

Die Bitcoin Bibel

Das Buch zur digitalen Wahrung



Dr. Philipp Giese • Maximilian Kops • Sven Wagenknecht
Danny de Boer • Mark Preuss

Die Bitcoin-Bibel

Das Buch zur digitalen Wahrung

BTC-ECHO

Copyright © 2017 BTC-ECHO

All rights reserved.

2. Auflage (07. Januar 2017)

ISBN-10: 1534733191
ISBN-13: 978-1534733190

BTC-ECHO

Die Bitcoin-Bibel

Das Buch zur digitalen Wahrung

Dr. Philipp Giese
Mark Preuss
Maximilian Kops
Sven Wagenknecht
Danny de Boer

IMPRESSUM

Texte: © Copyright by BTC-ECHO
BTC-ECHO UG (haftungsbeschränkt)
Albersallee 34
47533 Kleve
info@btc-echo.de

Alle Rechte vorbehalten.

Tag der ersten Veröffentlichung: 18.06.2016
www.btc-echo.de/impressum

Inhalt

INHALT	1
VORWORT	1
KAPITEL 1 DAS BITCOIN-SYSTEM	5
WAS IST BITCOIN	5
POLITISCHE DIMENSION UND REGULIERUNG	8
DAS BITCOIN-WHITEPAPER	13
ZUSAMMENFASSUNG DES WHITEPAPERS	13
WER HAT BITCOIN ERFUNDEN?	15
SATOSHI NAKAMOTO	15
WAR ER JAPANER?	16
WEISS IRGENDJEMAND, WER SATOSHI NAKAMOTO WAR?	17
WAS WISSEN WIR ÜBER IHN?	20
GESCHÄTZTES VERMÖGEN	21
WAS MACHT ER JETZT?	21
STEUERN UND RECHT	21
BITCOIN UND RECHT	21
RECHTLICHE UND STEUERLICHE PROBLEME	23
ERST RECHTLICHE PLANUNG, DANN START DES UNTERNEHMENS	24
BITCOIN UND STEUER	26
BITCOIN UND STEUER FÜR PRIVATANLEGER	26
BITCOIN UND STEUER FÜR UNTERNEHMEN	29
FRÜHZEITIGE BERATUNG IST SINNVOLL	31

KAPITEL 2 WELCHEN WERT HABEN BITCOINS?	35
ANGEBOT	37
NACHFRAGE	38
WERTENTWICKLUNG	41
KAPITEL 3 BITCOIN ALS WERTANLAGE	47
ZEIT IST GELD	50
KAPITEL 4 BLOCKCHAIN	55
WAS IST DIE BLOCKCHAIN	55
WIE FUNKTIONIERT DIE BLOCKCHAIN	57
FUNKTIONSWEISE UND SICHERHEIT EINER BITCOIN-TRANSAKTION	61
ALTERNATIVE BLOCKCHAIN-ANWENDUNGEN	70
AKTUELLE HERAUSFORDERUNGEN VON BITCOIN	72
KAPITEL 5 BITCOIN-MINING	77
WAS IST BITCOIN MINING?	77
BERECHNUNGEN	78
DIFFICULTY	81
WIE KANN ICH BITCOIN MINEN?	85
DIE 51%-ATTACKER	89
WAS IST EINE 51%-ATTACKER?	89
WIE FUNKTIONIERT EINE 51%-ATTACKER?	90
MÖGLICHKEITEN DER 51%-ATTACKER	93
KAPITEL 6 BITCOIN-WALLETS	97
MULTI-SIG-WALLETS – BRIEFASCHEN FÜR TEAMS	102

