Ewiger Speicher

Die Blockchain als Datenmüllhalde

Für alle Zeiten unveränderlich sind die Transaktionsdaten in der Bitcoin-Blockchain gespeichert. Doch nicht nur diese, auch Links, Texte und Fotos sind dort für alle Ewigkeit archiviert – und landen auf den Festplatten von Millionen Bitcoin-Nutzern. Wir zeigen Ihnen, wo sich kuriose, aber auch illegale Inhalte in der Blockchain verstecken.

Von Mirko Dölle

Die Bitcoin-Blockchain kann durchaus unterhaltsam sein, selbst wenn man kein Kryptogeld-Entwickler oder angehender Banker ist. Der überwiegende Inhalt sind harmlose Überweisungsdaten, die Blockchain bietet aber auch Platz für Links, Songtexte, ganze Artikel und Fotos. Manches ist für jedermann sichtbar gespeichert, bei anderem muss man wissen, wo es versteckt ist, um es zu finden.

Problematisch wird es, wenn es sich etwa um (vormals) geheime Informationen oder gar illegale Inhalte wie Kinderpornografie handelt: Genauso wenig, wie jemand die Transaktionen eines Blocks nachträglich verändern kann, lassen sich diese artfremden Informationen wieder entfernen. Sie sind bis zum Ende aller Tage des Bitcoin in die Blockchain gemeißelt und werden weltweit millionenfach kopiert. Wer einen Full-Client wie zum Beispiel Bitcoin Core benutzt, besitzt automatisch eine Kopie der Blockchain – und damit ziemlich brisante Daten.

Die prominenteste Stelle für nicht zahlungsrelevante Informationen in der Blockchain ist die sogenannte Coinbase eines Blocks. Dieses bis zu 96 Byte große Feld nutzen Miner, um die Belohnung für sich zu beanspruchen und die Unterstützung etwa für geplante Protokollveränderungen zu signalisieren. Den Rest des Felds können sie mit Grüßen, einer Kontaktadresse oder auch Zitaten füllen. Der mutmaßliche Bitcoin-Erfinder Satoshi Nakamoto nutzte die Coinbase bereits im allerersten Block der Blockchain für ein Zitat:

```
The Times 03/Jan/2009 Chancellor on ↵
↳ brink of second bailout for banks
```

Das stammt von der Titelseite der britischen The Times vom 3. Januar 2009 und beweist, dass Satoshi Bitcoin zwischen dem Erscheinungsdatum jener Ausgabe und der Veröffentlichung des ersten Bitcoin-Blocks am 9. Januar erfunden hat.

Die Möglichkeit, nicht zahlungsrelevante Daten in der Blockchain zu speichern, ist also so alt wie die Blockchain selbst und wurde von den Minern für viel, salopp gesagt, Unfug genutzt. Was dort steht, finden Sie auf der Website bitcoinstrings.com, die die Blockchain nach lesbaren Zeichenketten absucht. Satoshis Zitat findet sich in der Datei blk00000.txt. Haben Sie selbst eine Kopie der Blockchain, können Sie sich mit dem Kommandozeilenprogramm `strings` (Standard unter Linux und macOS, Windows-Version auf ct.de/y7c6) selbst auf die Suche nach geheimen Botschaften machen.

Untergeschoben

Es gibt noch eine weitere und umfangreichere Möglichkeit, Daten in der Blockchain unterzubringen – etwa im `OP_RETURN`-Feld, das dem Verwendungszweck einer Überweisung entspricht. 80 Bytes stehen hier zur Verfügung. Forscher der RWTH Aachen und der Goethe-Universität Frankfurt am Main haben diese und andere Möglichkeiten in einer im März veröffentlichten Studie untersucht. Eine seit Mitte 2010 häufig genutzte Methode ist, Inhalte nicht mehr nur in den Fußnoten der Blöcke und im Verwendungszweck einer Transaktionen, sondern in den Adressen von Transaktionen zu verstecken. Dabei können je nach Vorgehensweise zwischen 50 und knapp 100 KByte pro Transaktion eingeschleust werden, fanden die Forscher heraus.

Wie das funktioniert, lässt sich anhand einer Widmung für Nelson Mandela von Mitte 2013 gut nachvollziehen. Dabei wurde in einer über 1 KByte großen Transaktion ein kleiner Betrag an 32 Bitcoin-Adressen überwiesen. In den sogenann-

ten Output Scripts, die beschreiben, wie der Empfänger über das Geld verfügen kann, wurden jedoch nicht die Hashes echter Empfängeradressen eingefügt, sondern die Binärdaten mit einem Zitat und einem Bild Mandelas. Auf ct.de/y7c6 finden Sie den Link zu der Transaktion. Der Hash-Wert des ersten Output Scripts der Transaktion beinhaltet die ersten Worte des Zitats, das komplette Zitat ist neun Hashes lang.

Letztlich überweist man damit Geld ins Nirvana, kann aber durch Zufall auch eine aktive Bitcoin-Adresse erwischen. So wurde das Geld von einer der Adressen weiter transferiert, der Rest schlummert weiter in der Blockchain.

