BitCoin – ein geniales oder ein katastrophales Zahlungssystem?

Das Ziel: Ein sicheres weltweites System zur Abwicklung von billigen Geldüberweisungen ohne vertrauenswürdige Vermittler (Banken). Dabei soll die Buchhaltung öffentlich einsehbar sein, aber trotzdem die Anonymität der beteiligten Personen gewährleisten. Das System soll sich selbst organisieren und das begleitende Überwachungsinstitut soll keine Eingriffsmöglichkeiten in die Transaktionen haben. BitCoin und andere Kryptowährungen erreichen dieses Ziel auf ähnliche Weise. Der Artikel zeigt, wie BitCoin dies tut und zu welchem Preis.

Am 31. Oktober 2008 hat eine japanische Arbeitsgruppe unter dem Pseudonym Satoshi Nakamoto einen kurzen Artikel veröffentlicht (Nakamoto 2008). Darin wird dargelegt, wie ein bankenloses, sich selbst organisierendes Zahlungssystem funktionieren kann, dessen Buchhaltung transparent, öffentlich einsehbar und trotzdem anonym, unzerstörbar und fälschungssicher ist.

Die BitCoin Blockchain

Eine Blockchain ist eine nach bestimmten Regeln aufgebaute Datei. Ihr Bauplan unterscheidet sich von demjenigen von Textdateien, Bilddateien oder Videodateien, indem eine Blockchain-Datei aus einer Kette von zusammenhängenden Blöcken besteht – daher der Name Blockchain oder auf Deutsch Blockkette.

Die BitCoin-Blockchain kann wie andere Dateien auf jeden Computer heruntergeladen werden, sofern gegen 500 Gigabyte freier Speicher zur Verfügung steht. Auf diese Grösse ist die BitCoin-Blockchain seit der Erzeugung ihres ersten Blocks am 9. Januar 2009 gewachsen. Durchschnittlich wird alle 10 Minuten ein Datenblock angefügt, der alle in dieser Zeit mit BitCoin durchgeführten Zahlungen (Überweisungen, Transaktionen) enthält.

Mitte Januar 2023 enthielt ein neuer Block im Mittel jeweils 1700 Transaktionen; ein mittelgrosser Block war dementsprechend 850 000 Byte lang (ein Byte besteht aus 8 Bit; der Leadtext dieses Artikels ist beispielsweise 536 Byte lang). Die Blockchain umfasste zu diesem Zeitpunkt rund 770 000 Blöcke.

Diese stetig wachsende Datei ist die öffentlich einsehbare (unverschlüsselte) Buchhaltung über die gesamte Lebensdauer des BitCoin.

Drei grundsätzliche Forderungen

Die Blockchain muss drei Forderungen erfüllen, damit das oben formulierte Ziel eines anonymen, billigen und vertrauenswürdigen Zahlungssytems erreicht werden kann: Sie muss (a) die Anonymität der an den Transaktionen beteiligten Personen sicherstellen, (b) nachträgliche Manipulationen müssen sofort festgestellt werden können und (c) es sollte unmöglich sein, eine korrekte, aber gefälschte Fake-Blockchain innert nützlicher Frist herzustellen, welche die authentische Blockchain ersetzen könnte. Für alle drei Anforderungen spielt das im nächsten Abschnitt vorgestellte Gütesiegel eine zentrale Rolle. Die drei Forderungen werden folgendermassen erfüllt:

a) Anonymität: Alle Transaktionen werden über anonyme Nummernkonti abgewickelt, wobei die Kontonummer aus den Personendaten, dem Eröffnungszeitpunkt des Kontos (dem sog. «Wallet») und weiteren Angaben automatisch als Gütesiegel gebildet wird. Auf diesen Punkt wird hier nicht mehr weiter eingegangen.

b) Manipulationssicherheit: Gütesiegel halten die aufeinanderfolgenden Blöcke zusammen. Sie garantieren, dass Manipulationen durch periodische Überprüfungen der Integrität der Blockchain rasch entdeckt werden und korrigiert werden können (vgl. folgenden Abschnitt).

c) Fake-Blockchain: Damit niemand eine manipulierte, aber trotzdem korrekte Fake-Blockchain herstellen kann, wird ein rechentechnisch sehr aufwändiges Verfahren eingesetzt. Dabei wird jeweils automatisch eine Wettbewerbsaufgabe generiert, die gelöst werden muss, bevor ein neuer Datenblock an die Blockchain angehängt werden kann (vgl. späteren Abschnitt).

