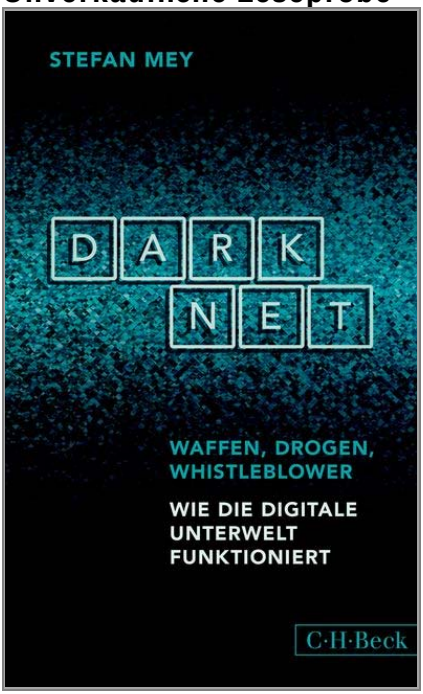
C.H.BECK
www.chbeck.de

Unverkäufliche Leseprobe



Stefan Mey
Darknet
Waffen, Drogen, Whistleblower
Wie die digitale Unterwelt funktioniert

2017. 239 S.: Klappenbroschur
ISBN: 978-3-406-71383-5

Weitere Informationen finden Sie hier:
http://www.chbeck.de/20384484

C·H·Beck
PAPERBACK

Stefan Mey

DARKNET

WAFFEN, DROGEN, WHISTLEBLOWER

Wie die digitale
Unterwelt funktioniert

C.H.Beck

Originalausgabe

© Verlag C.H.Beck oHG, München 2017
Gesetzt im Verlag
Druck und Bindung: Pustet, Regensburg
Umschlaggestaltung: Geviert, Grafik und Typografie, Christian Otto
Umschlagabbildung: shutterstock
Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)
Printed in Germany
ISBN 978 3 406 71383 5

www.chbeck.de

Inhalt

1

Einleitung

Reise ins Darknet

Da ist dieses Versprechen. Es lautet: Das Darknet ist ein freier, wilder Ort, an dem keinerlei Regeln gelten. Eine unkontrollierbare Unterwelt, in der der Staat mit seinen Ermittlungsbehörden und Geheimdiensten ausgesperrt bleibt und auch die großen Netzkonzerne nichts gelten.

Immer wieder geistert das «Darknet» durch die Medien. Es ängstigt uns und zieht uns gleichzeitig an. Es verheißt Freiheit, Abenteuer und Anarchie und scheint dabei nicht nur Traum, sondern zugleich auch Alptraum zu sein, ein Ort für die finstersten Seiten der menschlichen Seele.

Den meisten begegnet die digitale Unterwelt in Form medialer Horrorgeschichten: Im Darknet, so lesen wir, werde mit Waffen und gefährlichen Drogen gehandelt wie anderswo mit Büchern oder CDs, Cyberkriminelle und Terrorgruppen würden sich für digitale oder ganz realweltliche Attacken rüsten.

Und doch schimmert in den Berichten über das Darknet oft auch etwas Hoffnungsvolles hindurch. In ein oder zwei Sätzen heißt es meistens, dass die Anonymität des Darknets nicht nur für düstere Zwecke genutzt werde, sondern auch mutigen Oppositionellen und Whistleblowern helfe, die geheime Dokumente über Missstände an die Öffentlichkeit bringen.

Wie sieht diese Parallelwelt aus? Ist das Darknet gut, böse

oder irgendetwas dazwischen? Wer sucht warum Schutz in der digitalen Anonymität? Und lohnt sich ein Besuch in der digitalen Unterwelt?

Mit diesem Buch gehen wir gemeinsam auf eine Reise in diese digitale Unterwelt. Wir werden erfahren, dass vieles von dem, was über das Darknet bekannt ist, eher Mythos als Realität ist. Wir wollen das Darknet mit all seinen Widersprüchen, faszinierenden Momenten und Potenzialen erforschen. Die Zeit der großen Entdeckungen ist eigentlich vorbei, kaum ein Ort auf der Welt ist noch nicht beschrieben und vermessen. Doch das Darknet ist Terra Incognita – es ist unbekanntes, digitales Land.

