Bitcoin – Zahlungsmittel der Zukunft?

Florian Tropper

Leoben, 16.12.2020

Der Bitcoin-Euro-Kurs ist so hoch wie noch nie zuvor. Private Anleger, Firmen und Banken investieren zunehmend in die Kryptowährung Bitcoin. Aktienfonds nehmen Bitcoins in ihr Pool an Wertanlagen auf, sogenannte Miner lukrieren Bitcoins durch das Bereitstellen von Rechenzentren. Kurz: Der Bitcoin boomt. Aber was hat es mit diesen Bitcoins auf sich? Reichen uns Euro, Dollar, Rubel und Yuan noch nicht? Ein kleiner Überblick soll im Folgenden die grundlegendsten Einblicke geben.

1. Währung im Wandel der Zeit

Historisch gesehen hat das Geld ein paar Entwicklungsstufen durchlaufen, wobei diese parallel verwendet wurden und je nach Geografie noch werden. Im Anfang stand der Tauschhandel: Ein Schaf wurde beispielsweise gegen drei Säcke Reis eingetauscht und jeder hat seine eigenen Güter verwaltet. Aber bereits in der Frühgeschichte der Menschheit wurden schöne oder schmucke Naturalien als Primitivgeld verwendet. In küstennahen Gebieten waren dies oft Muscheln, während im Landesinneren u.a. Knochen als Gegenleistung für diverse Sachgüter oder Nahrungsmittel herhielten. Dieses Primitivgeld war alles andere als einheitlich. Je nach Vorkommen war eine Muschel größer oder kleiner, flacher oder bauchiger. Erst mit der Einführung des Münzgeldes kam es zu einer Normierung des Geldes. Die ältesten Metallmünzen wurden im Mittelmeerraum gefunden und dürften um 2000 v.Chr. gefertigt worden sein. Währung in Form von Münzen hat einen materiellen Wert, denn die Geldstücke bestehen meist aus Edelmetallen wie Kupfer, Gold oder historisch später auch Silber. Das änderte sich mit der Einführung des Papiergeldes, das bereits im 11. Jahrhundert in China während der Song-Dynastie erfunden wurde. Hierbei handelt es sich um sogenanntes Fiatgeld. Das lateinische «fiat» heißt übersetzt «es geschehe» und steht dafür, dass der Wert dem Papier beigemessen werden soll, der darauf abgebildet ist. Fiatgeld ist daher ein Objekt ohne inneren Wert, das als Tauschmittel dient. Die weitere Abstraktion erfolgte im letzten Jahrhundert durch die elektronische Speicherung und Übertragung von Zahlenwerten: Man spricht vom elektronischen Geld, das sich in Formen wie Online-Banking und Kartenzahlung manifestiert.

2. Anfang des Bitcoin-Konzeptes

Eine grundlegende Eigenschaft unseres bisherigen sowie aktuellen Finanzsystems ist, dass es auf Vertrauen basiert. Wenn Identität A einer Gegenpartei B Geld zukommen lässt, geschieht das durch eine Transaktion über eine Institution, der man vertrauen muss, dass sie das geschickte Geld verlässlich an B weiterleitet. Diese Institution ist im Allgemeinen eine Bank. Die Transaktion findet dabei unter Ausschluss der Öffentlichkeit statt (Traditionelles Privatsphäre Modell in Abb. 1).

Im Laufe der Finanzkrise 2008/09 sank das Vertrauen in das Banksystem, sodass alternative Konzepte diskutiert wurden, die eine Unabhängigkeit von solchen Institutionen anstrebten. Eine Antwort auf diese öffentliche Diskussion war das Ende 2008 unter dem Pseudonym Satoshi Nakamoto veröffentlichte White Paper «Bitcoin: A Peer-to-Peer Electronic Cash System». Die Frage nach dem

tatsächlichen Urheber dieses Papers ist bis heute ungeklärt. Darin wird erstmals ein Konzept erklärt, das ein neues Privatsphäre-Modell vorsieht und die Funktionsweise einer sogenannten Kryptowährung erklärt, mit welcher sich dieses System umsetzen lässt. Im Gegensatz zum herkömmlichen Finanzsystem, welches Währung durch zentrale Einheiten verwaltet und sendet, basiert das System der Kryptowährung auf einem dezentral organisierten Netzwerk. Hierbei kennen sich die Identitäten untereinander nicht, alle Transaktionen sind hingegen von jedem öffentlich einsehbar und überprüfbar. Keine Transaktion kann einer Identität zugeordnet werden (Neues Privatsphäre Model in Abb. 1).

