# Runde Sache

## 10 Jahre Bitcoin und Blockchain: Erstaunlich robust

**Klimakiller, ungeeignet als Zahlungsmittel, substanzlos und überhaupt viel zu beschränkt: Die Kryptowährung Bitcoin hat viele Fehler, glaubt man ihren Kritikern. Doch auch nach zehn Jahren arbeitet die Bitcoin-Blockchain noch immer nach denselben Regeln – während die Konkurrenz mitunter nur dank Notfallmaßnahmen und Hard Forks überleben konnte. Das muss dem Bitcoin-Erfinder Satoshi Nakamoto erst noch jemand nachmachen.**

**Von Mirko Dölle**

Ausgerechnet die globale Finanzkrise hatte sich der vorgebliche Japaner Satoshi Nakamoto als Zeitpunkt ausgesucht: Während die Regierungen aller Herren Länder damit beschäftigt waren, ihre strauchelnden Banken mit Abermilliarden Steuergeldern vor dem Untergang zu bewahren, veröffentlichte Satoshi am 9. Januar 2009 den ersten Block einer revolutionären neuen Währung. Sie sollte gänzlich unabhängig sein von Banken und Regierungen, dezentral und demokratisch, weder zu kontrollieren noch zu manipulieren – ein Kontrapunkt zum bestehenden Bankensystem, das sich damals an staatliche Rettungsringe klammerte und dennoch unterzugehen drohte.

Doch wie sollte eine Währung funktionieren, bei der es keine zentrale Stelle gibt, die Guthaben verwaltet oder Überweisungen ausführt? Wie sollten Betrug und Manipulationen verhindert werden, ohne Beschwerdestelle und ohne Gerichtsbarkeit? Der Schlüssel ist, sämtliche Transaktionen in einer öffentlichen Blockchain zu speichern – einer Datenstruktur, die Informatik-Studenten unter dem Begriff „einfach verkettete Liste“ schon damals im ersten Semester kennenlernten: Ein Knoten der Liste enthält neben den (Transaktions-)Daten einen Verweis auf den nächsten Knoten. Satoshi nannte die Knoten Blöcke und die verkettete Liste der Blöcke die Blockchain.

Neu war, dass die Blöcke nicht etwa anhand ihrer Nummer in der Blockchain verkettet wurden, sondern dass der Nachfolge-Block den Hash-Wert des vorhergehenden Blocks referenzierte. Damit wurde der Hash-Wert eines Blocks zu seinem Schlüsselelement. Der Clou liegt darin, dass ein Hash-Wert quasi der Fingerabdruck der Daten ist: Verändert man auch nur ein einzelnes Bit der Daten, ergibt das einen völlig anderen Hash-Wert.

Wie sich eine Änderung genau auswirkt, lässt sich nicht vorhersagen – es ist nicht möglich, die Daten gezielt so zusammenzustellen, dass sie einen bestimmten Hash-Wert ergeben. Wollte man einen bestimmten Hash-Wert erreichen, müsste man die Daten immer wieder verändern, den Hash-Wert neu berechnen und nachsehen, ob der neue Wert der Gesuchte ist. Bei Bitcoin ist dieses Unterfangen noch einmal schwieriger, weil aus dem SHA256-Hash-Wert der Daten wiederum ein SHA256-Hash berechnet wird, der dann die ID des Blocks darstellt.

Indem ein Block der einfach verketteten Bitcoin-Blockchain auf den Hash-Wert des vorangegangenen Blocks verweist, wird nicht nur die Reihenfolge der Blöcke in der Blockchain eindeutig festgelegt – gleichzeitig lässt sich mittels Hash-Wert überprüfen, ob auch nur ein einziges Bit des vorherigen Blocks nachträglich manipuliert wurde. Denn jegliche Änderung würde bedeuten, dass der Block einen anderen Hash-Wert besitzt, als im Nachfolge-Block referenziert ist.