Die Reise beginnt

Zum Anfang des Buchs schauen wir, was es mit den verschiedenen Begriffen wie «Darknet», «Deep Web» oder «Clearnet» auf sich hat. Nachdem wir das geklärt haben, gehen wir auf unsere Reise. Sie hat einen klaren Ausgangspunkt. Auf der Seite www.torproject.org laden wir ein Programm herunter, das der Türöffner zur digitalen Unterwelt ist: den Inhalten unter der inoffiziellen Darknet-Endung .onion, basierend auf der Anonymisierungssoftware Tor.

Will jemand das Darknet mit einem Browser wie Chrome, Internet Explorer oder Firefox betreten, spuckt dieser trotzig eine Fehlermeldung aus: «Der Server konnte nicht gefunden werden.» Das Darknet öffnet sich nur für den Tor-Browser, der als eine Art digitale Tarnkappe unsere Identität verschleiert.

Auf der ersten Station unserer Reise lernen wir, dass Darknet und Internet eines gemein haben: die treibende Kraft des Kommerzes, die aus der ideologisch so umkämpften digitalen Unterwelt vor allem eine große Einkaufsmeile für Drogen aller Art gemacht hat. Hier können sich harte Junkies ihren gefährlichen «Stoff» besorgen, hier holen sich Freizeitkon-

sument*innen bequem ihr Gras oder ihre Partypillen für den Rausch am Wochenende. Mit wenigen Klicks lassen sich auch verschreibungspflichtige Medikamente, teilweise Waffen, gehackte Kreditkartendaten und sogar Falschgeld bestellen. Eine hoch organisierte, illegale Kommerzlandschaft hat sich entwickelt, mit hohen Tagesumsätzen und mit Skurrilitäten wie AGBs und Empfehlungsprogrammen.

Dann schauen wir auf das «böse» Darknet, wie es uns in regelmäßigen Abständen auf den Titelbildern seriöser wie halbseidener Zeitschriften begegnet: die digitale Unterwelt als Hort für alles Schlechte, zu dem der Mensch fähig ist. Wir lernen, wie die Anonymität für den Tausch von Kinderpornographie missbraucht wird, und gehen der Frage nach, ob sich dort tatsächlich international agierende Terrorgruppen mit Waffen versorgen. Gegenpol dazu ist die Erzählung vom Darknet als Schutzraum – für Oppositionelle, für Whistleblower und einfach für Leute, die im Netz nicht länger gläsern sein wollen. Während die illegale Seite der digitalen Unterwelt mittlerweile zumindest schwach ausgeleuchtet ist, ist kaum bekannt, was sich auf der «guten» Seite befindet. Bekannt ist nur, dass das Darknet zwar zur Hälfte aus illegalen Inhalten besteht, zur anderen Hälfte aber nicht. Wir erfahren, wieso dieser Ort mit all seinen Widersprüchen einige Menschen dennoch zum Träumen bringt.

Sodann schauen wir genauer darauf, wie das Darknet und die damit verbundene Anonymisierung «funktioniert»: wie durch einen genialen Trick Anonymität im ansonsten fast flächendeckend überwachbaren Internet hergestellt wird. Wir staunen über ein Netzwerk, das sich über die halbe Welt erstreckt und durch seine Architektur dem Darknet seine robuste Unzensierbarkeit verleiht. Wir sehen, wie die technologische Basis dieses Wunderwerks einst von Forschern des US-Militärs erdacht wurde und heute Staaten so viel Kopfzerbrechen bereitet. Wir lernen die Organisation kennen, die heute hinter der Anonymisierungssoftware der digitalen Unterwelt steht und die so widersprüchlich wie das Darknet selbst ist.

Schließlich schauen wir Ermittlern über die Schulter, die berufsbedingt das Darknet verstehen wollen. Wir sehen, wie sie sich in einem niemals endenden Katz-und-Maus-Spiel diesen sperrigen Ermittlungsgegenstand vornehmen und mit den technologischen und rechtlichen Grenzen ihrer Arbeit kämpfen.

Wie jede größere Reise endet unser Trip mit einem Blick in die Zukunft. Wir überlegen uns, wie sich das Darknet entwickeln könnte. Vor allem könnte es eine Antwort auf den heutigen Zustand des «normalen» Internets sein, der besorgniserregend ist: Jede Kommunikation und jede kleinste Lebensäußerung im Netz ist überwachbar und landet auf den Servern großer Netzkonzerne, die daraus profitable Profile erstellen und sie auf Anfrage bereitwillig Geheimdiensten übergeben. Die Überwachungs- und Kontrollmöglichkeiten von Regierungen haben ein Ausmaß erreicht, bei dem sich manche Menschen an Dystopien wie den Science-Fiction-Klassiker «1984» erinnert fühlen.

