Christoph Bergmann

bitcoin

Die verrückte Geschichte vom Aufstieg eines neuen Geldes

MOBY Verlagshaus

Christoph Bergmann

Bitcoin

Die verrückte Geschichte vom Aufstieg eines neuen Geldes

1. Auflage 2018

Herausgeber

MOBY Verlagshaus
Postfach 1
89276 Neu-Ulm, Nersingen
www.bitcoin-buch.org

Gestaltung und Satz

Sarah Langenbucher Illustration, Bibertal
www.sl-illustration.de

Illustrationen und Umschlaggestaltung

Sarah Langenbucher Illustration, Bibertal

Lektorat

Brigitte Matern

Druck und Bindung

Druckhaus AJSp, LT-12187 Vilnius, Litauen

ISBN: 978 3 9819886 0 4

Die Rückeroberung der Kontrolle

Verbieten oder regulieren?

Die Mitglieder der Bitcoin-Szene haben ihre Gründe, weshalb sie Bitcoin, trotz aller mitunter erschreckenden Folgen, lieben. Aber das gilt nicht für die Regierung.

Warum sollten die Staaten Bitcoin dulden? Weshalb sollten sie ein Geld tolerieren, das die Arbeit der Polizei erschwert und die Hoheit der Regierung über das Geld hinterfragt, während es Anarchisten und Libertäre rund um die Welt reich macht? Das droht, am Ende gar die Steuereinnahmen auszutrocknen?

Einige Staaten haben gemacht, was am naheliegendsten ist: Sie haben Bitcoin verboten. Etwa Bangladesch, Bolivien, Ecuador, Island, Kirgisien, Nepal und Vietnam.[43] Die Begründung war meist simpel: Es ist nicht erlaubt, ein anderes als das offizielle Zahlungsmittel zu verwenden. Ob die Regierungen dieser Länder dabei tatsächlich wussten, womit sie es zu tun hatten, oder ob sie eher reflexhaft alles verbieten ließen, was nach einem Angriff auf die Währungshoheit riecht, ist schwer zu sagen.

Gründlicher mit Bitcoin hat sich die Volksrepublik China beschäftigt. Ende 2013, als in China ein Bitcoin-Hype ausbrach und der Preis gut 1000 Dollar erreicht hatte, wurde die Zentralbank aufmerksam. Sie erklärte, dass es nicht erlaubt sei, ein anderes Zahlungsmittel als den Yuan zu verwenden, und dass sich Banken und Finanzinstitute von der Kryptowährung fernhalten sollten. Es blieb jedoch erlaubt, mit Bitcoins zu handeln und sie zu schürfen. Mitte 2017 ging die Zentralbank jedoch noch einen Schritt weiter. Um zu verhindern, so die offizielle Begründung, dass die Finanzmärkte in Unordnung gebracht werden, verbot sie es Börsen zunächst, den Handel mit ICOs anzubieten. Kurz darauf untersagte sie jedoch auch den börslichen Handel mit Bitcoins.

---

43 Die Webseite coin.dance führt einen Index über die Legalität von Bitcoin auf der ganzen Welt. Diesem zufolge ist Bitcoin in 100 von 246 Ländern vollständig legal. Verboten ist die Kryptowährung dem Index zufolge in den folgenden Ländern in alphabetischer Reihenfolge: Afghanistan, Algerien, Bangladesch, Bolivien, Ecuador, Marokko, Mazedonien, Russland, Vanuatu. Zumindest für Russland scheint diese Einschätzung fragwürdig, da es dort eine offen handelnde Bitcoin-Szene gibt – wenn auch keine zugelassene Börse. Für die meisten Länder liegen aber keine Informationen vor, während ansonsten die Freigabe überwiegt. https://coin.dance/poli [01.03.2018]

Der Besitz, das Mining sowie der außerbörsliche Handel bleiben legal, auch wenn China Anstalten macht, das Mining strenger zu kontrollieren und auch Plattformen für den außerbörslichen Handel abzuschalten.

Viele Staaten – vermutlich auch China – haben mittlerweile begriffen, dass Bitcoin ein ungewöhnliches Phänomen ist, ein schwarzer Schwan des Finanzwesens. Man kann es nicht verbieten, selbst wenn man will. Natürlich könnte man ein Gesetz schreiben, das Bitcoin verbietet, oder die bestehenden Gesetze so auslegen, dass Bitcoin bereits verboten ist. Aber wie will man dies durchsetzen? Es gibt niemanden, dem man eine Anzeige zuschicken, keinen, den man verhaften kann. Bitcoin hat keinen CEO, keinen Besitzer, keine Aktionäre, keine Zentrale, kein Büro.

Bitcoins sind nicht mehr als ein Eintrag in einer Datenbank, der Blockchain, die dezentral auf Tausenden von Computern auf der ganzen Welt verteilt ist. Man kann sie nicht löschen. Kann man es verbieten, einen Schlüssel für diese Datenbank zu haben? Es gelingt Deutschland nicht, zu verhindern, dass kiloweise Bargeld in die Schweiz geschafft wird. Keine Grenze der Welt ist dicht genug, um nicht tonnenweise Cannabis, Kokain und Heroin durchzulassen. Wie soll man nur daran denken, einen Bitcoin-Schlüssel – eine Kombinationen von 50 Zeichen – zu verbieten? Soweit man hört, gibt es in Vietnam, Bolivien, Bangladesch, Venezuela und Ecuador weiterhin eine vitale Bitcoin-Szene, und selbst in China, wo der börsliche Bitcoin-Handel verboten wurde, blühen der außerbörsliche Handel und das Mining weiterhin auf.

Den meisten Regierungen wurde längst klar, dass man Bitcoin so wenig kriminalisieren kann wie Mathematik und dass allein schon der Versuch Nachteile bringt: Ein Land, das eine Innovation wie Bitcoin abwürgen möchte, wird als innovationsfeindlich gelten und bei den begehrten IT-Fachkräften unattraktiv werden. Schwerer dürfte wiegen, dass ein Bitcoin-Verbot die einheimischen Investoren nicht schützt, sondern sie ins Ausland treibt, auf die unregulierten Börsen in Steueroasen, wo die Kunden weder Rechtssicherheit noch Verbraucherschutz genießen. Nachdem die Regulierer in Deutschland und Frankreich Anfang 2013 anordneten, dass die beiden großen europäischen Börsen Bitcoin-Central (Paris) und Bitcoin24 (Deutschland) schließen mussten, strömten die europäischen Trader zu Mt. Gox. Das Ergebnis ist bekannt: Die Gewinne durch den Handel flossen nach Tokio, und die deutschen Ver-

braucher verloren durch die Insolvenz des Unternehmens am Ende ihre Bitcoin-Guthaben, ohne ernsthafte Chance, auf dem Rechtsweg entschädigt zu werden. Auch das Verbot der chinesischen Bitcoin-Börsen trieb lediglich die reichen chinesischen Bitcoin-Trader auf die Börsen von Südkorea und Japan.

Mit einem Bitcoin-Verbot verliert eine Regierung zudem ihren Handlungsspielraum. Bitcoin ist eine unbequeme, kontroverse und schwierige Innovation – aber wer sich nicht mit ihr beschäftigt, verliert. Das Finanzamt wird keine Steuergelder einnehmen, die Aufsicht kann den aufstrebenden Markt nicht regulieren, und die Polizei hat keinen direkten Ansprechpartner, um gegen Internet-Kriminelle zu ermitteln. Bitcoin zieht einen Kontrollverlust für den Staat nach sich – doch wenn er darauf mit einem Verbot reagiert, wird es nur noch schlimmer.

Vorausschauende Regierungen üben sich daher an einer feinen Balance. Einerseits sollen wachsende und global konkurrenzfähige Bitcoin-Unternehmen im Land bleiben – andererseits sollen sie auch reguliert werden. Die Staaten gehen eine Partnerschaft mit den Unternehmen ein. Sie lassen sie leben und üben bei der Regulierung vielleicht sogar Nachsicht, verlangen dafür aber auch Kooperation in Sachen Steuervollzug und Strafermittlung.

Da nur das reguliert werden kann, was legal ist, haben die meisten Länder begonnen, Bitcoin gesetzlich als Finanzprodukt oder Zahlungsmittel einzuordnen. Wenn es einen Namen bekommt, kann man es, so die Hoffnung, vielleicht beherrschen. Mitte 2013 begann dieser Prozess der Legalisierung von Börsen, Marktplätzen, Wallets, Zahlungsdienstleistern und Mining-Pools. Sie werden aus dem Graumarkt gehoben und gezwungen, nach den Regeln der Regierung zu spielen.

