Dobernig, Harald; Daube, Carl Heinz

Working Paper

Digitale Währungssysteme - Funktionsweise und Einsatzmöglichkeiten

Harald Dobernig, Carl Heinz Daube[*]

Digitale Währungssysteme

Funktionsweise und Einsatzmöglichkeiten

Abstract

Digital currency systems like Bitcoin want to overcome weaknesses of classical currency systems. The goal is to establish a global payment system, which is organized by the users alone independently of central instances. By executing transactions with a digital currency, anonymity and low transaction costs are expected.

The Bitcoin concept provides a complex algorithm that limits the amount of money and to prevent inflationary developments, but the assessment of this concept varies. Some authors see it as a chance to revolutionize the money system technologically, others see it as the most exciting open source software project of the present.

It is shown that the Bitcoin concept only partially meets the important requirements of a monetary system, such as acceptance, protection against inflation, security and stability. Therefore, digital currency systems are only partially able to remedy the weaknesses of classical currency systems. The main causes are the lack of value preservation and the volatility of the currency. Even a complete anonymity cannot be achieved even in a decentralized IT system. Nevertheless, digital currency systems have the potential for further development.

Zusammenfassung

Digitale Währungssysteme wie Bitcoin wollen Schwächen klassischer Währungssysteme überwinden. Ziel ist die Etablierung eines globalen Bezahlsystems, das unabhängig von

* *Die Autoren (Professur für Wirtschaftsinformatik und Professur für Finanzierung) lehren und forschen an der NBS Northern Business School am Institut für Unternehmensrechnung, Controlling und Finanzmanagement.*

zentralen Instanzen durch die Nutzer allein organisiert wird. Bei der Durchführung der Transaktionen werden vor allem Anonymität und geringe Transaktionskosten erwartet.

Das Bitcoin-Konzept sieht einen komplexen Algorithmus vor, der die Geldmenge begrenzt und damit vor allem inflationäre Entwicklungen verhindern soll. Die Bewertung dieses Konzepts ist unterschiedlich. Einige Autoren sehen darin die Chance, das Geldsystem technologisch zu revolutionieren, andere das gewagteste Open-Source-Softwareprojekt der Gegenwart.

Es wird gezeigt, dass das Bitcoin-Konzept nur teilweise die wichtigsten Anforderungen die an ein Geldsystem gestellt werden, wie Akzeptanz, Inflationsschutz, Sicherheit und Stabilität erfüllt. Digitale Währungssysteme sind daher nur bedingt in der Lage, die vermeintlichen Schwächen klassischer Währungssysteme zu beheben. Ursächlich sind vor allem die mangelnde Wertsicherungsfunktion und die Volatilität der Währung. Auch eine vollkommene Anonymität ist selbst in einem dezentralen IT-System nicht zur Gänze herstellbar. Dennoch haben digitale Währungssysteme das Potential zur Weiterentwicklung.

1. Einleitung

Digitale Güter und Netzeffekte haben das Potential zu grundlegenden ökonomischen Strukturveränderungen. Vor allem im Zusammenwirken beider Sachverhalte zeigt sich jedoch das gesamte Ausmaß an Innovationskraft. Im Kontext der Digitalisierung ist besonders das Beispiel digitaler Währungssysteme einprägsam.

Währungen wie der US-Dollar oder der Euro sind zentralisiert. Sie werden von einer kleinen Zahl von Institutionen (Notenbanken, Banken, Kreditkartenunternehmen etc.) kontrolliert. Im Fall digitaler Währungen wird mittels kryptografischer Verfahren Geld geschaffen, das in *Peer-to-Peer*-Computernetzwerken ausgetauscht wird. Diese *Peer-to-Peer*-Netzwerke sind quasi File-Sharing-Systeme, die zum gegenseitigen Austausch von Dateien genutzt werden. Jedes Endgerät arbeitet im Systemverbund als Client für andere Endgeräte.

Das digitale Geld steht dabei nicht unter der Kontrolle durch eine zentrale Instanz, sondern das Netzwerk kontrolliert die Zahlungen und stellt das digitale Geld bereit. Um dieses Geld nutzen zu können, muss der Nutzer eine Software in Form einer digitalen Geldbörse (*Digital Wallet*) vom Netzwerk herunterladen und lokal installieren. Diese Geldbörse lässt sich wie ein Onlinebankkonto nutzen. Die Transaktionen finden immer direkt von Nutzer zu Nutzer statt, so dass es keine Institutionen als Zwischenhändler gibt.

Digitale Währungssysteme können *per se* die Tausch-, Rechen- und Wertaufbewahrungsfunktion des Geldes erfüllen und hinzu kommen folgende (ideale) Anforderungen an digitales Geld:

- Beständigkeit: Geld ist langlebig und haltbar, sowohl physisch als auch in Bezug auf die Kaufkraft;
- Breite Anwendung: Grad an Akzeptanz seitens der Nutzer;
- Einmaligkeit: Es ist nicht möglich, Geld zu kopieren und die Kopie bei einem Zahlungsvorgang zu verwenden;
- Knappheit: Es existiert eine limitierte Menge von Währungseinheiten;

- Konsistenz: Trotz der leichten Teilbarkeit sind Wert und Qualität einer bestimmten (Teil-)Einheit immer gleich;
- Sicherheit: Geld ist schwer zu fälschen und seine Authentizität ist leicht zu überprüfen;
- Teilbarkeit: Geld muss leicht in kleinere Einheiten zerlegt werden können, um kleine Transaktionen zu ermöglichen.

Elektronische Geldkonzepte müssen sich daran messen lassen, ob und inwieweit sie diese Merkmale und Eigenschaften erfüllen können. Im Folgenden wird beispielhaft auf das Bitcoin-Konzept als digitales Geld eingegangen.[1] Die Grundlagen digitaler Währungen sind im Internet gut zu recherchieren. Man findet Angaben zur Theorie, die hinter der Digitalwährung stehen und Angaben zu deren Einsatzmöglichkeiten sowie zu den naheliegenden und praxisrelevanten Fragen: Wie kann man Bitcoins erwerben und wie kann man damit bezahlen?

In Deutschland ist Bitcoin nach der Feststellung der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine Rechnungseinheit (*Unit of Account*) gemäß § 1 Abs. 11 Satz 1 Kreditwesengesetz (KWG), die „in multilateralen Verrechnungskreisen eingesetzt" werden kann. Bitcoin ist damit eine mit Devisen vergleichbare Werteinheit.[2]

2. Bitcoin

Unter dem Pseudonym *Satoshi Nakamoto* erschien im Jahr 2009 das initiale *White Paper* zum Bitcoin-Konzept.[3] Seitdem wird die Idee von Softwareentwicklern der Open-Source-Gemeinschaft fortgeführt. Ziel ist es, eine Alternativwährung zu schaffen, die zum einen unabhängig von Notenbanken und Staaten und zum anderen inflationssicher ist. Bitcoin ähneln dabei vom Konzept her früheren Währungen, wie z.B. Gold oder Silber, die durch begrenzte Lagerflächen einer zu hohen Produktion Grenzen setzen. Bei Bitcoin wird die Limitierung durch einen mathematischen Algorithmus sichergestellt. Im Jahr 2012 wurde die

[1] Vgl. Clement, R., & Schreiber, D. (2016), S. 328 ff.
[2] Vgl. Münzer, J. (2013).
[3] Vgl. Nakamoto, S. (2009).

