Ketten für Bitcoin

Wie Regierungen Kryptowährungen regulieren

Dezentral, unabhängig, basisdemokratisch und vermeintlich unregulierbar: Bitcoin ist der Inbegriff für freien Handel, gegen den weder Banken noch Regierungen etwas unternehmen können. Mit der neuen EU-Geldwäscherichtlinie und der Einstufung von Initial Coin Offers als Aktie gelingt es den Regierungen trotzdem, den Handel mit Bitcoins zu beschränken.

Von Mirko Dölle

Die Eigenschaften von Bitcoin klingen nach Utopie, wenn man die Kryptowährung mit gesetzlichen Zahlungsmitteln vergleicht: Dezentral organisiert, unabhängig von Regierungen und Institutionen soll sie sein. Keine Regierung soll sie kontrollieren oder ihr Reglementierungen aufzwingen können und niemand Geringerer als die Weltöffentlichkeit als Aufsichtsgremium fungieren.

Trotzdem versuchen Regierungen in aller Welt, Kryptowährungen zu bändigen: In der EU droht eine Registrierungspflicht für Bitcoin-Adressen. Bitcoin-Börsen benötigen in Deutschland eine Erlaubnis der BaFin, sonst drohen viele Jahre Gefängnis. In Venezuela müssen sich Miner beim Staat registrieren und China will das Mining gänzlich verbieten. So wollen Regierungen für das eigentlich Unkontrollierbare die gleichen oder noch strengere Regeln durchsetzen wie für den Geldverkehr.

Dabei kommt Bitcoin ohne ein Aufsichtsgremium oder eine vertrauenswürdige Institution aus, dem man Vorschriften machen könnte. Das zentrale Element der Kryptowährung ist die Blockchain. Sie ermöglicht jedermann, sich selbst davon zu überzeugen, dass alles mit rechten Dingen zugeht – denn die Blockchain protokolliert sämtliche Transaktionen öffentlich einsehbar und für alle Zeiten.

Auch die einzelnen Transaktionen lassen sich mit wenig Aufwand von jedermann überprüfen. Dazu muss man nur wissen, dass Bitcoin-Adressen – ähnlich einer Kontonummer – der Hash-Wert des öffentlichen Schlüssels eines Public-/Private-Key-Paars sind. Eine Transaktion enthält also nicht nur Absender- und Zieladresse (genauer: die vorherige Empfangsadresse und die neue Empfangsadresse), sondern auch den öffentlichen Schlüssel der Absenderadresse. Außerdem muss der Absender die Transaktion mit dem dazugehörigen privaten Schlüssel signieren.

Durch Hashen des in den Transaktionsdaten enthaltenen Public Key lässt sich also gleichzeitig überprüfen, ob der Schlüssel zur angegebenen Absenderadresse passt, und durch den Key selbst außerdem, ob die Signatur korrekt mit dem zugehörigen privaten Schlüssel erfolgt ist. Eine Transaktion ist bei Bitcoin also selbstauthentifizierend.

Hash-Funktion als Sicherung

Doch was hindert jemanden daran, die Geschichte umzuschreiben, indem er eine Transaktion aus der Blockchain entfernt oder verändert? Im Wesentlichen der Hash-Algorithmus SHA256, der doppelt angewendet den jeweiligen Hash-Wert eines Blocks liefert.

Ein Hash-Wert ähnelt entfernt einer Quersumme: So wie sich die Quersumme einer langen Zahl leicht berechnen lässt, aber nur umständlich aus einer Quersumme eine passende Zahl, lässt sich mit einer Hash-Funktion leicht der Hash-Wert eines Datensatzes berechnen – umgekehrt ist aber noch keine Methode bekannt, wie man aus dem Hash-Wert einen passenden Datensatz berechnen könnte, ohne alle denkbaren Möglichkeiten durchzuprobieren (Brute-Force-Angriff). Außerdem haben kleinste Änderungen am Datensatz gravierende, unvorhersagbare Auswirkungen auf den Hash-Wert.

