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

Vorwort

Die digitale Währung Bitcoin übt eine eigenartige Faszination aus, die bei manchen Menschen an Sucht grenzt. Vielleicht sogar an Besessenheit. Für den, der einmal vom „Bitcoin-Virus“ gepackt wurde, gibt es oft keinen Weg mehr zurück. Bitcoin wird nicht nur zum Hobby, sondern zum Lebensinhalt.

Ein Grund für diesen oft bestaunten Enthusiasmus dürfte sein, dass Bitcoin eine magisch anmutende Technologie ist. Die digitale Währung erzeugt etwas, das es eigentlich gar nicht geben darf: digitale Knappheit und Unveränderlichkeit. Alles im Internet kann beliebig vervielfältigt und verändert werden. Nur Bitcoin nicht. Obwohl rein digital, verhalten sich die digitalen Münzen zuweilen so, als seien sie physische Objekte. Das fühlt sich an, als wäre die Technologie aus der Zukunft gefallen.

Nicht minder wichtig dürfte sein, dass Bitcoin nicht nur Technologie ist, sondern auch Politik und Revolution. Und Revolution ist hier nicht als Marketing-Floskel gemeint, wie bei der neuen Zahnbürste, sondern im eigentlichen, historischen Sinn: als Angriff auf die herrschende Ordnung. Bitcoin ist eine neue, staatenlose Währung, die von niemandem beherrscht oder kontrolliert werden kann. Sie verspricht eine globale Währungsunion, in der es keine Zentralbanken, keine Kapitalkontrollen, keine Wechselkurse und keine Inflation mehr gibt.

Auch ich gehöre zu den Menschen, die der virtuellen Währung verfallen sind. Als ich Mitte 2013 bei Recherchen zufällig auf Bitcoin stieß, war ich sofort fasziniert. Ich las mich ein, und je mehr ich erfuhr, desto größer wurde mein Staunen und meine Faszination.

Kurz darauf begann ich für die deutsche Handelsplattform Bitcoin.de als Redakteur des Bitcoinblog.de zu arbeiten. Langweilig wurde mir in den folgenden Jahren nie. Es passieren so viele große und kleine Dramen rund um die Entstehung dieses neuen Geldsystems, jede Woche, fast jeden Tag. Irgendwann wurde mir klar: Bitcoin könnte die größte Geschichte unserer Zeit sein. Dieser Gedanke wurde zum Leitmotiv meines Buches.

Was ist Bitcoin? Wie ist die digitale Währung entstanden? Welche Ideen, welche Personen stecken dahinter? Wie tritt sie in die Welt, welcher Widerstand formiert sich dagegen? Was bedeutet sie wirtschaftlich, was politisch, und welche Utopien und Dystopien liegen in ihr? Meine Absicht war, das Phänomen Bitcoin in all seiner schillernden Vielschichtigkeit zu erfassen. Ich wollte nicht nur erklären, was Bitcoin ist und welches Potenzial es hat, sondern auch in die dunklen Winkel hineinleuchten und die vielen Geschichten erzählen, die den Aufstieg dieses neuen Geldes begleiten.

Natürlich bin dabei nicht neutral. Es wäre Unsinn, das behaupten zu wollen. Ich finde Bitcoin faszinierend und bin überzeugt, dass die digitale Währung das Geld der Zukunft ist. Ich glaube auch, dass ein freies, dezentral organisiertes Geldsystem wie Bitcoin der Menschheit eine beispiellose monetäre Autonomie schenkt, und dass daraus sehr viel mehr Vor- als Nachteile erwachsen. Für mich ist Bitcoin ein Teil des gesellschaftlichen Fortschritts, ein besonders aufregender Zweig der Digitalisierung, und ich bin gespannt, in welche Welt er uns führen wird.

Allerdings bin ich mir bewusst, dass dies keine Tatsache, sondern nur meine Meinung ist. Manche finden Bitcoin erschreckend, und es gibt gute Gründe dafür: den Kontrollverlust des Staates, die Gefahr, dass Steuereinnahmen austrocknen, die Attraktivität für Kriminelle, die nicht von allen geteilte Vision eines harten, deflationären Geldes … Bitcoin ist vieles, aber es ist keine unschuldige Technologie. Ich werde daher versuchen, so neutral wie möglich zu bleiben. Ich will nicht werben, sondern informieren, und Ihnen das Wissen vermitteln, durch das Sie sich selbst eine Meinung bilden können.

Der erste Teil des Buches führt Sie in die kryptographischen Grundlagen ein und erzählt, warum so viele Versuche, ein digitales Bargeld zu schaffen, vor Bitcoin gescheitert waren. Sie erfahren, was der Bitcoin-Erfinder Satoshi Nakamoto anders gemacht hat und warum seine Schöpfung so erfolgreich wurde. Außerdem lernen Sie seine ersten Mitstreiter kennen – und können mitspekulieren, wer sich hinter dem Pseudonym Satoshi verbirgt.

Der zweite Teil des Buches betrachtet Bitcoin aus ökonomischer Sicht. Sie erfahren, wie aus einem obskuren Internetprojekt eine echte Währung entstanden ist, die mittlerweile zum Wertanker eines gigantischen

Ökosystems von Kryptowährungen geworden ist. Der rote Faden dieses Teils ist die Preisentwicklung von Bitcoin, dessen Wert von 1 US-Dollar im Jahr 2010 auf beinah 20.000 US-Dollar im Jahr 2017 kletterte. Sie erfahren aber auch, was für eine Art Geld Bitcoin ist und wo es einen Bedarf nach diesem gibt. Dabei lernen Sie die Investoren und Unternehmer kennen, die Bitcoin vorantreiben – und die damit märchenhaft reich oder durch Hacks in den Ruin getrieben wurden.

Im dritten Teil geht es darum, dass Bitcoin hochpolitisch ist. Die digitale Währung eliminiert Mittelsmänner wie Banken aus finanziellen Transaktionen, und sie entzieht dem Staat die Hoheit über die Geldpolitik. Dies macht Bitcoin zu einem libertären und anarchistischen Projekt – und zur Leitwährung der Schattenwirtschaft im Darknet. Wir werfen deshalb einen Blick auf die dunkle Seite von Bitcoin, etwa die Online-Märkte für Drogen. Daneben erfahren Sie mehr über die freiheitlichen Ideologien, die die Bitcoin-Szene antreiben, und sehen, mit welchen Strategien die Staaten versuchen, die Kontrolle wieder zu gewinnen.

Im vierten Teil des Buches geht es schließlich um den sogenannten Blocksize-Streit, der 2015 über die Zukunft des Bitcoin-Systems ausbrach. Da es dabei um die Grenzen der Technologie geht und um Wege, diese zu überwinden, ist dieser Teil vermutlich der technisch anspruchsvollste. Aber er wird auch die Geschichten jener Menschen erzählen, die sich in diesem lange anhaltenden Streit verlieren, und erklären, wie es geschehen konnte, dass aus einem scheinbar kleinen technischen Detail ein irritierend erbitterter Kampf um den weltanschaulichen Kurs der Kryptowährung wurde.

Bevor wir nun mit der verrückten Geschichte vom Aufstieg eines neuen Geldes beginnen, möchte ich noch einige Anmerkungen voranstellen:

1. In diesem Buch werden Dutzende von Personen auftreten. Leider sind es ausschließlich Männer. Dies liegt daran, dass es im Bitcoin-Universum so gut wie keine Frauen gibt. Doch man darf hoffen, dass Bitcoin in Zukunft weiblicher wird. Diese Tendenz zeichnet sich bereits ab.