Viele Bitcoin-Börsen haben diesen Prozess nicht überlebt. In den meisten Ländern blieben nur einige wenige, marktbeherrschende Unternehmen, die fortan unter Beobachtung der Regulierung arbeiten. In Deutschland sind das der Marktplatz Bitcoin.de und die Firmen um Bitcoins Berlin, vor allem Bitwala[44], in den USA die Börse, Wechsel-

44 Bitwala wurde aus Frust über die deutschen Behörden zunächst in Großbritannien anstatt in Berlin angemeldet. In einem wütenden Interview warf Gründer Jörg von Minckwitz der deutschen Finanzaufsicht BaFin vor, „alles im Keim zu ersticken, was auch nur im Ansatz Bitcoin-belastet ist". Um hier zu bestehen, brauche man ein Heer von Anwälten und viel Kapital. Bezeichnenderweise gelang es Bitwala mithilfe von Investoren, sich wieder in Deutschland anzusiedeln. Bitcoinblog.de,

stube und Online-Wallet Coinbase, der Zahlungsdienstleister BitPay sowie die Altcoin-Börsen Bittrex und Poloniex[45] und in China der Hersteller von Mining-Hardware Bitmain, um nur einige wenige Beispiele zu nennen.

Für eine lange Zeit bangte die Bitcoin-Szene, ob nicht ein weltweites Verbot erfolgen würde. Seit Anfang 2017 scheint dies vom Tisch zu sein. Bitcoin ist in so gut wie allen westlichen Staaten legal und selbst in an sich restriktiven Nationen wie Russland oder China nicht vollständig verboten, sondern eingeschränkt erlaubt. Der Markt ist aus der Grauzone herausgetreten.

Kenne deine Kunden!

Die Bitcoin-Unternehmen, die in den letzten Jahren zum Objekt der staatlichen Charme- und Regulierungsoffensive geworden sind, spielen dabei eine zwiespältige Rolle.

Auf der einen Seite teilen sie den weltanschaulichen Enthusiasmus ihrer Kunden. Die Unternehmen wurden aus Begeisterung gegründet, für monetäre Autonomie und ein staatenfreies, wertstabiles digitales Geld. Die Gründer haben nicht ihre Lebenszeit investiert, um Informationen für den Staat zu sammeln – aber auch nicht, um Drogenhandel, Steuerhinterziehung, Geldwäsche oder Erpressung zu befördern.

Oliver Flaskämper und seine Partner etwa haben Bitcoin.de gegründet, weil sie in der Kryptowährung das Geld der Zukunft und ein digitales Gold sehen. Dass Bitcoin auch von Kriminellen benutzt wird, ist für sie vor allem ein Ärgernis.

Ohnehin kann es sich kein Unternehmen leisten, Sachzwänge zu ignorieren. Egal wie stark das innere, ideologische Investment ist – kein Bitcoin-Unternehmen kann überleben, wenn es sich der Kooperation

„Irgendwann hat man die Wahl: Man hört auf oder wandert aus“, 01.07.2015, https://bitcoinblog.de/2015/07/01/irgendwann-hat-man-die-wahl-man-hort-auf-oder-wandert-aus/ [06.03.2018]

45 Gerade Bittrex und Poloniex sind gute Beispiele dafür, dass sich Plattformen selbst dann irgendwie halten können, wenn es sie eigentlich gar nicht geben dürfte. In den meisten Staaten der USA ist es strikt verboten, Finanzdienstleistungen wie den Umtausch von Kryptowährungen ohne umfangreiche Anti-Geldwäsche-Maßnahmen zu betreiben. Würde jedoch eine Altcoin-Börse dieselben Maßnahmen anwenden wie Börsen, die mit Fiat-Geld, also Bankkonten verbunden sind, wäre sie nicht mehr wettbewerbsfähig. Bittrex und Poloniex scheinen irgendwie einen Weg gefunden zu haben, sich mit den Aufsehern trotz allem zu verständigen.

mit der Polizei verweigert. Viele erfolgreiche Unternehmen begrüßen sogar den Kontakt mit den Behörden, weil er ihnen die Chance gibt, proaktiv auf die unvermeidbare Regulierung einzuwirken. So wie Bitcoin.de arbeiten zahlreiche andere europäische Firmen, etwa BitPanda und LocalBitcoins, mit der europäischen Polizeibehörde Europol sowie den nationalen Polizeibehörden zusammen und beteiligen sich zudem an kriminologischen Forschungsprojekten wie BITCRIME, in dem Juristen, Kriminologen, Informatiker und Ökonomen zusammentreffen, um Richtlinien für eine fruchtbare Regulierung auszuarbeiten.

Börsen und andere Handelsplattformen werden zu wichtigen Helfern der Strafverfolgung. So gut wie überall auf der Welt gelten mittlerweile starke KYC-Regeln. KYC steht für „Know Your Customer", übersetzt „Kenne Deine Kunden", und ist eine Kernstrategie im Kampf gegen Geldwäsche. Die Unternehmen müssen die Identität ihrer Kunden verifizieren. In Deutschland geschieht dies oft über das Post-Ident, also per Sichtprüfung des Ausweises in einer Postfiliale, im Ausland oft durch ein Video-Identifizierungsverfahren oder ein Selfie mit Ausweis.

Das Ziel der Regulierung ist es, die Punkte zu kontrollieren, an denen Kryptowährungen gegen Fiat-Geld wie Euro getauscht wird. Dies ermöglicht es der Polizei, Verbrecher zu überführen, wenn diese versuchen, ihre Bitcoins zu wechseln. Die Börsen übernehmen dabei die Rolle, die die Banken beim Fiat-Geld spielen – sie sind der Mittelsmann, der der Regierung berichtet und in ihrem Auftrag Maßnahmen gegen Geldwäsche ausführt.

Wie die konkrete Regulierung gestaltet sein soll, steht dabei noch nicht fest. Zwar hat die EU Bitcoins bereits unter das allgemeine europäische Geldwäschegesetz gestellt, doch nicht jeder ist überzeugt, dass dies in allen Bereichen, etwa Wallets, durchsetzbar ist, ohne Innovation abzuwürgen – während auf der anderen Seite bezweifelt wird, ob die herkömmlichen Anti-Geldwäsche-Maßnahmen ausreichen, um Kryptowährungen zu kontrollieren.[46]

46 Im Juli 2016 hat die EU-Kommission beschlossen, auch virtuelle Währungen unter die sogenannte Vierte Direktive zu stellen, die den Rahmen der Gesetze gegen Geldwäsche in der EU darstellt. Sie begrenzt Barzahlungen auf 7500 Euro, verpflichtet zahlreiche Unternehmer – darunter auch Makler und Glücksspielanbieter – zu KYC-Maßnahmen und dazu, bei bestimmten Verdachtsmomenten Meldung zu erstatten. Laut der Kommission soll jede Firma, die virtuelle Währungen für ihre Kunden aufbewahrt, also vor allem Börsen und Wallets, aber auch viele weitere Plattformen, diese Regeln einhalten. In mehreren Bereichen, etwa Wallets oder Altcoin-Börsen, verlieren

Die Juristin Paulina Pesch, die im BITCRIME-Projekt geforscht hat, erklärt einen möglichen ausbalancierten Ansatz der Regulierung: „Die Idee ist es, die Transaktionen, die in Zusammenhang mit Straftaten stehen, etwa bei der Lösegeldzahlung einer digitalen Erpressung, in einer Liste zu markieren und es Intermediären wie Börsen oder Wallets grundsätzlich zu verbieten, Bitcoins aus Transaktionen anzunehmen, die auf dieser Liste stehen. So können wir diese schmutzigen Bitcoins durch die ganze Blockchain verfolgen.“[47] Eine Blacklist hätte den Vorteil, dass man nicht jeden Bitcoin-Nutzer unter Generalverdacht stellen müsste, es aber gleichzeitig möglich wäre, gezielt zu verhindern, dass kriminell vorbelastete Bitcoins zurück auf den Markt strömen.

Um zu verstehen, was genau Frau Pesch meint, wenn sie davon redet, dass man „schmutzige Bitcoins durch die ganze Blockchain verfolgen“ kann, muss man mehr über die Privatheit von Bitcoins wissen.

Verräterische Bitcoin-Transaktionen

Manchmal wird gesagt, Bitcoin sei anonym. Dies ist falsch, sogar grundfalsch. Bitcoin ist nicht anonym, sondern transparent. Es ist sogar das transparenteste Geld, das die Menschheit jemals hatte.

Erinnern wir uns an das Prinzip, das Bitcoin und anderen Kryptowährungen zugrunde liegt: Jeder Knoten im Netzwerk speichert und prüft alles. Das ist der Kern des Designs. Damit eine Blockchain funktioniert, müssen alle Knoten in der Lage sein, alle relevanten Informationen zu verstehen und zu bewerten. Daher müssen Transaktionen immer im Klartext vorliegen, also unverschlüsselt. Jeder weiß, wer wem wie viel schickt. Nichts an einer Bitcoin-Transaktion ist geheim.

