

Bitcoin – was steckt hinter dem Hype?

Viele Anleger sind von Kryptowährungen gleichermaßen fasziniert und verwirrt. Wir geben deshalb im ersten Teil der vorliegenden Studie eine verständliche Einführung in das komplexe Thema Bitcoin und Co. Dabei fokussieren wir uns auf die für Anleger relevanten Fragen. Investoren, welche sich eingehender mit dem Thema beschäftigen wollen, bieten wir im zweiten Teil einen vertieften Blick in die Welt der Kryptowährungen.

Durch enorme Kursgewinne erfahren Kryptowährungen, allen voran Bitcoin, derzeit einen regelrechten Hype. Doch was ist Bitcoin überhaupt, und wie funktioniert die viel zitierte Blockchain? Sind Kryptowährungen und Bitcoins für Anleger überhaupt relevant? Und welche Risiken geht man dabei ein?

Ein kurzer Rückblick

Die Geschichte von Bitcoin ist mysteriös. Am 31. Oktober 2008, kurz nach dem Zusammenbruch der Investmentbank Lehman Brothers, erscheint auf einer Mailingliste für Kryptografen das Grundsatzpapier «Bitcoin: A Peer-to-Peer Electronic Cash System». Das neun Seiten lange Dokument beschreibt die technischen und ökonomischen Grundlagen des heutigen Bitcoin und gilt als Geburtsstunde der Kryptowährungen. Der Autor hinter dem bis heute nicht identifizierten Pseudonym Satoshi Nakamoto bemängelt das auf Vertrauen und Finanzintermediären basierende Papiergeld. Er propagiert eine elektronische Währung, die auf einem kryptografischen Beweis beruht und keine Mittelsmänner (wie beispielsweise Banken oder Verwahrstellen) benötigt.

Die Idee wird von zahlreichen enthusiastischen Programmierern aufgenommen und es entsteht eine kleine Bitcoin-Community. Anfang 2009 wird der erste Bitcoin getauscht, und im Februar 2010 geht die erste Bitcoin-Börse online. Im Mai 2011 kletterte der Bitcoin-Kurs, angefeuert durch die ersten medialen Berichte, auf rund USD 6. Im Jahr 2013 werden in den USA erste Bitcoin-Bankomaten aufgestellt, und immer mehr Unternehmen beginnen, Bitcoins als Zahlungsmittel zu akzeptieren. Heute, rund vier Jahre später, werden Bitcoins auf Dutzenden Onlinebörsen gehandelt – zu einem stolzen Kurs von rund USD 5'500. Mit der Bekanntheit ist auch die Akzeptanz als Zahlungsmittel sukzessive gestiegen. Mit Bitcoins können, abgesehen von zahlreichen kleineren Onlinehändlern, auch Taxis in New York, Reisen (Expedia) oder gar Edelmetalle (JM Bullion) bezahlt werden. Japan hat Bitcoins im März 2017 gar als legales Zahlungsmittel klassifiziert und selbst die Einwohnerkontrolle der kleinen Schweizer Provinzstadt Zug akzeptiert Bitcoins als Zahlungsmittel für kleinere Gebühren. Die Beispiele verdeutlichen, dass – entgegen der oftmals verbreiteten Meinung – Bitcoins ihren Platz als Zahlungsmittel nicht nur in der Schattenwirtschaft, sondern in ganz legalen Bereichen einnehmen konnten.

Wie funktionieren Bitcoins? Oder: Der Reiz der Bitcoins

Die Funktionsweise von Kryptowährungen ist eine völlig andere als die herkömmlicher Währungen. Statt durch Banken erfolgt die Schöpfung von Kryptowährungen durch ein ausgeklügeltes technisches Verfahren. Dabei liegen die Vorteile für Anleger auf der Hand: Die Ausweitung des «Geldes» ist nicht beliebig möglich, sondern für den sogenannten Miner mit Aufwand verbunden. Ausserdem ist beispielsweise bei Bitcoins die maximale «Geldmenge» limitiert. Nachdem die Notenbanken in den letzten Jahren ihre Geldmenge im Rahmen der Krisenbekämpfung fast beliebig ausgeweitet haben, üben Kryptowährungen einen besonderen Reiz auf Anleger aus, die eine hohe Geldentwertung befürchten.

Der zweite Vorteil besteht in der Verwahrung. Hier kommt die sogenannte Blockchain-Technologie zum Einsatz. Die Eigentumsrechte werden nicht einer an einer zentralen Stelle verwahrt, sondern anonymisiert und dezentral an verschiedenen Orten im Internet abgespeichert.

Wie kann ich in Bitcoin investieren?

Es gibt mittlerweile verschiedenste Möglichkeiten, in Bitcoins zu investieren. Wir unterscheiden zwischen einer direkten Investition (dem direktem Erwerb von Bitcoins) und einer indirekten Investition über Finanzprodukte.

Direkte Investitionen

Wer seine Bitcoins selbst halten oder Zahlungen und Überweisungen mit der Kryptowährung tätigen möchte, der sollte sich für eine direkte Investitionsform entscheiden. Wer Bitcoins selbst halten möchte, kann diese an einer Onlinebörse erwerben, selbst minen oder an einem Bitcoin-Automaten (beispielsweise an einem Billettautomaten der SBB) erwerben. In einem zweiten Schritt können die Bitcoins nun in ein sogenanntes Wallet übertragen werden. Obschon viele Onlinebörsen mittlerweile eine eingeschränkte Wallet-Funktionalität anbieten, kann sich ein dezidiertes Wallet lohnen. Bei den Wallets unterscheidet man zwischen Hot Wallets und Cold Wallets. Während Erstere direkt mit dem Internet verbunden sind, bleiben Letztere offline. Hot Wallets umfassen Web-Wallets, Mobile Wallets, Desktop-Wallets oder ganze Bitcoin-Clients wie beispielsweise Bitcoin-Core. Cold Wallets bieten deutlich mehr Sicherheit: Sie umfassen Hardware-Wallets, wie beispielsweise Trezor, aber auch Paper-Wallets, bei denen der private und der öffentliche Schlüssel auf Papier ausgedruckt werden. Grundsätzlich sollten längerfristige Anlagen eher in einem Cold Wallet verwahrt werden, während sich Hot Wallets für Bitcoins anbieten, die rasch verfügbar sein müssen.