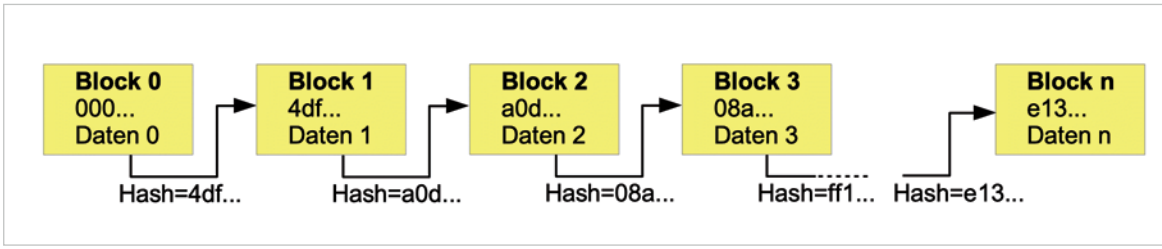

Abb. 1: Schematischer Aufbau einer Blockchain. Der Hash Code des ganzen Blocks 0 sei 4df... (die 3 Punkte stehen für die weiteren 61 Hexadezimalstellen). Dieser Hash Code wird an den Anfang des Blocks 1 geschrieben, gefolgt von einer beliebigen Anzahl Daten. Dieses Verfahren wird analog weitergeführt. Die BitCoin Blockchain wächst durchschnittlich um 6 Blöcke pro Stunde. (Bild: F. Gassmann)

Sicheres Gütesiegel für digitale Daten

Digitale Gütesiegel wurden entwickelt, damit im Internet Computerprogramme (z.B. Updates) verteilt werden können, bei denen kein einziges Bit falsch sein darf. Gütesiegel sollen schnell berechenbar sein und sich bei kleinsten Fehlern drastisch verändern. So wird vermieden, dass eine Kombination mehrerer Fehler dasselbe Gütesiegel ergibt.

Ein weit verbreitetes Gütesiegel-Programm ist der Secure Hash Algorithm, der ein 256 Bit langes Gütesiegel produziert: SHA-256 (manchmal auch SHA-2 genannt). Er wurde 2002 durch die US National Security Agency entwickelt und es gelang seither nie, durch Mehrfachfehler dasselbe Gütesiegel zu erzeugen.

SHA-256 wird beispielsweise für Internet-Zertifikate oder im Rahmen der Kryptowährung BitCoin verwendet. SHA-256 Gütesiegel kann jedermann selbst herstellen **(vgl. Lit. SHA-256)**. Aus jeder beliebigen Datei lässt sich mit SHA-256 ein «Hash Code» genanntes Gütesiegel mit einer Länge von 64 Zeichen zu je 4 Bit (Hexadezimalsystem) erzeugen. Das folgende Beispiel zeigt, wie drastisch das SHA-256 Gütesiegel auf die Änderung eines einzigen Bits reagiert (2 geändert in 3):

Hans Muster Beispielstrasse Zürich Tel. 044123 4567
Email h_muster@bluewin.ch
7f3e 3d81 212e 49b8 db29 a953 d51e ac7c 2022 458b eb6d c2a7 c6aa 764b 5033 c684
Hans Muster Beispielstrasse Zürich Tel. 044133 4567
Email h_muster@bluewin.ch
36d9 62e4 3522 5f36 e25b 934a 95d4 358e 7826 fa88 a443 c025 1159 72f5 12ec 4825

Es gibt keine Möglichkeit, vom Hash Code auf den Originaltext zurückzurechnen. Würde man im obigen Beispiel alle Zeichen der Adresse ausser der Telefonnummer zusammen mit dem Hash Code vorgeben, könnte man die fehlende Telefonnummer nur ermitteln, wenn man mit allen rund 500 Millionen möglichen Telefonnummern die Hash Codes bestimmt und mit dem vorgegebenen Hash Code vergleicht. Nur bei der genau der richtigen Telefonnummer würden die beiden 64-stelligen Hexadezimalzahlen übereinstimmen!

