



Bitcoins Selbstblockade

Die schnell wachsende Digitalwährung leidet an Kapazitätsengpässen, aber ihre Community streitet statt sie zu lösen.

Egal, ob im Supermarkt, am Bahnschalter oder im Call-Center, Kunden sind genervt, wenn sie zu lange warten müssen. So geht es auch Besitzern von Bitcoins, wenn sie ein paar ihrer digitalen Münzen im Internet überweisen wollen. Das Bitcoin-Zahlungsnetz stößt mit 300 Tausend Zahlungen täglich inzwischen an seine Kapazitätsgrenzen. Seine Netzgemeinde bestehend aus Entwicklern, Nutzern und Dienstleistern muss etwas unternehmen, kann sich aber nicht auf eine gemeinsame Lösung verständigen. So droht das 2008 erstmals beschriebene „Experiment einer Digitalwährung“ zu scheitern, während gleichzeitig etablierte Banken und Zahlungsdienste die Chancen der „innovativen Technologie“ für sich entdecken.

Hauptproblem sind die langen Liege- und Verarbeitungszeiten im Bitcoin-Netz. Das speichert seine Zahlungen in einer Art Kassenbuch, der sogenannten „Blockchain“. Wie der Name sagt ist das eine Kette von Blöcken, die für alle zugänglich im Netz liegt. Jeder der Blöcke fasst zirka 2000 Einzelzahlungen und trägt eine eindeutige Prüfziffer. Das Erstellen neuer Blocks beansprucht Zeit und Computerleistung. Das übernehmen weltweit verteilten Dienstleister, die sogenannten „Miner“. Laufen Zahlungen schneller ein als Miner in die Blockchain eingetragen können, kommt es zum Rückstau. Wie im Supermarkt stehen die Kunden dann in der Schlange, und warten. Am 24. November zum Beispiel, dem mit über 330.000 Überweisungen umsatzstärksten Tag des Jahres 2016, mussten permanent zwischen 30.000 und 70.000

Zahlungsaufträge warten, einige davon stundenlang. „Inakzeptabel“ in den Augen vieler Bitcoin-Nutzer, wie Kommentare in Foren wie coinforum.de belegen. Absehbar sind die Engpässe seit Anfang 2015 und seitdem auch streiten sich die Verfechter der einzelnen Lösungsansätze, die sich „Bitcoin Core“, „Bitcoin XT“ und „Bitcoin Unlimited“ nennen.

Bitcoin entstand nach dem Beinahe-Zusammenbruch des internationalen Finanzsystems 2008 als Alternative zu den herkömmlichen Zahlungssystemen. Das Platzen der Immobilienblase in Amerika, Kursmanipulationen und Steuerbetrügereien der Banken hatten zu einem massiven Vertrauensverlust geführt. Kein Wunder, dass da die Idee zu einer Alternative, die der Kontrolle etablierter Banken und Notenbanken entzogen ist, aufkam. Unter dem Pseudonym „Satoshi Nakamoto“ veröffentlichte 2008 ein bis heute unbekannter Entwickler genau das, das Konzept zu einem Zahlungssystem, in dem Internetnutzer direkt und weltweit kommunizieren. Er nannte es ein „Peer-to-Peer-Netz“ und das zugehörige Protokoll „Blockchain“. Anfang 2009 veröffentlichte Nakamoto eine erste Softwareversion und legte den ersten Block mit 50 Bitcoins an. Damit war Bitcoin geboren. Anfangs stiegen die Nutzerzahlen langsam, aber kontinuierlich. Bitcoin blieb in der öffentlichen Wahrnehmung relativ unbeachtet. Die junge Digitalwährung galt als nicht ernstzunehmendes Nischenzahlungsmittel für Geldwäscher, Whistleblower und Freaks. Auch staatliche Stellen und die Finanzindustrie ignorierten sie zunächst völlig. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) zum Beispiel beschäftigte sich erst 2013 mit der neuen „nichtstaatlichen Ersatzwährung“ und warnte in einer ersten Bewertung die Verbraucher vor drohenden Verlusten durch Softwarefehler, Hackerangriffe und Kursschwankungen in einem unkontrollierten Markt. Seit 2015, als erstmalig drei Millionen Nutzer gezählt wurden, steigen die Transaktionszahlen rapide. Bitcoin steht Anfang 2017 mit 11 Millionen Nutzern, knapp 80 Millionen Transaktionen pro Jahr und einem Börsenwert von umgerechnet 12 Milliarden US\$ an der Schwelle zum Massensystem. Ereignisse wie das Einziehen von Bargeld in Indien und Venezuela im Herbst 2016 könnten das Interesse weiter befeuern, weil Bitcoin als Ausweidlösung zum Bargeld entdeckt wird.