Bitcoin Foundation (vgl. https://bitcoinfoundation.org/) gegründet, um Bitcoin zu standardisieren, zu schützen und zu vermarkten.

Bitcoin ist nur ein Beispiel für eine dezentralisierte digitale Währung, die mittels eines *Peer-to-Peer*(P2P)-Netzwerks und auf Basis einer Verschlüsselungstechnologie arbeitet. Als Vorteile von Bitcoin gelten:[4]

- Ähnliche Eigenschaften wie Bargeld;
- Dezentralisierung, d.h. keine zentralen Ausgabestellen oder Kontrolleinrichtungen;
- Einfache und weitgehend kostenlose Transaktionen.

Das Herzstück von Bitcoin ist das Mining. Es dient zur Bestätigung von Transaktionen im Netzwerk, vor allem aber zur Schaffung neuer Bitcoins. Während des Miningprozesses werden neue Blöcke an Daten generiert, aus der die sogenannte Blockchain eine Art Meta-Datenbank entsteht, in der alle Transaktionen gespeichert und von den Bitcoin-Minern verifiziert werden. Im Miningprozess wird mittels einer speziellen Prüfwertberechnung, auch als sicherer Hash Algorithmus bekannt, ein Wert unterhalb eines gewissen Limits gesucht, der sich aus dem aktuellen Schwierigkeitsgrad (*Difficulty*) der Prüfwertberechnung ergibt. Als Eingabe für dessen Berechnung dienen dabei die Kopfdaten (*Header*) des neu zu generierenden Datenblocks (*Block*), bestehend aus folgenden Daten:

- Einmaliger Zufallswert (*Nonce*) mit dem Zweck, den Blockinhalt zu verändern;
- Liste von Transaktionen (*Transactions*);
- Prüfwert des Vorgängerblocks, um die Erzeugung einer durchgehenden Blockchain zu gewährleisten.

Ist das Ergebnis der durchgeführten Berechnung kleiner als das Limit, gilt ein neuer Datenblock als gefunden und wird der Blockchain hinzugefügt. Andernfalls wird die *Nonce* des

[4] Vgl. u.a. Kerscher, D. (2014), S. 16 ff.

Datenblocks verändert und erneut berechnet. Der Schwierigkeitsgrad ist dabei so ausgelegt, dass im Schnitt etwa alle zehn Minuten ein neuer Datenblock generiert wird.

Wenn nun von einem Miner ein gültiger Datenblock gefunden wurde, erhält dieser neben den Gebühren für die Transaktionen, die mit diesem Block bestätigt sind, noch eine festgelegte Summe an Bitcoins (12,5 Bitcoins pro Block) als Anreiz dafür, Rechenkapazität zur Lösung der Aufgabe bereit gestellt zu haben.[5] Würden die einzelnen Blöcke schneller generiert, entstünde zu viel virtuelles Geld.

Die Anzahl der pro Block verteilten Bitcoins halbiert sich alle 210.000 Blöcke. Rein rechnerisch ergibt sich daraus eine Maximalanzahl (*M*) von 21 Mio. Bitcoins:

$$M = \lim_{n\to\infty} \sum_{i=0}^{n} \left(210.000 \cdot \frac{50}{2^i}\right) = 210.000 \cdot 50 \cdot \lim_{n\to\infty} \sum_{i=0}^{n} \left(\frac{1}{2^i}\right) = 210.000 \cdot 50 \cdot 2 = 21.000.000 \text{ BTC} \quad (1)$$

Aktuell kommen pro Tag maximal 1.800 Einheiten hinzu.[6] Je näher das Limit rückt, desto weniger Bitcoins werden generiert. Aktuell ist der Schwierigkeitsgrad so hoch, dass sich das Mining mit dem privaten Computer nicht lohnt. Serverlandschaften sind nötig, um den steigenden Schwierigkeitsgrad bewältigen zu können. Dieser Aufwand gewährleistet zusätzlich die Sicherheit des Systems.[7] Wenn jemand mehr als 50 Prozent der Gesamtrechenleistung kontrollieren könnte, so würde er Überweisungen verfälschen, da er z.B. seine eigenen Überweisungen gewissermaßen selbst bestätigten könnte. Der Aufwand für eine sogenannte 51-Prozent-Attacke ist aber aufgrund der komplexen Rechenaufgabe hoch. Ein flexibler mathematischer Algorithmus stellt sicher, dass die Komplexität der von den Akteuren zu lösenden Berechnungen mit der Gesamtrechenleistung des Netzwerks Schritt hält. Desto mehr Rechenleistung vorhanden ist, je komplexer werden die Berechnungen.

[5] Nach der Einführung von Bitcoin im Jahr 2009 fand die erste Halbierung von 50 auf 25 Bitcoins pro Block im Jahr 2012 statt. Im Jahr 2016 fand eine Reduzierung um die Hälfte auf 12,5 Bitcoins pro Block statt.
[6] Pro Tag werden maximal 144 neue Blöcke erzeugt. Aktuell beträgt die Belohnung pro Block (*Block Reward*) bei 12,5 Bitcoin; daraus ergibt sich pro Tag eine Belohnung von 12,5·144=1800 Bitcoins. Das nächste *Block Reward Halving* wird im Jahr 2020 erwartet.
[7] Vgl. Sorge, C., & Krohn-Grimberghe, A. (2013).

Dem dahinterliegenden Algorithmus geschuldet, wird die maximale Anzahl an Bitcoins hypothetisch im Jahr 2130 erreicht sein. Zwischen dem Jahr 2033 und 2130 werden nur noch rund 330.000 Bitcoins hinzukommen. In diesem Zusammenhang muss berücksichtigt werden, dass Bitcoins z.B. wegen verlorener Passwörter oder fehlender Back-Ups faktisch nutzlos sind. Diese Bitcoins existieren zwar noch, da aber niemand sich als deren Eigentümer ausweisen kann, können diese Bitcoins nicht mehr genutzt werden. So gesehen wird die Anzahl aller Bitcoins, die sich im Umlauf befinden, langfristig schrumpfen.

Da 21 Mio. Bitcoins (vgl. Formel 1), gemessen an der Weltbevölkerung, nur eine verschwindend geringe Menge ist, lässt sich ein Bitcoin aktuell in 100 Mio. Untereinheiten (sogenannte Satoshis) aufteilen. Geläufig ist folgende Einteilung:

1 BTC	1 Bitcoin
0,01 BTC	1 cBTC (1 Centbitcoin)
0,001 BTC	1 mBTC (1 Millibitcoin)
0,000001 BTC	1 µBTC (1 Microbitcoin)
0,00000001 BTC	1 Satoshi (derzeit kleinste Untereinheit, benannt nach *Satoshi Nakamoto*)

Bei Bedarf kann die Aufteilung durch neue Bitcoin-Versionen noch feingranularer gestaltet werden. Da pro Block immer nur ein Prüfwert gültig und die Anzahl der gültigen Blöcke beschränkt ist, lässt sich eine deflationäre Eigenschaft der Bitcoin ableiten, sollte sich die Währung durchsetzen.