Aufbau der BitCoin Blockchain

Wie kann man eine durchschnittlich alle 10 Minuten wachsende Kette von ungleich grossen Datenblöcken mit einem Gütesiegel versehen, das die gesamte Kette schützt? Man bestimmt den Hash Code für alle Daten eines Blocks und schreibt diesen zu Beginn des nächsten Blocks.

Abb. 1 zeigt, wie auf diese Weise eine Kette von Blöcken entsteht, die durch Hash Codes zusammengehalten wird. Niemand kann an irgendeiner Stelle irgendwelche Daten verändern, ohne dass eine Bruchstelle entsteht. Ein Computer, der alle Hash Codes der Blockchain überprüft, würde diese in kurzer Zeit finden. Da weltweit Tausende von Kopien der BitCoin Blockchain existieren, kann ein fehlerhafter Block rasch durch einen korrekten ausgetauscht werden. Die BitCoin Blockchain ist also etwa gleich unzerstörbar wie ein weltweit verbreitetes Buch!

Es liegt auf der Hand, dass diese Blockchain-Technologie für viele verschiedene Datensätze anwendbar ist, die gegen Manipulation geschützt werden müssen. Es wäre auch möglich, digitalisierte Film- oder Tondokumente auf diese Weise mit einem Zertifikat zu versehen, so dass Veränderungen sofort festgestellt werden könnten. Noch so raffiniert manipulierte Film- oder Tondokumente könnten entlarvt werden. Weiter können die Blöcke ergänzt werden durch Zeitmarken (sog. Timestamps),

die beweisen, dass ein Dokument zu einem bestimmten Zeitunkt existiert hat, oder es können öffentliche Schlüssel und Unterschriften darin eingeschlossen werden. Alle diese Zusätze sind ebenfalls im Hash-Code enthalten und Manipulationen würden sofort entdeckt.

Wer erzeugt die Blockchain?

Eine entscheidende Frage ist nun: Wer erzeugt die Blockchain und sorgt damit dafür, dass die Daten fälschungssicher abgespeichert werden? In der traditionellen Vorstellung übernimmt diese Aufgabe ein vertrauenswürdiger Vermittler, also eine Bank oder ein Staat.

Diese Rolle wird bei BitCoin der Öffentlichkeit übergeben. Wer jeweils den nächsten Block an die Blockchain anfügen darf, wird in einem Wettbewerbsverfahren entschieden, an dem sich jedermann beteiligen darf. Die Wettbewerbsaufgabe besteht darin, dass die Teilnehmer eine aufwändige Rechenaufgabe lösen müssen. Der oder die schnellste erhält als Belohnung einen Gewinn in Form von BitCoins.

Die Wettbewerbsaufgabe wird im folgenden Abschnitt genauer beschrieben. Es sei aber bereits hier erwähnt, dass es keine intelligentere mathematische Methode gibt, um die Aufgabe zu lösen, als das völlig stupide Durchprobieren aller möglichen Zahlen, genau wie beim oben erwähnten Beispiel mit der Telefonnummer von Hans Muster. Per Zufall stolpert einer der vielen Computer (nicht unbedingt der schnellste), die am Wettbewerb teilnehmen, über die korrekte Kombination und gewinnt! Diese einer Spielbank ähnliche Zufallssituation hält die Teilnehmenden bei der Stange und lässt sie grosse Beträge in Hardware und Stromkosten investieren, um die Gewinnchancen zu erhöhen!

