ZUKUNFT

DIE GROßE KETTE DER SICHERHEITEN

Die Technologie von Bitcoin gibt Menschen, die einander nicht kennen oder vertrauen, Zahlungssicherheit. Dies hat Auswirkungen, die weit über die Kryptowährung hinausreichen.

Als die honduranische Polizei Mariana Catalina Izaguirre im Jahr 2009 zur Räumung ihres Hauses zwang, lebte sie bereits seit drei Jahrzehnten in ihrem bescheidenen Eigenheim. Im Gegensatz zu vielen ihrer Nachbarn in Tegucigalpa, der Hauptstadt des Landes, konnte sie einen gültigen Rechtsanspruch auf das Land vorweisen, auf dem ihr Haus stand. Doch in den Akten des Grundbuchamtes des Landes war auch noch eine andere Person als Eigentümer eingetragen, und diese Person hatte einen Richter dazu gebracht den Räumungsbefehls zu unterzeichnen. Als endlich alle rechtlichen Fragen geklärt waren, stand Frau Izaguirres Haus nicht mehr.

So etwas geschieht jeden Tag an Orten, in denen Grundbuchämter schlecht geleitet oder verwaltet werden oder gar korrupt sind, das heißt in weiten Teilen der Welt. Dieser Mangel an sicheren Eigentumsrechten ist eine endemische Quelle für Unsicherheit und Ungerechtigkeit. Dadurch ist es auch schwierig, ein Haus oder ein Stück Land als Sicherheit zu verwenden, was wiederum Investitionen und die Schaffung von Arbeitsplätzen behindert.

Mit „Bitcoin“ (Anm. d. R.: digitale Münze) scheint es nicht zu solchen Problemen zu kommen. Die digitale Währung basiert auf der Grundlage cleverer kryptographischer Techniken und hat eine treue Anhängerschaft hauptsächlich unter wohlhabenden, oft regierungskritischen und manchmal kriminellen Computerfreaks. Die sogenannte „Blockchain“ *(Anm. d. R.: Journal Datenbank, in der alle Transaktionen zwischen Computern aufgezeichnet werden)*, die dem

Bitcoin-System zugrunde liegende Verschlüsselungstechnologie, findet sogar weit über Bargeld und Währung hinaus Anwendung. Sie bietet Menschen, die einander nicht kennen oder vertrauen, eine Möglichkeit, genau festzuhalten, wem was gehört, und erzwingt dabei die Zustimmung aller Beteiligten. Sie bietet die Möglichkeit, Wahrheiten zu konstatieren und festzuhalten.

Deshalb haben Politiker, die im Grundbuchamt in Honduras aufräumen wollen, das amerikanische Start-up Factom gebeten, einen Prototypen für ein Grundbuch zu entwickeln, das auf Blockchain basiert. Auch Griechenland, wo es kein ordentliches Grundbuchamt gibt und wo nur sieben Prozent der Landesfläche präzise auf Karten verzeichnet sind, hat Interesse an dieser Idee bekundet.

Ein beliebiger Zeitpunkt in der Vergangenheit

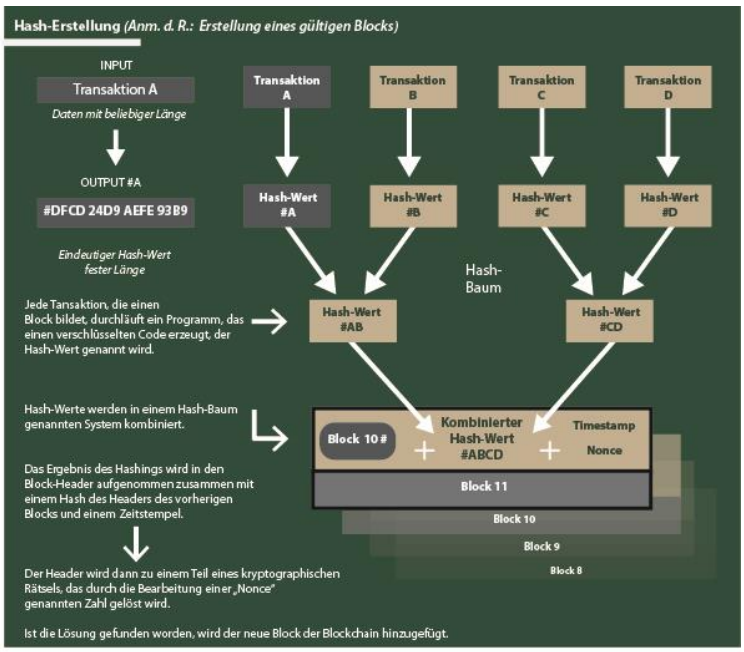
Andere Einsatzgebiete für Blockchain und ähnliche dezentrale Buchungssysteme oder Register reichen von der Vereitelung von Diamantendiebstahl bis hin zur Rationalisierung von Aktienbörsen: Die NASDAQ wird in Kürze Blockchain-basierte Systeme zur Erfassung des Handels mit Anteilen an Unternehmen einsetzen, die nicht an der Börse notiert sind. Die Bank of England, nicht gerade bekannt für technologische Innovationsfreude, scheint laut eines von ihr im vergangenen Jahr herausgegebenen Untersuchungsberichts überzeugt, dass dezentrale Register eine „bedeutende Innovation“ seien, die „weitreichende Auswirkungen“ auf die Finanzindustrie haben könnten.