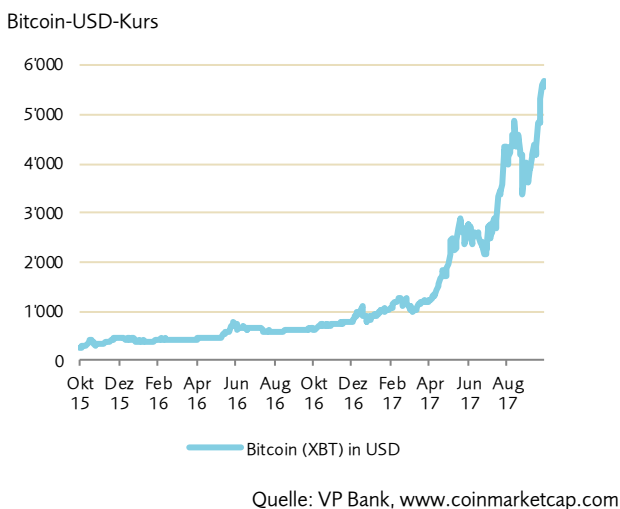
Indirekte Investitionen (Finanzprodukte)

Finanzprodukte auf Bitcoin sind kaum im Sinne des Erfinders.

Oder wie es Christian Mäder von Bitcoin News ausdrückt: «Ein Bitcoin-Zertifikat oder einen ETF statt eines Bitcoins zu kaufen, ist, als ob man eine E-Mail ausdrucken und sie per Fax versenden würde». Obschon diesen Einwänden eigentlich kaum etwas entgegenzusetzen ist, können Finanzprodukte auf Bitcoin für gewisse Anleger durchaus sinnvoll sein. Finanzprodukte bieten rasch und einfach Zugang zu Bitcoins, ohne dass sich die Anlegerin oder der Anleger mit der technischen Handhabung oder der Art des Verfahrens befassen muss.

Als bekanntestes Investmentvehikel mit einer Marktkapitalisierung von über USD 1 Mrd. gilt der Bitcoin Investment Trust. Aufgrund seiner Truststruktur ist es vielen Anlegern jedoch nicht möglich, in ihn zu investieren. Passive ETF auf Bitcoin wie beispielsweise der Winklevoss-ETF in den USA oder das Schweizer Pendant für professionelle Anleger der Zuger Firma Crypto Fund AG sind seit längerem angekündigt. Aufgrund von Vorbehalten des Regulators konnte bisher jedoch keiner der beiden Fonds lanciert werden.

Dank seines Emissions- und Handelsvolumens ist das Bitcoin-Tracker-Produkt der Bank Vontobel (vgl. Absatz «Die Tücken von Finanzinvestitionen» im zweiten Teil der Studie) eine Erfolgsgeschichte. Gerade bei strukturierten Produkten besteht jedoch weiterhin ein Gegenparteirisiko, was dem Grundgedanken der Blockchain diametral entgegenläuft.



Indirekte Investition über Aktien

Letztlich gibt es noch die Möglichkeit, über Aktien, welche vom Bitcoin-Boom profitieren, zu investieren. Insbesondere Grafikkartenhersteller wie Nvidia oder auch Advanced Micro Devices (AMD) mit seinen Radeon-Chips gehören zu den Profiteuren, da sie die notwendige Hardware zum Minen von Bitcoins liefern. Allerdings distanziert man sich mit einer Aktieninvestition noch weiter vom tatsächlichen Zweck und Grundgedanken der digitalen Währung.

In Bitcoins lauern durchaus Risiken

Die Vorteile der Kryptowährungen liegen auf der Hand: Durch die dezentrale Speicherung und die vergleichsweise sichere

Blockchain ist eine nachträgliche Manipulation der Daten aktuell faktisch ausgeschlossen. Die direkte Transaktionsabwicklung ohne externe Intermediäre ermöglicht zudem eine kosteneffiziente Verwendung. Trotz dieser offenkundigen Vorteile bergen Bitcoin-Transaktionen und das Netzwerk auch zahlreiche Risiken.

Diebstahl oder Verlust

Bitcoins können gestohlen oder vernichtet werden. Sowohl Onlinebörsen wie auch Wallets, die mit dem Internet verbunden sind, können Ziel eines Hackerangriffs werden.

Regulatorische Unsicherheit

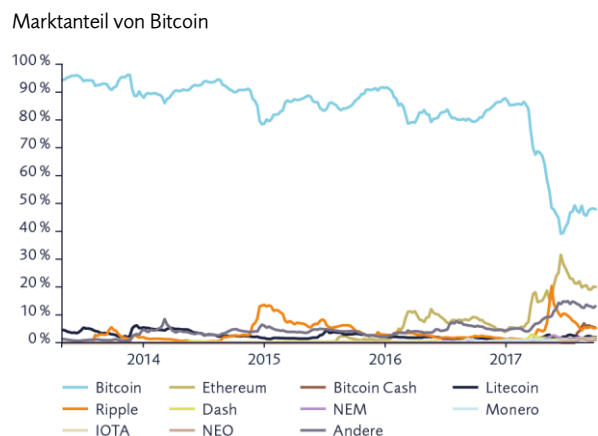
Der rechtliche Status von Kryptowährungen ist bisher noch nicht geklärt, was enorme Unsicherheiten birgt. Zuletzt äusseren sich viele Regulatoren kritisch, da Bitcoins für Verschleierung von Geldströmen (Geldwäsche) aber auch zur Umgehung von Kapitalverkehrskontrollen (China) missbraucht werden können. Kryptowährungen könnten auch den Notenbanken ein Dorn im Auge sein – schliesslich benötigen diese ein geldpolitisches Monopol, um eine effektive Geldpolitik betreiben zu können.

