

Zeitschrift: Schweizer Monat : die Autorenzeitschrift für Politik, Wirtschaft und Kultur
Band: 97 (2017)
Heft: 1045

Artikel: Blockchain statt Bürokratie
Autor: Jaag, Christian
DOI: <https://doi.org/10.5169/seals-736480>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

Download PDF: 29.04.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

6 Blockchain statt Bürokratie

Die Technologie setzt etablierte Institutionen unter Druck. Das ermächtigt die Bürger gegenüber potenziell unfähigen Autoritäten.

von Christian Jaag

Vielen Menschen ist die Blockchain bekannt als die Technologie hinter Kryptowährungen wie Bitcoin. Doch das System hat noch viel mehr Potenzial – es kann bestehende Institutionen ergänzen oder gar teilweise ersetzen. Das bringt mit sich, was die Digitalisierung oft nach sich zieht: eine Verschiebung von Macht weg von zentralen und vermittelnden Instanzen hin zu sich selber organisierenden Bürgern. Doch noch gibt es offene Fragen.

Zunächst zur Geschichte und Funktionsweise der Blockchain: sie beginnt mit dem Grundlagenpapier «Bitcoin: A Peer-to-Peer Electronic Cash System». Dieses wurde im November 2008 von Satoshi Nakamoto veröffentlicht, wobei bis heute niemand weiss, wer hinter diesem Pseudonym steht. Dem Aufsatz, der die Funktionsweise von Bitcoin beschreibt, folgte schon Anfang 2009 die konkrete Umsetzung mit dem Start von Bitcoin, der ersten und bisher erfolgreichsten Blockchain. «Be your own bank» bringt die Vision der Blockchain-Pioniere auf den Punkt. Der Slogan verweist auf die Möglichkeiten der ersten Anwendung einer Blockchain, nämlich als Währung und Zahlungssystem ohne Intermediäre. Auf dem Höhepunkt der Finanzkrise galt der Slogan auch als Aufforderung, von diesen Möglichkeiten Gebrauch zu machen und die Macht der traditionellen Institutionen im Finanzsystem zu brechen.

Christian Jaag

ist Ökonom. Er ist Managing Partner beim Beratungsunternehmen Swiss Economics und Lehrbeauftragter an den Universitäten St. Gallen und Zürich sowie an der ETH Lausanne.

Der Name Bitcoin steht sowohl für die entsprechende Blockchain beziehungsweise das entsprechende Zahlungssystem als auch für die Währung in diesem System und deren Werteinheit. Die Bitcoin-Blockchain kann mit einem Handelsbuch verglichen werden, in welchem in chronologischer Reihenfolge Betrag, Zeitpunkt sowie Absender und Empfänger jeder Transaktion ersichtlich sind. Im Gegensatz zum Handelsbuch ist die Bitcoin-Blockchain öffentlich einsehbar. Sie wird über das Internet verteilt und jedermann kann eine Kopie davon speichern. Die Bitcoin-Blockchain bildet die Eigentümerkette von Bitcoins in einer öffentlich zugänglichen Datenstruktur ab. Das Recht, einen Bitcoin-Betrag auszugeben, wird in kryptographischen Schlüsseln gespeichert, so dass Bitcoins auf jedem Computer, Smartphone oder sogar auf einem Blatt Papier gespeichert werden können. Auch Zahlungen sind mit Bitcoin direkt von Person zu Person (Peer-to-Peer) schnell und günstig sowie ohne Intermediär möglich. Insofern kommt das System ohne Geschäftsbanken aus. Deren traditio-



Transparent und papierschonend: Honduras und Georgien arbeiten bereits an einer Überführung des Grundbuchs auf die Blockchain. Bild: fotolia.

nelle Rollen als sicherer Ort zur Aufbewahrung von Vermögen und als Zahlungsverkehrsinstitut sind damit obsolet.

