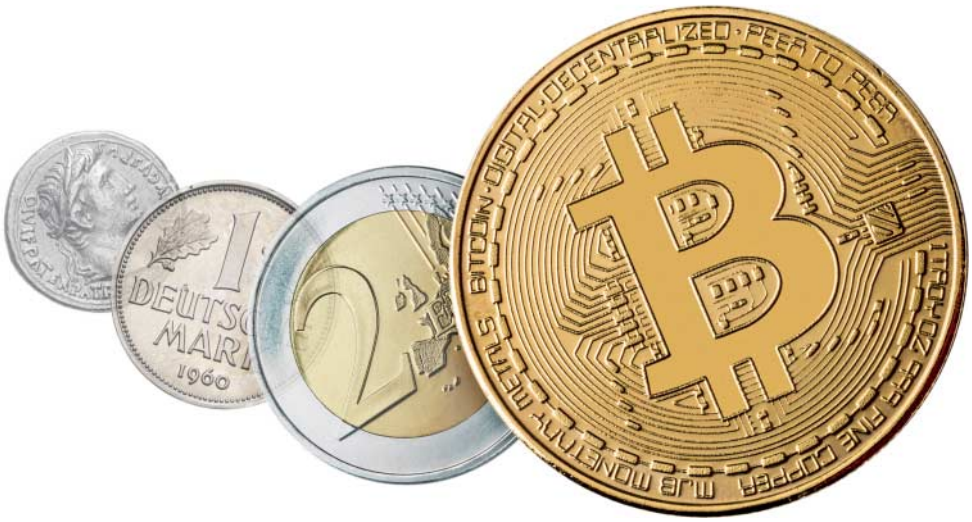

Unerwünschte Evolution

Wie Bitcoin Gold und Zcash um ihre Freiheit kämpfen

Nach dem Todesstoß durch einen 51-Prozent-Angriff, mutmaßlich mit neuen ASIC-Minern ausgeführt, soll ein Hard-Fork mit einem neuen Hash-Algorithmus die Kryptowährung Bitcoin Gold retten. Auch Zcash droht durch die Auslieferung der ersten ASIC-Miner für den Equihash-Algorithmus eine fundamentale Änderung der Machtverhältnisse.

Von Mirko Dölle

Der Angriff mit einer übermächtigen Mining-Farm auf Bitcoin Gold Ende Mai war eigentlich das Ende der Kryptowährung. Bis zu fünf Mal mehr Hash-Leistung als das reguläre Miner-Netzwerk sollen die Betrüger aufgeboten und so Bitcoin Gold drei Tage lang nach Belieben manipuliert haben. Nur wenige Tage später verschickte der chinesische Mining-Hardware-Spezialist Bitmain tausende Miner einer neuen Generation für Kryptowährungen mit Equihash-Algorithmus – zu denen neben Bitcoin Gold auch Zcash gehört.

Bei den Bitcoin-Gold-Entwicklern kam schnell der Verdacht auf, dass eben diese ASIC-Miner an dem Angriff beteiligt gewesen sein dürften – zumal die Zcash-Foundation und die Uni Luxemburg in einer Studie zu dem Ergebnis kamen, dass bereits im Mai 20 bis 30 Prozent der Hash-Leistung von ASIC-Minern bereitgestellt wurden.

Als ASIC-Miner bezeichnet man Miner, die anstelle von herkömmlichen CPUs oder GPUs speziell auf einen Hash-Algorithmus optimierte Prozessoren (Application-Specific Integrated Circuit, ASIC) verwenden. Durch die Spezialisierung und Optimierung auf genau eine Aufgabe arbeiten diese ASICs sehr viel schneller und effizienter als General-Purpose-Prozessoren für Rechner und Grafikkarten – und beim Mining ist die Effizienz, also eine möglichst hohe Hash-Rate bei gleichzeitig geringem Energieverbrauch, das wichtigste Kriterium.

Neue Spezies

Neu sind ASIC-Miner an sich nicht. Sie lösten bei Bitcoin bereits Anfang 2013 die weniger effizienten FPGA-Miner (Field Programmable Gate Array) ab, die ihrerseits zuvor die ineffizienteren Grafikkarten-Miner und die reinen CPU-Miner in Rente geschickt hatten. Damit veränderte sich jedoch gleichzeitig das Machtgefüge unter den Minern: Wurden die Bitcoin-Blöcke in den ersten Jahren überwiegend von Privatpersonen auf den CPUs und Grafikkarten ihrer heimischen PCs erzeugt, waren es überwiegend große Mining-Farmen, die FPGA- und ASIC-Miner kauften und betrieben. Heute werden über 75 Prozent aller Blöcke der Bitcoin-Blockchain in den Farmen der Betreiber BTC.com, AntPool, ViaBTC, SlushPool, BTC.TOP und F2Pool von Minern des Herstellers Bitmain erzeugt. Und da bei Veränderungen an der Kryptowährung die Miner das Sagen haben, wird Bitcoin heute praktisch von einem halben Dutzend Firmen kontrolliert.

