DEVISENFOKUS

23. April 2018

Kryptowährungen – vieles in Bewegung

AUTOR
Ralf Umlauf
Telefon: 0 69/91 32-18 91
research@helaba.de

REDAKTION
Dr. Stefan Mitropoulos

HERAUSGEBER
Dr. Gertrud R. Traud
Chefvolkswirt/
Leitung Research

Helaba
Landesbank
Hessen-Thüringen
MAIN TOWER
Neue Mainzer Str. 52-58
60311 Frankfurt am Main
Telefon: 0 69/91 32-20 24
Telefax: 0 69/91 32-22 44

Das Thema „Bitcoin und Kryptowährungen“ ist weiterhin präsent, auch wenn das mediale Echo seit dem Ende des letzten Jahres etwas abgenommen hat. Unverändert besteht ein hohes Interesse an grundlegenden Informationen zu diesem Themengebiet, auch im Hinblick auf den technologischen Rahmen – die Blockchain. Daher ist die in unserer Publikation **Wochenausblick** erschienene **Serie „Bitcoin und Kryptowährungen“** hier nochmals zusammengestellt.

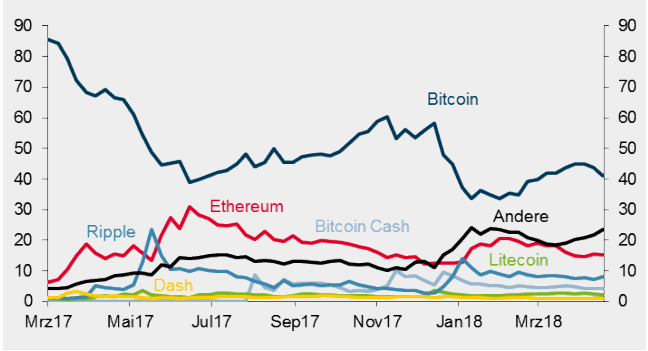
Das vorläufige Ende des Hypes

XBT (Wechselkurs in USD)

Quellen: Datastream Helaba Volkswirtschaft/Research

Sinkender Bitcoin-Anteil

% der Gesamtmarktkapitalisierung



Quellen: CoinMarketCap.com, Helaba Volkswirtschaft/Research

Auf dem Kryptomarkt ist weiterhin vieles in Bewegung. Das gilt für die Kurse, aber vor allem auch für Themen wie alternative Coins, von denen es laut coinmarketcap.com inzwischen fast 1.600 gibt. So wundert es nicht, dass Bitcoin, der Platzhirsch unter den Kryptowährungen, seinen Anteil an der Gesamtmarktkapitalisierung nicht mehr nachhaltig über 40 % steigern konnte (Anfang 2017 lag der Wert noch jenseits der 80 %-Marke). Auch andere, vormals ins Rampenlicht gerückte Coins haben angesichts der Flut neuer Assets Anteile einbüßen müssen. Die Gesamtmarktkapitalisierung liegt aktuell bei rund 340 Mrd. US-Dollar (rund 270 Mrd. Euro) und hatte ein Hoch Anfang Januar dieses Jahres bei über 800 Mrd. US-Dollar.

Die einzelnen Teile der Serie sind auf S. 2-6 nahezu unverändert wiedergegeben. Zusätzlich geben wir mit dem (aktuellen) Glossar auf S. 7-8 eine Hilfestellung, um sich in der Kryptowelt zurechtzufinden.

1 Einführung[1]

Mit der Finanzkrise 2007/08 und den folgenden unkonventionellen geldpolitischen Maßnahmen ist das Vertrauen vieler Wirtschaftssubjekte in das vorherrschende Geldsystem beschädigt worden. Bankenpleiten, staatliche Rettungspakete, Null- oder Negativzinspolitik sowie billionenschwere Anleihekäufe der Zentralbanken beförderten die Idee alternativer Geldsysteme. Warengeld, Vollgeld und Privatgeld wurden in diesem Kontext diskutiert.

