

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

Copyright © MOBY Verlagshaus
Neu-Ulm, Nersingen
www.moby-verlagshaus.de

Alle Rechte vorbehalten.

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 Wahrung Bitcoin ibt eine eigenartige Faszination aus, die bei manchen Menschen an Sucht grenzt. Vielleicht sogar an Besessenheit. Fur den, der einmal vom „Bitcoin-Virus“ gepackt wurde, gibt es oft keinen Weg mehr zuruck. Bitcoin wird nicht nur zum Hobby, sondern zum Lebensinhalt.

Ein Grund fur diesen oft bestaunten Enthusiasmus durfte sein, dass Bitcoin eine magisch anmutende Technologie ist. Die digitale Wahrung erzeugt etwas, das es eigentlich gar nicht geben darf: digitale Knappheit und Unveranderlichkeit. Alles im Internet kann beliebig vervielfaltigt und verandert werden. Nur Bitcoin nicht. Obwohl rein digital, verhalten sich die digitalen Munzen zuweilen so, als seien sie physische Objekte. Das fuhlt sich an, als ware die Technologie aus der Zukunft gefallen.

Nicht minder wichtig durfte 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 Zahnburste, sondern im eigentlichen, historischen Sinn: als Angriff auf die herrschende Ordnung. Bitcoin ist eine neue, staatenlose Wahrung, die von niemandem beherrscht oder kontrolliert werden kann. Sie verspricht eine globale Wahrungunion, in der es keine Zentralbanken, keine Kapitalkontrollen, keine Wechselkurse und keine Inflation mehr gibt.

Auch ich gehore zu den Menschen, die der virtuellen Wahrung verfallen sind. Als ich Mitte 2013 bei Recherchen zufallig auf Bitcoin stie, war ich sofort fasziniert. Ich las mich ein, und je mehr ich erfuhr, desto groer wurde mein Staunen und meine Faszination.

Kurz darauf begann ich fur die deutsche Handelsplattform Bitcoin.de als Redakteur des Bitcoinblog.de zu arbeiten. Langweilig wurde mir in den folgenden Jahren nie. Es passieren so viele groe und kleine Dramen rund um die Entstehung dieses neuen Geldsystems, jede Woche, fast jeden Tag. Irgendwann wurde mir klar: Bitcoin konnte die grote 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 beinahe 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 Kilo-byte, 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.

II. Das Geld des Internets



Wie Bitcoin erstmals Geld wurde

Die prämonetäre Phase

Bitcoin war zunächst kein Geld. Es war vielleicht eine Software, die etwas erzeugte, das wie Geld funktionierte – aber es war kein Zahlungsmittel, kein Wertspeicher, keine Rechnungseinheit. Bitcoin war in den ersten Jahren nicht einmal Spielgeld.

Einen echten Wert hatten die digitalen Münzen nicht. Es gab zwar Liebhaber und Sammler, die sie über Chats und Foren von den Minern kauften. SmokeTooMuch, der erste bekannte Bitcoiner aus Deutschland, hat einmal 10.000 Bitcoins für 50 Dollar zum Kauf angeboten, aber niemand wollte. Für dieselbe Summe gelang es Laszlo Hanyecz im Mai 2010, sich zwei Pizzen liefern zu lassen. Der Tag ist seitdem als Bitcoin-Pizza-Day bekannt, doch dies ändert nichts daran, dass Bitcoin in dieser Zeit in keinsten Weise echtes Geld war. Es war ein schrulliges, obskures Experiment in einem entlegenen Teil des Internets.

Viele bestritten, dass Bitcoin überhaupt jemals einen echten Wert haben könnte. Denn es gibt einen gravierenden Unterschied zwischen Bitcoins und den Münzen des althergebrachten Warengeldes aus Edelmetall. Letztere haben nicht nur einen Wert durch ihre Eignung als Speicher für Kaufkraft, sondern auch einen intrinsischen Wert. Dieser entsteht dadurch, dass sie materiell nützlich sind, etwa um zu Schmuck verarbeitet zu werden.