Wir entwerfen Szenarien für die weitere Entwicklung und stellen am Ende eine auf den ersten Blick gewagt anmutende Frage: ob sich aus der digitalen Unterwelt von heute nicht eines Tages eine freiere und bessere Variante des Internets entwickeln könnte. Und wir gehen noch einen Schritt weiter und schauen, wie eine konkrete Utopie des Darknets aussehen könnte. Dann gibt es noch einen Anhang mit unter anderem vier Kurzinterviews mit Gesprächspartner*innen aus dem Buch, einem Blick auf alternative Darknet-Technologien, einer Diskussion der Sicherheit von Tor und einem Glossar zum Darknet.

2

Was ist das Darknet?

Eine Begriffsklärung

Zuerst müssen wir klären, was das Darknet eigentlich ist. Viele kennen den emotional aufgeladenen Begriff aus Schlagzeilen, die periodisch in Medien auftauchen, meistens im Anschluss an eine Verhaftung wegen Waffen- oder Drogenhandels im Darknet.

Eine Schlacht um Begriffe

Für das «Darknet» existieren verschiedene, eher vage Definitionen. Eine sinnvolle lautet: Ein Darknet ist ein digitaler Ort, der sich mit technologischen Mitteln abschirmt und Anonymität bei der Nutzung herstellt. Verbindungsdaten und Standorte von Rechnern werden verschleiert, die Kommunikationsinhalte sind verschlüsselt. So sollen vor allem neugierige Blicke von Konzernen und Geheimdiensten ausgesperrt werden. Ein Darknet lässt sich nicht mit herkömmlichen Internet-Browsern, sondern nur mit einer speziellen Software betreten, und die üblichen Suchmaschinen listen die Inhalte nicht auf. Es gibt verschiedene Möglichkeiten, ein derart technisch abgeschirmtes Netz herzustellen. Das am meisten verbreitete ist das Darknet auf Basis der Software Tor, für das es einen speziellen Anonymisierungsbrowser gibt. Es ähnelt

aber sehr dem normalen World Wide Web, deswegen wird manchmal auch von «Dark Web» gesprochen.

Gegenbegriff ist das offene Netz, das auch «Clearnet» oder «Surface Web» (Oberflächen-Web) genannt wird. Dessen Inhalte werden mit üblichen Browsern angesteuert, und sie werden von gebräuchlichen Suchmaschinen wie Google, Yandex oder Bing angezeigt. Das können Texte der Online-Enzyklopädie Wikipedia sein, Artikel auf Nachrichten-Seiten und Blogs, Foren-Diskussionen oder die Produkte von Webshops.

Dann gibt es noch das «Deep Web», um das sich ähnlich viele Mythen wie um das Darknet ranken. Für dieses «tiefe Netz» ist charakteristisch, dass es zwar theoretisch mit jedem Browser besucht werden kann, dass seine Inhalte aber dennoch nicht von Suchmaschinen erfasst und somit auch kaum von Usern gefunden werden können. Das kann verschiedene Gründe haben: Einige Webseiten verbieten Suchmaschinen, sie zu durchsuchen, und diese halten sich meistens auch daran. Gar nicht zugänglich für Google & Co. sind Webseiten, die nur nach Eingabe eines Passworts ihre Inhalte preisgeben: Magazine, Foren oder Blogs, die nur einen bestimmten Personenkreis zulassen wollen, die Inhalte in sozialen Netzwerken oder auch journalistische Angebote, deren Inhalte hinter einer Bezahlschranke stehen. Auch Intranets von Unternehmen, Behörden oder Organisationen sind «von außen» nicht zugänglich.