Politisch Interessierte meinen, dass die Blockchain sogar noch tiefgreifender eingesetzt werden kann. Als Genossenschaften und Linke sich beim diesjährige OuiShare-Fest in Paris versammelten, um zu erörtern, wie Graswurzel-Organisationen *(Anm. d. R.: Aus der Bevölkerung entstehende politische oder gesellschaftliche Initiativen)* Riesen-Datenspeicher wie Facebook untergraben könnten, wurde die Blockchain in fast jeder Rede genannt. Anhänger des Libertarismus *(Anm. d. R.: Prinzip des Selbsteigentums*) träumen von einer Welt, in der staatliche Regulierungen in immer höherem Maße durch private Verträge zwischen Einzelnen ersetzt werden – Verträge, die sich mithilfe Blockchain-basierter Programmierung selbst durchsetzen könnten.

Die Blockchain wurde von Satoshi Nakamoto erdacht, dem brillanten, pseudonymen und bisher nicht identifizierten Schöpfer von Bitcoin – eine „reine Peer-to-Peer-Version *(Anm. d. R.: Rechner-Rechner-Verbindung)* von elektronischem Geld“, wie er es in einem 2008 veröffentlichten Aufsatz formulierte. Damit Bitcoins wie Bargeld verwendbar seien, müssen sie von Hand zu Hand gehen, ohne dass sie auf falsche Konten umgeleitet oder zweimal von derselben Person ausgegeben werden können. Um Nakamotos Traum von einem dezentralen Zahlungssystem Gestalt zu geben, musste ein derartiger Missbrauch ausgeschlossen werden,

ohne dabei auf Garanten herkömmlicher Zahlungssysteme zurückzugreifen, wie beispielsweise Banken.

Es ist die Blockchain, die diese vertrauenswürdige Instanz ersetzt. Die Blockchain ist eine Datenbank, die den Zahlungsverlauf jeder im Umlauf befindlichen Bitcoin enthält. Sie belegt für jeden beliebigen Zeitpunkt, wer was besitzt. Dieses dezentrale Buchungssystem oder Register wird auf Tausenden von Computern – den sogenannten „Nodes“ (Anm. d. R.: dt. Knoten) – rund um den Globus repliziert und ist öffentlich zugänglich. Bei all ihrer Öffentlichkeit ist diese Datenbank jedoch simultan vertrauenswürdig und sicher. Dies wird gewährleistet durch eine Mischung aus mathematischer Subtilität und gewaltiger Rechenleistung, die in ihren „Konsens-Mechanismus“ integriert ist, dem Prozess, in dem die Nodes sich darüber abstimmen, wie die Blockchain im Rahmen von Bitcoin-Überweisungen von einer Person zur anderen aktualisiert wird.



Nehmen wir einmal an, Alice möchte Bob für erbrachte Leistungen bezahlen. Beide verfügen über eine „Bitcoin-Wallet“ *(Anm. d. R.: Das virtuelle Portemonnaie des Teilnehmers)* - Software, deren Zugriff auf die Blockchain etwa so funktioniert, wie der Zugriff eines Browsers auf das Internet, wobei der Benutzer vom System nicht identifiziert wird. Die Transaktion beginnt damit, dass das Bitcoin-Wallet von Alice eine Änderung der Blockchain vorschlägt, bei der das Wallet von Alice ein wenig leerer und das von Bob ein wenig voller werden soll.

Um diese Änderung zu bestätigen, durchläuft das Netzwerk eine Reihe von Schritten. Während der Vorschlag im Netzwerk weitergeleitet wird, prüfen die verschiedenen Nodes, ob Alice tatsächlich über die Bitcoin verfügt, die sie jetzt ausgeben möchte. Dazu prüfen sie die Einträge der Blockchain. Wenn alles unbedenklich aussieht, bündeln spezialisierte Nodes, die sogenannten „Miner“ (Anm. d. R.: stellen Rechenleistung zur Verfügung), den Vorschlag von Alice mit anderen, ähnlich seriösen Transaktionen, um einen neuen Block für die Blockchain zu erstellen.