Liquidität – Volatilität

Verglichen mit anderen Börsen ist die Liquidität der Kryptowährungen äusserst gering. Dadurch sind die Kurse im Fall eines externen Schocks (Verbot, neue Technik) besonders korrekturanfällig. Ausserdem fehlen Handelsregeln.

Wachsende Konkurrenz und technischer Wandel

Zwar ist die Bitcoin-Menge limitiert, doch neue Währungen absorbieren Investorengelder. Neue, technologisch überlegene und flexiblere Währungen wie Ether (Ethereum) erobern in beinahe erschreckender Geschwindigkeit Marktanteile zu Lasten von Bitcoin.



Heute zu identifizieren, welche Währung sich langfristig durchsetzen wird, ist angesichts der enormen Vielfalt unmöglich.

Zudem stellt der Quantencomputer, an dem grosse Hersteller forschen, die kryptografische Sicherheit von Bitcoin langfristig in Frage.

Weitere Problemfelder entstehen aufgrund der limitierten Transaktionsabwicklungskapazität, der Endlichkeit der Bitcoins und der hohen Umweltbelastung durch den enormen Stromverbrauch des gesamten Netzwerkes.

Eine weitere und detailliertere Beschreibung der Risiken einer Investition in Kryptowährungen findet sich auf Seite 4ff.

Notenbanken und Kryptowährungen

Anonyme Geldtransfers, welche keinen zentralen Intermediär mehr benötigen sind ein Markenzeichen moderner kryptografischer Währungen wie Bitcoin & Co. Die Verbreitung dieser neuartigen und alternativen Zahlungsmittel bedroht das bestehende Geldmonopol der Notenbanken. Klassische monetäre Instrumente wie die Geldmengensteuerung verlieren dadurch an Bedeutung. Zahlreiche Notenbanken evaluieren derzeit Projekte, mit welchen die Vorteile von Kryptowährungen wie beispielsweise die erhöhte Anonymität, Peer-to-Peer Transaktionen ohne Intermediär oder auch dezentrale Blockchain-Technologie, kombiniert werden können, ohne dabei die geldpolitische Hoheit zu verlieren.

Konzepte zu sogenannten Central Bank Cryptocurrencies (CBCC) laufen unter den Namen Fedcoin, Cadcoin oder die schwedische eKrona. Obschon es sich noch mehrheitlich um Gedankenspiele der Notenbanker handelt, könnten die «offiziellen» digitalen Währungen das Bargeld zunehmend verdrängen. Der Vorteil: Durch die Blockchain lässt sich der Transaktionsverlauf jeder Währungseinheit lückenlos nachvollziehen, die Währung wäre elektronisch handelbar und Zinsentscheide wirken sich anders als bei Bargeld auch auf die elektronische Währung aus.

Der nächste Börsenhype: ICO und Token-Sales

Zahlreiche Finanzinstitute und Fondsanbieter versuchen, die Gunst der Stunde zu nutzen und mit neuen Exchange-traded Funds (ETF), strukturierten Produkten oder Konten in Bitcoins auf den bereits fahrenden Zug aufzuspringen.

Die Euphorie rund um Bitcoin hat auch zahlreiche Trittbrettfahrer in der Kryptoszene auf den Plan gerufen. Sogenannte Initial Coin-Offerings (ICO) und Token-Sales schiessen aktuell wie Pilze aus dem Boden. Solch ein ICO oder Token-Offering ist mit einem Börsengang eines Unternehmens (IPO) vergleichbar. Je nach Ausgestaltung erwirbt der Investor das Recht, die späteren Leistungen des Projekts zu nutzen, oder er partizipiert direkt, indem seine Investition an Wert zulegt.

Die neuen Währungen heissen Tezzies, Atoms oder Basic-Attention-Tokens. Derzeit befinden sich Dutzende weitere ICO in der Finanzierungsphase (Crowdfunding). Selbst Paris Hilton und der ehemalige Boxprofi Floyd Mayweather werben für neue Kryptowährungen oder neue Marktplätze. Anstelle eines stark regulierten Prozesses wie bei einem IPO sind ICO kaum reguliert. Es genügt ein sogenanntes White Paper, in dem die Jungunternehmen ihr Geschäftsmodell – meist leicht positiv gefärbt – darlegen.

Für Start-ups ist die Idee, Geld über ICO einzusammeln, nicht unattraktiv, profitieren sie doch vom derzeitigen Hype rund um das Thema digitale Währungen, ersparen sich mühsame und langwierige Verhandlungen mit Business-Angels oder der Börsenaufsicht und haben durch den Verkauf von Tokens oder Währungen bereits ihre ersten Kunden gesichert. Die berechnete Frage bleibt allerdings, warum man nun tatsächlich Hunderte neue digitale Währungen benötigt, welche man nur auf einem Marktplatz einsetzen kann, wenn umfassende digitale Währungen wie Bitcoin oder Ether bereits existieren. Der Verdacht liegt nahe, dass viele Unternehmen die herrschende Dynamik und letztlich auch das Niedrigzinsumfeld nutzen, um ihr ICO entsprechend zu forcieren und möglichst rasch und viel aufzunehmen. Während die amerikanische Börsenaufsicht Securities and Exchange Commission (SEC) noch vergleichsweise ruhig vor der aktuellen ICO-Welle warnt, wurden ICO und Token-Sales in China verboten.