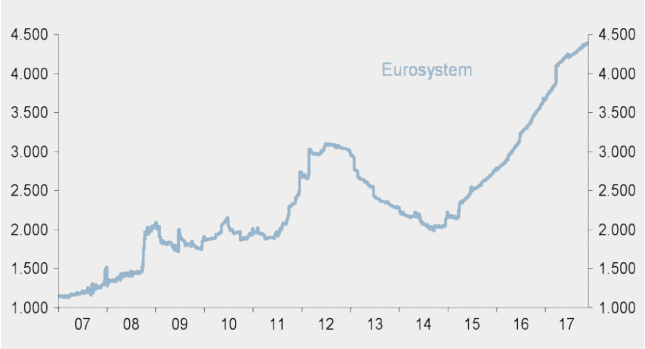
Satoshi Nakamoto ist vermutlich ein Pseudonym

Der technologische Fortschritt der letzten Jahrzehnte (globale Vernetzung, erhöhte Rechnerleistungen und Speicherkapazitäten), mithin die Möglichkeit zur breiten Anwendung von Verschlüsselungstechnologien ermöglichte die Entwicklung von Kryptowährungen. So wird versucht, die Kritik am Bankensektor in neue Lösungsansätze zu überführen. Mit der Referenzsoftware Bitcoin Core, die auf Basis eines „White Papers“ von Satoshi Nakamoto im Jahre 2008 entwickelt wurde, gelang Anfang 2009 eine Transaktion unter der Verwendung eines Bitcoins. Die erste Kryptowährung war geschaffen.

Konzipiert ist Bitcoin als private, dezentrale, digitale und verschlüsselte Alternative zu den bestehenden Währungen, die auf Vertrauen basieren. Die Gefahr, dass das Vertrauen gebrochen wird, erhöht die Transaktionskosten im etablierten Geldsystem. Daher sei es laut „White Paper“ nötig, eine Währung zu schaffen, die auf Mittelsmänner, d.h. Banken, verzichtet. Anstelle zentraler Drittparteien, die Zahlungsströme verifizieren und verbuchen, tritt ein „Netzwerk unter Gleichen“ (P2P, „peer-to-peer“, dezentral), in dem Transaktionen direkt zwischen Akteuren möglich werden.

Unkonventionelle Geldpolitik sorgt für Unbehagen

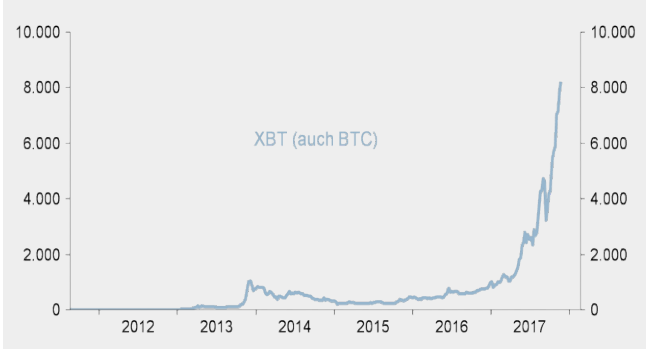
QE lässt Zentralbankbilanz wachsen — Bio. EUR



Quellen: Datastream Helaba Volkswirtschaft/Research

Bitcoin im Höhenrausch

Ungebremste Kursdynamik — XBT (Wechselkurs in USD)



Quellen: Datastream, Helaba Volkswirtschaft/Research

Neuer Sicherungsmechanismus – die Blockchain

Der Verzicht auf zentrale Gegenparteien (hier: Banken) führt zum Problem der Doppel- oder Mehrfachausgaben. Während im etablierten Geldsystem die Banken darüber wachen, dass ihre Kunden nicht mehr Geld überweisen/ausgeben als sie besitzen oder ihnen bei Bedarf Kredit geben, ist in einem P2P-Netzwerk keine Kontrollinstanz vorhanden. Die Konzeption des Bitcoin-Netzwerkes muss daher sicherstellen, dass es nicht zu Mehrfachausgaben kommt. Bitcoin-Transaktionen werden deshalb mit Zeitstempeln versehen, die in eine Kette von hash-basierten Arbeitsbeweisen („proof-of-work“) eingetragen werden: die Blockchain. Die Zeitstempel können nicht verändert werden, ohne den „proof-of-work“ neu auszuführen. Die längste Kette dient nicht nur als Nachweis der durchgeführten Transaktionen, sondern auch als Beweis, dass sie vom größten Teil der Rechenleistung stammt. Solange die Mehrheit der Rechenleistung von Teilnehmern kontrolliert wird, die nicht kooperieren, um Datensätze zu manipulieren, werden diese die längste Kette generieren und schneller sein als Betrüger, die Daten verändern wollen.

[1] erschienen am 24.11.2017

2 Technologie[2]

Im zweiten Teil unserer Serie beleuten wir die technologische Umsetzung von Bitcoin. Bereits in unserer Einführung kam die Blockchain-Technologie zur Sprache, denn diese stellt den Kern der Kryptowährungen dar und ist nötig, um eine hohe Fälschungssicherheit zu erreichen.

