Verschwindibus

Wie abgeschlossene Transaktionen aus der Blockchain verschwinden

Für alle Zeiten unveränderlich und durch millionenfache Kopien nicht auszumerzen – was in der Blockchain steht, ist wie in Stein gemeißelt. Denkt man. Und doch verschwinden immer wieder bereits ausgeführte Transaktionen, als hätte es sie nie gegeben. Das ist aber nicht das Werk von Gaunern, sondern des Bitcoin-Erfinders.

Von Mirko Dölle

Es spukt von Zeit zu Zeit in der Blockchain: Gerade hat man noch im Bitcoin-Client mit eigenen Augen beobachtet, wie eine Überweisung zum zweiten Mal bestätigt wurde – doch wenige Minuten später ist das Geld verschwunden, als hätte es die Transaktion nie gegeben. War das eine Halluzination? Oder eher ein Bug im Bitcoin-Client? Nichts dergleichen, sondern purer Zufall – oder der Versuch einer Mining-Farm, schnelles Geld zu machen.

Verstorben und vergessen

Bitcoin-Transaktionen können dann verschwinden, wenn einzelne Blöcke oder ganze Zweige der Blockchain absterben, in denen die Transaktionen für alle Welt sichtbar verbucht wurden. Das klingt paradox, ist doch die grundlegende Funktion der Blockchain, alle Blöcke und alle darin enthaltenen Transaktionen auf ewig unverlierbar und unveränderbar aufzubewahren. Tatsächlich enthält die Blockchain aber nur Blöcke, die aktuell eine Relevanz besitzen. Das sind all jene, die in der Kette vom zuletzt hinzugefügten Block rückwärts bis zum Genesis-Block aus 2009 vorkommen.

Der Knackpunkt ist, dass jeder Miner seine eigene Kopie der Blockchain besitzt, weil das Bitcoin-Netzwerk ein Peer-to-Peer-Netzwerk ohne eine zentrale Instanz ist. Findet ein Miner den aktuell gesuchten Block, etwa die Nummer 363997, so verbreitet er ihn über das Miner-Netzwerk an seine Nachbarn. Die Nachbarn hängen den Block 363997 an ihre Kopie der Blockchain an und verbreiten ihn wiederum an ihre Nachbarn weiter.

Außerdem brechen die Nachbarn des Finders ihre aktuell laufenden Schürfarbeiten ab, schließlich wurde der von ihnen gesuchte Block 363997 ja gerade gefunden, und entfernen die in dem neuen Block abgearbeiteten Transaktionen aus ihrem lokalen Mempool. Anschließend beginnen sie damit, den Block 363998 zu suchen, der als Vorgänger-ID die ID (genauer: den Hash-Wert) des gerade eingetroffenen Blocks 363997 enthält.

Stille Post modern

Die Netzwerktopologie sorgt dafür, dass sich die Kunde von dem neuen Block Nummer 363997 erst nach und nach im Bitcoin-Netzwerk verbreitet. Das kann in der Praxis einige Minuten dauern. In dieser Zeit versucht ein Teil der Miner weiterhin, eine eigene Lösung für den Block 363997 zu errechnen. Und manchmal haben sie damit Erfolg.

Dann verbreitet der zweite Finder seine Version des Blocks Nummer 363997 ebenfalls an alle seine Nachbarn, die von dem Erstfund noch nichts mitbekommen haben. Die Nachbarn hängen diese Version von Block 363997 an ihre Blockchain-Kopie an, verbreiten ihn weiter und beginnen sofort, den Block 363998 mit Referenz zum gerade empfangenen Block 363997 zu suchen.

So kommt es zu einer Spaltung der Blockchain: Ein Teil der Miner versucht, auf Basis der ersten Version von Block 363997 den nächsten Block 363998 zu finden, und der Rest auf Basis der zweiten Version. Da eine korrekte Altersbestimmung ohne eine zentrale Referenz unmöglich ist, können die Miner nicht einmal feststellen, welcher Block der Erstfund und welcher der Zweitfund war. Deshalb berücksichtigen sie stets nur den Block, von dem sie über ihre Nachbarn zuerst gehört haben.

Der mutmaßliche Bitcoin-Erfinder Satoshi Nakamoto hat diese Situation vorhergesehen und in den Regeln der Kryptowährung berücksichtigt: In der Blockchain landet stets der Block, der die meisten Nachfolger aufweist. Somit sind zunächst beide Blockchains mit beiden Versionen von Block 363997 gültig, denn

es hat noch niemand den Block 363998 gefunden. Findet ein Miner den Block 363998 und referenziert darin den Erstfund von Block 363997 als Vorgänger, so hat die erste Version von Block 363997 einen Nachfolger, die zweite Version aber nicht – weshalb die zweite Version von Block 363997 abstirbt und zu einem sogenannten Stale Block wird. Sobald Block 363998 im ganzen Miner-Netz verbreitet wurde, arbeiten alle Miner wieder mit derselben Blockchain.

