken betriebene Geldpolitik sorgt bei den Bürgern für Befürchtungen hinsichtlich des Werterhalts ihrer Geldanlage. Mögliche bevorstehende negative Zinsen auf Sparguthaben würden den Sparer schrittweise enteignen. Um negative Zinsen dauerhaft durchzusetzen, bedarf es zwar einer Bargeldbegrenzung oder gar eines Bargeldverbotes. Die Frage aber, wie ein privates Sparvermögen mittel- und langfristig ohne Kaufkraftverlust zu erhalten ist, stellt sich schon jetzt.

Gerold Lechner ist Inhaber einer Softwarefirma und als IT-Experte Bitcoin-Nutzer der ersten Stunde. Er ist Mitglied des Ludwig von Mises Institut Deutschland e.V. und befasst sich in seiner Freizeit mit Finanz- und Makroökonomie. Für den HAUPTSTADTBRIEF beschreibt er, wie Bitcoin funktioniert, wie ein Bitcoin-Konto eröffnet und wie mit Bitcoin bezahlt und gespart werden kann. Er zeigt die Chancen und Risiken dieser digitalen Währung, die ohne Staat und Währungshüter auskommt. FOTO: PRIVAT

Die bisher sinnvolle Investition in Vermögenswerte wie Aktien oder Immobilien wird zunehmend riskant: Die expansive Geldpolitik der letzten Jahre hat bereits zu einer starken Inflationierung dieser Werte geführt – eine Konsolidierung ist daher nicht ausgeschlossen. Der Wertverlust von Aktien wäre bei einer weltweiten Rezession besonders stark.

Eine Alternative, auch hinsichtlich der Wertaufbewahrung, bieten digitale Währungen. Die bekannteste unter ihnen ist Bitcoin. Bekanntheit ist aber nicht gleichbedeutend mit Kenntnis. Was ist, wie geht Bitcoin? Hinter Bitcoin steht kein realer Wert, der Wert eines Bitcoin ergibt sich ausschließlich durch Angebot und Nachfrage. Eine Geldmanipulation durch Währungshüter ist ausgeschlossen: Bitcoin werden dezentral in einem Rechnernetz mit Hilfe einer quelloffenen Software verwaltet und geschöpft. Es gibt keine Instanz, die Bitcoin in irgendeiner Form kontrolliert – diese digitale Währung kann weder von Staaten noch von Individuen gesteuert werden.

Hinter Bitcoin steht kein realer Wert, der Wert eines Bitcoin ergibt sich ausschließlich durch Angebot und Nachfrage.

Technisch gesehen besteht Bitcoin aus einem weltweiten Peer-to-Peer-Netzwerk, bei dem jeder beteiligte Rechner eine Kopie der Datenbank verwaltet, in der die Historie aller Transaktionen abgebildet ist. Die Technologie hinter Bitcoin heißt Blockchain und wird jetzt weltweit von Banken und Börsen auf Anwendbarkeit erprobt. Bei einer Blockchain ist es essentiell, dass es möglichst viele Rechner gibt, die dieses dezentrale System aufrechterhalten. Als Belohnung, dem System die Rechenleistung zur Verfügung zu stellen, gibt es eine beschränkte Geldschöpfung, das sogenannte Mining.

Hierfür müssen mathematische Aufgaben gelöst werden. Hat ein Rechner eine solche Aufgabe gelöst, erhält er einen Bitcoin, der neu geschaffen wurde. Die Geldschöpfung ist jedoch durch einen Algorithmus beschränkt. Die Anzahl der Bitcoin, die in einem Zeitraum, zum Beispiel in diesem Jahr 2016, geschöpft werden, ist determiniert. Aktuell gibt es zirka 15 Millionen Bitcoin. Die Menge an Bitcoins nähert sich asymptotisch 21 Millionen (siehe Abbildung „Vorhersage der Gesamtmenge an Bitcoin bis zum Jahr 2033“).

In der Begrenzung der Menge ähnelt Bitcoin ein wenig dem Gold, das sich auch nicht beliebig und schon gar nicht anstrengungslos vermehren lässt. Deshalb unterscheidet sich Bitcoin deutlich von staatlichen Währungen wie dem Euro oder dem Dollar, deren Menge beliebig vermehrbar ist, weil hier das Geld durch Kreditvergabe aus dem Nichts geschöpft wird. So hat sich die Geldmenge in der Eurozone seit dem Jahr 2000 mehr als verdoppelt, wie die Europäische Zentralbank 2015 mitteilte. Der Wert- und Kaufkraftverlust vermindert jedes noch so kleine private Vermögen und macht eine Alternative überlegenswert. Also, wie geht Bitcoin?