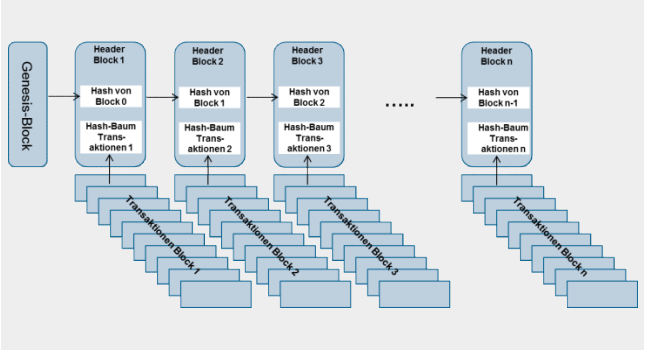
Dezentrale Datenbank als Kern der Kryptowährung

Unter Blockchain („block chain“, Blockkette oder Distributed Ledger) wird eine Datenbank verstanden, deren Integrität mittels vielfacher, dezentraler Speicherung verschlüsselter Daten gesichert wird. Der Verschlüsselungsalgorithmus erzeugt sogenannte Hashwerte unter der Einbeziehung der innerhalb des Netzwerkes angefallenen Transaktionsdaten und der vorherigen Hashwerte. Die Datensätze werden kryptographisch verkettet und auf allen Netzwerkknoten gespeichert.

Im Detail: Transaktionen innerhalb des Netzwerkes werden zu Blöcken zusammengefasst und über eine Hashfunktion verschlüsselt. Der sogenannte Hash-Baum der Transaktionen wird dann in der Kopfzeile (Header) eines Blocks gespeichert. Hinzu kommt der Hashwert des vorherigen Headers (dieser enthält wiederum Informationen über den vorherigen Block von Transaktionen und den vor-vorausgegangenen Header). Somit ergibt sich eine durchgängige Kette von Blöcken, in der alle als gültig anerkannten Transaktionen des Netzwerkes verbucht sind.

Von der Transaktion zum Block

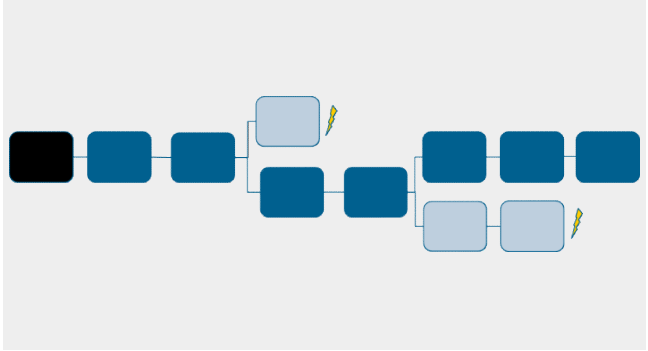
Blöcke werden verkettet



Quelle: Helaba Volkswirtschaft/Research

Die Blockchain wächst

Kette wächst an gültigen Blöcken am schnellsten weiter



Quelle: Helaba Volkswirtschaft/Research

Die längste Kette ist ***die*** Blockchain

Zur Erstellung eines neuen Blocks ist ein hoher Rechenaufwand nötig, denn neben den Verschlüsselungsberechnungen erfolgt ein „proof-of-work“ (Arbeitsbeweis), dessen Schwierigkeitsgrad variiert. Die Wahrscheinlichkeit, diesen Arbeitsbeweis als erster erfolgreich zu erstellen, steigt mit der eingesetzten Rechnerleistung. Erzeugt ein Teilnehmer einen Block, so sendet er diesen an alle Netzwerkteilnehmer, die einen gültigen Block akzeptieren und in die Blockchain einfügen. Hält die Mehrheit der Teilnehmer diesen für gültig, wird die Kette an derjenigen Stelle am schnellsten weiterwachsen, weil an dieser Stelle die Mehrheit der Rechenleistung ansetzt. Dadurch, dass dem neuen Block nun andere angehängt werden, wird der Block unwiderruflich in der Blockchain gespeichert. Die längste Blockchain ausgehend von der Wurzel (dem sogenannten Genesis-Block) wird immer als gültig angesehen.