EU-Bitcoin-Firmen damit fast jegliche Chance, auf den internationalen Märkten konkurrenzfähig zu sein. Dass es dennoch eine Vielzahl blühender Bitcoin-Unternehmen in der EU gibt, deutet darauf hin, dass die Einzelstaaten im Tausch gegen Einfluss und Handlungsmacht bereit sind, ein Auge bei der Umsetzung der Direktive zuzudrücken. Siehe Bitcoinblog.de, Virtuelle Währungen sollen EU-weit reguliert werden. Weil es alle Arten von Wallets treffen kann, droht die EU zur No-Go-Area für Bitcoin-Start-ups zu werden, 06.07.2017,
https://bitcoinblog.de/2016/07/06/virtuelle-waehrungen-sollen-eu-weit-reguliert-werden-weil-es-alle-arten-von-wallets-treffen-kann-droht-die-eu-zur-no-go-area-fuer-bitcoin-startups-zu-werden/ [01.03.2018]

47 Interview mit Paulina Pesch: Bitcoinblog.de, „Wir streben eine innovationsfreundliche Regulierung an“, 26.01.2017,
https://bitcoinblog.de/2017/01/26/wir-streben-eine-innovationsfreundliche-regulierung-an/ [01.03.2018]

Die einzige gute Nachricht für die Privatsphäre ist, dass keine Namen, sondern nur die Adressen gespeichert werden. Eine Adresse ist eine Kette aus etwa 34 willkürlich erscheinenden Zeichen, die von einem privaten Schlüssel abgeleitet werden.[48] Es hilft, sich eine Adresse zunächst wie eine IBAN-Kontonummer vorzustellen, da sie für den Benutzer eine ähnliche Funktion erfüllt – man kann mit ihr Geld empfangen.

Allerdings gibt es zahlreiche Unterschiede zwischen der Adresse und der IBAN-Nummer. So ist es bei einer Adresse für jeden ersichtlich, welches Guthaben sie hat und welche Transaktionen auf sie ein- und von ihr ausgehen. Zudem hat man nicht nur eine Adresse, sondern kann in einer Wallet beliebig viele bilden. Es wird sogar empfohlen, für jeden neuen Geldeingang eine neue Adresse zu verwenden.

Eine bessere Analogie als die IBAN-Nummer ist die Geldbörse, in der Münzen liegen. Jede Münze ist bei Bitcoin ein sogenannter Unspent Output[49]. Sie überweisen mir 0,01 Bitcoin: Ich erhalte eine Münze von 0,01 Bitcoin. Wenn Sie mir nun erneut 0,01 Bitcoin überweisen, erhöht sich nicht einfach mein Guthaben wie auf dem Bankkonto, sondern ich habe zwei Münzen à 0,01 Bitcoin.

So, wie ich im Supermarkt bezahle, indem ich mehrere Münzen übergebe, bildet eine Wallet eine Transaktion, indem sie passende Outputs zusammensetzt. Ich bezahle 0,02 Bitcoin, indem ich zwei Outputs à 0,01 Bitcoin nehme und diese als Inputs für eine neue Transaktion benutze. Dieses Verschmelzen von Münzen führt uns zu einer grundsätzlichen Problematik der Privatsphäre von Bitcoin-Transaktionen.

Wenn ich meine beiden Münzen mit unterschiedlichen Adressen empfangen habe, gibt es für einen Beobachter der Blockchain zunächst keinen Hinweis darauf, dass die beiden Münzen denselben Besitzer haben. Wenn ich beispielsweise auf meinem Blog eine Adresse für Spenden veröffentliche, sagt diese noch nichts darüber aus, wie viele Bitcoins ich auf den anderen in meiner Wallet verwalteten Adressen habe. Sobald ich sie aber verschmelze, wird dies sichtbar. Wenn man nicht sehr

48 Eine Adresse entsteht, wenn man aus dem privaten Schlüssel den öffentlichen Schlüssel bildet und diesen zweimal durch eine Hashfunktion treibt (s. Kapitel Geld: Monetäre Autonomie.)

49 Unspent Output, kurz: UTXO, repräsentieren bei Bitcoin tatsächlich eine Münze. Im Folgenden werden sie der Einfachheit wegen nur Output genannt.

genau aufpasst, verbinden sich über kurz oder lang alle Münzen in einer Wallet. Meist reicht es, eine einzige Adresse mit der Person zu verbinden, wie die Spendenadresse, die offensichtlich mir gehört, um das Guthaben und die Historie der gesamten Wallet preiszugeben. Ihre Finanzen werden gläsern.

An dieser Stelle dürfte auch die Rolle von KYC klar werden: Indem Börsen eine oder mehrere Ihrer Adressen mit Ihrem Namen verknüpfen, können Blockchain-Beobachter, die Daten von der Börse erhalten, jede Ihrer finanziellen Aktivitäten, damals, heute und morgen, beobachten. Viele, denen Privatsphäre am Herzen liegt, sind daher wenig begeistert von Bitcoin. Len Sassaman, ein 2011 verstorbener belgischer Cypherpunk, schrieb Jon Matonis, einem Bitcoin-Anhänger der ersten Stunde:

„Bitcoin ist weniger anonym als physikalisches Bargeld. DigiCash war im Vergleich anonymer […] Bitcoin fehlt die Eigenschaft der Unlinkbarkeit […] Jeder Gegner auf Staatsebene kann Bitcoin mit der echten Identität verbinden – oder zumindest mit einem echten Computer. Man fährt vermutlich geringfügig besser, wenn man Prepaid-Visa-Karten benutzt.“ [50]

Die Kryptoanarchie, deren dunklen Schatten wir weiter oben erahnt haben, rückt plötzlich in weite Ferne. An ihrer Stelle taucht ein totalitäres Finanzregime auf, in dem es überhaupt keine finanzielle Privatsphäre mehr gibt. Es könnte sein, dass sich mit Bitcoin die Rede des DigiCash-Erfinders David Chaum bewahrheitet: dass „gute oder schlechte Kryptographie den Unterschied zwischen Demokratie und Diktatur ausmacht“. Bitcoin wäre hier die schlechte Kryptographie.

Katz und Maus

Einmal wurde Satoshi in einer Mail darauf hingewiesen, dass man in der Kryptographie keine Lösung für politische Probleme finde. Satoshi stimmte zu, ergänzte aber: „Man kann eine wichtige Schlacht in einem Wettrüsten gewinnen und ein neues Gebiet der Freiheit für einige Jahre halten.“ [51]

50 The Monetary Future, Len Sassaman on Bitcoin, 05.06.2011, http://themonetaryfuture.blogspot.de/2011/07/len-sassaman-on-bitcoin.html [01.03.2018]

51 Satoshi in der Cryptography-Mailingliste, 07.11.2008, http://satoshi.nakamotoinstitute.org/emails/cryptography/4/ [01.03.2018]

Dieser Kampf um Terrains ist längst in vollem Gange. Es findet ein Katz-und-Maus-Spiel zwischen den Verfechtern der Privatsphäre und den Überwachern statt. Zug folgt auf Zug. Wir schauen uns im Folgenden die Taktiken und Gegentaktiken an.

Was in keiner Datenbank ist, hinterlässt keine Spur: Eine der wirkungsvollsten Strategien, um zu verhindern, dass Bitcoin-Adressen mit dem eigenen Namen verbunden werden, ist, zu vermeiden, dass der eigene Name in einer Datenbank steht. Logisch. Ohne Name läuft die Analyse ins Leere.

Also werden Bitcoins nicht per Banküberweisung gekauft – denn diese sind mit einem Namen verbunden –, sondern mit Bargeld. Plattformen wie LocalBitcoins bringen Käufer und Verkäufer zusammen, die sich dann treffen und Bitcoins gegen Bargeld tauschen. Einen ähnlichen Effekt haben die Bitcoin-Geldautomaten.

Die Behörden reagieren. In den USA mischten sich Undercover-Polizisten unter die Szene, Verkäufer wurden wegen wissentlicher Beihilfe zur Geldwäscherei angeklagt. In Deutschland hat die Aufsicht den Handel über LocalBitcoins nicht verboten, aber zumindest rechtlich so sehr erschwert, dass die Plattform 2014 den Betrieb in Deutschland einstellte. Auch Bitcoin-Geldautomaten sind hierzulande so gut wie nicht existent, da die Aufsicht fast ausnahmslos eine Erlaubnis verlangt, aber noch niemals eine vergeben hat.

In anderen Ländern, wo die Automaten präsenter sind, etwa in der Schweiz, in Österreich oder Großbritannien, machen die Behörden oft Auflagen. So müssen die Automaten-Betreiber etwa die Identität der Kunden durch biometrische Prüfungen sicherstellen. Zudem hat die Polizei zum Teil begonnen, die Bitcoin-Automaten zu überwachen.

Die Transaktionen mischen: Sobald größere Summen im Spiel sind, führt kaum ein Weg an einer Börse vorbei. Dadurch wird der echte Name mit einer Bitcoin-Adresse verbunden. Man kann nun nur noch versuchen, den Schaden zu begrenzen, indem man die Spuren auf der Blockchain verwischt.