Die Gewinnerin darf den nächsten Block (zusammen mit der gefundenen Lösung der Wettbewerbsaufgabe) an die Blockchain anfügen und auch den Gewinn in Form von BitCoins auf ihr Konto gutschreiben. Dieser Gewinn belastet niemanden, da er nur die Menge der im Umlauf befindlichen BitCoins erhöht. Es ist nicht möglich, sich einen höheren Gewinn gutzuschreiben als der durch das Nakamoto Institut festgelegte, weil dies durch alle anderen BitCoin-Knoten (sog. «Nodes») bemerkt würde. Der neue Block würde nicht akzeptiert und das Recht, den neuen Block anzuhängen, ginge an den zweitschnellsten Knoten.

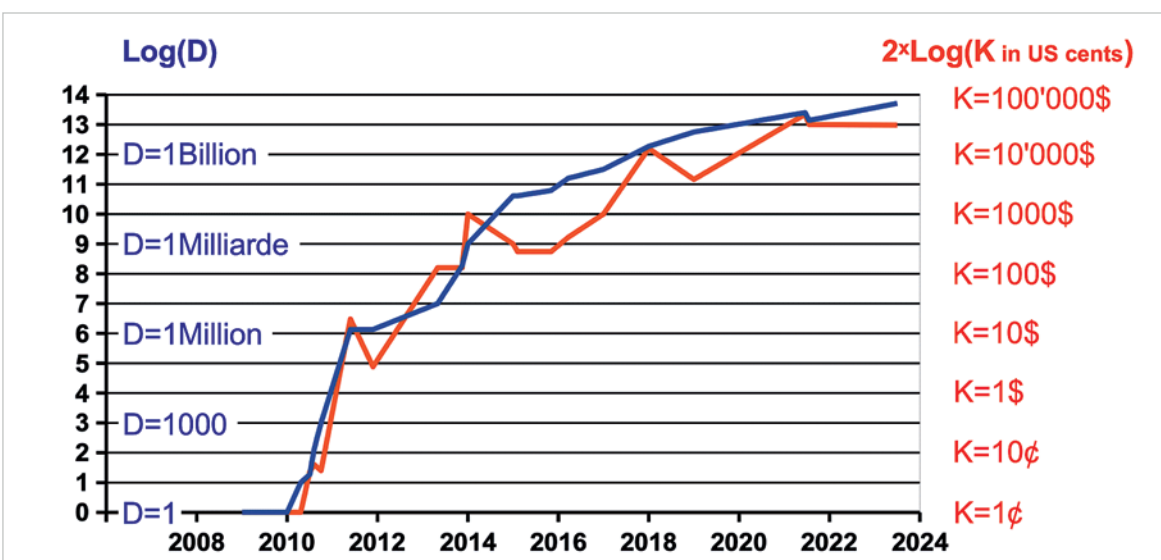

Abb. 2: Die Mining Difficulty D (2009 bis Juli 2023) ist mit dem Bitcoin-Kurs K korreliert. Es gilt etwa K ≈ √D, wenn K in US cents gemessen wird. D ist proportional zur Rechenleistung der gesamten Miningflotte, die eng mit dem Energieverbrauch des Bitcoin-Systems verknüpft ist. Der Bitcoin-Kurs ist also ein Indikator für die durch Bitcoin verursachte Umweltbelastung. (Bild: Daten aus: https://en.bitcoinwiki.org/wiki/Difficulty_in_Mining und weitere Quellen, Kurven durch Autor geglättet)

Abb. 3: Bitcoin Mining Rechnerfarm in Medicine Hat, Alberta, Canada im Oktober 2018. Jede Einheit ist mit Lastwagen transportierbar, um Orte mit niedrigem Strompreis aufzusuchen. Hinter den Jalusien sind Ventilatorfelder zur Kühlung der vielen parallel arbeitenden Computer angebracht. Mining ist in der Schweiz nicht rentabel, da der Strom zu teuer ist. (Bild: Curtis Huisman, CC BY 4.0)

Die Blockchain ist so durch weltweit rund 44 000 Knoten (in der Schweiz 500-600) stabilisiert, die sich gegenseitig kontrollieren und keine Verstösse gegen die Regeln tolerieren, weil sie selbst von der einwandfreien Funktion des Systems profitieren. Ein einzelner Knoten kann deshalb das System nicht betrügen. Es ist aber offen, was einer grossen kriminellen Organisation mit einer genügend mächtigen Flotte von Knoten gelingen würde oder was der Einsatz eines Quantencomputers verursachen würde.