Mining als Belohnung für eingebrachte Rechen-leistung

Der Teilnehmer, der einen neuen Block erstellt, fügt der gemeinsamen Buchhaltung nicht nur die im Block enthaltenen Transaktionen hinzu, sondern darf sich auch eine Transaktion in Form neugeschaffener Coins auf seinem „Konto“ eintragen (Mining). Daher sind die Marktteilnehmer bestrebt, neue Blöcke zu erstellen, und sichern so die erforderliche Rechenleistung des Netzwerks. Die Spezifikation der Bitcoin-Software sieht vor, dass etwa alle 10 Minuten ein Block mit der Größe von rund 1 MB geschaffen wird. Der Schwierigkeitsgrad des „proof-of-work“ wird dementsprechend angepasst. Es ist zudem festgelegt, dass sich der Mining-Ertrag (aktuell 12,5 Bitcoin je Block) alle 210.000 Blöcke halbiert. Somit verlangsamt sich der Zuwachs der Währungseinheiten und konvergiert langfristig bei ca. 21 Mio. Stück, von denen bereits 16,6 Mio. „geschürft“ wurden.

[2] erschienen am 01.12.2017

3 Energieverbrauch, Gebühren, Forks, „Altcoins“[3]

Die grundlegende Funktionsweise der Blockchain nebst der Schaffung von neuen Coins (Mining) haben wir im vorherigen Teil beschrieben. An dieser Stelle setzen wir uns mit weiteren technischen Fragen auseinander.

Energieverbrauch steigt, trotz geringer Zahl an Verbuchungen

Die Software von Bitcoin sieht nicht nur eine auf 21 Mio. begrenzte Zahl von Währungseinheiten vor, sondern auch, dass etwa alle 10 Minuten ein neuer Block mit einer Größe von rund 1 MB geschaffen wird. Das bedeutet, dass etwa 7 Transaktionen pro Sekunde oder 600.000 pro Tag verbucht werden könnten. Tatsächlich schwankte die Anzahl zuletzt stark um 300.000. Selbst der Bedarf einer mittleren deutschen Großstadt wäre nicht gedeckt. Der dafür nötige Energieverbrauch lässt sich nur schätzen. Die Webseite digiconomist.net gab ihn Ende Dezember mit rund 37 TWh an, was die Jahresleistung von drei Kernkraftwerken überstiege.

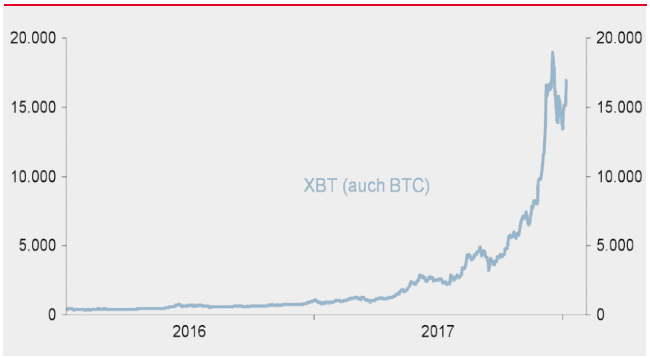
Für das Erstellen eines Blocks erhält der Marktteilnehmer nicht nur den Mining-Ertrag in Form neuerzeugter Bitcoins, sondern auch Gebühren je verarbeiteter Transaktion. Der Betrag wird vom Bitcoinsender festgelegt, wobei gewisse Mindestgrößen eingehalten werden müssen. Aktuell liegt die erhaltene Gebühr je Block bei rund 1/4 des Mining-Ertrags. Ob die Gebühren auch nach dem Ende des Minings (faktisch wohl in den 2040er Jahren) genügend Anreize zur Aufrechterhaltung des Netzwerkes geben, bleibt abzuwarten.

Aufspaltungen verdoppeln die Anzahl von Coins im Geldbeutel

Die Zukunft des Netzwerkes und des Kurswertes wird zudem von einem intensiven Wettbewerb bestimmt. Zum einen ist die Tatsache hervorzuheben, dass es immer wieder zu technologischen Anpassungen kommen kann. Werden die neuen, veränderten Computerprotokolle nicht von einer Mehrheit der Teilnehmer akzeptiert, werden diese wieder verworfen oder aber es kommt zu einer Aufspaltung der Community (Fork). So geschehen bei Neuerungen, die sich dann unter den Namen Bitcoin Cash und Bitcoin Gold zu eigenen Netzwerken, mithin zu zwei neuen Kryptowährungen weiterentwickelten. Die Tatsache, dass Bitcoin-Besitzer im Moment der Abspaltung eine entsprechende Anzahl von Bitcoin Cash (und später auch Bitcoin Gold) in den elektronischen Geldbeuteln (Wallets) vorfanden, weist auf Risiken hin. Eine Coin-Vermehrung auf Knopfdruck ist mit dem ursprünglichen Gedanken einer nicht erweiterbaren Menge von Währungseinheiten nur schwierig in Einklang zu bringen.

