Elfriede Sixt

Bitcoins und andere dezentrale Transaktionssysteme

Blockchains als Basis einer Kryptoökonomie

Springer Gabler

Bitcoins und andere dezentrale Transaktionssysteme

Elfriede Sixt

Bitcoins und andere dezentrale Transaktionssysteme

Blockchains als Basis einer Kryptoökonomie

Springer Gabler

Elfriede Sixt
Wien, Österreich

ISBN 978-3-658-02843-5 ISBN 978-3-658-02844-2 (eBook)
DOI 10.1007/978-3-658-02844-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Gabler

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Gabler ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer Fachmedien Wiesbaden GmbH

Vorwort

> In the future I see a public Blockchain – whether that's Bitcoin or some other open one in the future which is a way of registering ownership of all sorts of assets and it's a way of transferring ownership of those assets in a single system that can be read by all of the right people and none of the wrong people. So it becomes very simple for me to swap my dollars for your IBM shares, or your pounds for my house. Any asset that we assign a value to and want to be sure about who owns it can be registered using this technology. (James Smith, CEO of Elliptic)[1]

Stellen Sie sich vor, Sie wachen an einem Sonntagmorgen irgendwann in der nahen Zukunft auf. Das Wetter ist traumhaft und Sie beschließen, sich mit Ihren Freunden auf einen Brunch zu treffen. Sie schnappen sich Ihr Smartphone und öffnen Ihren persönlichen Lifestyle-Assistenten. Das ist eine App, die Ihr Nutzungsverhalten kennt und Sie in Ihren Entscheidungen des täglichen Lebens unterstützt. Ohne einen derartigen Lifestyle-Assistenten ließe sich das Leben in dieser nahen und vollständig digitalisierten Zukunft auch nicht bewältigen.

Wie heute bereits durch die Software Siri (Abkürzung für: Speech Interpretation and Recognition Interface) von Apple® kann man mit der Lifestyle-App mündlich kommunizieren. Sie beauftragen Ihren Lifestyle-Assistenten also, ein geeignetes Lokal für den Brunch auszusuchen und den Zeitpunkt für den Brunch auch gleich mit den Lifestyle-Assistenten Ihrer Freunde abzustimmen. Das Lokal ist schnell ausgewählt, die kommunizierenden Lifestyle-Assistenten haben auch rasch den optimalen Zeitpunkt dafür abgestimmt.

Ihr Lifestyle-Assistent bestellt also einen Tisch für fünf Personen, zahlt sofort per Kryptowährung die Reservierungsgebühr und Sie erhalten umgehend den Online-Voucher. Dieser enthält auch eine Gutschrift für einen vollautomatischen Car-Service. Mittlerweile ist der Straßenverkehr durch selbst fahrende Autos geprägt, die nach dem Prinzip des Carsharings funktionieren. Im Stadtbereich befindet sich das nächste Auto üblicherweise nur rund 100 bis 150 m vom eigenen Standort entfernt.

[1] Top five Quotes from Bitcoin Experts on Banks Building Blockchains, http://cointelegraph.com/news/115395/top-5-quotes-Bitcoin-expert-quotes-on-banks-building-blockchains?ref=45 (Abruf: 11.10.2015).

Die Autos werden über das Internet und entsprechende Applikationen und Leitsysteme gesteuert.

Ihr Lifestyle-Assistent erkundigt sich nun bei Ihnen, ob Sie den Voucher einlösen und einen Car-Service bestellen wollen. „Natürlich“, sagen Sie. Also wird das passende Angebot ausgewählt und bestellt. Die Bestätigung der Einlösung des Vouchers samt exaktem Standort Ihres Autos wird auf Ihr Smartphone gesandt. Das für Sie bereitgestellte Auto befindet sich nur knapp 30 m von Ihrem Hauseingang entfernt. Mit dem digitalen Voucher auf Ihrem Smartphone öffnen sich die Türen des Autos automatisch, sobald Sie sich dem Auto auf einen Meter genähert haben. Da das Fahrtziel vorab bekannt gegeben wurde, müssen Sie nach dem Einsteigen nichts mehr tun. Denn jedes dieser Autos verfügt über die jeweils aktuellste Kommunikationstechnologie. Da diese intelligenten Autos so gut wie keine Unfälle verursachen, brauchen sie auch keinen Sicherheitsgurt und alle Sitze sind zur Mitte des Autos hin ausgerichtet.

Im Auto haben Sie Zeit, schnell die wichtigsten Schlagzeilen in den für sie interessanten Onlinemedien bei einer Tasse Kaffee zu lesen. Danach erledigen Sie noch ein paar kurze Postings auf Facebook. Für jedes Like oder jeden Kommentar zu einem Posting bekommen Sie von Facebook ein paar Coins in eines ihrer digitalen Wallets gutgeschrieben. Da Sie viele Freunde auf Facebook haben und fleißig posten, reicht das Einkommen von Facebook üblicherweise aus, um Ihre monatlichen Kosten für die Nutzung des Internets zu bezahlen.

