Ein Schwarm fleissiger Bienen

Ein Schwarm fleissiger Bienen

Wie Blockchain funktioniert. Eine Einführung.

von Benno Luthiger

Die Technologie der Blockchain ist Grundlage für Währungssysteme wie Bitcoin. Schon jetzt pflügt diese Technologie die Finanzwelt um. Dabei kann sie weit mehr. Wenn die Blockchain Alternativen zu Dienstleistungen wie etwa dem Grundbuchregister schafft, wird sie auch Staatswesen als solche verändern.

Als Bürger sollte man spätestens jetzt versuchen, die Blockchain zu verstehen. Dies ist das Ziel dieses Artikels. Er ist bewusst technisch anspruchsvoller als die Artikel, die über Bitcoin und Blockchain üblicherweise zu lesen sind. Ich gehe davon aus, dass die Leserschaft des «Schweizer Monats» ein Interesse an einem tieferen Verständnis dieser Technologie hat und bereit ist, sich in die Tiefen dieser Technologie zu begeben.

Benno Luthiger
ist Physiker und Ethnologe und hat an der Universität Zürich in Ökonomie promoviert. Er arbeitet als Softwareingenieur an der ETH Zürich und ist seit Jahren aktiv in der Politik, zuerst bei der SP, heute bei den Piraten.

Am Anfang steht das Kassenbuch

Beginnen wir mit einem einfachen Bezahlvorgang. Ich kaufe in einem Laden etwas Gemüse und Obst für 10 Franken, die ich aus meinem Portemonnaie nehme und der Person an der Kasse gebe. Wenn ich den Laden verlassen habe, ist mein Portemonnaie etwas leichter und die Kasse im Geschäft etwas voller. Betrachtet man den wirtschaftlichen Austausch als eine Art Kassenbuch, kann man sagen: mein Kontostand ist um 10 Franken gesunken, während im gleichen Moment der Kontostand des Ladens um 10 Franken gestiegen ist.

In einer modernen Welt mit digitaler Technik können wir diesen alltäglichen Vorgang vereinfachen. Statt das Geld wirklich in die Hand zu nehmen, zu übergeben, zu transportieren und schliesslich zu verbuchen, könnten wir auch schlicht festhalten, dass ich jetzt 10 Franken weniger und der Laden ebenso viel mehr auf dem Konto hat. So wie eine Bezahlung mit Bankkarte – nur eben viel schneller und günstiger.

Dazu müssen wir uns darauf einigen, die Führung unserer Konti an eine Instanz auszulagern, der wir gemeinsam Vertrauen schenken. Diese Instanz war bislang üblicherweise eine Geschäftsbank. Auch andere Vermittler wie das einstige eBay-Tochterunternehmen und heute unabhängige PayPal bieten an, diese Rolle zu übernehmen. Je mehr Personen sich einem dieser Intermediäre anschliessen, desto einfacher wird die Überweisung von Geld. Wir müssen uns dann nicht mehr darüber verständigen, über welchen Intermediär wir die Bezahlung abwickeln. Gleichzeitig erhält natürlich der abwickelnde Vermittler eine immer mächtigere Position.

Jedenfalls: Grundlage für ein digitalisiertes Geldsystem muss ein vertrauenswürdiges, transparentes Kassenbuch sein. Transparent bedeutet, dass sämtliche Buchungen für alle Beteiligten nachvollziehbar sind. Die Kontostände müssen zuverlässig alle Transaktionen abbilden, aber eben nur diese Transaktionen. Keinesfalls dürfen die Kontostände durch irgendwelche Manipulationen verändert werden können. Die erstaunliche Innovation der Blockchain besteht nun darin, dass diese Technologie ein für alle transparentes Kassenbuch schafft, ohne dass es zu dessen Führung und Kontrolle eine zentrale Instanz bräuchte. Stattdessen funktioniert das Kassenbuch eben dezentral: Transaktionen werden gleichzeitig auf ungezählten Rechnern rund um den Globus festgehalten; ein Angriff auf nur einzelne von ihnen vermag das System nicht zu erschüttern. Wie funktioniert das genau? Wie kann der Kassenstand von zahllosen Personen auf ebenso zahllosen Rechnern synchron gehalten werden?