Dies beinhaltet die wiederholte Verarbeitung der Daten durch eine kryptographische „Hash-Funktion“, die den Block auf eine Ziffernfolge mit bestimmter Länge reduziert (siehe Diagramm). Wie bei kryptographischen Verarbeitungen üblich, ist das Hashing eine Einbahnstraße. Es ist nicht schwer, aus Daten ein Hash abzuleiten, jedoch unmöglich, aus einem Hash Daten abzuleiten. Doch obwohl das Hash die Daten selbst nicht enthält, ist es doch einmalig und ihnen

eindeutig zugeordnet. Ändert man die Bestandteile des Blocks in irgendeiner Weise – verändert man eine Transaktion auch nur um eine einzige Ziffer – ist das Hash nicht mehr dasselbe.

Betrieb hinter den Kulissen

Das Hash wird zusammen mit anderen Daten dem Header des vorgeschlagenen Blocks hinzugefügt. Dieser Header bildet dann die Grundlage für ein anspruchsvolles mathematisches Rätsel, bei dem die Hash-Funktion erneut Verwendung findet. Dieses Rätsel kann nur durch systematisches Probieren gelöst werden. Im gesamten Netzwerk berechnen Miner Trillionen und Abertrillionen von möglichen Antworten. Hat ein Miner endlich eine Lösung gefunden, werden sie von anderen Nodes in kurzer Zeit geprüft (das ist wieder eine Einbahnstraße: die Lösung zu finden ist schwer, doch sie zu kontrollieren ist leicht) und jeder Node, der die Richtigkeit der Lösung bestätigt, aktualisiert die Blockchain dementsprechend. Das Hash des Headers wird zum Identifizierungsstring des neuen Blocks und dieser Block ist nun ein Teil der Blockchain beziehungsweise des Bitcoin-Registers. Die Zahlung von Alice an Bob und alle anderen Transaktionen, die der Block enthält, sind nun bestätigt.

Dieser Rätselschritt trägt in drei Punkten in hohem Maße zur Sicherheit von Bitcoin bei. Einer davon ist der Zufall. Es ist nicht möglich vorherzusagen, welcher Miner ein Rätsel lösen wird und deshalb ist es unmöglich zu wissen, wer die Blockchain zu einem bestimmten Zeitpunkt aktualisieren wird. Es steht allein fest, dass es einer der hart arbeitenden Miner sein muss und nicht ein zufälliger Eindringling. Dadurch wird Betrug deutlich erschwert.

Die zweite Ergänzung im Prozess sind Informationen zum Verlauf. Jeder neue Header enthält ein Hash des Headers des vorhergehenden Blocks, das wiederum einen Hash-Wert des vorhergehenden Headers enthält und so weiter und so weiter bis zurück zum Anfang. Es ist diese Verkettung, die die Blöcke erst miteinander verbindet. Hat man alle Daten in diesem Bitcoin-Registers vorliegen, ist es ein Leichtes, den Header für den neuesten Block zu reproduzieren. Nähme man jedoch irgendwo eine Änderung vor – selbst an einem der ersten Blöcke – so änderte sich der Header des geänderten Blocks. Daraus würde folgen, dass sich auch die Header des nachfolgenden Blocks sowie alle diesem nachfolgenden Blöcke änderten. Das Register stimmt so nicht mehr mit der Kennung des neuesten Blocks überein und würde abgelehnt.

Gibt es eine Möglichkeit, diesen Prozess zu umgehen? Stellen wir uns vor, dass Alice es sich anders überlegt und Bob doch nicht mehr bezahlen möchte. Sie versucht, die Verlaufsinformationen umzuschreiben, sodass ihre Bitcoin in ihrem Bitcoin-Wallet bleibt. Wäre sie eine kompetente Minerin, könnte sie das erforderliche Rätsel lösen und eine neue Version der Blockchain erstellen. Doch in der Zeit, die sie dazu benötigt, hätte das übrige Netzwerk die ursprüngliche Blockchain bereits weiter verlängert. Und Nodes arbeiten immer an der längsten Version der Blockchain, die es

gibt. Diese Regel verhindert Situationen, in denen zwei Miner die Lösung fast gleichzeitig finden, sodass dabei nichts weiter als eine temporäre Gabelung in der Kette entsteht. Auch dies verhindert Betrug. Um das System dazu zu bringen, ihre neue Version der Blockchain zu akzeptieren, müsste Alice sie schneller verlängern können, als der Rest des Systems die ursprüngliche Version verlängert. Dies wäre nur möglich, wenn sie mehr als die Hälfte der Computer steuert, was im Fachjargon „51-Prozent-Angriff" genannt wird.