Die Mathematik der Wettbewerbsaufgabe

Die Wettbewerbs-Aufgabe entspricht dem oben erwähnten Problem, aus dem Hash Code die Telefonnummer zu bestimmen. Weltweit schätzt man, dass darin heute über 300 000 «Miners» (moderne Goldgräber) involviert sind. Diese beschäftigen sich jedoch zum grössten Teil nicht mit Computern, sondern haben ein Abo bei einem Mining-Center und sind gewinnbeteiligt, wenn ihr Center gewinnt.

Die Wettbewerbs-Aufgabe kann von jedem Knoten formuliert werden. Ich habe sie mit einem Minicomputer (Raspberry Pi) simuliert: Zuerst habe ich den Hash Code HT von einem beliebigen Text gebildet und dessen letzte 8 Hexadezimalzahlen als sog. «once»-Feld definiert. Die Aufgabe ist, das once-Feld so lange zu verändern, bis der Hash Code von HT mit variiertem once-Feld mit 5 Nullen beginnt. Ein korrektes Resultat sieht dann so aus:
00000 2eb b511568536d56ce04506886dc7f48ef4 a2a4a5ad1d77986a 4264039f

Ich habe dieses Resultat erreicht, indem ich mit Hilfe eines Zufallszahlengenerators das once-Feld von HT so lange neu gewählt habe, bis der Hash Code von HT mit 00000 begann. Dafür habe ich 610 582 mal probieren müssen. Für eine zweite Lösung habe ich weitere 484 706 mal probiert. Insgesamt habe ich mit 49 Mio. Versuchen 50 Lösungen gefunden.

Der SHA-256 Algorithmus ist derart ausgefeilt, dass man alle diese Zusammenhänge statistisch einfach verstehen kann: Die 16^8 verschiedenen möglichen Werte des once-Feldes werden regelmässig auf die 16^5 möglichen Werte des führenden 5er-Feldes verteilt (man hätte statt Nullen irgendeine Zahlenfolge nehmen können, z.B. 12345 oder man hätte auch das 5er-Feld mehr rechts hinsetzen können oder man hätte es sogar aufteilen können auf ausgewählte Stellen irgendwo: das Resultat wäre dasselbe geblieben). Zusammengefasst gibt es also $16^{8-5} = 4096$ mögliche Lösungen. Es erstaunt deshalb nicht, dass meine 50 Lösungen alle verschieden waren!

Aus dieser Überlegung folgt auch, dass die Wahrscheinlichkeit für eine Lösung bei jedem Versuch 16^{-5} ist. (Analog ist die Wahrscheinlichkeit, dass sich ein Zahlenschloss mit drei Zahlen im Zehnersystem öffnet, bei jedem Versuch ein Promille oder 10^{-3}.)

Eine Transaktion mit BitCoin verschwendet ca. 1300 kWh Strom

Nun berechnen wir den für den Anwender von BitCoin versteckten Preis des an sich genialen Zahlungssystems. Zuerst bestimmen wir die Wahrscheinlichkeit, dass der Computer eines Miners mit einem einzigen Versuch einen Treffer erzielt.

Bei Bitcoin wurde als «Target M» die folgende Hexadezimalzahl definiert, bei der unüblicherweise auch die führenden Nullen angegeben sind, die die Zahl auf 64 Stellen ergänzen:
TM = 0000 0000 FFFF ...52 Nullen.
Damit der Aufwand zur Lösung der Wettbewerbsaufgabe in kleinen Schritten so geregelt werden kann, dass die gesamte Miner-Computerflotte im Mittel 10 Minuten braucht, wird nicht die Anzahl führender Nullen verlangt, sondern vorgegeben, dass dasjenige once-Feld gesucht werden muss, das einen Hash Code ergibt, der kleiner ist als T = TM/D.