Sollte das Wachstum so weiter gehen, ist es unumgänglich das Skalierungsproblem, wie die Kapazitätsengpässe in der Fachsprache der Softwareentwickler heißen, zu lösen. „Bitcoin Core“, das fünfköpfige Team um Gavin Andresen, Chefentwickler und Nachfolger von Satoshi Nakamoto,

möchte an der ursprünglichen Idee möglichst wenig ändern. Vor allem wollen er und seine Mitstreiter die derzeitige Blockgröße von einem Megabyte nicht erhöhen. Begründet wird das mit dem Rechenaufwand beim Erzeugen der Blöcke, dem Minen. Der soll möglichst klein bleiben, damit Miner mit weniger leistungsfähiger Hardware eine gerechte Chance haben gegen große mit schnelleren Rechnern. Das Core-Team veröffentlicht dazu im Oktober 2016 die Version „Core 0.13.1“, die das Problem lösen will, indem der Speicherplatz eines Blocks besser genutzt wird. So passen dann 70% mehr Zahlungen in einen Block, bei gleichbleibender Blockgröße.

Die Gegner der Core-Lösung, darunter auch einige große Miner und Bitcoin-Börsen, sprechen ihr ab, dass Skalierungsproblem wirklich langfristig zu lösen. Ihr Argument: Bei weiter steigenden Nutzerzahlen sei Bitcoin in Kürze wieder mit Kapazitätsengpässen konfrontiert und das Beharren auf der Blockgröße von einem Megabyte sei in Anbetracht ständig leistungsfähigerer Computerhardware unsinnig. Die Lösungsansätze „Bitcoin XT“ und „Bitcoin Unlimited“ sehen deshalb vor die Blocks gleich zu vergrößern. Die beiden unterscheiden sich lediglich darin in welchen Schritten, das zu tun ist: auf zwei oder acht Megabyte pro Block oder gleich unbegrenzt.

Zunächst diskutiert die Bitcoin-Community die Lösungsvorschläge noch gemeinsam im Rahmen der „Scaling Bitcoin Workshops“ 2015 in Montreal, und 2016 in Hongkong und Mailand (scalingbitcoin.org). Aber es kristallisiert sich kein Konsens heraus. Im Gegenteil, die Fronten verhärten sich. Mike Hearn, ein Entwickler der ersten Stunde und Vertreter von Bitcoin XT, wirft seinen Kollegen unkooperatives, ja undemokratisches Verhalten vor. Er verlässt mit Gleichgesinnten das Core-Team und bezeichnet Bitcoin im seinem Blog als „gescheitertes Experiment“. Sein Fazit: „Es (Bitcoin) ist gescheitert, weil seine Community gescheitert ist.“ Und: „Was mal gemeint war als ein neue, dezentralisierte Form des Geldes ist inzwischen zu einem System verkommen, das durch eine Handvoll Leute kontrolliert wird.“ Diese Leute sind seiner Meinung nach Andresen und sein Team, sowie zwei große chinesische Miner.