Wollte man die Daten des vorletzten Blocks manipulieren, so müsste man nicht nur dessen Hash-Wert neu berechnen, sondern anschließend zusätzlich den neuen Hash-Wert des letzten Blocks, damit der im letzten Block genannte Hash-Wert des Vorgängers mit dem manipulierten Block übereinstimmt. Um etwas im drittletzten Block zu verändern, wären schon drei Blöcke neu zu berechnen, damit die Manipulation unbemerkt bleibt. Je weiter zurück der zu manipulierende Block liegt, desto mehr Blöcke müssen neu berechnet werden.

### Hürdenlauf

Keine große Hürde: Selbst die in 2009 gängigen CPUs schafften es, den Hash eines Block mehrere Millionen Mal pro Se-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

kunde neu zu berechnen – die Hash-Leistung herkömmlicher Desktop-CPUs lag damals im Bereich von etwa 1 bis 25 Mega-Hashes pro Sekunde (MH/s). Schon ein einzelner Rechner hätte die Bitcoin-Blockchain nach Belieben verändern können.

Damit das nicht passiert, hat Satoshi die Aufgabe buchstäblich durch einen zusätzlichen Schwierigkeitsgrad (Difficulty) erschwert. Dieser besagt, dass der Hash-Wert eines akzeptablen Blocks mindestens eine gewisse Anzahl Nullbits am Anfang aufweisen muss. Hat der Hash-Wert eines neuen Blocks nicht genügend Nullen, so kann der Rechner eine eigens dafür vorgesehene Zahl im Block hochzählen, die sogenannte Nonce. Da die Änderung an der Nonce unvorhersagbare Auswirkungen auf den Hash-Wert hat, bleibt dem Computer nichts anderes übrig, als den Hash-Wert erneut zu bestimmen und zu hoffen, dass er genügend Nullen aufweist. Die Suche nach einem ausreichend kleinen Hash-Wert ist also im Prinzip eine Lotterie.

Außerdem wollte Satoshi, dass Bitcoin dezentral und demokratisch organisiert ist. Jeder sollte an der Fortsetzung der Blockchain mitarbeiten dürfen, niemand sollte die Kryptowährung kontrollieren können. Wenn jedoch mehrere Rechner gleichzeitig einen geeigneten Hash-Wert suchen, erhöht sich die Wahrscheinlichkeit, dass einer erfolgreich ist. Mit zunehmender Anzahl der Rechner musste deshalb auch der Schwierigkeitsgrad ansteigen.

## Bauchlandung

Satoshis geniale Lösung: Er legte fest, dass sich der Schwierigkeitsgrad automatisch im Abstand von zwei Wochen so anpasst, dass alle zehn Minuten ein neuer Block gefunden wird. Wurden die letzten 2016 Blöcke der Blockchain schneller als in exakt zwei Wochen berechnet, steigt die Difficulty automatisch um den Faktor an, die die Rechner zu schnell waren. Hat es hingegen länger als zwei Wochen gedauert, 2016 neue Blöcke zu finden, sinkt die Difficulty um den entsprechenden Faktor. So kann jeder selbst anhand der Blockchain die gerade geltende Difficulty bestimmen, es braucht dafür keine zentrale Stelle oder Organisation, die über die Difficulty wacht. Welchen Weitblick Satoshi beim Design des Difficulty-Algorithmus und der Wahl der Blockzeit von zehn Minuten bewies, zeigt der Bitcoin-Fork Bitcoin Cash.

Ein Kritikpunkt der Bitcoin-Cash-Entwickler an Bitcoin war, dass die Difficulty über einen so langen Zeitraum gemessen wird und sich deshalb nur gemächlich der weltweiten Rechenleistung anpasst. Als sie im August 2017 Bitcoin Cash von Bitcoin abspalteten, bauten sie deshalb einen eigenen, vermeintlich viel besseren Algorithmus ein, der die Difficulty viel schneller der Hash-Leistung anpassen sollte. Und legten eine glatte Bauchlandung hin: In manchen Phasen entstanden mehrere neue Blöcke im Abstand von nur wenigen Sekunden bis Minuten, dann wiederum dauerte es eine halbe Stunde, in der gar nichts passierte – bis wieder ein Schwall neuer Blöcke gefunden wurde. Das Ergebnis war so schlimm, dass sie bereits drei Monate später einen weiteren Hard Fork durchführen und den Difficulty-Algorithmus austauschen mussten.

