Rückkehr der Bitcoin-Wale

Wie mit riesigen Vermögen der Bitcoin-Kurs manipuliert wird

Im August und September wurden zehntausende Bitcoins im Wert von mehreren hundert Millionen US-Dollar bewegt. An den Kryptobörsen sorgte das für Kursreaktionen. Doch woher kommt das Geld und wem gehört es? Eine Spurensuche.

Von Mirko Dölle

Für Jahre waren sie in den Tiefen der Blockchain untergetaucht, bevor sie vor wenigen Wochen wieder an die Oberfläche kamen: die Überreste eines ehemaligen Bitcoin-Wals, ein alter Bekannter aus dunkleren Zeiten der Kryptowährung.

Als Wale bezeichnet man einzelne Wallet-Adressen, auf denen mehr als zehntausend Bitcoins im Wert von abermillionen US-Dollar lagern. Die beiden größten bringen es auf jeweils über eine Milliarde Dollar – also richtig dicke Fische[1]. Wie bei den Walen in den Weltmeeren handelt es sich um eine bedrohte Art, aktuell gibt es nur gut 100 Bitcoin-Wale.

Ende August sind über 1000 Wallets entstanden, in denen die Überreste eines zuvor in kleine Häppchen filetierten kapitalen Wals mit über 111.000 Bitcoins zusammengeführt wurden und die mit 999,99 Bitcoin knapp unterhalb des Radars vieler Marktbeobachter liegen.

Nun wird spekuliert, ob der Besitzer an einem der größten Bitcoin-Diebstähle aller Zeiten beteiligt war. Dank der Blockchain und sogenannten Block-Explorern kann jeder den Weg des Geldes nachvollziehen und so Indizien sammeln. Die Spur lässt sich bis zum legendären MtGox-Betrug zurückverfolgen, bei dem die Täter etwa 650.000 Bitcoins entwendeten – was 2014 den damals weltweit größten Bitcoin-Händler in den Ruin trieb und einen Schaden von fast einer halben Milliarde US-Dollar verursachte. Die bislang nicht wieder aufgetauchte Beute hat heute einen Wert von rund 3,5 Milliarden Euro.

Um selbst die Spur aufzunehmen, genügt es, eine an einer bestimmten Transaktion beteiligten Bitcoin-Adresse oder eine Transaktions-ID der Transaktion zu kennen und sie auf der Website eines Block-Explorers einzugeben – etwa auf blockexplorer.com, blockchain.info oder explorer.bitcoin.com/btc. Dort erhält man dann eine Liste aller Transaktionen einer Adresse sowie die an der Transaktion beteiligten Adressen – sodass man leicht den Weg des Gelds nachverfolgen kann.

Das Problem: Wem einzelne Bitcoin-Adressen gehören, weiß die Öffentlichkeit in der Regel nicht. Bekannt sind allenfalls die Wallets der Kryptobörsen oder Dienstanbieter, sodass sich oft nachvollziehen lässt, wenn jemand Bitcoins an eine Börse verkauft oder dort einkauft. Die Börsen wiederum verlangen von ihren Kunden meist, sich zu identifizieren. Diese Daten nutzen auch Strafverfolger, um Kriminellen auf die Schliche zu kommen.

Abgetaucht

Bei dem MtGox-Betrug wurden wahrscheinlich über 3 Jahre lang Gelder der Firma entwendet. Eins der Wallets, auf denen sich Gelder von MtGox ansammelten, ist 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a: Von dort transferierte jemand im März 2014 über 111.000 Bitcoin an eine neue Adresse – ein stattlicher Wal war geboren.

Noch ist nicht klar, wer diese Person ist. Aufgrund der Transaktionshistorie der genannten Adresse ist aber davon auszugehen, dass es sich um einen (ehemaligen) Kunden von MtGox handelt. Ob er etwas mit dem Betrug zu tun hat oder einfach über Jahre so viel eingezahlt hatte, lässt sich nicht beurteilen: Die Betrüger nutzten eine Schwachstelle in der Wallet-Implementierung von MtGox, um sich Gelder mehrfach auszahlen zu lassen. In der Historie des besagten Wallets finden sich zwar etliche Transaktionen, wo mehrfach große, identische Beträgen gutgeschrieben wurden – ein Beweis ist das jedoch nicht.

Während MtGox im März 2014 in die Insolvenz ging, wurde der Wal in einer ganzen Serie von Transaktionen zerlegt: in zwei 50.000 und 60.000 Bitcoin große Brocken, die in vier Wallets mit 20.000 und 30.000 Bitcoin, diese wiederum in mehrere mit 10.000 und 20.000 Bitcoin. In den nächsten Stufen wurden alle größeren Wallets auf mehrere mit jeweils exakt 10.000 Bitcoin aufgeteilt, dann 5000, 1000, 500 und schließlich exakt 100 Bitcoin pro Wallet. So filetiert ging der Wal weitgehend unbeobachtet für über vier Jahre auf Tauchstation.