Als Folge gibt es parallel zur Core-Lösung weitere Softwarevarianten für Bitcoin XT und Bitcoin Unlimited. Keine der drei Lösungen findet eine ausreichende Mehrheit im Bitcoin-Netz. Eine selbstverordnete Regel fordert nämlich 95% Zustimmung, bevor eine Änderung der Blockchain für alle zum verbindlichen Standard werden kann. Damit will man verhindern, dass sich Bitcoin in Teilnetze

spaltet. Zum Jahreswechsel 2017 hat Bitcoin Core 0.13.1 erst 25% Befürworter. Mit unter 10% sind es bei Bitcoin XT und Bitcoin Unlimited noch viel weniger. Ob sich in naher Zukunft eine Mehrheit für eine der Lösungen herausbilden wird, ist fraglich. Laut Andresen ist „die Konsensfindung in einem verteilten Netz von Gleichen ein offenes Problem, für das es bisher keine Lösung gibt“. Neben seinen technischen Problemen krankt Bitcoin also auch noch an der Selbstblockade einer zerstrittenen Entwicklergemeinde. Solange sich aber kein Konsens bildet, kann Bitcoin nicht weiter wachsen, geschweige denn seine Wartezeiten reduzieren.

Fortschritte bei der Lösung des Skalierungsproblems könnten sich aber von einer ganz anderen Seite ergeben, nämlich genau von jenen etablierten Banken und Zahlungsdiensten, die Nakamoto mit der Idee vom „direkten Zahlen ohne Konto“ überflüssig machen wollte. 2016 hatten die meisten von ihnen Projekte zur Erarbeitung von Blockchain-Lösungen gestartet oder bereits in Arbeit. Dabei sind unter anderem die Britische und Europäische Zentralbank, die Technologiebörse Nasdaq, die amerikanische Citigroup und die Deutsche Bank. Warum tun sie das, wenn Bitcoin - die größte Blockchain - immer noch weit entfernt davon ist die technischen Voraussetzungen erfüllen zu können? Von welchen Anforderungen die Rede ist, wird klar, wenn man drei der größten Zahlungsdienstleister betrachtet: den Internet-Bezahldienst Paypal, den Finanznachrichtendienst SWIFT und den Kreditkartenanbieter VISA. Deren global genutzten Zahlungssysteme bearbeiten pro Tag ein Vielfaches der bescheidenen 300 Tausend bei Bitcoin. Paypal mit 192 Millionen Kunden prozessiert 16 Millionen Zahlungen. SWIFT verschickt für seine 11.000 Teilhaber - hauptsächlich Banken - bis zu 27,5 Millionen Finanztransaktionen. Das größte Volumen muss VISA bewältigen mit 2,5 Milliarden Kartenkunden und 230 Millionen Transaktionen pro Tag.

Der Hauptgrund für das Interesse der Finanzbranche ist: Bitcoin kommt ohne Konten und Zwischenstellen aus. Seine Nutzer transferieren Geld zwar mit langen Wartezeiten, aber immerhin direkt zum Empfänger, weltweit und meistens innerhalb eines Tages. Mit keinem herkömmlichen Zahlungsverfahren geht das so direkt. Banküberweisungen ins nichteuropäische Ausland zum Beispiel benötigen derzeit drei bis fünf Tage. Daran beteiligt sind mindestens zwei Geschäfts- und zwei Zentralbanken. Jedes der Institute führt eigene Konten und leitet die Zahlung durch seine Buchungssysteme. Das sind enorme Datenmengen. Wären die in einer Blockchain für alle verfügbar im Netz

abgelegt, würden die internen Systeme der Beteiligten massiv entlastet und der Umweg über Zentralbanken könnte entfallen. All das wäre deutlich einfacher, schneller und kostengünstiger als heute, so die Annahme. Der Bundesverband Deutscher Banken nennt die Technologie eine, „die das Potential hat die heutigen Wertpapier- und Zahlungsabwicklungssysteme zu revolutionieren“. Grund genug also für Global Player wie Paypal, SWIFT und VISA sich mit Blockchain zu beschäftigen. Und natürlich werden gerade sie - erfahren im Umgang mit großen Transaktionsmengen - das Potential der „revolutionären Idee“ genau prüfen. Gut möglich, dass dabei die erste wirklich massenfähige Blockchain entsteht.

Währenddessen stagniert das Vorbild, und seine Community vergibt die Chance aus Bitcoin eine konkurrenzfähige Alternative zu etablierten Bezahlssystemen zu machen. Aber vielleicht einigt man sich ja doch noch.