2. Um die vielen auftretenden Personen greifbarer zu machen, hat die Gestalterin dieses Buches die wichtigsten von ihnen porträtiert. Diese wundervollen Illustrationen stehen mit kurzen Informationen zur Person vor den entsprechenden Teilen des Buches. Sie sollen als Übersicht

dienen – wie am Anfang von Theatertexten die Dramatis Personae, das Register der handelnden Akteure.

3. An vielen Stellen lassen sich englische Wörter und Fachbegriffe nicht vermeiden. Bei deren Übersetzung würde ein Großteil der Bedeutung verloren gehen. Deshalb bleibt etwa der „Hash", ein fester Begriff der Kryptographie, englisch, anstatt in „Zerhäckseltes" übersetzt zu werden, und die „Wallet", englisch für „Geldbeutel", bleibt im Original, da sie anders als ihr deutsches Pendant auch Software beschreibt, mit der Geld verwaltet wird. Zur Orientierung habe ich ans Ende des Buches ein umfangreiches Glossar gestellt. Dort aufgeführte Wörter sind im Text bei der ersten Nennung *kursiv* gesetzt.

4. Das Buch enthält keine mathematischen Formeln. Stellenweise tauchen aber relativ viele Zahlen auf, vor allem Kurse. Diese Kurse sind oft in US-Dollar angegeben, da manche Werte nur in US-Dollar verfügbar waren. Der Euro war in der Zeit, in der das Buch spielt, etwa 1,10 bis 1,30 US-Dollar wert. Maßeinheiten, die zuweilen auftreten, sind Kilobyte, Megabyte und Gigabyte und im Allgemeinen Dezimalpräfixe wie kilo, mega, giga oder tera. Eine Tabelle am Ende dieses Buches hilft, diese Größeneinheiten besser vorstellbar zu machen.

5. Es gibt etliche Fußnoten im Text. In der Regel verweisen sie auf Quellen im Internet. Die Datumsangaben in den eckigen Klammern am Ende der Fußnote geben den Zeitpunkt an, wann ich diese zum letzten Mal geprüft habe.

6. Schließlich sollte ich noch erwähnen, dass ich bei der Benennung von Personen keiner bestimmten Logik folge. Die deutschsprachigen Konventionen gebieten eigentlich, dass man Personen nach der ersten Einführung mit dem Nachnamen benennt. Im Englischen hingegen – und im Internet im Allgemeinen – werden öffentliche Personen eher mit dem Vornamen angeredet. Ich werde es in diesem Buch mal so, mal so handhaben.

Christoph Bergmann, im Juni 2018

I. Bitcoin

Das Scheitern der Cypherpunks am digitalen Bargeld

Das Aussterben der Geheimnisse

In der echten Welt gehören Geheimnisse zum Alltag. Man flüstert oder unterhält sich in einer stillen Ecke, und wenn keiner mitschreibt, besteht Kommunikation nur als Erinnerung fort, vage und nicht beweisbar. Im digitalen Raum dagegen schreibt immer jemand mit. Sobald ein *Knoten* im Internet eine Information an einen anderen Knoten weitergibt – wenn man eine Webseite aufruft oder eine Mail versendet – geht diese Information in eine Datenbank ein. Das Internet kennt keine Geheimnisse.

Dieser Unterschied zwischen realer und digitaler Welt hat fürchterliche Folgen. Der IT-Sicherheitsexperte Bruce Schneier konstatierte 2015: „Die Wahrheit ist: Die heutige Technologie ermöglicht es Regierungen und Unternehmen, fundamentale Massenüberwachung zu betreiben. […] Sie wird benutzt, um zu kontrollieren, was wir sehen, was wir tun können und letztlich auch, was wir sagen. Sie wird durchgeführt, ohne dass der Bürger Regressionsansprüche oder auch nur die Möglichkeit hätte, sich dagegen zu entscheiden.“ [5]

Zwei Jahre zuvor hatte Edward Snowden enthüllt, in welchem Ausmaß die NSA die globale elektronische Kommunikation überwacht. Die NSA und andere Geheimdienste speichern und durchsuchen potenziell jede Information, die durchs Internet geht. Viele Intellektuelle traf dies wie ein Schock.

Natürlich, jeder hatte geahnt, dass digitale Nachrichten irgendwie überwacht werden. Aber kaum jemand hatte damit gerechnet, dass es in diesem Umfang geschah. Redakteure, Schriftsteller, Bürgerrechtler und Juristen waren entsetzt. Mehr als 60 deutsche Schriftsteller schrieben in einem offenen Brief an Kanzlerin Angela Merkel, dass damit „der ‚gläserne Mensch‘ endgültig Wirklichkeit geworden“ sei.: „Wir erleben einen historischen Angriff auf unseren demokratischen Rechtsstaat, nämlich die Umkehrung des Prinzips der Unschuldsvermutung hin zu einem millionenfachen Generalverdacht.“ [6]

5 Bruce Schneider, Data und Goliath, Redline, 2015.

6 Veröffentlicht wurde der Brief etwa am 25. Juli 2013 in der FAZ, http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/offener-brief-an-angela-merkel-deutschland-ist-ein-ueberwachungsstaat-12304732.html [05.01.2018]

Mehr als 1000 Rechtsanwälte haben die sogenannte Hamburger Erklärung unterschrieben. Darin bezeichnen sie die durch Edward Snowden aufgedeckte „Totalüberwachung aller Bürger" als einen „historisch beispiellosen Angriff auf das verfassungsmäßige Grundrecht auf Privatsphäre". Diese Totalüberwachung „nimmt unserer freiheitlich-demokratischen Gesellschaftsordnung den Nährboden. Sie erstickt den Widerspruch des Bürgers gegen den Staat. Sie fördert Konformismus, obrigkeitshöriges Denken und den Rückzug ins Privatleben."[7]

Der Welt wurde klar, dass es einen fundamentalen Unterschied zwischen physischen und digitalen Geheimnissen gibt – und dass dies grauenhafte Konsequenzen haben wird. In der physischen Welt bleibt privat, was nicht aufgezeichnet wird – während in der digitalen Welt nichts privat bleibt, was nicht verschlüsselt ist.

Die Cypherpunks hatten all das schon lange kommen sehen. Dass das Internet zu einem Mittel der Massenüberwachung wird, war für sie kein Betriebsunfall der Digitalisierung, sondern deren immanente Logik. Die historische Mission der Cypherpunks war es, diese Entwicklung zu verhindern.

Die Cypherpunks: Propheten des digitalen Zeitalters

Die Cypherpunks waren eine lose verbundene Gruppe von Intellektuellen, die schon früh die digitale Revolution diskutierten. Sie sahen vieles von dem voraus, was uns heute beunruhigt.