Algorithmen statt Notenbanker

Die Blockchain kann also – und damit sind wir wieder beim Anfang – langfristig etablierte Institutionen in Frage stellen. Neben den Geschäftsbanken spielen im bestehenden Finanzsystem auch die Zentralbanken eine wichtige Rolle: Sie sollen insbesondere die Preisstabilität gewährleisten. Dabei haben sie einigen Spielraum. Dieser erfordert ein Vertrauen der Wirtschaft in die Kompetenz und Integrität der Entscheidungsträger der Geldpolitik, ihre Währung nicht durch übertrieben grosszügige Geldschöpfung abzuwerten. Bei Bitcoin und anderen Kryptowährungen wird die Geldmenge mit einem Algorithmus gesteuert, der fester Bestandteil des Gesamtsystems ist. Damit ist die Geldpolitik regelgebunden und Vertrauen ist nur in die Regeln der Mathematik und die Programmierung des Systems notwendig. Letztere ist im Fall von Bitcoin durch den offenen Quelltext vollkommen transparent.

Die Blockchain kann also sowohl traditionelle Geschäftsbanken als auch Zentralbanken ersetzen – und selber als neue Art von Institution angesehen werden. Als solche ist sie eine besonders wertvolle Alternative in Ländern, in denen die traditionellen Institutionen des Finanzsystems versagen. Stabile Währungen und der Zugang zu vertrauenswürdigen Banken sind weltweit eher eine Ausnahme als die Regel. Ein grosser Teil der Weltbevölkerung hat keinen Zugang zu einem formalen Finanzinstitut und zu einer Kreditkarte. Damit ist auch der Zugang zu einem grossen

Teil der Weltwirtschaft verschlossen. Kryptowährungen, die ohne formale Institutionen auskommen, können hier Abhilfe schaffen und einen Beitrag zur «Financial Inclusion» leisten.

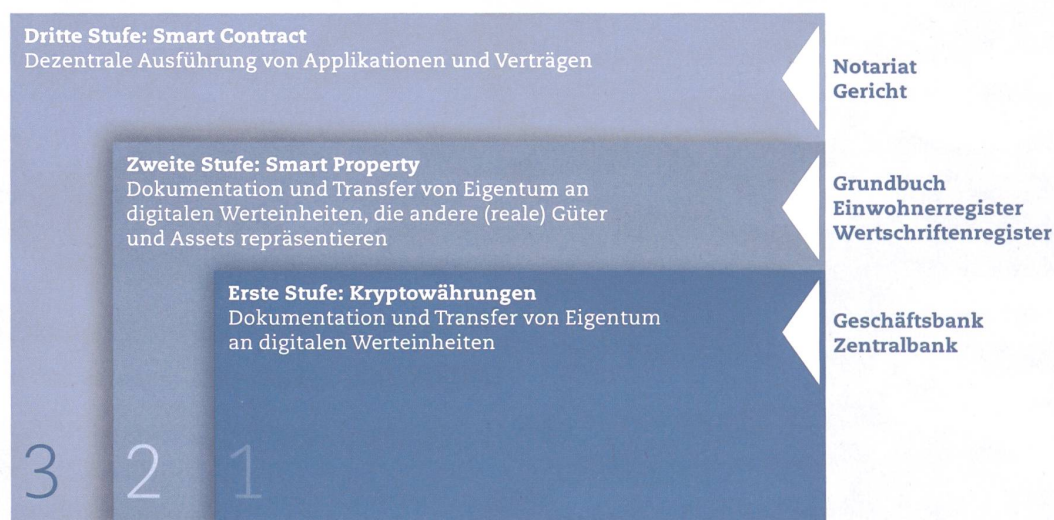
Die Bitcoin-Blockchain und ihre Klone – weil der Bitcoin-Quellcode öffentlich zugänglich ist, sind daraus bereits mehrere hundert eigenständige Kryptowährungen entstanden – sind allerdings nur die erste Anwendungsstufe der Blockchain (vgl. Abbildung). Ihr Potenzial ist damit aber bei weitem noch nicht ausgeschöpft.