Die Begriffe ermöglichen eine grobe Orientierung, sie sind technisch aber nie ganz trennscharf. Neben den klassischen Webseiten gibt es im großen, weiten Internet verschiedene Inhalte, die für einen Browser nicht zugänglich sind, weil sie über eigene Programme ablaufen. Es gibt spezielle Software für Text- und Videochat, Software zum legalen oder illegalen Streaming von Musik. Auch viele Games mit ihren komplexen Spielewelten lassen sich mit Chrome, Firefox oder Internet Explorer nicht betreten. Hinzu kommen die mobilen Nutzungswelten. Auf dem Smartphone werden Inhalte oft nicht über Browser abgerufen, sondern es wird eine App ins-

talliert, ein vom jeweiligen Anbieter bereitgestelltes mobiles Programm.

Der Eisberg lockt

Die Verwirrung steigt noch dadurch, dass die Begriffe «Darknet» und «Deep Web» mitunter unbeholfen durcheinandergeworfen werden. In Berichten über das Darknet taucht oft das Bild eines Eisbergs auf. Das World Wide Web, wie wir es kennen, sei nur die Spitze, die aus einem digitalen Meer voller Informationen ragt. Und so, wie die im Meer sichtbare Spitze sehr viel kleiner als der darunter liegende Eisberg ist, sei auch das uns allen bekannte Netz winzig im Vergleich zum Deep Web (von dem das Darknet wiederum ein Teil ist). Von den «Tiefen des Internets» spricht eine Illustration des Bundeskriminalamts. Und dieses Deep Web soll, wie es wenig präzise heißt, «10- bis 100-mal größer als das Surface Web» sein. Andere Medienberichte legen sogar nahe, das Deep Web sei mindestens 400-mal so groß. Dieses Bild legt nahe, dass es irgendwo einen digitalen Kosmos an Informationen und Inhalten gibt, den noch kaum jemand betreten hat.

Das klingt spannend, gehört aber zu den Mythen, die sich in die Berichterstattung über das Darknet eingeschlichen haben. Die Eisberg-Metapher wird oft unhinterfragt verwendet – vielleicht, weil sie so einleuchtend klingt und zum gesicherten Wissen über das Darknet zu gehören scheint, vielleicht auch, weil sich digitale Phänomene schwer bebildern lassen, so dass man lieber nicht fragt, wie valide die Erkenntnis dahinter ist.

Und sie ist es in diesem Fall nicht. Die Aussage, dass das Deep Web sehr viel größer als das «bekannte» Web sei, entstammt nicht universitärer Forschung, sondern einem «Whitepaper» der Firma BrightPlanet, die sich darauf spezialisiert hat, für Kunden Inhalte und Entwicklungen im Internet zu beobachten – beispielsweise, um Urheberrechtsverlet-

zungen aufzuspüren. Das Whitepaper wurde im Jahr 2000 veröffentlicht. Ein Forscher von BrightPlanet war durch grobe Hochrechnungen zum Schluss gekommen, dass das Deep Web 400- bis 550-mal größer als das normale World Wide Web sei.

Damals waren Suchmaschinen nur in der Lage, statische Webseiten mit fest definierten Inhalten auszulesen. Probleme hatten sie hingegen bei Datenbanken, die ihre Inhalte erst nach Eingabe eines Suchbegriffs anzeigen, etwa staatliche Geo- oder Patent-Datenbanken, aber auch Webshops oder Kleinanzeigenportale. Heute gelingt es Suchmaschinen und vor allem Google allerdings sehr gut, alle denkbaren Inhalte zu finden und mittels automatisierter Abfragen zu erschließen. Es gibt immer noch unzugängliche digitale Bereiche: Inhalte, die hinter Login-Fenstern oder Bezahlschranken stehen, Intranets von Firmen und Organisationen und Datenbanken mit allzu komplexen Eingabeformularen.

Dem steht aber ein gigantisches Reservoir an Inhalten im offenen Netz gegenüber: Millionen oder Milliarden an Youtube-Videos, die mit Textbeschreibungen versehen und somit Suchmaschinen-verständlich sind, an Blogposts und Nachrichtenartikeln, an Fotos auf Social-Media-Portalen. Seit dem Jahr 2000 hat sich sehr viel verändert. Das eingängige Bild vom Eisberg namens Deep Web, das gleichsam aus dem Frühmittelalter der Internet-Entwicklung stammt, wird trotzdem noch verwendet.

Auf ins Darknet

Auch das Darknet, das als Teil dieses Deep Webs gilt, ist nicht riesig. Es ist dennoch spannend. Mit seiner Unkontrollierbarkeit, seiner Anonymität und Unzensierbarkeit hebelt es sonst geltende Regeln des Netzes aus und hat vielleicht sogar das Potenzial, Machtverhältnisse der Gesellschaft als Ganzes in Frage zu stellen.