Die Bewegung entstand Anfang der 90er Jahre. In einem Bürogebäude in San Francisco, in dem zahlreiche Tech-Start-ups beheimatet waren, trafen sich 16 Männer, um sich über Kryptographie, das Internet, Politik und Freiheit zu unterhalten. Die bekanntesten von ihnen waren Tim May, Eric Hughes und John Gilmore. Thomas Rid beschreibt May als „einen echten Krypto-Cowboy", der für die Freiheit, Waffen zu tragen, eintrat, und einen radikalen, libertären Individualismus predigte. May hatte als Ingenieur bei Intel genügend Geld verdient, um in seinen frühen 40ern nicht mehr auf Erwerbsarbeit angewiesen zu sein. Hughes war ein Mathematiker, kaum 30, der an einer Universität Kryptographie

7 Die Hamburger Erklärung wurde am 30. September 2013 offiziell veröffentlicht.
Sie finden sie im Internet auf
https://rechtsanwaelte-gegen-totalueberwachung.de/hamburger-erklaerung/ zu lesen. [05.01.2018]

lehrte. Gilmore schließlich war einer der ersten fünf Mitarbeiter von Sun Microsystems, einem der frühen Internet-Unternehmen, gewesen und dadurch, wie May, relativ früh finanziell unabhängig geworden.[8]

Die Runde wurde immer größer. In der IT-Szene von San Francisco war es vermutlich hip, an den Cypherpunk-Treffen teilzunehmen. 1992 setzte John Gilmore die Cypherpunk-Mailingliste auf einem Server seines Start-ups auf. Diese Mailingliste war der erste sogenannte Remailer: Der Server leitete die Mails weiter, ohne zu wissen, woher sie kamen. Man konnte E-Mails einreichen, ohne bekanntzugeben, wer man war.[9]

Die Mailingliste hatte bald einige hundert Abonnenten auf der ganzen Welt. In ihr wurden Ideen und Gedanken formuliert und diskutiert, die damals obskur erschienen, aber heute brandaktuell sind. Die Cypherpunks waren ihrer Zeit voraus, und sie wussten es.

„In dieser Zeit wurde viel über Kryptographie, Schlüssel-Treuhänder, das Netz, die Datenautobahn, Cyberterroristen und Kryptoanarchie geschrieben. Wir fanden uns selbst im Auge eines Hurricanes wieder", erzählte May 1994 im Cyphernomicron, seinem online veröffentlichten Buch über die Cypherpunk-Bewegung[10].

Den Cypherpunks wurde schon früh klar: Massenüberwachung war in die DNA des „elektronischen Zeitalters" eingeschrieben. Kein Versprechen des Staates, die Privatsphäre zu schützen, würde dies aufhalten können. Die einzige Hoffnung, das Geheimnis ins elektronische Zeitalter zu überführen, lag in der Kryptographie.

„Ich will eine Garantie – durch die Physik und Mathematik, nicht durch Gesetze –, dass wir echte Privatheit in der persönlichen Kommunikation genießen", hatte John Gilmore schon 1991 in einer Rede gefordert. Er hatte eine klare Vision: „Was, wenn wir eine Gesellschaft bilden können, in der Informationen niemals gesammelt werden? In der man ein Video ausleihen kann, ohne eine Kreditkarten- oder Kontonummer

8 Mehr über die Cypherpunks und ihre Entstehung in Thomas Rid, Rise of the Machines. The lost history of cybernetics, S. 256–280, Victory 2016.

9 Die Cypherpunk-Mailingliste ist eine hervorragende historische Quelle für Themen rund um Kryptographie in den 90ern. Es gibt mehrere Archive der Mails, unter anderem auf https://marc.info und https://cryptome.org

10 Tim May, Cyphernomicron, 1994, https://www.cypherpunks.to/faq/cyphernomicron

zu hinterlegen? In der du beweisen kannst, dass du die Erlaubnis hast, ein Auto zu fahren, ohne deinen Namen zu verraten? In der du Nachrichten senden und empfangen kannst, ohne deine räumliche Adresse zu enthüllen?“ [11]

Gilmore redete von Kryptographie. Kryptographie besteht zwar im Kern aus kühler, nüchterner, unparteiischer Mathematik. Doch tatsächlich ist sie eine politische Wissenschaft. Sie ersetzt Vertrauen in Personen durch Vertrauen in Mathematik. Man muss nicht einem Amt glauben, dass es vertraulich mit Daten umgeht – man verschlüsselt. Man vertraut nicht dem Wort, sondern prüft die Signatur.

Das Denken und Diskutieren der Cypherpunks kreiste vor allem um Geheimnisse. Sie wussten, dass das elektronische Zeitalter, das in den frühen 90ern anbrach, unbedingt eine Methode brauchte, um (Mit-) Wissen zu verhindern. So, wie es in der analogen Welt möglich war – selbst wenn dies bedeutet, dass Drogen verkauft, Kinder entführt, Terroraktionen vorbereitet, Staatsgeheimnisse verraten und Bombenbauanleitungen verbreitet werden. Denn ohne die Freiheit, Geheimnisse zu haben, würde das Internet eine reine Überwachungsmaschine werden.

Die Cypherpunks diskutierten nicht nur. Sie kämpften für ihre Vision. Eric Hughes schrieb 1992 im Cypherpunk Manifesto: „Wir können nicht erwarten, dass uns die Regierungen, Unternehmen und andere große, gesichtslose Organisationen freiwillig Privatheit gewähren […]. Wir müssen unsere Privatheit verteidigen, wenn wir erwarten, eine zu haben. Wir müssen zusammenkommen und Systeme schaffen, die anonyme Transaktionen ermöglichen. Wir, die Cypherpunks, widmen uns dem Aufbau anonymer Systeme. Wir verteidigen unsere Privatheit durch Kryptographie, durch anonyme Mail-Systeme, durch digitale Signaturen und durch elektronisches Geld. Cypherpunks schreiben Code. […] Wir wissen, dass Software nicht zerstört und ein weites, verteiltes System nicht ausgeschaltet werden kann.“ [12]

Bitcoin wurde, um vorauszugreifen, zur mächtigsten Inkarnation dieser Worte.

---

11 http://www.toad.com/gnu/cfp.talk.txt

12 Eric Hughes, A Cypherpunk Manifesto, 1993, https://www.activism.net/cypherpunk/manifesto.html

Die kryptographische Kluft wird Politik

Und die Cypherpunks schrieben Code. Eric Hughes' Aufforderung, den Kontrollstaat durch Mathematik zu bekämpfen, ging um die Welt. Man könnte zwar meinen, dass die Cypherpunks verloren haben. Das Netz ist zu jener alptraumhaften Überwachungsmaschine geworden, die sie gefürchtet hatten. Google sammelt unsere Fragen, Facebook unsere Fotos, Microsoft unsere Dokumente; jeder beliebige Blog setzt ein Cookie in unseren Browser, um zu beobachten, wohin wir surfen, und unser Navi speichert, wohin wir fahren. Man könnte aber ebenso gut sagen, dass die Cypherpunks gewonnen haben.

Es gibt die Massenüberwachung, ja, aber – und das übersehen viele – es gibt auch Werkzeuge, um ihr zu entgehen. Man muss nicht wie die Anwälte hinter der Hamburger Erklärung den Staat auffordern, der Überwachung einen Riegel vorzuschieben. Man kann es selbst machen. Die dafür notwendigen Instrumente haben die Cypherpunks entwickelt. Man kann E-Mails mit *PGP* verschlüsseln, mit dem *Tor*-Browser anonymisiert surfen, über WikiLeaks unerkannt Informationen veröffentlichen.

Alle Werkzeuge des widerspenstigen, dunklen Netzes bestehen aus Kryptographie. Sie sind Kryptographie. Sie verschlüsseln, signieren, hashen, entschlüsseln, verifizieren. Wenn es eine Chance gibt, die Massenüberwachung zu besiegen, dann – und das wussten die Cypherpunks – muss man Chancengleichheit auf dem Schlachtfeld der Kryptographie schaffen. Man muss Software schreiben, die jene Methoden der Geheimniswahrung, die eigentlich der Regierung vorbehalten sind, allen zur Verfügung stellt. Daher der Name, Cypherpunk: Cipher, der englische Begriff für Chiffre, und Punk.

Die Kryptographie liegt im Kern der Cypherpunk-Bewegung. In ihr findet man, wie vermutlich in jeder Wissenschaft, eine innere Grundhaltung zur Welt. Biologen sehen Zellen, Mathematiker Formeln, Ökonomen Profite und Handwerker Baustellen. Die Cypherpunks haben aus der sehr speziellen Perspektive, die die Kryptographie zur Welt einnimmt, eine politische Agenda gemacht.

