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

II. Das Geld des Internets

Wo werden Bitcoins gespeichert?

Kein Fort, kein Safe, kein Panzerwagen ist so sicher wie eine Bitcoin-Adresse. Um sie mit der Methode Brute-Force zu knacken, muss man nach allem, was bekannt ist, die Energie mehrerer Sonnen verbrennen. Andere Angriffe sind nicht bekannt.

Bitcoin-Adressen sind nicht nur extrem sicher. Es gibt von ihnen auch genug für alle. Denn eine Bitcoin-Adresse, wie etwa 1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy, ist lediglich eine kryptographische Ableitung aus dem öffentlichen Teil eines Schlüsselpaars. Jede Wallet ist in der Lage, beliebig viele Schlüsselpaare zu generieren.[35]

In manchen Wallets können Sie sich den privaten Schlüssel anzeigen lassen (viele verbergen sie der Sicherheit wegen, aber nutzen andere Möglichkeiten für Backups). Sie können den Schlüssel dann ausdrucken, um Ihre Bitcoins schwarz auf weiß zu haben. Diese etwa 50 Zeichen – zum Beispiel L5JW94YJHRSxhqUmu6RwmTLiitkXGqFcjgztkbWB1EsXqTnwDism – sind alles, was Sie brauchen, um so viel Geld aufzubewahren, wie Sie wollen. Sie müssen sich dafür nirgendwo anmelden, sondern lediglich eines von vielen frei verfügbaren Programmen benutzen. Wenn Bitcoins irgendwo gespeichert werden, dann in diesen Zeichen. Wenn Sie sie ausgedruckt haben, können Sie die Festplatte formatieren oder den Computer in eine Müllpresse stecken. Sie besitzen weiterhin die Bitcoins, und niemand, der nicht den privaten Schlüssel hat, kann sie Ihnen wegnehmen.

Ein solcher Schlüssel kann riesige Vermögen aufbewahren. Auf der oben genannten Adresse liegen etwa 124.178 Bitcoin, was derzeit rund einer Milliarde Euro entspricht. Sie können das mit jedem beliebigen Blockexplorer nachprüfen.[36] Wem diese aktuell reichste Adresse gehört, ist nicht bekannt, zumindest mir nicht.

35 Probieren Sie es aus: Für den PC, egal welches Betriebssystem, ist die Wallet Electrum für den Anfang sehr gut geeignet. Für Android und iOS Breadwallet, für Windows Phone CoPay.

36 Etwa auf blockchain.info. Hier können Sie einfach die Adresse eingeben, um sich den Kontostand anzeigen zu lassen.

Bitcoin verkörpert die größte vorstellbare monetäre Autonomie. Noch niemals in der Geschichte der Menschheit gab es die Möglichkeit, in so weitem Ausmaß Herr seines Geldes zu sein.

Zypern: Das Geld auf der Bank gehört der Bank

Im Frühjahr 2013 zeigte sich in Zypern, wie weit die Banken davon entfernt sind, eine mit Bitcoin vergleichbare Autonomie zu gewähren. Die sogenannte Staatsschuldenkrise hatte den Inselstaat erreicht. Es kam wie so oft, etwa in Griechenland, Spanien, Portugal und Irland: Die Banken schlitterten in die Zahlungsunfähigkeit, aber weil sie zu groß waren, um scheitern zu dürfen, rettete die Regierung sie mit Steuergeldern und stellte dann fest, dass sie sich damit übernommen hatte. Die EU und, in diesem Fall, der IWF sprangen ein, um die zypriotische Regierung mit Notkrediten über Wasser zu halten.

Allerdings weicht die Geschichte auf Zypern in einem wesentlichen Punkt von der in den anderen Euro-Krisenstaaten ab: Die Kreditgeber bestanden darauf, dass sich die Kunden der Banken an der Rettungsaktion beteiligten. Noch während der Verhandlungen über das Abkommen ließ die Regierung die Banken schließen und blockierte größere elektronische Überweisungen. Anschließend erhielt sie ein Rettungspaket von 10 Milliarden Euro, von dem jedoch 6 Milliarden durch die Bankkunden aufgebracht werden mussten, die mehr als 100.000 Euro auf dem Konto hatten.