Eine grundlegende Taktik und mittlerweile längst Best Practice ist es, immer eine neue Adresse zu verwenden, wenn man Geld erhält. Da man langfristig aber nicht daran vorbeikommt, Münzen zu verbinden, wird

es schwierig, den Überblick zu bewahren, welche Bündel an Wallets man verschmilzt.

Diese Wallet-Hygiene verlangt viel Disziplin und ist aufwändig und langfristig unzureichend. Daher werden zuweilen sogenannte Mixer verwendet: Sie mischen Transaktionen, so dass nicht mehr erkennbar ist, wer wem was gesendet hat. Das ist, wie wenn Sie mir ein Glas Wasser geben, indem Sie es in einen großen Eimer schütten, aus dem ich es selbst schöpfe: Es ist nicht zu rekonstruieren, dass das Wasser von Ihnen kommt.

Allerdings kranken die Mixer daran, dass jeder, der sie benutzt, sehr schnell mit kriminellem Geld in Verbindung gebracht wird. Man läuft also Gefahr, dass das Guthaben auf eine Blacklist kommt, und macht sich ohne Not zum Ziel von Polizeiermittlungen. Darüber hinaus muss man dem Besitzer des Mixers vertrauen, dass er weder das Geld unterschlägt noch die Logdateien an die Polizei weiterreicht. Schließlich gibt es ohnehin bereits Analysewerkzeuge, die manche Formen der Mixer durch komplexe Heuristiken brechen können.

Für viele Kryptographen ist es ein dankbares Feld, sich bessere und dezentrale Mixer auszudenken. So haben etwa Forscher der Universität Saarbrücken mehrere Versionen der Mixer-Software CoinShuffle entworfen, die das Potenzial hat, Mixing zum Bestandteil von Wallets zu machen.[52] Kryptographen des berühmten MIT, Massachusetts Institute of Technology, haben mit TumbleBit ein Konzept entwickelt, bei dem die Münzen gemischt werden, ohne dass sie die Blockchain berühren und ohne dass eine Zwischenpartei sie stehlen kann oder ihre Herkunft kennt.[53] Confidential Transactions schließlich ist eine von der Bitcoin-Firma Blockstream – speziell vom Bitcoin-Entwickler Gregory Maxwell[54] – entwickelte und mithilfe von Forschern der Universität

52 Tim Ruffing, Pedro Moreno-Sanchez, Aniket Kate: CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin; 19th European Symposium on Research in Computer Security (ESORICS 14). Mittlerweile hält Tim Ruffing CoinShuffle für gebrochen, hat aber bereits eine verbesserte Version entwickelt.

53 Ethan Heilman, Leen Al-Shenibr, Foteini Baldimtsi, Alessandra Scafuro, Sharon Goldberg: TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub, NDSS '17, Juni 2016, https://eprint.iacr.org/2016/575.pdf [01.03.2018]

54 Gregory Maxwell, Confidential Transactions, https://people.xiph.org/~greg/confidential_values.txt [01.03.2018]

Stanford verfeinerte[55] Methode, um die versendeten Beträge zu verschleiern.

All dies sind wundervolle, ausgefeilte, hochkomplexe Methoden. Das Problem ist jedoch, dass keine davon im Einsatz ist und auch keine Ambitionen erkennbar sind, sie in mittelfristiger Zukunft zum Einsatz zu bringen. Die Bitcoin-Blockchain ist, muss man feststellen, ein offenes Buch für geschulte Beobachter.

Sich auf anderen Blockchains verstecken: Eine immer wichtigere Rolle beim Erhalt der Privatsphäre spielen die Altcoins, die alternativen virtuellen Währungen neben Bitcoin: Ethereum, Litecoin, Dash, Monero und so weiter.

Auf den meisten Altcoin-Börsen werden nur Kryptowährungen gegen Kryptowährungen gehandelt. Es ist kein Fiat-Geld und keine Bank im Spiel, weshalb diese Börsen oft wenig bis gar nicht reguliert werden. Meist reicht eine E-Mail-Adresse, um sich anzumelden. Für einige Jahre war es einfach, durch sie die Kette von Transaktionen zu brechen: Man tauscht Bitcoins auf einer Altcoin-Börse gegen, sagen wir, Litecoin, sendet diese an eine andere Börse und tauscht sie dort gegen Bitcoins. Solange man kein international gesuchter Terrorist oder Administrator eines großen Darknet-Marktplatzes ist, wird der Aufwand, bei beiden Börsen Daten einzuholen, größer sein als die Motivation, Transaktionen zu verbinden.

Allerdings haben die Regulierer bereits begonnen, sich die Altcoin-Börsen vorzunehmen. Wie von anderen Börsen verlangen sie von diesen, ihre Kunden zu kennen (KYC). Heute lassen die meisten Altcoin-Börsen es zwar zu, dass man sich nur mit einer E-Mail-Adresse anmeldet, doch sobald man Kryptowährungen abbuchen möchte, muss man sich ausweisen.

Eine Ausnahme sind Plattformen wie ShapeShift, eine weitere Erfindung von Eric Vorhees, dem Gründer der Bitcoin-Glücksspiel-Seite Satoshi Dice. Bei ShapeShift kann man unzählige Kryptowährungen gegeneinander tauschen, ohne sich anzumelden. Man wählt ein Währungspaar aus, sagen wir, Bitcoin gegen Ethereum, und gibt eine

55 Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell: Bulletproofs: Short Proofs for Confidential Transactions and More“, https://eprint.iacr.org/2017/1066.pdf [01.03.2018]

Zieladresse an, in unserem Fall auf Ethereum. ShapeShift gibt dann eine Bitcoin-Adresse zurück, tauscht die Bitcoin, die dort eingehen, gegen Ethereum und sendet diese an die angegebene Ethereum-Adresse. So wie bei Satoshi Dice nutzt ShapeShift die Blockchain, um auf Accounts zu verzichten. Und wo es keine Accounts gibt, kann es auch kein KYC geben.

Allerdings legt ShapeShift alle Daten, die die Firma hat, offen und gibt auf Anfrage bereitwillig Informationen an Behörden weiter. Auf diese Weise ist es weiterhin möglich, die Kette von Transaktionen zu rekonstruieren, wenn man bereit ist, die Blockchains verschiedener Kryptowährungen zu analysieren.

Also begann die Kryptoszene, Altcoins mit besserer Privatsphäre zu benutzen. Dash beispielsweise. Diese als Darkcoin gestartete Kryptowährung hat ein integriertes Mixing-Verfahren durch sogenannte Master-Nodes. Noch weiter geht die Kryptowährung Monero. Sie hat Ring-Signaturen und Confidential Transactions implementiert, was sowohl die Beträge von Transaktionen verschleiert als auch die Verbindung zwischen Sender und Empfänger kappt. Zcash schließlich hat einen Zero-Knowledge-Proof integriert, der es ermöglicht, sämtliche zu einer Transaktion gehörende Daten zu verschlüsseln und dennoch zu prüfen, ob diese korrekt sind. Diese Altcoins übertragen an sich lediglich die Privatheit des analogen Bargeldes in den digitalen Raum und setzen damit das Versprechen um, das die Cypherpunks und David Chaum in digitalem Bargeld sahen. Europol registriert ihre immer verbreitetere Nutzung in der Internetkriminalität jedoch mit Besorgnis.[56]

Man könnte dieses Katz-und-Maus-Spiel noch lange fortsetzen. Es wäre aber falsch, wenn nicht gefährlich, es sich lediglich als Wettrüsten zwischen Kriminellen und der Polizei vorzustellen und das Brechen der

56 Europol, IOCTA, S. 61, erwähnt vor allem Monero und Zcash. Insbesondere Monero scheint bei lichtscheuen Internet-Usern an Beliebtheit zu gewinnen: „Transaktionen können nicht einem bestimmten User / einer Adresse zugeschrieben werden, alle Coins darin sind standardmäßig ‚versteckt', und die Historie der Transaktionen ist privat. Monero wird von einer wachsenden Anzahl an Darknet-Märkten akzeptiert und seit 2017 auch von der ersten Ransomware verlangt."
Neben Monero und Zcash erwähnt Europol auch Ethereum. Während diese Kryptowährung an sich keine besonderen Maßnahmen zur Erhöhung von Privatsphäre implementiert hat, könnten es die Smart Contracts möglich machen, dass sich dezentrale Märkte bilden, auf denen Währungen getauscht und Drogen gehandelt werden. Auch wenn dies noch nicht realisiert ist, versetzt auch diese Möglichkeit Strafverfolger in Sorge, da solche Märkte selbst bei erfolgreichem Abschluss der Ermittlungen nicht mehr vom Netz genommen werden können.