Tim May beschrieb die Weltanschauung, die die Kryptographie auferlegt, dadurch, dass sie „keinen Mittelweg" kenne: „Eine Verschlüsselung kann entweder gebrochen werden oder nicht. […] Die

Region ‚dazwischen' ist klein und in ständiger Bewegung."[13] Kryptographen operieren aus einem permanenten Zustand der Paranoia heraus. Sie sind im ständigen Krieg mit einer feindlichen Welt, die die Verschlüsselung knacken will. Sie bauen mathematische Festungen.

Sieg und Niederlage sind in der Kryptographie eindeutig. Die brutale Klarheit der Mathematik zerquetscht jedes „vielleicht". Entweder man macht alles richtig – dann bleibt das Geheimnis gewahrt – oder man macht einen einzigen, kleinen Fehler – dann ist der Code gebrochen. Entweder ein Hash geht auf – dann ist das Programm authentisch – oder sie geht nicht auf – dann ist es manipuliert. Dazwischen gibt es nichts.

Die große Magie der Kryptographie ist, dass ein absoluter Sieg möglich ist. Das ist ein physikalischer Fakt. Man braucht weniger Zeit, ein Chaos anzurichten, als dafür, es aufzuräumen, und weniger Energie, eine Nachricht in ein Rauschen zu zerlegen, als dafür, sie zu rekonstruieren. Diese Asymmetrie von Verschlüsselung und Entschlüsselung macht absolute Sicherheit möglich.

Moderne Kryptoalgorithmen sind so gebaut, dass sie von keinem Großcomputer geknackt werden können. Die energetische Spanne zwischen Ordnung und Chaos ist einfach zu groß. Um die Nachricht durch einen Brute-Force-Angriff zu rekonstruieren, braucht man Energiemengen, wie sie die Implosion der Sonne freisetzt. Das ist die Macht großer Zahlen.

Die Cypherpunks münzen diese mathematische Absolutheit in politischen Fatalismus um. Entweder kann der Staat mithören, oder er kann es nicht. Es gibt Geheimnisse, oder es gibt sie nicht. „Die Sprödigkeit der Kryptographie bedeutet, dass die wahre Entscheidung die ist zwischen einem totalen Staat und der Kryptoanarchie", schreibt Tim May. „Es gibt keinen ‚Kompromiss' am Horizont und keinen Mittelweg, der für beide Seiten akzeptabel ist. Hoffnungen auf einen Kompromiss in der Stärke von Kryptoalgorithmen oder auf eine Hintertüre im Code basieren auf einem naiven Verständnis der involvierten Mathematik."[14]

13 Tim May, Cyphernomicron,
https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html

14 Tim May, Untraceable Digital Cash, Information Markets and BlackNet, Vortrag 1997,
http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm

Kryptographie kennt keine Türen, die Polizisten nur per Gerichtsbeschluss aufbrechen können. Wenn Kryptographie scheitert, kann sie immer und von jedem entschlüsselt werden. Dann kann die Polizei jederzeit auf Ihren Computer, in Ihr Auto, in Ihr Schlafzimmer schauen, und Sie bemerken es nicht einmal. Wenn die Kryptographie dagegen hält, kann niemand sie knacken. Dann kann die Polizei ohne Ihre Einwilligung nicht in Ihr Auto, Ihren Computer, Ihr Schlafzimmer, egal mit wie viel Sprengstoff sie anrückt, egal wie viele Dietriche sie mitbringt. Auch die größte Krypto-Organisation der Welt, die NSA, ist machtlos. Das bestätigte Edward Snowden in einer legendären Pressekonferenz: „Verschlüsselung funktioniert. Richtig implementierte, starke Krypto-Systeme gehören zu den wenigen Dingen, auf die man sich verlassen kann."

Es gibt keine Grauzone. Entweder mündet die Digitalisierung in jenen totalitären Horrorstaat, vor dem Bruce Schneier, Edward Snowden und so viele andere warnen: in eine Welt, in der jede Bewegung von jedem ununterbrochen dokumentiert und analysiert wird. Oder die Kryptographie führt zu jenem entgegengesetzten Szenario, das May bereits 1992 schilderte: „Die Computertechnologie ist kurz davor, es den Individuen und Gruppen zu ermöglichen, in einer vollkommen anonymen Weise miteinander zu kommunizieren und zu interagieren. Zwei Personen werden Nachrichten austauschen, Geschäfte betreiben und elektronische Verträge verhandeln können, ohne den echten Namen und die rechtliche Identität des anderen zu kennen. […] Diese Entwicklungen werden die Natur von Regierung und Regulierung vollständig verändern."

Der technische Fortschritt, prophezeite May, führe unvermeidbar in eine „Kryptoanarchie". Er selbst kann es kaum erwarten: „Erwacht, ihr habt nichts zu verlieren als eure Zäune aus Stacheldraht!" [15]

Kryptoanarchie: Die Rückkehr der Dunkelheit

Für Tim May ist Anarchie die politische Grundordnung des Internets. „Keine zentrale Kontrolle, kein Herrscher, kein Führer, keine ‚Gesetze'. Keine Nation kontrolliert das Netz, kein Verwaltungsorgan diktiert die

15 Tim May, The Crypto Anarchist Manifesto, 1992, https://www.activism.net/cypherpunk/crypto-anarchy.html

Politik. Der Ayatollah im Iran hat nicht die Macht, eine Newsgruppe auszuschalten, die er nicht mag, so wie der französische Präsident nicht die Macht hat, etwa den Missbrauch der französischen Sprache im Netz aufzuhalten. Auch die CIA kann Newsgruppen oder Webseiten nicht daran hindern, Geheimnisse zu verraten." [16]

Im Internet kann man anonym sein, und wenn man anonym ist, kann einen niemand für das bestrafen, was man macht. Kryptoanarchie bedeutet einen Kontrollverlust des Staates. Den Cypherpunks war klar, dass dies auch gruselige Folgen haben würde. „Und viele von uns, die über das Thema Kryptoanarchie nachgedacht haben, waren entsetzt über die Folgen, die unvermeidlich erscheinen", schrieb May 1994. Er prophezeite, dass der Staat versuchen werde, die Kryptoanarchie zu verhindern, und sich dabei auf „Gründe der nationalen Sicherheit" berufen werde, wie die Bekämpfung von Drogenhandel und Steuerflucht oder, abstrakter, der sozialen Desintegration. Viele dieser Sorgen seien, so May, berechtigt: „Kryptoanarchie wird es ermöglichen, dass Staatsgeheimnisse, verbotene Waren und Diebesgut gehandelt werden. Ein anonymer computerbasierter Markt wird es sogar möglich machen, dass abscheuliche Marktplätze entstehen für Erpressung und Auftragsmorde." Insgesamt meinte May aber, dass die Vorteile die Nachteile überwiegen würden.

An sich bedeute Anarchie ja nur „die Abwesenheit eines Herrschers, der einem sagt, was man tun soll". Das Fernsehen stellt den Zusammenbruch der gesellschaftlichen Kontrolle zwar lustvoll als barbarisches Inferno dar, in dem sich Menschen in mordende Tiere verwandeln. In der Wirklichkeit ist die Abwesenheit von Kontrolle aber meist weniger aufregend: „Sie ist gebräuchlich in vielen Aspekten des Lebens, bei der Wahl der Bücher, die man liest, der Filme, die man sieht, den Freunden, mit denen man sich trifft," schreibt May. Und auch wenn es vorkommt, dass man die falschen Filme sieht, sich mit schlechten Menschen anfreundet oder die Wahlfreiheit generell missbraucht – im Großen und Ganzen ist die Abwesenheit von Kontrolle nicht der Anfang vom Ende der Zivilisation, sondern das Gegenteil: ihre Blüte. Menschen bleiben Menschen, sie behalten ihren moralischen Kompass und ihr Mitgefühl, selbst dann, wenn sie niemand dazu zwingt. Denn Menschen machen

16 Tim May, „Cryptoanarchy and Virtual Communities", 1994, http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html

auch freiwillig das Richtige. Sie können gut sein, wenn man sie lässt.