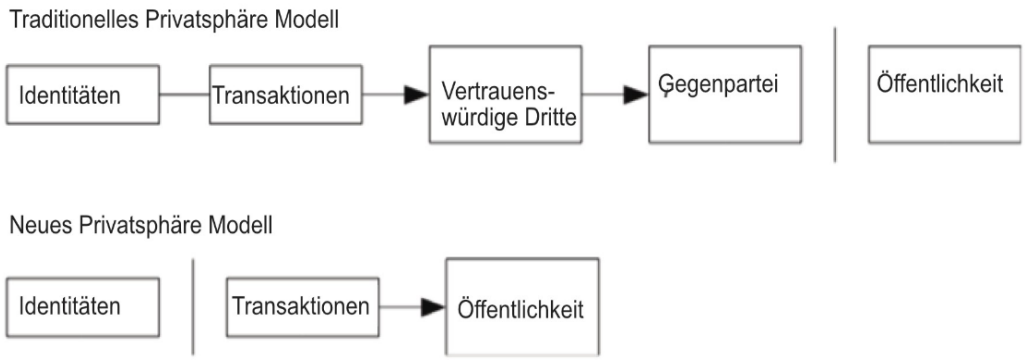

Abb. 1: Vergleich der Privatsphäre Modelle im Finanzsystem

Die ersten Bitcoins wurden Anfang 2009 vermutlich durch den Urheber selbst in Umlauf gebracht und zu Beginn wie Spielgeld mit geringstem Wert geschaffen und gehandelt.

3. Bezahlen mit Bitcoin

Bitcoins werden in einer digitalen Geldbörse («Wallet») aufbewahrt, indem sie in einer Applikation lokal auf einem Gerät (Smartphone, PC) gespeichert sind. Geht das Gerät verloren, sind auch die Bitcoins weg. An speziellen Automaten lassen sich Euro in Bitcoin umtauschen und in die Wallet laden. Möchte man jemanden mit Bitcoin bezahlen, so benötigen Sender sowie Empfänger jeweils eine Wallet. Der Sender benötigt die Adresse des Empfängers (Kette aus alphanumerischen Zeichen), um diesem Bitcoin zu schicken. Er signiert die Transaktion mit einem persönlichen Passwort (= privaten Schlüssel) und gibt den Transfer in Auftrag. Nachdem die Nachricht verschlüsselt, versendet, entschlüsselt und verifiziert worden ist, wird der entsprechende Betrag beim Sender abgebucht und dem Empfänger gutgeschrieben. Jede Transaktion wird dabei auch mit einem Zeitstempel versehen, um die Transaktionen in der richtigen Reihenfolge auszuführen. Hiermit wird verhindert, dass von einem Konto mehr abgebucht wird, als verfügbar ist.

Eine Zahlungsadresse wird im Gegensatz zu einem IBAN in der Regel nur einmal verwendet. Adressen können auch mehrmals verwendet werden; davon wird aber abgeraten, damit keine Rückschlüsse auf den physikalischen Besitzer der Adresse gemacht werden können. Bezahlungen mit Kryptowährungen sind daher anonym, solange keine persönlichen Daten bei einer Transaktion bekanntgegeben werden.

4. Blockchain

Um die korrekte Abhandlung aller Transaktionen ohne vertrauenswürdige Dritte zu gewährleisten, übernimmt die Öffentlichkeit die Kontrollfunktion. Hierfür werden alle Transaktionen veröffentlicht. Grund ist, dass nur so der Zahlungsempfänger (und auch alle anderen) verifizieren kann, dass der vorhergehende Besitzer die Bitcoins nicht doppelt ausgegeben hat. Außerdem besteht die einzige Möglichkeit, das Fehlen einer Transaktion zu bestätigen, darin, alle Transaktionen zu kennen. Die Veröffentlichung erfolgt in einer sogenannten Blockchain, die eine chronologische Liste aller bisherigen Transaktionen darstellt. Diese Blockchain wird durch jede erfolgreiche Transaktion um ein paar Daten erweitert (Sender- und Empfängernummer, Zeitstempel etc.) und wächst somit ständig. Dabei werden mehrere Transaktionen in verschlüsselte Datenschnipsel zerlegt und finden als Hash Eingang in einen Block. Das Aneinanderreihen dieser Blocks führt zur Bildung der Blockchain, die somit ein Kassenbuch mit perfekter Nachvollziehbarkeit aller Transferleistungen darstellt.

5. Mining

Nicht nur der Datentransfer, sondern vielmehr die Verschlüsselung und Entschlüsselung der Daten, benötigt große Mengen an Rechenleistung. Das System ist dergestalt konzipiert, dass jeder Computer mit Internetzugang einen Teil seiner Rechenkapazität in Form einer im Hintergrund laufenden Anwendung zur Verfügung stellen kann. Anreiz hierfür ist die Vergabe von Bitcoin – quasi als Entlohnung für die Bereitstellung der Rechenleistung. Bitcoin werden dabei in festgelegten Zeitintervallen je nach zur Verfügung gestellter Rechenleistung für die Computerbetreiber ausgeschüttet. Analog zum Goldschürfen wurde diese Art der Generation von Bitcoin als Schürfen oder Mining bezeichnet. Durch dieses System hat sich in der letzten Dekade erwartungsgemäß ein dezentrales Netzwerk privater Rechner etabliert, die die Gesamtheit der anfallenden Rechenprozesse abhandelt. Während anfangs noch einfache PCs am Mining beteiligt waren, kommen heutzutage bereits riesige Datenzentren zum Einsatz. Mit dem eigenen Laptop lässt sich dadurch kaum mehr rentables Mining betreiben. Eine solche Recheneinheit (ganz gleich ob großes Datenzentrum oder einfacher Laptop) werden als Knoten in dem Netzwerk aller beteiligten Rechner bezeichnet.

