

Eine kurze Währungsgeschichte¹

Oft wird in Lehrbüchern geschrieben, dass Geld erfunden wurde, um den Tauschhandel zu ersetzen. Tatsächlich gehen die Ursprünge des Geldes auf Kreditsysteme zurück, die innerhalb von Gemeinschaften entstanden, in denen die Beteiligten regelmäßig interagierten. Tauschhandel und später das Bezahlen mit Gold- und Silbermünzen fand überwiegend nur zwischen Gemeinschaften und Akteuren statt, die wenig Kontakt miteinander hatten. Der daraus entstehende Edelmetallstandard hatte jedoch zwei große Nachteile. So gab es vor allem im Mittelalter viel zu wenig (Klein-)Geld, sodass sich viele nutzbringende Wirtschaftstransaktionen nicht abwickeln ließen. Darüber hinaus kam es oft zu Instabilitäten, da ein großer Bestand an Silber- oder Goldmünzen ins Ausland abfließen konnte, wenn es gewinnbringend war. Eine Lösung für die Geldknappheit war es, die Geldproduktion den Geschäftsbanken zu übertragen und es ihnen zu erlauben, auf ihren Goldbestand mehrfach Kredite zu vergeben. Das sogenannte „Mindestreserven-Bankwesen“ entstand. Damit verlagerten sich die Instabilitäten auf das Bankensystem, das aber in Krisenzeiten nicht genug Gold hatte, um die Goldforderungen aller Gläubiger zu bedienen. In der Folge wurde die Goldbindung aufgehoben. Damit fiel jedoch auch eine natürliche Beschränkung der Kreditvergabe, und die Banken konnten nunmehr (theoretisch) unbegrenzt Kredit vergeben. Das ausstehende Kreditvolumen ist daher seit den 1970er-Jahren regelrecht explodiert, und die gesamtwirtschaftliche Bedeutung des Finanzsektors hat rapide zugenommen. Die Erfindung der Kryptowährungen könnte eine Weiterentwicklung des Geldsystems ermöglichen. So wäre es denkbar, dass die Zentralbanken ihre eigenen Kryptowährungen ausgeben, die nur durch Staatsanleihen gedeckt wären – und nicht wie jetzt durch Kredite an den Privatsektor. Die Banken würden dann nicht mehr mit der Vergabe eines Kredits neues Geld schöpfen, sondern müssten Geld einwerben, um damit Kredite vergeben zu können. Das Bankensystem wäre damit sicherer, aber die Verfügbarkeit von Krediten würde merklich sinken.

Eine kurze Währungstheorie¹

Eigentlich produziert ein Staat Geld, um damit seine Ausgaben zu finanzieren. Wäre dies alles gewesen, wäre über die Zeit immer mehr Geld in Umlauf gekommen – und die Akzeptanz von Geld als Zahlungsmittel für private Transaktionen wäre dann abhängig vom Vertrauen der Privathaushalte in die Geldwertstabilität. Durch die Erhebung von Steuern sammelt der Staat jedoch das ausgegebene Geld zumindest teilweise wieder ein, sodass die Geldmenge nur begrenzt wächst. Die Steuern haben jedoch eine noch weit wichtigere Funktion: Jedes Wirtschaftssubjekt benötigt das staatliche Geld, um seine Steuerschulden zu begleichen. Dadurch gibt es eine „erzwungene“ Nachfrage nach dem staatlichen Geld, die es nahezu unmöglich macht, das „staatliche“ Geldsystem durch ein „privates“ Geldsystem wie Kryptowährungen abzulösen. Auch ist das staatliche Geld in der Regel gesetzliches Zahlungsmittel, das es Schuldner erlaubt, ihre Schulden jederzeit damit zu begleichen. Ein staatliches Währungssystem kollabiert meistens nur dann, wenn ein „schwacher“ Staat zwar viel Geld ausgibt, es aber nicht mehr über das Steuersystem einsammeln kann. Simbabwe und Venezuela sind dafür zwei Beispiele aus der jüngeren Geschichte. Eine Anekdote veranschaulicht den Zusammenhang sehr schön: Als die Engländer eine neue Kolonie eroberten, benötigten sie einheimische Arbeitskräfte. Sie boten Gold- und Silbermünzen sowie britische Pfund als Zahlung an, was die einheimische Bevölkerung jedoch ablehnte. Erst als die Engländer eine Kopfsteuer in einer neugeschaffenen Währung einführten, fanden sich Arbeitskräfte. Gleichzeitig entstanden sogar Märkte, sodass der Teil der Bevölkerung, der nicht für die Regierung arbeitete, die notwendigen Einnahmen zur Entrichtung der Steuer erwirtschaften konnte. Kryptowährungen dürften vor diesem Hintergrund keine echte Alternative zu staatlichem Geld sein, sondern eher vom Staat eingesetzt werden.