Ohnehin – was ist die Alternative? Es gibt kein Sowohl-als-auch. Entweder Anarchie oder umfassende Kontrolle. Für die Cypherpunks, die zum größten Teil liberal oder libertär, also für starke Bürgerrechte, einen schwachen Staat und einen freien Markt eintraten, war damals klar: Im Zweifel für die Freiheit. Lieber zu viel Anarchie als zu viel Kontrolle.

Die Cypherpunks sahen sich auf historischer Mission. David Chaum, einer der bedeutendsten Kryptographen der 80er Jahre, bekannt als „Pate der anonymen Kommunikation" und als Vordenker der Cypherpunks – wir werden ihn bald besser kennen lernen – sagte:

„Die Struktur der Gesellschaft im nächsten Jahrhundert hängt davon ab, welche Entscheidung wir heute treffen."

Tim May war überzeugt, dass die Cypherpunks gewinnen würden. „Die Technologie für diese Revolution – und es wird garantiert sowohl eine soziale als auch eine ökonomische Revolution – hat in der Theorie bereits in der vergangenen Dekade existiert", prophezeite er in seinem Manifest der Kryptoanarchie. „Doch erst seit kurzem haben Netzwerke und private Computer eine ausreichende Geschwindigkeit erreicht, um diese Ideen praktisch realisierbar zu machen. Und die kommenden zehn Jahre werden genügend Beschleunigung bringen, um viele dieser Ideen wirtschaftlich machbar und damit essenziell unaufhaltbar werden zu lassen."

Digitales Bargeld: Ein technischer Meilenstein

Jene tiefe, unüberwindbare Kluft, die die Weltsicht der Cypherpunks prägt, begegnet uns wieder, wenn wir uns der Digitalisierung des Geldes zuwenden.

Eric Hughes beschrieb 1992 im Cypherpunk-Manifesto eindringlich, wie die Digitalisierung zum Verlust finanzieller Privatsphäre führt: „Da wir Privatheit wünschen, müssen wir gewährleisten, dass jede Partei einer Transaktion nur das Wissen erhält, das sie für diese Transaktion benötigt. Da jede Information dokumentiert werden kann, müssen wir

dafür sorgen, dass wir so wenig wie möglich enthüllen. In den meisten Fällen ist die persönliche Identität nicht notwendig. Wenn ich in einem Laden ein Magazin kaufe und bar bezahle, muss der Händler nicht wissen, wer ich bin. Wenn ich meinen E-Mail-Provider bitte, Nachrichten zu versenden und zu empfangen, muss er nicht wissen, mit wem ich kommuniziere oder was ich schreibe oder was andere mir schreiben; mein Provider muss nur wissen, wie er die Mail ausstellt und wie viel ich ihm dafür schulde. Wenn der einer Transaktion unterliegende Mechanismus meine Identität enthüllt, habe ich keine Privatheit. Ich kann mir nicht aussuchen, wann ich mich enthülle; ich muss mich immer enthüllen.[17]"

Wenn Sie sich im Supermarkt genau umschauen, werden Sie vielleicht irgendwo ein Schild entdecken, das, klein und unscheinbar, erklärt, dass die Daten aus Ihren elektronischen Transaktionen für Werbe- und Analysezwecke weitergegeben werden. Finden Sie das nicht auch etwas gruselig?

Jedes Mal, wenn wir Geld digital verwenden, als Kreditkarte, Online-Überweisung oder per PayPal, geben wir ein Stück Freiheit und Privatheit auf, ohne es zu bemerken. Die Digitalisierung droht, ein Fundament der bürgerlich-freiheitlichen Gesellschaft – die monetäre Privatheit – zu zerstören. Hughes forderte daher: „Privatheit in einer offenen Gesellschaft braucht ein anonymes Transaktionssystem. Bis heute ist Bargeld das primäre dieser Systeme. Ein anonymes Transaktionssystem ist kein geheimes Transaktionssystem. Ein anonymes System erlaubt es Individuen, ihre Identität preiszugeben, wenn – und nur wenn – sie es wollen. Das ist die Essenz der Privatheit."

Daher verlangten die Cypherpunks ein digitales Bargeld. Es war notwendig, um die Privatsphäre und damit die Freiheit des Individuums zu verteidigen. Auf der anderen Seite war aber auch allen klar, dass digitales Bargeld mehr als ein bloßes Verteidigungsmanöver gegen die Begehrlichkeiten der Geheimdienste und Konzerne war. Digitales Bargeld ist ein Meilenstein auf dem Weg in die Kryptoanarchie.

17 Hughes Manifest ist auf mehreren Internetseiten archiviert.
Übersetzung durch Christoph Bergmann.
http://nakamotoinstitute.org/cypherpunk-manifesto/ [05.01.2018]

Erst wenn man ein wahrhaft unverfolgbares, anonymes digitales Bargeld hat, können all die schauerlichen Folgen, die Tim May aufzählt, in die Wirklichkeit strömen: Staaten verlieren die Macht, Steuern einzuziehen und die Transaktionsströme ihrer Bürger zu kontrollieren. Es wird digitale Schwarzmärkte geben, auf denen neben Drogen alle denkbaren Scheußlichkeiten gehandelt werden, Erpressung in jeder Form wird sich dank unproblematischer Zahlungen wieder lohnen, es entstehen Märkte für Informationen, die jegliche Art der Geheimhaltung unterlaufen. Der ehemalige Intel-Ingenieur Jim Bell, einer der radikalsten Kryptoanarchisten, beschrieb in seinem Essay über den „Assassination Market", wie mit digitalem Bargeld per Crowdfunding Auftragskiller finanziert werden können, um unbeliebte Politiker zu beseitigen. Bell beschrieb dieses Szenario als Utopie – als wünschenswerten Zustand, um die Politik zu verbessern oder gleich ganz zu beseitigen.

Ob man digitales Bargeld wollte oder nicht – für die Cypherpunks war es unvermeidbar. Die Technologien waren bereits in den frühen 90ern da, und es sah aus, als stünde die Einführung nun unmittelbar bevor.

Ein brillantes Produkt floppt

Der ambitionierteste Versuch dieser Jahre, ein digitales Bargeld zu schaffen, war eCash von David Chaum [18]. Chaum war selbst nicht direkt ein Cypherpunk. Zumindest ist keine Aktivität von ihm in der Mailingliste bekannt. Doch er war ein Vordenker der Bewegung, und viele Cypherpunks bewunderten seine Arbeit. Hal Finney, Cypherpunk, Mitentwickler der PGP-Verschlüsselung und der erste Bitcoin-Miner nach Satoshi, schrieb über Chaum: „Es kam mir so offensichtlich vor. Wir stehen vor den Problemen des Verlustes der Privatsphäre, der schleichenden Digitalisierung, riesiger Datenbanken, mehr Zentralisierung – und Chaum bietet uns eine komplett andere Richtung an, in die wir gehen können, eine, die die Macht in die Hände der Individuen anstatt der Regierungen und der Unternehmen legt. Der Computer kann ein

18 Dies hat wohlgemerkt nichts mit der EC-Karte zu tun. Das EC steht hier zwar auch für Electronic Cash, aber das EC-Kartensystem ist weit davon entfernt, ein digitales Bargeld zu sein, wie Chaum es angestrebt hatte.

