DIE BLOCKCHAIN BIBEL

DNA einer revolutionären Technologie

Von den Autoren des Bestsellers „Die Bitcoin Bibel“

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

BTC-ECHO
Deutschsprachige Bitcoin-News

Die Blockchain Bibel

DNA einer evolutionären Technologie

BTC-ECHO

BTC-ECHO

Die Blockchain Bibel

DNA einer evolutionären Technologie

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

Impressum

BTC-ECHO
Mark Preuss
Albersallee 34
47533 Kleve
info@btc-echo.de

Tag der Veröffentlichung: 22.10.2016
www.btc-echo.de

Vorwort

Gemäß der Technologie-Analyse des Marktforschungsunternehmens Gartner, erlebt die Blockchain gerade einen Hype. Nicht wenige sehen in der Blockchain-Technologie als die bislang größte Erfindung seit dem Internet. Um den Wahrheitsgehalt dieser Aussage zu prüfen, werden wir uns im ersten Teil des Buches mit den Grundlagen dieser neuen Technologie befassen. Schritt für Schritt erklären wir das Konzept, das hinter der Blockchain steckt und gehen dabei auf die technischen und nicht-technischen Elemente ein. Nach den theoretischen Grundlagen zu Beginn des Buches, bilden praxisnahe Anwendungen den Schwerpunkt der Blockchain Bibel. Einige wenige Kapitel im Buch verlangen ein gewisses Grundlagenwissen im Bereich IT und IT-Programmierung, um die Thematik vollständig erfassen zu können. Diese Kapitel sind entsprechend gekennzeichnet. Damit möchten wir die Vielfalt der Blockchain-Einsatzmöglichkeiten aufzeigen. Das Spektrum reicht von wirtschaftlich-technischen bis hin zu sozialgesellschaftlichen Bereichen, die von der Blockchain-Technologie bedeutend beeinflusst werden. Den gegenwärtig größten Einfluss aber übt die Blockchain auf unser Finanzsystem aus. Entsprechend haben wir dem Themenbereich Blockchain und Finanzen ein eigenes Kapitel gewidmet.

Schließlich haben auch Unternehmen und vor allem Banken das Potenzial dieser neuen Technologie für sich entdeckt und versuchen mithilfe der Blockchain bestehende Geschäftsprozesse zu optimieren und neu zu erfinden. Es ist ein Wettlauf um das disruptive Potenzial der Blockchain ausgebrochen, da viele Geschäfts- und Tätigkeitsfelder durch die Blockchain automatisiert bzw. ersetzt werden können. Die Angst, dass sich innovative Startups die Blockchain zu Nutze machen und die beste-

henden Geschäftsstrukturen etablierter Unternehmen neu definieren, ist hoch. Aus diesem Grund wurden bereits enorme Investitionen (Stand Okt. 2016 rund 1,11 Mrd. US-Dollar) unternommen, um den Anschluss an die Blockchain-Technologie nicht zu verpassen.

Auch Staaten und politische Institutionen interessieren sich für die Blockchain. Genaue Details darüber, welche Länder, Unternehmen und Institutionen bereits an Blockchain-Lösungen arbeiten, erfahrt ihr im Verlauf des Buches.

Das Interesse wurde ursprünglich durch die digitale Währung Bitcoin, die wohl bekannteste Blockchain-Anwendung geweckt. Wie wir später noch ausführlich erläutern werden, stellen digitale Währungen und auch andere Blockchain-Anwendungen Behörden und Regierungen vor große Herausforderungen. Der Grund liegt in der Logik der Blockchain, die auf dem Prinzip der Dezentralität aufbaut. Die Möglichkeit dezentrale Strukturen zu nutzen und auf zentrale Akteure und Steuerungseinheiten zu verzichten macht die Blockchain zu einem vollkommen neuen und kaum greifbaren Phänomen. Entsprechend wird uns das Konzept der Dezentralität das gesamte Buch über begleiten.

Trotz erster konkreter Anwendungsmöglichkeiten, insbesondere im Finanzsektor, kann noch niemand genau abschätzen, in welchem Ausmaß die Blockchain unser Leben verändern wird. Eines ist aber sicher: theoretisch können alle Bereiche unseres Lebens von der Blockchain erfasst und beeinflusst werden. Umso wichtiger ist es, sich möglichst rechtzeitig über die Blockchain zu informieren, um die Chancen und Risiken einschätzen und nutzen zu können.