Die Tür Ihrer Wohnung hat sich hinter Ihnen geschlossen, sobald sie den Hauseingang verlassen haben. Die Tür zu Ihrem Heim kann nur von Personen geöffnet werden, die im Besitz eines speziellen Krypto-Tokens sind, der von Ihnen unter Nutzung kryptografischer Verschlüsselung auf die Smartphones der einzelnen Personen übertragen wurde.

So gut wie alle Dinge des täglichen Lebens, von Ihrem Toaster bis zu Ihrer Waschmaschine, sind intelligente Dinge, ausgestattet mit Mikroprozessoren und untereinander vernetzt. Nutzung und Verwaltung erfolgt über sogenannte Smart Contracts. Es erfolgt ein ständiges Abgleichen, Speichern und Weitergeben der Daten zwischen den Geräten. Die Geräte können Remote kontrolliert werden. Viele Haushaltsgeräte sind geleast, die Verwaltung dieser Leasingverträge erfolgt ebenfalls mittels intelligenter Verträge. Nehmen wir als Beispiel die Kaffeemaschine. Für jede zubereitete Kaffeetasse wird dem Verleiher digitalisiert und vorprogrammiert in dem entsprechenden Smart Contract die Nutzungsgebühr gutgeschrieben (auf sein Wallet) und eines ihrer Wallets entsprechend belastet. Ähnlich funktionieren Ihre Waschmaschine, Ihr TV-Gerät, Ihr Computer und natürlich Ihr 3D-Drucker. Der 3D-Drucker ist so gut wie unverzichtbar für Haushalt und Büro. Kleine Dinge des täglichen Lebens werden in Realtime vom 3D-Drucker erzeugt. Auch die Nutzung und Anbindung von Strom, Gas und Wasser wird von Smart Contracts verwaltet und per Kryptowährung bezahlt.

Sie zahlen für fast alle Dinge des Lebens nutzungsabhängig und in Realtime. Durch Nutzung von Kryptotransaktionssystemen ist die Bezahlung solcher Klein- und Kleinstbeträge keine Herausforderung mehr. Die Algorithmen der genutzten Smart Contracts steuern die mit ihnen verbundenen Dinge automatisch, sorgen im Bedarfsfall – wie bei

der Kaffeemaschine – für Nachschub und stellen, falls keine Zahlung erfolgt, die Nutzungsmöglichkeit ein. Dafür braucht es keine Menschen mehr. Das *Internet der Dinge* funktioniert von Maschine zu Maschine.

All das ermöglicht es Ihnen, auf Ihrem Weg zum Brunch die Waschmaschine – bei Bedarf – remote ein- und auszuschalten.

Ohne auf die Vor- bzw. Nachteile dieses nach Science Fiction klingenden Szenarios einzugehen, sollte uns klar sein, dass dieses bereits innerhalb weniger Jahre Realität werden könnte. Gemäß einer Gartner-Studie wird das Internet of Things (IoT) 2020 bereits 21 Mrd. Geräte und ein Wirtschaftsvolumen von 3 Mrd. US-Dollar umfassen.[2]

Für die Umsetzung von IoT und intelligenten Verträgen (Smart Contracts) ist die Sicherheit der IT-Systeme eine der am meisten noch diskutierten Herausforderungen.

Dieses Thema der Sicherheit kann nun mit dem Konzept der dezentralen kryptografisch verschlüsselten Transaktionssysteme vielversprechend adressiert werden: Die Bitcoin Blockchain hat inzwischen bewiesen, dass Werte jeglichen Ausmaßes auf einer Blockchain sicher zugeordnet und transferiert werden können.

Doch auch wenn die Bank von England Bitcoin bereits als Internet des Geldes[3] bezeichnet, und die Federal Reserve Bank von St. Louis Bitcoin als *Geniestreich*[4] betrachtet, stehen die heutigen Kryptowährungs- bzw. Kryptotransaktionssysteme in ihrer Entwicklung erst dort, wo das World Wide Web in den frühen 90er Jahren war.

Da es sich bei den Kryptowährungstechnologien jedoch meist um Open-Source-Technologien handelt, haben die weltweit intelligentesten und kreativsten Softwareentwickler nun offene Plattformen, auf denen sie Produkt- und Dienstleistungsansätze weiterentwickeln, die es Einzelpersonen, Organisationen und sogar Maschinen ermöglichen werden, Transaktionen flexibler, effizienter und produktiver auszuführen.