Träume sind manchmal ansteckend

Ganz abgesehen von den Schwierigkeiten, die mit dem Versuch verbunden sind, das Netzwerk zu untergraben, stellt sich eine viel wichtigere Frage: warum sollte man überhaupt an all dem teilnehmen? Weil der letzte Bestandteil, der mit dem Lösen des Rätsels in den Prozess einfließt, einen Anreiz bietet. Die Erstellung eines neuen Blocks erzeugt neue Bitcoins. Der Miner, der zuerst das Rätsel löst, erhält 25 Bitcoins mit einem aktuellen Gegenwert von rund 7.500 USD.

All dies macht Bitcoin jedoch nicht zu einer besonders attraktiven Währung. Ihr Wert ist instabil und unberechenbar (siehe Grafik auf der folgenden Seite) und die im Umlauf befindliche Gesamtmenge dieser Währung ist bewusst begrenzt. Doch der Blockchain- Mechanismus funktioniert sehr gut. Laut der Webseite blockchain.info werden der Blockchain pro Tag durchschnittlich mehr als 120.000 Transaktionen hinzugefügt, was etwa 75 Mio. USD entspricht. Es gibt aktuell 380.000 Blöcke und die Blockchain hat derzeit eine Größe von beinahe 45 Gigabyte.

Die meisten Daten in der Blockchain betreffen Bitcoin. Dies ist jedoch nicht zwingend der Fall. Satoshi Nakamoto hat etwas entwickelt, was Computerfreaks eine „offene Plattform" nennen – ein verteiltes System, dessen Funktionsweise offen gelegt ist und das erweitert werden kann. Das Vorbild solcher Plattformen ist das Internet selbst; weitere Beispiele sind Betriebssysteme wie Android oder Windows. Anwendungen, die von grundlegenden Funktionen der Blockchain abhängen, können somit entwickelt werden, ohne dass um Erlaubnis eingeholt oder dafür bezahlt werden müsste. „Das Internet hat endlich eine öffentliche Datenbank", sagt Chris Dixon von Andreessen Horowitz, einem Risikokapitalgeber, der mehrere Bitcoin-Start-ups finanziert hat, darunter Coinbase, das digitale Wallets anbietet, und 21, welches Bitcoin-Mining-Hardware für die breite Masse entwickelt.

Bis jetzt können Blockchain-basierte Angebote in drei Gruppen unterteilt werden. Die erste Gruppe nutzt die Tatsache, dass mithilfe der Blockchain jegliche Arten von Vermögenswerten übertragen werden können. Eines der Start-ups, die auf dieser Idee aufbauen, ist Colu. Die Firma hat einen Mechanismus entwickelt, mit dem sehr kleine Bitcoin-Transaktionen (sogenannter „Bitcoin-Staub") mit zusätzlichen Daten ergänzt werden können, sodass sie Anleihen, Aktien oder Anteile von Edelmetallen darstellen können.

Der Schutz von Grundeigentum ist ein Beispiel für die zweite Gruppe. Hier finden sich Anwendungen, welche Blockchain verwenden, um beispielsweise alle bisherigen Transaktionen festzuhalten. Bitcoin-Transaktionen können mit Schnipseln von zusätzlichen Informationen kombiniert werden, die so ebenfalls unveränderlich in der Datenbank festgeschrieben werden.

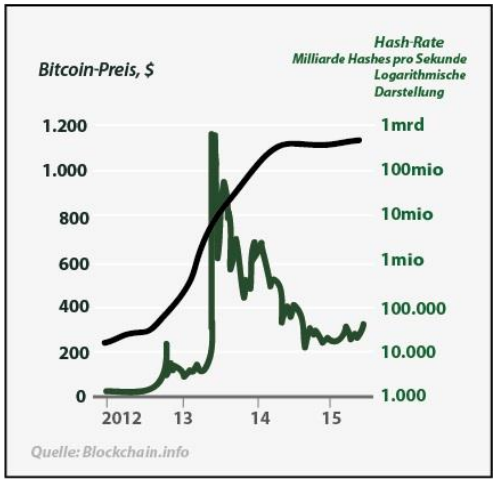
Die Blockchain kann somit zu einem Register von Dingen werden, die es wert sind, ganz genau verfolgt zu werden. Dienstleister wie Everledger nutzen die Blockchain, um Luxusgüter zu schützen. Dazu erfasst das Programm beispielsweise Daten von eindeutigen Merkmalen, zum Beispiel Zertifikate und Aufbewahrungsorte, eines Diamanten in die Blockchain und bietet so einen unbestreitbaren Beweis für dessen Identität, falls er gestohlen oder gehandelt werden sollte. Onename speichert persönliche Daten auf eine Art, die Passwörter überflüssig machen soll. CoinSpark fungiert als Notar. Beachtenswert ist jedoch, dass für diese Anwendungen, anders als bei reinen Bitcoin-Transaktionen, ein gewisses Maß an Vertrauen erforderlich ist. Man muss darauf vertrauen, dass der Vermittler die Daten korrekt und fehlerfrei abspeichert.