Werkzeug sein, um die Menschen zu befreien und zu beschützen, anstatt sie zu kontrollieren.“ [19]

Auf dem Gebiet des digitalen Bargeldes war Chaum, schrieb Tim May 1992 im Cyphernomicron, „ohne Zweifel der einflussreichste Denker.“ Chaum hatte in den 80er Jahren wegweisende kryptographische Methoden erfunden, um die Verbindung zwischen digitalen Nachrichten zu kappen. Der Remailer, mit dem die Cypherpunks anonym E-Mails in die Mailingliste einreichen konnten, beruhte auf Chaums Arbeit. Mit eCash wollte er diese Methoden auch für digitales Bargeld einsetzen.

Der US-Amerikaner stammt aus einer relativ wohlhabenden technisch-akademischen Familie und zog in den späten 80er Jahren nach Amsterdam, um am Centre of Mathematics and Computer Science der Universität die Abteilung für Kryptographie zu leiten. Dann gründete der vollbärtige, langhaarige Kryptograph die Firma DigiCash, um seine Vision von digitalem Bargeld zu verwirklichen. Für Chaum stand dabei alles auf dem Spiel: „Ob wir ein gutes oder ein schlechtes digitales Zahlungssystem bekommen, wird darüber entscheiden, ob wir in Zukunft in einer Diktatur oder einer wirklichen Demokratie leben.“

Chaum benutzte ein cleveres System, um es einer Bank zu erlauben, Überweisungen mit digitalen Münzen auszuführen, ohne selbst zu wissen, wer wem was sendete. Die von ihm entwickelten Blinden Signaturen waren der Kern der Technologie. Sie können es sich so ähnlich vorstellen, als würde jemand einen Briefumschlag aus Kohlepapier unterschreiben, in dem ein Geldschein ist.

Man kann den Schein „blind“ unterschreiben. [20] Alle Experten in dieser

19 Hal Finney erklärte so 1992, weshalb er einen Remailer betrieb. http://fennetic.net/irc/finney.org/~hal/why_rem1.html

20 Für diejenigen, die es genauer wissen wollen: Chaums eCash-System funktionierte, in sehr groben Zügen, etwa so: Der Kunde einer Bank nimmt eine zufällig erstellte Seriennummer – nennen wir sie „x“ – und verschlüsselt sie mit seinem eigenen öffentlichen Schlüssel „c“. Nur er selbst, als Besitzer des zugehörigen privaten Schlüssels, kann die selbstgewählte Seriennummer entschlüsseln. Mathematisch sieht das Paket so aus: c(x). Man kann es sich aber auch als einen Geldschein in einem Briefumschlag vorstellen. Die Bank empfängt die verschlüsselte Seriennummer. Dann zieht sie von meinem Bankkonto sagen wir zehn Euro ab und signiert die Seriennummer mit ihrem privaten Schlüssel s‘. Sie können es sich so vorstellen, als würde sie den in Kohlepapier verpackten Geldschein unterschreiben. Dann schickt sie die doppelt codierte Seriennummer zurück. Als Formel sieht das Paket nun so aus: s‘(c(x)). Die Bank hat den Briefumschlag mit dem Geldschein unterschrieben, ohne ihn zu öffnen. Mit dem RSA-Algorithmus ist es möglich, die Seriennummer zu entschlüsseln, ohne die Signatur der Bank zu entfernen. Er ersetzt das erwähnte Kohlepapier. Der Kunde öffnet den Umschlag – er entfernt seine eigene Verschlüsselung c – und hat einen von der Bank unterschriebenen Geldschein. Die Bank hat die Seriennummer signiert, ohne sie zu kennen. Jede beliebige, von

Zeit waren verzückt von Chaums System, dessen technische Schönheit nicht zu leugnen war.

Im Mai 1994 war es so weit. eCash startete. Stolz kündigte DigiCash den Launch in einer Pressemitteilung an: „Dienstag, 26. Mai 1994: Das erste elektronische Bargeld, mit dem über Computernetzwerke bezahlt werden kann. Zahlungen von irgendeinem PC an irgendeinen anderen, über E-Mails oder das Internet: Das wurde durch die Technologie des elektronischen Bargeldes zum ersten Mal demonstriert. ‚Man kann nun für den Zugang zu einer Datenbank bezahlen, Software oder einen Newsletter per E-Mail kaufen, ein Computerspiel über das Netz spielen, 5 Dollar von einem Freund erhalten oder einfach nur eine Pizza bestellen. Die Möglichkeiten sind wahrhaft endlos', so David Chaum, Direktor von DigiCash, der das Produkt angekündigt und vorgestellt hat." [21]

Chaum hatte es geschafft: Geld war digital geworden. Man konnte es auf der Festplatte speichern und damit bezahlen, ohne Informationen im Cyberspace preiszugeben. Bargeld war Software geworden. Der Informatiker und „Internetguru" Nicholas Negroponte nannte eCash damals „das aufregendste Produkt, das ich in den letzten 20 Jahren gesehen habe". Chaum machte Amsterdam zum Mekka der Finanz-Kryptographie. „Die Firma hatte ein brillantes Produkt", schrieb das niederländische Magazin Next, „sogar das Silicon Valley war neidisch auf die Avantgarde-Technologie, die im Amsterdamer Science Park erfunden wurde." Chaums eCash war eine so elegante Lösung für das Problem des digitalen Bezahlens, dass Leute aus den USA nach Amsterdam flogen, „um die Geburt von etwas so Schönem mitzuerleben." [22]

Chaum erhielt Angebote von Investoren, die ihm ohne zu zögern zweistellige Millionenbeträge anboten. Microsoft, Netscape, die Deutsche Bank, Visa, Mastercard, die Credit Suisse, Banken aus den USA und Südafrika – alle wollten mit ihm zusammenarbeiten. Es lag etwas in