So wie im frühen Web der 90er Jahre niemand Entwicklungen und Phänomene wie YouTube und Facebook vorhersehen konnte, entstehen derzeit unzählige Anwendungen, in denen diese neuen Formen der Kryptotechnologie auf unvorhergesehene Weise genützt werden.

Noch betonen all die Befürworter der dezentralen Datenbanken aus dem Finanzbereich, dass sie nur die Idee der Blockchain an sich befürworten, aber von *bitcoin* als Zahlungsmittel und auch von der genutzten Geldschöpfungsform (dem Miningprozess) nichts halten bzw. von der Nutzung abraten. Und doch ist der momentane Hype um die Vorteile der dezentralen Datenbanken auch bei den Finanzinstituten der erste Schritt, sich mit den Kryptowährungstechnologien auseinanderzusetzen und ihre archaischen Backend-Systeme mit all ihren schwerfälligen Verzögerungen und unnötigen Kosten abzulösen. Und

[2] http://www.gartner.com/newsroom/id/3165317, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015 (Abruf: 20.02.2015).

[3] Innovations in payment technologies and the emergence of digital currencies, http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesBitcoin1.pdf (Abruf: 12.10.2015).

[4] https://www.stlouisfed.org/Dialogue-with-the-Fed/The-Possibilities-and-the-Pitfalls-of-Virtual-Currencies/Videos/Part-1-Introduction-and-Welcoming-Remarks (Abruf: 12.10.2015).

dann wird es viel einfacher sein, zu verstehen, dass es am Ende des Tages wohl Blockchains mit/und ohne Kryptowährungen geben wird und die Ansätze jetzt nur der erste Schritt sein können in eine neue Welt mit vielen Möglichkeiten. Diese Zeit werden die Kryptowährungstechnologien ohnehin noch brauchen, um ihre eindeutig gegebenen Unzulänglichkeiten auszumerzen.

Festzuhalten ist vorweg noch, dass sich die gesamte Kryptotechnologieindustrie momentan in einem massiven Innovationsprozess befindet. Konzepte, Terminologien, Standards, Parameter ändern sich ständig. Vielleicht gibt es die Bitcoin-Kryptowährungstechnologie in der in diesem Buch beschriebenen Form in fünf Jahren nicht mehr. Der Zweck des Buches ist es, einen umfassenden Einblick in den momentanen Stand der Idee und Systematik dieser angedachten Basis einer Kryptoökonomie zu geben und das mögliche Potenzial aufzuzeigen.

Wien/Österreich, im Frühjahr 2016 Elfriede Sixt

Vorbemerkung

Bitcoin und bitcoin – **Bitcoin** mit einem großen B steht für das Peer-to-Peer-Netzwerk, für die Open-Source-Software, für das dezentrale Hauptbuch (Blockchain), für die Software Entwicklungsplattform sowie für die Transaktionsplattform. **bitcoin** geschrieben mit dem Kleinbuchstaben b meint die Einheit der Kryptowährung.

Inhaltsverzeichnis

Kryptoökonomie

1

> The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A. That kind of thing will develop on the Internet and that will make it even easier for people to use the internet. (Milton Friedman, 1999)

Nur acht Jahre nach dieser wohl prophetisch anmutenden Aussage von Milton Friedman, veröffentlichte am 31. Oktober 2008, 14:10 Uhr Ortszeit, New York ein Kryptograf unter dem Pseudonym Satoshi Nakamoto ein Diskussionspapier mit dem Titel Bitcoin:[1] *A Peer-to-Peer Electronic Cash System*. In einer E-Mail an einige Kryptografieexperten und -interessierte weist er auf dieses Diskussionspapier hin und schreibt:

> Ich habe an einem neuen elektronischen Zahlungssystem gearbeitet, das vollständig auf gleichberechtigten Rechner-zu-Rechner-Verbindungen beruht und keinen vertrauenswürdigen Dritten erfordert.[2]

Bei dem von Sathosi Nakomoto vorgestellten Open-Source basierten Bitcoin-Protokoll handelte es sich vereinfacht um ein Gefüge grundlegender Programmieranweisungen, die es Computern erlaubt, miteinander zu kommunizieren. Die dabei vorgesehene Verschlüsselung erlaubt es den Nutzern, ihr Passwort einzugeben und einander direkt digitale Werte zu schicken, ohne eine dritte Person oder Institution involvieren zu müssen. Der im Protokoll vorgesehene Konsens-Algorithmus bestimmt, welche Schritte die Computer im Netzwerk ausführen müssen, um zu einem Konsens bezüglich der Gültigkeit jeder einzelnen Transaktion zu gelangen. Wird dieser Konsens erzielt, wird unwiderlegbar, un-

[1] Bitcoin und *Bitcoin* – **Bitcoin** mit einem großen B steht für das Peer-to-Peer-Netzwerk, für die Open- Source-Software, für das dezentrale Hauptbuch (Blockchain), für die Software Entwicklungsplattform sowie für die Transaktionsplattform. ***Bitcoin*** geschrieben mit dem Kleinbuchstaben b ist die Einheit der Kryptowährung.