Um die Macht in den Händen der Enthusiasten und Investoren zu halten, entschieden sich die Entwickler der Kryptowährungen Zcash und Bitcoin Gold für den Hash-Algorithmus Equihash, der sich gut auf Grafikkarten rechnen oder verarbeiten lässt, sich aufgrund der hohen Speicheranforderungen aber nicht wirtschaftlich auf ASICs berechnen lassen sollte. So waren Mining-Farmen gezwungen, Consumer-Grafikkarten für ihre Miner zu kaufen, was teuer und aufgrund der geringen Liefermengen der Hersteller schwierig war.

Die Rechnung der Kryptogeldentwickler schien aufzugehen – bis Bitmain Ende 2017 den Antminer Z9 mini für Equihash ankündigte, der zehn Mal effizienter sein sollte als Grafikkarten. Ein halbes Jahr später kam es zur Auslieferung und zum fatalen Angriff auf Bitcoin Gold.

Wiederbelebung

Doch die Entwickler wollten die Kryptowährung angesichts eines Marktvolumens von 500 Millionen US-Dollar nicht verloren geben. Hastig entwickelten sie einen

neuen Hash-Algorithmus und führten ihn Anfang Juli im Rahmen eines Hard-Forks ein. Der neue Algorithmus ist nicht nur 15 Mal schwerer zu berechnen, er braucht außerdem viel mehr Speicher als Equihash – und mehr Speicher macht die ASICs sehr viel teurer und ineffizienter. Bitcoin Gold soll nunmehr sicher vor neuen 51-Prozent-Angriffen und weiterhin unter der Kontrolle von Grafikkarten-Minern sein.

Die Zcash-Foundation ist hingegen noch in der Beratungsphase und hat bislang nicht entschieden, wie sie den drohenden Generationenwechsel hin zu ASIC-Minern und die damit verbundene Zentralisierung der Macht bei wenigen Mining-Farm-Betreibern verhindern will. Bitmain hat jedoch seit Ende Mai über 10.000 Antminer Z9 ausgeliefert, die zusammengenommen gut 20 Prozent der gesamten Hash-Leistung des Zcash-Miner-Netzes besitzen.

Die nächste Charge Antminer Z9 befindet sich bereits in Produktion und soll Ende August verschickt werden. Solange die ASIC-Miner zehn Mal so effizient sind wie gleichteure Grafikkarten, werden weitere Mining-Farmen die neuen Antminer kaufen. So droht Zcash die gleiche Explosion der Hash-Leistung, wie sie bei Bitcoin schon vor Jahren stattfand und noch immer andauert.

Problematische Anreize

Ein Grund für die immer noch steigende Zahl der Bitcoin-Miner ist, dass Mining weiterhin ein gutes Geschäft ist. Eigentlich müssten sich die Miner allein aus den Gebühren der von ihnen verarbeiteten Transaktionen finanzieren. Doch diese betragen aktuell nicht einmal 0,15 Bitcoin pro Block, das sind umgerechnet deutlich weniger als 1000 Euro. Den Löwenanteil macht die Belohnung (Reward) aus, also die Subvention, die jeder Miner zusätzlich für jeden von ihm gefundenen Block erhält. Sie liegt bei aktuell 12,5 Bitcoin oder rund 70.000 Euro pro Block.

Im Dezember 2017 bekamen die Miner, bedingt durch den Wechselkurs und durch die Exzesse bei den Transaktionsgebühren, bis zu 25 Bitcoins im Wert von 350.000 Euro für jeden neuen Block – kein Wunder, dass die Bestellungen beim Hersteller Bitmain explodierten und Mining-Farmen wie Pilze aus dem Boden schossen.

