MAERKI BAUMANN & CO. AG

PRIVATBANK

Kryptowährungen - Was ist das eigentlich?

Finanzthema, Januar 2019

Die turbulente Wertentwicklung von Bitcoin hat das Interesse der breiten Öffentlichkeit im vergangenen Jahr auf diese Kryptowährung gelenkt. Dabei besteht diese Währung bereits seit fast zehn Jahren und seitdem sind schätzungsweise über 1600 weitere Währungen hinzugekommen. Oft wird die Frage gestellt, ob es sich bei diesen Konstrukten, die lediglich als digitaler Code existieren, überhaupt um Währungen vergleichbar mit Dollar, Euro oder Yen handelt. Diese Frage wird später noch einmal kurz beleuchtet. Zunächst ist es hilfreich zu wissen, was hinter den Kryptowährungen wie Bitcoin, Ether oder Ripple eigentlich steckt.

Diese Währungskonstrukte basieren auf der im Jahr 2008 entwickelten Blockchain-Technologie. Diese Computertechnologie basiert darauf, dass Daten verschlüsselt, gleichzeitig auf vielen Rechnern gespeichert werden. Ebenso werden die Daten des Eigentümers und die Daten zum Eigentumsübertrag in die Verschlüsselung mit einbezogen. Mit jeder Übertragung werden die verschlüsselten Daten ergänzt. Damit diese Informationen nicht verfälscht oder nachträglich korrigiert werden können, werden alle Angaben zu einer einzelnen Zeichenkette zusammengerechnet. Diese Zeichenfolge wird als Hash bezeichnet, da alle Daten zerkleinert und vermengt werden. Eine Blockchain besteht aus einer Abfolge dieser Hashs, die zwar von allen gelesen werden können, aber nur Derjenige, der über den Schlüssel zur Decodierung verfügt, kann daraus auch wieder sinnvolle Daten entschlüsseln. Eine Weitergabe eines Blockes ist nur möglich, wenn die Mehrzahl der Rechner die Richtigkeit der Zeichenkette bestätigt. Eine Manipulation des Codes ist somit kaum möglich.

Durch die dezentrale Konstruktion dieser Technologie ist es möglich, dass man zwischen völlig Fremden einen Tausch durchführen kann, ohne dass diese sich kennen oder vertrauen müssen. Das Vertrauen wird durch die Sicherheit der Codierung und die Unbestechlichkeit des Systems sowie die Anzahl der Teilnehmer gewährleistet. Eine rückwirkende Änderung der Blockchain, d. h. ein Betrug, erfordert zwei Dinge, die – nach heutigem Wissensstand – nur mit unverhältnismässig hohem Aufwand – erreicht werden können. Zum einen, muss die Codierung einer Blockchain ohne privaten Schlüssel fehlerfrei entschlüsselt und verändert werden. Zum anderen muss diese Änderung auf mindestens 51 % aller im Netzwerk verbundenen Rechner hinterlegt werden. Denn nur wenn die Mehrzahl aller Rechner einer Transaktion zustimmt und diese für korrekt befindet, kann die Übertragung stattfinden.

Diese Technologie kann nicht nur für Kryptowährungen genutzt werden, sondern für jegliche Art von Übertragung von materiellen oder immateriellen Wertgegenständen. So wird diese Technologie beispielsweise bereits heute beim Handel von Diamanten verwendet.

> Diese Technologie kann für jegliche Art von Übertragungen von materiellen und immateriellen Wertgegenständen genutzt werden.

Nun stellt sich die Frage, welchen Wert diese Währungen repräsentieren. Abgesehen von Kryptowährungen, die von einem Staat herausgegeben werden, wie der kritisch betrachtete venezolanischen Petro, sind diese Währungen nicht durch die Finanzkraft eines Landes gesichert. Beim Handel von Kryptowährungen handelt man also im Vertrauen darauf, dass ein anderer, diese als Tauschmittel gegen Franken, Dollar oder Euro akzeptiert.

Wie kann man Kryptowährungen handeln?