Jeder Rechner schreibt mit

Man kann sich die Blockkette vorstellen als eine Aneinanderreihung von Seiten eines Kassenbuches. Jeder sogenannte Block entspricht einer Seite im Kassenbuch, der die Transaktionen der letzten 10 Minuten festhält. Er enthält eine innere Struktur, nämlich – in der Sprache der Informatik – einen Kopf und einen Körper. Der Kopf enthält neben anderen Angaben einen Verweis auf den Vorgängerblock und Informationen, auf die ein Nachfolger verweisen kann; er knüpft also sozusagen die Kette weiter. Im Körper werden die detaillierten Transaktionen notiert. So entsteht eine potenziell unendliche Kette von Seiten, die immer nur dadurch funktionieren, dass sie an einen legitimen Vorgänger an-

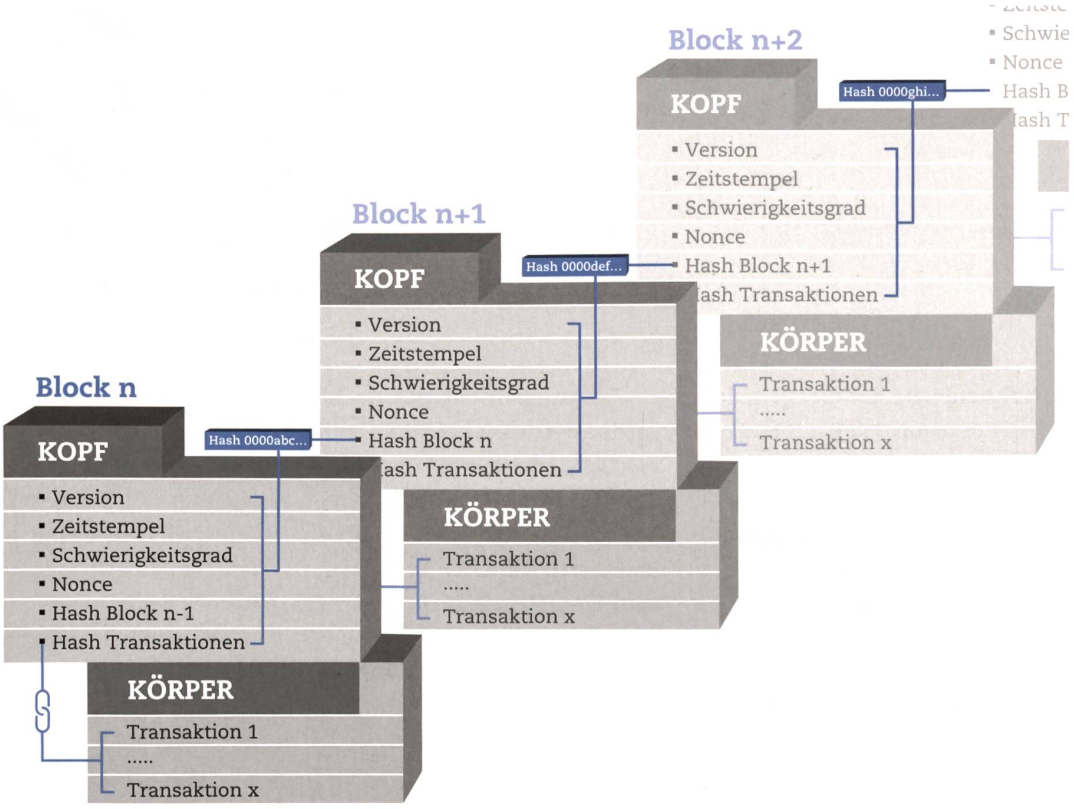

Abbildung
Die Blockkette

Jeder Block besteht aus einem Körper (dieser hat die Transaktionen registriert) und einem Kopf.