Ohne zu vergessen, dass es verschiedene technologische Möglichkeiten zur Errichtung eines abgeschirmten Parallelnetzes gibt, wollen wir uns in diesem Buch auf eines konzentrieren: das Tor-Darknet, unter der inoffiziellen Endung .onion, das als bisher einziges eine nennenswerte Dynamik entwickelt hat und auch jenseits von Tech-Kreisen bekannt ist.

3

Das Darknet als Einkaufsmeile

Die großen illegalen Marktplätze

Fünf Gramm Koks für 400 Euro bietet ein Händler an und verspricht «Top Qualität». Ein anderer Verkäufer hat Falschgeld im Angebot: zehn nachgemachte 50-Euro-Noten zum Preis von 100 Euro. Willkommen in der Kommerz-Welt des Darknets, scheinbar alles lässt sich hier mit wenigen Klicks bestellen. Man muss nicht mehr nachts in den Park gehen, um Zugang zu verbotenen Produkten zu bekommen. Auf den hoch illegalen Darknet-Märkten mit breiter «Produktpalette» lässt sich fast alles bequem von zu Hause aus bestellen.

Ist der anfängliche Schock über die offene Abwicklung eindeutig zweifelhafter Geschäfte überwunden, drängt sich ein anderes Gefühl auf: Diese illegale Welt im Darknet erscheint seltsam vertraut. Sie erinnert an den klassischen Onlinehandel, wie wir ihn von Amazon oder Zalando kennen. Der «Dark Commerce» ist der kleine, gerne verschwiegene Bruder des E-Commerce, und er hat viel von ihm gelernt.

Illegaler Handel auf hohem Niveau

Knapp 100 000 Produktangebote gibt es laut Eigenangaben auf Dream Market, dem momentanen Marktführer der Darknet-Wirtschaft. Und Dream Market ist nur ein Vertreter einer

immer größer werdenden Zahl an Märkten. Etwa ein Dutzend von ihnen listet Deepdotweb.com auf, das als eine Art Branchenblog die Szene begleitet. Die Märkte heißen «Valhalla», «The Majestic Garden» oder «House of Lions». Ein Markt namens «Darknet Heroes League», kurz DHL, hat dreist Logo und Kürzel der Deutschen-Post-Tochter gekapert. Während sich die Menschen, die Tor-Software entwickeln, wünschen, dass Whistleblower und Oppositionelle das Darknet für sich entdecken, wird das Darknet zurzeit überwiegend für eines genutzt: den hoch professionellen Kauf und Verkauf von Drogen. Die treibende Kraft des Kommerzes hat die digitale Unterwelt in eine große, illegale Einkaufsmeile verwandelt.

In Aufbau und Funktionsweise ähneln die Marktplätze ihren legalen Pendants im klassischen Internet. Wie auf Amazon oder Zalando gibt es ein Dreieck aus drei beteiligten Gruppen: Die einen kaufen und wählen aus der Vielfalt der Produkte aus. Dafür können sie die einzelnen Produktangebote mit internen Suchmaschinen filtern: welche Drogen genau es sein sollen, wer auch nach Deutschland verschickt, sogar eine gewünschte Preisspanne lässt sich angeben. Die anderen bieten ihre «Ware» an, oft unter identischem Namen auf verschiedenen Handelsplattformen. Sie verschicken die Produkte und erhalten im Gegenzug Zahlungen über die Digitalwährung Bitcoin. Die Leute hinter den Marktplätzen wiederum stellen die technische Infrastruktur zur Verfügung und entwickeln sie technisch weiter. Von allen getätigten Verkäufen erhalten sie eine Provision.

In einer Langzeit-Erhebung zwischen 2013 und 2015 haben zwei Forscher der US-amerikanischen Carnegie Mellon University die Welt des Dark Commerces beobachtet. Den Umsatz der großen Marktplätze schätzen sie auf 300 000 bis 600 000 Dollar pro Tag, den der kleineren Portale auf täglich wenige Tausende. Auf allen beobachteten Plattformen zählten sie insgesamt 9000 einzelne Händler*innen, die ihre Produkte durchschnittlich auf drei unterschiedlichen Marktplätzen an-

boten. Meist hatten sie sich spezialisiert, einige boten nur bestimmte Drogengruppen an, einige eine breite Palette an Rauschmitteln und Medikamenten. Andere hatten sich auf Falschgeld, Waffen oder gehackte Daten spezialisiert.