Handlungsempfehlung: Vom Hype nicht blenden lassen

Über Kryptowährungen, allen voran Bitcoin, und deren Nutzen teilen sich die Meinungen. Jamie Dimon, CEO der Bank J.P. Morgan, hält Bitcoin schlicht für Betrug und droht seinen Mitarbeitenden mit der Kündigung, sollten sie Bankgelder in Kryptowährungen investieren. Der Harvard-Wissenschaftler Dennis A. Porto ist sich hingegen sicher, dass der Bitcoin bereits in den nächsten fünf Jahren auf über USD 100'000 steigen wird. Die Idee der Kryptowährungen und insbesondere der dezentralen Blockchain-Technologie ist revolutionär. Durch die Blockchain kann auf viele bisherige Finanzintermediäre wie beispielsweise Verwahr- und Depotstellen weitgehend verzichtet werden. Dass zahlreiche Finanzinstitute wie beispielsweise die UBS mit ihrem Utility-Settlement-Coin (USC) stark auf die Blockchain setzen, zeigt, dass gerade in der Finanzindustrie das Potenzial für eine neue dezentrale und sichere Technologie gross ist.

Doch Bitcoin ist nicht gleich Blockchain. Bitcoin ist weiterhin eine kryptografische Währung mit enormen Unsicherheiten und Risiken. Die aktuelle Berichterstattung profitiert von den Kurssteigerungen der letzten Monate und wirkt einseitig. Analysen zeigen, dass die starke Kursentwicklung des Bitcoins einen hohen Gleichlauf mit den Google Suchanfragen betreffend Bitcoin, Bitcoin Price und Bitcoin Value aufweist.

Damit steht fest, dass der Kursanstieg in erster Linie durch Marktpsychologie getrieben wurde. Bitcoins wurden unfreiwillig zum Spekulationsobjekt, obwohl ihr eigentlicher Zweck in der sicheren Wertbewahrungsfunktion liegt.

ICO, Tokens und letztlich auch Bitcoins erfahren derzeit einen gewaltigen Hype. Wir raten Anlegern zur Zurückhaltung. So interessant das Konzept der Kryptowährungen auch sein mag, es bestehen erhebliche Risiken. Gerade der noch weitestgehend unklare Umgang mit gesetzlichen Vorschriften birgt erhebliches Rückschlagpotenzial. Für einen allfälligen Einstieg sollten interessierte Investoren auf eine Abkühlung des Marktes und mehr regulatorische Klarheit warten. Bis dahin dürfte der Markt der Kryptowährungen weiterhin als Tummelplatz für Spekulanten dienen.

Hintergrund – Ein Blick hinter die Kulissen

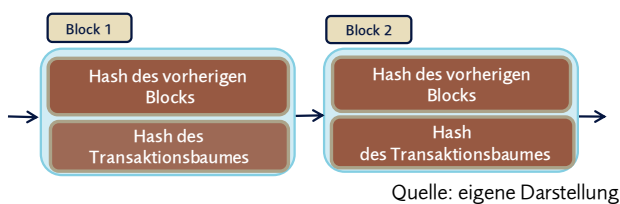
Im zweiten Teil unserer Studie zeigen wir zunächst die technische Funktionsweise von Bitcoins auf. Da den Risiken ein besonderer Stellenwert zukommt, analysieren wir diese ausführlich. Bei indirekten Finanzinvestitionen können die Tücken im Detail liegen. Wir schliessen unsere Analyse mit einer volkswirtschaftlichen Würdigung ab.

Die Funktionsweise von Bitcoin

Wer die Funktionsweise von Bitcoin verstehen will, muss sich mit Begriffen wie Blockchain, Miner, Nodes, Keys, Hashes oder Wallets vertraut machen – doch dies ist im Endeffekt gar nicht so kompliziert. Wir erklären die grundlegende Funktionsweise anhand von Bitcoins; die meisten anderen Kryptowährungen funktionieren nach einem ähnlichen Prinzip.

Als wohl wichtigster Begriff gilt die Blockchain. Wie der Name impliziert, handelt es sich dabei um eine Aneinanderreihung von Datenblöcken, welche die einzelnen Bitcoin-Transaktionen beinhalten (ca. 2'000 Transaktionen). Jeder Datenblock enthält eine einzigartige kryptografische Prüfziffer (Block-Hash-/SHA-256-Algorithmus) des vorangegangenen Blocks. Die Verkettung der einzelnen Datenblöcke schützt jeden einzelnen Baustein vor nachträglicher Veränderung, da bereits die kleinste Manipulation einer Transaktion alle nachfolgenden Blöcke verändern würde und alle Block-Hashes neu berechnet werden müssten. Vereinfacht ausgedrückt bildet die Blockchain also ein dezentral abgespeichertes Transaktionsregister, welches durch eine kryptografische Verschlüsselung und Verkettung vor nachträglichen Veränderungen geschützt ist und ohne klassische Intermediäre auskommt.

Schematische Darstellung der Blockchain:



Bitcoin-Schürfer, also sogenannte Miner, nehmen in diesem System eine besonders wichtige Rolle ein. Mining-Pools wie beispielsweise AntPool oder BTC.TOP sind mit gewaltigen Computeranlagen (Mining-Farms) für die zeitaufwendige Berechnung der Hash-Werte verantwortlich. Haben sie einen Hash-Wert eines Blocks richtig errechnet, erhalten sie eine Belohnung in Form neu kreierter Bitcoins. Die Belohnung, aktuell 12.5 Bitcoins, halbiert sich alle 210'000 Blöcke. Diese Halbierung der Belohnung limitiert die Anzahl an jemals verfügbaren Bitcoins auf 21 Mio. Stück.