Diese Währungen werden an hunderten von unterschiedlich vertrauenswürdigen Tauschbörsen im Internet gehandelt. Dabei können je nach Tauschbörse sowohl Kryptowährungen gegeneinander, also z. B. Ripple gegen Ether aber auch die erworbenen Bitcoins wieder in US-Dollar oder Yen getauscht werden. Auch können Bruchteile von Kryptowährungen gehandelt werden, da die Währungseinheiten sehr einfach in kleinere Einheiten aufgeteilt werden können. Ebenso kann von einem einmal gekauften Bestand auch nur ein Teil wieder veräussert werden.

Für das Eröffnen eines Kontos und den Kauf von Kryptowährungen ist eine Wallet (elektronische Geldbörse) erforderlich. Eine Wallet ist ein kleines Programm, das auf dem Smartphone oder dem Rechner installiert wird und zwei Aufgaben hat. Zum einen, kann damit ein privater Schlüssel erzeugt werden, der für die Unterschrift bei Transaktionen und dem Zugriff auf das eigene Konto unerlässlich ist. Geht dieser private Schlüssel verloren, sind auch die damit gesicherten Werte verloren, da diese ohne den Schlüssel weder entschlüsselt noch übertragen werden können. Zum zweiten dient die Wallet der Aufbewahrung von Ether, Bitcoin und Co. Im wahrsten Sinne des Wortes ist es ein Portemonnaie in dem die virtuellen Geldeinheiten aufbewahrt werden, bis man sie verkauft oder damit bezahlt.

Wie bewahrt man Kryptowährungen auf?
Die Wallet-Applikationen sind in der Regel kostenlos und erlauben es, ähnlich wie ein privater Tresor, das Vermögen in Kryptowährungen unabhängig von Banken oder Börsen aufzubewahren. Man kann jederzeit und von überall her auf diese Wallet zugreifen, was sie besonders attraktiv für Menschen macht, die sich in unsicheren Umgebungen bewegen, z. B. Flüchtlinge oder Einwohner von Staaten ohne funktionierendes Rechtssystem.

Für die Aufbewahrung von Kryptowährungen kommen daneben noch drei weitere, unterschiedlich sichere Speichermöglichkeiten in Frage. Der unsicherste Ort ist ein Konto bei einem der vielen Handelsplattformen bzw. Kryptobörsen. Diese Konten werden auch als Hot Wallet bezeichnet. Die Sicherheitsstandards dieser Einrichtungen sind höchst unterschiedlich, da es bislang praktisch keine Regulierung für solche Marktplätze gibt. Die immer wieder kolportierten Diebstähle von Bitcoins beziehen sich fast immer auf erfolgreiche Hackerangriffen auf diese Börsen, bei dem die Diebe die Konten der Kunden leerräumen. Wesentlich sicherer ist es, grössere Beträge bei vertrauenswürdigen Kryptobrokern in deren gesicherten Speichern aufbewahren zu lassen. Natürlich können die Kryptowährungen auch in der privaten Wallet auf dem eigenen Rechner oder Smartphone gespeichert werden.

Noch mehr Sicherheit versprechen spezielle Geräte, die nur bei Bedarf mit dem Rechner bzw. dem Smartphone und damit dem Internet verbunden werden müssen. Dabei handelt es sich eigentlich um eine Art besonders gesicherter Geräte, z. B. Verschlüsselungsboxen. Im Fachjargon werden diese Geräte auch als cold store bezeichnet. Die sicherste Möglichkeit, den eignen Bestand an Ether, Ripple oder Bitcoin aufzubewahren ist immer noch, den Blockchain-Code und den privaten Schlüssel auszudrucken und in einen Stahltresor zu legen.

Je nachdem, wie man die Währungseinheiten aufbewahrt, sind diese auch unterschiedlich schnell verfügbar. Für tägliches Trading an einer Börse ist es sinnvoll, eine gewisse Menge auf dem Konto bei einer Börse oder einem Broker vorzuhalten. Einig wenige Anbieter trennen von sich aus die Trading-Bestände von den grösseren Beständen, die aktuell nicht für den täglichen Handel benötigt werden. Da es etwas umständlicher ist, Bitcoins und privater Schlüssel vom Papier oder aus dem cold store zu veräussern, eignen sich diese Aufbewahrungen auch eher für grössere Beträge, auf die man selten zurückgreift.