Bitcoin hat offensichtlich keinen solchen intrinsischen Wert. Daher waren und sind viele Ökonomen und Investoren überzeugt, dass der Wert von Bitcoin auf Null fallen kann. Am ausgeprägtesten ist dieses Misstrauen ausgerechnet bei jenen Ökonomen, die Bitcoin an sich viel Gutes abgewinnen: bei den Vertretern der Österreichischen Schule und bei den Liberalen. Jeffrey Tucker, einer der Direktoren der US-amerikanischen Foundation of Economic Education, einem libertären Think-Tank, hatte lang nicht geglaubt, dass man Geld durch einen Computer-Code erzeugen kann. „Das erschien mir absurd, wie eine Techno-Version der Alchemie“, schrieb er rückblickend 2014. „Geld musste aus Gütern entstehen, die im Tauschhandel genutzt werden. Das hatte Carl Menger bewiesen. Wenn Bitcoin einen Wert hat, dann muss das ein Irrtum sein, oder das Ergebnis eines guten Marketings.“

Später gestand sich Tucker ein, sich geirrt zu haben. Verblüfft stellte er fest:

„Bitcoin ist Geld. Es wird jeden Tag benutzt. Man kann es auf den Börsen in Echtzeit sehen. Es ist kein Märchen. Es ist echt.“²⁹

Wie aber kann etwas, das absolut keinen inneren Wert hat, zu Geld werden? Bereits Satoshi hatte 2010 versucht, diese Frage zu beantworten: „Stell dir vor, es gibt ein Metall, das so knapp ist wie Gold, aber die folgenden Eigenschaften hat: Es ist langweilig grau, kein guter Leiter von Strom, nicht besonders fest, aber auch nicht besonders weich, nicht nützlich für irgendwelche praktischen oder dekorativen Zwecke, aber es hat die eine magische Eigenschaft, dass es über einen Kommunikationskanal transportiert werden kann. Wenn es auf irgendeine Weise irgendeinen Wert erhält, aus welchem Grund auch immer, dann könnte jeder, der Vermögen über eine weite Distanz transportieren möchte, ein wenig von diesem Metall kaufen, es transferieren, und der Empfänger verkauft es.“³⁰

Dies zeigt, wie tief verwurzelt Satoshi im Modell des Warengeldes ist. Er begreift Bitcoin als eine Ware, die man kaufen kann, um sie als Speicher und Transportmittel für Werte zu verwenden. Der Wert der Einheit liegt im Zahlungssystem. Dies überzeugte auch Jeffrey Tucker: „Wenn man das einmal versteht“, schrieb er, „erkennt man, dass der Wert von Bitcoin an das angehängte Zahlungsnetzwerk gebunden ist. Das ist der Wert, den Mises meint. Er liegt nicht in der Einheit der Währung, sondern in dem brillanten und innovativen Zahlungssystem, auf dem Bitcoin lebt.“

Die digitale Münze Bitcoin bekommt also einen Wert, wenn es eine Nachfrage nach dem Zahlungssystem Bitcoin gibt, nach dieser ganz speziellen Kaufkraft, die man nur erwerben kann, wenn man Bitcoins kauft. Diese Nachfrage bestand bis Anfang 2011 nicht.

²⁹ Jeffrey A. Tucker, What Gave Bitcoin Its Value? (2014) <https://fee.org/articles/what-gave-bitcoin-its-value/> [20.02.2018]

³⁰ Satoshi, Re: Bitcoin does NOT violate Mises' Regression Theorem, 27.08.2010, <https://bitcoin-talk.org/index.php?topic=583.msg11405#msg11405> [20.02.2018]

Drogen aus dem Darknet

Im Februar 2011 eröffnete Ross Ulbricht alias *Dread Pirate Roberts* den Online-Drogenmarkt Silk Road. Wir werden darüber später noch mehr erfahren. Hier nur so viel: Die Silk Road war ein Amazon-artiger Marktplatz im verborgenen Teil des Internets, dem sogenannten Darknet, auf dem man illegale Waren kaufen konnte, vor allem Drogen.

Die Silk Road war etwas Neues, Unerhörtes: der erste Online-Schwarzmarkt mit einem nutzerfreundlichen Händlersystem. Bisher liefen solche Geschäfte meistens über klandestine Foren ab. Hier hingegen konnten die Händler ein Profil aufbauen, sich einen Shop einrichten, und die Kunden konnten bequem stöbern und bestellen. Es gab mehr Auswahl als in jedem Amsterdamer Coffeeshop, und die Drogen kamen einige Tage später mit der Post an. Fast alles, was eine Legalisierungs-Kampagne jemals erreichen konnte, war mit der Silk Road über Nacht Wirklichkeit geworden.

Möglich wurde dies durch Bitcoin. Man konnte die Drogendealer mit Bitcoin bezahlen, ohne dass ein Mittelsmann wie eine Bank Überweisungen blockieren oder der Polizei melden konnte, und die Dealer konnten bequem Geld empfangen, ohne ihre Identität verraten zu müssen. Die Geschichte von Bitcoin geht zwar weit über die Silk Road hinaus. Doch deren Bedeutung ist gigantisch: Sie schuf eine Nachfrage nach Bitcoin. Sie war der Schwarze Schwan, ein statistisch unwahrscheinliches, aber nicht unmögliches Ereignis, dessen Auftauchen extreme Konsequenzen haben kann: Sie machte Bitcoin, ein freies, obskures Softwareprojekt, zu einer Währung.