Transaktionshistorie mit Geldwäsche gleichzusetzen. Denn wer würde es akzeptieren, dass sein Bankkonto in einer öffentlichen Datenbank ausliegt, in die nicht nur das Finanzamt, sondern jeder einsehen kann? Wie kann etwas, das im normalen Leben vollkommen selbstverständlich ist, zu Geldwäsche werden, nur weil es digital passiert?

Wenn die Instrumente, mit denen man die Privatsphäre von Bitcoins erhöht, verboten oder nur von Kriminellen benutzt werden, wird Bitcoin zur transparentesten, gläsernsten Währung, die es jemals gab. Die Kryptowährung droht dann, nicht in eine Kryptoanarchie, sondern in einen digitalen Kontrollstaat zu führen. Dies sollte man sich vor Augen führen, wenn man die Erhöhung der Privatsphäre von Bitcoin-Transaktionen kurzerhand mit Geldwäsche gleichsetzt. Das ist sie nicht.

Fußarbeit funktioniert weiterhin

Die Sorge, dass die Polizei nicht in der Lage ist, mit den Cyber-Gangstern Schritt zu halten, lässt sich leicht beschwichtigen. Man muss lediglich einen Blick auf die Schlagzeilen der Webseite deepdotweb.com werfen.

Das Blog ist eine Art „Branchenmagazin" der Schwarzmärkte im Darknet. Die meiste Zeit über veröffentlichte es Tipps, wie man die Schattenmärkte benutzt, brachte Interviews mit deren Admins und schrieb Leitfäden, wie man sich anonym im Netz bewegt. Mittlerweile handeln die Berichte aber fast nur noch von den neuesten Festnahmen.

Die Polizei erringt fast täglich Erfolge im Deepweb. Einige Schlagzeilen aus einer beliebigen Woche: In der Wohnung eines Online-Drogendealers in Nordrhein-Westfalen werden 2 Kilogramm Cannabis gefunden. Ermittler nehmen in Berlin einen Mann fest, der sich Waffen im Darknet bestellt hat. Ein junger Mann aus Sachsen wird verhaftet, weil er Falschgeld in Umlauf gebracht hat. Bei der Razzia findet die Polizei eine Cannabis-Plantage und einen Haufen chemischer Drogen. Und so weiter. Beinah Tag für Tag vermeldet irgendeine Zeitung aus irgendeinem Land, dass ein weiterer Darknet-Verbrecher überführt wird, in den USA, in Indien, China, Deutschland, Frankreich, Russland.

Meist sind es nicht die Analysen der Blockchain, die die Polizei zu den Kriminellen führen – sondern die guten, alten, mühsamen Ermittlungen. Interpol, Europol und das BKA sind längst Experten für das

Darknet und für Bitcoin. Die Polizei gründet internationale Arbeitsgruppen, veranstaltet Workshops, in denen die Darknet-Markets simuliert werden, arbeitet mit der Post zusammen, wird selbst zum Käufer oder Verkäufer auf den Märkten, lokalisiert Pakete und so weiter. Man könnte es Fußarbeit nennen. Es ist arbeitsintensiv, aber es wirkt.

Neben vielen Festnahmen von Dealern und zum Teil auch Konsumenten gelingt der Polizei gelegentlich auch ein großer Schlag gegen die Darknet-Markets selbst. Ihnen gehen meist langwierige, krimireife Ermittlungen von verschiedenen, oft internationalen Polizeibehörden voraus. Sie sind die Speerspitze der gegenwärtigen Polizeiarbeit im Cybercrime.

Der bekannteste und am besten dokumentierte Fall ist die Akte Silk Road. Er wurde mittlerweile von Dutzenden Journalisten ausgeleuchtet und erzählt und im Prozess von Ross Ulbricht öffentlichkeitswirksam ausgerollt.[57] Er ist eine hervorragende Fallstudie, die zeigt, wie die Polizei in mühevoller Fußarbeit die Verbrecher aus dem Deepweb zu Fall bringt.

Der Silk Road Shutdown

Ross Ulbricht alias Dread Pirate Roberts wurde schon 2011, als einige Senatoren in den USA danach riefen, die Silk Road abzuschalten, zu einem der meistgesuchten Kriminellen der USA. Mehrere Ermittlerteams verschiedener Behörden suchten einige Jahre lang nach ihm. Bemerkenswert sind hier vor allem zwei Teams: eine Cyber-Einheit des FBI in New York und die Baltimore Task Force der Drogenfahndung DEA.

Bei der DEA tat sich vor allem der Undercover-Agent Carl Force IV hervor. Force nahm über Chat-Räume Kontakt zu Dread Pirate Roberts auf, wobei er sich als „Nob", einen mexikanischen Drogenschmuggler ausgab. Im Lauf mehrerer Monate gewann er das Vertrauen von Ross Ulbricht. Irgendwann überredete Force den Silk-Road-Administrator, bei einem Drogengeschäft zu vermitteln, einer großen, günstigen Kokain-

57 Im US-amerikanischen Journalismus gibt es Dutzende exzellent geschriebener und gründlich recherchierter Artikel zu Ross Ulbricht und der Silk Road. Hier reicht es, auf die ausführliche, spannende zweiteilige Story der Wired, The Untold Stories of Silk Road, hinzuweisen. Diese Reportage erzählt die Geschichte von Aufstieg und Fall der Silk Road aus der Perspektive Ross Ulbrichts sowie der Ermittler der beteiligten Behörden. Siehe:
https://www.wired.com/2015/04/silk-road-1/ [01.03.2018]
https://www.wired.com/2015/05/silk-road-2/ [01.03.2018]

lieferung. Ross Ulbricht gab ihm eine Adresse in Utah, an die die Drogen geliefert werden sollten. Force schickte das Kokain an die Adresse – und ein Einsatz-Team der Polizei gleich hinterher.

Die Polizisten verhafteten Curtis Green, einen 47-jährigen Mann, als er das Paket mit dem Kokain öffnete. Force klappte den Laptop von Green auf. Darin fand er, zu seinem eigenen Erstaunen, Login-Daten für den Administratoren-Bereich der Silk Road und Chat-Protokolle mit *Dread Pirate Roberts*. Ihm wurde klar, dass er einen großen Fang gemacht hatte. Doch Dread Pirate Roberts, sein Hauptziel, sowie die Server der Silk Road waren weiterhin unerreichbar.

Also griff er zu einem fragwürdigen Mittel. Gemeinsam mit dem Computerexperten der Baltimore Task Force stahl er aus Greens Admin-Account heraus einen Haufen Bitcoins von der Wallet der Silk Road, damals etwa 300.000 Dollar wert. Als Dread Pirate Roberts später Nob von dem Vorfall berichtete und den Verdacht äußerte, dass ihn ein Mitarbeiter verraten habe, bot der DEA-Beamte an, Green um die Ecke zu bringen. Ross Ulbricht sendete Force einen Scan von Greens Führerschein und einen Vorschuss, den Akten zufolge auf ein Bankkonto in den USA. Allerdings schien all dies nicht wirklich weiterzuführen, weshalb die Geschichte von Carl Force an dieser Stelle im Sand verläuft.

Mehr Erfolg hatte eine New Yorker Cyber-Abteilung des FBI. In ihr suchten Computerexperten nach Schwachstellen im Tor-Netzwerk, um darin kriminelle Webseiten zu enttarnen. Ihr begehrtestes Ziel war die Silk Road. Mitte 2013 gelang es den FBI-Beamten schließlich, den Server in einem Rechenzentrum in Island zu finden.

Wie dies dem FBI gelang, bleibt bis heute ein Rätsel. Denn eigentlich sind Server in den Hidden Services von Tor anonym. Es sollte technisch gar nicht möglich sein, den physischen Ort des Servers zu lokalisieren. Die offizielle Version des FBIs lautet, dass es an einem Fehler der Seite lag, einem schlecht implementierten Captcha. Einige Experten bezweifeln dies aber. Das FBI habe die wahre Adresse erhalten, indem es die Silk Road gehackt habe, etwa durch eine sogenannte SQL-Injection[58].

58 SQL-Injection bedeutet, dass man in einem Eingabefeld auf einer Webseite, etwa einem Kontaktfeld, ein Stück Code eingibt, das in der Datenbank, auf dem Server der Webseite, einen Befehl triggert. Dies ist eine beliebte Methode, um Webseiten zu hacken, und auf den meisten Seite laufen täglich Dutzende von Versuchen ein, Kontaktfelder durch SQL-Injektionen zu manipulieren (was in der Regel durch aktualisierte Software blockiert wird).

Und da die Ermittler keine Genehmigung für einen solchen Hack gehabt hätten, baue die Anklage auf unzulässigen Beweismitteln auf.