Kryptowährungen sind weit mehr als nur Bitcoins

Als erste Kryptowährung wurde Bitcoin 2009 ins Leben gerufen. Seitdem entstanden mehr als 1.500 Kryptowährungen, deren gesamte Marktkapitalisierung heute 332 Mrd. USD beträgt. Bitcoin dominiert 44 % des Markts. Jedoch gibt es einige starke Konkurrenten: beispielsweise den für intelligente Verträge besonderes geeigneten Ethereum (16 %) und dessen chinesische Version NEO (1,4 %), den von Finanzinstituten verwendeten Ripple (8 %), die Bitcoin-ähnliche Bitcoin Cash

¹ Quellen: William N. Goetzmann: Money Changes Everything; Sargent und Velde: The Big Problem of Small Change; Christine Desan: Making Money; David Graeber: Debt: The First 5,000 Years

(5 %), Litecoin (3 %) mit erhöhter Transaktionseffizienz, IOTA, die Kryptowährung für das Internet der Dinge (1,1 %), und den Monero (1,0 %) mit verstärkten Anonymitätsfeatures.

Blockchain-Technik ermöglicht direkte dezentrale Transaktionen

Das grundsätzliche Problem digitaler Währungen ist, dass ein Eigentümer seine digitale Währung theoretisch mehrfach ausgeben kann. Daher überwogen bisher zentrale Systeme wie Kreditkarten, bei denen alle Transaktionen über eine zentrale Stelle abgewickelt werden müssen, um deren Rechtmäßigkeit zu bestätigen. Die Blockchain ermöglicht nunmehr direkte dezentrale Transaktionen zwischen zwei Akteuren. Grundsätzlich gibt es bei auf Blockchain beruhenden digitalen Währungen wie Bitcoins zwei Gruppen von Akteuren: diejenigen, die die Transaktionen abwickeln, und diejenigen, die den Wahrheitsgehalt der Transaktion bestätigen und in die Blockchain eintragen, die sogenannten „Miners“. Als Belohnung für ihre Arbeit erhalten die Miners neue Bitcoins. In der Blockchain von Bitcoins wurde damals arbiträr festgelegt, dass nur insgesamt 21 Mio. Bitcoins entstehen können. Bisher gibt es etwa 16,9 Mio. Bitcoins. Nachdem alle 21 Mio. Bitcoins „geschürft“ worden sind, soll eine Transaktionsgebühr für die Miners als Belohnung eingeführt werden.

In die Blockchain werden Transaktionsdaten eingetragen, die zu Blöcken zusammengefügt werden und in einer kettenartigen Struktur miteinander verbunden sind. Man kann sich die Blöcke wie Seiten im Kontobuch vorstellen, die über fortlaufende Seitennummern verbunden sind. Es ist nahezu unmöglich, bereits bestehende Blöcke zu löschen oder deren Inhalt zu ändern, da gleichzeitig alle folgende Blöcke auch geändert werden müssten, was die Rechenkapazitäten der Computer eines Miners überfordern würde. Neue Blöcke werden der Blockchain durch das „Proof-of-Work“-Konsensverfahren hinzugefügt. Das Verfahren besteht aus zwei Schritten: Im ersten Schritt müssen alle Miners das gleiche Rechenpuzzle lösen, das mit steigender Zahl an Blöcken immer schwieriger wird. Der Miner, der als erstes das Rechenpuzzle löst, schickt seine Lösung an die anderen Miner, die mit einer Mehrheit von 50 % die Richtigkeit der Lösung bestätigen müssen. Die Mehrheit von über 50 % bezieht sich dabei nicht auf die Anzahl der Miner, sondern auf ihre Rechenkapazität. Die richtige Lösung des Rechenpuzzles bewirkt, dass automatisch die wahren Transaktionsdaten in der Blockchain eingetragen werden. Theoretisch könnte ein

Miner, der mehr als 50 % der Rechenkapazität besitzt, das Blockchain-System vollständig kontrollieren. Praktisch ist das jedoch eher unwahrscheinlich, da die Miner mit sehr hohen Investitionen in Rechenkapazität von einem anhaltend hohen Vertrauen in die Kryptowährung abhängig sind. Ein Betrug würde das Vertrauen zerstören und die Investitionen wertlos machen.

Bitcoin-Versprechen lassen sich nur schwer einlösen

Bitcoin verspricht Dezentralisierung und die damit verbundene Sicherheit, reduzierte Transaktionskosten und -zeit sowie Anonymität. Leider lassen sich diese Versprechen nur beschränkt einlösen.

Dezentralisierung ist das wichtigste Merkmal des Bitcoin-Zahlungssystems, bei dem keine zentrale Autorität mehr nötig ist. In der Theorie sollte eine Verteilung auf viele verschiedene Miner die damit verbundene Systemintegrität gewährleisten. In der Realität ist die geforderte Rechenleistung jedoch nur mittels kostspieliger Spezialhardware zu erreichen, sodass zunehmend Konzentrationsprozesse unter den Minern zu beobachten sind. Die Risiken einer unerwünschten Zentralisierung des Bitcoin-Zahlungssystems steigen somit. Darüber hinaus sollte das dezentrale Bitcoin-Zahlungssystem eigentlich Transaktionskosten und -zeit reduzieren. In der Realität kann jedoch das Bitcoin-Zahlungssystem nur etwa drei bis sieben Transaktionen in der Sekunde ausführen. Im Vergleich dazu können zentralisierte Zahlungsplattformen wie Visa etwa 1.700 Transaktionen pro Sekunde verarbeiten. Außerdem sind die Transaktionskosten des Bitcoin-Zahlungssystems sehr hoch, da es nur mithilfe einer sehr energieintensiven Spezialhardware möglich ist, am schnellsten das Rechenpuzzle zu lösen. Nach einer Schätzung von Digiconomist verbraucht das Bitcoin-Zahlungssystem derzeit etwa 32,56 TWh pro Jahr an Strom – und somit sogar mehr als ganz Dänemark mit 30,7 TWh pro Jahr.

Nicht zuletzt verspricht Bitcoin Anonymität im Gegensatz zu den auf nachweisbaren Identitäten basierenden zentralisierten Zahlungssystemen. Bitcoin-Transaktionen werden nur auf virtuelle Konten mit virtuellen Identitäten gebucht, bei denen die echten Identitäten der Inhaber weder gesammelt noch gespeichert werden. Trotzdem bietet Bitcoin nur begrenzten Datenschutz für die Kontoinhaber, da die Transaktionsdaten und die virtuellen Identitäten öffentlich und permanent verfügbar sind. Daher ist es möglich, die virtuellen Identitäten mit anderen Daten zu kombinieren, um so die echten

Identitäten der Bitcoin-Kontoinhaber zu ermitteln. Laut Prof. Sebastian Faust von der Universität Darmstadt nutzt zum Beispiel das FBI diese Methode, um Personen ausfindig zu machen, die illegale Transaktionen mit Kryptowährungen ausgeführt haben.

Ausblick: Auch künftig sind Kryptowährungen keine Alternative zu staatlichem Geld

Eine schleichende Zentralisierung, ein relativ gemächliches Transaktionstempo, ein hoher Energieverbrauch sowie Datenschutzlücken gehören zu den großen Herausforderungen für das Bitcoin-Zahlungssystem. Daher halten wir es für wahrscheinlich, dass es Bitcoins in einigen Jahren nicht mehr geben wird. Die Entwicklung wird jedoch weitergehen, und neue Kryptowährungen werden entstehen. Dabei sind noch viele technische Probleme zu lösen, weil oft Sicherheit, Transaktionsgeschwindigkeit und Anonymität im Widerspruch zueinander stehen.

Ein interessanter Weg zu mehr Sicherheit und höherer Transaktionsgeschwindigkeit ist die Änderung des Mehrheitswahlrechts. So gibt es erste Kryptowährungen, bei denen nicht mehr als 50 % der Rechenleistung eine Transaktion validieren, sondern die Besitzer von mehr als 50 % der ausstehenden digitalen Währung. Dahinter steht die – auch aus Spieltheorien bekannte –

Überzeugung, dass Miners mit einem hohen Anteil an der digitalen Währung einen starken Anreiz haben, die Integrität des Systems zu erhalten. Zusätzlich würde sich mithin die Transaktionsgeschwindigkeit merklich erhöhen und der Energieverbrauch reduzieren. Die Kryptowährung Ethereum hat bereits damit begonnen, das neue Wahlsystem sukzessive einzuführen.

Insgesamt dürften noch viele neue Kryptowährungen entstehen – und alte dürften wieder von der Bildfläche verschwinden. Sicherlich stehen wir da vor einer spannenden Entwicklung. Solange die Staaten aber stark genug bleiben, um ausreichend Steuern zu erheben und ihre Verschuldung in Grenzen zu halten, dürften private Kryptowährungen nicht das staatliche Geld ersetzen. Staatliches Kryptogeld könnte in Zukunft sogar ein Mechanismus werden, um zum Vollgeldstandard überzugehen. Die Zentralbank würde in diesem Fall eine jährliche Wachstumsrate der Kryptogeldmenge festlegen und damit die Geldproduktion wieder vollständig übernehmen. Die Banken würden im Gegensatz dazu ihre Funktion als Geldproduzenten verlieren und nicht mehr exzessiv Kredite vergeben können, was ihre Krisenanfälligkeit reduzieren könnte.

Edgar Walk
Chefvolkswirt Metzler Asset Management

Metzler Asset Management

Metzler Asset Management GmbH
Untermainanlage 1
60329 Frankfurt am Main
Telefon (0 69) 21 04 - 5 32
Telefax (0 69) 21 04 - 11 79
asset_management@metzler.com
www.metzler-fonds.com

Rechtliche Hinweise

Diese Unterlage der Metzler Asset Management GmbH (nachfolgend zusammen mit den verbundenen Unternehmen im Sinne von §§ 15 ff. AktG „Metzler“ genannt) enthält Informationen, die aus öffentlichen Quellen stammen, die wir für verlässlich halten. Metzler übernimmt jedoch keine Garantie für die Richtigkeit oder Vollständigkeit dieser Informationen. Metzler behält sich unangekündigte Änderungen der in dieser Unterlage zum Ausdruck gebrachten Meinungen, Vorhersagen, Schätzungen und Prognosen vor und unterliegt keiner Verpflichtung, diese Unterlage zu aktualisieren oder den Empfänger in anderer Weise zu informieren, falls sich eine dieser Aussagen verändert hat oder unrichtig, unvollständig oder irreführend wird.

Ohne vorherige schriftliche Zustimmung von Metzler darf/dürfen diese Unterlage, davon gefertigte Kopien oder Teile davon nicht verändert, kopiert, vervielfältigt oder verteilt werden. Mit der Entgegennahme dieser Unterlage erklärt sich der Empfänger mit den vorangegangenen Bestimmungen einverstanden.