Wie kann man Kryptowährungen schürfen?
Die Sicherheit und das Funktionieren von Blockchains hängt entscheidend von der Anzahl der Rechner ab, die Transaktionen prüfen und für korrekt befinden. Diese Arbeit – Transaktionen von Dritten prüfen und die veränderten Blockchains lokal speichern – erfordert Rechenaufwand und Speicherkapazität. Um diesen Aufwand zu vergüten, können Teilnehmer auch neue Währungseinheiten errechnen und diese dann als persönlichen Gewinn verbuchen. Diesen Vorgang nennt man Mining oder Schürfen. Um zum Beispiel neue Bitcoins zu schürfen, ist es erforderlich, dass die Daten von Informationsblöcken zu einem Hash verschlüsselt werden. Als Belohnung erhält der Miner nach Abschluss der Verschlüsselung (momentan) 12,5 Bitcoins. Im Algorithmus sind zusätzlich Regeln hinterlegt, die in Zukunft die Verschlüsselung immer schwerer machen. Gleichzeitig werden für jede Verschlüsselung immer weniger Bitcoins vergütet. Daher sind inzwischen nur noch grosse Serverfarmen beim Schürfen nach neuen Bitcoins wirklich profitabel.

Aber auch Privatpersonen ohne Dutzende von Rechner können noch immer von diesem Mining profitieren. Oft arbeiten mehrere Miner gleichzeitig an einem Block und die Belohnung wird dann je nach Anteil verteilt. Für diese Zwecke gibt es «Mining Pools», die dafür sorgen, dass der Mining-Ertrag berechenbarer und regelmässiger wird. Allerdings kostet die Mitgliedschaft hier etwas, was den Ertrag schmälert. Für ein effektives Mining ist die Leistungsfähigkeit der Prozessoren des Rechners entscheidend, da diese die Geschwindigkeit bestimmt, mit der die Verschlüsselung erfolgt. Die Kosten für aktuelle Generation solcher Chips, zusammen mit den anfallenden Stromkosten, machen das Mining in kleinem Rahmen nur bedingt profitabel.

Wie unterscheiden sich die Kryptowährungen?
Derzeit existiert eine sehr grosse Zahl von unterschiedlichen Währungen, Token, Coins etc., die auf der Blockchain-Technologie basieren. Grundsätzlich lässt sich sagen, dass man diese Konstrukte – analog zu der Einteilung der Eidgenössischen Finanzmarktaufsicht – danach einteilen kann, was sie repräsentieren. Somit kann man von Konstrukten sprechen, die Vermögenswerte repräsentieren (Asset Token), solche die Nutzungsrechte darstellen (z. B. Mitgliedschaften, Utility Token) und Zahlungstoken (Payment Token, z. B. Ether). Im Folgenden konzentrieren wir uns auf die dritte Gruppe.

Bitcoin ist sicherlich die bekannteste und bedeutendste Kryptowährung. Die weite Verbreitung bietet eine hohe Akzeptanz und hohe Liquidität beim Handel. Gleichzeitig zieht diese Währung auch Kriminelle und Betrüger an, die die Unerfahrenheit von Neulingen ausnutzen.

Ether ist die Währung, die auf der Ethereum-Plattform basiert, die eine weiterentwickelte und flexiblere Blockchain-Technologie verwendet. Der grosse Vorteil gegenüber Bitcoin ist, dass mit dem Übertrag von Ether weitere Bedingungen verknüpft werden können, die direkt im

Code der Blockchain hinterlegt werden. Dieses Verfahren, smart contract genannt, erlaubt damit eine wesentlich grössere Anwendungsvielfalt als Bitcoin. Ausserdem ist in diesem Code keine maximale Anzahl von Einheiten hinterlegt, sodass bei Bedarf stets weitere Ether geschaffen werden können.

Ripple ist eine Währung, die nicht über die dezentrale Struktur von verschiedenen, unabhängigen Rechnern setzt. Vielmehr erfolgt hier das zentrale Mining und die Authentifizierung über die Firma Ripple Labs. Die Währung wurde vor allem für Banken entwickelt, um deren Zahlungsverkehr zu vereinfachen und zu beschleunigen.

Litecoin ist eine Abspaltung (Fork) von Bitcoin, das heisst, technologisch basiert die Währung auf der gleichen Technologie, bietet aber eine wesentlich schnellere Abwicklung von Transaktionen. Dazu nutzt die Währung das Lightning Netzwerk, das wesentlich mehr Transaktionen verarbeiten kann, als herkömmliche Netze. Zusätzlich ist Litecoin wesentlich günstiger in der Nutzung als Bitcoin.