Damit nicht alle Bitcoins auf einmal geschürft werden, wird die Schwierigkeit (Difficulty) der Hash-Berechnung alle 2016 Blöcke angepasst, sodass die Miner durchschnittlich nur alle 10 Minuten einen neuen Block einreichen. Der Schwierigkeitsgrad richtet sich nach der gesamten Rechenkapazität des Bitcoin-Netzwerks und steigt in der Regel kontinuierlich an. Dieses etwas umständlich anmutende Verfahren (Proof-of-Work) stellt sicher, dass nicht alle 21 Mio. Bitcoins sofort geschürft werden können. Bitcoin-Miner verarbeiten also Transaktionen zu Datenblöcken. Sie erhalten dafür eine Entschädigung in Form von neu geschaffenen Bitcoins und sind somit die treibende Kraft hinter der Geldschöpfung im Bitcoin-System. Das Rückgrat im dezentralisierten Peer-to-Peer-System Bitcoin bilden sogenannte Full Nodes. Full Nodes sind Rechner im Bitcoin-Netzwerk, welche sowohl Transaktionen als auch Blöcke auf ihre Gültigkeit überprüfen. Jede Full Node speichert die komplette Blockchain und sorgt für die Weiterleitung an andere Schnittstellen.

Aber wie funktioniert nun eine Transaktion in Bitcoins? Um überhaupt Bitcoins transferieren zu können, benötigt man erst einmal ein Wallet mit einer Adresse und einem dazugehörigen privaten Schlüssel. Durch den privaten Schlüssel, eine Kette aus Zahlen und Buchstaben, erhält der Eigentümer nun die Verfügungsgewalt über seine Bitcoins. Der private Schlüssel sollte also besonders sorgfältig aufbewahrt werden.

Möchte man seine Bitcoins versenden, so benötigt man eine Empfängeradresse sowie den eigenen privaten Schlüssel. Mit Hilfe des privaten Schlüssels wird die Transaktion signiert, und das Bitcoin-System (Miner und Nodes) kann nun verifizieren, dass die Transaktion tatsächlich vom aktuellen Inhaber der Bitcoins ausgeführt wurde.

Ist die Transaktion erst einmal genehmigt, wird sie in einem Block aufgenommen, der Blockchain hinzugefügt und dezentral auf allen Full Nodes abgespeichert. Mit jedem weiteren Block gilt die Transaktion als sicherer.

Risiken

Diebstahl oder Verlust

Bitcoins können gestohlen oder vernichtet werden. Als der bekannteste und zugleich grösste Diebstahl in der Geschichte der Bitcoins gilt der Fall Mt.Gox. Infolge eines mysteriösen Diebstahls musste der damalige Marktführer des Bitcoin-Handels Konkurs anmelden. Trotz technologischer Fortschritte folgten weitere Hackerangriffe auf andere Onlinebörsen. Grundsätzlich gilt: Jedes Wallet, das mit dem Internet verbunden ist, kann Ziel eines Hackerangriffs werden, und der private Schlüssel kann entwendet werden. Sogenannte Cold Wallets bieten zwar höheren Schutz, allerdings kann es auch hier zu einem Hardwaredefekt kommen, oder das ausgedruckte Paper-Wallet kann verlorengehen. Ist der private Schlüssel einmal weg, so sind auch die Bitcoins verloren.

Regulatorien und rechtliche Handhabung

Der rechtliche Status von Kryptowährungen unterscheidet sich von Land zu Land. Insgesamt gelten die neuen digitalen Währungen aber als wenig oder nicht reguliert. Dies könnte sich angesichts des aktuellen Hypes um Bitcoin und Co. allerdings bald ändern. Sowohl die amerikanische Börsenaufsicht Securities and Exchange Commission (SEC) als auch die britische Financial Conduct Authority (FCA) hat bereits vor den Risiken der jüngsten Welle von Initial Coin-Offerings (ICO), etwa vergleichbar mit einem Börsengang, gewarnt. Die Chinesische Volksbank (PBoC) hat die Geldaufnahme durch ICO gar ganz verboten, und es gibt bereits Spekulationen, wonach Bitcoin im Reich der Mitte ein ähnliches Schicksal erleiden könnte. Die kritische Haltung vieler Regulatoren gegenüber Bitcoins ist nicht ganz unbegründet. Gemäss einer Studie der Universität von Kentucky haben viele Bitcoin-Transaktionen einen kriminellen Hintergrund. So dienen Bitcoins beispielsweise als Zahlungsmittel im Darknet, zur Verschleierung von Geldströmen (Geldwäsche), aber auch zur Umgehung von Kapitalverkehrskontrollen (China). Die jüngsten Kurssprünge aufgrund der Ereignisse in Japan (offizielles Zahlungsmittel) oder China (Verbot von ICO) verdeutlichen, wie empfindlich der Bitcoin-Kurs auf regulatorische Änderungen reagieren kann.

Liquidität – Volatilität

Definitionsgemäss ist das Angebot von Bitcoins limitiert; lediglich Miner erhöhen in begrenztem Umfang die Geldmenge. Der Markt ist weitgehend nachfragegetrieben. Steigt diese, so wie dies aktuell der Fall ist, sind stark steigende Preise die Folge und umgekehrt. Bei Bitcoin gibt es keine regulierende Notenbank oder Handelspausen wie bei anderen Finanzmärkten. Dreht die aktuell euphorische Stimmung aufgrund eines externen Schocks (Verbot, neue Technologie, Hackerangriff) einmal ins Negative, so kann dies katastrophale Folgen für den Kurs haben, zumal die Marktliquidität relativ beschränkt ist. Im August 2017 wurden täglich rund 158'000 Bitcoins gehandelt. Bei einem Durchschnittspreis von USD 3'800 entspricht dies in etwa dem täglichen Handelsvolumen von IBM (ca. USD 600 Mio.). Die Liquidität ist allerdings auf zahlreiche Börsen aufgeteilt, deren Kurse teilweise deutlich voneinander abweichen können.