Mt. Gox, die erste echte Bitcoin-Börse

Die ersten Plattformen, auf denen man Bitcoins handeln konnte, waren bereits im Frühjahr 2010 entstanden. Doch sie waren träge Marktplätze, die keine Preisfindung in Echtzeit zuließen. Ein richtiger Börsenhandel wurde erst im Juli jenes Jahres möglich, als ein Jed McCaleb im Bitcoin-Forum Mt. Gox ankündigte: „Hallo miteinander, ich habe eine neue Bitcoin-Börse aufgesetzt. Bitte sagt mir, was ihr darüber denkt.“

Damit war jene Börse geboren, die den Bitcoin-Handel für die kommenden Jahre dominieren sollte. Der Name steht eigentlich für Magic:

The Gathering Online Exchange, denn Jed McCaleb hatte Mt. Gox als Online-Börse für das gleichnamige Sammelkartenspiel gegründet, nun jedoch „auf die Schnelle“ für den Bitcoin-Handel umgebaut.

Mt. Gox war die erste Bitcoin-Börse, auf der man in Echtzeit mit Bitcoins handeln konnte. Das tägliche Handelsvolumen stieg rasch an. Im Februar wurden bereits mehr als 10.000 Bitcoins am Tag gehandelt. Bei einem Preis von etwa 5 Cent je Stück waren dies zwar kaum mehr als einige hundert Dollar, aber, immerhin: Bitcoin hatte einen Wert, der durch den fortlaufenden Handel immer wieder bestätigt wurde. Nachdem die Silk Road eröffnet worden war, wuchs das Handelsvolumen noch rascher. Es gab Tage, an denen auf Mt. Gox bereits Bitcoins im Wert von 50.000 Dollar den Besitzer wechselten.

In dieser Zeit schien das Projekt seinem Gründer McCaleb jedoch über den Kopf zu wachsen. Es machte immer mehr Arbeit und vor allem auch Ärger. Im Februar war ein Hacker in den Account eines Kunden der Börse eingebrochen und hatte sich 45.000 Dollar auf sein eigenes Konto überwiesen. McCaleb fand rasch heraus, was geschehen war, und for die Guthaben des Hackers ein. Der wiederum machte in Foren öffentlich Druck, während McCaleb der Polizei zu erklären versuchte, was geschehen war.

Zwei Wochen später verkaufte er die Börse „an jemanden, der besser geeignet ist, die Seite auf das nächste Level zu bringen“, wie er schrieb. Der Käufer war Mark Karpeless, der unter dem Pseudonym MagicalTux auftrat.³¹ Karpeless wurde damit zum Besitzer der größten Bitcoin-Börse – und zur vermutlich ersten Person der Welt, die Bitcoin zu einem Vollzeitjob machte. Er sollte für die kommenden Jahre eine so große Rolle im Bitcoin-Universum spielen, dass es sich lohnt, ihn näher kennenzulernen.

Der König des Bitcoin-Handels

Mark Karpeless hat zwei Gemeinsamkeiten mit Roger Ver: Der gebürtige Franzose lebte in Tokio, und als er Ende 2010 Bitcoin ent-

³¹ „MagicalTux hat bereits viel für die Bitcoin Community gemacht, und er wird in vielerlei Hinsicht besser darin sein, die Seite zu betreiben, als ich es bin.“ Jed McCaleb auf Bitcointalk, 6. März 2011, <https://bitcointalk.org/index.php?topic=4187.msg60628#msg60628> [0.02.2018]

deckte, war es für ihn eine Offenbarung. Während Roger Ver jedoch ein Geschäftsmann ist, ist Mark Karpeless ein Programmierer, und Roger liebt es, öffentlich aufzutreten, während Mark lieber mit Computern kommuniziert als mit Menschen.



Karpeless wurde 1985 in Chenôve geboren, besuchte diverse Internate und studierte in Paris. Bereits mit zehn Jahren programmierte er (laut seiner Mutter hat er einen Intelligenzquotienten von 190 – „normal“ sind 100). Auf den Internaten verbrachte er seine Zeit zurückgezogen mit japanischen Mangas und einem Notizbuch, in dem er für zu Hause Code für Computerprogramme aufschrieb, da er im Internat keinen PC hatte.