In der dritten Gruppe finden sich die ehrgeizigsten Anwendungen: „Intelligente Verträge“, die sich unter den richtigen Umständen automatisch selbst ausführen. Bitcoin kann „programmiert“ werden, sodass es nur unter bestimmten Bedingungen zur Verfügung steht. Diese Funktion wird zum Beispiel genutzt, um die Belohnung, die Miner für die Lösung eines Rätsels erhalten, solange aufzuschieben, bis 99 weitere Blöcke hinzugefügt wurden. Dies bietet einen zusätzlichen Anreiz, die Blockchain immer weiterzuführen.

Lighthouse, ein Projekt, das Mike Hearn, ein führender Bitcoin-Programmierer, ins Leben rief, ist ein dezentraler Crowdfunding-Dienst, der sich dieses Prinzips bedient. Wenn genügend Geld für ein Projekt zugesagt worden ist, wird es ausgezahlt. Wird die anvisierte Geldmenge nicht erreicht, geschieht nichts. Laut Hearn ist sein Projekt sowohl billiger als die Projekte der Wettbewerber, die nicht Bitcoin verwenden, als auch unabhängiger, da Regierungen nicht in der Lage sind, Projekte zu unterbinden, die ihnen nicht gefallen.

Energie ist ansteckend

Das Aufkommen von solchen „dezentralen Buchungssystemen oder Registern“ eröffnet einen „völlig neuen Bereich der Möglichkeiten“, so Albert Wenger von USV, einer New Yorker Kapitalbeteiligungsgesellschaft, die in Start-ups investierte wie beispielsweise OpenBazaar, einem vermittlerfreien Peer-to-Peer-Markt. Doch so offen und spannend die Blockchain auch sein mag, Skeptiker fürchten, dass ihre Sicherheit trügerisch und ihre Prozesse möglicherweise nicht skalierbar seien. Was für Bitcoin und einige Nischenanwendungen funktioniert, ist möglicherweise nicht in der Lage, Tausende von verschiedenen Diensten mit Millionen von Benutzern zu unterstützen.



Auch wenn Satoshi Nakamotos subtiles Design sich bisher als unbezwingbar erwiesen hat, haben Wissenschaftler Taktiken identifiziert, die es einem raffinierten und mit ausreichend finanziellen Mitteln ausgestatteten Miner ermöglichen könnten, die Blockchain zu kompromittieren, auch ohne 51 Prozent der Blockchain direkt zu kontrollieren. Und die Kontrolle über einen nennenswerten Anteil der Ressourcen des Netzwerks zu erlangen, erscheint heute

weniger unwahrscheinlich als noch vor einiger Zeit. Bitcoin-Mining, früher die Domäne ambitionierter Laien, wird heute von großen „Pools“ dominiert, in denen kleine Miner ihre Bemühungen kombinieren und die Belohnungen teilen, sowie von Betreibern großer Rechenzentren, von denen viele in China liegen, besonders in der Inneren Mongolei, wo Strom billig ist.

Weitere Sorge bereitet der Einfluss auf die Umwelt. Da die Redlichkeit von Minern nicht anders geprüft werden kann, zwingt die Bitcoin-Architektur sie, viel harte Berechnungsarbeit zu leisten. Dieser „Arbeitsnachweis“, ohne den es keine Belohnung gibt, stellt sicher, dass alle Beteiligten es ernst mit ihrem Einsatz meinen. Doch dies erfordert eine ungezählte Menge an Berechnungen, die keinen anderen Sinn verfolgen. Laut blockchain.info schlagen die Miner des Netzwerks derzeit etwa 450 Tausend Billionen Lösungen pro Sekunde vor. Und jede dieser Berechnungen verbraucht Strom.

Da die Miner Details zu ihrer Hardware geheim halten, weiß niemand, wie viel Strom das Netzwerk tatsächlich verbraucht. Angenommen, jeder von ihnen verwende die effizienteste Hardware, läge der jährliche Stromverbrauch bei etwa zwei Terrawattstunden – etwas mehr als die 150.000 Einwohner des Bezirks King's County im kalifornischen Central Valley pro Jahr verbrauchen. Schätzt man die Effizienz der von den Minern genutzten Hardware grundsätzlich pessimistisch ein, kann der Stromverbrauch jedoch bei bis zu 40 Terrawattstunden liegen. Das ist fast zwei Drittel dessen, was die 10 Millionen Menschen in Los Angeles pro Jahr verbrauchen. Sicher ist dies eine Übertreibung, doch je breiter die Anwendung von Bitcoin wird, desto größer könnte auch die Stromverschwendung werden.

