Im Stollen des neuen Goldes

Das Schürfen von Bitcoin ist kein Selbstzweck. Das komplizierte Verfahren dient der Sicherheit des Netzwerks und ist für die Umwelt besser als sein Ruf.

von Aroosh Thillainathan

Vor sieben Jahren hörte ich das erste Mal von Bitcoin und damit von der Idee eines globalen Zahlungsmittels, das über Ländergrenzen hinweg ganz ohne Banken, Scheine oder Münzen auskommen würde. Das klang revolutionär. Ein Algorithmus, der tatsächlich etwas Digitales zu schaffen vermag, das einmalig und nicht kopierbar ist.

Für mich war klar, dass ich mit Bitcoin Bahnbrechendes entdeckt haben muss. So wurde ich zum Miner der ersten Stunde. Noch heute fasziniert mich die Infrastruktur rund um Bitcoin, die die hohe Rechendichte sowie die enorme Abwärme zu bewältigen imstande ist: viele weltweit verteilte Rechner, die das Herzstück des Bitcoins bilden und die im Protokoll-Code definierten Rechenvorschriften ausführen und das System so am Laufen halten.

Die Rechner sind es, welche das Bitcoin-System vor Fälschungen bewahren. Eine jede Bitcoin-Transaktion ist kryptografisch verschlüsselt, was eine gegenseitige Kontrolle unter den Rechnern ermöglicht. Ohne das Dazutun der Rechner wäre keiner der nur digital existierenden Bitcoin so einmalig wie ein nummerierter Geldschein. Wer einmal verstanden hat, wie der geniale Algorithmus hinter Bitcoin funktioniert, den wird Bitcoin nicht mehr loslassen.

Bitcoin-Mining im Schnelldurchlauf

Man stelle sich ein grosses Kassenbuch vor. In diesem wird jedes Bitcoin-Konto registriert. Ein solches entspricht einer Adresse, die Teil des Bitcoin-Netzwerkes ist. Auf einer jeden Adresse können Bitcoin verbucht sein, die dann eben im Kassenbuch aufgeführt sind. Wird eine Bitcoin-Transaktion – angenommen, ein halber Bitcoin – ins Netzwerk eingespeist und durchgeführt, wird diese verrechnet und im Kassenbuch niedergeschrieben. Konkret bedeutet das: Bei einer Adresse im Netzwerk wurde der Gesamtstand soeben um einen halben Bitcoin reduziert, während dieser halbe Bitcoin einer anderen Adresse gutgeschrieben worden ist. Mit der Transaktion wird sogleich der neue Stand einer jeden Adresse im Kassenbuch vermerkt. So weit, so gut.

Hier beginnt nun die Arbeit der Miner (von engl. «to mine», schürfen). Gewissermassen als dezentralisierte Buchhalter führen sie gemeinsam das Kassenbuch, die Bitcoin-Blockchain. Jeder Miner hat Einsicht in das Kassenbuch und nur, was die Mehrheit der Miner als korrekt ansieht, schafft es auch in die Bitcoin-Blockchain.

Mining ist das neue Goldschürfen

Der Begriff des Minings ist in Anlehnung an das Schürfen von Gold gewählt. Das Edelmetall ist eine endliche Ressource auf unserem Planeten. Das heisst: Je mehr Gold geschürft wird, desto weniger ist davon noch auf der Erde vorhanden. Jede weitere Goldeinheit zutage zu fördern, wird daher schwieriger und kostspieliger.

Diese Beschaffenheit ahmt Bitcoin nach. Die Gesamtmenge aller je existierenden Bitcoin ist auf 21 Millionen limitiert. Voraussichtlich im Jahr 2140 soll diese Obergrenze erreicht sein. Bis dahin wird die neugeschaffene Bitcoin-Menge, die pro Block ausgeschüttet wird, alle vier Jahre halbiert.

Doch zurück zu den Transaktionen. Alle Transaktionen, die abgewickelt werden sollen, landen zunächst in einem grossen Pool, auf den alle Miner Zugriff haben. Daraus suchen sich diese ständig Transaktionen heraus und vergleichen, ob letztere nach dem aktuellen Stand des Kassenbuchs gültig sind. Verfügte diejenige Adresse, von der Bitcoin verschickt werden sollen, auch über den nötigen Betrag? Dies ist eine zwingende Voraussetzung, kann ein Bitcoin-Konto doch niemals überzogen werden.

Sind die Transaktionen gültig und stimmen mit dem aktuellen Stand der Blockchain überein, werden sie in einem Block zusammengefasst. Damit ein Miner diesen Block nun an die Blockchain anhängen kann, also neue Transaktionen ins Kassenbuch eingetragen werden, muss er ihn mit einem speziellen Code aus Zahlen und Buchstaben mathematisch verschlüsseln. Diese Aufgabe erfordert ungemein viel Rechenaufwand. Der Miner muss durch ständiges Ausprobieren einen Schwellenwert finden, der bestimmte, durch das Bitcoin-Protokoll festgelegte Kriterien erfüllt. Auf diese Weise konkurrieren Miner rund um die Uhr um den nächsten Eintrag ins Kassenbuch beziehungsweise darum, den nächsten Block an die Blockchain anzufügen. Findet ein Miner den richtigen Wert und hängt seinen Block der Blockchain an, wird er mit neu geschaffenen Bitcoins belohnt. Diese erhält er allerdings erst, wenn an seinen Block mindestens 100 weitere Blocks angehängt worden sind.

Die Blockchain ist also eine Kette von Blöcken und fungiert als Transaktionshistorie. Ist bloss eine Transaktion ungültig, schafft es der entsprechende Block nicht in die Blockchain. Einen ungültigen Block zu produzieren, lohnt sich nicht. Als Miner hat man letztlich den starken Anreiz, für seine Blöcke nur gültige Transaktionen zu akzeptieren. Nur so wahrt man sich die Chance auf die Belohnung in Form neuer Bitcoin. Es ist dieses geniale Anreizsystem des Minings, das den Bitcoin quasi fälschungssicher macht.

Wertspeicher einer digitalen Welt

Dieser faszinierende Algorithmus macht Bitcoin zu einer neuen Art der Aufbewahrung und Übertragung von Werten, die unserer globalisierten Welt mit ihren digitalen Strukturen und Lebensstilen gerecht wird. Bitcoin kennt keine Ländergrenzen. Wer über einen Internetzugang, einen Computer oder ein Smartphone verfügt, kann das Netzwerk nutzen. Innerhalb von höchstens 10 Minuten sind Bitcoin zwischen beliebigen zwei Teilnehmern weltweit in beliebiger Menge übertragbar.

«Es ist das geniale Anreizsystem des Minings, das den Bitcoin quasi fälschungssicher macht.»

Aroosh Thillainathan

Weder Banken noch Regierungen können die Geldpolitik des Bitcoins manipulieren. Das macht ihn letztlich zu viel mehr als einem Zahlungsmittel oder einer Anlageform – es macht ihn zu einem gesellschaftlichen und damit politischen Phänomen. Werte sicher und komplett unabhängig vom Bankensystem zu verschicken, dafür steht Bitcoin.

Zumal die Bitcoin-Blockchain nicht manipulierbar ist, können mit den Transaktionen in einem Block auch beliebige Dokumente fälschungssicher abgelegt werden. Gerade für Bereiche, wo Informationen unverfälschbar gespeichert werden müssen, kann die Bitcoin-Blockchain interessant sein. Im Vertragswesen könnte das beispielsweise dazu führen, dass Vermittlungsdienstleister obsolet werden oder dass Liefer- und Transportketten in der Logistik lückenlos nachverfolgt werden können.

Seinen Kritikern ist vor allem der hohe Energieverbrauch des Bitcoin-Netzwerks ein Dorn im Auge. Forscher des MIT und der TU München gehen zurzeit von rund 46 Terawattstunden (TWh) aus, die pro Jahr für die Aufrechterhaltung von Bitcoin anfallen. Eine lose Zahl taugt jedoch wenig, nur im Vergleich zu anderen Dingen ergibt sie unter Umständen Sinn. So verbraucht alleine das Drucken von Scheinen und Prägen von Münzen 11 TWh pro Jahr. Damit das globale Bankensystem täglich läuft, wird sogar von einem offiziellen Verbrauch von 650 TWh pro Jahr ausgegangen. Selbst der arbeitsintensive Abbau von Gold soll jährlich 132 TWh in Anspruch nehmen.

Im Lichte dieser Vergleiche relativiert sich der Energieverbrauch von Bitcoin. Noch weniger Sinn macht die Kritik am Energieverbrauch Bitcoins, wenn man ihn nicht für eine überflüssige, verschwenderische digitale Spielerei hält, sondern sein enormes Innovationspotenzial als erstes neutrales, zensurresistentes und rein digitales Zahlungsmittel vor Augen hat. Dass Bitcoin sich zum Beispiel auch preisgünstige Wasserkraft zunutze macht und diesen Kraftwerken somit eine Mindestabnahme und Planungssicherheit garantiert (die wiederum Entwicklung und den Ausbau erneuerbarer Energien fördert), sei hier nur am Rande erwähnt.

Entwicklungssprung durch Bitcoin

Heute bin ich nicht mehr Bitcoin-Miner, sondern CEO eines Grosskonzerns, welcher Rechenleistung verkauft. Noch immer nutze ich meine Erfahrungen, die ich über sieben Jahre während des eigenen Bitcoin-Minings gesammelt habe. In meiner Industrie war Bitcoin-Mining die erste grosse kommerzielle Anwendung des High-Performance-Computings (HPC). Derzeit haben wir ein riesiges Rechenzentrum in Texas im Bau: über 300 Meter lange Hallen auf 40 Hektar, einer Fläche, die insgesamt 57 Fussballfeldern entspricht. Bis Anfang nächsten Jahres soll das Rechenzentrum rund ein Gigawatt Strom aufnehmen können. Unter unseren Kunden sind zwei japanische Milliardenkonzerne, welche im grossen Stil Bitcoin-Mining betreiben. Interessanterweise besteht der Strommix schon heute zu rund 25 Prozent aus erneuerbaren Energien. Texas ist heute derjenige Bundesstaat mit der höchsten Produktion an Windstrom – Tendenz steigend.

Positiv hinzu kommt: Wir als Entwickler und Betreiber von globalen Infrastrukturlösungen sind in der Lage, auf Basis der beim Bitcoin-Mining gesammelten wertvollen Erfahrungen auch jede andere Anwendung des High-Performance-Computings für unsere Kunden zu realisieren. Diese Innovationen gehen längst weit über Bitcoin hinaus und betreffen längst auch Berechnungen in Bereichen wie Deep Learning, künstlicher Intelligenz oder Rendering. ‹

Aroosh Thillainathan
ist CEO der Northern Data AG mit Sitz in Frankfurt am Main.