Die Difficulty ändert sich stets nur für neue Blöcke der Bitcoin-Blockchain, niemals für alte. Das führt dazu, dass es heute ein Leichtes wäre, sämtliche in 2009 veröffentlichten Blöcke binnen weniger Stunden zu manipulieren und anschließend neu zu berechnen – heutige Spezial-Hardware ist billionenfach leistungsfähiger als damalige CPUs. Doch nach den Blöcken aus 2009 müsste man auch alle Blöcke aus 2010 neu berechnen, was schon deutlich länger dauert – denn damals verwendete man bereits Grafikkarten zur Hash-Wert-Berechnung, die ein Vielfaches mehr an Leistung besaßen als die CPUs, weshalb die Difficulty entsprechend anstieg.

Ist man bei der Neuberechnung der Blöcke aus 2013 angelangt, wird es wieder deutlich schwerer. Dann nahmen die ersten ASIC-Rechner den Betrieb auf, die bis heute Standard sind und deren Leistung sich in den letzten Jahren noch mehrmals vervielfacht hat. Je näher man mit seinen Manipulationen der Gegenwart kommt, desto länger dauert es, den nächsten Block zu finden. Während all dieser Zeit entstehen im Takt von zehn Minuten immer neue Blöcke, die man später ebenfalls neu berechnen muss – in weniger als zehn Minuten, weil man sonst nicht aufholen kann. Aussicht auf Erfolg hätte also nur jemand, der mehr als 50 Prozent der weltweiten Rechenleistung für Bitcoin kontrolliert. Man spricht in einem solchen Fall von einem 51-Prozent-Angriff [1], mit dem es (langfristig) möglich wäre, die Kryptowährung nach Belieben zu manipulieren.