Und trotz all dieses Verbrauchs bleibt Bitcoin in seiner Leistung beschränkt. Da Satoshi Nakamoto beschloss, die Größe eines Blocks auf ein Megabyte oder etwa 1.400 Transaktionen zu begrenzen, können nur sieben Transaktionen pro Sekunde verarbeitet werden. Im Vergleich dazu verarbeitet Visa in den USA 1.736 Transaktionen pro Sekunde. Die Blöcke könnten vergrößert werden, doch würde es länger dauern, größere Blöcke im Netzwerk zu verbreiten, was das Risiko einer Verzweigung der Blockchain erhöhen würde. Frühere Plattformen haben ähnliche Herausforderungen erfolgreich bewältigt. Als Millionen Nutzer in den 1990er-Jahren nach der Erfindung des Web-Browsers online gingen, sagten Experten voraus, dass das Internet zum Erliegen kommen würde – eppur si muove (Anm. d. R.: „und sie bewegt sich doch“). Genauso wenig steht das Bitcoin-System still. Spezialisierte Mining-Computer können sehr energieeffizient sein und es gibt Vorschläge für weniger energiehungrige Alternativen zum Arbeitsnachweis-Mechanismus. Entwickler arbeiten auch an einem Add-on namens „Lightning“, das eine große Zahl von kleineren Transaktionen außerhalb der Blockchain verarbeiten könnte. Schnellere Verbindungen verteilen größere Blöcke ebenso schnell wie früher kleinere Blöcke.

Das Problem ist nicht so sehr der Mangel an Lösungsvorschlägen. Es ist vielmehr so, dass der Bitcoin-Verbesserungsprozess des Netzwerks die Wahl erschwert. Eine Veränderung erfordert gemeinschaftsweite Einigkeit zwischen Menschen, denen Konsens nicht gerade leicht fällt. Man betrachte nur den Kampf, der um die Größe der Blöcke geführt wird. Ein Lager zeigt sich besorgt, dass die schnelle Erhöhung der Blockgröße zu einer weiteren Konzentration der Mining-Industrie führen könnte, wodurch Bitcoin noch mehr zu einem herkömmlichen Bezahlsystem werden würde. Die andere Seite argumentiert, dass das System bereits im nächsten Jahr zusammenbrechen könnte, wenn nichts getan wird, da Transaktionen Stunden dauern würden.

Waffenruhe

Mike Hearn und Gavin Andresen, eine weitere Bitcoin-Größe, führen das Big-Block-Lager an. Sie haben Mining-Firmen aufgerufen, eine neue Version von Bitcoin zu installieren, die eine wesentlich größere Blockgröße unterstützt. Einige Miner, die der Aufforderung nachgekommen sind, scheinen jedoch Cyber-Angriffen ausgesetzt zu sein. In scheinbar konzertiertem Bemühen, die Notwendigkeit – oder aber die Gefahren – eines solchen Upgrades aufzuzeigen, wird das System durch eine große Zahl von kleinen Transaktionen an seine Grenzen getrieben.

Dies alles hat den Versuchen, eine Alternative zur Bitcoin-Blockchain zu entwickeln, neue Impulse gegeben. Eine solche Alternative könnte vielleicht eher für die Speicherung von dezentralen Registern optimiert werden, als für den Betrieb einer Kryptowährung. MultiChain von Coin Sciences, ein weiteres Start-up, das eine Plattform bietet Blockchains selbst zu erstellen, demonstriert die Möglichkeiten. Neben den nötigen Mitteln für die Erstellung einer öffentlichen Blockchain wie der von Bitcoin, bietet MultiChain auch die Möglichkeit, private Blockchains zu erstellen, die nur zuvor geprüften Benutzern offen stehen. Könnte man allen Benutzern von vornherein vertrauen, würde die Notwendigkeit für das Mining und die Arbeitsnachweise vermindert oder gar eliminiert werden und eine das Register ergänzende Währung wäre bloß optional.

Der erste Wirtschaftssektor, der derartige Abwandlungen der Blockchain aufgreift und verwendet, könnte durchaus derjenige sein, dessen Versagen ursprünglich die Idee von Satoshi Nakamoto inspirierte: der Finanzsektor. In den vergangenen Monaten gab es einen Sturm der Begeisterung unter Bankern für private Blockchains, die eine Möglichkeit bieten, manipulationssichere Hauptbücher zu führen. Einer der Gründe dafür ist ironischerweise, dass diese – aus regierungsfeindlichem Libertarismus entstandene – Technologie es Banken erleichtern könnte, regulatorische Anforderungen zu erfüllen, wenn es darum geht, ihre Kunden zu kennen und Anti-Geldwäsche-Regeln umzusetzen. Doch ein Anreiz liegt noch tiefer.