COLD-STORAGE – DAS OFFLINE-TRESORSYSTEM VON BITCOIN	104
WIE ERSTELLE ICH EIN WALLET?.....	106
ONLINE-WALLET	106
MOBILE-WALLET	108
PAPER-WALLET	109
BRAIN-WALLET	111
HARDWARE-WALLET	113
BITCOIN CORE	114
WIE SICHER IST MEIN WALLET?	116
<u>KAPITEL 7 BITCOIN KAUFEN UND VERKAUFEN</u>	<u>121</u>
MÖGLICHKEITEN, BITCOIN ZU KAUFEN.....	123
BITCOIN-BÖRSEN	124
BITCOIN-BROKER	126
FACE TO FACE	127
<u>KAPITEL 8 MIT BITCOIN BEZAHLEN</u>	<u>129</u>
WER AKZEPTIERT BITCOINS?.....	129
HILFSMITTEL ZUM BEZAHLEN MIT BITCOINS	130
ANDROID	131
IOS	134
WINDOWS-PHONE	135
ÜBERSICHT: WALLET-APPS FÜR UNTERWEGS	136
<u>KAPITEL 9 BITCOIN-AKZEPTANZ</u>	<u>137</u>
GRÜNDE FÜR DIE INTEGRATION VON BITCOIN	137
ERWEITERUNG DER ZIELGRUPPE	137
GERINGE TRANSAKTIONSGEBÜHR	138

ZAHLUNGSSICHERHEIT	140
INTERNATIONALITÄT	140
SCHNELLIGKEIT	142
COINMAP	145
BTC-ECHO-VERZEICHNIS	146
RISIKEN.....	147
DER KUNDE ZAHLT DIE GEBÜHREN	147
KEIN FIXER UMTAUSCHWERT FÜR BITCOIN	148
SICHERE AUFBEWAHRUNG VON BITCOINS	149
BESTANDSDIVERSIFIKATION	150
BITCOINS IN DER STEUERERKLÄRUNG	150
<u>KAPITEL 10 DAS DEEP- UND DARKNET</u>	<u>153</u>
DEEP-WEB	155
LEGALE INHALTE	155
DARKNET	156
WIE KOMME ICH REIN?	157
1. INSTALLATION TOR-BROWSER	157
2. KONFIGURATION TOR-BROWSER	158
SURFEN IM DARKNET	158
UND JETZT?	160
<u>KAPITEL 11 PANIC FAQ</u>	<u>161</u>
SIND BITCOINS SICHER?	161
WO KANN MAN SICH BEI BITCOIN ANMELDEN?	163
SIND BITCOINS VERBOTEN?	163
WIE VIEL IST EIN BITCOIN WERT?	163
UND WAS MACHST DU, WENN DU GEHACKT WIRST?	164

DIE WICHTIGSTEN VORTEILE VON BITCOIN	164
DIE NACHTEILE VON BITCOIN	166
ERKLÄRE MIR BITCOIN IN EINEM SATZ	167
<u>KAPITEL 12 QUELLEN</u>	168
KAPITEL 1 - DAS BITCOIN SYSTEM	168
KAPITEL 2 – WELCHEN WERT HABEN BITCOINS	168
KAPITEL 3 – BITCOIN ALS WERTANLAGE	168
KAPITEL 4 - BLOCKCHAIN	169
KAPITEL 5 – MINING	169
KAPITEL 6 – BITCOIN WALLET:	170
KAPITEL 7 – BITCOIN KAUFEN UND VERKAUFEN	170
KAPITEL 8 – MIT BITCOIN BEZAHLEN	170
KAPITEL 9 - BITCOIN AKZEPTANZ	170
KAPITEL 10 – DAS DEEP UND DARKNET.....	171

Vorwort

Hast du schon mal versucht, Geld in die USA zu überweisen? Wenn ja, dann hast du bestimmt ein längeres Formular für Auslandsüberweisungen bei deiner Bank ausfüllen müssen. Neben den Gebühren und den Wechselkurschwankungen kann es gut und gerne bis zu zwei Wochen dauern, bis das Geld auf dem entsprechenden Konto gelandet ist. Vor 50 Jahren war das sicherlich eine sehr zeitgemäße und schnelle Art Geld zu überweisen. Nun hat sich aber durch das Internet und die Digitalisierung einiges geändert, sodass sich die Frage stellt, ob die heutigen Bankdienstleistungen noch zeitgemäß sind. Zwar bietet heute jede Bank Online-Banking an und an den Finanzmärkten können ausgeklügelte Finanzderivate gehandelt werden, doch hat sich das Bankwesen als solches kaum verändert. Entsprechend groß ist der Innovationsstau, insbesondere was den Zahlungsverkehr anbelangt. Gleichzeitig sinkt das Vertrauen der Bevölkerung gegenüber den Banken und scheint sich auch mehrere Jahre nach Ausbruch der Finanzkrise von 2008 noch nicht erholt zu haben. Als Konsequenz versuchen viele Startups im Finanzwesen, sogenannte Fin-Techs, die Bankenbranche mit

neuen, innovativen Lösungen zu revolutionieren. Vorreiter sind hier die USA, wo immer weniger Überweisungen von Bankkonto zu Bankkonto erfolgen. Auch das Bezahlen mit Bargeld wird dort immer stärker aus dem Alltag verbannt. Aber nicht nur in den USA, sondern auch in vielen Ländern Europas, vor allem in den Niederlanden und den skandinavischen Ländern, ist das bargeldlose Bezahlen bereits populärer als in Deutschland.