Der Prozess der Wertfindung gestaltet sich schwierig, denn theoretisch könnte ein Bitcoin ca. 43.000 EUR $\left(= \frac{900\ Mrd.\ EUR}{21\ Mio.\ BTC}\right)$ wert sein, wenn Bitcoin sämtliches Eurobargeld (geschätzt auf 900 Mrd. EUR) ersetzen würde. Wenn hingegen im anderen Extremfall Bitcoin-Zahlungen entweder massiv reguliert würden oder sich nur als vorübergehende Erscheinung erweisen, könnte der Wert gegen Null tendieren.[8]

[8] Vgl. Eckert, D., & Zschäpitz, H. (2017).

3. Technische Ausgestaltung

Das Bitcoin-System lässt sich in drei Elemente einteilen, die wechselseitig miteinander verknüpft sind:[9]

- Die Nutzer, die Bitcoins besitzen und Transkationen tätigen.
- Die Blockchain, die die Transaktionshistorie abbildet und zeigt, welche Adressen über wie viele Bitcoins verfügen.
- Die Miner, die dafür zuständig sind, Bitcoins-Transaktionen und die Blockchain anzufügen und dafür mit neuen Bitcoins belohnt werden.

Bitcoins funktionieren wie ein Online-Bankkonto und die Blockchain-Technik verbindet dabei die Elemente der Nutzer mit den Minern. Des Weiteren existiert eine Liste an Konten sowie eine weitere Liste der Transaktionen aller Teilnehmer. Es bestehen aber folgende Unterschiede zu konventionellen Bankkonten:[10]

- Alle Teilnehmer des Netzwerks haben eine Kopie aller Konten und können alle Transaktionen einsehen;
- Alle Teilnehmer des Netzwerks können diese Liste speichern und anderen zur Verfügung stellen;
- Der Eigentum von digitalen Geldeinheiten lässt sich durch die vollständige Liste an Transaktionen zurückverfolgen.

3.1 Digitale Buchführung und digitale Geldbörse

Bitcoins lassen sich gegen herkömmliche Währungen wie z.B. Dollar oder Euro eintauschen. Onlinebörsen (vgl. z.B. https://www.bitcoin.de/) unterstützen den Währungstausch gegen Zahlung einer Gebühr. Bitcoins lassen sich dann grundsätzlich zur Bezahlung von Waren und Dienstleistungen verwenden.

[9] Vgl. Kerscher, D. (2014), S. 10 ff.
[10] Vgl. Pfnür, C. (2014), S. 6.

Die Zahlungen können nicht mehr rückgängig gemacht werden. Dies stellt im Onlinehandel für den Verkäufer einen Vorteil dar, da Rückbuchungen z.B. bei betrügerischen Käufen nicht möglich sind. Bitcoins besitzen keinen in anderen Währungen ausdrückbaren Wert. Im Jahr 2010 wurden die ersten Wechselkurse von Akteuren in Bitcoin-Foren ausgehandelt. Gegenwärtig wird der Wechselkurs tagesaktuell ausgewiesen (vgl. z.B. https://bitcointicker.co/).

Bitcoins als Buchführungssystem

Bitcoins sind Datenpakete, die durch die gemeinsame Arbeit einer Vielzahl von Computern geschaffen und von den Nutzern in digitalen Geldbörsen gespeichert werden. Im Unterschied zu anderen Zahlsystemen (z.B. Kreditkarten) ist Bitcoin ein dezentrales System, bei dem Transaktionen nicht über eine zentrale Stelle abgewickelt werden. Es muss daher immer eine Instanz geben, die dafür sorgt, dass

- digitales Geld nicht kopiert und mehrfach verwendet wird,
- keine falschen Transaktionen stattfinden bzw.
- Transaktionen nicht mehrfach vorkommen.

Die Lösung besteht in einer öffentlichen digitalen Meta-Datenbank (*Blockchain*), die, vergleichbar einem Orderbuch, jede Transaktion präzise aufzeichnet. Erfasst werden alle Überweisungen, die zwischen den Konten getätigt werden. Dabei werden Sender, Empfänger und der Geldbetrag aufgelistet.

Diese Datenbank soll das Problem des doppelten Bezahlens (*Double Spending*) verhindern. Jede Transaktion wird immer in der Blockchain gespeichert. Damit lässt sich der Weg der Bitcoins bis zu ihrer Entstehung zurückverfolgen. Jeder Teilnehmer des Bitcoin-Netzwerks kann die vollständige Blockchain herunterladen und anhand dieser nachträglich jede Transaktion verifizieren.

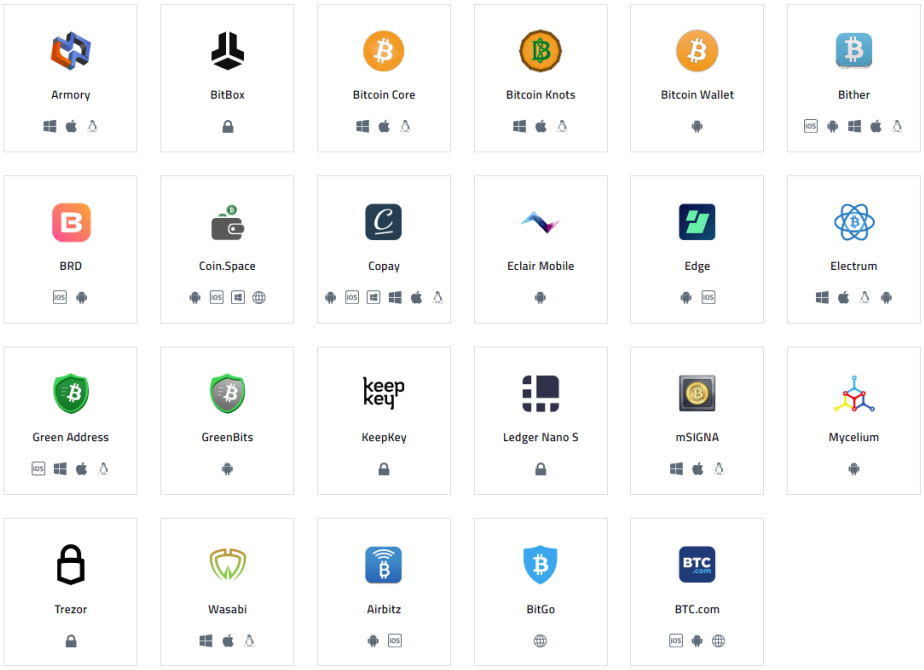
In der Wirtschaftsinformatik werden bereits seit den 1980er Jahren anonyme Bezahlverfahren diskutiert, bei denen der Nutzer einzelne Zahlungen den Teilnehmern nicht zuordnen kann

und Händler anhand eines Bezahlvorgangs nicht erkennen können, ob der gleiche Nutzer schon einmal eine Transaktion mit ihnen durchgeführt hat. Würde nun ein Nutzer versuchen, sein Geld doppelt auszugeben, wäre das für andere Nutzer sofort nachvollziehbar und die Transaktion selbst würde als ungültig verworfen. Bitcoins bieten dabei einen hohen Grad an Anonymität. Nur beim Umtausch von herkömmlichen Geld in Bitcoins können Daten über den Nutzer erhoben werden. Die einzelnen Transaktionsprozesse lassen sich jedoch nicht zurückverfolgen.