Ob die Blockchain nun die größte Erfindung seit dem

Internet ist, ist eine Frage die jeder Leser für sich selbst beantworten muss – die dafür notwendigen Informationen liefern wir mit diesem Buch.

Über die BTC-ECHO Redaktion

Wir sind die BTC-ECHO Redaktion und betreiben Deutschlands größtes Online-Magazin im Bereich Bitcoin und Blockchain (BTC-ECHO.de). Unser Team aus Redakteuren ist bunt gemischt, sodass es für jeden Fachbereich – egal ob IT, Wirtschaft oder Politik – mindestens einen Experten gibt. Aus diesem Grund werden wir in der Blockchain-Bibel auf das gesamte Spektrum der Blockchain eingehen.

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.

Zur besseren Lesbarkeit werden in diesem Buch personenbezogene Bezeichnungen, die sich zugleich auf Frauen und Männer beziehen, generell nur in der im Deutschen üblichen männlichen Form angeführt, also z. B. „Leser“ statt „LeserInnen“ oder „Leserinnen und Leser“. Dies soll jedoch keinesfalls eine Geschlechterdiskriminierung oder eine Verletzung des Gleichheitsgrundsatzes zum Ausdruck bringen.

Die BTC-ECHO Redaktion wünscht Dir eine interessante und spannende Lektüre!

KAPITEL 1 DIE BLOCKCHAIN

WAS IST DIE BLOCKCHAIN?

Das Internet hat bereits viele bedeutende Errungenschaften hervorgebracht, die unser heutiges Leben entscheidend prägen. Doch je stärker wir das Internet in unser Leben einbinden, desto öfter werden wir mit den Grenzen und Schwachstellen des Internet konfrontiert. Jedes Mal, wenn wir ein Rechtsgeschäft im Internet tätigen, sind wir auf die Hilfe von Drittanbietern bzw. zentralen Vermittlerstellen angewiesen. Schließlich ist es uns nicht möglich die Identität unseres Geschäftspartners zu überprüfen und sicherzustellen, dass sich dieser an die Geschäftsvereinbarungen hält. Im Internet können wir niemandem trauen, sodass wir Dritte, in Form von Banken, Treuhändern oder Plattformanbietern, hinzuschalten müssen. Diese Akteure kosten oftmals viel Geld und sammeln zusätzlich unsere persönlichen Daten, um diese dann für kommerzielle Zwecke weiterzunutzen.

Trotz dieser zentralen Vermittler hat sich die Sicherheitsinfrastruktur des Internets nur wenig weiterentwickelt und die Cyberkriminalität nimmt weiter zu, wie später im Kapitel „Einführung in die Kryptographie“ beschrieben wird. Korrespondierend dazu sammeln auch Staaten bzw. Sicherheitsbehörden immer öfter unsere privaten Daten. Gleichzeitig ist unsere Abhängigkeit von Unternehmen und Institutionen so hoch wie nie zuvor. Um die Möglichkeiten des Internets vollumfänglich zu nutzen, sind wir gezwungen, auf verschiedene Anbieter zurückzugreifen und deren Geschäftsbedingungen zu akzeptieren.

Egal ob wir uns in sozialen Netzwerken aufhalten, eine App auf unser Smartphone herunterladen oder eine geschäftliche Transaktion im Internet abwickeln – jedes Mal müssen wir den AGBs zustimmen und uns meist bereit erklären, unsere Daten weiterzugeben.

Entsprechend groß ist der Bedarf nach einer Netzwerkstruktur, der jeder, auch ohne das Zuschalten von Dritten, vertrauen kann. Diese neue Struktur muss ermöglichen, dass jeder Einzelne einsehen kann, ob es sich um wahrheitsgemäße Informationen, wie z. B. Eigentumsrechte, handelt, ohne dabei auf die vermeintliche Expertise eines Unternehmens oder einer Organisation zurückgreifen zu müssen. Was es braucht, ist eine Netzwerktechnologie, die den Menschen Unabhängigkeit zurückgibt und gleichzeitig eine neue Vertrauensbasis schafft.