Bitcoin: Höhenrausch vorerst beendet

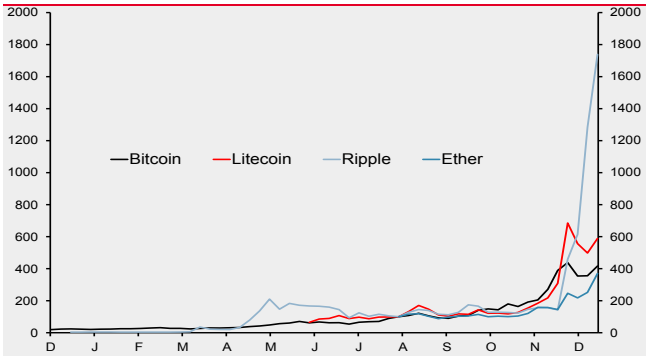
XBT, Wechselkurs in US-Dollar



Quellen: Datastream, Helaba Volkswirtschaft/Research

„Altcoins“ teilweise stärker gesucht

Rebasiert, 18. August 2017=100



Quellen: Bloomberg, Helaba Volkswirtschaft/Research

Inflationäre Schaffung von „Altcoins“

Zum anderen sind die durch Forks neu entstandenen Kryptowährungen bei weitem nicht die einzigen Alternativen zum Bitcoin. Unter dem Begriff „Altcoins“ werden diese zusammengefasst, von denen es inzwischen mehr als 1.300 Stück gibt, Tendenz steigend. Bitcoin stellt zwar alle anderen Kryptowährungen in Sachen Medieninteresse, Verbreitung und Marktkapitalisierung in den Schatten, dennoch besteht die Gefahr, dass eine von diesen Neuerscheinungen Bitcoin verdrängen könnte. Entsprechend waren jüngst die Kursgewinne deutlich größer als die von Bitcoin.

[3] erschienen am 12.01.2018

4 Sind Bitcoins Geld?[4]

Im vierten Teil der Serie soll die Frage beantwortet werden, ob Bitcoins Geld darstellen. Dies geschieht anhand der Geldfunktionen: Tauschmittel, Recheneinheit und Wertaufbewahrung.

Geld existiert, weil es effizient ist

Unter Geld verstehen Ökonomen Aktiva, die von Gläubigern zur Tilgung von Verbindlichkeiten angenommen werden. Dies kann aufgrund gesetzlicher Verpflichtung oder der Marktkonventionen geschehen. Geld ist also das allgemein akzeptierte Tausch- oder Zahlungsmittel. Ohne Geld würde die Natural-Tauschwirtschaft vorherrschen und mit ihr hohe Informations- und Transaktionskosten. Geld reduziert diese Kosten erheblich und fördert somit eine arbeitsteilige Wirtschaft. Ohne Geld bestünde der Zwang, simultan den Austausch zweier Güter (Waren oder Dienstleistungen) in Einklang zu bringen, während mit der Einführung des Zwischentauschgutes Geld zunächst ein Verkauf und anschließend ein Kauf abgewickelt werden können – in der Regel zeitlich und räumlich voneinander getrennt. Geld existiert, weil es effizient ist!

Die Akzeptanz eines Gutes als Universaltauschmittel beruht im Wesentlichen auf der Wertaufbewahrungsfunktion, denn ohne diese wäre die zeitliche Trennung von Verkauf und Kauf nur bedingt sinnvoll. Aus praktischen Erwägungen heraus ist zudem die Verwendung als Recheneinheit zu erwarten, denn der Vergleich der Wertigkeit von Gütern – ausgedrückt in ihrem Preis – ergibt in Bezug auf das Zwischentausch- und Wertaufbewahrungsmittel den meisten Sinn. Eine Umrechnung auf eine andere, zusätzliche Recheneinheit ist obsolet.

Bitcoin: Ernüchterung nach der Euphorie

Wechselkurs in USD

Quellen: Bloomberg, Helaba Volkswirtschaft/Research

Unterschiede zwischen Geld und Bitcoin

Gegenüberstellung

Geld	Bitcoin
Forderungen gegenüber (Noten-) Banken	Keine Forderungen; keine Zentralinstanz vorhanden
Erzeugung durch Kreditvergabe (reguliert)	Erzeugung durch Rechenoperationen (Fiat lux!)
Menge abhängig von Kreditnachfrage/-angebot in Bezug zur Realwirtschaft	Menge begrenzt, kein Bezug zur Realwirtschaft
Außenwert richtet sich nach Angebot und Nachfrage; innerer Wert als Orientierung	Kurswert richtet sich nach Angebot und Nachfrage, kein realer Wert (virtueller Charakter)