Um Bitcoin nutzen zu können, wird eine digitale Brieftasche (englisch Wallet) benötigt. Eine Wallet besteht aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel ist die Adresse, die als Identifizierung

Aktuell gibt es zirka 15 Millionen Bitcoin. Die Menge an Bitcoins nähert sich asymptotisch 21 Millionen.

der Wallet dient. Der private Schlüssel wird benötigt, um Transaktionen zu autorisieren und durchzuführen. Wer über den privaten Schlüssel einer Wallet verfügt, ist damit zugleich der Inhaber. Es ist also elementar, den privaten Schlüssel zu schützen. Den öffentlichen Schlüssel kann man sich wie eine Briefkastennummer vorstellen: Jeder kann sie sehen und dorthin Bitcoin überweisen. Bitcoin können in beliebig kleiner Stückelung transferiert werden. Mittlerweile ist es üblich, Überweisungen in Millibitcoin (mBTC) durchzuführen. 1 Millibitcoin entspricht einem Tausendstel Bitcoin (0,001 BTC), das bedeutet: 1 mBTC = 0,38 Euro, 10 mBTC = 3,76 Euro usw. und 1 BTC dann = 375,82 Euro (Kurs vom 28. März 2016).

Es gibt mehrere Möglichkeiten, Bitcoin zu erwerben oder zu veräußern. Die einfachste ist, Bitcoin über einen Marktplatz zu erwerben. Der mit 260 000 Benutzern in Europa bekannteste Marktplatz ist bitcoin.de. Über diese mehrsprachige Online-Plattform lassen sich mittels Banküberweisung Bitcoin zum aktuellen Marktpreis kaufen. Wer sich dort erfolgreich registriert hat, für den wird auch automatisch eine Wallet erstellt, mit der man Bitcoin empfangen und überweisen kann. Bitcoin.de verwaltet den privaten Schlüssel intern, d.h. man tritt mit der technischen Ebene, auf der Bitcoin verwaltet werden, nicht direkt in Kontakt. Das hat den Vorteil: Jeder Benutzer mit grundlegenden Internet-Kenntnissen kann über bitcoin.de Bitcoins erwerben und Transaktionen durchführen.

Hier liegt zugleich ein Nachteil: Sollte die Plattform einmal gehackt werden, wie es bei dem japanischen Marktplatz Mt. Gox der Fall war, und sollten dabei Bitcoin entwendet werden, kann die Plattform insolvent werden und den Benutzern, die keinen direkten Zugriff auf den privaten Schlüssel haben, die ihnen eigentlich zustehenden Bitcoin nicht mehr ausbezahlen oder transferieren. Das ist wie bei einer Bank, bei der man ein Sparbuch hat, die insolvent ist – nur dass es bei Bitcoin keine Einlagensicherung bis 100 000 Euro gibt.

Wer Bitcoin zu hundert Prozent anonym, also ohne Abbuchung von einem Bankkonto, erwerben möchte, muss einen Bitcoin-Automaten nutzen, um Bitcoin gegen Bargeld zu erwerben. Die österreichische Firma Coinfinity (coinfinity.co) betreibt solche Automaten in Wien, Graz und Klagenfurt. Die Benutzung ist denkbar einfach: Man hält den öffentlichen Schlüssel in Form des QR-Codes (ausgedruckt oder per Smartphone) an einen Scanner und füttert den Automaten mit Bargeld. Im Anschluss wird der Gegenwert in Bitcoin auf die private Wallet überwiesen. FOTO: GENERALBYTES.COM

Dafür hat Bitcoin eine Möglichkeit, die das Bankensystem nicht bietet: Das Risiko einer Insolvenz des Marktplatzes lässt sich für dessen Nutzer ausschließen. Wer hundertprozentige Kontrolle haben und exklusiv über die Bitcoin verfügen möchte, kann sich eine Wallet selber erstellen. Laut bitcoin.de werden rund 98 Prozent der Bitcoin nicht auf Servern, sondern offline auf einer so genannten Cold-Wallet gespeichert. Wer sich so eine Cold-Wallet anlegen und darauf direkt Zugriff mittels privaten Schlüssels haben möchte, kann dafür verschiedene Generatoren verwenden. Technisch gesehen können nahezu beliebig viele öffentliche und private Schlüssel durch Zufallsgeneratoren erstellt werden. Ein bekannter Generator ist die Webseite bitaddress.org, die auch offline genutzt werden kann. (Das Ergebnis dieses Generators zeigt die Abbildung „Mittels bitaddress.org generierte Cold-Wallet“.)

Mittels bitaddress.org generierte Cold-Wallet

Wer hundertprozentige Kontrolle haben und exklusiv über die Bitcoin verfügen möchte, kann sich eine sogenannte Cold-Wallet anlegen, auf die nur deren Besitzer direkten Zugriff mittels privaten Schlüssels hat. Den öffentlichen und den privaten Schlüssel für eine Cold-Wallet erstellt ein Zufallsgenerator wie die Webseite bitaddress.org (Abbildung).

Die Schlüssel können auch als QR-Code dargestellt werden – das ist nur eine andere Darstellung der Zahlen- und Buchstabenkombination – und dann von mobilen Geräten gelesen werden. Der öffentliche Schlüssel kann mit jedem geteilt werden und dient wie beschrieben als Identifizierung der Wallet. Der private Schlüssel wird für ausgehende Transaktionen benötigt. Es bietet sich an, diesen auszudrucken und an einem sicheren Ort zu verwahren.

Um eine mittels bitaddress.org neu erstellte und anfangs leere Cold-Wallet aufzuladen, sind anschließend die auf bitcoin.de erworbenen Bitcoin auf die erstellte Cold-Wallet zu überweisen. Das geht direkt und sehr einfach über bitcoin.de. Wer so verfährt, nutzt bitcoin.de ausschließlich für den Erwerb und sorgt für die Aufbewahrung in seiner Cold-Wallet selber – und muss eine Insolvenz des Marktplatzes nicht fürchten.

Dieses Verfahren ist für fortgeschrittene oder technisch versierte Bitcoin-Halter sinnvoll, die gerne selber über den privaten Schlüssel verfügen und außer dem Erwerb nichts mit der Plattform bitcoin.de zu tun haben möchten. Ein durchschnittlicher Benutzer muss nicht unbedingt so verfahren, da bitcoin.de als seriös und sicher anerkannt ist. Dann bliebe die Wallet in der Verwaltung von bitcoin.de – und das aus heutiger Sicht geringe Restrisiko, dass bitcoin.de etwa durch einen Hacker-Angriff insolvent wird.

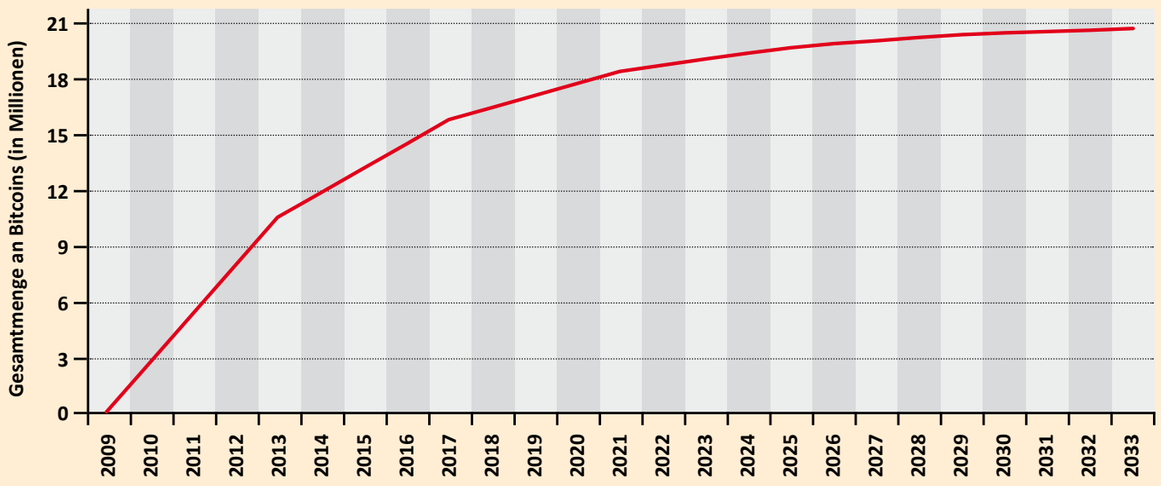
Wenn man Überweisungen von einer Cold-Wallet durchführen möchte, so bietet sich die kostenlose Software Bitcoin Core an. Es existieren auch diverse Smartphone-Apps, mit denen man Wallets erstellen und Transaktionen durch Scannen von QR-Codes durchführen kann. Es gibt bereits mit Schwerpunkten in Berlin etliche Geschäfte und Lokale, in denen man mit Bitcoin bezahlen kann. Die dortige Tageszeitung taz akzeptiert online Bitcoin zur Bezahlung von Inhalten. Ein Meilenstein für die Alltagsnutzung von Bitcoin war die Rechtsprechung des Europäischen Gerichtshofes vom 22. Oktober 2015 (Rechtssache C-264/14). Der EuGH hat festgelegt, dass auf Bitcoin-Transaktionen keine Umsatzsteuer abzuführen ist und Bitcoin als Devise zu behandeln ist. Folglich haben Unternehmen in Sachen Bitcoin die gleichen rechtlichen und buchhalterischen Pflichten wie bei anderen Devisen zu beachten.

Bitcoin wurde nicht konzipiert, um staatliches Geld zu ersetzen. Bitcoin stellt jedoch eine Alternative zum Staatsgeld dar.

Bleibt die Frage: Ist Bitcoin als dauerhaftes Wertaufbewahrungsmittel sinnvoll? Aktuell (Stand vom 28. März 2016) kostet ein Bitcoin um die 375 Euro. Bei 15 Millionen Bitcoin entspricht das einer Marktkapitalisierung von zirka 5,5 Milliarden Euro. Zum Vergleich: Die Marktkapitalisierung von Apple beträgt etwa 520 Milliarden Euro. Im Umkehrschluss bedeutet das, dass der Bitcoin-Kurs noch deutlich Potential bietet. Sollten Turbulenzen an den Finanzmärkten auftreten, so sind die Chancen hoch, dass mehr Investoren und Privatpersonen als Alternative einen Teil ihrer Gelder in Bitcoin anlegen – es gibt bereits jetzt erste Hedgefonds, die aktiv in Bitcoin investiert sind.

Auf der anderen Seite ist das Risiko nicht außer Acht zu lassen: Bitcoin lebt ausschließlich von Angebot und Nachfrage. Sollten sich langfristig andere digitale Währungen durchsetzen und die Nachfrage an Bitcoin dadurch sinken, so ist es möglich, dass Bitcoin an Wert verlieren und am Ende wertlos werden. Das geschähe jedoch nicht über Nacht, sondern wäre Ergebnis eines digitalen Währungswettbewerbs. Der marktwirtschaftliche Wettbewerbsgedanke hat überhaupt erst zur Entstehung des digitalen Geldes geführt: Bitcoin wurde nicht konzipiert, um staatliches Geld zu ersetzen. Es ist aus machtpolitischen Gründen auch nachvollziehbar, dass Zentralbanken dieses Privileg nicht aufgeben werden – Bitcoin stellt jedoch eine Alternative zum Staatsgeld dar, das sich nun seinerseits unversehens in einem Währungswettbewerb befindet. Gut so, auch wenn er noch bescheiden ist. ♦

Vorhersage der Gesamtmenge an Bitcoins bis zum Jahr 2033



Die Geldschöpfung von Bitcoin ist durch einen Algorithmus beschränkt, die Anzahl der Bitcoins ist deshalb endlich. Aktuell gibt es zirka 15 Millionen Bitcoin. Die Menge an Bitcoin nähert sich asymptotisch 21 Millionen.

„Mein erster Bitcoin oder Wie kaufe ich einen Bitcoin auf dem bitcoin.de Marktplatz“ ist eine Gebrauchsanweisung, die das von unserem Autor Gerold Lechner geschilderte Verfahren Schritt für Schritt mit Abbildungen am Computer nachvollziehbar macht. Website dieses Bitcoin-Blogs: http://bitcoinblog.de/mein-erster-bitcoin

IMPRESSUM

Die Hintergrund-Seiten in der Berliner Morgenpost entstehen in Zusammenarbeit mit DER HAUPTSTADTBRIEF – Informations- und Hintergrund-Dienst aus Berlin.

Ausgabe vom 6. Mai 2016

Verlag: HAUPTSTADTBRIEF Berlin Verlagsgesellschaft mbH, Tempelhofer Ufer 23–24, 10963 Berlin, Tel. 030 / 21 50 54 00, Fax 030 / 21 50 54 47, info@derhauptstadtbrief.de

Herausgeber: Detlef Prinz
Redaktionsdirektor: Dr. Rainer Bieling
Layout: Mike Zastrow, Manuel Schwartz
Verantwortlich im Sinne des Pressegesetzes: Dr. Rainer Bieling
Anschriften für alle siehe Verlag

Anzeigen: Jan Schiller (Leiter Vermarktung), Berliner Morgenpost GmbH, Kurfürstendamm 21–22, 10719 Berlin, Tel. 030 / 88 72 776 – 00, jan.schiller@morgenpost.de

Druck: Axel Springer SE, Druckhaus Spandau GmbH & Co. KG, Brunsbütteler Damm 156–172, 13581 Berlin

Diese Ausgabe finden Sie auch online unter www.derhauptstadtbrief.de