Doppelt gefährlich

Wie ein Double-Spend-Bug die Existenz des Bitcoin gefährdete

Kryptogeld zu kopieren ist einfach, es sind ja nur herkömmliche Binärdaten. Die Bitcoin Nodes verhindern jedoch, dass man Geld mehr als einmal ausgibt – normalerweise. Ein jetzt behobener Bug ermöglichte es für über ein Jahr, Bitcoins mehrfach zu benutzen – und gefährdete sogar die Existenz der Kryptowährung.

Von Mirko Dölle

Bei Bargeld sorgen aufwendige Drucktechniken, diverse Sicherheitsmerkmale und nicht zuletzt die Seriennummer jeder Banknote dafür, dass niemand einen Geldschein kopieren und dann mehrfach ausgeben kann. Bei Kryptowährungen lassen sich Kopien nicht verhindern, es handelt sich schließlich um ganz normale Binärdaten in Dateien. Dort sorgen die Blockchain und die Bitcoin Nodes dafür, dass niemand virtuelles Geld doppelt ausgibt. Doch genau diese Überprüfung der Node- und Client-Software Bitcoin Core enthielt für über ein Jahr lang einen Fehler, der es möglich machte, Bitcoins mehrfach auszugeben.

Um zu verstehen, wie solche „Double Spends“ bei Bitcoin und den meisten anderen Kryptowährungen normalerweise verhindert werden, muss man sich die Funktionsweise von Wallets und Bitcoin-Adressen genauer ansehen. Die weit verbreitete Vorstellung, ein Wallet oder eine Adresse seien virtuelle Konten und die Blockchain ein Kassenbuch, hilft hier nicht weiter. Viel mehr Ähnlichkeit haben Bitcoin-Adressen und die Blockchain mit Schecks und einem Scheckbuch – das Wallet ist nur die Geldbörse, in der man seine Schecks aufbewahrt, bis man sie verwendet.

Kauft man sich zum Beispiel Bitcoins, so erhält man für sein Bargeld einen Scheck über einen bestimmten Betrag in Bitcoin. Wie Bargeld besitzen auch Schecks eine Seriennummer – bei den Bitcoin-Schecks ist das die Bitcoin-Adresse. Will man die Bitcoins ausgeben, stellt man einen neuen Scheck über den entsprechenden Betrag aus und reicht ihn zusammen mit dem alten Scheck bei den Bitcoin Nodes ein. Im globalen Scheckbuch, der Blockchain, wird dann die Seriennummer des alten Schecks als verbraucht notiert und der Betrag und die Seriennummer des neuen Schecks für jedermann sichtbar aufgeschrieben. Solche noch nicht verbrauchten Schecks bezeichnet man als „Unspent Transaction Outputs“, kurz UTXOs.

Ganz oder gar nicht

Genau wie bei Bar- oder Verrechnungsschecks gibt es auch bei Bitcoin keine Möglichkeit, nur Teilbeträge zu verwenden: Es wird stets der Gesamtbetrag eingelöst, wenn man einen Scheck einreicht. Es lassen sich aber problemlos mehrere neue Schecks ausstellen – vorausgesetzt, dass der Gesamtbetrag der neuen Schecks den Betrag der eingelösten nicht übersteigt. Man transferiert also den gewünschten Betrag auf die Bitcoin-Adresse des Empfängers und den Rest auf eine andere, eigene Bitcoin-Adresse. Bleibt Geld übrig, kassieren das die Miner, die die Transaktion letztlich verarbeiten – das ist die Transaktionsgebühr (Fee).

Um herauszufinden, über welche Höhe ein Bitcoin-Scheck einmal ausgestellt wurde, genügt ein Blick ins Scheckbuch, die Blockchain. Die Aufgabe der Bitcoin Nodes ist, bei eingehenden Transaktionen zu überprüfen, dass der Gesamtbetrag der neu ausgestellten Schecks den der eingereichten nicht übersteigt – andernfalls wird die Transaktion abgelehnt. War die Prüfung erfolgreich, leiten die Nodes die Transaktion an die Mem-Pools der Miner zur Verarbeitung weiter.

Die Miner ihrerseits melden neu gefundene Blöcke ebenfalls an die Bitcoin Nodes. Die Nodes überprüfen wiederum, ob alles mit rechten Dingen zuging, es sich also wirklich um einen gültigen Block mit korrekten Transaktionen handelt. Ist alles in Ordnung, hängen sie den neuen Block an ihre lokale Blockchain an und melden den Block auch an andere Nodes sowie die Bitcoin Clients der Anwender weiter.

Die Bitcoin Nodes bilden also das Rückgrat des Bitcoin. Sie stellen sicher, dass niemand betrügt. Deshalb sind Bugs in den Verifizierungsroutinen, wie einer in den Bitcoin-Core-Versionen 0.14 bis 0.16.2 enthalten war, besonders kritisch. Erschwerend hinzu kommt, dass fast 90 Prozent aller Nodes mit Bitcoin Core arbeiten – es sich also quasi um eine Monokultur handelt.