Einer anderen Theorie zufolge hat sich das FBI von Forschern einer Universität verdächtige Tor-IP-Adressen geben lassen und diese zum Ausgangspunkt einer Analyse der IP-Adresse des Silk-Road-Servers gemacht. Schließlich wird auch spekuliert, dass das FBI die NSA gebeten habe, die Tausende von Internet-Knoten zu nutzen, die sie weltweit betreibt, um einen großen Lauschangriff auf das Tor-Netzwerk zu fahren. Das eine wie das andere wäre illegal gewesen.

Wie auch immer es dazu kam: Einige FBI-Mitarbeiter flogen nach Island, statteten dem Thor-Rechenzentrum einen Besuch ab und ließen sich eine Festplatte aushändigen. Auf dieser Festplatte war die Silk Road, der größte Online-Schwarzmarkt dieser Zeit und vermutlich die erste große kriminelle Organisation, die man in eine Aktentasche stecken konnte.

Als Ross Ulbricht im Sommer 2013 der Forbes ein Interview als Dread Pirate Roberts gab und tönte, er werde die Silk Road niemals aufgeben, war die Seite bereits unter Kontrolle des FBI. Während der König des Online-Schwarzmarktes erklärte, dass die Regierung den Krieg gegen die Drogen wegen seiner Plattform verloren habe, durchwühlten Computer-Forensiker die Daten des Servers nach Spuren und kamen dem Menschen, der hinter dem Pseudonym Dread Pirate Roberts stand, unweigerlich näher.

Die meisten IP-Adressen, die das FBI in den Logdateien der Silk Road fand, gehörten zum Tor-Netzwerk. Sie waren nutzlos. Allerdings fanden die Ermittler auch einige andere IP-Adressen, die zu „virtuellen privaten Netzwerken“ (VPN) führten. VPNs sind Dienstleister, durch deren Server man seinen Datenverkehr „tunneln“ kann. In der Darknet-Szene wird ein VPN gewöhnlich dem Einstieg ins Tor-Netzwerk vorgeschaltet, um zu verhindern, dass der Internet-Provider – oder die NSA – mitbekommt, dass man Tor benutzt. Offenbar hatten also Administratoren der Silk Road vergessen, nach dem Einwählen ins VPN auch Tor zu aktivieren. Das FBI fragte bei den VPN-Anbietern nach den Daten und erhielt einige echte IP-Adressen. Eine davon führte sie nach San Francisco – zu Ross Ulbricht.

Dies waren noch sehr vage Hinweise, weit davon entfernt, Beweise

zu sein. Als sich die Ermittler diesen Ross Ulbricht jedoch näher anschauten, konnten sie den Verdacht durch weitere Spuren erhärten, die er ganz am Anfang seiner Karriere als Darknet-König hinterlassen hatte. So hatte er etwa in den ersten Wochen der Silk Road unter dem Namen Altoid in Online-Foren auf den Marktplatz und seine dort angebotenen Zauberpilze hingewiesen. In einem anderen Forum hatte er mit demselben Namen, aber seiner echten, auf Ross Ulbricht lautenden Gmail-Adresse gefragt, wie man eine Seite im Tor Hidden Service hostet. Auch dies ist ein kleiner, schwacher Hinweis, ein Puzzlestück unter vielen.

Ross Ulbricht war der Hauptverdächtige – aber es fehlten die harten Beweise. Ein Ermittler sagte einmal, der einzige hieb- und stichfeste Beweis wäre es, wenn man Ross Ulbricht dabei erwische, wie er als Dread Pirate Roberts eingeloggt sei. Im Sommer 2013, etwa einen Monat nach dem Interview, gelang dies: Die Polizei beobachtete Ross Ulbricht, wie er in einer Bibliothek in San Francisco am Laptop saß und arbeitete. Gleichzeitig chatteten mehrere Agenten des DEA undercover mit Dread Pirate Roberts, und das FBI überwachte den gekaperten Silk-Road-Server. Dann beendete Dread Pirate Roberts die Chats. Das FBI sah, dass sich der Admin der Silk Road ausloggte. Kurz darauf klappte Ross Ulbricht seinen Laptop zu.

Das reichte. Die Beamten von DEA und FBI, die getarnt in der Bibliothek gelauert hatten, verhafteten Ross Ulbricht. Anschließend ging die Silk Road offline. Besucher sahen nun das grüne Silk-Road-Kamel, darüber das Logo des FBI und die Nachricht, dass diese Webseite konfisziert sei.

Transparenz auch für den Staat

Der Shutdown der Silk Road hatte einige hochinteressante Folgen. Die erste war, dass die US-Regierung erstmals in den Besitz einer bemerkenswerten Menge Bitcoins gekommen war.

Unmittelbar nach der Verhaftung von Ross Ulbricht wurden gut 144.000 Bitcoin auf eine Adresse gesendet. Das FBI bestätigte, dass es sich dabei um Coins handelte, die man von dem Administrator der Silk Road beschlagnahmt hatte. Damals waren diese Bitcoins etwa 20 Millionen Dollar wert. Da die Regierung die Einheiten der Kryptowährung nicht als Geld betrachtete, sondern als Sache, behandelte sie sie wie

andere konfiszierte Dinge: Sie versteigerte sie. Bis zur Versteigerung sollten noch einige Monate vergehen, und weil der Kurs von Bitcoin bis dahin von etwa 100 auf 600 Dollar gestiegen war, wurde die US-Regierung unfreiwillig zu einem der erfolgreichsten Bitcoin-Investoren dieser Zeit.[59]

Die Auszahlung der Bitcoins an die Gewinner der Auktion dürfte die transparenteste Transaktion sein, die jemals von einer Regierung gezeichnet wurde. Jeder wusste, wo die Coins lagen, und jeder sah, wie sie ihren Besitzer wechselten. Als etwa der prominente Investor Tim Draper das erste Paket von 30.000 Bitcoins ersteigerte, konnte jeder nachvollziehen, dass exakt jene Anzahl Bitcoins an eine einzelne Partei ausgezahlt wurde. Selten kam eine kryptographische Technologie dem hehren Ziel der Cypherpunks so nahe wie in diesem Moment: Privatsphäre für die Bürger, Transparenz für den Staat.

Dasselbe Thema, allerdings verzerrt im Spiegel der menschlichen Gier, finden wir in der zweiten Folge des Shutdowns. Diese bringt Carl Force IV, den Undercover-Drogencop, wieder ins Spiel. Nachdem er unter dem Pseudonym Nob für Dread Pirate Roberts angeblich den Auftragsmord an Green begangen hatte, konnte er nicht widerstehen, sich selbst in einem klassischen Bitcoin-Verbrechen zu versuchen: Er erpresste den Silk-Road-Admin mit einer anderen Identität um einige tausend Bitcoin. Mit Erfolg. Rein formal würden auch diese Bitcoins dem Staat gehören, da sie im Zuge einer Ermittlung erbeutet wurden, und müssten versteigert werden. Allerdings hätte Force sie, juristisch betrachtet, niemals haben dürfen. Also machte er das, was er von Dread Pirate Roberts gelernt hatte: Er versuchte, die Bitcoins zu waschen und auf verschiedenen Börsen zu verkaufen.

Die Kommission, die die Ermittlungen im Fall Silk Road prüfte, entdeckte zahllose Ungereimtheiten bei Force: halbdienstliche Anrufe bei

59 Allgemein profitieren die Regierungen durch Beschlagnahmungen massiv von der Kryptowährung und ihrem rasanten Wertzuwachs. Das extremste Beispiel ist Bulgarien, das angeblich mehr als 200.000 Bitcoins durch das Zerschlagen eines Schmuggelrings eingenommen hat. Theoretisch machte der Wert dieser Bitcoins ein Drittel der jährlichen Steuereinnahmen des Landes aus – doch es ist unklar, ob die Regierung tatsächlich im Besitz der Coins ist, ob sie es jemals war oder ob sie irgendwie versickert sind. Auch Thailand wurde mit der Beschlagnahmung von 100.000 Bitcoins nach der Verhaftung des Infraud-Administrators zu einem der großen Gewinner des Aufstiegs von Bitcoin. Die 129 Bitcoins, die das Land Hessen Ende 2017 für knapp 2 Millionen Euro verkauft hat, nehmen sich dagegen sehr klein aus – waren aber, immerhin, auch eine gern gesehene Einnahme für die Staatskasse.

Börsen, seltsame Transaktionen, Interessenskonflikte, Nebenjobs, eine Verschlüsselung von Nachrichten, die nicht notwendig gewesen wäre.[60] Die Analyse der Blockchain bewies schließlich, dass Force von Ross Ulbricht Bitcoins empfangen und diese verkauft hatte.

Das öffentliche Kontobuch von Bitcoin zeigt eben alles und vergisst nichts. Der Erste, der diese Lektion mit voller Härte lernen sollte, war vermutlich der korrupte Staatsdiener Force. Er wurde zu einer mehrjährigen Gefängnisstrafe verurteilt.