Ab 2003 arbeitete er als Entwickler der Programmiersprache PHP und stieg in den inneren Kreis der PHP-Entwickler auf. Sein Chef nannte ihn ein „Computer-Genie, das neben seinem Laptop aß und schlief“.

Allerdings langweilte er sich schnell. Er verbrachte seine Arbeitszeit damit, zu chatten und einen Server für ein Online-Rollenspiel zu entwickeln. Nachdem er deswegen seinen Job verloren hatte, begann eine depressive Phase, angeblich hatte er sogar versucht, sich mit einem Computerkabel zu erhängen. 2009 zog er nach Japan, ins Land der Spielzeugroboter und Mangas. In Tokio gründete er Tibanne, eine Firma, die Websites hostete. Er lernte rasch Japanisch und verliebte sich.

Ende 2010 entdeckte er Bitcoin. Wie so viele andere war er sofort hin und weg. Vermutlich hat er sich ununterbrochen mit Bitcoin beschäftigt und kaum geschlafen. Seine Posts im Bitcoin-Forum zeigen, mit welcher Energie er sich auf die Kryptowährung stürzte: Er akzeptierte Bitcoins für seinen Hosting-Service KalyHost (vermutlich als Erster überhaupt), baute eine eigene Wallet (um Bitcoins zu speichern und zu versenden), schrieb Teile des Codes in PHP um, gründete ein Bitcoin-Wiki und sammelte IP-Adressen des Bitcoin-Netzwerkes in einer Datenbank – und all dies in zehn Tagen. Wer schon einmal versucht hat, auch nur eine einzige dieser Aufgaben zu lösen, weiß, dass dies selbst für sehr gute Programmierer eigentlich unmöglich ist.

Einige Monate später übernahm Mark Karpeless Mt. Gox. Damit begann die große Geschichte seines Lebens. Er wurde, schrieb der Rolling Stone 2015, „versehentlich zum Herrscher von Bitcoin. Ein unglücklicher Geek wurde, auch zu seiner eigenen Überraschung, zum mächtigsten Fürsten des digitalen Bargelds.“³²

Die erste Blase (\$30)

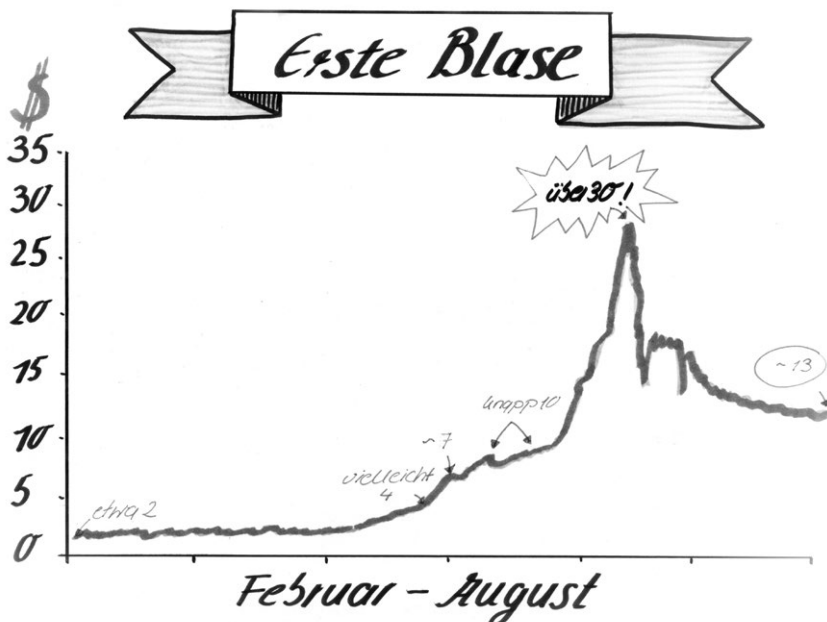
Mark Karpeless hatte einen glücklichen Zeitpunkt erwischt. Im Frühjahr 2011 setzte sich der Bitcoin-Zug in Bewegung. Roger Ver kaufte für 50.000 Dollar auf Mt. Gox Bitcoins. Im Mai stieg der Preis bereits auf 3 Dollar. Die einen kauften Bitcoins, um auf der Silk Road zu shoppen, und die anderen, weil sie darauf spekulierten, dass der Wert weiter stieg. Ab einem gewissen Moment gab es kein Halten mehr. Die vielleicht mächtigste aller Blasen in der Geschichte des Bitcoins blähte sich auf.