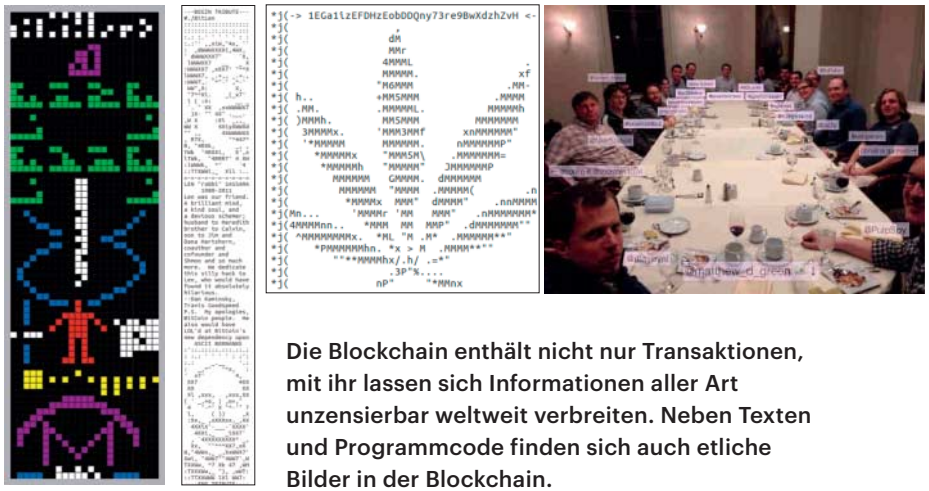
## Feindliche Übernahme

Der Bitcoin-Ableger Bitcoin Gold wurde Mitte Mai 2018 Opfer zweier 51-Prozent-Angriffe, der Super-Gau jeder Kryptowährung. Dabei kontrollierten Angreifer erheblich mehr Rechenleistung als zu der Zeit öffentlich bekannt war und von der Difficulty berücksichtigt wurde. So konnten sie zunächst Bitcoin Gold im Wert von 18 Millionen US-Dollar verkaufen und dank der übermächtigen Rechenleistung wenig später neue, manipulierte Blöcke ohne die Verkaufstransaktionen erzeugen. Damit verschwand der ursprüngliche Verkauf aus der Bitcoin-Gold-Blockchain und die Täter hatten Geld ohne Gegenleistung kassiert. Auch der Bitcoin-Fork Bitcoin Private wurde Mitte Oktober 2018 feindlich übernommen – zu Demonstrationszwecken: Der Hacker Geocold zeigte im Rahmen eines Live-Video-Streams, wie einfach das ist.

Der Raubzug bei Bitcoin Gold war möglich, weil vergleichsweise wenige Rechner an der Bitcoin-Gold-Blockchain arbeiteten. Indem die Täter mutmaßlich für wenige Tage ein Rechenzentrum anmieteten, verfügten sie über weitaus mehr Hash-Leistung für Bitcoin Gold als der Rest der Welt. Für den Angriff auf Bitcoin Private war der Aufwand sogar noch ge-

**AntMiner der aktuellen Generation (hier neun in einem Server-Rack) berechnen Bitcoin-Hashes billionenfach schneller als CPUs in 2009. Die Difficulty sorgt dennoch dafür, dass nur alle zehn Minuten ein neuer Block entsteht.**

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover



Die Blockchain enthält nicht nur Transaktionen, mit ihr lassen sich Informationen aller Art unzensierbar weltweit verbreiten. Neben Texten und Programmcode finden sich auch etliche Bilder in der Blockchain.

ringer, Geocold hatte die nötige Mining-Leistung für wenige hundert Dollar eingekauft.

Bei Bitcoin wäre ein solcher Angriff selbst für Regierungen nicht mehr durchführbar: Es gibt bei der Bitcoin-Blockchain einfach zu viel Rechenleistung, weltweit sind es aktuell etwa 40 EH/s. Das entspricht rund 3 Millionen der derzeit leistungsfähigsten Rechner mit einer Leistungsaufnahme von 4 Gigawatt. Es ist also ausgerechnet die große Anzahl an Rechnern und deren hoher Stromverbrauch, der Bitcoin gegen Manipulationen absichert.

Der Grund für die große Zahl ist, dass die Arbeit an der Bitcoin-Blockchain in den letzten Jahren äußerst rentabel war – denn es gibt eine Belohnung in Form von neuen Bitcoins für jeden neu gefundenen Block. Deshalb bezeichnet man die Rechner, die Transaktionen zu neuen Blöcken verarbeiten, als Miner – wie Goldgräber finden sie neue Blöcke und damit neue Bitcoins. Ein weiterer genialer Einfall Satoshis, der gleich mehrere Probleme löste.

## Geld aus dem Nichts

Als Satoshi Nakamoto Anfang Januar 2009 den sogenannten Genesis-Block der Bitcoin-Blockchain von Hand berechnete, gab es weder Bitcoins, die man hätte transferieren können, noch Rechner, die Transaktionen zu neuen Blöcken verarbeiten und die Blockchain fortsetzen konnten. Heute wird dieses Henne-Ei-Problem häufig dadurch gelöst, dass der Erfinder einer neuen Kryptowährung zunächst alle Währungseinheiten vorab errechnet und diese gegen Geld an Investoren verkauft – mitunter noch bevor die zugehörige Blockchain überhaupt ihren Betrieb aufnimmt. Dies nennt man Initial Coin Offerings, kurz ICO. Für den Erfinder ist das äußerst lukrativ, er hat seine Idee für viel Geld verkauft, noch bevor sie bewiesen hat, dass sie überhaupt funktioniert. Damit fehlt der Anreiz, die Kryptowährung überhaupt an den Start zu bringen. Besonders 2017 und Anfang 2018 wurden viele unwissende Investoren auf diese Weise geschröpft – aufgrund des massiven Missbrauchs sind ICOs inzwischen in vielen Ländern streng reguliert.