Plattform für Eigentumsrechte

Der Wert von Bitcoin und anderen Kryptowährungen ist sehr volatil: 2016 bewegte er sich zwischen 350 und 980 Franken. Je nach Anwendung sind sie deshalb als eigenständige Zahlungsmittel noch wenig geeignet. Die zweite Anwendungsstufe der Blockchain besteht deshalb darin, die einzelnen Werteinheiten («Token») als Repräsentanten anderer Güter zu interpretieren (sogenannte «Smart Property»). Ein Beispiel für dieses Konzept sind «Colored Coins»: Genauso wie eine Banknote den grössten Teil ihres Werts erst durch die Färbung eines Stücks Papier erhält, kann auch ein bestimmter Bruchteil eines Bitcoins durch dessen «Farbe» einen definierten Wert erhalten – zusätzlich zum Wert des Bitcoins selbst, der bei einem kleinen Bruchteil allerdings vernachlässigbar ist.

Das bringt eine Reihe interessanter Anwendungsmöglichkeiten mit sich. Beispielsweise kann ein Token eine Aktie repräsentieren. Der Eigentümer dieses Token gilt auch als Eigentümer der entsprechenden Aktie, und das Eigentum kann durch eine Bit-

Abbildung: Anwendungsstufen der Blockchain



«Die erhöhte Transparenz von Transaktionen auf einer Blockchain ermöglicht es dem Staat, detailliert Rechenschaft über seine Tätigkeit abzulegen, und bemächtigt seine Bürger, diese auch einzufordern.»

Christian Jaag

coin-Transaktion übertragen werden. Durch eine solche «Tokenization» können (Eigentums-)Rechte mit geringen Transaktionskosten verbriefte und gehandelt werden. Das lässt neue Märkte entstehen, stellt aber weitere öffentliche oder staatliche Institutionen in Frage: Aktien des US-amerikanischen Unternehmens Overstock sind bereits auf der Bitcoin-Blockchain (statt im Register einer zentralen Depotbank) abgelegt. Ähnlich funktionieren Versuche in Honduras und Georgien, das Grundbuch auf einer Blockchain abzulegen.

Auch grosse Finanzinstitute haben die Technologie für sich entdeckt und arbeiten an Lösungen, um mit ihr das Interbanken-Clearing zu vereinfachen und zu beschleunigen. Die dazu verwendeten Blockchains sind nicht öffentlich, so dass der Zugang dazu kontrolliert und gesteuert werden kann. Solche Systeme verzichten auf die vollständige Dezentralisierung und damit auch die Resilienz und Zensurfreiheit einer offenen Blockchain. Verglichen mit anderen Datenstrukturen oder -banken erlauben sie einen raschen Geschäftsverkehr mit tiefen Transaktionskosten: Der Verzicht auf Intermediäre erlaubt es Finanzmarktteilnehmern, Kosten zu senken sowie Clearing- und Settlementprozesse zu beschleunigen. Damit können sie ihr Eigenkapital reduzieren und ihre operationellen Risiken senken. Gleichzeitig ist mit der zentralen Verwaltung und der Zugangskontrolle die Einhaltung regulatorischer Vorgaben einfacher, da Transaktionen massgeschneidert abgewickelt, vor den Konkurrenten verborgen und gleichzeitig gegenüber Aufsichtsbehörden dokumentiert werden können.

Solche Anwendungen motivieren auch Staaten dazu, die Zentralbank in die Welt der Blockchain einzubinden. Wenn ein Wertpapierverkauf auf einer Blockchain abgewickelt und in Schweizer Franken bezahlt werden soll, muss der Käufer den Kaufpreis be-

gleichen, indem er Guthaben von seiner Hausbank an die Bank des Verkäufers überweist. Die Übertragung des Frankenbetrags erfolgt anschliessend zwischen den beiden Banken über die bestehenden Kanäle des Zahlungsverkehrs. Das ist langsam und teuer. Wenn aber die Nationalbank in die Blockchain eingebunden wäre, könnte sie Notenbankgeld schaffen, das direkt auf der Blockchain überwiesen wird. Der Käufer eines Wertpapiers könnte dann solche Krypto-Schweizer-Franken mittels Blockchain an den Verkäufer übertragen. Die Übertragung des Wertpapiers und des Geldbetrags könnte so simultan abgewickelt werden und der Bedarf an Intermediation durch die beiden Banken entfielen.