Der Knackpunkt ist, dass ein neuer Block der Blockchain neben den Transaktionen auch den Hash-Wert des vorhergehenden Blocks und eine vom Miner frei gewählte Zahl enthält. Von diesem Datensatz ermittelt der Miner nun den Hash-Wert. Das Ergebnis vergleicht er mit der Vorgabe aus der Blockchain, der sogenannten Difficulty: Sie wird automatisch so angepasst, dass die Vorgabe so schwer zu erfüllen ist, dass alle weltweit zur Verfügung stehenden Mining-Farmen erst nach etwa zehn Minuten eine Lösung finden.

Ist der Hashwert kleiner als die Difficulty, so hat der Miner einen gültigen Block zusammengestellt und kann das Gesamtergebnis – den Hash-Wert des Vorgänger-Blocks, die Transaktionen, die von

ihm gewählte Zahl und den Hash-Wert des Ganzen – veröffentlichen.

Passt der Hash-Wert des Datensatzes nicht zur Vorgabe, so verändert der Miner die selbst gewählte Zahl und somit den Hash-Wert des gesamten Datensatzes so lange, bis er ein passendes Ergebnis erhält – oder bis jemand anderer einen gültigen Block ermittelt und veröffentlicht hat.

Glied um Glied

Würde jemand eine Transaktion aus einem Block nachträglich entfernen, etwa weil er die Lösegeldzahlung an einen Ransomware-Erpresser rückgängig machen will, ändert sich dadurch der Hash-Wert dieses Blocks. Das fällt jedoch sofort auf, denn der ursprüngliche Hash-Wert des Blocks ist ja im Folgeblock enthalten. Man müsste also nicht nur den Block mit der Lösegeldzahlung ändern, sondern auch den darauf folgenden Block, um dort den neuen Hash-Wert des Vorgängers einzutragen – womit sich aber auch der Hash-Wert des Nachfolgers ändert, weshalb man auch dessen Nachfolger verändern müsste und so weiter.

Schlimmer noch: Die Hash-Werte der modifizierten Blöcke müssten, um nicht aufzufallen, auch jeweils die für sie geltende Difficulty erfüllen. Da man kaum über genauso viel Rechenleistung wie sämtliche Bitcoin-Miner der Welt zusammen verfügen dürfte, dauert es wesentlich länger als zehn Minuten, um einen alten Block zu fälschen und sich dem Nachfolger zuzuwenden – und in der Zwischenzeit hat der Rest der Welt die Blockchain um weitere Blöcke verlängert, die man ebenfalls noch fälschen müsste. Man müsste also mehr als die Hälfte aller Bitcoin-Miner kontrollieren, um aufzuholen und so überhaupt eine Chance zu haben, die Blockchain zu manipulieren.

Faktisch haben Behörden also keine Möglichkeit, etwa Erpressungs- oder Drogengelder sicherzustellen. Doch ganz machtlos sind sie nicht: Immer dann, wenn Bitcoins in eine reale Währung umgetauscht werden sollen, können sie die Kryptowährung in Schranken weisen.

Handelsbarrieren

Eine Grundlage für solche Handelsschranken ist die bereits 2014 von der Europäische Bankenaufsichtsbehörde EBA vorgenommene Einordnung von Kryptowährungen als „virtuelle Währungen“. Damit handelt es sich bei Bitcoin und allen anderen Kryptowährungen um nichtstaatliche Ersatzwährungen mit begrenzter Geldmenge.

Die deutsche Finanzaufsicht BaFin hat für ihren Einflussbereich festgelegt, dass etwa die Bezahlung von Leistungen und Gütern mit Bitcoin generell erlaubt ist. Da dabei faktisch nur Bitcoins von einer Adresse des Käufers an eine Adresse des Verkäufers transferiert werden, wäre es der BaFin ohnehin unmöglich, etwas dagegen zu unternehmen. Auch Mining hat die BaFin im Grundsatz erlaubt.