Es ist fairer, die Anleger für die Rettung der Banken bluten zu lassen, als die Steuerzahler zur Kasse zu zerren. Ohne Zweifel. Dennoch ist das Vorgehen verheerend. Es untergräbt das Vertrauen in Banken und in Geld im Allgemeinen. Das Geld gehört euch nicht, lautete die Botschaft, wenn Regierungen und Banken es wollen, nehmen sie es euch weg. Bitcoin als ein Instrument monetärer Autonomie könnte eine Versicherung gegen derartige Enteignungen sein.

Das spiegelte sich damals fast unmittelbar im Bitcoin-Preis wider. Als die Zypernkrise begann, betrug er 40 Dollar. Zwei Wochen später erreichte er 100 Dollar. Mehr als 20 Monate hatte der Kurs gebraucht, sein altes Hoch von 2011 wieder zu erreichen; doch nun waren die Bullen zurück. Endlich.

Ölpreisschock hoch zehn

Zypern war ein starker Impuls. Aber es war nicht der einzige Grund, weshalb sich im April 2013 eine neue Bitcoin-Blase aufblähte. Vielleicht war es noch nicht mal ein besonders wichtiger Grund.

Wesentlich entscheidender dürfte das erste Halvening gewesen sein. Sie erinnern sich an die kontrollierte Ausschüttung neuer Bitcoins: Alle 210.000 Blöcke halbiert sich die Förderrate. Am 29. November 2012 war es so weit. Bisher hatten die Miner 50 Bitcoins erhalten, wenn sie einen Block fanden, was etwa alle zehn Minuten geschieht. Nun bekamen sie nur noch 25 Bitcoins. Anstatt 7200 flossen nun am Tag nur noch 3600 neu erzeugte Bitcoins auf den Markt.

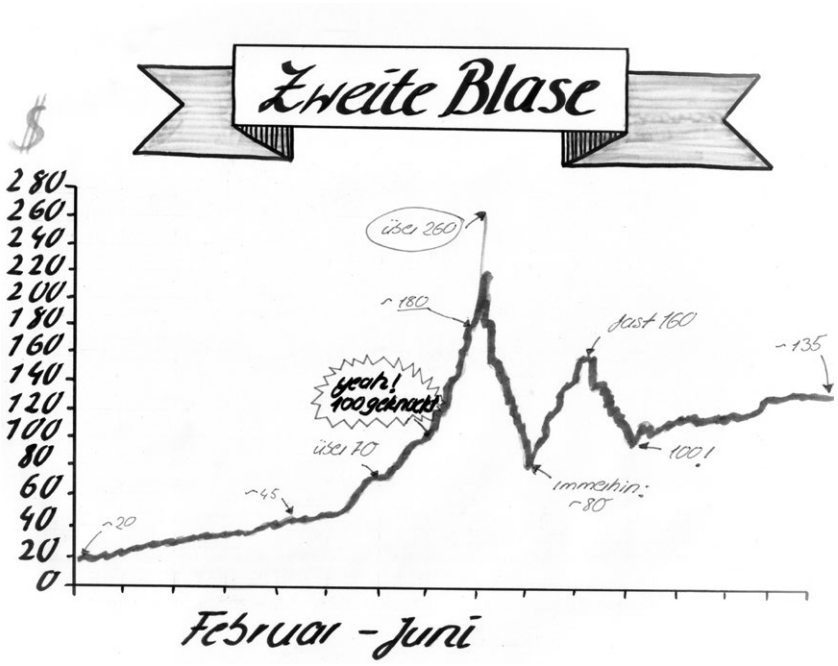
Denken Sie an die Ölpreiskrise. In den 1970ern kappte die OPEC die Förderrate von Rohöl um 5 Prozent. Da die Nachfrage gleich blieb oder sogar stieg, schnellte der bisher stabile Ölpreis von 3 auf 5 Dollar je Barrel. Ein Jahr später kostete er bereits zwölf Dollar. Dies war die Folge einer Verknappung um nur 5 Prozent. Was passierte erst, wenn man die Förderrate um 50 Prozent kürzte wie bei Bitcoin?