Diesbezüglich sind verschiedene Staaten der Schweiz voraus. Tunesien, Senegal, Benin und Togo planen bereits, ihre Landeswährungen als Kryptowährungen auszugestalten. Die Bank of England und die Bank of Canada machen sich ebenfalls öffentlich darüber Gedanken und die Schwedische Reichsbank arbeitet schon an einer «E-Kroner». Auch Luxus- und Handelsgüter werden bereits auf Blockchains registriert, so dass sich deren Eigentümer- und Wertschöpfungskette transparent nachverfolgen lässt. Beispielsweise verfolgt Dubai das Ziel, bis 2020 sämtliche Import- und Exportprozesse auf einer Blockchain abzubilden.

Diese Beispiele zeigen, wie die Blockchain bestehende Institutionen ergänzen, teilweise ersetzen, aber möglicherweise nicht vollständig überflüssig machen kann. All diesen Anwendungen ist nämlich gemeinsam, dass sie zusätzlich zur Blockchain, wo die Eigentumsrechte abgelegt sind, eine Institution benötigen, welche die virtuelle Werteinheit mit dem physischen Gut oder der traditionellen Währung verknüpft, gewissermassen als Brücke zwischen der virtuellen und der physischen Welt. Sie muss sicherstellen und dafür einstehen, dass letztere tatsächlich existieren und dem Ei-

gentümer der virtuellen Geldeinheit gehören. Die Blockchain kann also einzelne Aufgaben bestehender Institutionen, beispielsweise des Aktienregisters, des Grundbuchs oder des Einwohnerregisters, übernehmen, diese aber nicht vollumfänglich ersetzen.

In einem kürzlich erschienenen Bericht kommt die britische Regierung zum Schluss, dass die Blockchain für den Staat die Grundlage schaffe, Betrug, Korruption, Fehler und die Kosten papierbasierter Prozesse zu reduzieren. Sie habe das Potenzial, die Beziehung des Staats und seiner Bürger bezüglich Datenaustausches, Transparenz und Vertrauens neu zu definieren. Die erhöhte Transparenz von Transaktionen auf einer Blockchain ermöglicht es dem Staat, detailliert Rechenschaft über seine Tätigkeit abzulegen, und bemächtigt seine Bürger, diese auch einzufordern.

Nicht nur Güter lassen sich auf einer Blockchain registrieren, sondern auch Personen. So können Identitäten und Zugangsrechte zu digitalen Diensten verwaltet werden. Estland basiert seine Infrastruktur für digitale Identitäten auf eine Blockchain. So können seine Bürger ihre digitale ID für Schulzeugnisse, Abstimmungen, Steuererklärungen und ihr Testament sowie rund 3000 weitere Anwendungen nutzen.

Intelligente Verträge

Die dritte Anwendungsstufe der Blockchain ist ihre Nutzung als Plattform zur dezentralen Ausführung von Applikationen und Verträgen (sog. Smart Contracts). Dazu besonders geeignet ist die (neben Bitcoin) zweite grosse Blockchain «Ethereum». Sie erlaubt es, Verträge zu programmieren, die sich beim Eintreffen gewisser Ereignisse selbständig ausführen. So kann die Blockchain die Rolle von Notaren und Gerichten übernehmen, weil Verträge damit theoretisch ohne Notwendigkeit einer Auslegung programmiert und automatisch beglaubigt werden können.

Die Idee von Smart Contracts – und deren Grenzen – lässt sich eindrücklich am Beispiel von «dezentralen autonomen Organisationen» (DAO) illustrieren. Eine DAO ist ein virtuelles Unternehmen, welches ausschliesslich als Code existiert und durch diesen gelenkt und geführt wird. Es besteht aus einem Zusammenspiel sich selbständig durchsetzender Verträge. Eine der ersten DAO (selbstbewusst «The DAO» genannt) wurde als Investmentgesellschaft konzipiert, welche sich an Projekten finanziell beteiligen kann, die ihr von Dritten vorgeschlagen werden. Die dieser DAO zugrunde liegenden Smart Contracts wurden auf der Ethereum-Blockchain abgelegt. Mit der ausschliesslichen Verwendung von Computercode und Smart Contracts, das heisst ohne weitere Statuten oder Organe, erhoffte man sich, späteren Streit über die geltenden Regeln der Organisation und deren Auslegung vermeiden zu können.