Digitale Geldbörse

Um an der Bitcoin-Welt teilnehmen zu können, ist eine elektronische Geldbörse (*Digital Wallet*) bzw. ein Konto erforderlich (vgl. Abb. 1). Dieses Konto wird automatisch mit dem Herunterladen der Software angelegt. Die Datei enthält einen privaten Schlüssel zum eigenen Konto, der vergleichbar ist mit einem Passwort oder einer PIN, wie sie beim Zugang zu einem herkömmlichen Bankkonto am Geldautomaten oder beim Onlinebanking erforderlich sind. Der Zugangsschlüssel besteht aus 51 Zeichen, z.B.:
3ytmu88XZgwSccpfucHb4y9yyo76DtFxSyc9rQyNb5JfrgNL828

Abb. 1 Digitale Wallets



Quelle: bitcoin.org (2019).

Der private Schlüssel sollte kopiert und immer sicher verwahrt werden. Es existieren Software-Programme, die diesen kryptischen Schlüssel z.B. in einen Quick Response(QR)-Code umwandeln, der sich mithilfe einer Kamera und entsprechender Scanner-Software auf Notebooks, Tablets oder Smartphone einlesen lässt.

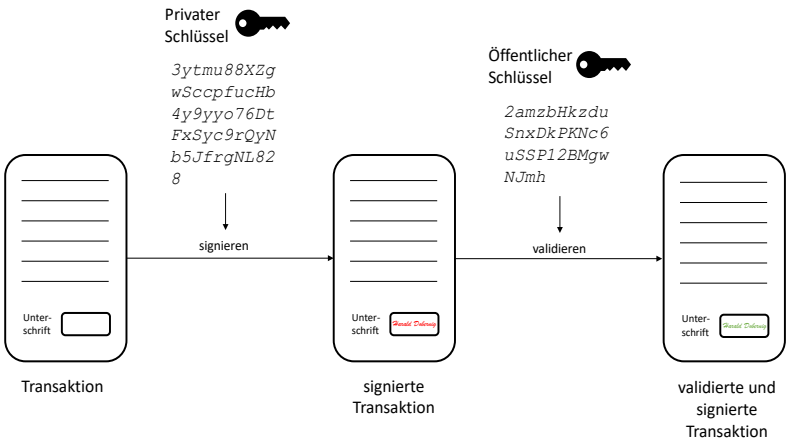
Geht jedoch der Schlüssel verloren oder gelangen Unbefugte in seinen Besitz, ist das Konto nicht mehr sicher. Im Offline Wallet (*Cold Storage*) können z.B. Ersparnisse gespeichert werden. Bitcoins sind verloren, wenn der Wallet-Speicherort oder die Passwörter nicht mehr verfügbar sind.

Zudem enthält das Wallet weitere Daten, wie z.B. die Transaktionshistorie, die jedoch nur benötigt werden, damit die Software nicht die gesamte Blockchain durchleuchten muss. Auch ohne diese Historie sind die Bitcoins mit dem privaten Schlüssel wiederherstellbar.

3.2 Verschlüsselung und digitale Signatur

Bei den Überweisungen von einem Bitcoin-Konto zu einem anderen wird der private Schlüssel verwendet, um die jeweiligen Transaktionen zu signieren (vgl. Abb. 2).

Abb. 2 Digitales Signaturverfahren

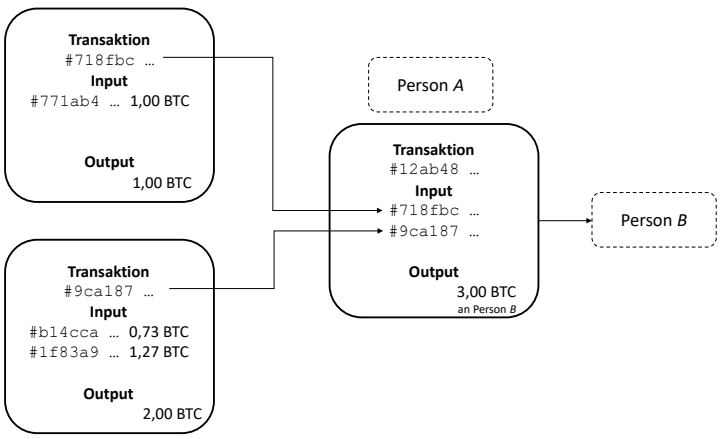


Quelle: In Anlehnung an Pfnür, C. (2014), S. 7.

Mit dieser Signatur wird gewährleistet, dass nur der Eigentümer des privaten Schlüssels (Inhaber des Bitcoin-Kontos) eine Überweisung durchführen kann. Damit das Bitcoin-Netzwerk erkennt, dass eine Überweisung valide signiert wurde, gibt es einen weiteren zweiten Schlüssel, der als öffentlicher Schlüssel bezeichnet wird. Dieser Schlüssel besteht aus 34 Zeichen, wie z.B.: *2amzbHkzduSnxDkPKNc6uSSP12BMgwNJmh*

Mithilfe dieses öffentlichen Schlüssels kann der Inhalt einer Nachricht entschlüsselt werden. Der öffentliche Schlüssel kann beliebig verteilt werden, da er nicht zum Unterzeichnen einer Überweisung berechtigt. Die Bitcoin-Adresse stellt eine Kurzform des öffentlichen Schlüssels dar. Diese Adresse ist dem Netzwerk bekannt und wird immer in der Blockchain abgespeichert. Bei dieser Adresse handelt es sich um eine beliebige Zeichenkette, die kürzer als der öffentliche Schlüssel und der private Schlüssel ist. Im Bitcoin-Netzwerk wird bei jeder Transaktion, die von einer Bitcoin-Adresse aus gemacht wird, die Signatur mit dem öffentlichen Schlüssel des Absenders zur Bestätigung entschlüsselt. Entspricht der entschlüsselte Inhalt dem Format einer gültigen Überweisung, so ist damit bewiesen, dass der private Schlüssel zur Verschlüsselung benutzt wurde. Im Bitcoin-Netzwerk existiert ein Wert nicht als absolute Zahl wie bei einem herkömmlichen Bankkonto. Es setzt sich der verfügbare Wert eines Bitcoin-Kontos aus der Historie aller zugrundeliegenden Transaktionen zusammen (vgl. Abb. 3).

Abb. 3 Ablauf einer Transaktion



Quelle: In Anlehnung an Pfnür, C. (2014), S. 10.

Möchte z.B. eine Person *A* an eine Person *B* einen bestimmten Bitcoin-Betrag übersenden, muss Person *A* belegen, dass sie zuvor bereits Transaktionen in mindestens gleicher Höhe erworben hat. Person *A* gibt also gegenüber Person *B* alle Transaktionen an, die sie selbst erworben hat. Diese werden als *Coins* beschrieben. Person *B* kann nun mithilfe der Blockchain in der gesamten Historie recherchieren, woher diese Inputs stammen, wie viel sie wert sind und ob Person *A* diese bereits ausgegeben hat oder nicht. Für *A* ist die Übertragung an *B* ein Output, für *B* ist die Transaktion von *A* ein Input. Abbildung 3 zeigt die Transaktion von *A* an *B* unter Verwendung zweier Inputs. Die Transaktion `#12ab48...` ist die Transaktion an *B*. Für *B* ist dies ein Input, den *B* bei einer späteren Transaktion benutzen kann.