Satoshi hingegen führte eine Belohnung (Reward) für neu gefundene Blöcke ein. So erhielt Satoshi für seinen von Hand geklöppelten Genesis-Block eine Belohnung von 50 Bitcoin – womit die ersten 50 Bitcoin der Kryptowährung entstanden. Damit gab es einen Anreiz, den eigenen Rechner neue Blöcke berechnen zu lassen und so die Blockchain am Leben zu erhalten. Viele Kryptowährungs-Enthusiasten der ersten Stunde ließen deshalb ihre Rechner Bitcoins schürfen, wenn sie gerade nicht gebraucht wurden.

So manches Bitcoin-Vermögen stammt aus jener Zeit, auch das des Informatikers James Howell aus Newport. Er hatte bereits in 2009 mit dem Mining auf seinem PC angefangen und stolze 7500 Bitcoin geschürft. 2013 warf er aber dummerweise seine Festplatte auf den Müll, auf der sich die einzige Kopie seines Bitcoin-Wallets befand. Das war ärgerlich, aber keine Katastrophe: Bis Anfang 2011 war ein Bitcoin nur wenige Cent wert, Anfang 2013 lag der Preis immerhin schon bei gut zehn Dollar. Ihren ersten Höhenflug hatte die Kryptowährung Ende November 2013, als kurzzeitig bis zu 1000 US-Dollar pro Bitcoin bezahlt wurden. Im folgenden Jahr sank der Preis allerdings wieder auf 250 Dollar.

Erst Ende 2016 erreichte der Bitcoin wieder den alten Höchststand und stieg weiter. Im Dezember 2017 wurden zeitweise bis zu 20.000 US-Dollar pro Bitcoin bezahlt – Howells verloren gegangenes Wallet war plötzlich rund 150 Millionen US-Dollar wert. Kein Wunder, dass der Informatiker seinen Fehler bereute und die Müllkippe von Newport nach seiner Festplatte umgraben lassen wollte. Doch man verweigerte ihm die Genehmigung. So sind die 7500 Bitcoin von Howell und damit 0,36 Promille der gesamten Kryptowährung für immer verloren.

Denn Satoshi hat die Menge an Bitcoins, die durch die Belohnung erschaffen werden, auf maximal 21 Millionen begrenzt: Die Reward halbiert sich alle vier Jahre, sodass im Jahr 2140 die Belohnung auf null fällt, weil die kleinste darstellbare Einheit ein hundert-millionstel Bitcoin ist – zu Ehren ihres Erfinders Satoshi genannt. Danach wird es keine neuen Bitcoins mehr geben.

Die Halbierung der Belohnung nach jeweils 210.000 Blöcken sorgt dafür, dass sich die Miner nicht auf der Subventionierung ausruhen können: Langfristig müssen sie ihre Strom- und Betriebskosten anderweitig decken. Dafür gibt es die sogenannte Transaction Fee, eine Art Überweisungsgebühr. Während man als Kunde bei Banken nicht um die Überweisungsgebühr feilschen kann, liegt es bei Bitcoin vollständig in der Hand des Anwenders, wie viel Geld er für die Ausführung einer Überweisung bezahlen möchte. Sparfüchse können ihre Transaktionen sogar zum Nulltarif losschicken.

Doch wie in der Marktwirtschaft üblich bestimmen letztlich Angebot und Nachfrage den Preis: Betreiber von Minern werden natürlich jene Transaktionen zur Verarbeitung aussuchen, die ihnen die meisten Transaktionsgebühren einbringen. Überweisungen ohne Gebühren werden sie allenfalls dann berücksichtigen, wenn keine weiteren bezahlten Transaktionen mehr anstehen. So kann es mitunter Tage dauern, bis eine Transaktion ohne Fee ausgeführt wird.