32 Rolling Stone, The Rise and Fall of a Bitcoin Kingpin, (27.08.2015)
<http://www.rollingstone.com/culture/features/the-rise-and-fall-of-a-bitcoin-kingpin-20150827>
[20.02.2018]

Der Kurs verzehnfachte sich innerhalb eines Monats und schoss auf atemberaubende 30 Dollar. Das tägliche Handelsvolumen von Mt. Gox, im März noch einige Tausend Dollar, erreichte 3 Millionen Dollar. Die Börse war zu einer Riesensache geworden, Mark Karpeless saß auf einer Goldgrube. Die Einnahmen flossen, er heiratete seine japanische Freundin und kaufte sich in einem angesehenen Viertel Tokios eine Wohnung.

Der Bitcoin-Preis verharrte für einen kurzen Moment bei 30 Dollar. Dann geschah das, was bei allen Blasen passiert: Einige Verkaufsangebote blieben unbeantwortet. Der Kurs zitterte, dann knickte er plötzlich ein, fing sich wieder, federte zurück und fiel noch tiefer. Die Blase platzte.

Wenn man den Kurs logarithmisch betrachtet (S.167), sich also nicht die absoluten, sondern die relativen Preissteigerungen anschaut, war die Blase im Juni 2011 der steilste Kursanstieg in der Geschichte von Bitcoin. Nachdem der Gipfel erreicht war, fiel der Preis für eine lange Zeit, und wer auf der Spitze der Blase eingekauft hatte, blieb für viele Monate im Minus. Doch wie alle Blasen hatte auch diese ihre gute Seite: Sie zog neue Nutzer, Investoren und Unternehmer an.



Es entstand eine Basis-Infrastruktur. Unternehmen wie die Online-Wallet Blockchain.info, der Zahlungsdienstleister *BitPay* oder die Börse *BitStamp* wurden gegründet. Sie sind bis heute Säulen der Bitcoin-Ökonomie. Programmierer entwickelten Software-Bibliotheken, die Bitcoin besser benutzbar machten, Leute wie Roger Ver nutzten die Vermehrung ihres Kapitals, um in Bitcoin-Start-ups zu investieren. Der „Bitcoin Jesus“ Roger Ver reiste um die Welt, um von Bitcoin zu kündigen. Er bezahlte Radio-Spots, ließ riesige Werbeplakate aufstellen und machte den Honigdachs zum beliebtesten Maskottchen von Bitcoin: So, wie dieses furchtlose Mardertier es im Zweifel sogar mit Löwen und Büffeln aufnimmt, fordert der kleine Bitcoin die großen Zentralbanken heraus.³³

Die Blase von 2011 wirkte wie ein Turbolader – sie gab der dezentralen Währungsreform einen mächtigen Schub.

Die Gründung von Bitcoin.de

Eine der Gründungen dieser Zeit ist der deutsche Bitcoin-Marktplatz Bitcoin.de. Oliver Flaskämper gründete ihn im Sommer 2011.

Flaskämper ist eine interessante Unternehmerpersönlichkeit. Er war in den späten 90ern auf ungewöhnliche Weise in das Internet-Business eingestiegen: Er kaufte sich Internet-Domains mit Namen, von denen er annahm, dass andere sie einmal haben wollten. „Alle dachten, ich hätte eine Schraube locker“, erzählte er später. „Wie kann man so viel Geld in nichts investieren? In Bits und Bytes? Niemand verstand mich. In den Augen der anderen war ich ein verrücktes Alien. Als ich eine Domain für 10.000 D-Mark kaufen wollte, machten sich einige Freunde und Familienmitglieder ernsthaft Sorgen um meine geistige Gesundheit. Ich kaufte die Domain und wollte noch weitere kaufen. Also ging ich zu meiner Bank und wollte die Domain als Sicherheit für einen Kredit hinterlegen, mit dem ich mehr Domains kaufen würde. Ich versuchte, meinem Bankberater zu erklären, was Domains sind, warum sie einen Wert haben und warum sie sogar eine bessere Sicherheit darstellen als ein Haus oder ein Auto.“ Zwei Jahre später verkaufte er die

³³ Das Guinness-Buch der Rekorde listete den Honigdachs 2002 in der Kategorie „furchtlosestes Tier der Welt“. Inzwischen wurde die Kategorie jedoch mangels objektiver Messbarkeit geschlossen.

erste Domain für 50.000 Euro. Es folgten weitere gute Geschäfte mit Domains. Mit den Gewinnen baute er sein Internet-Imperium auf.