Wachsende Konkurrenz und technischer Wandel

Der Markt für Digitalwährungen ist hart umkämpft. Derzeit existieren über 1'000 Alternativen zu Bitcoin, und Dutzende weitere sind kurz vor der Lancierung. Neue Währungen wie Ether, Ripple, Dash oder auch Litecoin erobern in beinahe erschreckender Geschwindigkeit Marktanteile. Anfang 2017 belief sich der Marktanteil (die Marktkapitalisierung) von Bitcoin noch auf 90 Prozent. Dieser Wert ist aktuell auf unter 50 Prozent gesunken. Die junge Konkurrenz ist in vielen Bereichen fortschrittlicher und flexibler als der Vorreiter Bitcoin. So können beispielsweise bei Ethereum sogenannte Smart Contracts (virtuelle, automatisierte Verträge) eingebaut werden, was ganz neue Geschäftsmodelle eröffnet. Auch der

rechen- und damit stromintensive Mining-Prozess, welcher bei Bitcoin auf der Proof-of-Work-Methode basiert, wird bei neueren Währungen zunehmend energiefreundlicher gehandhabt. Das Risiko, dass neue und modernere Kryptowährungen dem Bitcoin zunehmend den Rang ablaufen, ist enorm. Momentan die Kryptowährung zu identifizieren, welche sich langfristig durchsetzen wird, ist angesichts der enormen Vielfalt unmöglich. Eine andere Herausforderung für Bitcoin bleibt der Quantencomputer. Besonders Google und Microsoft, aber auch IBM versuchen schon seit Längerem, einen ersten Quantencomputer zu entwickeln. Die ersten Erfolge wurden in diesem Jahr vorgestellt. Unter gewissen Laborbedingungen ist ein Quantencomputer rund 100 Millionen Mal schneller als seine binären Pendanten. Für Bitcoin wäre ein Quantencomputer definitiv ein Problem. Die Entschlüsselung des wichtigen SHA-256-Algorithmus, eines zentralen Bestandteils der Bitcoin-Technologie, wäre für einen Quantencomputer sehr rasch möglich.

Limitierte Transaktionsabwicklung

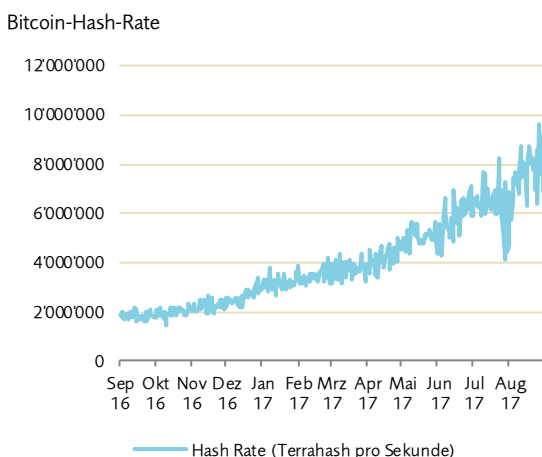
Einer der grössten Mängel bei Bitcoin ist die limitierte Abwicklungskapazität. Eine durchschnittliche Transaktion bei Bitcoin benötigt rund 250 Byte in einem einzelnen Block der Blockchain. Derzeit ist die Blockgrösse im klassischen Bitcoin-Netzwerk noch auf 1 Megabyte (MB) pro Block begrenzt. Rein rechnerisch finden also maximal 4'000 Transaktionen Platz in einem Block. Der Schwierigkeitsgrad (Difficulty) wird bei Bitcoin so festgelegt, dass alle 10 Minuten ein neuer Block erstellt wird. Dies führt dazu, dass pro Sekunde nur rund 7 Transaktionen verarbeitet werden können. Für ein globales Zahlungssystem ist dieser Wert völlig unzureichend, was letztlich die Verbreitung von Bitcoin als weltweit akzeptiertes Zahlungssystem behindert. Der Kreditkartenanbieter Visa verarbeitete bereits im Jahr 2010 rund 1'700 Transaktionen pro Sekunde. Eine Folge dieser doch sehr zaghaften Orderverarbeitung ist ein Rückstau. Dies limitiert den Einsatz von Bitcoin als Zahlungssystem, wo Orderbestätigungen rasch benötigt werden (beispielsweise im Detailhandel). Die Lösung des Problems wäre technisch einfach umsetzbar, allerdings gestaltet sich die Konsensbildung in der Bitcoin-Community sehr schwierig. Mit der Änderung des Transaktionsformats (SegWit) konnten die Blöcke etwas entschlackt werden, sodass mehr Transaktionen in einem Block Platz finden. Die angedachte Erhöhung der Blockgrösse auf 2 MB (SegWit2x) per November dieses Jahres spaltet aber die Community. Eine weitere Spaltung der Bitcoin-Blockchain (Hard Fork), wie sie im September bereits zur Entstehung von Bitcoin Cash geführt hat, erscheint als wahrscheinliches Szenario. Jede Spaltung der bestehenden Blockchain führt letztlich zu einer weiteren Kryptowährung, wodurch der ursprüngliche Bitcoin geschwächt wird. Anleger müssen sich daher stets darüber auf dem Laufenden halten, ob die neu abgespaltete Währung auch in ihrem Wallet Einzug findet und ob sie an Börsen gehandelt werden kann.