Der Prozess der Digitalisierung lässt sich weder von Staaten noch von Banken aufhalten. Es ist daher nur eine Frage der Zeit, bis der durch die Digitalisierung hervorgerufene Strukturwandel den Zahlungsverkehr und andere Finanzdienstleistungen flächendeckend verändern wird. Im Zentrum dieser Evolution steht die digitale Währung Bitcoin. Bitcoin ist die bekannteste aller digitalen Währungen und verfügt über die am besten ausgebaute Infrastruktur – es gibt keine andere digitale Währung mit mehr Akzeptanzstellen als Bitcoin. Wie jede andere technische Innovation wird auch Bitcoin kontrovers von sämtlichen Akteuren diskutiert. So haben viele nationale Regierungen, Zentralbanken und die Europäische Union verschiedenste Positionspapiere zum Thema Bitcoin veröffentlicht. Oftmals geht es um den Vorwurf, dass Bitcoin

aufgrund seiner Anonymität kriminelle Geschäfte begünstige. Inwiefern das wirklich zutrifft, werden wir in diesem Buch noch kritisch hinterfragen. Daneben geht es vor allem um die Technologie, die hinter der Währung Bitcoin steht: die sogenannte Blockchain-Technologie, auf die wir später ebenfalls noch ausführlich eingehen.

Neben der Politik haben natürlich vor allem Unternehmen und insbesondere Banken ein großes Interesse, die Vorteile von Bitcoin und der dahinter stehenden Technologie Blockchain für sich zu nutzen. So haben sich bereits mehrere Banken zusammengetan, um digitale Währungen zu erforschen. Zusätzlich werden die Entwicklungen von den Universitäten vorangetrieben. An der Stanford University kann man beispielsweise den Studiengang „Bitcoin Engineering“ belegen.

Es bleibt festzuhalten: Auch wenn das Potenzial von Bitcoin noch längst nicht ausgeschöpft ist, ist die digitale Währung bereits im Mainstream angekommen. Umso wichtiger ist es, sich möglichst rechtzeitig über Bitcoin zu informieren, um die Chancen und Risiken einschätzen und nutzen zu können. Deshalb geben wir dir mit der Bitcoin-Bibel eine Anleitung an die Hand, mit der du lernst, alle wichtigen Vorgänge und Funktionen rund um Bitcoin

zu beherrschen.

Die Informationen in diesem Buch wurden mit größter Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Die Autoren übernehmen keine juristische Verantwortung oder irgendeine Haftung für eventuell verbliebene Fehler und deren Folgen.

Kapitel 1 Das Bitcoin-System

Was ist Bitcoin

Bevor wir uns mit der technischen Dimension von Bitcoin auseinandersetzen, macht es Sinn, erst einmal den Begriff Bitcoin zu erläutern. Bitcoin setzt sich aus dem Wort „Bit“ – der kleinsten Maßeinheit für eine Datenmenge – und dem Wort „Coin“, was im Englischen Münze bedeutet, zusammen. Entsprechend handelt es sich um digitale Münzen, die ein eigenes Währungssystem, wie Euro und US-Dollar, darstellen.

Im nächsten Schritt stellt sich die Frage, welche Eigenschaften Bitcoin zu einer Währung machen und ihnen einen Handelswert verleihen. Genau wie die von Staaten bzw. Notenbanken emittierten Währungen erfüllen auch Bitcoin alle Funktionen, die Geld per Definition erfüllen muss:

- 1) **Tauschfunktion** – z. B. Bitcoin gegen Schuhe und Schuhe gegen Bitcoin.
- 2) **Wertaufbewahrungsfunktion** – Das Versprechen, dass Bitcoin einen speicherbaren Gegenwert darstellt und sich zu einer anderen Zeit an einem anderen Ort einlösen

lässt.