Quelle: Helaba Volkswirtschaft/Research

Kryptowährungen erfüllen Geldfunktionen nicht

Bitcoins stellen hierzulande und in der Eurozone kein gesetzliches Zahlungsmittel dar. Eine breite gesellschaftliche Nutzung ist nicht zu konstatieren, denn die Zahl der Akzeptanzstellen ist nach wie vor äußerst gering, wenngleich die Verbreitung von Bitcoin auf niedrigem Niveau zugelegt hat. Zudem fehlt die Auszeichnung von Preisen in Bitcoin, sodass dieser auch nicht als Recheneinheit genutzt wird. Die Wertaufbewahrung gestaltet sich ebenfalls schwierig, denn eine zukünftige, allgemeine Akzeptanz des Cybergeldes als Tauschmittel ist ungewiss. Darüber hinaus zeugen die Kursschwankungen von einem sehr hohen Risiko und die inflationäre Schaffung von neuen Kryptowährungen (aktuell existieren über 1.300) sorgt für zusätzliche Unsicherheit.

In Japan dagegen ist die Zahl der Akzeptanzstellen größer und seit dem 1. April 2017 ist Bitcoin dort als „offizielles“ Zahlungsmittel zugelassen. Die Zahl der weltweit im Bitcoin-Netzwerk pro Tag verbuchten Transaktionen schwankt stark um 300.000, sodass auch in Japan nicht von einem allgemeinen Einsatz als Zahlungsmittel auszugehen ist. Die Leistungsfähigkeit des Bitcoin-Netzwerkes ist einer der wesentlichen Kritikpunkte, denn ein massenhafter Einsatz erscheint unter den gegebenen technischen Spezifikationen bis auf weiteres unrealistisch. Im dritten Teil unserer Serie hatten wir zudem im Zusammenhang mit der Leistungsfähigkeit auf den hohen Energieverbrauch hingewiesen. Bitcoins erfüllen die Geldfunktionen per saldo nicht und sind somit nicht als Geld anzusehen. Auch in absehbarer Zukunft ist nicht davon auszugehen.

[4] erschienen am 26.01.2018

5 Keine Zukunft?[5]

In den vorangegangenen Beiträgen wurden technische Aspekte des Phänomens Bitcoin ebenso beleuchtet wie die Frage, ob die Cyberwährung Geld darstellt. Kritikpunkte und Risiken werden im letzten Teil unserer Serie nochmals dargelegt.

Stärkere Regulierung eine Gefahr

Von der Bitcoin-Community wird oftmals die Unabhängigkeit von Banken und staatlichen Institutionen als besonderer Vorteil hervorgehoben. Wie so oft erweist sich dies aber als zweischneidiges Schwert. Während das Vertrauen der Kryptoanhänger in das etablierte Geldsystem spätestens seit der Finanzkrise 2007/08 geschwächt ist, ist ein System gänzlich ohne Vertrauen nicht möglich. Anstatt auf Banken und staatlichen Institutionen zu bauen, müssen Bitcoin-Nutzer nun auf Internetdienstleister setzen, die keiner speziellen Regulierung unterliegen. Die Gefahr von Hacker-Angriffen besteht und in der Vergangenheit haben solche schon erhebliche Verluste verursacht. Des Weiteren stellt die Tatsache der fehlenden Regulierung ein Risiko dar, denn ein späteres Eingreifen von Regierungen und Notenbanken würde die Rahmenbedingungen mitunter deutlich verändern. In China gibt es neben dem Handelsverbot Bestrebungen, das Mining zu reduzieren, und in Südkorea wurde Banken der Handel mit Kryptowährungen untersagt, weitere Verbote und Regulierungen sind in der Diskussion. Dahinter steht unter anderem die Befürchtung, dass Kryptogeld zur Umgehung von Kapitalverkehrskontrollen und zur Geldwäsche oder zu anderen illegalen Zwecken genutzt wird.

Damit zusammenhängend ist klarzustellen, dass Bitcoin im Gegensatz zum Euro weder allgemeines Zahlungsmittel ist noch damit eine Forderung gegen eine Institution begründet wird. Das auf Euro denominierte Buch- und Bargeld stellt jeweils Rechtstitel dar. Ein Bitcoin, besser der private Schlüssel in einem Wallet, legitimiert lediglich zum Transfer an eine andere Adresse. Bitcoins existieren nur so lange es das Bitcoin-Netzwerk gibt. Sollte der Anreiz zum Verbuchen der Transaktionen (Mining, „Schürfen“) wegen der festgelegten Maximalzahl an Bitcoins irgendwann abnehmen oder ganz verschwinden, würde das Netzwerk als Ganzes gefährdet. Wer garantiert eine ausreichende Zahl von Minern, die das dezentrale Kontobuch pflegen?