Wie man eine Hydra enthauptet

Nach der Schließung der Silk Road ging die Welt des Darknet-Handels nicht unter. Im Gegenteil: Alle Zeitungen, Online-Magazine und sogar die 20-Uhr-Nachrichten berichteten darüber, und es wurde zum Allgemeinwissen, dass man im Internet Drogen bestellen und mit dem Online-Drogenhandel Millionen verdienen kann.

In der Szene begann ein Wettbewerb darum, der nächste Dread Pirate Roberts zu werden. Erst übernahmen Sheep Market und BlackmarketReloaded die vakante Führungsposition. Sheep Market tauchte nach einigen Monaten ab – der Besitzer machte den berühmten Exit Scam[61]. BlackmarketReloaded wickelte den Markt etwas später geordnet ab, vermutlich, weil der Betreiber Angst bekam, von Ermittlern gefunden zu werden.

Danach kam die Silk Road II. Dann Agora, Evolution, Alphabay, Hansa und viele weitere Märkte. Immer, wenn ein Kopf abfiel oder abgeschlagen wurde, wuchsen neue nach. Die Polizei ermittelte weiter. Sie analysierte Daten, tauschte Wissen aus und bildete internationale Netzwerke, um die Darknetmarkets länderübergreifend zu verfolgen. Ein Meilenstein war die Operation Onymous im November 2014. Behörden aus 17 Ländern, darunter Europol, das FBI, die Polizei von

60 Force und Dread Pirate Roberts verschlüsselten ihre E-Mails auf Initiative des Polizisten. Da gute PGP-Verschlüsselung Beweisstücke effektiv vernichtet und Ermittler es daher wenn möglich vermeiden, PGP zu benutzen, erregte dies den Verdacht der Prüfer.

61 Exit Scam ist im Bitcoin-Bereich eine beliebte Methode anonymer Administratoren, das Geschäft auf lukrative Weise abzuwickeln: Der Betreiber nimmt die Plattform einfach vom Netz, behält die vielen Bitcoins der Kunden, die er auf seinen Wallets verwahrt, und taucht in der Anonymität des Internets ab. Gerade bei den Darknetmarkets ist der Exit Scam die bei weitem häufigste Variante, eine Plattform aufzulösen.

Irland und Australien, zerschlugen laut Polizeiangaben 400 Webseiten im Tor-Netzwerk, darunter das Hauptziel Silk Road II, der zu dieser Zeit beliebteste Markt, aber auch weitere Märkte, Geldwäsche-Plattformen, Foren und Shops. Rund 17 Administratoren von Märkten und Drogendealer wurden verhaftet, rund eine Million Dollar in Bitcoin beschlagnahmt.

Doch wie stets wuchsen der Hydra neue Köpfe. Es kam, wie es ein Bericht von Europol und dem Europäischen Zentrum für Drogen und Drogenmissbrauch (EMCDDA) schildert:[62] Der Shutdown einzelner Märkte und Plattformen lässt den Handel kurzzeitig abflauen, doch die Szene ist „resilient". Innerhalb von wenigen Wochen bildeten sich neue Leitmärkte, zu denen die Dealer und ihre Kunden migrierten. Man kann eine Hydra nicht besiegen, wenn man die Köpfe nur abschneidet.

Daher suchte die Polizei nach anderen Strategien. In der griechischen Mythologie besiegte Herkules die Hydra, indem er ihre Köpfe ausbrannte. Vielleicht hatte sich die Polizei an dieser Geschichte orientiert, denn im Sommer 2017 – just zu jener Zeit, als sich die pompöse Rallye jenes Jahres gerade aufheizte – glückte ihr ein brillanter und nachhaltiger Schlag gegen das Darknet.

Es handelte sich erneut um eine internationale Aktion, an der das FBI, die Polizei von Thailand sowie deutsche und niederländische Polizeieinheiten die Hauptrollen spielten. Als Erstes wurde in Thailand der Administrator von Alphabay festgenommen. Alphabay war zu dieser Zeit bereits seit mehr als einem Jahr der mit Abstand größte Markt. Der Admin war ein 26-jähriger Kanadier, der in einer Villa lebte, Lamborghinis sammelte und sich für 60.000 Dollar den seiner Meinung nach schnellsten Gamer-PC der Welt gekauft hatte. Nach der Festnahme erhängte er sich in seiner Zelle in Bangkok. Alphabay war wichtig gewesen, und der Shutdown würde die Szene irritieren, doch der Polizei war klar, dass es nicht lange dauern würde, bis sich ein anderer Markt an seine Stelle setzen würde. Daher kombinierte sie den Shutdown mit einer zweiten Aktion, die den Boden ausbrennen sollte, auf dem die Märkte ewuchsen.

62 Europol und European Monitoring Center for Drugs and Drug Addiction: Drugs and the Darknet. Perspective for Enforcement, Research and Policy, 2017, http://www.emcdda.europa.eu/system/files/publications/6585/TD0417834ENN.pdf [02.03.2018]

Die Darknet-Community reagierte auf das Ende von Alphabay so wie immer: Sie wanderte beinah routinemäßig auf den zweitgrößten Markt aus, was zu dieser Zeit Hansa war. Genau, wie die Polizei es geplant hatte. Denn Hansa stand zu diesem Zeitpunkt längst unter der Kontrolle der niederländischen Ermittler. Diese hatten bereits einige Monate vorher herausgefunden, dass sich der Server der Seite in einem Datenzentrum in Litauen befand, was dann zu zwei Männern aus Nordrhein-Westfalen geführt hatte, 30 und 31 Jahre alt, welche umgehend von der deutschen Polizei verhaftet wurden. Anstatt den Markt abzuschalten, übernahmen jedoch die niederländischen Beamten die Kontrolle.

Als der Exodus von Alphabay kam und Drogendealer und -konsumenten in Scharen auf die Seite strömten, hatte die Polizei bereits die Accounts von großen Händlern übernommen und die PGP-Schlüssel anderer Händler so manipuliert, dass sie die Nachrichten der Kunden im Klartext lesen konnten. Die Behörden sammelten einen Berg von Informationen, die zu Dutzenden und Hunderten Anklagen gegen Dealer und deren Kunden führten und noch führen werden.

Diese Festnahmen sind aber nicht der wichtigste Effekt dieser Operation. Viel wichtiger ist der Abschreckungseffekt. Er zielt direkt auf den Rumpf, aus dem die neuen Köpfe nachwachsen. Wer soll noch den Märkten vertrauen, ihnen Bitcoins und private Daten geben, wenn die Polizei jeden Händler und jeden Administrator austauschen konnte? Natürlich vernichtete auch dieser Schlag die Darknet-Märkte nicht. Auf ihnen wird weiterhin gehandelt. Aber es scheint, dass die Polizei es geschafft hat, ihr weiteres Wachstum auszubremsen.

Vinnik der Geldwäscher

Beinah zur selben Zeit, als Alphabay und Hansa geschlossen wurden, gelang der Polizei ein weiterer großer Schlag gegen den Cybercrime.

Erinnern Sie sich an die Hacks, die in den Jahren 2011 und 2012 die Bitcoin-Börsen umgetrieben haben? An die angeblichen 400.000 Bitcoin, die bei Mt. Gox Ende 2013 verschwunden sind? Das Rätsel um den Verbleib dieser Coins wurde im Sommer 2017 gelöst, als die Polizei Alexander Vinnik, einen 37-jährigen russischen Staatsbürger, in Griechenland verhaftete. Vinnik wird vorgeworfen, mehr als eine

Milliarde Dollar gewaschen zu haben und in die Börse BTC-E involviert gewesen zu sein.

BTC-E war schon immer ein Mysterium der Bitcoin-Welt. Es war eine der ältesten Börsen überhaupt, und den Besitzern war es, über komplizierte Zahlungswege, irgendwie gelungen, Dollar anzunehmen, aber anonym zu bleiben. Man munkelte, dass die Betreiber irgendwo in Bulgarien, Russland oder Zypern saßen. Gelegentlich klagten User, dass BTC-E Bitcoins unterschlug, aber im Großen und Ganzen galt die Börse als Hort der Stabilität in den Bitcoin-Märkten – als ein geradezu seriöses Piratennest.

Im Sommer 2017 konfiszierte das FBI die Server von BTC-E. In den Daten der Seite entdeckten sie, dass Vinnik beteiligt war. Einige Berichte sagen, er sei der Administrator gewesen, andere, ein Mitglied im Kundensupport, und wieder andere, dass er schon längst nicht mehr für die Börse gearbeitet habe. Egal. Es gab eine Verbindung, und dies reichte, um einen Verdacht zu erhärten, den Ermittler aus den USA und Japan schon lange verfolgten.