Bei einer Transaktion kann es durchausvorkommen, dass die Inputwerte nicht die benötigte Höhe des zu versendenden Transaktionsvolumens haben. Sobald ein Nutzer z.B. 4 BTC zur Verfügung hat, jedoch einen geringeren Betrag ausgeben möchte, muss eine Art Wechselgeld eingeführt werden. Daher wird der Output immer auf zwei Zieladressen aufgeteilt: die erste ist die des eigentlichen Empfängers und trägt genau die zu versendende Geldsumme, die zweite ist die eigene Adresse, auf die der Gesamtbetrag der verwendeten Inputs, abzüglich des versendeten Betrags und einer Transaktionsgebühr, übertragen wird (vgl. Abb. 4).

Abb. 4 Typische Inputs und Outputs einer Transaktion

Inputs	
von Adresse	Betrag (BTC)
`e3fhsxs1 ...`	0,21943440
`e3fhsxs1 ...`	0,10179509
`e3fhsxs1 ...`	0,2242057
Gesamt	0,54543519

Outputs	
von Adresse	Betrag (BTC)
`e2mzvj12 ...`	0,50000000
`e3fhsxs1 ...`	0,04533519
Gesamt	0,54543519
Gebühr	-0,0001

Quelle: In Anlehnung an Pfnür, C. (2014), S. 12.

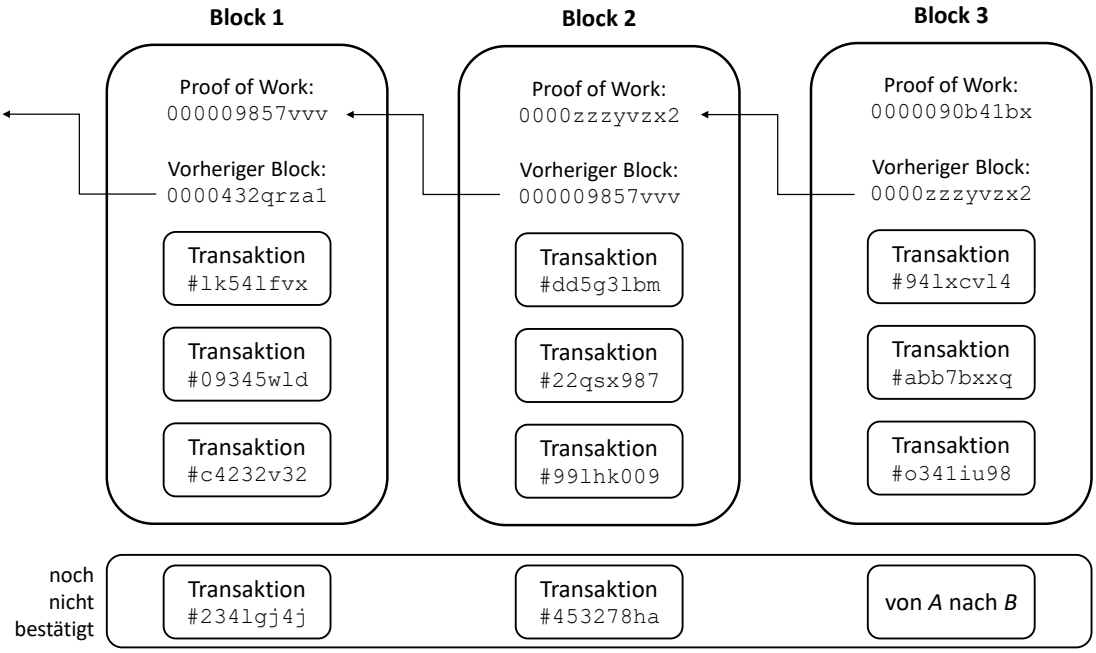
3.3 Digitale Verwaltung und Blockchain

In einem dezentralen und verteilten System ist zu klären, wie in einer Gruppe alle unabhängig voneinander zum gewünschten Ergebnis kommen. Mögliche Angreifer, die sich unter eine Gruppe mengen, dürfen das System nicht stören. In der Informatik ist diese Sachlage als das Problem der Byzantinischen Generäle bekannt. Im Bitcoin-Konzept wird die Lösung in der

Blockchain gefunden. Die Blockchain selbst besteht aus Blöcken, die jeweils folgende Informationen enthalten (vgl. Abb. 5):

- Bisherige Referenz, als Verweis auf vorhergehende Blocksätze als Zeitleiste;
- Nachweis der Arbeit (*Proof of Work*);
- Transaktionen oder Nachrichten, die zwischen Nutzern gesendet worden sind.

Abb. 5 Blöcke und Blockchain



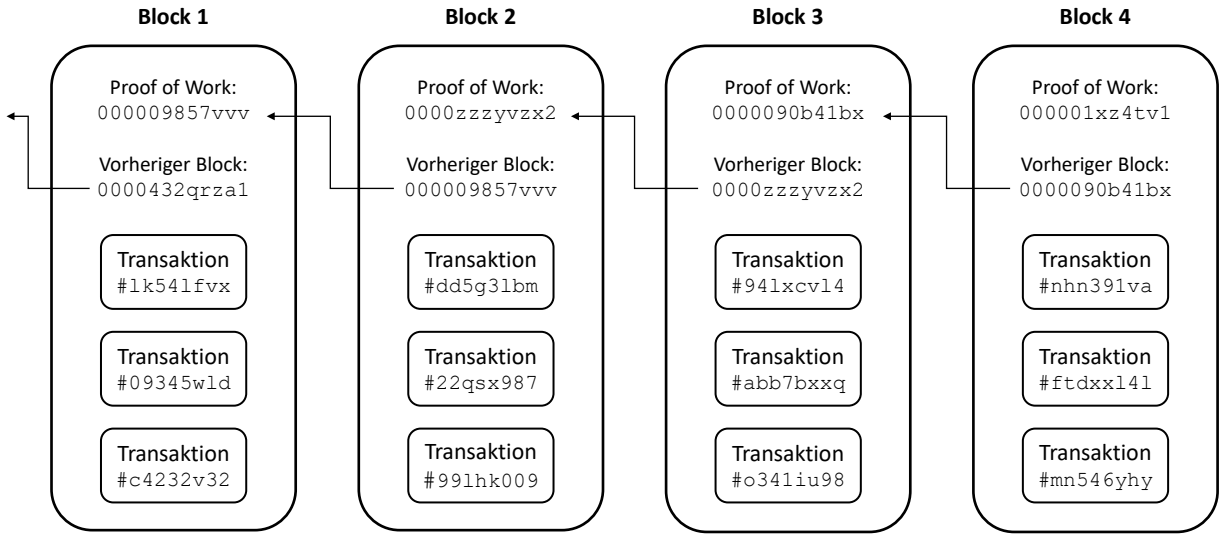
Quelle: Eigene Darstellung.