Die Subvention ist ein Überbleibsel aus den Anfangstagen des Bitcoin. Sie wurde von Satoshi Nakamoto eingeführt, um die Kryptowährung ohne ein Initial Coin Offering (ICO) oder Pre-Mining allein durch den Betrieb der Miner entstehen zu lassen. So erhielt er als Belohnung für die Veröffentlichung des ersten Blocks der Bitcoin-Blockchain die ersten Bitcoins geschenkt. Um die Blockchain und damit die Kryptowährung am Leben zu erhalten, mussten jedoch weiterhin im Abstand von 10 Minuten neue Blöcke berechnet werden – die Belohnung sollte dafür den notwendigen Anreiz schaffen, damit überhaupt jemand Strom und Zeit in den Betrieb eines Bitcoin-Miners investierte.

Doch das Ende ist absehbar: Mit Block Nummer 630.000, der voraussichtlich Ende Mai 2020 erreicht wird, halbiert sich die Belohnung von aktuell 12,5 auf 6,25 Bitcoin – und weitere 210.000 Blöcke oder vier Jahre später erneut auf dann 3,125 Bitcoin. Das Gleiche gilt für Bitcoin Gold und andere Bitcoin-Forks.

Schwieriger Sparkurs

Sofern sich der Bitcoin-Kurs nicht simultan verdoppelt, werden die Miner ihre Kosten entsprechend senken oder sich vermehrt über die Transaktionsgebühr finanzieren müssen. Der größte Kostenposten bei Minern ist Strom, weshalb sich in der Vergangenheit viele Miner in China niedergelassen haben, wo die Kilowattstunde mitunter nur 2 Cent kostet. Doch diese Zeiten sind absehbar vorbei, die chinesische Regierung hat den landesweiten Ausstieg aus dem Mining verkündet und die Farmen müssen in andere Gegenden mit höheren Strompreisen umziehen. Hier ist also sogar von einer Kostensteigerung auszugehen.

Eine andere Einsparmöglichkeit wäre der Einsatz effizienterer Miner, die mit gleicher Leistungsaufnahme mehr Hash-Leistung liefern. Durch die jetzt ausgelieferten ASIC-Miner für Equihash hat sich bei der Kryptowährung Zcash gerade ein großes Potenzial eröffnet: So liegt die Leistungsaufnahme des neuen Antminer Z9 bei nur gut 30 Watt für 1000 Sol/s (Solutions per Seconds, entspricht Hashes pro Sekunde), während die bisher gängigen Miner mit Grafikkarten gut 250 Watt für 1000 Sol/s benötigen.

Bei Bitcoin hingegen arbeiten die Mining-Farmen bereits seit vielen Jahren mit ASIC-Minern. Die Fertigung der Chips ist inzwischen auf dem Niveau großer Prozessorhersteller wie Intel oder Nvidia angekommen. Mit einem großen Sprung bei der Hash-Leistung ist nicht mehr zu rechnen.

Mining-Farmen werden es daher schwer haben, in den nächsten Jahren ihre laufenden Kosten zu senken. Das Geschäft wird mit sinkender Subvention immer weniger rentabel, weshalb davon auszugehen ist, dass es weniger neue Miner geben und deshalb die Hash-Rate nicht mehr so stark ansteigen wird wie bisher.

Langfristig müssen die Transaktionsgebühren alle (Strom-)Kosten der Miner decken. Heute würde dies einen Anstieg von aktuell 0,15 BTC pro Block um den Faktor 50 auf 5 bis 10 BTC pro Block bedeuten – ab dieser Schwelle sind viele Miner profitabel. Eine einzelne Überweisung müsste sich dadurch von derzeit etwa 8 Cent auf 4 Euro verteuern, komplexe Überweisungen mit mehreren Adressen würden schnell 15 bis 20 Euro kosten. Es ist unwahrscheinlich, dass die Bitcoin-Nutzer auf Dauer solch hohe Transaktionsgebühren akzeptieren.

Das bedeutet jedoch nicht das baldige Ende des Bitcoin als Kryptowährung: So gibt es mit dem Lightning Network bereits eine etablierte Alternative, um Bitcoins ganz ohne Transaktionsgebühr zu überweisen. Außerdem könnten die Blöcke vergrößert werden, sodass mehr Transaktionen pro Block abgewickelt und damit auch mehr Transaktionsgebühren kassiert werden. Bitcoin Cash hat einen solchen Fork erst vor Kurzem durchgeführt und die Größe auf 32 MByte pro Block erhöht. Die steigende Abhängigkeit von den Transaktionsgebühren dürfte trotzdem dazu führen, dass der Gesamtstromverbrauch der Bitcoin-Miner weltweit langfristig sinkt, damit Bitcoin-Transaktionen bezahlbar bleiben. *(mid@ct.de)* c't