Wer jedoch gewerblich mit virtuellen Währungen handeln möchte, also den Umtausch von Bitcoins in andere Währungen oder von Währungen in Bitcoins anbietet, erbringt damit Finanzdienstleistungen. Diese sind schon heute erlaubnispflichtig und Anbieter müssen weitreichende Auflagen zu Kundenidentifizierung, Geldwäsche und Terrorismusfinanzierung befolgen. Wer keine Erlaubnis der BaFin erhält, muss dicht machen – so wie Crypto.exchange aus Berlin, der die BaFin Ende Januar den Geschäftsbetrieb verbot.

Sobald die im vergangenen Dezember beschlossene EU-Geldwäscherichtlinie in nationales Recht umgesetzt wird, droht zudem eine Registrierungspflicht für alle Bitcoin-Adressen – denn anonyme Geldtransfers sollen abgeschafft werden. Außerdem müssen Finanzdienstleister dann alle Kundeninformationen und Transfers der Financial Intelligence Unit (FIU) zum Abruf bereitstellen.

Zusammen mit den Transferdaten aus der Blockchain könnten Behörden dann große Teile des Krypto-Zahlungsverkehrs überwachen. Davon betroffen sind insbesondere Online-Wallets, bei denen Kunden ihre Kryptowährungen über den Webbrowser verwalten: Verwenden beide Transaktionsteilnehmer ein solches Online-Wallet, können die Behörden die Identität beider Geschäftspartner spielend leicht ermitteln.

Es geht noch drastischer: So hat die venezolanische Regierung im Vorfeld der Einführung der Kryptowährung Petro eine Registrierungspflicht für alle Miner im Land erlassen. Es wäre nun leicht, die Miner per Gesetz zu verpflichten, künftig ausschließlich Petros zu minen. Kontrolliert die Regierung die Miner, kann sie auch beeinflussen, welche Transaktionen die Miner abarbeiten – und könnte unliebsame Zahlungen, etwa Panikverkäufe bei einem Kursrutsch, per Dekret unterbinden. Die Transaktionen würden schlicht nicht ausgeführt, und der Staat könnte die zuvor eingenommenen Devisen behalten.

Strenge Auflagen für ICOs

Auch in den USA laufen Bemühungen, Kryptowährungen zu zügeln. In der Senatsanhörung Anfang Februar ging es allerdings in erster Linie um Initial Coin Offerings (ICO). Dabei verkauft eine zentrale Institution, etwa eine Firma, Einheiten einer neuen Kryptowährung an Investoren. Die Analogie einer Aktienausgabe oder Unternehmensanleihe fand der Vorsitzende der Kommission für den Handel mit Optionen und Futures (CFTC), J. Christopher Giancalor, sehr naheliegend und kündigte Regulierungsmaßnahmen an, damit Firmen künftig nicht mehr an den Aktiengesetzen vorbei Kapital aufnehmen können.

Zu einer ähnlichen Ansicht kommt auch die BaFin in ihrem Hinweisschreiben vom 20. Februar: Demnach will sie im Einzelfall bewerten, ob es sich bei ICOs um Unternehmensanteile, Wertpapiere oder eine Vermögensanlage handelt, und hat ICOs generell unter Erlaubnisvorbehalt gestellt. Somit muss jeder, der künftig in Deutschland neue Kryptowährungen per ICO herausgeben will, eine Klärung bei der BaFin beantragen. Tut man das nicht, drohen bis zu fünf Jahre Haft.

Indem die BaFin und andere Behörden freie Konvertierbarkeit von Bitcoin und Realwährungen beschränken, haben sie großen Einfluss auf die eigentlich unregulierbaren Kryptowährungen: Wer Bitcoins kaufen oder verkaufen möchte, kommt schon heute kaum noch um eine Identifizierung herum. Sollten die Behörden künftig etwa eine Erlaubnispflicht zur Nutzung von Kryptowährungen für Austauschgeschäfte (also Käufe) einführen, bliebe nur der Tausch Bitcoins gegen andere Bitcoins, um von der Regulierung verschont zu bleiben. Der Arm des Gesetzes reicht also viel weiter, als den Bitcoin-Verfechtern lieb sein kann. *(mid@ct.de)* c't