Dieser Kopf enthält sechs Werte, nämlich die Versionsangabe (der vom Miner verwendeten Software), den Link zum vorherigen Block in Form eines Hashs, einen Vermerk zu den im Block enthaltenen Transaktionen, einen Zeitstempel, eine Angabe zum Schwierigkeitsgrad des Blocks (der Befehl zur Anzahl Nullen) sowie eine Zeichenkette, die *Nonce* genannt wird.

Diese sechs Werte werden mit einem Prozess, der *Proof-of-Work* genannt wird, zusammengefügt und zu einem Hash-Wert umgewandelt. Dieser Hash wird wiederum in den Kopf des nächsten Blocks aufgenommen.

gedockt sind. Von jedem beliebigen Block aus kann entsprechend das ganze Kassenbuch bis zurück zum Anfang rekonstruiert werden. Konrad Hummler spricht von einer lückenlosen und nicht veränderbaren Historie. Die Beteiligten können sich darauf verlassen, dass ihre Guthaben sicher registriert sind.

Technisch funktioniert das Notieren so, dass zahlreiche ans Internet angeschlossene Rechner – das können Rechner von Privatpersonen ebenso wie solche von Unternehmen sein – die Stützen oder sogenannten Knoten des Netzwerks bilden. Wenn ich nun mein Gemüse mit Bitcoin statt mit Franken bezahle, wird von meinem Rechner oder Smartphone aus eine Meldung über die

«Jeder Block entspricht einer Seite im Kassenbuch.»

Benno Luthiger

Transaktion an einige am Netzwerk beteiligte Rechner geschickt. In dieser Meldung steht, dass mein Konto um den Kaufbetrag gesenkt und das Konto des Gegenübers um den gleichen Betrag erhöht werden soll. Die Rechner – die ja alle ständig über alle Informationen verfügen – prüfen die Anfrage, also beispielsweise meinen Kontostand. Wird die Transaktion zugelassen, wird sie in Windeseile wie eine Welle bei allen Rechnern des Netzwerks registriert. Jeder Rechner im Netzwerk kann und muss also Transaktionen registrieren, prüfen und melden. Das ist genau die dezentrale Funktionsweise des Systems: die Integrität der Buchungen wird von allen gemeinsam geprüft und bestätigt.

Die Blöcke, von denen wie erwähnt alle 10 Minuten ein neuer erstellt wird, werden von zurzeit schätzungsweise 10 000 speziell damit beauftragten Rechnern erstellt. Sobald mein Gemüsekauf vom Netzwerk geprüft, gutgeheissen und schliesslich gemeinsam mit anderen Transaktionen in einem neuen Block registriert wurde, sind ab diesem Zeitpunkt mein neuer Kontostand und der meines Geschäftspartners festgehalten und können als Grundlage der nächsten Aktionen dienen. Damit ist sichergestellt, dass ich den entsprechenden Betrag nicht noch einmal ausgeben kann. Auf diese Weise werden die Bitcoin-Transaktionen fälschungssicher.

Nun stellt sich natürlich, wie Sie, liebe Leserin, lieber Leser, zu Recht bemerken, eine grosse Frage. Wenn unsere eigenen Geräte ja oft schon an der Synchronisation unseres Bürokalenders mit dem Smartphone scheitern – wie schafft es ein solch riesiges Netzwerk, all diese gleichzeitig und überall auf der Welt erstellten Informationen zu synchronisieren, ohne einen Fehler zu machen?

Die Antwort darauf ist sehr einfach: Das Netzwerk muss so gebaut sein, dass zwar die Meldung der einzelnen Transaktionen möglichst gleichzeitig, die Erstellung neuer Blöcke hingegen in einer geordneten zeitlichen Abfolge stattfindet. Alle Knoten im Netzwerk müssen sich darüber verständigen, dass es nur eine Blockkette gibt, und sie müssen das autonom entscheiden können. Zu diesem Zweck gibt es ein einfaches Kriterium: Nur die längste Blockkette ist gültig und ein neuer Block muss an den letzten Block der gültigen Kette anschliessen. Wie wird nun ein neuer Block erzeugt? Hier kommt das viel zitierte «Mining» ins Spiel, und wenn Sie das verstanden haben, dann haben Sie die Blockchain verstanden.

