Kettenreaktion

Wie 51-Prozent-Angriffe Bitcoin & Co. bedrohen

In einem groß angelegten Angriff haben Kriminelle die Kontrolle über Bitcoin Gold an sich gerissen – der Super-GAU für Kryptowährungen. Damit ist Bitcoin Gold eigentlich Geschichte. Doch Totgesagte leben erschreckend lange.

Von Mirko Dölle

Die Kernschmelze von Bitcoin Gold begann am 16. Mai zur Mittagszeit: Kriminelle Angreifer ließen gezielt den Hauptzweig der Blockchain absterben, um darin enthaltene Transaktionen ungeschehen zu machen. Der Angriff galt dem verwundbarsten Punkt von Bitcoin Gold, den es in gleicher Weise bei Bitcoin, allen Bitcoin-Forks sowie den meisten anderen Kryptowährungen mit dezentraler Blockchain gibt. Bitcoin-Erfinder Satoshi Nakamoto beschrieb ihn bereits 2009: Sie führten eine sogenannte 51-Prozent-Attacke aus, indem sie die Mehrheit der Hash-Leistung weltweit unter ihre Kontrolle brachten. Auf diese Weise konnten sie Händler von Kryptowährungen um mehrere Millionen US-Dollar betrügen – und könnten das jederzeit wiederholen.

Längenvergleich

Der wunde Punkt von Bitcoin & Co. ist, dass die Blockchain dieser Kryptowährungen dezentral und von allen Minern eigenständig fortgeführt wird. Das Design sieht explizit keine zentrale Instanz vor, bei der sich Miner die aktuell gültige Blockchain herunterladen könnten. Stattdessen besorgen sich die Miner aus dem Bitcoin-Netz die längste bekannte Blockchain.

Die längste Kette müsste theoretisch auch die aktuellste sein: Der Schwierigkeitsgrad (Difficulty) wird alle 2016 Blöcke so angepasst, dass es genau zwei Wochen dauert, weitere 2016 Blöcke zu berechnen. So kommen Bitcoin und Bitcoin Gold auf eine reguläre Blockzeit von zehn Minuten. Ist eine Blockchain kürzer als eine andere, ist sie potenziell mehrere Minuten älter und damit überholt.

In der Praxis passiert es gelegentlich, dass zwei Miner nahezu gleichzeitig zwei verschiedene Lösungen für den aktuell gesuchten Block finden. Dann gibt es zunächst zwei gültige, gleich lange Blockchains, die sich nur im letzten Block unterscheiden. Beide verbreiten sich gleichzeitig im Bitcoin-Netz, sodass ein Teil der Miner mit der einen und der Rest mit der anderen Blockchain weiterarbeitet.

Welche Blockchain sich durchsetzt, hängt davon ab, für welche der beiden Ketten zuerst neue Blöcke gefunden werden – die Blockchain mit den meisten Blöcken überlebt, die andere stirbt ab. In seltenen Fällen gelingt es den Minern, nahezu gleichzeitig für beide Blockchains weitere Blöcke zu finden, dann spricht man von Zweigen. Mitte 2015 etwa wurden für drei aufeinander folgende Blöcke der Bitcoin-Blockchain jeweils zwei Lösungen gefunden, bevor der Block 364000 die Entscheidung brachte und den anderen Zweig absterben ließ.

Absolute Mehrheit

Sollte jemand die Mehrheit der Miner einer Blockchain unter seine Kontrolle bringen, könnte er sich zum Alleinherrscher über die Kryptowährung aufschwingen: Mit 51 Prozent der Hash-Leistung und mehr könnte er sicher sein, auf Dauer mehr neue Blöcke zu finden als der Rest des Netzwerks. Seine Blockchain wäre also stets länger als die der übrigen Miner, deren Zweige regelmäßig absterben würden.

Stirbt ein Zweig der Blockchain ab, so werden alle darin enthaltenen Blöcke und Transaktionen gegenstandslos. Es ist, als hätten die Transaktionen nie stattgefunden, da sie in der aktuell gültigen Blockchain nicht mehr enthalten sind. So könnte sich der 51-Prozent-Angreifer aussuchen, welche Transaktionen er berücksichtigt oder die Kryptowährung sogar komplett zerstören, indem er nur noch leere Blöcke

ohne Transaktionen veröffentlicht – womit der Handel vollständig zum Erliegen käme und die Währung schlagartig wertlos würde. Ein 51-Prozent-Angriff ist deshalb der Super-GAU jeder Kryptowährung mit dezentraler Blockchain.