---

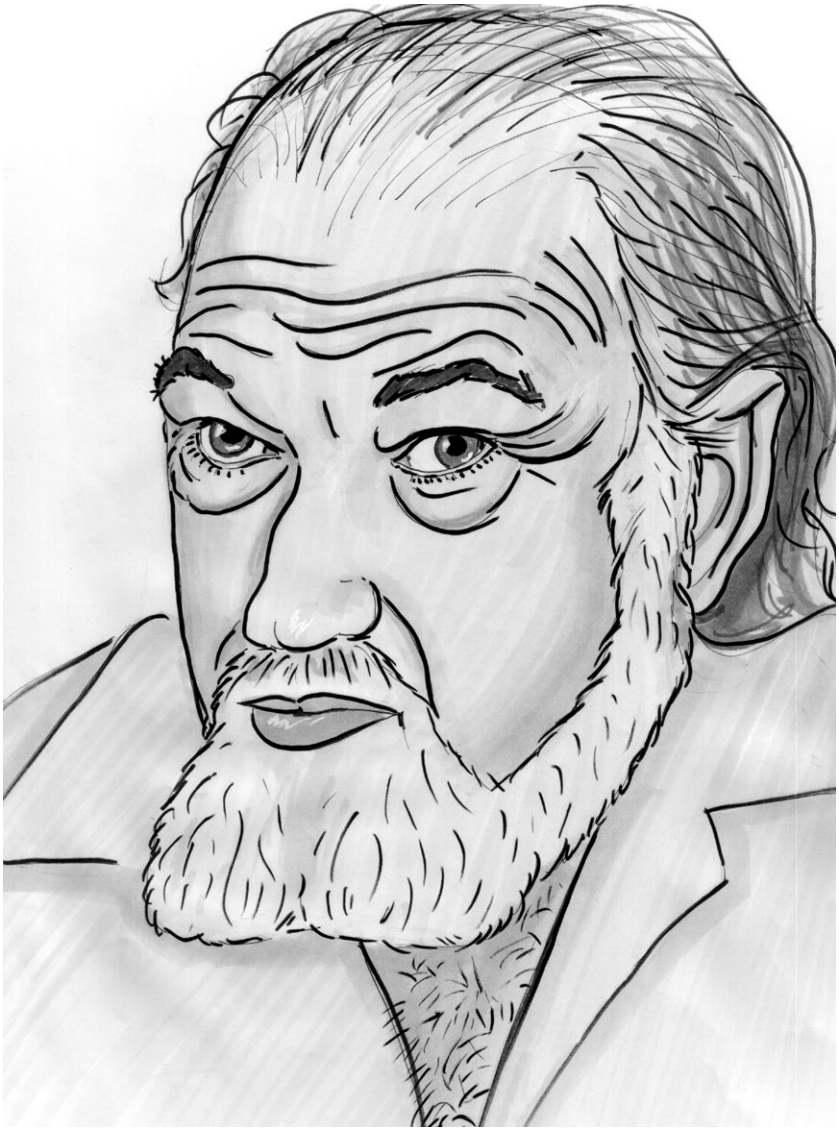
der Bank signierte Seriennummer kann nun so verwendet werden wie ein elektronischer Schein von, sagen wir, zehn Euro. Siehe auch David Chaum, Blind Signatures for Untraceable Payments, 1993 (http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF); David Chaum, Amos Fiat, Moni Noar, Untraceable Electronic Cash, 1990 (http://blog.koehntopp.de/uploads/chaum_fiat_naor_ecash.pdf).

21 Pressemitteilung vom 27. Mai 1994, https://w2.eff.org/Privacy/Digital_money/?f=digicash.announce.txt

22 Next, „How DigiCash Blow Everything", 1999, Übersetzung aus dem Holländischen, https://cryptome.org/jya/digicrash.htm

der Luft. Einige Banken, darunter die Deutsche Bank, starteten Pilotprojekte. Microsoft verkündete, eCash zum integralen Bestandteil von Windows zu machen; Netscape wollte das virtuelle Bargeld in den Browser bringen. Es sah so aus, als wäre der Siegeszug von eCash unaufhaltsam.

Doch 1998 platzte der Traum. DigiCash ging bankrott. Chaum war gescheitert.



Ein paranoider Chef und verdummende Nutzer

Ein Artikel erklärte damals das Scheitern von DigiCash mit Chaums Persönlichkeit. „Ein brillanter Wissenschaftler zu sein bedeutet nicht, dass man ein guter Manager ist. David Chaum war ein Kontroll-Freak, einer, der keine Aufgaben delegieren konnte und ständig über jedermanns Schultern schaute […].“ [23]

Die meisten Mitarbeiter von DigiCash waren Idealisten. Sie teilten Chaums Vision vom digitalen Bargeld. Aber er machte die Leute verrückt. „So gut wie jeder Ex-DigiCash-Mitarbeiter kann eine Geschichte von seinen legendären Verdächtigungen erzählen. ‚Paranoid‘ ist ein Wort, das man oft hört, wenn man über Chaum spricht.“ Chaum traute niemandem außer sich selbst. Das machte es oft schwierig, die Dinge vorwärtszubringen. Investoren oder Partner wollten Verträge abschließen, aber Chaum änderte in letzter Sekunde die Bedingungen, weigerte sich zu unterschreiben und verlangte viel zu hohe Gebühren.

Er war also nicht nur ein unangenehmer Chef, sondern auch ein anstrengender Geschäftspartner. Die Mitarbeiter liefen ihm davon. Kein Projekt ging vorwärts, die Partner sprangen ab. Irgendwann setzten die Investoren durch, dass Chaum als Geschäftsführer zurücktrat, doch auch das rettete DigiCash nicht mehr. Am Ende gab es einen Streit um Patente.

War eine großartige Idee wirklich nur an der Persönlichkeit ihres Schöpfers gescheitert? Der Next-Artikel legt das nahe, es ist aber nicht die ganze Geschichte. Chaum erzählte später, dass das Interesse der Kunden schlicht zu gering gewesen sei. „Es war schwierig, genügend Händler davon zu überzeugen, digitales Geld zu akzeptieren, so dass man nicht genügend Kunden dazu brachte, es zu benutzen, und andersherum.“ Launisch fügte er hinzu: „Als das Web wuchs, fiel die durchschnittliche Intelligenz der Nutzer. Es war schwierig, ihnen zu erklären, wie wichtig Privatheit ist.“

Berichte über die Bankenpartner von DigiCash bestätigten das. Unter dem Titel „Requiem for a Bright Idea“ (Requiem für eine hellsichtige Idee) schrieb das Wirtschaftsmagazin Forbes: „Eine schöne neue Währung für eine schöne neue Welt, mit einem einzigen Problem: Niemand

23 Siehe Next, Anm. 22

will sie – keine Bank, kein Händler, und, am wichtigsten, kein Kunde. Der E-Commerce blüht, aber es sieht aus, als seien Visa und Mastercard anstelle von digitalem Bargeld die Währung der Wahl.“ [24]

Und es ging damals nicht nur eCash so. Es gab Dutzende von Versuchen, digitales Bargeld zu etablieren, aber sie gingen alle ein. James A. Donald, ein regelmäßiger Autor in den Cypherpunk-Mails und der erste, der Satoshis Bitcoin-Whitepaper kommentieren sollte, konstatierte 1998, dass es von mehr als 20 Projekten keines über die kritische Schwelle geschafft hatte.

Für die Cypherpunks war dies kaum zu fassen: Die Technologie war endlich möglich – doch die Welt wollte sie nicht? Tim May konstatierte damals resigniert: „Zehn Jahre und noch immer kein nützliches digitales Bargeld. Ich schrieb mein Cryptoanarchist Manifesto vor beinah elf Jahren. Ich traf Chaum 1988. Ich wusste, digitales Bargeld würde nicht so schnell kommen, aber ich hatte nicht erwartet, dass mehr als zehn Jahre später noch immer nichts Nützliches da sein würde.“ [25]

Digitales Bargeld, so schien es, war eine technologische Sackgasse. Aber war das Desinteresse der Kunden wirklich allein schuld?