Endlichkeit der Bitcoins

Das Angebot an Bitcoins ist endlich und im Quellcode auf 21 Mio. Stück begrenzt. Dies wird von Verfechtern oft als grosser Vorteil aufgeführt, mit dem sich eine schleichende Geldentwertung effektiv verhindern liesse. Die Geldschöpfung bei Bitcoins geschieht über den Mining-Mechanismus. Derzeit erhält ein Miner für jeden gültigen Block eine Entschädigung von 12.5 Bitcoins. Diese Entschädigung wird alle 210'000 Blöcke halbiert. Die Halbierung wird voraussichtlich im Juni 2020 stattfinden, und der letzte Bitcoin wird wohl im Jahr 2140 geschaffen werden. An der Endlichkeit der Bitcoins ist an und für sich nichts auszusetzen. Allerdings werden die für Bitcoin-Transaktionen zentralen Miner mit immer weniger Bitcoins belohnt, obwohl der dafür nötige Rechenaufwand tendenziell immer höher wird. Dies kann effektiv dazu führen, dass sich der Aufwand für viele Miner nicht mehr lohnt und es zu einer Konzentration auf wenige Mining-Anbieter oder zu einer Erhöhung der zusätzlichen Transaktionskosten kommt.

Stromverbrauch und Umwelt

Die Validierung von Bitcoin-Transaktionen (Mining) und der dafür notwendige Proof-of-Work-Prozess ist ökologisch vollkommen unverantwortlich. Aktuell leistet das Bitcoin-Netzwerk rund 8 Mio. Terahashes pro Sekunde. Ein klassisches Mining-Gerät wie der Antminer S9 benötigt etwa 0.098 Watt pro Gigahash/s. Die etwas vereinfachte Rechnung besagt also, dass das aktuelle Bitcoin-Netzwerk rund 800 Megawatt Strom benötigt. Dies entspricht in etwa der doppelten Leistung des Kernkraftwerks Mühleberg in der Schweiz und wäre genug, um mehr als 500'000 amerikanische Haushalte zu versorgen.



Quelle: VP Bank, www.blockchaininfo.info

Das Magazin Vice errechnet, dass man pro Bitcoin-Transaktion rund 1.5 US-Haushalte für einen Tag lang mit Energie versorgen könnte. Dieser enorme Energieverbrauch ist angesichts des weltweiten Bestrebens nach mehr Energieeffizienz höchst problematisch. Die Hauptschuld trägt daran das implementierte Proof-of-Work-System, wonach jeder Bitcoin-Miner unzählige

Rechenaufgaben zu lösen hat, bis er einen gültigen Hash errechnet hat und den Block einreichen kann. Viele Bitcoin-Miner haben sich entsprechend auch an Orten mit niedrigen Strompreisen angesiedelt, beispielsweise in China (70 Prozent der Miner) oder Island (Geothermie).

Die Tücken der Finanzinvestitionen

Das bereits seit längerem verfügbare Zertifikat der Bank Vontobel zeigt, dass solche Finanzprodukte nicht ganz einfach in der Handhabung sind. Durch die Hard-Fork-Aufspaltung der Blockchain in Bitcoin und Bitcoin Cash im August war Vontobel gezwungen, ihren Bitcoin-Anlegern zusätzliche Bitcoin-Cash-Zertifikate mit stark eingeschränkter Liquidität auszuhändigen. Kommt es im November aufgrund der SegWit2x-Problematik erneut zu einer Gabelung der Blockchain, hätten ursprüngliche Zertifikathalter entsprechend drei unterschiedliche Zertifikate im Depot, wovon zwei nur eingeschränkt handelbar wären. Ähnlich verhält es sich bei den neu eingeführten Bitcoin-Konten der Swissquote Bank oder der Falcon Private Bank. Investoren, welche das Risiko von Bitcoins dennoch nicht scheuen, aber sich wenig für die technische Abwicklung interessieren, sollten auf existierende Finanzprodukte setzen, wie sie beispielsweise von Vontobel angeboten werden. Technisch interessierte Anleger, welche sich besonders für die Funktionsweise von Bitcoins interessieren und auch allfällige Überweisungen damit tätigen wollen, sollten eine direkte Investition mit begrenztem Kapitaleinsatz riskieren.

Bitcoin aus volkswirtschaftlicher Sicht

Die Währungsausgabe ist ein staatliches Monopol. So ist der Schweizer Franken das gesetzliche Zahlungsmittel der Schweiz, für die Eurozone ist es der Euro. Das Wort «gesetzlich» zeigt schon, dass hier der Staat die Hoheit besitzt. Im staatlichen Auftrag übernehmen die jeweiligen Zentralbanken die Kontrolle über das Geldsystem. Im Idealfall wird der Notenbank eine institutionelle, funktionelle, finanzielle und personelle Unabhängigkeit zugewiesen. Kritiker sehen aber genau hierin die Schwäche unseres Geldsystems. Zentralbanken seien in der Praxis eben doch nicht unabhängig und tendierten im Interesse der Schuldenreduktion zu einer Inflationierung, lautet kurz und knapp das Fazit. Die sogenannte österreichische Schule der Nationalökonomie, die von Carl Menger (1840 bis 1921) etabliert wurde, gab der Kritik am Papiergeldsystem einen theoretischen Unterbau. Einer der berühmtesten Vertreter dieser Denkschule war Friedrich August von Hayek (1899 bis 1992), der sich sogar für eine Entstaatlichung des Geldsystems und für konkurrierende Währungen aussprach. Durch die Konkurrenz werde sich am Ende die stabilste Währung durchsetzen, so die Kernthese Hayeks.

Der Bitcoin kommt dem, was Hayek sich wünschte, sicherlich sehr nahe. Doch auch der Bitcoin hat Schwächen. Zwar ist eine inflationäre Wirkung aufgrund der Begrenzung auf 21 Millionen Stück theoretisch reduziert, doch die Währung hat andere wunde Punkte. Genau diese Mengenbegrenzung kann im Zuge der Krisenbewältigung zum Bumerang werden.