[2] Cryptocurrency: Wie virtuelles Geld unsere Gesellschaft verändert, Michael Casey, Paul Vigna, deutschsprachige Ausgabe, Ullstein Buchverlage GmbH, Berlin 2015.

E. Sixt, *Bitcoins und andere dezentrale Transaktionssysteme*,
DOI 10.1007/978-3-658-02844-2_1

korrumpierbar und für jeden nachvollziehbar eindeutig der Besitz der digitalen Werte zugeordnet.

Dieses von Satoshi Nakamoto im E-Mail vom 31. Oktober 2008 beschriebene Konzept eines neuen Transaktionssystems und die dahinter liegenden Technologieansätze haben sich in den letzten Jahren zu einem immer größer werdenden Phänomen entwickelt.

Mittels der Architektur solcher Kryptotransaktionssysteme kann das Vertrauensproblem, das vielen wirtschaftlichen Geschäftsprozessen inhärent ist und bis dato durch die Involvierung einer Heerschar entsprechender Intermediäre (beispielsweise Banken, Notare, Rechtsanwälte usw.) adressiert wurde, nun mittels kryptografischer Algorithmen gelöst werden.

Ein Phänomen, das eine Revolution in vielen Bereichen unserer Wirtschaftssysteme hervorrufen wird. Es wird von der Entstehung einer Kryptoökonomie gesprochen, deren Herzstück dezentrale und fälschungssichere Datenbanken sind und deren Wertschöpfung auf kryptotechnologischen Abläufen (Algorithmen) basiert. Die Nutzung dieser dezentralen Transaktionssysteme als elektronische Zahlungsabwicklungssysteme bildet dabei nur die Speerspitze dieser Kryptoökonomie.

Die immensen Erwartungen, die an den Erfolg der Kryptotransaktionssysteme gestellt werden, lassen sich am besten anhand der Entwicklung des Wechselkurses und der Marktkapitalisierung der ersten und wohl auch bekanntesten Kryptowährung, den bitcoins, zeigen (vgl. Abb. 1.1).

Im Juli 2010 wurden bitcoins erstmals über die Bitcoin-Börse Mt. Gox zu einem Kurs von 0,06 US-Dollar pro bitcoin gehandelt. Der Gesamtwert aller bitcoins betrug damals 277.000 US-Dollar. Im Februar 2011 erreichte der Wert eines bitcoins den Wert eines US-Dollars. Zwei Jahre später durchbrach der Kurs die Barriere von 25 US-Dollar und begann massiv zu steigen. Am 29. November 2013 erreichte der bitcoin den bis dato höchsten Wert mit 1242 US-Dollar und einer Marktkapitalisierung von rund 13,5 Mrd. US-Dollar. Inzwischen, nach dem medienwirksamen Kollaps der Mt. Gox-Börse, massiven und an-

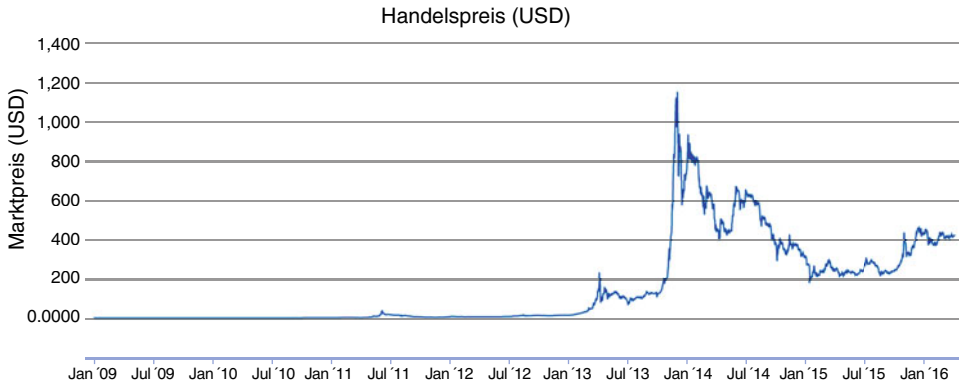

Abb. 1.1 Kursentwicklung des bitcoin über die letzten Jahre. (Quelle: blockchain.info)

dauernden Hackerangriffen und auch politischen Aussagen gegen den Bitcoin, beträgt der Wert des bitcoins 247,78 US-Dollar[3] mit einer Marktkapitalisierung von 3,6 Mrd. US-Dollar.[4]