Die Blockchain ist das gemeinsame öffentliche Buchungssystem des gesamten Bitcoin-Netzwerks und alle bestätigten Buchungen werden in der Blockchain gespeichert. Integrität und Chronologie der Transaktionen in der Blockchain werden durch die Kryptographie sichergestellt.

Für die Bestätigung müssen die Transaktionen in einen Block gepackt werden, der kryptographischen Regeln entsprechen muss, die wiederum durch das Bitcoin-Netzwerk verifiziert werden (vgl. Abb. 6). Durch diese kryptographischen Regeln wird verhindert, dass vorangehende Blöcke abgeändert werden. Eine Veränderung würde alle folgenden

Datenblöcke nutzlos machen. Wartende und noch nicht bestätigte Transaktionen (wie z.B. eine Überweisung von *A* an *B*) müssen in die Blockchain mitaufgenommen werden. Dieser Prozess entspricht dem oben dargestellten Mining-Prozess.

Abb. 6 Sicherheit von Blöcken



Quelle: Eigene Darstellung.

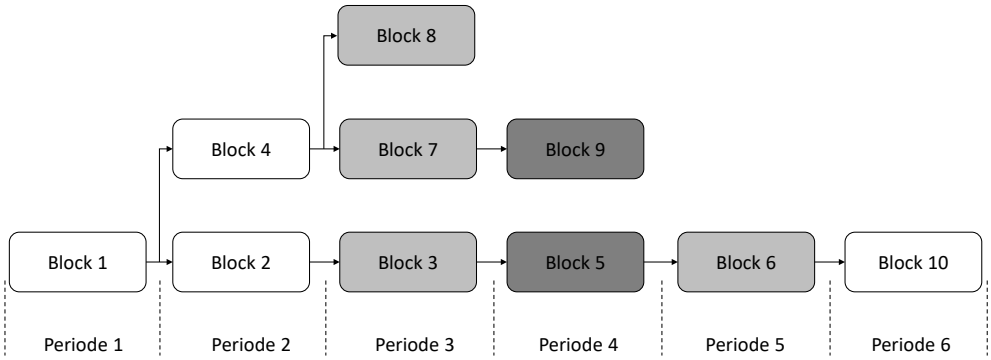
Eine Fälschung von Bitcoins oder von Transaktionen ist – mit aktuellen technischen Mitteln – aufgrund des verwendeten asymmetrischen kryptographischen Verfahrens, das digitale Signaturen erzeugt und überprüft, nicht möglich. Das doppelte Ausgeben derselben Bitcoins wird mittels eines sogenannten *Proof of Work*-Verfahrens verhindert. Ein Angreifer müsste im Durchschnitt mehr Rechenzeit aufwenden als alle legalen Bitcoin-Nutzer zusammen, um den *Proof of Work* zu fälschen.

Ist eine Transaktion durch das Bitcoin-Netzwerk bestätigt worden, so gilt diese Transaktion als verifiziert und eine Rückabwicklung der Transaktion ist unwahrscheinlich. Transaktionen erhalten immer eine Bestätigung, wenn sie in einem Block gespeichert sind. Für kleine Transaktionen kann eine einzelne Bestätigung als sicher betrachtet werden. Bei größeren

Geldmengen (z.B. im Wert von 1.000 EUR) ist es sinnvoll, auf mehrere Bestätigungen zu warten, von denen jede zusätzliche das Risiko einer Rückabwicklung reduziert.

Die Transaktionsgebühr beträgt gegenwärtig 32 Satoshis/Byte (abhängig von der Implementierung der Bitcoin-Software). Für eine mittlere Transaktionsgröße von 225 Bytes ergibt sich eine Gebühr von 7.200 Satoshis. Bei einem Kurs von rund 3.190 EUR kostet die Bestätigung einer Transaktion von 7.200 Satoshis (=0,072 mBTC) etwa 0,23 EUR (Stand: 12.02.2019).[11] Diese Gebühr wird dem Netzknoten, der den *Proof of Work* erstellt, angerechnet. Das Verfahren soll verhindern, dass das Bitcoin-Netzwerk durch kleine Transaktionen überlastet wird. Perspektivisch sind die Transaktionsgebühren als Belohnung für die Bereitstellung von Rechenleistung vorgesehen. Sollte zeitgleich eine Lösung für den *Proof of Work* gefunden werden, gilt die längste Blockchain als gültig, da in ihr die größere Rechenleistung enthalten ist (vgl. Abb. 8).

Abb. 8 Entwicklung simultaner Blockchains



Quelle: Eigene Darstellung.

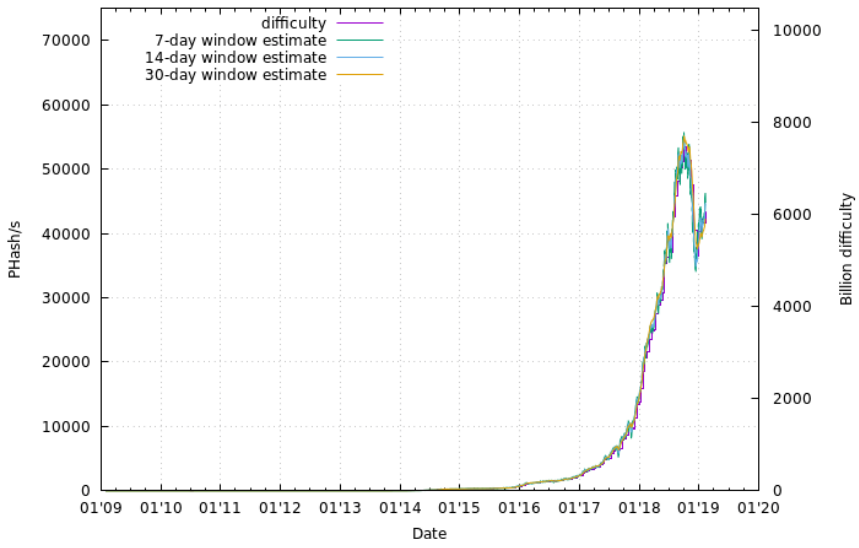
In Abb. 8 wird beispielhaft angenommen, dass sich die Blockchain, ausgehend von Periode 1, in Periode 2 teilt, da die Blöcke 2 und 4 gleichzeitig erstellt worden sind. In Periode 3 werden

[11] Vgl. bitcoinfees.earn.com (2019).

drei Blöcke gleichzeitig erstellt, einer davon aufbauend auf Block 2 und zwei weitere aufbauend auf Block 4. In Periode 4 fällt die Kette 1 – 4 – 7 weg, weil in den beiden anderen Ketten jeweils ein neuer Block geschaffen wurde. In Periode 5 ist zu erkennen, dass nur noch Block 6 erzeugt wurde und alle Nutzer auf die Blockkette 1 – 2 – 3 – 5 – 6 umschwenken. In Periode 6 wird Block 10 erstellt und es hat sich die mit ihm verbundene Kette durchgesetzt. Alle Transaktionen, die in diesen Blöcken enthalten sind, sind gültig. Nach sechs aufeinander folgenden Blöcken wird eine verbindliche Bestätigung unterstellt.