## Künstlich beschränkt

Gibt es ein hohes Transaktionsaufkommen, kann es durchaus passieren, dass Überweisungen mit geringer oder gar keiner Gebühr überhaupt nicht mehr ausgeführt werden. Der Grund dafür ist, dass Bitcoin-Blöcke nur maximal 1 MByte groß sein dürfen, was bis Mitte 2017 einem Ma-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

ximum von etwa 2000 Transaktionen entsprach. Als Bitcoin erfunden wurde, gab es zunächst keine Größenbeschränkung – Satoshi führte sie erst am 12. September 2010 im Rahmen eines sogenannten Soft Forks ein. Er wollte damit verhindern, dass ein Angreifer durch die Veröffentlichung riesiger gefälschter Blöcke viel Rechenleistung und Speicherplatz bindet und so den Handel mit Bitcoins zum Erliegen bringt.

Die nachträgliche Beschränkung auf 1 MByte pro Block war es, die zum Abspalten der neuen Kryptowährung Bitcoin Cash von Bitcoin führte: Ein Teil der Bitcoin-Miner wollte die Maximalgröße auf 8 MByte ausweiten, wozu jedoch ein Hard Fork des Bitcoin notwendig gewesen wäre. Letztlich setzte sich eine Umgestaltung der Bitcoin-Blöcke durch, wobei Teile der zuvor im Block gespeicherten Daten ausgelagert wurden (SegWit, Segregated Witness). Dadurch passte nunmehr nahezu die doppelte Menge an Transaktionen in einen Block. Diese Änderung war kompatibel mit älteren Bitcoin-Clients, also nur ein Soft Fork der Kryptowährung. Ein Teil der Entwickler wollte die Vergrößerung der Blöcke auf 8 MByte trotzdem durchsetzen und erzeugte gleichzeitig einen Hard Fork – Bitcoin Cash war geboren.

Durch Satoshis Weitblick und indem Änderungen stets behutsam durchgeführt wurden, war in den vergangenen zehn Jahren kein einziger Hard Fork bei der ältesten noch gehandelten Kryptowährung notwendig. Die Entwicklung von Bitcoin ist aber noch längst nicht am Ende. So könnte man einfach die Blockzeit auf fünf Minuten halbieren und so das Transaktionsvolumen noch einmal verdoppeln. Oder die Bitcoin-Gemeinde einigt sich doch auf einen Hard Fork und erhöht die maximale Blockgröße. Mit dem Lightning-Netzwerk gibt es außerdem eine interessante Erweiterung, die sich besonders für schnelle Transfers kleiner Beträge anbietet – ideal, um etwa seinen Kaffee mit Bitcoin zu bezahlen.

Sogar als Werkzeug für die freie Meinungsäußerung taugt die Bitcoin-Blockchain. Sie ist der ideale Ort, um Informationen unzensierbar weltweit zu verbreiten. Das haben verschiedene Personen genutzt, um Texte, Programmcode und sogar Bilder in der Blockchain zu verewigen. Den Anfang machte Satoshi Nakamoto höchst persönlich, und zwar im Genesis-Block: Dort zitiert er die Titelgeschichte der London Times vom 3. Januar 2009, in der über Pläne des damaligen Finanzministers Alistair Darling berichtet wird, Banken in einer zweiten Rettungsaktion mit Billionen Pfund Steuergeldern zu retten. Banken, die es dank Bitcoin und seiner Nachfolger eines Tages vielleicht gar nicht mehr gibt. Schauen wir einfach, was bis zum zwanzigsten Geburtstag geschieht. *(mid@ct.de)* c't

**Literatur**

[1] Mirko Dölle, Kettenreaktion, Wie 51-Prozent-Angriffe Bitcoin & Co. bedrohen, c't 14/2018, S. 26

Anzeige

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover