«Ich wäre nicht überrascht, wenn Bitcoin verboten würde»

ETH-Informationstechnologe Roger Wattenhofer über den Energiebedarf der Kryptowährung und bessere Alternativen

Bitcoin-Mining in der Inneren Mongolei: Noch ist das Schürfen einträglich

Foto: Getty Images

Prof. Dr. Roger Wattenhofer vom Departement Informationstechnologie und Elektrotechnik der ETH Zürich

Joachim Laukenmann

Der mit dem Bitcoin-Boom einhergehende Stromverbrauch, heisst es, gefährde die Energiewende. Das ist doch kompletter Unsinn, oder?

Ob die Energiewende gefährdet ist, das weiss ich nicht. Das ist nicht mein Fachgebiet. Sicher ist aber, dass der Energieverbrauch von Bitcoin riesig ist.

Warum verschlingt diese Kryptowährung viel Energie?

Das hat mit ihrer Konstruktion zu tun. Wie bei unserer normalen Währung haben wir auch bei Bitcoin Transaktionen: Person A möchte Geld an Person B überweisen. Wenn man physisches Geld nimmt, dann ist das eine klare Sache: Person A kann das Geld nur Person B geben und nicht gleichzeitig einer Person C. Bei einer Kryptowährung sind aber nur Zahlen im Spiel. Daher kann Person A das gleiche Geld im Prinzip an Person B und an Person C überweisen. Diese Doppelausgaben sind ein Grundproblem der Kryptowährungen.

Okay, aber wo steckt hier die Energie?

In der Lösung des Problems der Doppelausgaben. Bitcoin ist so konstruiert, dass keine Bank entscheidet, welche der beiden Transaktionen auch wirklich durchgeführt wird. Diese Machtkonzentration wollte man vermeiden. Daher entscheidet ein ganzes Netzwerk von Rechnern über die Transaktionen. Zunächst wandern alle Transaktionen ins Bitcoin-Netzwerk und dort in einen sogenannten Block. Sich widersprechende Transaktionen wie versuchte Doppelausgaben sind in verschiedenen Blöcken. Dann müssen sich die Rechner einig werden, welche Blöcke auch tatsächlich durchgeführt werden.

Und wie geht das?

Indem alle Rechner im Bitcoin-Netzwerk versuchen, ein mathematisches Rätsel zu knacken. Wer das Rätsel löst, darf einen Block mit Transaktionen an die sogenannte Blockchain anhängen. Das macht es sehr schwierig, die totale Kontrolle über das Bitcoin-Netzwerk zu kriegen. Man müsste dazu mehr Rechenleistung reinstecken als alle anderen Teilnehmer zusammen.

Und die Rechenleistung, die es braucht, um ein Rätsel nach dem anderen zu knacken, verschlingt Energie.

Genau. Früher hat man einfache Desktop-Computer genommen. Heute nutzt man spezielle Hardware, die nichts anderes kann, als diese Rätsel zu lösen. Es gibt ganze Lagerhallen voller Bitcoin-Rechner. Denn die Lösung des Rätsels – mathematisch gesprochen muss man eine sogenannte Hash-Funktion berechnen – ist mittlerweile sehr schwierig. Die Komplexität der Aufgabe wird so gewählt, dass im Mittel nur alle zehn Minuten ein Rechner die Lösung findet und somit einen Block anhängen kann. Zum Vergleich: Es ist viel wahrscheinlicher, direkt zweimal hintereinander das Schweizer Zahlenlotto zu gewinnen, als das Hash-Rätsel zu lösen.

Warum lohnt es sich, in diese Rechenzentren zu investieren?

Weil man Geld verdient, wenn man das Rätsel knackt. Mit jeder gelösten Hash-Funktion erhält man als Belohnung die Gebühren für die Transaktionen im jeweiligen Block plus derzeit 12,5 neue Bitcoins. Daher bezeichnet man das Lösen der Hash-Funktion auch als Mining: Die 12,5 Bitcoins werden neu geschaffen.

Das bedeutet, dass man alle zehn Minuten 12,5 Bitcoins schürfen plus die Transaktionsgebühren einstreichen kann.

Exakt. Bei einem Wert von 17 000 Franken pro Bitcoin sind das alle zehn Minuten mehr als 200 000 Franken plus die Transaktionsgebühren. Pro Stunde lassen sich also mehr als 1,2 Millionen Franken verdienen.

Das ist ein ganz ordentlicher Markt.

Klar. Man muss zwar Kosten für die Hardware, für den Strombedarf der Rechner und deren Kühlung aufbringen. Aber wenn der Strom günstig genug ist, dann lohnt sich das. Wegen des billigen Stroms stehen die Rechenzentren vorwiegend in China. Dort gibt es aber viel Kohlestrom, der wegen der CO_2-Emissionen für eine schlechte Klimabilanz sorgt.

Können Sie beziffern, wie viel Energie Bitcoin heute benötigt?

Genau weiss man das nicht. Aber man kann den Energiebedarf auf verschiedene Arten abschätzen. Man weiss, wie viele Rätsel pro Sekunde gelöst werden, und wie viel Energie die effizienteste Hardware für das Lösen der Rätsel benötigt. Damit kommt man auf circa 1,3 Gigawatt. Die reale Leistung ist sicher höher, da man die Geräte auch noch kühlen muss, und nicht alle die beste Hardware benutzen. Anderseits: Wenn man die 1,2 Millionen Franken pro Stunde durch die Stromkosten in China von circa 8 Rappen pro Kilowattstunde teilt, erhält man circa 15 Gigawatt elektrische Leistung. Wenn man mehr als 15 Gigawatt aufwendet, lohnt sich das Mining nicht mehr. Wenn der Wert darunter ist, dann lohnt es sich, neue Hardware zu kaufen und anzuschliessen.

Was heisst das für den tatsächlichen Energieverbrauch?

Das heisst: Um Bitcoin zu betreiben, braucht es derzeit mindestens ein, maximal 15 Kernkraftwerke wie Leibstadt mit einer Leistung von rund einem Gigawatt. Die Wahrheit liegt wohl irgendwo in der Mitte, bei vier bis fünf Gigawatt oder Kernkraftwerken. Das entspricht ungefähr dem Strombedarf der Schweiz.

Und wenn man das auf eine Überweisung umrechnet?

Dann erhält man eine unfassbar hohe Zahl: Eine einzige Bitcoin-Überweisung verschlingt etwa 250 Kilowattstunden elektrische Energie. Das heisst: Zehn Bitcoin-Überweisungen benötigen so viel Strom wie ein durchschnittlicher Schweizer Zwei-Personen-Haushalt in einem ganzen Jahr.

Wo führt das hin?

Wenn sich der Wert eines Bitcoins verdoppelt, dann kann man erwarten, dass sich auch der Stromverbrauch verdoppelt. Alle vier Jahre ist es immerhin so, dass die Anzahl neuer Bitcoins pro Block halbiert wird, beim nächsten Mal von 12,5 auf 6,25 Bitcoins. Ein Bitcoin-Miner kriegt dann etwas weniger Geld, und es lohnt sich nicht mehr so sehr, den Aufwand zu betreiben. Aber wenn sich der Bitcoin-Preis jedes Jahr verdoppelt, dann nützt das wenig. Dann wird es immer attraktiver, neue Rechenzentren zu bauen. Der Strombedarf steigt folglich weiter an. Irgendwann landet man vielleicht bei 100 Gigawatt.

Das würde der Leistung von rund hundert Kernkraftwerken entsprechen – oder der gleichen Menge an Kohlestrom. Gibt es Alternativen?

Ja, es gibt Methoden, die würden fast keinen Strom verbrauchen. Ich unterrichte sie seit Jahren unseren Studenten. Die Person, die Bitcoin erfunden hat, war offenbar nicht in meiner Vorlesung! Neue Kryptowährungen versuchen, diese bekannten und bewährten Methoden in die Praxis umzusetzen. Damit entfällt die irrsinnige und unnötige Rechenleistung für das Lösen der Rätsel.

Was bedeutet das wohl für die Zukunft von Bitcoin?

Das Bitcoin-Protokoll sollte sich reformieren. Allerdings ist das schwierig, da die Miner gut verdienen und eine Reform nicht unterstützen würden. Ich wäre nicht überrascht, wenn Staaten sich entschliessen würden, Bitcoin ganz zu verbieten. Das ist aber auch nicht einfach, da Bitcoin vollkommen anarchisch ist.

Besitzen Sie Bitcoin?

Nein. Ich besitze keine Kryptowährungen. Ich interessiere mich nur beruflich dafür.

Wichtige Begriffe: Miner, Blockchain und Wallet

BITCOIN Das ist eine digitale Währung. Im Gegensatz zum herkömmlichen Zahlungsverkehr werden keine zentralen Abwicklungsstellen, also keine Banken, benötigt. Überweisungen werden von Rechnern getätigt, die über das Internet verknüpft sind. Das Bitcoin-Zahlungssystem wurde 2008 in einem unter dem Pseudonym Satoshi Nakamoto veröffentlichten Dokument beschrieben. Welche reale Person oder welche Gruppe von Personen dahintersteckt, ist nicht bekannt.

BLOCK Das ist ein Datensatz, der circa 2000 ausstehende Bitcoin-Überweisungen enthält.

MINER Sie sammeln noch nicht erfasste Transaktionen und bündeln sie in einem Block. Dann führen sie aufwendige mathematische Berechnungen durch, um die Bitcoin-Transaktionen zu bestätigen. Als Belohnung für ihre Dienste erhalten Miner die Transaktionsgebühren für die von ihnen bestätigten Transaktionen sowie pro Block 12,5 neu erschaffene (geschürfte) Bitcoins.

BLOCKCHAIN Das ist eine öffentliche Liste aller bestätigten Blöcke in chronologischer Reihenfolge, also aller Bitcoin-Transaktionen. Im Durchschnitt wird etwa alle zehn Minuten ein neuer Block mitsamt den Transaktionen an die Blockchain angehängt.

WALLET Das ist die Brieftasche beim Bitcoin, also der Ort, von dem aus man Bitcoins empfängt, speichert oder sendet.