Die verwendeten Zeichenketten garantieren, dass eine Transaktion nur einmal bestätigt und durchgeführt wurde. Danach ist sie nicht mehr als offen gekennzeichnet und kann für die Berechnung neuer Blöcke verwendet werden. Ein Angreifer, der z.B. Bitcoins doppelt ausgeben möchte und dazu einen in der Vergangenheit liegenden Block verändern will, müsste in der Lage sein, den Arbeitsbeweis des vergangenen Blocks zu berechnen, ihn zu verändern und alle folgenden Blöcke schneller zu berechnen als die anderen Teilnehmer des Bitcoin-Netzwerks. Solange sich der größere Teil der Rechnerleistung in den Händen ehrlicher Nutzer befindet, erscheint diese Gefahr nicht gegeben. Die im Netzwerk insgesamt verfügbare Rechnergeschwindigkeit lässt sich tagesaktuell in Erfahrung bringen.

Abb. 9 Steigerung der Rechengeschwindigkeit des Bitcoin-Netzwerkes



PHash/s … Peta (10^{15}) Hash pro Sekunde

Quelle: bitcoin.sipa.be (2019).

In Abb. 9 ist die *Hash Rate*, die die Maßeinheit der Rechengeschwindigkeit des Bitcoin-Netzwerks darstellt, abgebildet; des Weiteren ist die *Difficulty* mitabgebildet. Diese Größe stellt ein relatives Maß dar, wie schwierig es ist, einen neuen Block zu finden. Sie wird immer an der Anzahl bzw. der Schnelligkeit der Miner angepasst, damit im Schnitt alle zehn Minuten ein Datenblock generiert wird.

4. Charakterisierung des Bitcoin-Konzepts

Nachfolgend wollen die Autoren das Bitcoin-Konzept anhand vier beispielhafter Kategorien wie Akzeptanz, Inflationsschutz, Sicherheit und Stabilität mit einer klassischen Währung (hier: Euro) vergleichen.[12]

Akzeptanz

Eine digitale Währung hat nur dauerhaft Bestand, wenn sie mehrheitlich unabhängig von der zugrundeliegenden IT-Technologie akzeptiert wird. Bezogen auf Bitcoin ist es sinnvoll, zu analysieren, wie viele Unternehmen bzw. Händler Bitcoin als Zahlungsmethode anbieten und wie viele Kunden mit Bitcoin zahlen.

Die Erstellung genauer statistischer Erhebungen zu den Teilnehmerzahlen ist schwierig, da sich niemand für die Teilnahme am System registrieren muss. Die Zahl der Konten, die an Transaktionen beteiligt sind, lässt sich zwar ermitteln, jedoch kann jeder Teilnehmer sich beliebig viele Konten anlegen. Das Bitcoin-Konzept verspricht kostengünstige Transaktionen und vor allem Anonymität. Empirische Umfragen zeigen, dass vielen Verbrauchern bisher das Konzept nur unzureichend bekannt ist. Das Potential ist jedoch vorhanden.

Auf der Anbieterseite liegt bei Zahlungen mit Bitcoin der größte Vorteil in den geringen Transaktionskosten. So müssen Händler bei Kreditkarten mit ca. 2-3% des Umsatzes erheblich mehr an Transaktionskosten an das ausgebende Unternehmen abführen. Aufgrund der relativ hohen Volatilität von Bitcoin ist aber die Akzeptanz eher gering. Größere Unternehmen,

[12] Vgl. Daube, C. H., & Dobernig, H. (2019).

Handelsplattformen und Zahlungsverfahren (z.B. Paypal) gehen vermehrt dazu über, Bitcoin zu akzeptieren.

Inflationsschutz

Der Euro wird als gesetzliches Zahlungsmittel von der Europäischen Zentralbank herausgegeben. Sie entscheidet über Höhe und Zusammensetzung wichtiger Geldmengenaggregate. Im Prinzip ist eine unbegrenzte und damit inflationäre Ausgabe neuen Geldes möglich, da es sich um eine ungedeckte und nicht durch Sachwerte hinterlegte Währung handelt.

Das Bitcoin-Konzept verspricht, inflationären Gefahren vorzubeugen bzw. diese komplett auszuschalten. Die Geldschöpfung erfolgt komplett dezentral und ist – zumindest rein theoretisch – bei 21 Mio. BTC gedeckelt. Aufgrund defekter Festplatten, Schadsoftware oder allgemeiner Datenverluste gehen mit den verlorenen Wallets auch die Bitcoins verloren, sodass die zur Verfügung stehende Geldmenge durchaus als inflationssicher eingeordnet werden kann.

Die Open-Source Gemeinschaft könnte den Entschluss fassen, den Algorithmus zu ändern. Würde durch die regelmäßige Halbierung der gutgeschriebenen Bitcoins ein Wert nahe Null erreicht, wäre Mining nicht mehr attraktiv, falls nicht die Transaktionsgebühren entsprechend stiegen. Um das Netzwerk trotzdem weiter zu betreiben, könnte eine Änderung des dahinterliegenden Bitcoin-Protokolls notwendig werden.

Am Anfang wurde das BTC-Konzept nicht durch das Zahlungsversprechen einer zentralen Stelle gesichert und die Nutzung war aufgrund fehlender Angebote nicht möglich. Bitcoins hatten daher keinen bezifferbaren Wert. Inzwischen wird ein großer Teil der in Umlauf befindlichen Bitcoins von wenigen Institutionen gehalten, die vom Wertzuwachs profitieren.

Es ist damit zu rechnen, dass konkurrierende digitale Währungssysteme entstehen. Es existiert bereits jetzt ein Wettbewerb unter digitalen Währungen und spekulativ orientierte Nutzer könnten beliebig zwischen verschiedenen Währungen wechseln.

Sicherheit

In Deutschland ist die Einlagensicherung der Banken je Kunde gesetzlich auf 100.000 EUR begrenzt. Sparkassen und Genossenschaftsbanken schützen Kundeneinlagen in unbegrenzter Höhe. Bitcoins sind durch Verschlüsselungstechnologien gesichert, die grundsätzlich ein hohes Maß an Schutz bieten. Ein Verlust des digitalen Wallets, z.B. durch einen Schaden der Festplatte oder durch Hackerangriffe, ist jedoch nicht auszuschließen.

Aus Sicht der Autoren kann der Entwurf des Bitcoin-Protokolls als gelungen gelten. Bislang sind keine schwerwiegenden Fehler bekanntgeworden. Allerdings darf kein Angreifer mehr Rechenleistung zur Verfügung haben als alle Teilnehmer zusammengenommen. Ein 51-Prozent-Angriff könnte dazu führen, dass Bitcoins doppelt und mehrfach ausgegeben würden. Gegenwärtig droht ein solches Szenario zwar nicht – vollkommen auszuschließen ist es nicht.

Für Einzelnutzer ist das Mining nicht attraktiv. Wer Bitcoins nutzen möchte, ist gezwungen, die Währung über eine Online-Plattform zu beziehen. Auf diesem Gebiet galt die Handelsplattform Mt. Gox als Pionier, die im Februar 2014 Insolvenz anmelden musste, nachdem öffentlich wurde, dass rund 850.000 BTC verloren gegangen waren. Diese Summe entsprach den kompletten Einlagen des Unternehmens (100.000 BTC) und seiner Kunden (750.000 BTC). Ursächlich hierfür waren Programmierlücken.[13]

Die Insolvenz von Mt. Gox weist auf einen wichtigen Aspekt des Bitcoin-Konzepts hin. Im Vergleich zu Einlagen im herkömmlichen Bankensystem kann der Besitzer von Bitcoins jederzeit vollumfänglich darüber verfügen. Auslagerungen größerer Beträge auf Dritte bedürfen daher umfassender Sicherungsmaßnahmen und einer gewissen Regulierung.