Genau hier kommt die Blockchain-Technologie ins Spiel, da sie die oben beschriebenen Probleme und Schwachstellen beheben und uns alternative Nutzungsmöglichkeiten aufzeigen kann.

Mit der Blockchain hat man Zugang zu einer vollkommen neuartigen Netzwerk-Infrastruktur. Das wichtigste Merkmal dieser Infrastruktur ist die Dezentralität, die bedingt, dass die Steuerung und Verwaltung nicht durch eine zentrale Institution erfolgt. Entsprechend wird die Blockchain vom gesamten Netzwerk organisiert. Das Netzwerk wiederum setzt sich aus den Teilnehmern zusammen, die sich durch den Download der Software dem Netzwerk angeschlossen haben. Server, die von Unternehmen oder Institutionen an einem bestimmten Ort betrieben und zentral kontrolliert werden, sind damit nicht mehr nötig. Jeder einzelne Rechner, egal wo auf der Welt, stellt die Infrastruktur für das Netzwerk bereit. Durch dieses Funktionsprinzip wird die Notwendigkeit

einer vermittelnden dritten Instanz unnötig. Banken, Notare, zentrale Serverbetreiber und viele andere können dadurch überflüssig gemacht werden.

Neben der technischen Effizienz und potentiellen Kostenersparnis ist es daher vor allem die Unabhängigkeit von zentralen Akteuren und Instanzen wie Staaten, Notenbanken oder großen IT-Unternehmen, die den Reiz der Blockchain ausmacht. Dazu gehört auch die Vermeidung von Intransparenz. Dadurch, dass jede jemals getätigte Transaktion in der Blockchain aufgezeichnet wird und von jedem eingesehen werden kann, handelt es sich um ein sehr transparentes System. Aus diesen Gründen ist die Nutzung der Blockchain nicht nur aus technischer und ökonomischer Sicht relevant, sondern auch aus gesellschaftlicher und politischer.

GESCHICHTE DER BLOCKCHAIN

Als J. C. R. Licklider im August 1961 die ersten Gedanken zum „Galactic Network“ hatte, die später die Entwicklung des Internets vorangetrieben haben, ahnte der Forscher am MIT höchstwahrscheinlich noch nicht, welchen großen Einfluss diese Technologien auf die Weltgeschichte haben würden. Seine Vision, verschiedene Geräte auf der ganzen Welt miteinander zu vernetzen und aus der Ferne auf Daten und Programme zuzugreifen, war die erste dieser Art. Die Welt, in der wir heute leben, wäre zum damaligen Zeitpunkt nicht vorstellbar gewesen.

Maschinen waren einzelne Geräte, die ihre Aufgaben verrichteten. Basierend auf der Mathematik befolgten sie, was ihnen in Form von Programmen auferlegt wurde. Allein die Idee, Maschinen gegenseitig voneinander abhängig zu machen und über das Internet eine Kommu-

nikation zu ermöglichen, lag damals nicht in unserer Vorstellungskraft.

Im Nachhinein betrachtet ist der technische Fortschritt, der sich seitdem im Bereich des Internets gezeigt hat, nahezu unglaublich. Im Jahr 1964 untersuchte der Informatiker Paul Baran auf Anfrage der US Air Force für die RAND Corporation, wie sich Kommunikationsnetzwerke gegen einen Nuklearangriff sichern lassen. Seine Forschungen (veröffentlicht in „On Distributed Communications“) ergaben, dass dezentrale Netzwerke am besten gegen Ausfall gesichert sind. Darauf folgten Licklider und andere Forscher mit weiteren Versionen. So entwickelte man im Jahr 1969 das *Advanced Research Project Agency* (ARPA). Es war vornehmlich für Forschungszwecke gedacht und sollte das Problem der stark begrenzten Rechenkapazitäten an Universitäten lösen, indem man viele Ressourcen miteinander verknüpft, die physisch nicht direkt verbunden sind.

ARPA war für Menschen, die nicht in diesen Forschungsfeldern aktiv waren, keine technologische Revolution, die sie merklich spüren konnten. Schließlich war die Anwendung rein auf die Forschung beschränkt und eine private Nutzung aufgrund des hohen Aufwands zunächst undenkbar.