Auch das verschlüsselte Material der Cabel-Gate-Affäre von WikiLeaks wurde in der Blockchain gespeichert, quasi als öffentliches, unveränderliches Backup. Die Wörterliste für sogenannte Seeds des Bitcoin-Clients Electrum, die zum Wiederherstellen von Wallets benötigt wird, ist ebenfalls in der Blockchain verewigt. Wer selbst Daten in der Blockchain speichern möchte, kann dazu den Online-Dienst Cryptograffiti.info oder die Programme Apertus und Satoshi Uploader verwenden.

Die dunkle Seite

Unbekannte haben diese Möglichkeiten bereits 2012 genutzt, um eine Link-Sammlung für Pädophile mit ausführlicher Beschreibung, was man dort findet, aus dem Hidden Wiki des Darknets in der Blockchain zu speichern. Viele der Links verweisen auf sogenannte Hidden Services, die nur über den Tor-Browser erreichbar sind. Wir haben die Erreichbarkeit der genannten Onion-Domains überprüft, die einzige noch immer aktive war das Hidden Wiki selbst. Insofern hat sich die Situation inzwischen entspannt.

Die Blockchain enthält nicht nur Buchungsdaten, auch Botschaften an Außerirdische (links), Nachrufe für Verstorbene, ein Aufruf zur Legalisierung von Cannabis und Fotos von Personen sind dort für immer und ewig gespeichert.

Entfernen ließe sich eine solche Linksammlung nur durch einen Hard-Fork der Blockchain – etwa indem man die Transaktionen, die die problematischen Daten enthalten, durch einen irregulären Block ersetzt. Damit würde jedoch die Blockkette unterbrochen und so die oberste Regel verletzt: Die Blockchain ist unveränderlich.

Dass ein aus guten Gründen durchgeführter Hard-Fork nicht das Todesurteil für eine Kryptowährung sein muss, zeigt das Beispiel von Ethereum. Dort wurde Mitte 2016 der DAO-Hack, bei dem Hacker unter Ausnutzung eines Bugs Ether im Wert mehrerer Millionen Euro abzogen, nachträglich durch einen Fork ausgebügelt. Dieser Fork zerstörte allerdings auch einiges an Vertrauen in die Beständigkeit der Blockchain und der Smart Contracts – um regelmäßig illegale Inhalte der Blockchain auszumerzen, ist diese Ultima Ratio ungeeignet.

Inzwischen schützen manche Miner die Blockchain vor offensichtlichem Missbrauch, indem sie besonders große Transaktionen mit vielen Output-Adressen nicht verarbeiten. Es dürfte noch eine Weile dauern, bis dies überall Standard ist. Dieses Vorgehen hat in der Vergangenheit schon einmal funktioniert: Nicht-Standard-Transaktionen, die ein noch höheres Missbrauchspotenzial bieten, berücksichtigt heute praktisch kein Miner mehr. Auch ist es durch die Vielzahl der Miner schwierig geworden, als Einzelperson einen Link in der Coinbase unterzubringen.

Eine gezielte Suche nach problematischen Inhalten findet jedoch nicht statt, Links auf Kinderporno-Seiten und auch Bilder lassen sich weiterhin einschmuggeln, wenn man es darauf anlegt. Absolute Sicherheit kann es ohnehin nicht geben: Niemand weiß, ob nicht irgendwo ein Link oder ein Foto binär invertiert oder anderweitig verschleiert über mehrere Transaktionen verteilt eingefügt wurde.

Aufgebohrt

Die Entwickler der Kryptowährung Bitcoin Cash haben ungeachtet des Unfugs, der ohnehin schon mit der Blockchain getrieben wird, beim bislang letzten Fork der Kryptowährung am 15. Mai den Platz für den Verwendungszweck von Transaktionen sogar noch vergrößert: Bis zu 220 Bytes sind nun erlaubt. Außerdem funktionieren Tricks wie Transaktionen mit unzähligen Auszahlungsadressen ebenfalls.

Mit Memo.cash gibt es außerdem einen Client, mit dem man ähnlich wie bei Twitter Kurznachrichten für immer und ewig in der Blockchain speichern, aber auch anderen Bitcoin-Cash-Besitzern folgen oder ihre Beiträge liken kann. Worüber auf der Bitcoin-Cash-Blockchain geredet wird, lässt sich auf der Website Wewo.cash nachlesen.

Bei Redaktionsschluss versuchten die Ersten, über mehrere Memos verteilte Fotos in der Blockchain zu speichern. Es bleibt nur die Hoffnung, dass niemand Kinderpornos einschleust. Denn der Besitz und die Verbreitung von Kinderpornografie ist und bleibt strafbar, egal, ob sie in der Blockchain oder in einzelnen Dateien gespeichert sind. Anwendern bliebe nur die Möglichkeit, auf Light-Clients wie Electrum umzusteigen, die nicht die ganze Blockchain, sondern nur einzelne Transaktionen für das eigene Wallet von speziellen Servern herunterladen. *(mid@ct.de)* c't

Strings für Windows und Links zu Mandela-Transaktionen: **ct.de/y7c6**