Stabilität

Ebenso wie der Euro ist auch BTC eine sogenannte Fiat-Währung, also ein Tauschmittel ohne eigenen Wert, das vom Vertrauen getragen wird. Bei Bitcoins fehlen eine zentrale Instanz und

[13] Vgl. Kannenberg, A. (2014).

der Status als gesetzliches Zahlungsmittel. Da es keine Anbieter gibt, sind z.B. Angaben zum Binnenwert schwierig bzw. nicht möglich.

Bitcoins können – vor allem im Internet – zum Einkaufen verwendet werden. An unregulierten Tauschbörsen ergibt sich der Kurs aus Angebot und Nachfrage. Bezogen auf den Außenwert kann der Bitcoin-Kurs gegenüber anderen Währungen analysiert werden. Ein Blick auf Marktplätze zeigt eine relativ hohe Volatilität des BTC-Wechselkurses gegenüber anderen Währungen.[14] Zusammenfassend kann festgehalten werden, dass das Bitcoin-Konzept nur teilweise die Anforderungen, die an ein Geldsystem gestellt werden, erfüllt (vgl. Tab. 1).

Tab. 1 Charakterisierung des Bitcoin-Konzepts

Kriterium	**Charakteristik**	**Kommentar**
Akzeptanz	eher nicht	perspektivisch ist eine größere Akzeptanz bei Verbrauchern und Anbietern möglich, wenn das Vertrauen in die Stabilität des Bitcoin-Netzwerks hergestellt wird
Inflationsschutz	tendenziell ja, nämlich durch kontrollierte Geldschöpfung	perspektivisch gesehen, so ist eine Änderung des Protokolls nicht auszuschließen; zu erwarten ist eine zunehmende Konkurrenz durch andere digitale Währungssysteme
Sicherheit	technologisch ja, dies ist durch die Verschlüsselung gegeben	persönlicher Verlust ist möglich; 51-%-Problematik ist nicht auszuschließen; bei Auslagerung auf Handelsplattformen entstehen ggf. Sicherheitslücken
Stabilität	eher nicht	bisher starke Volatilität, z.T. Tendenz zur Blasenbildung, die kennzeichnend für spekulative Währungen ist

Quelle: Eigene Darstellung.

5. Fazit

Es haben digitale Währungssysteme das Potential zur Weiterentwicklung. Am Beispiel des Bitcoin-Konzepts wurden die Idee, die Technik und die Unterschiede zu klassischen Währungssystemen diskutiert. Wird sich nur eine kleine Zahl von Nutzern als Miner beteiligen, wird der ursprüngliche Charakter als System gleichberechtigter Nutzer allerdings ein Stück weit verlorengehen.[15]

[14] Vgl. Daube, C. H., & Dobernig, H. (2019).
[15] Vgl. Sorge, C., & Krohn-Grimberghe, A. (2013).

Das Bitcoin-Konzept wurde anhand von vier Kategorien wie Akzeptanz, Inflationsschutz, Sicherheit und Stabilität mit einer klassischen Währung bewertet. Bitcoin hat das Potential, zukünftig von Verbrauchern und Anbietern akzeptiert zu werden. Die Zukunftsfähigkeit des Konzepts hängt aber von der Stabilität des Bitcoin-Netzwerks und dem Vertrauen ab, das die Nutzer ihm schenken. Vom Grundgedanken her ist Bitcoin deflationär, aber die tatsächlichen Preisänderungsraten lassen sich aufgrund fehlender Güterangebote nicht ermitteln. In diesem Zusammenhang sind zukünftige Veränderung des Bitcoin-Protokolls und eine Konkurrenz zu anderen digitalen Währungen nicht ausgeschlossen. Die Verschlüsselungstechnologien gewähren ein entsprechendes Maß an Sicherheit.

Der Erfolg von Bitcoin ist davon abhängig, ob transparente Geschäftsmodelle vorhanden sind, die auf Online-Handelsplattformen ein sicheres Kaufen und Verkaufen mit dieser Währung ermöglichen. Schließlich zeigt Bitcoin eine hohe Volatilität und zum Teil sogar Blasenbildung. Diese Eigenschaften sind eher typisch für eine Spekulationswährung und eine stabile Wertaufbewahrungsfunktion ist gegenwärtig nicht gegeben.

6. Literatur

bitcoin.org (2019). Choose your Bitcoin wallet. Abgerufen am 12.02.2019 von https://bitcoin.org/en/choose-your-wallet

bitcoin.sipa.be (2019). Bitcoin network graphs. Total network hashing rate. Abgerufen am 12.02.2019 von http://bitcoin.sipa.be/

bitcoinfees.earn.com (2019). Predicting Bitcoin fees for transactions. Abgerufen am 12.02.2019 von https://bitcoinfees.earn.com/

Clement R., & Schreiber D. (2016). Peer-to-Peer Märkte. In: R. Clement & D. Schreiber (Hrsg.): Internet-Ökonomie: Grundlagen und Fallbeispiele der vernetzten Wirtschaft. 3. A., Springer Gabler, Berlin, Heidelberg, S. 313-339

Daube, C. H., & Dobernig, H. (2019). Digitale Währungssysteme: Kryptowährungen in der Unternehmensfinanzierung. In: ZBW econstor-publish

Eckert, D., & Zschäpitz, H. (2017). Blase oder Revolution? Die Wahrheit über die Bitcoin-Exzesse. Abgerufen am 12.02.2019 von https://www.welt.de/finanzen/article164826508/Blase-oder-Revolution-Die-Wahrheit-ueber-die-Bitcoin-Exzesse.html

Kannenberg, A. (2014). Bitcoin-Börse Mt. Gox sperrt alle Bitcoin-Abhebungen. heise online (Februar 2014). Abgerufen am 12.02.2019 von https://www.heise.de/newsticker/meldung/Bitcoin-Boerse-Mt-Gox-sperrt-alle-Bitcoin-Abhebungen-2108053.html

Kerscher D. (2014). Bitcoin: Funktionsweise, Risiken und Chancen der digitalen Währung. 2. A., Kemacon, Dingolfing

Münzer J. (2013). Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer. BaFin Journal (Januar 2014). Abgerufen am 12.02.2019 von https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Abgerufen am 12.02.2019 von https://bitcoin.org/bitcoin.pdf

Pfnür, C. (2014). Vergleich dezentraler elektronischer Währungen. Bachelor Thesis, Hochschule für Technik und Wirtschaft Dresden. Abgerufen am 12.02.2019 von https://www2.htw-dresden.de/~jvogt/abschlussarbeiten/Pfn%C3%BCr.pdf

Sorge, C., & Krohn-Grimberghe, A. (2013). Bitcoin – das Zahlungsmittel der Zukunft? Wirtschaftsdienst, 93(10), S. 720-722