Pro und Contra

Übersicht

Globaler Ansatz	Realer Wert nicht zu bestimmen
(Relativ) fälschungssicher	Hoher Energieverbrauch
Keine „Inflationierung“	Gefahr von Spaltungen („fork“)
Anonymität	Inflation von neuen Kryptowährungen
Frei von institutioneller/ staatlicher Einflussnahme	Deflationsrisiko
	Geldfunktionen nicht erfüllt
„Demokratisch“ (Konsensverfahren)	Spekulationsmotiv im Vordergrund
	Anonymität / Kriminalität
	Fehlende Regulierung
	Gefahr von Hacker-Attacken

Quelle: Helaba Volkswirtschaft/Research

Bitcoin nach Erholung wieder unter Druck

Wechselkurs in USD

Quellen: Datastream, Helaba Volkswirtschaft/Research

Weitere Entwicklungen der Kryptowährung beobachten

Ein weiterer wesentlicher Nachteil insbesondere von Bitcoin und seinen Klonen (Bitcoin Cash, Bitcoin Gold, Litecoin, u.v.m.) ist der hohe Energieverbrauch. Laut digiconomist.net liegt der Energieverbrauch allein des Bitcoin-Netzwerkes inzwischen jenseits der 50-TWh-Marke. Der Anstieg der Rechenoperationen (Hashrate) ist im Verhältnis zur geringen Anzahl der Transaktionen unseres Erachtens das Hauptproblem der Kryptowährungen. Ein Fortschreiben dieser exponentiellen Entwicklung über einen längeren Zeitraum ist nicht möglich. Andere Kryptowährungen, von denen immerhin über 1.500 Stück auf coinmarketcap.com gelistet werden, könnten diese Probleme lösen. Daher müssen die weiteren Entwicklungen rund um das Thema Blockchain und Kryptowährungen in den kommenden Jahren intensiv beobachtet werden.

[5] erschienen am 09.03.2018

Glossar

Bitcoin	Älteste und bekannteste Kryptowährung; basierend auf Blockchain-Technologie; Mining mit Hilfe SHA-256 (Verschlüsselungsalgorithmus); Anteil an der gesamten Marktkapitalisierung (laut CoinMarketCap.com) bei 42 %; bis März 2017 bei 75-100 %; gebräuchliche Kürzel BTC und XBT.
Bitcoin Cash	Erste erfolgreiche Abspaltung vom Bitcoin(-Core)-Netzwerk, um eine Erhöhung eines Blockgrößen-Limits durchzuführen; vorherige Abspaltungsversuche (Bitcoin XT, Bitcoin Unlimited, Bitcoin Classic) waren nicht erfolgreich; Marktanteil: 4 %; Kürzel: BCC oder BCH.
Bitcoin Core	Umbenennung von Bitcoin nach Abspaltungsversuchen (wie Bitcoin Classic, Bitcoin Unlimeted, Bitcoin XT oder Bitcoin Cash).
Bitcoin Gold	Weitere Abspaltung von Bitcoin (Core), um das Mining mit herkömmlichen GPUs (Grafikkarten) wieder zu ermöglichen; Umstellung auf Equihash als Verschlüsselungsalgorithmus; Kürzel BTG.
Blockchain	Auch Blockkette oder „block chain“; dezentral verwaltetes Kontobuch (Distributed Ledger Technology oder DLT); Aneinanderreihung und kryptografische Verkettung von Datensätzen sorgt für stetig wachsende „Blockkette“; relativ fälschungssicher; Kern vieler Kryptowährungen; Technologie, die zukünftig eine weite Verbreitung finden dürfte – unabhängig von Kryptowährungen.
Cybergeld	Auch Kryptogeld, Digitalgeld, Netzgeld, u.ä.; andere Bezeichnung für Kryptowährung.
Dash	Unter 1 % Anteil am Gesamtmarktvolumen; Mining über X11 (Verschlüsselungsalgorithmus); Kürzel: DASH.
Distributed Ledger	„Verteiltes Kontobuch“; siehe Blockchain.
Ethereum	Datenbanksystem zum Ausführen von Smart Contracts mit Ether als Verrechnungseinheit; Ether ist die zweitwichtigste Kryptowährung; Anteil am Gesamtmarktvolumen von rund 15 %; Spitzenwert Mitte Juni 2017 bei über 30 %; Kürzel: ETH.
Ethereum Classic	Abspaltung (Hard Fork) von Ethereum, nachdem die Mehrheit eine Transaktion rückgängig machte, bei der Ether im Gegenwert von 65 Mio. USD unbrauchbar wurden; Teilnehmer von Ethereum Classic weigerten sich, daran teilzunehmen; Kürzel: ETC.
Hashfunktion	Hier: kryptologische Hashfunktion zur Verschlüsselung von Datensätzen; Erstellung der Hash-Werte; Beispiele: SHA-256; Scrypt, Ethash, X11, CryptoNight oder Equihash.
Hard Fork	Abspaltung von einer bestehenden Blockchain; führt zur Etablierung eines neuen Astes der Kette, die von anderen Mitgliedern des Netzwerks nicht akzeptiert wird; führt zu unterschiedlichen Blockchains; Bsp.: Bitcoin Cash als Abspaltung von Bitcoin (Core).
Instant payment	Sofort-Überweisung.
Initial Coin Offering	ICO; Token Sale; Form des Crowdfundings in Anlehnung an IPO; „Anteile“ am zu finanzierenden Objekt werden verkauft; ICOs sind in China inzwischen verboten und auch andere Regulierungsbehörden diskutieren Beschränkungen.