6. Ablauf einer Transaktion

Nachdem ein Sender den Auftrag gegeben hat, wird die neue Transaktion an alle Knoten gesendet. Jeder Knoten sammelt neue Transaktionen in einem Block. Dabei müssen nicht notwendigerweise alle Knoten des Netzwerks erreicht werden. Solange die Übertragungsdaten viele Knoten erreichen, geraten sie in Kürze in einen Block. Block-Sendungen sind auch tolerant gegenüber gelöschten Nachrichten. Wenn ein Knoten keinen Block empfängt, wird er ihn anfordern, wenn er den nächsten Block empfängt und erkennt, dass er einen verpasst hat.

Jeder Knoten arbeitet daran, einen kryptografischen Beweis der Gültigkeit für den Block zu finden und sendet, nachdem er das geschafft hat, den Block an alle Knoten. Diese akzeptieren den Block nur dann, wenn alle darin enthaltenen Transaktionen gültig und nicht bereits verbraucht sind, was durch Zeitstempel und frühere Daten aus der Blockchain hervorgeht. Schließlich hängen die Knoten den neuen Block an die Blockchain.

Knoten halten immer die längste Kette für die richtige und arbeiten weiter daran, sie zu verlängern. Wenn zwei Knoten nun gleichzeitig verschiedene Versionen des nächsten Blocks senden, können einige Knoten das eine oder das andere zuerst empfangen. In diesem Fall arbeiten sie an der ersten, die sie erhalten haben, aber speichern die andere Verzweigung für den Fall, dass sie länger wird. Die

Verbindung wird unterbrochen, wenn der nächste kryptografische Beweis von einem Knoten gefunden wird und ein Zweig länger wird. Die Knoten, die an dem anderen Zweig arbeiteten, werden dann zu dem längeren Zweig wechseln.

7. Sicherheit gegen Cyber-Angriff

Stabilität erlangt das Netzwerk über das auf die Rechenknoten verteilte Konsens-System: Es erzwingt eine chronologische Reihenfolge der Blockchain und sorgt dafür, dass sich die verschiedenen Computer über den Status des Systems einig sind. Kryptografische Regeln, die von der Mehrheit der Netzknoten akzeptiert werden müssen, verhindern, dass vorangegangene Blöcke modifiziert werden können: Eine Änderung würde nämlich alle darauffolgenden Blöcke ungültig machen. Auf diese Weise kann kein Einzelknoten kontrollieren, was in die Blockchain aufgenommen wird. Ebenso können Teile der Blockchain nicht so modifiziert werden, dass eigene Ausgaben rückgängig gemacht werden.

Um einen vergangenen Block zu fälschen, müsste ein Angreifer den kryptografischen Beweis des Blocks und aller Blöcke danach wiederholen und dann die Arbeit der vertrauenswürdigen Knoten einholen und überholen. Es müsste hierfür mehr als die Hälfte aller Knoten gehackt werden, um die nötige Rechenleistung aufzubringen, was praktisch so gut wie unmöglich ist. Das vorgestellte System ist daher sicher, solange vertrauenswürdige Knoten gemeinsam mehr CPU-Prozessorleistung steuern als kooperierende Gruppen von böswilligen Knoten.
Hinzu kommt, dass sich mit Mining in so einem Fall einfacher und dazu ehrlich Geld verdienen lässt, was das System intrinsisch vor solch groß angelegten Cyberattacken schützt.

8. Zahlen, Daten, Fakten

- Die Blockchain umfasst derzeit 660.000 Blöcke und eine gesamte Datengröße von 340 GB.
- Die aktuelle Anzahl an Bitcoins im Umlauf beträgt 18 Mio.
- Alle 10 min werden neue Bitcoins ausgeschüttet (aktuell: 900/Tag).
- Weltweite Rechenleistung für Bitcoin pro Jahr …
  - 2018: 42 TWh, entsprach dem jährlichen Energieverbrauch von ganz Dänemark
  - Heute: ~ 70 TWh
- Anzahl an verschiedenen Kryptowährungen: > 4000
- Bitcoin Besitzer in der EU: 5% der Bevölkerung. In den USA: 11% der Bevölkerung.
- 1 Bitcoin = 100 Mio. Satoshi
- Die Transaktionsdauer liegt durchschnittlich bei 10 Minuten.

Quellen

1) Satoshi Nakamoto (2008): Bitcoin: A Peer-to-Peer Electronic Cash System
2) https://bitcoin.org/de/
3) https://www.blockchain.com/de/chartsed
4) https://de.statista.com/themen/2087/bitcoin/
5) https://www.youtube.com/watch?v=yz8ymvqUMrU
6) https://www.finanzfluss.de/geldanlage/bitcoin/