Oliver Flaskämper ist Gründer aus Passion. Er schafft Unternehmen, zieht sie groß, übergibt die Führung dann aber an jemand anderen und berät als Teilhaber aus dem Hintergrund. Er hat eine Begabung dafür, die richtigen Impulse zu setzen und durchzusetzen, lässt seinen Mitarbeitern aber gleichzeitig viel Freiheit. In ihm treffen neuer Markt und Bodenständigkeit zusammen. Während die Start-up-Szene nach Berlin zog, blieb er seiner Heimat, dem ostwestfälische Städtchen Herford, treu, wo er Mitglied in der Vollversammlung der IHK ist und ein hervorragendes Verhältnis zu Banken und anderen Unternehmen unterhält. Flaskämper geht nicht nach Berlin, sondern bringt ein Stückchen Berlin in seine Heimat, etwa indem er ein altes Industriedenkmal renoviert und zu seinem Hauptquartier macht, oder indem er gemeinsam mit der Sparkasse ein großes Coworking-Haus gründet.

Als Oliver Flaskämper Bitcoin kennenlernte, setzte jene Reaktion ein, die wir schon von Roger Ver und Mark Karpeless kennen: Ihm dämmerte, dass Bitcoin funktionierte, dass darin altes und neues Gold verschmelzen konnte und dass sich das wiederholte, was er schon mit den Domains erlebt hatte, allerdings mit einem viel größeren Potenzial: Sein Instinkt sagte ihm, dass hier ein riesiger, vollkommen unerschlossener Markt auf ihn wartete. Elektrisiert rief er sein Team zusammen. „Meine Stimme zitterte. Ich sah, dass viele Leute ungläubig ihre Augen verdrehten. Am Ende gelang es mir aber, meine Idee durchzuboxen, und wir begannen, den Marktplatz Bitcoin.de zu entwickeln. Nur drei Monate später, im September 2011, gingen wir online.“

Oliver Flaskämper und sein Team ahnten nicht, auf was für ein Abenteuer sie sich damit eingelassen hatten.³⁴

Der Bankraub kehrt zurück

Schauen wir uns noch mal die Unterschiede zwischen Bitcoin und einem traditionellem Bankguthaben an. Wenn Sie eine App benutzen oder eine Software wie PayPal, öffnen Sie ein Programm, das Ihnen

³⁴ Ich bin hier nicht vollständig neutral, da Bitcoin.de mich seit 2013 dafür bezahlt, das Bitcoinblog.de zu schreiben. Allerdings kann ich aufrichtig sagen, dass der Bitcoin-Marktplatz der beste Auftraggeber ist, den ich jemals als freier Autor hatte.

zeigt, wie hoch Ihr Guthaben ist, und das Ihnen ermöglicht, dieses zu überweisen. Dasselbe macht die Bitcoin-Software.

Unter der Oberfläche stoßen wir jedoch auf einen bemerkenswerten Unterschied. Das Guthaben auf der Bank ist virtuell, es ist, mehr oder weniger, nur ein Eintrag in einer Datenbank, den man, wenn es unbedingt sein muss, zurückbuchen kann. Bitcoins verhalten sich eher wie Geldscheine oder Goldbarren: Wenn man sie einmal übergeben hat, kann man die Transaktion nicht mehr revidieren. Keiner kann sie rückgängig machen. Nicht die Polizei, nicht Satoshi Nakamoto, nicht die Miner. Bitcoins sind zwar rein digital, verhalten sich hier aber wie physische Dinge. Diese Eigenschaft ist extrem faszinierend – doch sie bringt auch eine Plage zurück, von der man dachte, dass sie nahezu ausgerottet sei: den Bankraub.

Der klassische Bankraub hat eine lange Geschichte. Von den Piraten, die die spanische Silberflotte enterten, über die Banditen im Wilden Westen bis zu den großen Überfällen des 20. Jahrhunderts – es lohnte sich, eine Bank oder einen Geldtransporter zu überfallen. Noch in den 1990ern konnte die Beute sechs- oder siebenstellig sein. Als die Digitalisierung jedoch auch im Geldwesen um sich griff und Kartenzahlungen und Online-Banking zur Norm wurden, schien sich der Bankraub aus der Geschichte zurück- zuziehen. Es rentierte sich nicht mehr, die Beute wurde immer kleiner, weil Banken immer weniger Bargeld vorrätig haben müssen.

Natürlich greifen auch Hacker Banken an, was man einen digitalen Bankraub nennen könnte. Aber die Überweisungen, die sie ausführen, wenn sie sich in ein System gehackt haben, bleiben in den Datenbanken der Banken, und die Beute ist erst sicher, wenn es gelingt, das Geld als Banknote am Automaten abzuheben. In sehr seltenen Fällen, wie beim SWIFT-Hack 2016, bringt ein Bankraub noch einige Millionen Euro.