Zunächst passierte gar nichts. Die Märkte schienen das Ereignis zu ignorieren. Der Bitcoin-Preis blieb beim damaligen Kurs von etwa 13 Dollar. Die stoische Ruhe, mit der die Märkte eine so drastische Kürzung des Angebots aufnahmen, war bemerkenswert. Warum blieben sie bei Bitcoin so ruhig, während sie bei der Ölpreiskrise so heftig reagiert hatten? Es könnte daran liegen, dass der Schock mit Ansage geschah. Bitcoin ist, in dieser Hinsicht, ein einzigartiges Experiment, das beweist, dass Märkte selbst mit drastischen Änderungen von Angebot und Nachfrage sehr gut umgehen können, sofern diese angekündigt werden. Als das Halvening geschah, war es längst eingepreist. Möglicherweise hätten die Bitcoin-Märkte es ohne die Aussicht auf dieses Ereignis gar nicht geschafft, den Bärenmarkt zu verlassen.

Ohne Effekt blieb das Halvening jedoch nicht. Denn mittelfristig führte die Verknappung des Angebots zu einem beispiellosen Anstieg des Preises. Ob aber Zypern nun der Grund war oder nur Auslöser – einige Monate nach dem Halvening stürmte Bitcoin in die nächste Blase.

Die zweite Blase ($260)

Am 10. April 2013 erreichte der Bitcoin-Preis einen neuen Rekord von 260 Dollar. Wenn man bedenkt, dass er am Anfang jenes Jahres noch bei 10 bis 15 Dollar lag, ist dieser Anstieg beachtlich.



Vitalik Buterin, ein damals 19-jähriger Kanadier mit russischen Wurzeln, der später als Chefentwickler der Kryptowährung Ethereum das wertvollste Wunderkind der Erde werden sollte, schrieb zu dieser Zeit noch für das Bitcoin Magazine. Akribisch schilderte er die Ereignisse jenes Tages:

„Am Mittwoch, den 10. April, erreichte der Preis um 12.00 Uhr ein neues *Allzeithoch* von 266 Dollar. Danach sank der Kurs langsam wieder. Nach einem Absacken auf 240 Dollar erholte er sich kurz auf 258 Dollar, rutschte aber rasch weiter abwärts. Nach vier Stunden war er auf 225 Dollar gefallen, nach fünf Stunden auf 200, und um 19.20 Uhr erreichte er ein Tief von 105 Dollar. Dann sprang er wieder für einige Minuten auf 203 Dollar.“ Der Kurs hüpfte wie ein Gummiball. Ab, auf, ab, auf, ab. Auf den Börsen wurde wie verrückt gehandelt, das Volumen überstieg alles bisher Dagewesene, viele Plattformen waren dem Ansturm nicht gewachsen.

Dann überschlugen sich die Ereignisse. Das Gerücht, Mark Karpeless' Mt. Gox stehe unter einem sogenannten DdoS-Angriff, fegte durchs Internet. DdoS steht für Distributed Denial of Service, was meint, dass ein Hacker mit einem Netzwerk aus gekaperten Computern sein Opfer mit so vielen Anfragen überhäuft, dass die Server überlastet sind. Karpeless bestritt dies zunächst, erklärte kurz darauf jedoch, dass es nun doch einen solchen Angriff gebe. Er musste – wie auch die anderen Börsen – die Systeme herunterfahren.

„Die Bitcoin-Ökonomie war bereits im Schockzustand. Der Ausfall der größten Börse, auf der etwa 60 Prozent des Handels stattfand, versetzte die Märkte in Panik. Die anderen Börsen – von denen viele ebenfalls abgeschaltet werden mussten, weil sie entweder durch DoS angegriffen wurden oder wegen der hohen Aktivität überlastet waren – konnten sich nicht einigen, was der richtige Preis war. Aber über eines bestand Konsens: Der Preis fiel." [37]

37 Vitalik Buterin, „The Bitcoin Crash: An Examination", in: Bitcoin Magazine, 13. April 2013, https://bitcoinmagazine.com/articles/the-bitcoin-crash-an-examination-1365911041/ [20.02.2018]