Industriehistoriker weisen darauf hin, dass Innovationen oft verfügbar sind, lange bevor die Prozesse, denen sie am besten dienen, entwickelt wurden. Die ersten Elektromotoren wurden wie die großen, massigen Dampfmaschinen eingesetzt, die vor ihnen da waren. Es dauerte Jahrzehnte, bis die Hersteller verstanden, dass sie mit vielen, dezentralen Elektromotoren alle Aspekte ihrer Herstellungsprozesse neu organisieren konnten. In ihrem Bericht über digitale Währungen sieht die Bank of England eine ähnliche Bewegung im Finanzsektor. Dank billiger Rechenleistung haben Finanzinstitute ihre inneren Abläufe digitalisiert, aber ihre Organisation

haben sie noch nicht entsprechend angepasst. Zahlungssysteme sind zumeist noch immer zentralisiert. Die Zentralbank übernimmt das Clearing von Transaktionen. Wenn Finanzinstitute miteinander Geschäfte machen, kann die Aufgabe ihre internen Register zu synchronisieren mehrere Tage dauern, wodurch Kapital gebunden und Risiken erhöht werden.

Dezentrale Register, die Transaktionen in Minuten oder Sekunden ausführen, könnten die Lösung solcher Probleme weit vorantreiben und die Vorstellung einer digitalen Bank Realität werden lassen. Dabei könnten Banken auch eine Menge Geld sparen: laut der spanischen Bank Santander könnten solche dezentralen Register bis zum Jahr 2022 die Kosten der Branche um bis zu 20 Milliarden USD pro Jahr senken. Anbieter müssten noch beweisen, dass sie mit Transaktionsraten umgehen können, welche die von Bitcoin weit übersteigen, doch große Banken drängen bereits auf Standards, um die neue Technologie nach ihren Bedürfnissen zu gestalten. Eine dieser Banken, UBS, hat die Schaffung einer Standard- „Abrechnungswährung“ vorgeschlagen. Der erste Geschäftsauftrag für R3 CEV, ein Blockchain-Start-up, in welches UBS neben Goldman Sachs, JPMorgan und 22 anderen Banken investiert hat, ist die Entwicklung einer standardisierten Architektur für private digitale Register.

Das zugrundeliegende Problem beschränkt sich nicht auf Banken. Unternehmen und öffentliche Einrichtungen aller Art leiden unter schwer zu pflegenden und oft nicht kompatiblen Datenbanken und den hohen Transaktionskosten, die damit verbunden sind, sie miteinander kommunizieren zu lassen. Dieses Problem will Ethereum, das wohl ehrgeizigste Projekt im Zusammenhang mit dezentralen Registern, lösen. Ethereums Blockchain ist die Idee von Vitalik Buterin, einem 21-jährigen kanadischen IT-Wunderkind, und soll in der Lage sein, mehr Daten zu verarbeiten als die Blockchain von Bitcoin. Geschrieben wird Ethereum in einer Programmiersprache, mit der Anwender noch anspruchsvollere, intelligente Verträge verfassen können: So können zum Beispiel Rechnungen erstellt werden, die sich selbst bezahlen, wenn eine Lieferung getätigt worden ist, oder Aktienzertifikate ausgestellt werden, die ihren Besitzern automatisch Dividenden ausschütten, wenn die Gewinne ein bestimmtes Niveau erreicht haben. Diese Art von künstlicher Intelligenz, so hofft Buterin, wird die Bildung von „dezentralen autonomen Organisationen“ ermöglichen – virtuellen Unternehmen, die eigentlich nur Regelsätze sind, die auf Ethereums Blockchain ausgeführt werden.

Eines der Gebiete, auf denen solche Ideen radikale Auswirkungen haben könnten, ist das „Internet der Dinge“, ein Netzwerk von Milliarden von bislang stummen Alltagsgegenständen wie Kühlschränken, Türstoppern und Rasensprengern. Ein kürzlich veröffentlichter Bericht von IBM mit dem Titel „Device Democracy“ argumentiert, dass es unmöglich wäre, den Überblick zu behalten, wenn man diese Milliarden von Geräten zentral verwalten wollte, und dass es

unklug wäre, es überhaupt zu versuchen. Solche Versuche würden diese Gegenstände anfällig für Hacker-Angriffe und Überwachung durch Regierungen machen. Dezentrale Register scheinen eine gute Alternative hierzu zu sein.