Bitcoin-Mining

Als erstes ist zu vermerken, dass hinter den Knoten nicht Menschen stehen, die zum Wohl des Bitcoin-Netzwerks ihren Computer eigenhändig an das Stromnetz und das Internet anschliessen und aufspringen, wenn irgendwo eine Lampe leuchtet. Der Vorgang, einen neuen Block anzulegen und dort die jüngsten Transaktionen festzuhalten, ist zu wichtig, als dass man diesen Prozess dem Edelmut einiger Leute überlassen könnte. Stattdessen kassieren die Wildbienen – also jene rund 10 000 Rechner, die neue Blöcke erstellen – für das Erstellen eines gültigen Blocks eine Prämie von aktuell 25 Bitcoins. Dies entspricht beim derzeitigen Tauschkurs mehr als 15 000 Franken (Stand: 21.06.2016, 11:00 Uhr). Das ist gleichzeitig auch der einzige Weg, wie überhaupt neue Bitcoins geschaffen und in den Kreislauf eingespeist werden

– schliesslich gibt es in diesem System keine Notenbank, die Geld druckt. Aus diesem Grund wird diese Tätigkeit Mining genannt, in Anlehnung an das Gewinnen von Rohstoffen aus der Erdkruste. Jedenfalls ist festzuhalten: die Bienen haben einen Anreiz, neue Blöcke zu schaffen.

Nun also zum Ablauf, wie das geht. Jeder Block hat wie erwähnt einen Kopf. Darin enthalten sind jeweils sechs Informationen (unter anderem der Zeitstempel der Erstellung und das Fazit aller darin festgehaltenen Transaktionen). Diese Informationen werden verrechnet zu einem Wert, dem sogenannten Hash, und weitergegeben an den nächsten Kopf, wo er wiederum zu einer der sechs Informationen wird. So weit, so einfach. Die Blockchain bewegt sich fort wie Dominosteine.

Etwas kompliziert wird es bei der Entscheidung, wer den neuen Block schreiben und den Gewinn kassieren darf. Die 10 000 Kandidaten müssen nämlich eine «schwierige Rechenaufgabe» lösen, wie es in den Medien jeweils heisst. Konkret funktioniert das so: die sechs Informationen des künftigen Kopfes müssen verrechnet einen künftigen Hash ergeben. Der Hash ist eine Zeichenkette, welche 64 Zeichen enthält, wobei eine bestimmte Anzahl der Zeichen am Anfang Nullen sein müssen. Diese Zeichenkette mit ihrer speziellen Form wird Proof-of-Work genannt. Dabei ist die Anzahl der Nullen so gewählt, dass mit der gesamten Rechenleistung des Netzwerks im Schnitt nur alle 10 Minuten ein solcher Hash berechnet werden kann.

Das ist grob vergleichbar mit einer Addition, wie sie alle aus der Schule kennen: ein bestimmtes Ergebnis ist gewünscht, nun sind die Inputs so zu wählen, dass ebendieses herauskommt. Im vorliegenden Fall sind fünf der sechs Informationen vorgegeben. Nur eine Zeichenkette, Nonce genannt, kann frei gewählt werden. Bei einer Addition würden Sie den freien Summanden berechnen, indem Sie die Differenz zur gewünschten Summe bestimmen. Bei einem Hash ist das nicht möglich. Bei einer Hashfunktion lässt der berechnete Hashwert keinerlei Aussagen über den Input zu. Da hilft nur eines: der frei wählbare Teil des Inputs muss so lange variiert werden, bis der errechnete Hash die gewünschte Form hat. Sobald einer der Knoten im Netz mit seinem Input eine gültige Kombination, das Proof-of-Work, berechnet hat, werden diese Informationen zum neuen Block im Netzwerk verteilt. Dann rasten alle Rädchen ein und sein Block wird befestigt. Damit sind auch die neusten Transaktionen für immer in der Kette verankert.