In einer etwas jüngeren Studie untersuchte die Suchtforscherin Meropi Tzanetakis vom Wiener Zentrum für sozialwissenschaftliche Sicherheitsforschung in Zusammenarbeit mit der IT-Spezialistin Tanja Bukac ausschließlich den zu der Zeit tonangebenden (und im Sommer 2017 von der Polizei geschlossenen) Darknet-Marktführer Alphabay. Im Beobachtungszeitraum von September 2015 bis August 2016 ermittelte sie einen Gesamtumsatz von 94 Millionen Dollar, wobei die monatlichen Werte stark differierten. Im Sommer stieg der Umsatz auf einen Maximalwert von 16 Millionen an. Aus der allgemeinen Drogenforschung ist bekannt, dass in der Zeit besonders viele Rauschmittel gekauft werden, vermutlich, da sich User für den Besuch von Musik-Festivals eindecken.

Tzanetakis schaute auch, von wo aus verschickt wird. Wenig überraschend gab das Mutterland des Internets auch hier den Ton an. 25 Prozent der Händler*innen saßen in den USA, mit einigem Abstand folgten das Vereinigte Königreich (9 Prozent) und Australien (9 Prozent). Auf Platz 4 dann mit 8 Prozent die Niederlande, gefolgt wiederum von der Bundesrepublik Deutschland, wo 7 Prozent ihren Sitz hatten. Die Umsätze der Händler*innen waren sehr ungleich verteilt. Oft schien sich das Ganze eher auf einem Freizeit- und Zuverdienst-Level zu bewegen. 56 Prozent hatten innerhalb des Beobachtungszeitraums von einem Jahr weniger als 10 000 Dollar umgesetzt. 5 Prozent kamen auf Umsätze von mehr als 200 000 Dollar, so dass sich nur bei wenigen vermuten lässt, dass sie tatsächlich professionell und erwerbsmäßig handeln.

Leitwährung Bitcoin

Die Preise der illegalen Waren werden je nach Marktplatz in US-Dollar oder Euro angegeben, tatsächlich bezahlt wird aber in Bitcoin. Die Ende 2008 erdachte Geldeinheit spielt trotz großer Medienaufmerksamkeit in der klassischen Wirtschaft nur eine Nischenrolle, in der Darknet-Ökonomie ist sie dagegen zur Leitwährung geworden, ohne die nichts gehen würde. Auf den Marktplätzen stellt der Bitcoin oft die einzige Zahlungsmöglichkeit dar, nur gelegentlich werden auch alternative Digitalwährungen akzeptiert. Der Gegenwert der Hackerwährung schwankt erheblich, zurzeit ist ein Bitcoin etwa 2000 Euro wert. Er lässt sich aber in bis zu 100 Millionen unterscheidbare Einzelteile untergliedern, über diese «Satoshis» lässt sich auch jeder Kleinstbetrag ausdrücken.

Der Bitcoin ermöglicht ein anonymes Verschieben von Geldeinheiten, genauer gesprochen ein pseudonymes: Mit Herunterladen der Bitcoin-Software bekommt man eine Adresse zugewiesen, ein aus zufällig zusammengestellten Zeichen bestehendes Nummernkonto. Überweisungen werden direkt zwischen diesen Nummernkonten abgewickelt.

Das Besondere daran ist, dass es keine zentralen Stellen gibt, die wie ansonsten in der Finanzwirtschaft Überweisungen protokollieren und Guthaben verwalten, Bank oder Paypal sind nicht erforderlich. Anders als im klassischen Geldverkehr ist es somit nicht möglich, Gelder einzufrieren oder Konten zu sperren. Die Kontrollfunktion zentraler Stellen übernimmt eine ausgefeilte, dezentrale Buchhaltung, die als eigentliches Meisterstück hinter der Erfindung des Bitcoins gilt: eine große Datenbank, in der für jeden einzelnen Coin und jeden Teil davon aufgezeichnet wird, wem er gerade gehört. Dieses Kassenbuch liegt nicht als Geschäftsgeheimnis auf den Servern eines Finanzdienstleisters, sondern ist über das Internet verteilt: Wer immer sich die Bitcoin-Software herunterlädt, holt sich automatisch auch eine Kopie der Daten-

bank mit auf den Rechner. Die aktualisiert sich regelmäßig, sie gehört allen und niemandem zugleich.