Gibt es Alternativen zu Direktanlagen?
Insbesondere für mit Kryptowährungen weniger vertraute Anleger gibt es inzwischen eine Auswahl von Anlageprodukten (Investmentfonds, Strukturierte Produkte bzw. Zertifikate). Diese bilden entweder die Wertentwicklung einzelner Währungen oder die eines definierten Korbs von Kryptowährungen ab. Während so das Handels- und Aufbewahrungsrisiko für die Währungen wegfällt, ist die Qualität des Emittenten und die Anlagepolitik des Emittenten zu beachten. Hier sind Produkte bekannter Unternehmen aus der Schweiz oder den Nachbarländern zu bevorzugen.

Wertentwicklung: eine Achterbahnfahrt
Die Preisentwicklung von Kryptowährungen glich in der Vergangenheit einer Achterbahnfahrt. Die Gründe für diese Kursausschläge sind vielfältig, haben aber nichts mit den üblichen Faktoren zu tun, die die Wechselkurse klassischer Währungen bestimmen. Deren Kurse werden überwiegend durch die aktuellen und erwarteten Zinssätze im jeweiligen Währungsraum, die erwartete wirtschaftliche Entwicklung sowie - zu einem gewissen Grade – durch politische Faktoren bestimmt. Für Kryptowährungen sind solche Rahmenbedingungen nicht relevant, da sie unabhängig von Volkswirtschaften und Währungsräumen sind. Aus diesem Grund sind hier andere Preisfaktoren am Werk.

Wie bei allen Gütern sind zunächst Angebot und Nachfrage entscheidend für die Preisbildung. Im Fall von Bitcoin ist unter diesem Aspekt zu beachten, dass die maximal mögliche Anzahl von Währungseinheiten auf knapp 21 Millionen beschränkt ist. Das heisst, bei steigender Nachfrage und gleichbleibendem Angebot wird der Preis tendenziell steigen. Andere Kryptowährungen haben keine solche Einschränkung. Einige Experten sind der Meinung, dass für die Kursentwicklung auch die Nützlichkeit und Anwendungshäufigkeit einer Kryptowährung wichtig ist. In jedem Fall beeinflusst es die Liquidität einer Währung, wenn sie in vielen Bereichen als Zahlungs- und Tauschmittel akzeptiert ist. Kurzfristig sind Nachrichten über diese neuen Währungen der grösste Einflussfaktor auf die Kurse. Die Meldungen über Diebstähle von Währungen, Sicherheitsprobleme in Handelsplattformen oder das Verbot von Initial Coin Offerings (eine Art Wertpapieremission auf Grundlage von Blockchain-Technologie) durch einzelne Staaten können den Kurs einer Währung drücken. Hinzu kommen – wie in anderen Märkten – allgemeine Marktstimmungen und –erwartungen sowie die Einschätzungen anderer Vermögensklassen, die als Anlagealternativen dienen können.

Preisentwicklung Bitcoin vs. USD

Quelle: Bloomberg

So sind die Gründe für die starken Verluste der Kryptowährungen im vergangenen Jahr vielfältig. Durch die Verschärfung der Regulierungen für den Handel, Besitz und das Mining in diversen Ländern haben diese Währungen an Attraktivität verloren. Grosse Investoren haben nach dem massiven Anstieg im Jahr 2017 Gewinne realisiert oder sind Wetten eingegangen, die auf einen Kursrückgang setzen (Short-Position). Die wiederholte Ablehnung der US-Aufsicht, Fonds für Kryptowährungen zuzulassen taten ein übriges. Schliesslich dürfte die Abspaltung von Bitcoin Cash von Bitcoin viele Anleger verunsichert haben.