Hin und wieder weg

Das Absterben eines Blocks hat massive Auswirkungen auf die Bitcoin-Nutzer, deren Transaktionen darin enthalten waren: So haben die Bitcoin-Clients die Transaktionen des Blocks bereits als einfach bestätigt und damit abgewickelt angezeigt. Da der Block jedoch gestorben ist und durch den überlebenden ersetzt wurde, verschwinden diese zuvor als bestätigt angezeigten Transaktionen mit Ankunft des überlebenden Blocks, als hätte es nie eine Bestätigung gegeben.

Außerdem haben die Miner, die den gerade verstorbenen Block in ihre Blockchain aufgenommen hatten, die im Block enthaltenen Transaktionen bereits aus ihrem Mempool gelöscht, in dem die anstehenden Transaktionen auf ihre Bearbeitung warten. Das bedeutet schlimmstenfalls, dass die im verstorbenen Block gelisteten Transaktionen im Nirvana verschwinden, als wären sie nie abgeschickt worden – weshalb der Absender die Transaktion noch einmal versenden muss.

Eigentlich soll die Difficulty der Blockchain (siehe c't 7/2018, S. 16) verhindern, dass mehrere Miner nahezu gleichzeitig gültige Blocke finden. Der Schwierigkeitsgrad wird automatisch alle zwei Wochen so angepasst, dass die Miner durchschnittlich zehn Minuten benötigen, bis der erste einen passenden Block findet.

Durch Zufall oder weil kurzfristig sehr viele zusätzliche Miner in Betrieb gehen, kann es aber zu Doppelfunden kommen. In der Praxis passiert dies alle paar Monate, dann aber aufgrund der verzögerten Anpassung der Difficulty meist mehrfach innerhalb weniger Tage.

Kettenreaktion

Deutlich seltener ist, dass ganze Zweige mit mehreren Blöcken absterben, so wie in der Abbildung unten, die einen Ausschnitt aus der Blockchain von Mitte 2015 zeigt. Damals entstanden nicht nur zwei Blöcke mit der Nummer 363997, die das Bitcoin-Netzwerk spalteten. In den beiden Zweigen wurden auch für die Blöcke 363998 und 363999 jeweils zwei gültige Lösungen gefunden. Erst Block 364000, der nur einmal gefunden wurde, brachte die Entscheidung und ließ den aus drei Blöcken bestehenden ersten Zweig endgültig absterben. Die Blöcke des Zweigs werden als orphaned (verwaist) bezeichnet, auch wenn der erste strenggenommen ein Stale Block ist.

Weil solche Zweige durchaus mehrere Blöcke lang sein können, darf man nicht darauf vertrauen, eine Bitcoin-Zahlung endgültig erhalten zu haben, wenn die Transaktion im letzten oder vorletzten Block der Blockchain aufgeführt ist. Der Bitcoin-Client Electrum etwa verbucht Transaktionen erst dann, wenn der Block mit der Transaktion fünf weitere Blöcke als Nachfolger hat – was gut eine Stunde dauern sollte. Das bremst allerdings auch den Handel aus: Wer einen Kaffee mit Bitcoins bezahlt, müsste bei Electrum eine ganze Stunde warten, bis die Zahlung verbucht ist und er ihn serviert bekommt.

Doch selbst damit ist man nicht unbedingt auf der sicheren Seite: Am 4. Juli 2015 gab es ab Block Nummer 363730 sogar einen Zweig mit sieben Transaktionen, der anschließend abstarb. So verschwanden auf einmal die Transaktionen der letzten zwei Stunden – ein Albtraum für alle Shops, die Bitcoins akzeptieren und digitale Güter vollautomatisch nach einer gewissen Anzahl Bestätigungen ausliefern. In der Blockchain selbst lässt sich dieses Ereignis nicht mehr nachvollziehen, denn alle Blöcke des abgestorbenen Zweigs wurden mit der Veröffentlichung von Block 363738 entfernt.

Auf blockchain.info/orphaned-blocks sind solche abgestorbenen Blöcke archiviert. Das hilft Betroffenen zu verstehen, was mit den verschwundenen Transaktionen passiert ist oder warum ein Shop eine Bestellung ausgeliefert hat, obwohl kein Zahlungseingang zu erkennen ist. Hinter solchen Effekten steckt also nicht unbedingt ein Software-Bug, die Blockchain verursacht sie selbst. *(mid@ct.de)* c't

Abgestorbene Zweige in der Blockchain

Finden mehrere Miner durch Zufall oder provoziert nahezu gleichzeitig den nächsten gültigen Block, teilt sich die Blockchain. Welcher Zweig überlebt, hängt davon ab, für welchen mehr Nachfolgeblöcke gefunden werden. Mitte 2015 wurden für drei aufeinanderfolgende Blöcke jeweils zwei Lösungen gefunden, bevor der Block 364000 die Entscheidung brachte und den oberen Zweig absterben ließ.