Die Wiedererweckung begann Ende August: Damals wurden die Guthaben von jeweils 100 Bitcoins von 10 Adressen auf eine einzelne neue Adresse transferiert. Abzüglich Transaktionsgebühr entstanden dadurch Zwergwale mit knapp unter 1000 Bitcoin pro Wallet. Auffällig ist daran zweierlei: Erstens sind ausgewachsene Wale selten und genießen allein aufgrund ihrer Größe eine gewisse allgemeine Aufmerksamkeit. Auch kleinere Wallets mit 1000 bis 10.000 Bitcoins, nennen wir sie Zwergwale, gibt es nur gut 1500 Mal weltweit. Indem der Eigentümer des ehemaligen Wals seine Wallets mit knapp unter 1000 Bitcoin bestückte, blieb er unter dem Radar der Öffentlichkeit.

Ungewaschen transferiert

Zweitens fällt auf, dass die Bitcoins nicht in sogenannten Mixern gewaschen wurden. Bitcoin-Mixer verschleiern die Nachverfolgbarkeit von Zahlungsflüssen, indem sie Bitcoins auf dem ersten Wallet entgegennehmen und den gleichen Betrag von einem zweiten auszahlen – abzüglich einer zufällig ausgewählten Bearbeitungsgebühr und mit einer wählbaren Verzögerung. Je nach Anbieter lässt sich die Auszahlung zudem auf mehrere Wallet-Adressen verteilen.

Die Verzögerung und die zufällige Bearbeitungsgebühr sorgen dafür, dass man selbst bei einer sorgfältigen Analyse der Blockchain keinen Bezug zwischen Einzahlung und Auszahlung herstellen kann, weil weder der Betrag noch der Buchungszeitpunkt übereinstimmen. Sind auch noch mehrere Auszahlungsadressen im Spiel, kann man allenfalls noch raten.

Mehr noch: Da andere Nutzer für die Einzahlung das zweite Wallet zugewiesen bekommen und die Bitcoins aus dem ersten Wallet zurückerhalten, endet die Spur der Bitcoins nicht im Wallet des Mixers. Alle Mixer-Nutzer bekommen letztlich die Bitcoin anderer Mixer-Nutzer zurück.

Der Besitzer des Wals hat diese Möglichkeit bislang nicht genutzt, sondern gut 15.000 Bitcoin im Wert von fast 100 Millionen US-Dollar direkt bei den Kryptobörsen Bitfinex und Binance eingezahlt. Der Weg der Bitcoins lässt sich lückenlos in der Blockchain nachvollziehen. Der Walbesitzer scheint also keine Angst davor zu haben, dass Behörden den Geldfluss nachvollziehen und über die Kryptobörsen seine Identität ermitteln – oder er hat seine Bitfinex- und Biance-Accounts unter einer falschen Identität angelegt.

Die übrigen fast 100.000 Bitcoins schlummern in Form von Zwergwalen wieder in der Blockchain. Die Stückelung legt allerdings nahe, dass es sich um Vorbereitungen für einen Verkauf handelt: Andernfalls hätte der Eigentümer den ehemaligen Wal einfach weiterhin in 100-Bitcoin-Wallets verteilt ruhen lassen können.

Ein spontaner Verkauf so vieler Bitcoins würde in jedem Fall Einfluss auf den Kurs haben – er dürfte ihn kräftig auf Talfahrt schicken. Aus diesem Grund wird das Auftauchen eines neuen Wals von Experten argwöhnisch beobachtet: Er entstand Mitte September, ist 30.000 Bitcoin oder umgerechnet gut 150 Millionen Dollar schwer und entstand aus einem bekannten Wal der Kryptobörse Bitfinex.

Auffällig an diesem neuen Wal ist nicht nur seine Größe, sondern auch, dass mit ihm das Transaktionsvolumen der Blockchain künstlich aufgeblasen wurde. So wurde das Geld in ein und demselben Block 541229 von dem Wal-Wallet auf ein zweites und sogleich wieder zurück auf das erste Wallet transferiert. Das steigerte das Volumen der transferierten Bitcoins von ansonsten unter oder um 10.000 Bitcoins pro Block auf über 70.000 Bitcoin, was wiederum eine hohe Aktivität des Bitcoin-Markts vorspiegelte. Hinzu kam die ursprüngliche Auszahlung in Höhe von 30.000 Bitcoin, die nur 4 Blöcke zuvor stattfand.

Die Auswirkung des künstlich erhöhten Transaktionsvolumens lässt sich am Bitcoin-Kurs ablesen: Als sich der Wal am Morgen des 13. September erstmals zeigte und im Kreis schwamm, stieg der Kurs plötzlich von 6200 auf über 6500 US-Dollar.

Walbeobachtung ist also nicht nur eine Aufgabe für Sea Shepherd und Umweltschützer, sondern auch die Pflicht von Investoren und Marktanalysten von Kryptowährungen. Denn das Auftauchen oder Verschwinden eines Wals kann durchaus die Kursentwicklung beeinflussen. Wer sich nicht die Mühe macht, auffällige Transaktionen zu analysieren, kann solche Kursmanipulationen auch nicht erkennen und sich so nicht vor Fehlinvestitionen schützen. Nicht umsonst lautet das Motto der Blockchain: Vertraue nicht, prüfe! *(mid@ct.de)* c't

[1] Wale sind natürlich keine Fische, das Sprichwort nimmt darauf aber keine Rücksicht.