Soll man investieren?
Die Dynamik im Bereich der Kryptowährungen wie Bitcoin, Ether oder Ripple hatte 2017 und 2018 mit der dramatischen Berg- und Talfahrt diverser Währungen, der massiven Zunahme von Initial Coin Offerings (ICO) und den regulatorischen Reaktionen in verschiedenen Staaten einen Höhepunkt erreicht. Hinzu kommt inzwischen auch eine weitere Form der Blockchain-basierten Finanzierung. Die als Security Token Offering (STO) bezeichneten Aktionen verbriefen – anders als bei ICO – einen Anspruch auf Erträge oder Vermögenswerte der herausgebenden Firma. Dies bietet Investoren eine grössere Sicherheit, als bei ICOs. Gleichzeitig ist die rechtliche

Stellung von Kryptowährungen und Tokens aus ICO noch nicht abschliessend geklärt. So unterscheidet sich die pragmatische Beurteilung der FINMA sehr stark von der in den USA üblichen Haltung der Aufsichtsbehörde, dass alle Kryptowährungen als Wertpapiere gelten. Ob den Kryptowährungen ein langfristiger Erfolg beschieden sein wird, ist derzeit noch nicht abzusehen. Allerdings gehen wir davon aus, dass Kryptowährungen nicht mehr vollständig verschwinden werden. Vielmehr sind wir überzeugt, dass eine regulierte Anwendung der Blockchain-Technologie für den Handel von Vermögenswerten, die per Token einfach übertragen werden können, grosse Chancen bietet.

Derzeit sehen wir eine gewisse Stabilisierung sowohl in den Märkten als auch in den Regulierungen. Allerdings sind bei letzteren stark divergierende Entwicklungen zu beobachten. Einige Staaten fördern die Entwicklung dieser Instrumente durch eine wohlwollende Regulierung und damit eine Regelung von rechtlichen Fragen (Schweiz, Japan, Grossbritannien, Schweden). Bei anderen Staaten steht das Verbot des Handels und der Gewinnung (Mining) von Kryptowährungen derzeit im Vordergrund, während gleichzeitig Überlegungen für eine staatliche Blockchain-basierte Währung bestehen (China, Südkorea, Russland).

Die Annahme und Verwahrung von Geldern, die aus der Gewinnung (Mining) und dem Handel mit Kryptowährungen stammen, birgt für Banken und Investoren rechtlich noch diverse Unsicherheiten, da Vorgaben der verschiedenen nationalen Aufsichtsbehörden fehlen. Ein lückenloser Nachweis der Mittelherkunft ist aufgrund der technischen Konstruktion von Kryptowährungen prinzipiell möglich. Allerdings kann dies je nach Umfang der Handelsaktivität sehr aufwändig sein.

Maerki Baumann beobachtet die Entwicklung dieser Anlageinstrumente und die zugrundeliegende Regulierung aufmerksam, ohne dass wir uns in diesem Bereich derzeit engagieren wollen. Dies betrifft sowohl Investitionen in Kryptowährungen wie auch in die erforderlichen Technologien zum Handel und der Aufbewahrung dieser Instrumente. Wir sehen Kryptowährungen zurzeit als Alternative Anlageinstrumente, für die aber nur begrenzte Erfahrungswerte und Daten (Kurse, Volatilität, Handelsvolumen) verfügbar sind. Maerki Baumann ist grundsätzlich offen für Vermögen aus Kryptowährungen, sei es aus Spekulationsgeschäften, als erhaltene Zahlungen für eine erbrachte Leistung oder aus Mining-Erfolgen. Generell raten wir derzeit von grösseren Anlagen in Kryptowährungen ab. Kryptowährungen sind, aufgrund der oben ausgeführten Unsicherheiten nach unserer Einschätzung nicht als Basis für langfristige Investments geeignet. Nur Personen, die sich der Risiken, die mit diesen Anlageinstrumenten verbunden sind, bewusst sind, sollten einen begrenzten Teil ihres verfügbaren Vermögens investieren. Allen anderen Personen raten wir derzeit von grösseren Investments ab. Direktinvestitionen bietet Maerki Baumann nicht an, wir sind aber gerne bei der Beurteilung von Anlageprodukten behilflich. Maerki Baumann gibt keine Empfehlungen bezüglich der Qualität von Kryptobörsen und/oder Aufbewahrungslösungen («Wallets») ab, stellt aber bei Bedarf gerne den Kontakt zu Fachexperten im Bereich der Blockchain-Technologie oder Kryptowährungen her.

Redaktion: Milko G. Hensel, IT & Digitalisierung

Redaktionsschluss: 9. Januar 2019

Maerki Baumann & Co. AG
Dreikönigstrasse 6, CH-8002 Zürich
T +41 44 286 25 25, info@maerki-baumann.ch
www.maerki-baumann.ch