Neue Zürcher Zeitung

Bitcoin

Der 620-Millionen-Dollar-Schwindel

28. März 2014

Die insolvente Bitcoin-Börse Mt. Gox hat 200'000 verlorengeglaubte Einheiten der digitalen Währung wiedergefunden.
(Bild: Imago)

Der angebliche Diebstahl bei MtGox, der den Zusammenbruch dieser Bitcoin-Börse verursachte, hat möglicherweise gar nicht stattgefunden. Dies vermuten Computerwissenschafter der ETH-Zürich, die seit Januar 2013 Bitcoin-Transaktionen überwachen.

S. B. Im Laufe des vergangenen Jahres hat sich der Wert der virtuellen Währung Bitcoin von 13 Dollar auf über 1000 Dollar rasant erhöht. Dann kam der Absturz: Heute, Ende März 2014, ist ein Bitcoin noch gut 500 Dollar wert. Bitcoin ist ein verteiltes Zahlungssystem, das ohne Zentralbank auskommt. Doch hat das System stark von Börsen profitiert, die den Handel mit diesem virtuellen Geld erleichterten. Diese Handelsplätze sind eine Schwachstelle des dezentralen Systems.

Technische Fehler

Eine der ersten und lange Zeit populärsten Bitcoin-Börsen war MtGox. Der jüngste Absturz des Bitcoin-Kurses hängt mit der Schliessung dieser Börse zusammen. Am 7. Februar 2014 stoppte MtGox die Auszahlungen, bald darauf war die Website nicht mehr erreichbar, am 28. Februar 2014 stellten die Betreiber der Börse in Japan einen Antrag auf Gläubigerschutz.

Ein technischer Fehler der Bitcoin-Software, so begründeten die MtGox-Betreiber ihre Probleme, habe es Angreifern ermöglicht, virtuelles Geld zu stehlen. Bei dem Fehler handelt es sich um die sogenannte Transaction Malleability, die seit 2010 bekannt ist. Das englische Wort steht für Formbarkeit, Schmiedbarkeit und bezeichnet im Zusammenhang mit Bitcoin die Möglichkeit, bei der Quittung für eine Bitcoin-Transaktion im Nachhinein den Absender zu verändern. Es gibt dann zu einer Transaktion zwei Belege, und wenn der manipulierte Beleg zuerst in die Hauptbuchhaltung übernommen wird, wird der echte abgelehnt werden, und der Absender wird dann unter Umständen annehmen, die Transaktion sei nicht zustande

gekommen. Auf diese Weise, so behaupteten die MtGox-Betreiber, seien dem Unternehmen 850'000 Bitcoins oder rund 620 Millionen Dollar gestohlen worden.

849'600 Bitcoins fehlen

Eine Studie der ETH Zürich zieht nun diese Darstellung in Zweifel. Roger Wattenhofer und Christian Decker von der Distributed Computing Group des Computer Engineering and Networks Laboratory haben seit Januar 2013 Bitcoin-Transaktionen überwacht. Sie fanden verschiedene Unregelmässigkeiten, aber keine Hinweise auf einen gross angelegten Bitcoin-Raub bei MtGox mit Hilfe der Transaction Malleabilty.

«Die Transaction Malleability ist ein reales Problem», schreiben die beiden Computerwissenschafter am Schluss ihrer Studie. Doch: «Wir konnten nur 302'000 Bitcoins finden, die von Malleabilty -Angriffen betroffen waren. Nur 1811 Bitcoins waren von solchen Angriffen betroffen bevor MtGox die Auszahlungen stoppte. Zudem glückten nur 78,64 Prozent der Angriffe. Deshalb können bei MtGox oder anderen Börsen nur 386 Bitcoins gestohlen worden sein. Selbst wenn sich alle diese Angriffe auf MtGox konzentrierten, muss MtGox den Verbleib von 849'600 Bitcoins erklären.»