Heute werden täglich mehr als 200.000[5] Bitcoin-Transaktionen mit einem Gesamtvolumen bis 100 Mio. US-Dollar ausgeführt und Unternehmen, wie Microsoft®, Dell® und Overstocks akzeptieren bitcoins als Zahlungsmittel. Das Bitcoin-Mining-Netzwerk, das die Integrität der dezentralen Datenbanken sicherstellt, umfasst schon heute eine Rechenleistung, die 300-mal so groß ist wie diejenige der 500 leistungsstärksten Supercomputer zusammen.[6]

Das Bitcoin-Transaktionssystem ist dabei lediglich das Fundament, auf dem weitere Werkzeuge für die Gestaltung wirtschaftlicher Beziehungen entwickelt werden können. Da dieses *vom Vertrauen einzelner* unabhängige System eine verifizierbare, transparente Besitz-/Inhaberschaftsbestätigung beinhaltet, die keine zentralisierte Registrierung erfordert, wird es Menschen in die Lage versetzen, unterschiedlichste digitalisierte Werteinheiten mit der Gewissheit auszutauschen, dass die Angaben zu den rechtlichen Verhältnissen korrekt sind.

Das Entstehen einer Kryptoökonomie, manchmal auch Trusted Web[7] genannt, ist dabei bedingt abhängig vom Grad der persönlichen Akzeptanz und Nutzung von Kryptowährungen wie *bitcoins*[8] und geht auch bei Weitem über die Ablösung der Nutzung der archaischen Backend-Systeme der Finanzdienstleistungsunternehmen durch dezentrale Datenbanken hinaus. Diese Kryptoökonomie wird vor allem durch die Nutzung dezentral arbeitender Datenbanken und den darauf aufsetzenden intelligenten Verträgen entstehen.

Getrieben auch durch neue sozioökonomische Entwicklungen (z. B. allgemeine Zunahme der Peer-to-Peer Transaktionen) wird die Nutzung der Architekturen der Kryptotransaktionssysteme neue effizientere Geschäftsmodelle und neue Wertschöpfungsquellen entstehen lassen.[9] Beispiele hierfür sind:

---

[3] http://www.coindesk.com/ (Abruf: 11.10.2015).

[4] https://blockchain.info/de/charts/market-cap (Abruf: 11.10.2015).

[5] www.blockchain.info (Abruf: 07.04.2016)

[6] The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy, David Garcia, Claudio J. Tessone, Pavlin Mavrodiev, Nicolas Perony. Published 6 August 2014, DOI: 10.1098/rsif.2014.0623, http://rsif.royalsocietypublishing.org/content/11/99/20140623 (Abruf: 11.12.2015).

[7] Netz des Vertrauens bzw. Web of Trust (WOT) ist in der Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen), kombiniert mit dem individuell zugewiesenen Vertrauen in die Bestätigungen der anderen („Owner Trust"), zu sichern. Es stellt eine dezentrale Alternative zum hierarchischen PKI-System dar, entnommen aus Wikipedia, https://de.wikipedia.org/wiki/Web_of_Trust (Abruf: 30.06.2015).

[8] http://www.ofnumbers.com/the-guide/ (Abruf: 30.06.2015).

[9] How The Cryptoeconomy Will Be Created, geschrieben von William Mougayar, erschienen im Onlinemagazin Forbes am 20.01.2015 http://www.forbes.com/sites/valleyvoices/2015/01/20/how-the-cryptoconomy-will-be-created/ (Abruf: 30.06.2015).

1. Zertifizierungs- und Verifizierungsdienstleistungen, wie Bestätigungen über bestehende Mitgliedschaften, Eigentumsverhältnisse, Stimmrechte usw., können mittels der dezentralen (und implizit mit einem Zeitstempel versehenen) Netzwerke zu geringen Kosten erbracht werden.
2. Die Erfassung und Verwaltung intelligenter Verträge kann zur Gänze über diese dezentralen Datenbanken erfolgen: Warum einen Dritten involvieren, wenn die Vertragsparteien sich auf die Vertragsbedingungen einigen können und eine entsprechende Softwareprogrammierung in den Transaktionssystemen vornehmen können?
3. Dezentrale Peer-to-Peer-Marktplätze werden Weiterentwicklungen heute erfolgreicher Marktplätze, wie UBER, eBay und Amazon, darstellen. Auf einem dezentralen Peer-to-Peer-Marktplatz kann jeder verkaufen und jeder kaufen. Die dezentralen Netzwerke agieren dabei als dezentrale virtuelle Kontrollapparate, gesteuert durch einen unbeeinflussbaren Algorithmus, durch den die Einhaltung der Regeln, die Identitäten sowie die erfolgten Wertetransfers überprüft werden.
4. Verteilte anonyme Organisationen (DAO) oder auch verteilte anonyme Gesellschaften (DAC), deren Geschäftstätigkeit ausschließlich über dezentrale Netzwerke abgewickelt wird. Jedes Mitglied dieser rein digitalen Organisationsformen kann auch ein Mitarbeiter der DAO/DAC sein und mittels ihrer gemeinsamen Aktionen und Aktivitäten tragen sie zum steigenden Wert der DAO/DAC bei. Nutzer können beispielsweise durch Zurverfügungstellung ihrer Rechnerleistung oder auch Speicherkapazität einen Betrag zur gemeinsamen Unternehmung leisten. Eine selbst geschaffene Kryptowährung könnte (muss aber nicht) dabei der Energieträger sein, der das Tausch- und Zahlungsmittel im System darstellt. Die Berichterstattung (Reporting) der Organisationen erfolgt für die einzelnen Mitglieder transparent einsehbar in einer gemeinsamen dezentralen Datenbank. Geschäftsmodelle ebenso wie Geschäftsregeln sind in Algorithmen festgeschrieben und können nur durch gemeinsamen Konsens geändert werden.