Ausgenutzt wurde der Bug jedoch nicht, denn er betraf nur eine ganz bestimmte Fallkonstruktion. Prinzipiell gibt es zwei Möglichkeiten, Bitcoins doppelt auszugeben: Man verwendet den Bitcoin-Scheck und eine Kopie bei zwei verschiedenen Transaktionen oder man reicht den Bitcoin-Scheck und die Kopie bei ein und derselben Transaktion doppelt ein. Außerdem kann eine solche Transaktion von einem Anwender bei einem Node eingereicht werden, oder sie ist in einem neuen Block enthalten, den ein Miner gefunden hat.

Der jetzt behobene Fehler in Bitcoin Core betraf nur den Fall, dass ein Miner einen Block mit einer Transaktion meldet, in der ein Bitcoin doppelt ausgegeben wird. Während Bitcoin Core 0.14 kurzerhand abstürzte, wodurch der Node lahmgelegt worden wäre, akzeptierten Bitcoin Core 0.15 bis 0.16.2 solche Blöcke als einwandfrei.

Um die Lücke auszunutzen, hätte ein Angreifer über eine stattliche Mining-Farm verfügen müssen – groß genug, um in einem überschaubaren Zeitraum von einigen Tagen einen mit Double Spends präparierten Block als Erster weltweit zu generieren. Die Hürde war also erheblich und die Erfolgsaussichten begrenzt. Außerdem finden sich in der Blockchain im fraglichen Zeitraum keine Blöcke, die illegale Double Spends enthalten. Deshalb ist klar, dass der Bug von niemandem ausgenutzt wurde – glücklicherweise.

Bitcoin am Abgrund

Denn die eigentliche Gefahr war nicht, dass sich ein Angreifer hätte Geld erschleichen können – sondern dass die Blockchain seit der Veröffentlichung von Bitcoin Core 0.15.0 im September 2017 illegale Blöcke enthalten haben könnte, ohne dass dies jemand bemerkt hat. Da jeder Folgeblock eine Referenz des vorherigen Blocks enthält, wäre es unmöglich, solche fehlerhaften Blöcke nachträglich zu korrigieren: Illegale Blöcke können gemäß der geltenden Regeln kein Teil der Blockchain sein. Also sind auch alle darauffolgenden Blöcke illegal, die sich auf einen illegalen Block beziehen. Schlimmstenfalls hätten über 50.000 Blöcke verworfen werden müssen – die darin verarbeiteten Abermillionen Transaktionen hätten niemals stattgefunden.

Da es aber auch keinen parallelen Zweig aus dem September 2017 gibt, der bis heute fortgeführt wurde, hätte der gesamte Bitcoin-Zahlungsverkehr um ein Jahr zurückgedreht werden müssen. Sämtliche Transaktionen des vergangenen Jahrs wären hinfällig, alle Käufe und Verkäufe nicht erfolgt, reihenweise würden Kryptobörsen Pleite gehen – und die Blockchain hätte für alle Zeiten eine Lücke von zwölf Monaten statt der sonst üblichen zehn Minuten. Das Vertrauen in Bitcoin wäre grundlegend zerstört, ein Kursabsturz die unvermeidliche Folge – und der würde auch die Kurse aller anderen Kryptowährungen mit in die Abgrund ziehen.

Zurückgedreht

Doch das ist noch immer nicht der Worst Case: Wenn 50.000 Blöcke verworfen würden, würde damit auch die Belohnung von derzeit 12,5 Bitcoin pro Block für die Miner wieder zurückgezogen. Die Mining-Farm-Betreiber würden

bis zu 3,5 Milliarden Euro verlieren – Geld, das sie für Strom und Hardware benötigen. Eine Pleite der großen Miner ließe sich kaum verhindern. Ohne die Miner kann der Bitcoin aber nicht überleben, und ohne Vertrauen in die Kryptowährung hat sie keinen Wert.

Die Bitcoin-Core-Entwickler haben aus diesem schweren, zum Glück nicht verheerenden Fehler gelernt, dass sie bei Änderungen an den Verifizierungsalgorithmen sehr viel gründlicher vorgehen und alle Randeffekte überprüfen müssen. Auch sollen die Testszenarien, die jedes neue Release von Bitcoin Core durchläuft, um einige Sonderfälle erweitert werden. Denn Fehler wird es auch in Zukunft geben und man muss sie unbedingt rechtzeitig finden. Bei einer Marktkapitalisierung von 100 Milliarden Euro für Bitcoin und gut 160 Milliarden Euro für Kryptowährungen insgesamt steht einfach zu viel auf dem Spiel. *(mid@ct.de)* c't