Ein besonderes Modell finanzieller Anreize sorgt dafür, dass Betrügereien und Manipulationen so gut wie unmöglich sind. Vor allem ein Problem hatte jede dezentrale Digitalwährung vor dem Bitcoin unzuverlässig gemacht: das betrügerische «Double Spending». Wie lässt sich verhindern, dass eine Geldeinheit doppelt ausgegeben wird? Wenn eine Zahlung vollzogen werden soll, prüft ein Teil der Bitcoin-«Crowd», die aus weltweit verteilten Rechnern besteht, ob alles mit rechten Dingen zugeht. Will beispielsweise Frau Müller dem Darknet-Händler ihres Vertrauens einen Bitcoin überweisen, wird in der Datenbank nachgeschaut, ob der jeweilige Bitcoin ihr zum jeweiligen Zeitpunkt tatsächlich gehört und ob sie ihn vielleicht zuvor schon einmal ausgegeben hat. Ist alles okay, wird die geplante Überweisung zusammen mit allen anderen Transaktionen zusammengefasst, in einen digitalen Block, der aus vielen Einzelinformationen besteht. Der wird an eine lange Kette vorheriger Transaktionsblöcke gehangen, die so genannte Blockchain. In ihrer Gesamtheit stellt diese Kette an Transaktionsblöcken das Kassenbuch des Bitcoins dar.

Rechner, die sich an der Prüfung und Verifikation von Überweisungen beteiligen, nehmen als Belohnung an einer Art Lotterie teil, sie lösen ein mathematisches Rätsel. In der Software des Bitcoin-Systems ist festgelegt, dass alle zehn Minuten eine bestimmte Zahl neuer Bitcoins entsteht, zurzeit sind es 12,5 Bitcoins. Wer das Rätsel knackt, erhält diesen kleinen Jackpot. Der hohe Stromaufwand, den das Checken von Transaktionen erfordert, wird dadurch ausgeglichen, dass statistisch jeder Rechner der Verifizierungs-Crowd irgendwann einmal die Belohnung kassiert.

Dieses Modell einer verlässlichen, dezentralen Datenbank ermöglicht es überhaupt erst, dass in großem Stil am Staat und an etablierten Instituten vorbei Gelder verschoben werden können. Es ist aber auch die Crux des Ganzen. Für jeden ein-

zelnen Bitcoin ist in der Blockchain protokolliert, welche Adresse ihn wann gehalten und an welche andere Adresse geschickt hat. Prinzipiell ist nicht bekannt, welche tatsächliche Identität sich hinter einem Bitcoin-Konto verbirgt. Es kann aber leicht geschehen, dass man sich doch ungewollt selbst verrät. Meist werden Bitcoins auf großen Börsen wie der deutschen Plattform Bitcoin.de gekauft. Damit das möglich ist, muss man vorher erst Geld vom normalen Bank-Konto auf das der Börse überweisen. In deren Datenbank schlummert somit potenziell die Information, welche Bitcoin-Adresse mit welchem realweltlichen Konto verknüpft ist. Und es besteht zumindest die Möglichkeit, dass Ermittlungsbehörden an diese Information gelangen.

Um die Bitcoin-Nutzung dennoch anonym gestalten zu können, werden verschiedene Wege eingeschlagen: Passionierte «Nerds» verabreden in einem Darknet-Forum einen Offline-Tausch. Mit heruntergezogenem Baseball-Cap treffen sie sich an einem dunklen Ort. Geldscheine werden herübergereicht, und vor Ort wird per Smartphone der gewünschte Betrag von Nummernkonto zu Nummernkonto transferiert. Es gibt aber auch technologische Lösungen. Bitcoin-Mix-Dienste haben sich darauf spezialisiert, gegen Zahlung einer kleinen Provision die Herkunft von Bitcoins zu verschleiern. Man zahlt Coins ein, innerhalb des Systems des Dienstleisters wird der Wert immer wieder von Konto zu Konto geschickt. Schließlich werden Bitcoins zurücküberwiesen, deren bisheriger Weg sich, so das Versprechen, nicht mehr rekonstruieren lässt.

[…]