Die damit einhergehende Änderung der Wirtschaftsabläufe wird – so die Annahmen – zu einer Auflösung der gegebenen Machtstrukturen führen.

Die Kryptoökonomie hat damit das Potenzial, die Art, wie wir Unternehmen betreiben, wie Regierungen und auch die verschiedenen Kulturen funktionieren, massiv umzugestalten, wahrscheinlich viel mehr, als es das Internet vor 20 Jahren getan hat.

Was sind Kryptotransaktionssysteme? 2

> We could envisage proposals in the near future for issuers of electronic payment obligations, such as stored value cards or digital cash, to set up specialized issuing corporations with strong balance sheets and public credit ratings. (Alan Greenspan 2006)

Zusammengefasst nutzen Kryptotransaktionssysteme den hohen technischen Fortschritt auf dem Gebiet der asymmetrischen Kryptologie, um Transaktionen verschlüsselt durchzuführen und in einer transparenten, nachvollziehbaren und fälschungssicheren Datenbank (Blockchain oder Cryptoledger genannt) zu erfassen. Sowohl die Durchführung als auch die Erfassung der Transaktionen in der Datenbank erfolgt dabei zur Gänze in einem (dezentralen) Peer-to-Peer-Netzwerk, dessen Algorithmus auf einem Konsensus-Mechanismus basiert.

Der derzeit bekannteste Vertreter dieser Technologien ist das Bitcoin-Protokoll, dessen erster Client (Version 0.1) als Open-Source im Januar 2009 von Satoshi Nakamoto[1] veröffentlicht wurde.

2.1 Hintergrund und philosophische Betrachtung

> Privatsphäre ist ein Recht wie jedes andere. Man muss es in Anspruch nehmen oder man riskiert es, zu verlieren. (Phil Zimmermann)[2]

[1] Die Identität vom Bitcoin-Entwickler Satoshi Nakamoto ist unbekannt. Wobei auch nicht geklärt ist, ob es sich bei Satoshi Nakamoto um eine Einzelperson oder um eine Gruppe von Personen handelt. Laut den vorliegenden Aufzeichnungen (Forenpostings usw.) hat Satoshi Nakamoto bereits 2007 begonnen, am Design und am Code des Bitcoin-Protokolls zu arbeiten. Sein letztes dokumentiertes Posting in einem der Bitcoin-Foren stammt aus Dezember 2010.

[2] https://de.wikipedia.org/wiki/Phil_Zimmermann; Philip R. Zimmermann (* 12. Februar 1954 in Camden, New Jersey) ist der Erfinder der E-Mail-Verschlüsselungssoftware Pretty Good Privacy (PGP). Er hat einen B.S.-Abschluss für Informatik an der Florida Atlantic University (Abruf: 01.01.2016).

E. Sixt, *Bitcoins und andere dezentrale Transaktionssysteme*,
DOI 10.1007/978-3-658-02844-2_2

Die ersten Überlegungen zur Notwendigkeit und Nutzung von Kryptografie in neuen digitalen Geld- und Währungssystemen gab es bereits vor mehr als 25 Jahren ausgehend von den Cypherpunks, einer Gruppe von Datenschutzaktivsten. Bereits zu Beginn der 90er Jahre arbeitete diese Online-Commmunity an einem digitalen Zahlungsmittel, dessen Anonymitätsgrad der Anonymität von Bargeldzahlungen entsprechen sollte.

