
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 interessantesten 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 Nutzungsg Gebühr 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 Geldes³ 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



<http://www.springer.com/978-3-658-02843-5>

Bitcoins und andere dezentrale Transaktionssysteme

Blockchains als Basis einer Kryptoökonomie

Sixt, E.

2017, XIV, 195 S. 17 Abb., Softcover

ISBN: 978-3-658-02843-5