Todsicher

Tausende Bitcoins als Grabbeigabe

Kryptobörsen und andere Profis bewahren den größten Teil ihres Bitcoin-Vermögens in Cold Wallets auf. Dort kommt kein Hacker heran – und wenn der Wallet-Besitzer stirbt, schlimmstenfalls auch sonst niemand.

Von Mirko Dölle

Ein Pharao war Gerald Cotten zu Lebzeiten nicht, doch die Grabbeigaben des ehemaligen Gründers und CEO der kanadischen Kryptobörse QuadrigaCX können es durchaus mit denen von Tutanchamun aufnehmen: Als der Kanadier am 9. Dezember starb, nahm er Bitcoins und andere Kryptowährungen im Wert von über 100 Millionen Euro mit ins Grab.

Der Fall zeigt, wie wichtig es ist, sein Kryptovermögen selbst zu verwalten – aber auch, welches Risiko unregulierte Finanzdienstleister für Otto Normalverbraucher darstellen. Denn eine Absicherung der für die Kunden verwalteten Kryptogelder gibt es nicht. Auch nicht bei deutschen Kryptobörsen wie zum Beispiel Bitcoin.de, dort sind lediglich Euro-Guthaben über die gesetzliche Einlagensicherung abgesichert.

Der Grund für die sprichwörtliche Pleite bei QuadrigaCX ist eine übliche Vorsichtsmaßnahme, wie sie weltweit von allen Kryptobörsen praktiziert wird: Damit kein Angreifer sämtliche Bitcoins klauen kann, wird nur ein kleiner Teil des Vermögens für das Tagesgeschäft auf einem herkömmlichen Bitcoin-Wallet verwaltet. Die Reserven hingegen transferiert man in ein sogenanntes Cold Wallet, wo sie sicher sind.

Kalte Bitcoins

Die Besonderheit von Cold Wallets ist, dass die für Auszahlungen nötigen privaten Schlüssel oder Seeds nicht auf einem herkömmlichen Rechner gespeichert werden, sondern vorzugsweise auf einem Hardware-Wallet oder zumindest auf einem Rechner, der über keinerlei Netzwerkverbindungen verfügt. Ein Angreifer benötigt also physischen Zugriff auf das Hardware-Wallet oder den isolierten Rechner, um Kryptogeld zu stehlen.

Während Auszahlungen von einem Cold Wallet erwünschterweise sehr aufwendig sind, ist für Einzahlungen keinerlei Mehraufwand vonnöten: Überweisungen auf ein Cold Wallet sind jederzeit und ohne Spezialwissen möglich. Man benötigt lediglich die Bitcoin-Adresse. Ein solches Cold Wallet lässt sich also gut mit einem Banktresor mit Einwurfschlitz vergleichen.

Das Problem von QuadrigaCX ist, dass Cotten als CEO der Einzige war, der wusste, wo die Schlüssel des Cold Wallets gespeichert und mit welchem Passwort sie geschützt sind. Auch als er Ende 2018 zu einer Reise nach Indien aufbrach, verriet er niemandem, wie man an die Gelder des Cold Wallet herankommt. Wie das Fortis Escorts Hospital in Jaipur öffentlich bestätigte, in das Cotten am Morgen des 8. Dezember eingeliefert wurde, starb der Kanadier keine 24 Stunden später an einem septischen Schock, der durch akute Komplikationen seiner chronischen Darmerkrankung Morbus Crohn ausgelöst wurde.

Heiße Gerüchteküche

Durch die Stellungnahme des Krankenhauses wurde das Gerücht entkräftet, Cotten sei in Wahrheit nach einem sogenannten Exit Scam untergetaucht und die von seiner Frau vorgelegte indische Sterbeurkunde eine Fälschung. Als Exit Scam bezeichnet man im Darknet den letzten großen Beutezug eines Betrügers, bevor er auf Nimmerwiedersehen verschwindet.

Nahrung erhielt dieses Gerücht zunächst durch weitere, nahezu parallele Ereignisse. So fror eine kanadische Bank, über die QuadrigaCX Dollar-Überweisungen an Kunden abwickelte, genau eine Woche vor Cottens Tod Guthaben von über 15 Millionen Euro ein. Kunden bekamen deshalb vorübergehend gar kein Geld mehr, später wurde ein Auszahlungslimit verhängt.