Die Cypherpunks erkannten bereits damals, dass durch die zunehmende Digitalisierung der Schutz der Privatsphäre im Web eine Herausforderung werden würde. Dies war lange, bevor mit Hilfe von Edward Snowden im Jahre 2013[3] Details über das tatsächliche Ausmaß der Spionageprogramme der National Security Agency (NSA) bekannt wurden.

Seit ihren Anfängen im alten Ägypten liegt das Wesen der Kryptografie in der Kunst, Botschaften zu verschlüsseln, um Nachrichten geheim zu halten. Kryptografie im informationstechnologischen Sinne beschäftigt sich mit den Konzepten und Implementierungen von Systemen, die für den Schutz persönlicher, betrieblicher und behördlicher Daten in Computersystemen zuständig sind.

Die Cypherpunks sehen die Notwendigkeit eines erhöhten Schutzes der Privatsphäre im digitalen Zeitalter, um eine offene Gesellschaft aufrechtzuerhalten und entwickeln dementsprechend Instrumente, mit denen die Internetbenutzer ihre Anonymität erhalten können. Gleichzeitig soll der Einflussbereich und die Macht der großen, zentralen Institutionen auf die Menschen eingeschränkt werden.

Das elektronische Geld, an dem die Kryptografen seit 1993 arbeiteten, sollte all jene Merkmale aufweisen, die notwendig waren, um es zu richtigem „Geld“ zu machen: Es sollte haltbar, übertragbar, teilbar und nur beschränkt verfügbar sein.

Folgende wesentliche Konzepte und Technologien, die sich teilweise in der Folge auch in der Bitcoin-Architektur wiederfinden, wurden diskutiert:

- Die Freeware-E-Mail-Verschlüsselungssoftware Pretty Good Privacy (PGP) wurde 1991 vom Kryptografen Phil Zimmermann veröffentlicht[4].
- Bereits 1989 wurde das Unternehmen DigiCash, vom bekannten Kryptografen David Chaum, gegründet. Chaum bezeichnete den von ihm konzipierten Wert in den 90er Jahren als *Cybercoin*. Das Peer-to-Peer-Zahlungssystem eCash der DigiCash nutzte ein Gutscheinsystem, bei dem jede digitale Münze anonym durch eine digitale Seriennummer dargestellt wurde, die auf der Festplatte des Benutzers in einem Wallet gespeichert wurde. Die Anonymisierung der Nutzer erfolgte bereits anhand einer Public-Key-Kryptografieanwendung. Jede einzelne Transaktion musste jedoch, um ein Double Spending zu verhindern, von zentralen Servern bestätigt werden.[5]

[3] Alles Wichtige zum NSA-Skandal, http://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal von Patrick Beuth (Abruf: 03.09.2015).

[4] Phil Zimmermann war der erste, der die asymmetrische Kryptografie (auch Public-Key-Kryptografie genannt) als Software der Allgemeinheit leicht zugänglich machte. https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html (Abruf: 03.09.2015).

[5] The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, Paul Vigna und Michael J. Casey, St. Martin's Press (January 27, 2015), Pos 1140.

- Hashcash, ein Proof-of-Work-System, wurde im Mai 1997 von Adam Back, einem britischen Kryptografen ursprünglich entwickelt, um E-Mail-Spam und Denial-of-Service-Angriffe zu begrenzen. Computer müssen nach diesem Konzept kostspielige Arbeit verrichten, ehe sie Informationen versenden dürfen, sodass für jeden, der ein Netzwerk mit Nachrichten überfluten will, erhebliche Kosten anfallen.[6]
- Die Idee eines Hauptbuches bzw. einer Datenbank mit einer nachvollziehbaren chronologischen Erfassung aller darin gespeicherten Transaktionen datiert bereits aus 1991 und stammt von Haber und Stornetta.[7] Das Konzept von Haber und Stornetta sah dabei einen zentralen Server vor, der ein erhaltenes Dokument zusätzlich zu einem Zeitstempel auch mit einem Link zu dem vorhergehenden erhaltenen Dokument versieht und so eine vollständige chronologische Dokumentenerfassung ermöglicht. In der Folge erweiterten Harper und Stornetta ihr Konzept, indem nicht mehr einzelne Dokumente verknüpft wurden, sondern Dokumente in Blöcke zusammengefasst wurden. Einerseits wurden dabei innerhalb der Blöcke die Dokumente miteinander verlinkt und andererseits wurden die Blöcke verknüpft und in Form einer Kette aneinandergereiht.
- Das Konzept des *b-money*, entwickelt von Wei Dai 1998, sah sowohl die Möglichkeit des Schaffens einer Kryptowährungseinheit als Hashcash-Funktion als auch ein Peer-to-Peer-Netzwerk vor.
- Zwischen 1998 und 2005 entwickelte Nick Szabo das digitale Währungssystem *BitGold*. Auch BitGold basierte bereits auf dem Proof-of-Work-Ansatz von Adam Back und löste eines der offenen Punkte des Hashcash-Konzepts: Im System von Adam Back konnte jede Hashcash-Einheit nur einmal verwendet werden. Das System von Nick Szabo kreierte digitale Werteinheiten, die wiederholt genutzt werden konnten.
- Im Jahr 2005 stellte Hal Finney (der später auch eine wichtige Rolle in der Verbreitung des Bitcoin-Systems spielen sollte) das *Reusable Proof-of-Work*-Konzept vor, dass die Ansätze des b-moneys von Wei Dai verwendete und mit den von Adam Back entwickelten Hashcash-Puzzles ergänzte, um einen Vorschlag für eine Kryptowährung zu schaffen.