Das Unternehmen wurde von pseudonymen Eignern getragen, welche sich durch den Kauf von Anteilen gegen Ether (der Kryptowährung auf der Ethereum-Blockchain) daran beteiligen konnten. In den ersten vier Wochen nach der Gründung der DAO im Frühling 2016 wurden Anteile im Gegenwert von über 150 Millionen Franken gezeichnet.

Doch bevor das erste Projekt regulär finanziert werden konnte, nahm die Erfolgsgeschichte der DAO im Juni 2016 ein jähes Ende. Einem der Anteilseigner gelang es, rund ein Drittel des DAO-Vermögens auf eigene Konten abzuzweigen. Nur mit einer Regeländerung in der Ethereum-Blockchain gelang es, die abhandengekommenen Ether den ursprünglichen Eigentümern zurückzugeben. Damit wurde die Irreversibilität von Transaktionen – eigentlich ein Grundprinzip der Blockchain – geopfert. Gleichzeitig wurde damit ein Systemteilnehmer (die DAO) als «too big to fail» eingestuft – ein Problem des traditionellen Finanzsektors, das man mit der Blockchain als entschärft geglaubt hatte. Zudem kann sowohl die Aktion des Angreifers als auch deren Rückabwicklung als Diebstahl betrachtet werden.

Aktuelle Herausforderungen

Die Grenzen freier, offener und dezentraler Blockchains zeigen sich bereits in der ersten Anwendungsstufe, bei den Kryptowährungen. «Be your own bank» heisst auch, für das eigene Geld selber verantwortlich zu sein. Weil sich manche nicht zutrauen, ihre Bitcoins auf dem eigenen Computer sicher aufzubewahren, hat sich in den letzten Jahren ein weites Ökosystem an Dienstleistern entwickelt, welche die Nutzer in ihrem Umgang mit Kryptowährungen unterstützen. So sind verschiedene bankähnliche Institute entstanden, welche Kryptowährungen als Einlagen entgegennehmen und aufbewahren oder deren Tausch in traditionelle Währungen anbieten. Während das Bitcoin-System aufgrund seiner Dezentralität extrem resilient ist und bisher sämtlichen Angriffen getrotzt hat, sind es solche Intermediäre, deren Verletzlichkeit in der Vergangenheit wiederholt für negative Schlagzeilen gesorgt hat. Mybitcoin.com ist im Sommer 2011 mitsamt den Einlagen seiner Nutzer plötzlich verschwunden – noch ohne ausserhalb der kleinen Bitcoin-Community grosses Aufsehen zu erregen. Der Kollaps von mtgox.com, der damals grössten Plattform, auf der Bitcoins gegen andere Währungen getauscht werden konnten, hat das Bitcoin-System im Winter 2014 an den Rand des Abgrunds geführt. Mittlerweile hat es sich kommerziell erholt; das juristische Nachspiel dauert aber an.

Dennoch: die Blockchain hat grosses Potenzial. Traditionelle staatliche und private Institutionen haben zwar auch in der Blockchain-Welt noch eine Existenzberechtigung. Deren wirtschaftliche und soziale Rolle wird sich aber fundamental verändern, indem die Blockchain sie zu transparenteren und überprüfbareren Prozessen zwingen kann. Nach vielen Rückschlägen zeichnet sich ab, dass die Blockchain doch noch zu dem werden könnte, wofür sie ursprünglich erfunden wurde: für den Austausch von Werten und Identitäten das zu werden, was das Internet für die Übermittlung von Informationen ist – eine transparente und dezentral aufgebaute Plattform. Damit trägt sie auch zu einer weiteren Machtverschiebung bei: weg von den Institutionen und hin zu den Individuen. ◀