IOTA	Basiert nicht auf der Blockchain-Technologie, sondern auf dem Tangle-Prinzip; soll Transaktionen im „Internet der Dinge“ ermöglichen; Kein Mining; Marktanteil 1,2 %; Kürzel: MIOTA.
Litecoin	Ähnlich aufgebaut wie Bitcoin; 2,3 % Anteil am Gesamtmarktvolumen; Mining über Scrypt; Kürzel: LTC.
Mining	„Schürfen“; Prozess der Blockerstellung in der Blockchain; wird durch Buchung von Währungseinheiten aus dem Nichts auf das eigene Konto belohnt; derjenige Client, der als erstes einen gültigen Block erzeugt, erhält den Mining-Ertrag; bei Bitcoin sind dies aktuell 12,5 XBT/Block.
Monero	Neue Entwicklung des zugrunde liegenden Codes; 1,0 % Anteil am Gesamtmarktvolumen; Mining über CryptoNight; Kürzel: XMR.
NEM	0,8 % Anteil am Gesamtmarktvolumen; kein Mining, Kürzel: XEM.
NEO	System zum Abwickeln von Smart Contracts; chinesische Version von Ethereum; Marktanteil 1,0 %; Kürzel: NEO.
Nonce	Veränderlicher Wert innerhalb eines Blocks, der dazu dient, den Hashwert des gesamten Blocks unter einen festgelegten Schwellenwert zu reduzieren; je niedriger der Schwellenwert ist, desto unwahrscheinlicher wird der Fund eines passenden Nonces; Rechenleistung muss erhöht werden, um schnellstmöglich gültigen Nonce (und damit gültigen Block) zu finden.
Nxt	„Next Generation of Cryptocurrency“; im Unterschied zu Bitcoin u.a. basierend auf dem Proof-of-stake-Ansatz; kein Mining; Kürzel: NXT.
POS	Point of Sale; Verkaufsort; auch Kassenplatz.
P2P	Peer-to-peer-Netz; Netzwerk oder Kommunikation unter „Gleichen“.
Proof-of-stake	„Berechtigungsnachweis“; Prinzip, nach dem Blöcke in der Blockchain geschrieben werden können; nicht Rechenleistung wie beim PoW ist entscheidend, sondern die Anzahl der nachgewiesenen Coins.
Proof-of-work	„Arbeitsnachweis“; PoW; Methode in der Informatik, um den übermäßigen Gebrauch von Diensten zu verhindern; Lösung einer Aufgabe durch den Computer, um Zugang zu einem Dienst zu erhalten; PoW liegt dem Mining z.B. bei Bitcoins zugrunde.
Ripple	Marktkapitalisierung 7-8 %; kein Mining; Kürzel: XRP; deutliche Unterschiede zu anderen Kryptowährungen.
Satoshi Nakamoto	Pseudonym unter dem das „White Paper“ für Bitcoin 2008 erschienen ist; vermutlich Gruppe von Programmierern/ Entwicklern.
Satoshi	Untereinheit von Bitcoin, Bitcoin Cash; Verhältnis: 1/100.000.000.
Smart Contracts	Computerprotokolle, die Verträge abbilden oder überprüfen oder Verhandlungen und Abwicklung von Verträgen unterstützen.
Wallet	Elektronischer Verwahrort für „private und öffentliche Schlüssel“, die zum Tausch von Kryptowährungen wie Bitcoin berechtigen. ■