Schwindler scheitern an der Kette

Wenn sie richtig funktioniert, schafft die Blockchain als dezentrales System Glaubwürdigkeit, Verlässlichkeit und Stabilität. Wie wir gesehen haben, enthält jeder Blockkopf den Hash des vorherigen Blockkopfs und dieser den Hash seines Vorgängers und so weiter. Auf diese Weise ist in der Blockkette das Bitcoin-Kassenbuch zurück bis zum ersten Block abgebildet. Würde ein Schwindler versuchen, einen einzigen Wert in einer Transaktion in der Blockkette zu seinen Gunsten zu verändern, so würde das den Hashwert dieses Blocks verändern und somit auch die Werte aller Köpfe, die auf den veränderten Block folgen. Er würde unmittelbar auffliegen.

Stellen wir uns weiter vor, eine Person ändere ihre Meinung und wolle einen Bitcoin, den sie eben ausgegeben hat, doch wieder zurückhaben. Diese Person müsste die Geschichte in der Blockkette so umschreiben, dass der Bitcoin in ihrer Tasche bleibt. Sie könnte nun den Rechner anwerfen und versuchen, eine neue Version des Blocks zu erzeugen, welcher die Transaktion ihres Bitcoins registriert hat. Nach genügend langer Zeit wird es ihr gelingen, einen solchen Block mit korrektem Proof-of-Work zu erzeugen. Das Bitcoin-Netzwerk wird ihren Block allerdings nicht akzeptieren. In der Zwischenzeit ist die ursprüngliche Blockkette gewachsen, und weil neue Blöcke nur an die längste Blockkette angehängt werden, passt der manipulierte Block nicht mehr.

Wenn die Regeln transparent und die Anreize richtig gesetzt sind, wird ein dezentrales System umso stabiler, je weiter verzweigt es ist. Die Glaubwürdigkeit liegt in den Regeln begründet und nicht im Ruf der Institution, beispielsweise einer Notenbank. Ein dezentrales System arbeitet idealerweise auch dann noch stabil, wenn die Betreiber einiger Knoten versuchen, zu schwindeln. Wenn hingegen eine zentrale Institution wie die Notenbank unter Druck der Politik kommt und aus diesem Grund die Glaubwürdigkeit verliert, ist schlagartig die Stabilität des ganzen Systems bedroht.

Und jetzt?

Die Technologie der Blockkette ist bislang am bekanntesten geworden als das Rückgrat von Bitcoin. Zu Bitcoin gibt es allerlei durchaus legitime Kritik, beispielsweise an der Tatsache, dass die maximale Anzahl Bitcoins auf 21 Millionen festgelegt ist. Das wird sichergestellt, indem die für einen neuen Block ausbezahlte Prämie alle vier Jahre halbiert wird. Beim Start der Blockkette 2009 betrug sie 50 Bitcoins, seit 2013 sind es 25 Bitcoins. Entsprechend bemängeln Kritiker unter anderem, dass das Geldmengenwachstum nicht an das Wachstum einer Volkswirtschaft angepasst werden kann. Solche Einwände sind bedenkenswert.

Wichtig aber ist: die Blockchain hat eine Existenzberechtigung ganz unabhängig von Bitcoin. Beispielsweise gibt es Überlegungen, die Blockkette als Grundlage für Immobilienverträge zu verwenden, also als Grundbuchersatz. Damit könnten speziell in Ländern mit schwachen staatlichen Institutionen die Eigentumsrechte vieler Leute vor Manipulationen geschützt werden. Es ist selbstverständlich nicht vorherzusehen, in welche Richtung sich die Möglichkeiten der Blockchain entwickeln werden. Weiter begleiten wird sie uns aber ganz bestimmt, und es lohnt sich, sie zu verstehen zu versuchen. Ich hoffe, ich konnte dazu einen Beitrag leisten. ‹

Literatur:
Konrad Hummler: «Blockchain – der nächste Wohlstandsschock», NZZ vom 3.5.2016.
The Economist, 2015: «The Great Chain of Being Sure about Things».