Ein Bitcoin-Bankraub hingegen lohnt sich. Wenn ein Hacker in eine Börse einbricht und es ihm gelingt, sich eine gültige Bitcoin-Transaktion auszuzahlen – so, als würde er eine Banküberweisung veranlassen –, dann ist das so, als würde er sich das Geld in Scheinen auszahlen. Eine einzige Transaktion kann Millionen oder gar Hunderte von Millionen Euro unwiderruflich in den Besitz des Hackers bringen. Bitcoins sind das perfekte Diebesgut für digitale Raubzüge.

Wie ein Hacker beinah Bitcoin vernichtet

Es ist nicht schwer, im Bitcoin-Raum das beliebteste Ziel der Hacker im Jahr 2011 zu identifizieren: Mt. Gox, die größte Börse. Am 19. Juni – nur wenige Tage nachdem die Blase geplatzt war – geschah das Unvermeidliche: Ein Hacker griff an und verschaffte sich Zugang zu Hunderten von Accounts.

Theoretisch war es für den Hacker nun möglich, sich die Bitcoins der anderen Kunden auszuzahlen und damit unwiderruflich in seinen Besitz zu bringen. Allerdings gab es ein Tageslimit für Abhebungen. Dieses Limit hatte jedoch eine Schwachstelle: Es war in Dollar angegeben. Der Hacker verkaufte daraufhin fast alle Bitcoins in den gehackten Accounts, was den Preis abstürzen ließ. Dann kaufte er die Bitcoins günstig wieder ein und zahlte sie aus, während der Preis noch so tief lag, dass das Tageslimit in Dollar keine Auswirkung hatte.

Damit löste er den schlimmsten Crash aus, den wohl jemals eine Börse gesehen hatte. Der Preis, eben noch bei 17,50 Dollar, sank innerhalb weniger Minuten auf den geringsten möglichen Wert, auf 0,01 Dollar. Panik ist ein zu harmloses Wort, um zu beschreiben, was danach passierte. Die anderen Börsen kollabierten, sie stoppten den Handel oder gingen unter der Datenlast in die Knie. Auch Mark Karpeless fuhr die Plattform herunter.

Es sah nicht gut aus. Die Wirtschaftszeitschrift Forbes schrieb damals eine der ersten „Bitcoin-Grabreden“: „All das bedeutet nicht zwingend das Ende von Bitcoin, aber es sieht ganz danach aus. Bitcoins sind nicht sicher, wie der Diebstahl und die Passwort-Probleme gezeigt haben. Sie sind nicht liquide, und sie sind kein Wertspeicher, wie der Preiskollaps zeigt. Und wenn sie all das nicht sind, dann sind sie kein gutes Tauschmittel.“

Bitcoin war beinah gestorben. Aber eben nur beinah. Mark Karpeless hatte gerade noch verhindert, dass der Hacker sich alle Bitcoins auszahlen konnte. Einige Tage später ging Mt. Gox wieder online und Karpeless setzte den Preis zurück auf den Wert, den er vor dem Hack gehabt hatte. Die anderen Börsen und der Markt folgten ihm. Es war noch einmal gutgegangen.

Bitcoin ist Krieg

Der Mt.-Gox-Hack war der erste spektakuläre Raub in der Geschichte von Bitcoin. Er war aber beileibe nicht der letzte. Ganz im Gegenteil. Ihm folgte eine Welle an Schreckensberichten über Hacks und Verluste, die bis heute anhält. Man könnte einhundert Beispiele nennen, von den beiden Bitcoinica-Hacks, bei denen 2011 mehr als 50.000 Bitcoins geraubt wurden, über die Hacks bei den großen Bitcoin-Unternehmen *BitStamp*, *BitPay*, *BitFinex* und *ShapeShift* bis zu *CoinCheck*, jener japanischen Börse, der Anfang 2018 die Einheiten einer anderen Kryptowährung im Wert von rund 500 Millionen Dollar gestohlen wurden.

Bitcoin-Unternehmen, das begriff man im Jahr 2011 unter Schmerzen, agieren im Kriegsgebiet. Und je mehr Bitcoins wert werden, desto schlimmer werden die Angriffe. Am Anfang waren es noch Skript-Kiddies, die aus irgendeinem Hobbykeller heraus Börsen infiltrierten. Später wurden daraus Hacker-Banden, die mit Zombie-Netzen aus tausenden gekaperten Computern DoS-Angriffe auf Börsen fuhren. Je höher der Preis und je größer demnach die Beute, desto professioneller die Hacker, und desto mehr müssen die Firmen ihre Plattformen zu einer Festung ausbauen.