3) **Rechenfunktion** – Bitcoin ist ein Wertmaßstab und kann in Preisen ausgedrückt werden, z. B. ein Paar Schuhe = 0,554 Bitcoin.

Das Erfüllen dieser Voraussetzungen erklärt allerdings noch nicht, warum Bitcoin einen realen Tauschwert besitzt und wir viele Euros oder Dollars bezahlen müssen, um im Gegenzug einen Bitcoin zu erhalten. Die Antwort ist die gleiche wie bei allen anderen staatlichen Währungen auch: Einzig und allein das Vertrauen in die Währung und die Erwartung, auch zukünftig Waren oder Dienstleistungen mit der Währung erwerben zu können, lassen den Bitcoin als eine werthaltige Währung erscheinen. Angebot und Nachfrage bestimmen den Bitcoin-Marktwert.

Ganz anders gestaltet sich die Struktur und Herausgabe von Bitcoin gegenüber den klassischen Währungen. Während Euro und Co. der zentralen Kontrolle einer Notenbank unterliegen, wird die Währung Bitcoin von keiner zentralen Institution gesteuert. Auch Staaten bzw. Regierungen haben praktisch keine Möglichkeit, Einfluss auf Bitcoin zu nehmen. Das entscheidende Merkmal von Bitcoin und der dahinterliegenden Technologie Blockchain

ist die dezentrale Struktur des Systems. Durch die Blockchain, die als digitales und dezentrales Transaktionsbuch fungiert, werden alle jemals getätigten Transaktionen aus dem Bitcoin-Netzwerk aufgezeichnet. Es bedarf also keiner zentralen Server, wie bei klassischen Geldüberweisungen, um Bitcoin-Transaktionen zu ermöglichen. Der Grund dafür liegt in den sogenannten Peer-to-Peer-Anwendungen, was bedeutet, dass alle Rechner gleichberechtigt ein Rechnernetzwerk darstellen. Demnach kann also auch jeder einfache Home-PC Teil des Bitcoin-Netzwerkes werden. Einen kompletten Zugang zum Netzwerk erhält man durch die Open-Source-Software Bitcoin-Core, die von den Teilnehmern genutzt wird, um die dezentrale Datenbank zu verwalten – im weiteren Verlauf des Buches wird geschildert, warum selbst das nicht unbedingt immer notwendig ist. Staaten, Notenbanken, Geschäftsbanken oder sonstige Unternehmen sind dafür nicht nötig.

Ein weiterer wichtiger Punkt und Unterschied zu den klassischen Währungen ist die Anonymität bzw. Pseudonymität von Bitcoin. Anstatt der Namen der Personen sind nur die jeweiligen Adressen, bestehend aus Zahlen und Buchstaben, einsehbar. Um Transaktionen im Bitcoin-Netzwerk durchzuführen, bedarf es im Gegensatz

zum Bankenzahlungsverkehr keiner Identitätsprüfung bzw. -offenlegung. Jeder, der über einen Internetzugang verfügt, kann sich eine Bitcoin-Adresse und ein Wallet (= digitale Brieftasche) zulegen, ohne dabei seine Identität preisgeben zu müssen.

Auch wenn sich das Ganze sehr unsicher und riskant anhört, sind Bitcoin-Transaktionen extrem sicher. Dafür sorgen kryptographische Techniken, die gewährleisten, dass nur der Eigentümer der Bitcoins Überweisungen vornehmen kann und die Geldeinheiten nicht mehrmals ausgegeben werden können. Aus diesem Grund wird die digitale Währung Bitcoin auch als Kryptowährung bezeichnet.

Politische Dimension und Regulierung

Das Potenzial struktureller Veränderungen durch Bitcoin und die Blockchain-Technologie ist aus politischer, gesellschaftlicher und ökonomischer Sicht enorm. Entsprechend kontrovers wird die Entwicklung digitaler Währungen von verschiedenen Akteuren diskutiert. Da wären zum einen die Staaten und Notenbanken, die die Geld- und Währungspolitik steuern und damit Kontrolle ausüben können. Ein dezentrales Zahlungssystem wie Bitcoin