Die wichtigsten Kommunikationsmechanismen des Internets, die wir noch heute nutzen, gingen allerdings aus ARPA hervor. Im Jahr 1981 spezifizierte man unter anderem IPv4 und TCP. Das System der IP-Adressen IPv4 hielt sich bis 1998, als die neue Version IPv6 standardisiert wurde. Der erste wirkliche Anstieg der IPv6-Nutzung begann im Jahr 2013. Letztlich nutzen wir nach wie vor oft IPv4 und damit eine Technologie, die bereits im Jahr 1981 entwickelt wurde. Eine Langlebigkeit, die man dem Internet nur selten unterstellt.

Nachdem die grundlegenden Protokolle spezifiziert und entwickelt wurden, legte man den technischen Grundstein des Internets. Die Vision, dass Geräte drahtlos miteinander kommunizieren können, rückte immer näher: In den 2000er Jahren wurde das Internet zum Endprodukt für jedermann. Kleine Schwierigkeiten machten die Verbreitung der Technologie, die für viele Menschen zunächst unverständlich klang, etwas mühsam. Dennoch entwickelte sich das Internet mit einer unglaublichen Geschwindigkeit, sodass es heute längst zum Alltag gehört.

Was einst ein technisches Experiment war, von dem nur wenige wussten, ist heute eine allgegenwärtige Technologie. Sie krempelte die Arbeitsweise auf der gesamten Welt um. Das Internet trägt seinen Teil dazu bei, dass alle stetigen und kontinuierlichen Tätigkeiten automatisiert mit einer wesentlich geringeren Manpower durchgeführt werden können. Die reine Bereitstellung von Informationen bedarf nicht mehr eines physischen Weges wie bspw. der Post. Statt mehrere Tage auf die Zustellung zu hoffen, können Daten binnen Sekunden oder sogar in Bruchteilen von Sekunden ausgetauscht werden. Der Einfluss auf wirtschaftliche Prozesse ist gewaltig: McKinsey geht von einem Wachstum des Bruttosozialprodukts durch das Internet um 21 % in den Jahren 2006–2011 aus.

Man hat die Welt der Informationen zu einem liberalen Raum entwickelt. Sie sind nicht mehr nur der Oberschicht oder Forschern zugänglich, sondern jedem Menschen – und das in vielen Fällen sogar kostenlos. Kostenlose WiFi-Zugänge sollen in allen europäischen Städten verfügbar gemacht werden. Im Jahr 2020 soll dann noch das ultraschnelle Mobilfunknetz 5G gestartet werden.

Auch wenn es oft nicht so wahrgenommen bzw. von großen Medienportalen skizziert wird, bedeutet das Internet für uns vor allem eins: Wissen.

Wir strukturieren unsere Zusammenarbeit nicht mehr nur nach physischen Verfügbarkeiten und Mitarbeitern, die im selben Büro sitzen, sondern auch nach inhaltlicher Relevanz. Wir suchen lieber in einer Datenbank, auf die nahezu jeder Mensch Zugriff hat, eine Antwort auf unsere Frage, statt der Ideologie zu folgen, dass wir alles wissen müssen.

Wir spezialisieren uns, weil unser Beitrag in der Wirtschaft und Forschung besser ineinandergreifen kann. Wir müssen keine rudimentären Ergebnisse in einer großen Bandbreite liefern, sondern konkrete Feststellungen in sehr speziellen Teilgebieten. Wir können sie anschließend mit denen von anderen Experten vereinbaren, um gemeinsam eine stärkere Lösung zu entwickeln.

Die politischen, wirtschaftlichen und gesellschaftlichen Auswirkungen des Internets sind unglaublich und kaum unterzubringen, ohne den Rahmen dieses Buches zu sprengen. Wie aber können wir die Blockchain in der heutigen Zeit einordnen?

Stehen wir vor einer neuen Revolution in der Weltgeschichte, oder betrachten wir ein unter IT-affinen Menschen interessantes Produkt, das es nicht über die Entwicklung hinaus in die Verbreitung schafft?

DIE ANFÄNGE DER BLOCKCHAIN: UNVERHOFFTE VISIONEN

Geldtransaktionen funktionieren heute schneller als früher, was zunächst nicht sonderlich überraschend klingen dürfte. Schließlich stellen wir mittlerweile eine automa-