Warum die zentralisierten Ansätze gescheitert sind

Es gibt noch eine andere Theorie, warum Chaums eCash nicht gezündet hatte. James A. Donald schrieb: „Angst und Gier haben es abgewürgt […]. Die Macher hatten Angst, dass irgendjemand zu Schaden kommt. Daher haben sie ihr digitales Bargeld verstümmelt, bis sie jeden überprüfen konnten, der es verwenden wollte, und dann haben sie ihre Vetomacht benutzt, um den größten Markt für frühe Nutzer auszuschließen: die Pornografie.“ [26]

Auch Orlin Grabbe, ein Autor, der sich intensiv mit digitalem Bargeld beschäftigt hatte, fand, dass David Chaum nicht weit genug gegangen sei. Grabbe bestritt sogar, dass eCash ein echtes digitales Bargeld war:

---

24 Alle Zitate dieser Passage, auch die von David Chaum, stammen aus dem Forbes-Artikel „Requem for a Bright Idea“ von Julie Pitta (1999), https://www.forbes.com/forbes/1999/1101/6411390a.html#1ddb77ae715f

25 http://marc.info/?l=cypherpunks&m=95280154624228&w=2

26 James A. Donald, „Current Net Cash Proposals“, http://echeque.com/Kong/existing_proposals.htm

„Es gibt keine Anonymität für den Empfänger von eCash. Nur für den Bezahlenden. Laut DigiCash wollen Kriminelle meistens Geld einnehmen, und daher werden sie durch die Nicht-Anonymität von eCash gehindert. Dies klingt wie ein Anbiedern an die Aufsicht oder wie die Entschuldigung für einen grundsätzlichen Fehler im System.“ [27]

Chaums eCash verschleierte zwar, wer wem was überwies, doch die Banken wussten, wer wie viel Mark oder Dollar in eCash verwandelte und auszahlte. Die Banken waren bei eCash weiterhin die zentralen Türsteher. Das war der wesentliche Unterschied zwischen Chaums eCash und echtem Bargeld. Chaum wollte ein Geldsystem, in dem der anständige User anonym bleibt, der Verbrecher jedoch enttarnt wird. Er wollte kein System, in dem Kriminelle Geld waschen können, sondern eines, das die Privatsphäre der lauteren Bürger schützt. Das war nobel gedacht – doch er schloss gerade die aus, für die Anonymität am wichtigsten war. Die *Early Adopter* blieben aus. Damit es die kritische Schwelle erreiche, schrieb James A. Donald, brauche ein echtes digitales Bargeld gerade die zwielichtigen Gewerbe wie die Pornographie oder den Drogenhandel. [28]

Auf Banken wirkte dies schon in den 90er Jahren abschreckend. Wenige Jahre später stürzten Flugzeuge ins World Trade Center. Die Stimmung verdüsterte sich, die Gesetze wurden strenger, die Kontrollen schärfer. Große Banken in den Industriestaaten, die zu diesem Zeitpunkt noch mit digitalem Bargeld zu tun hatten, beendeten die Projekte. Die Entwicklerfirmen flüchteten in Steuer- und Regulierungsoasen. Doch auch dort wurden sie vom langen Arm der US-Justiz eingeholt.

So war etwa E-Gold eine der populärsten bargeldähnlichen Transaktionssysteme. Es war eine Art E-Mail-System für eine goldbasierte Währung. Als einziges Projekt der 90er erreichte es so etwas wie eine kritische Masse. Es wurde allerdings schon bald von Betrügern missbraucht, woraufhin die Betreiber mit Anklagen überflutet wurden und die Plattform schließlich schlossen.

27 Orlin Grabbe, „Introduction to Digital Cash“, 1997, https://www.hermetic.ch/crypto/dig_cash/grabbe1.htm

28 James A. Donald, „A Plan for the Introduction of Internet Cash“, http://echeque.com/Kong/plan.htm

In Costa Rica eröffnete der Autor Orlin Grabbe den Digital Monetary Trust: ein Computersystem, das nicht nur die Transaktionen, sondern auch die Identität der Besitzer von Konten beim Trust kryptographisch verschleierte. Es bot die vielleicht größte Anonymität, die zu dieser Zeit möglich war. Doch auch Grabbe bekam ab 2004 Ärger mit den Behörden und musste die Plattform schließen. Es schien aussichtslos zu sein.

Satoshi, der Erfinder von Bitcoin, beschrieb im Januar 2009 den damaligen Zustand des digitalen Bargelds. „In den 90ern waren viele Leute daran interessiert, aber nach einer Dekade gescheiterter, auf Vertrauen basierender Systeme, sehen sie es als eine verlorene Sache an." Für ihn war klar, weshalb alle vor ihm gescheitert waren: weil eine dritte Partei im Spiel war, die zwischen Sender und Empfänger einer Transaktion stand. Solche Systeme werden, so Satoshi in einer E-Mail, „unvermeidbar heruntergefahren, wenn die dritte Partei kalte Füße bekommt".[29] Als er das schrieb, hatte er mit Bitcoin bereits ein System gegründet, das eben jene Mittelsmänner überflüssig machte.

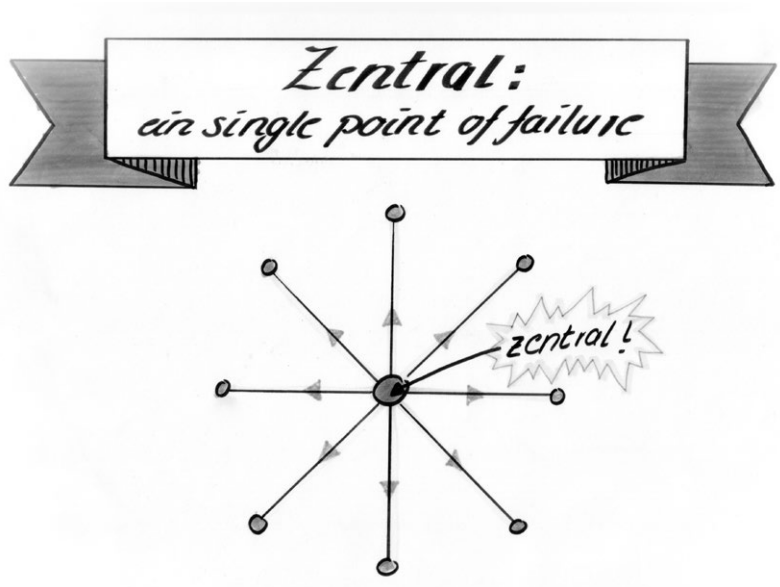
„Ich hoffe, sie begreifen den Unterschied: Wir haben hier zum ersten Mal überhaupt ein System, das nicht auf Vertrauen basiert." Satoshi Nakamotos Erfindung ermöglichte es, „Online-Zahlungen direkt von einer zur anderen Partei zu senden, ohne über eine finanzielle Institution zu gehen". Geld war dezentral geworden – eine ungeheuerliche, weltverändernde Idee.

29 So Satoshi in einer E-Mail an Dustin Trammell am 17. Januar 2009. Übersetzung durch Christoph Bergmann. http://satoshi.nakamotoinstitute.org/emails/cryptography/17/ [05.01.2018]

Bitcoin: Ein digitales P2P-Bargeld

Was kein Zentrum hat, kann nicht sterben

Menschen sind es gewohnt, Dingen eine Mitte zu geben. Alles, was ist, hat ein Zentrum. Ein Zentrum bedeutet, einen Angriffspunkt zu haben. Das Zentrum kann das, was zu ihm gehört, beherrschen. Es kann es steuern, verändern und vernichten. Alles, was ein Zentrum hat, kann sterben. Man muss nur das Zentrum finden und abschalten.



Auch bei digitalem Bargeld vor Satoshi war das Zentrum entscheidend. Jede Firma hat einen Firmensitz, jede Software einen Server. Ob David Chaums DigiCash, Orlin Grabbes Digital Monetary Trust oder E-Gold – sie alle hatten ein Zentrum: eine dritte Partei, einen Mittelsmann, der zum Angriffspunkt werden konnte, um das System zu zerstören.

Es ist schwer, sich ein dezentrales Zahlungssystem vorzustellen. Kann es eine Firma oder Organisation ohne Kopf und Zentrale geben? Seit Beginn der Zeit kann man Geld zwar „bar“ – als Münze oder als Muschel – von Person zu Person übergeben, ohne eine zentrale Autorität zu benötigen. Sobald man jedoch den Raum der physischen Kopräsenz verlässt und Geld als Schein, Scheck oder Überweisung versendet, benötigt man einen Mittelsmann. Dieser wird dann zum Zentrum der Transaktionen.