Nachdem Mt. Gox im Frühjahr 2014 so spektakulär pleite gegangen war, hatte das Gericht von Tokio die Cyberdetektei WizSec damit beauftragt, die angeblich verlorenen 400.000 Bitcoins auf der Blockchain zu suchen. Einen Tag, nachdem Vinnik verhaftet worden war, präsentierte WizSec die Resultate der Nachforschungen: „Wir werden nicht lange darum herumreden: Vinnik ist unser Hauptverdächtiger beim Diebstahl von Mt. Gox (oder beim Waschen der Beute danach). Das ist das Ergebnis von Jahren der geduldigen Arbeit, und das, was wir herausgefunden haben, wurde mit Sicherheit auch unabhängig von uns von anderen Ermittlern enthüllt. Jeder, der an dem Fall arbeitete, verhielt sich ruhig, während wir unsere Erkenntnisse an die Strafverfolger weiterleiteten, damit die Verdächtigen nicht gewarnt und die Chancen auf eine Festnahme maximiert werden.“[63]

Neben den Gox-Coins entdeckten die Ermittler in den Wallets von Vinnik auch die Beute zahlreicher berühmter Hacks der Jahre 2011 und 2012, etwa von Bitcoinica oder BitFloor und vielen anderen. Im Grunde gab es kaum einen großen Hack, dessen Beute nicht irgendwie

63 WizSec: Breaking Open the Mt. Gox Case, Part 1, https://blog.wizsec.jp/2017/07/breaking-open-mtgox-1.html [02.03.2018]

in Vinniks Waschstraße gelandet war. Über ein Gewimmel von Adressen führte der Russe die Coins auf verschiedene Börsen, überwiegend BTC-E, aber zum Teil auch auf Mt. Gox selbst, um sie dort gegen Dollar zu tauschen.

Vinnik wusste mit Sicherheit, was er tat. Er vertraute nicht blauäugig darauf, dass Bitcoins anonym sind. Am Ende fiel aber auch er der Transparenz der Kryptowährung zum Opfer. Denn Bitcoin-Transaktionen stehen für alle Ewigkeit im großen Kontobuch.

Der bemerkenswert geringe Umfang der Darknet-Märkte

Die Erfolge der Polizei gegen die Darknetmarkets haben auch Antworten auf eine Frage erbracht, die lange Zeit die Diskussion von Bitcoin dominiert hat: Wie wichtig sind die Drogenmärkte für die Kryptowährung? Ist Bitcoin einfach nur eine avantgardistische Methode, um Geld zu waschen, die nebenbei als Wertspeicher und Spekulationsobjekt gehypt wird?

Bis etwa 2016 haben die Massenmedien Bitcoin fast immer mit Drogen und anderen kriminellen Machenschaften in Verbindung gebracht. Einmal, 2013, haben engagierte Bitcoiner in einem Online-Forum für Computerspiele dafür geworben, Bitcoin als Währung in Spielen zu verwenden. Ein Gamer sagte, er wolle nicht, dass über seinen Computer Drogen verkauft würden. Dies war lange der allgemeine Eindruck, und ohne Zweifel hat die Silk Road eine große Rolle bei der Geldwerdung von Bitcoin gespielt. Erst auf den Schwarzmärkten wurde Bitcoin zu einer echten Währung.

Allerdings war die Bedeutung des Drogenhandels schon 2013, als die Silk Road geschlossen wurde, überschaubar. Die Daten des Servers zeigten, wie viele Bitcoins die Plattform tatsächlich prozessiert hatte: seit Mitte 2011 etwa 9,5 Millionen. Klingt nach viel, aber man muss bedenken, dass ein Bitcoin 2011 und 2012 nicht mal zehn Euro wert war. Der Umsatz auf der Silk Road machte nicht einmal 5 Prozent des gesamten auf der Bitcoin-Blockchain umgesetzten Volumens aus. Satoshi Dice, die damals populärste Bitcoin-Glücksspiel-Seite, brachte ebenso viel auf.

Die Darknetmarkets sind seitdem gewachsen. Aber längst nicht so sehr, wie man erwarten könnte, und wesentlich langsamer als Bitcoin als Ganzes. Im Sommer 2017 zeigte sich, dass der Umsatz auf Alphabay, dem größten Marktplatz, etwa zwei- bis viermal so hoch wie der der Silk Road gewesen war. Über einen Zeitraum von vier Jahren, so die Studie von Europol und EMCDDA, wurden in der EU auf den vier größten Darknetmarkets etwa 70 Millionen Euro umgesetzt. Dies ist ein kaum signifikanter Teil des gesamten Drogenhandels der EU, und die Summe wird noch irrelevanter, wenn man sie in Relation zum allgemeinen Bitcoin-Handel auf den Börsen setzt. Auch der neueste Europol-Bericht notiert, dass die Darknet-Märkte im Vergleich zu anderen Spielarten des Cybercrimes deutlich langsamer wachsen.

Europol folgert daher, dass der Drogenhandel im Darknet es bisher nicht in den Mainstream der Kriminellen geschafft hat. Es könnte sein, dass er es einmal wird. Aber derzeit ist er noch weit davon entfernt, und es gibt auch keine Anzeichen dafür. Das echte Drogenproblem findet weiterhin auf der Straße und nicht im Netz statt.

Privatsphäre für die Kleinen oder für die Großen?

David Chaum hatte versucht, die Quadratur des Kreises zu lösen, als er in den 90ern eCash entwickelte. Er wollte ein digitales Bargeld schaffen, das die Privatsphäre der ehrlichen Bürger schützt, aber unattraktiv für Kriminelle ist. eCash sollte vollkommen anonym sein – aber nicht für Verbrecher.

Die meisten Datenschützer stimmen zu, dass dies ein nobles Ziel ist. Massenüberwachung muss bekämpft werden, da sie Demokratie und Freiheit bedroht. Sie ist das, was Facebook, Google und die NSA machen: Sie speichern alles, was man speichern kann. Jeder wird anlasslos und umfänglich überwacht, und der hehre Grundsatz, dass jeder als unschuldig zu gelten hat, bevor das Gegenteil bewiesen ist, wird auf den Kopf gestellt. Das Internet ist zu einer Überwachungsmaschinerie geworden, gegen die die Bespitzelung durch die Stasi in der DDR harmlos wirkt.

Observation gilt für die meisten dagegen als in Ordnung und sogar wünschenswert. Observation meint die Fußarbeit der Polizei. Beamte ermitteln auf den verschiedensten Wegen, verfolgen, recherchieren,

beobachten, um schließlich Kriminelle wie Ross Ulbricht oder den Admin von Alphabay zu überführen. Kaum jemand würde dagegen protestieren. Es ist gut, dass der Staat in der Lage ist, Verbrecher aufzuspüren. Auch mit digitalen Methoden.

In der idealen Welt sollte Massenüberwachung nicht möglich sein, Observation dagegen schon. Bei Bitcoin könnte es auf das Gegenteil hinauslaufen: keine Observation, aber Massenüberwachung. Denn es ist zwar schwierig, die Kette der Transaktionen zu brechen, aber mit dem entsprechenden Know-how nicht unmöglich. Ein technisch gewiefter Verbrecher, der unerkannt bleiben will, weiß der Observation zu entgehen. Wer hingegen weder den dringenden Wunsch noch das Wissen hat, seine Spuren auf der Blockchain zu verwischen, dem droht die Massenüberwachung. Seine gesamten finanziellen Aktivitäten können analysiert, gedeutet und auf ihn zurückgeführt werden, automatisch und in Echtzeit.

An sich liegt in Bitcoin eine große Chance für den Schutz der Privatsphäre. Die Kryptowährung stellt das gewohnte Verhältnis auf den Kopf: Während bei Banken Guthaben und Transaktionshistorie privat, aber der Klarname bekannt ist, bleibt dieser bei Bitcoin privat, aber Guthaben und Historie werden öffentlich. Es wäre möglich, dass dieses Verhältnis das Versprechen der Cypherpunks erfüllt: Privatsphäre für die Kleinen, aber Transparenz für die Großen. Denn es ist kaum möglich, auf einer Blockchain richtig große Summen zu verbergen. Wenn beispielsweise die Staatsfinanzen auf ihr prozessiert würden, könnten die Bürger in Echtzeit verfolgen, was damit geschieht. Gleichzeitig wären die alltäglichen Ausgaben der Menschen klein genug, um sich mit relativ einfachen Methoden effizient im Schwarm zu verstecken. Die Kleinen wären strukturell im Vorteil. Auch eine solche Zukunft könnte mit Bitcoin Wirklichkeit werden.

Die Geschichte des Geldes steht also erneut an einem Scheidepunkt, und die Richtung, die wir einschlagen, wird darüber entscheiden, wie die Welt aussieht, in der wir einmal leben werden.

» Hier in der Schweiz gibt es schöne Seen und Flüsse, die Leute haben Wege drum herum gebaut, weil es schön ist, drum herum zu laufen.

➳ ➳ ➳ ➳ ➳ ➳ ➳

Dann haben sie Straßen gebaut, und mittlerweile haben wir zwei- bis dreispurige Straßen und auch Zuglinien um die Seen herum. «

– Jonas Schnelli