Under Cover

Der Angriff auf Bitcoin Gold war jedoch nicht auf die Zerstörung der Währung ausgerichtet, sondern diente dazu, Geld zu stehlen: Dazu mieteten sich die Ganoven Miner, die über sehr viel mehr Hash-Leistung als das offizielle Bitcoin-Gold-Netzwerk verfügten. Manche sprechen von bis zu 170 Mega-Hashes pro Sekunde (MH/s), die die Kriminellen zur Verfügung gehabt haben sollen – während das öffentliche Miner-Netz nur über gut 30 MH/s verfügte.

So konnten die Kriminellen die Kryptowährung nach Belieben kontrollieren. Doch anstatt den ersten neuen Block unmittelbar zu veröffentlichen, nachdem er gefunden wurden, ließen sie nur die Miner ihrer geheimen Farm mit dem gerade gefundenen Block weiterarbeiten und Nachfolgeblöcke berechnen, die wiederum nicht veröffentlicht wurde. So entstand ein geheimer Zweig der Bitcoin-Gold-Blockchain, der länger war als der Zweig der offiziellen Blockchain.

Gleichzeitig verkaufte man öffentlich große Mengen Bitcoin Gold an Händler, blockierte diese Transaktionen jedoch bei den geheimen Minern, sodass sie von fremden Minern verarbeitet und Teil des offiziellen Zweigs der Blockchain wurden.

Anschließend verkauften die Gauner dieselben, bereits verkauften Bitcoin Gold an einen anderen Händler – ließ diese Transaktion aber nur von den eigenen Minern verarbeiten, die von dem ersten Verkauf nichts wussten. Somit wurde der zweite Verkauf Teil der geheimen Blockchain.

Double Spend

Erst jetzt veröffentlichten die Ganoven ihre geheime Blockchain. Da sie länger war als die bisher bekannte, wurde die vormals geheime Blockchain augenblicklich zur einzig gültigen. Der andere Zweig, der den ersten Verkauf der Bitcoin Gold enthielt, starb ab – und damit verschwand der Erstverkauf der Bitcoin Gold, als hätte es ihn nie gegeben.

Das Perfide war, dass die Gauner den zweiten Verkauf in ihre vormals geheime Blockchain aufnahmen, die Coins also offiziell bereits ausgegeben waren. Damit verhinderten sie, dass ein Händler eine Kopie der ursprüngliche Transaktion erneut ins Bitcoin-Netz übertragen und so doch noch an sein Geld kommen konnte.

Dieses Spiel wiederholten die Gauner in der Zeit vom 16. bis zum 18. Mai mehrfach und erbeuteten so Schätzungen zufolge 18 Millionen US-Dollar, bevor sie ohne erkennbaren Grund aufhörten. Teilweise waren die geheimen Zweige 50 Blöcke lang, sodass selbst längere Karenzzeiten wirkungslos blieben. Den Schaden haben die Händler der Kryptowährungen, die etwas ausbezahlt, aber letztlich nichts dafür erhalten haben.

Crash voraus?

Erschreckend ist auch, dass dieser Angriff keine Auswirkungen auf den Kurs der Kryptowährung hatte. Inzwischen ist die durchschnittliche Hash-Leistung der Bitcoin-Gold-Miner auf etwa 25 MH/s gefallen, sodass die Gauner es sogar noch leichter hätten, den Angriff zu wiederholen oder Bitcoin Gold jederzeit auszulöschen. Die Investoren scheint dieser drohende Totalverlust nicht zu interessieren, bei Redaktionsschluss lag die Marktkapitalisierung von Bitcoin Gold noch immer bei rund 500 Millionen US-Dollar.

Und nicht nur Bitcoin Gold ist betroffen, auch Bitcoin Cash und andere Kryptowährungen mit wenigen Minern sind real bedroht: Die Hash-Leistung der Bitcoin-Cash-Miner etwa beträgt nur zehn Prozent der Hash-Leistung der Bitcoin-Miner.

Würden nur zehn Prozent der Bitcoin-Miner koordiniert auf Bitcoin Cash schwenken, könnten sie dort dieselben Angriffe durchführen wie bei Bitcoin Gold – der Schaden wäre bei einer Marktkapitalisierung von rund 15 Milliarden US-Dollar jedoch um ein Vielfaches größer. Schützen kann man sich davor nicht. Das einzige Gegenmittel wäre, die Betrüger per Hard Fork der Blockchain wieder zu enteignen, so wie es Ethereum nach dem DAO-Hack tat. Doch dafür bräuchte man die Mehrheit unter den Minern. *(mid@ct.de)* c't