In den Krisenmonaten der Jahre 2008 und 2009 konnten die Notenbanken gerade aufgrund der Tatsache, dass die Geldmenge nicht konstant ist, zusätzliche Liquidität bereitstellen und dadurch noch Schlimmeres verhindern. Die konstante Geldmenge des Bitcoins hätte dies unmöglich gemacht. Die «Knappheit» des Bitcoins und die mangelnde Liquidität schlagen sich in einer entsprechend deutlichen Volatilität nieder, das heisst, die Schwankungsanfälligkeit ist sehr hoch. Die Kursausschläge machen eine Nutzung im täglichen Gebrauch aber unmöglich. Ein Einzelhändler, der Bitcoins akzeptiert und anschliessend beispielsweise in US-Dollars tauschen möchte, kann unter Umständen Kursschwankungen von über USD 1'000 innerhalb weniger Handelstage unterliegen. Die Nutzung in der Praxis ist damit kaum möglich – eine sichere Kalkulationsgrundlage fehlt. Dadurch, dass er als Zahlungsmittel im täglichen Gebrauch de facto ausscheidet, führt sich der Bitcoin jedoch ad absurdum.

Bei der Beurteilung von Kryptowährungen sollte auch Folgendes bedacht werden: Der Bitcoin hat wie das Papiergeld keinen inneren Wert. Es handelt sich lediglich um virtuelles Geld, das nicht mit Wertgegenständen wie etwa Gold hinterlegt ist. Damit wird der Bitcoin aber ebenfalls beliebig bzw. austauschbar. Selbst in Zeiten der Hyperinflation besitzt eine offizielle Währung noch einen minimalen Restwert, da es sich dabei um ein gesetzliches Zahlungsmittel handelt und somit noch ein gewisser Tauschwert gegeben ist. Dies fehlt dem Bitcoin: Ein Totalverlust ist möglich. Es sollte auch nicht vergessen werden, dass der Bitcoin gerade aufgrund des fehlenden Status als gesetzliches Zahlungsmittel auch jederzeit verboten werden kann.

Zusammenfassend gilt: Der Bitcoin taugt nur begrenzt als Ersatz für unser bestehendes Geldsystem. Die virtuelle Währung weist bei genauer Analyse eklatante Schwächen auf. Weiterentwicklungen der österreichischen Schule gehen deshalb davon aus, dass das Geld, das auf dem freien Markt entsteht, immer eine Metall- oder Rohstoffwährung sein wird. In einem freien Wettbewerb würden die Menschen gedeckte Währungen den ungedeckten immer vorziehen. Neu herausgegebenes, ungedecktes Geld habe ohne staatlichen Zwang keinen Wert, da es keine Möglichkeit der Wertermittlung gäbe. Der innere Wert gehe deshalb gegen null, weshalb auch beim Bitcoin der Totalverlust drohe.

Kontakt

VP Bank AG

Aeulestrasse 6
9490 Vaduz · Liechtenstein
T +423 235 66 55 · F +423 235 65 00 · info@vpbank.com

VP Bank (Schweiz) AG

Bahnhofstrasse 3
8001 Zürich · Schweiz
T +41 44 226 24 24 · F +41 44 226 25 24 ·
info.ch@vpbank.com

VP Bank (Luxembourg) SA

26, Avenue de la Liberté
L-1930 Luxemburg · Luxemburg
T +352 404 770-1 · F +352 481 117 · info.lu@vpbank.com

VP Bank (BVI) Ltd

VP Bank House · 156 Main Street · Postfach 2341
Road Town · Tortola VG1110 · Britische Jungferninseln
T +1 284 494 11 00 · F +1 284 494 11 44 ·
info.bvi@vpbank.com

VP Bank (Singapore) Ltd

8 Marina View · #27-03 Asia Square Tower 1
Singapur 018960 · Singapur
T +65 6305 0050 · F +65 6305 0051 · info.sg@vpbank.com

Verantwortlich für den Inhalt

Bernd Hartmann, Leiter Group Investment Research

Analyse: Rolf Kuster, Senior Investment Strategist

Bitcoin aus volkswirtschaftlicher Sicht: Dr. Thomas Gitzel,
Senior Economist

Wichtige rechtliche Hinweise

Diese Dokumentation wurde von der VP Bank AG (nachfolgend Bank) erstellt und durch die Gesellschaften der VP Bank Gruppe vertrieben. Diese Dokumentation stellt kein Angebot und keine Aufforderung zum Kauf oder Verkauf von Finanzinstrumenten dar. Die darin enthaltenen Empfehlungen, Schätzungen und Aussagen geben die persönliche Auffassung des betreffenden Analysten der VP Bank AG im Zeitpunkt des auf der Dokumentation genannten Datums wieder und können jederzeit ohne vorherige Ankündigung geändert werden. Die Dokumentation basiert auf Informationen, welche als zuverlässig eingestuft werden. Diese Dokumentation und die darin abgegebenen Einschätzungen oder Bewertungen werden mit äusserster Sorgfalt erstellt, doch kann ihre Richtigkeit, Vollständigkeit und Genauigkeit nicht zugesichert oder gewährleistet werden. Insbesondere umfassen die Informationen in dieser Dokumentation möglicherweise nicht alle wesentlichen Angaben zu den darin behandelten Finanzinstrumenten oder deren Emittenten.

Weitere wichtige Informationen zu den Risiken, welche mit den Finanzinstrumenten in dieser Dokumentation verbunden sind, zu den Eigengeschäften der VP Bank Gruppe bzw. zur Behandlung von Interessenkonflikten in Bezug auf diese Finanzinstrumente sowie zum Vertrieb dieser Dokumentation finden Sie unter https://www.vpbank.com/rechtliche_hinweise