Der Ruf von QuadrigaCX wurde dadurch erheblich beschädigt: Auszahlungsstopps und Limits sind Alarmzeichen, die bedeuten, dass eine Kryptobörse nicht mehr liquide genug ist, um kurzfristig die Einlagen der Kunden zurückzuzahlen. Über die Limits verhindert man, dass Kunden ihr Geld schneller abziehen können, als man neue Investitionen einwirbt.

Als das Nachrichtenportal Coindesk Mitte Januar auch noch aufdeckte, dass QuadrigaCX keinen Zugriff auf über 99 Prozent des gesamten Vermögens hat, war die Verschwörungstheorie komplett: eine Kryptobörse, deren Konten eingefroren wurden, die Auszahlungslimits einführt, deren CEO auf einer Wohltätigkeitsreise in Indien überraschend stirbt und dabei fast das komplette Firmen-

vermögen von 100 Millionen Euro mit ins Grab nimmt, weil er als einziger Zugriff auf das Cold Wallet hatte – das war einfach zu viele Indizien für einen Exit Scam. Und doch war es wohl keiner.

Kundengelder beerdigt

Erschreckend daran ist, wie grob fahrlässig vermeintliche Profis wie Cotten und QuadrigaCX mit den ihnen anvertrauten Geldern umgingen. Die Vorfälle werfen insbesondere kein gutes Licht auf Aaron Matthews, dem früheren Betriebsleiter, der auf Empfehlung von Cottens Witwe als Interims-Präsident und -CEO die Geschäfte von QuadrigaCX weiterführen soll. Ihm bescheinigt sie Führungsqualitäten und ein tiefes Verständnis des Geschäfts mit Kryptowährungen. Das Gegenteil ist offenkundig der Fall, Matthews hätte niemals zulassen dürfen, dass nur Cotten allein Zugriff auf das Cold Wallet hat.

Wenn ein Geschäftsführer seinen Mitarbeitern so wenig vertrauen kann, dass nur er die Kombination des Firmentresors kennt, so ist das nicht viel mehr als das Eingeständnis einer verfehlten Personalpolitik. Sollte dem Geschäftsführer etwas zustoßen, ist es lediglich sehr aufwendig, den Tresor aufbrechen zu lassen, um die Geschäfte weiterführen zu können.

Die Blockchain lässt sich aber nicht aufbrechen, niemand kann ohne den richtigen Schlüssel an das Kryptogeld gelangen. Ein Sturz auf der Treppe, ein Unfall auf dem Heimweg, man muss nicht erst nach Indien reisen, um auch in jungen Jahren im Koma zu landen oder zu sterben. QuadrigaCX hätte keinen dieser Fälle überlebt.

Sicher mit Multisignatur

Die korrekte Vorgehensweise wäre gewesen, ein Multisignatur-Wallet vom Typ „2 of 3“ als Cold Wallet zu verwenden, wobei Cotten, Matthews und ein Notar jeweils einen Seed oder ein Hardware-Wallet erhalten hätten. Einzahlungen auf ein solches Multisignatur-Wallet unterscheiden sich nicht von herkömmlichen Bitcoin-Transaktionen, eine Auszahlung ist jedoch nur möglich, wenn mindestens zwei der drei Personen die Transaktion signieren. Im Regelfall wären das Cotten und Matthews gewesen, womit auch das sonst in der Finanzbranche übliche Vier-Augen-Prinzip umgesetzt worden wäre. Stößt einem der beiden etwas zu, könnte der andere mithilfe des beim Notar hinterlegten Seed das Firmenvermögen retten. Es sind auch andere Konstellationen möglich, die Kryptobörse Bitfinex etwa verwendet ein Cold Wallet, bei dem 3 von 6 Signaturen erforderlich sind. Hier ist ein Totalverlust aufgrund eines Unfalls einzelner Personen nahezu ausgeschlossen.

Mangels Einlagensicherung für Kryptowährungen und weil Kryptobörsen üblicherweise nicht offenlegen, wie sie ihre Cold Wallets ausgestalten, sollte man sein Geld nicht bei Kryptobörsen parken. Legen Sie sich stattdessen ihr eigenes Cold Wallet an, etwa als Multisignatur-Wallet vom Typ „1 of 2“: Dann können Sie den Seed für den zweiten Schlüssel getrost in einem Bankschließfach deponieren oder in ihrem Testament aufschreiben und sicher sein, dass Sie Ihr Kryptovermögen nicht mit ins Grab nehmen. *(mid@ct.de)* c't