D ist die «Difficulty», die das Nakamoto Institut als Justierschraube benutzt. Für D=1 wird T=TM und die Aufgabe entspricht dem obigen Beispiel, wobei anstelle von 5 Nullen nun 8 Nullen gefordert werden. Die dafür im Mittel benötigte Anzahl Versuche $N = 1/p = 16^8 \approx 4{,}3 \times 10^9$ kann mit der heutigen Computerflotte in etwa einer hundertstel Nanosekunde erledigt werden. 2009 wurden dafür jedoch rund 10 Minuten gebraucht! **Abb. 2** zeigt den Anstieg der Difficulty seit der Geburt des BitCoin zusammen mit der Kursentwicklung.

Für den Block Nr. 773 097, der am 22. Januar 2023 vom Knoten *F2Pool* an die BitCoin-Blockchain angehängt wurde, betrug $D = 37{,}5905 \times 10^{12}$ und die führenden 21 Stellen von T waren 0000 0000 0000 0000 0000 00078...

F2Pool hatte eine once-Zahl gefunden, bei der der entsprechende Hash Code kleiner war als dieses T, nämlich 0000 0000 0000 0000 0000 52... Er hat dafür einen Gewinn von 6,25 BitCoins erhalten, was umgerechnet einem Betrag von rund 143 000 US-Dollars entspricht **(vgl. Lit. Block 773 097)**.

Die gesamte Rechnerflotte, die sich am BitCoin-Wettbewerb beteiligt, führt in 10 Minuten im Mittel $D \times 16^8 \approx 1{,}62 \times 10^{23}$ Versuche durch. Pro Sekunde leistet die Flotte also 270×10^{18} Versuche, was als 270 EHash/s bezeichnet wird (E = Exa = 10^{18}). Ein für die Flotte repräsentativer Computer mit Baujahr 2019 leistet etwa 20 GHash/s pro Watt elektrische Leistung **(vgl. https://minerstat.com/hardware/). Abb. 3** zeigt ein Beispiel einer grossen, mobilen Mining Rechnerfarm.

Die durch die gesamte Rechnerflotte benötigte elektrische Dauerleistung beträgt demnach etwa (270 EHash/s) / (20 GHash/s/W) = 13,5 GW (Gigawatt). Aufsummiert über ein Jahr sind dies 118 TWh (Terawattstunden), was dem 1,9-fachen des schweizerischen Elektrizitätsverbrauchs **(nach BfE 2022)** oder 0,43 Prozent des globalen Elektrizitätsverbrauchs entspricht.

Mit 1710 Transaktionen pro Block ergeben sich 13,5 GW × 1/6 h / 1710 ≈ 1300 kWh pro Transaktion. In der Schweiz würde dies je nach Tarif um 260 CHF kosten! Ein Elektroauto, das 15 kWh/100 km verbraucht, könnte mit 1300 kWh rund 8800 km weit fahren, also je nach Fahrleistung ein halbes bis ein ganzes Jahr in Gebrauch sein!

Diese Überlegungen zeigen, dass BitCoin als Zahlungssystem für eine Massenanwendung zur Überweisung von Kleinbeträgen nicht zukunftsfähig ist, obschon Reklameschriften genau dies glaubhaft machen wollen.

Fritz Gassmann

Literatur

Block 773 097: https://blockchair.com/bitcoin/block/773 097 (entsprechende Angaben sind für jede andere Blocknummer abrufbar)

Nakamoto S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Download von: https://nakamotoinstitute.org/bitcoin/

SHA-256: https://xorbin.com/tools/sha256-hash-calculator oder mit Download von Hash Generator oder ähnlichen Programmen aufs Handy.