All diese Konzepte erforderten jedoch durch das ungelöste Double Spending-Problem (unbeschränkte Möglichkeit der Reproduktion eines digitalen Gutes) des digitalen Geldes einen vertrauenswürdigen Dritten in welcher Form auch immer.

Das von Satoshi Nakamoto am 31. Oktober 2008 an den E-Mailverteiler der Kryptografiegruppe (cryptography@metzdowd.com) versandte neunseitige Konzept mit dem Titel *Bitcoin: A Peer-to-Peer Electronic Cash System* unterschied sich insbesondere in zwei Aspekten von den bisher diskutierten Ideen:

[6] https://en.wikipedia.org/wiki/Hashcash (Abruf: 03.09.2015).
[7] https://en.wikipedia.org/wiki/Linked_timestamping (Abruf: 19.02.2016)

- Im Ausmaß des dezentralen Netzwerks und der Auslagerung der Bestätigung der Transaktionen an die Teilnehmer des Netzwerks.
- In der Form des Mining-Belohnungsalgorithmus, der eine Weiterführung des b-money-Konzepts von Wei Dai darstellte.

Die Kombination der Nutzung des Proof-of-Work-Konzepts zur Generierung von digitalem Geld mit dem Konzept von Harper und Stonetta (Zeitstempel und Verlinkung der Transaktionen/Blöcke) und der dadurch entstehenden Bitcoin-Blockchain zur Vermeidung des Double Spending-Problems erfolgte damit auf diese Weise erstmals durch ein dezentrales Computernetzwerk.

Die Bitcoin Architektur verwendet kryptografische Verschlüsselungstechniken zur Regelung des Geldschöpfungsprozesses und zur Verifizierung der durchgeführten Transaktionen. Das Netzwerk basiert auf einer dezentralen Struktur, die aufbaut auf der Anonymität der Nutzer damit auch die Gleichheit der Teilnehmer sicherstellt und durch den Proof-of-Work-Ansatz die Möglichkeit für Manipulationen Dritter beseitigt.

Mittels des Proof-of-Work-Konzeptes bestimmt sich das Ausmaß der möglichen Einflussnahme auf den Algorithmus durch den wirtschaftlichen Aufwand, den man bereit ist, in das System zu investieren (z. B. in Form von Mining-Hardware).

2.2 Definitionen

Automated Clearing Houses (ACH-Systeme)[8] Elektronisches U.S. Clearing-System, in dem vorrangig über Telekommunikationsnetzwerke übermittelte Zahlungsaufträge zwischen Finanzdienstleistern in einem Rechenzentrum des Betreibers verrechnet und ausgetauscht werden. Die Verrechnung der Zahlungen erfolgt brutto (je Datei) oder netto (nur Saldo) zu vorgegebenen Zeitpunkten über Konten der teilnehmenden Finanzdienstleister bei der Zentralbank oder einer privaten Settlement-Bank. Es handelt sich meist um eine große Anzahl von Überweisungen bzw. Lastschriften. Die Abwicklung erfolgt in Form der Stapelverarbeitung (Zusammenfassung in Dateien).

Bitcoin-Blockchain ist die öffentlich einsehbare Datenbank, die von den Nutzern des Systems, die sich einen Bitcoin Core heruntergeladen haben (auch Nodes genannt), dezentral auf ihren Computern gehostet wird. Die Bitcoin-Blockchain kann öffentlich eingesehen werden auf Internetseiten wie www.blockchain.info, hier kann man den Transaktionsstrom durch Eingabe einer Bitcoin-Adresse nachverfolgen.

Blocks sind Transaktionen, die in Transaktionsgruppen zusammengefasst sind und die sequentiell in der Blockchain erfasst werden.

[8] Springer Gabler Verlag (Hrsg.), Gabler Wirtschaftslexikon, Stichwort: Automated Clearing House (ACH), online im Internet: http://wirtschaftslexikon.gabler.de/Archiv/5035/automated-clearing-house-v9.html, (Abruf: 01.01.2016).