Handelsplattformen wie Bitcoin.de hatten im Herbst 2011 ein tägliches Handelsvolumen von vielleicht einigen tausend Euro. Heute werden auf Bitcoin.de am Tag Bitcoins im Wert von mehreren Millionen Euro gehandelt, und der Marktplatz speichert auf seinen Wallets Kunden-Bitcoins im mehrstelligen Millionenwert. Ein Hack kann katastrophale Folgen haben.

Die gute Nachricht ist jedoch: Man kann bei Bitcoin, im Prinzip, relativ einfach ein sehr hohes Maß an Sicherheit erreichen. Denn im Unterschied zu den Bitcoin-Börsen ist Bitcoin selbst offensichtlich nicht zu hacken. Dan Kaminsky, der berühmte Sicherheitsforscher, der jedes System für knackbar hält, versuchte es und scheiterte, wie alle vor und nach ihm.

Dies macht Hacks auf der einen Seite so fürchterlich, weil Transaktionen absolut irreversibel sind. Auf der anderen Seite erlaubt es Unternehmen, sich gut zu schützen: Eine Börse muss nur die für eine gültige Transaktion notwendigen Schlüssel so speichern, dass sie keinen Kontakt zum Internet haben. Wie sollten die Bitcoins gehackt

werden, wenn die Schlüssel vom Netz getrennt sind? Bitcoin.de lagert deshalb rund 98 Prozent der Kunden-Bitcoins auf sogenannten Cold Wallets, die nicht online zugänglich sind. Mark Karpeless ging nach dem Hack 2011 sogar so weit, dass er die privaten Schlüssel der Wallets von Mt. Gox in mehrere Teile zerschnitt und diese in verschiedenen Tresoren in Tokio bunkerte.

Leider reichte dies damals nicht aus, um die Erosion des Vertrauens aufzuhalten, die die vielen Hacks jenes Jahres verursacht hatten. Der Preis, der ohnehin schon gefallen war, wurde immer weiter gedrückt: Bitcoin ging durch seinen ersten *Bärenmarkt*, eine Baisse.

Wenn die Bären übernehmen

Bulle und Bär sind die beiden natürlichen Kontrahenten auf der Börse. Der Bulle ist ein Optimist, er erwartet steigende Preise, kauft nach und treibt den Kurs nach oben. Der Bär dagegen ist pessimistisch. Er erwartet sinkende Kurse, verkauft und wartet darauf, dass der Preis tief genug ist, um wieder einzukaufen.

Auf allen Börsen ringen Bullen und Bären miteinander. Immer wieder gewinnt eine Seite die Oberhand. Wenn sich die Bullen durchsetzen, steigen die Preise – wie bei Bitcoin im Frühjahr 2011. Ab einem bestimmten Zeitpunkt kapitulierten die Bären. Sie warteten nicht mehr auf sinkende Kurse und kauften zähneknirschend ein. Nachdem die Blase geplatzt war, setzten sie sich jedoch wieder durch. Ein von Bären dominierter Markt ist wie ein langer, zäher Winter, da der Trend, egal was passiert, nach unten weist. Bärenmärkte machen nicht viel Spaß.

Der Kurs sank monatelang, immer weiter. Es gab noch mehr Hacks, und die Presse unkte, dass Bitcoin kaputtgegangen sei. Das Technik-Magazin Gizmodo schrieb: „Ohne jeden Zweifel war der Aufstieg von Bitcoin so amüsant wie interessant. Eine quasi-anonyme Internet-Währung, deren Preis auf 32 US-Dollar schießt, ist fesselnd. Aber die Flitterwochen sind vorbei, und Bitcoin fällt. Und zwar schnell.“ Am Ende würden die Investoren mit nichts zurückbleiben, prophezeite das Magazin.

Im November sackte der Preis auf 2 Dollar ab. Das war der Boden. Es sollte noch lange dauern, bis er wieder nennenswert stieg. In der

öffentlichen Wahrnehmung war Bitcoin, wie das Magazin Wired in einem ausführlichen Artikel schrieb, „über Nacht von der Währung von morgen zu einem dystopischen Witz geworden“. Oliver Flaskämper fragte sich, ob er sich geirrt hatte. War es so wie damals, als er 1996 eine Dating-Plattform aufgebaut hatte und irgendwann einsehen musste, dass es nichts brachte, da beinahe 100 Prozent seiner Kunden Männer waren? Das Internet war noch nicht reif für seine Idee gewesen. War er auch mit Bitcoin seiner Zeit zu weit voraus?

Doch Bitcoin war noch nicht am Ende.