Die Programmierbarkeit, die Ethereum bietet, ermöglicht es nicht nur, das Eigentum von Benutzern zu registrieren und zu verfolgen. Sie ermöglicht es auch, es auf neue Art zu nutzen. So kann ein Autoschlüssel, der in der Blockchain von Ethereum eingebettet ist, auf viele, regelbasierte Arten verkauft oder vermietet werden, sodass neue Peer-to-Peer-Systeme für die Vermietung oder den Verleih von Autos entstehen könnten. Visionäre sprechen bereits davon, die Technologie in selbstfahrenden Autos einzusetzen und diese vollständig autonom werden zu lassen. Solche Fahrzeuge könnten einen Teil des digitalen Geldes, das sie durch die Vermietung ihrer Schlüssel verdienen, darauf verwenden, nach vorprogrammierten Regeln Treibstoff, Reparaturen und Parkplätze zu bezahlen.

Was hätte Rousseau wohl dazu gesagt?

Es kann kaum überraschen, dass manche solche Pläne für zu ehrgeizig halten. Ethereums erster Block (der „Genesis"-Block) wurde erst im August erstellt, und obwohl sich ein kleines Ökosystem von Start-ups um Ethereum gebildet hat, hat Buterin kürzlich in einem Blog-Post eingeräumt, dass das Projekt zurzeit etwas knapp bei Kasse ist. Doch die Details darüber, welche Blockchains am Ende Erfolg haben werden, sind weit weniger bedeutungsvoll als die große Begeisterung für die Idee der dezentralen Hauptbücher, die sowohl Start-ups als auch große, etablierte Unternehmen dazu animiert, ihr Potenzial zu untersuchen. Obwohl Buchhalter von der Gesellschaft oft als Witzfiguren verlacht werden, ist die Funktionsweise von Registern durchaus wichtig.

Die Welt ist heute nämlich zutiefst abhängig von doppelter Buchführung. Das standardisierte System, mit dem Soll und Haben minutiös festgehalten werden, ist Grundlage für jeden Versuch, die finanzielle Lage eines Unternehmens zu verstehen. Ob der moderne Kapitalismus diese Art der Buchführung unbedingt für seine Entwicklung benötigte, wie der deutsche Soziologe Werner Sombart Anfang des 20. Jahrhunderts behauptete, bleibt ungeklärt. Obwohl das System unter italienischen Kaufleuten in der Renaissance entstanden ist – was eine interessante Koinzidenz des Timings darstellt – hat es sich viel langsamer in der Welt verbreitet als der Kapitalismus und stieß erst im späten 19. Jahrhundert auf breiten Zuspruch. Klar ist jedoch, dass die Technik von grundlegender Bedeutung ist. Nicht nur als Aufzeichnung dessen, was ein Unternehmen tut, sondern auch als eine Möglichkeit, zu definieren, was es sein könnte.

Register, die nicht mehr von einem Unternehmen oder Staat gepflegt werden müssen, könnten mit der Zeit verändern, wie Unternehmen und Staaten funktionieren, was von ihnen erwartet wird und was ohne sie getan werden kann. Die Erkenntnis, dass Systeme ohne zentrale Aufzeichnungen genauso vertrauenswürdig sein können, wie diejenigen mit, könnte radikale Veränderungen herbeiführen.

Ideen dieser Art müssen mit einiger Skepsis rechnen. Blockchains sind noch immer ein Novum, das nur in wenigen Nischen Anwendung findet, und die Zweifel daran, inwieweit sie verbreitet

und erweitert werden können, mögen durchaus begründet sein. Solche Ideen stoßen auch immer auf Widerstand. Einige Kritiker sehen Bitcoin schon lange als letzten Versuch der Technologie-Jünger an, eine „kalifornische Ideologie“ zu verbreiten, die Erlösung durch technologie-induzierte Dezentralisierung verspricht, während sie gleichzeitig die Realitäten der Macht ignoriert und verschleiert – und gerne hinnimmt, dass großer Reichtum in den Händen einiger Weniger konzentriert wird. Die Idee, Vertrauen zu einer Frage des Programmcodes zu machen, anstatt von demokratischer Politik, Legitimität und Verantwortung, ist nicht unbedingt ansprechend oder beflügelnd.

Auf der anderen Seite hätte eine Welt mit einer Buchhaltung, die mathematisch immun gegen Manipulation ist, viele Vorteile. In einer solchen Welt wäre es Mariana Catalina Izaguirre besser ergangen. Gleiches gilt für viele andere Menschen in vielen anderen Situationen. Das grundlegende Paradox der Blockchain ist folgendes: Gerade weil sie eine Möglichkeit bietet, Vergangenheit und Gegenwart in kryptographischen Stein zu meißeln, könnte sie der Zukunft eine neue Richtung weisen.