Donnerstag, 04. Februar 2021, 14:00 Uhr
~17 Minuten Lesezeit

Die Geldrevolution

Die Blockchain-Technologie ist mehr als nur ein neues Zahlungsmittel — sie könnte ganze Branchen und sogar unser Zusammenleben grundlegend verändern.

von Dharmendra Laur
Foto: NicoElNino/Shutterstock.com

Die Geschichte beschleunigt sich. Vor allem die der Technologie. Die Behauptung, eine bestimmte Innovation werde eine neue Epoche der Menschheit einleiten, wird derzeit eher inflationär gebraucht. In diesem Fall könnte sie aber zutreffen. Denn die beiden entscheidenden Domänen Geldsystem und Digitalisierung sind gleichermaßen betroffen. Vor etwa elf Jahren erblickte eine bis dahin unbekannte Technologie das Licht der Welt. Ihr Name lautet Blockchain. Sie schafft neue Möglichkeiten der verbindlichen Interaktion zwischen zwei oder mehr Parteien, die auf einer bisher unbekannten Form

gegenseitigen Vertrauens beruhen. Dieser Artikel gibt eine Übersicht darüber, was eine Blockchain ist, wie sie funktioniert, welches Potenzial sie bietet und was schon heute Realität ist.

Bahnbrechende, technologische Entwicklungen entstehen häufig beinahe als Nebenprodukt. Die Dampfmaschine wurde zunächst hauptsächlich als Antrieb von Pumpen zur Entwässerung von Bergwerksgruben entwickelt und eingesetzt. Sie löste damit zwar ein wichtiges Problem ihrer Zeit, ihr Potenzial ist jedoch nicht auf das Pumpen von Wasser beschränkt. Vielmehr erlaubte sie erstmals, die von brennenden Stoffen erzeugte Wärme in Bewegung umzuwandeln.

Ähnlich verlief die Geschichte des Internets. Sie begann Ende der 1960er Jahre mit der Entwicklung des sogenannten Arpanets. Dessen Bestrebung war es, Großrechner von Universitäten und Forschungseinrichtungen miteinander zu vernetzen, um deren Rechenleistung effizienter zu nutzen.

Im Falle der Dampfmaschine wie auch des Arpanets wurden für spezifische Probleme Lösungen entwickelt, deren prinzipielle Funktionsweisen viele Möglichkeiten eröffneten, die zuvor jenseits der Vorstellungskraft vieler Menschen gelegen hatten. Beide Technologien hielten im Laufe der Zeit Einzug in viele traditionelle Lebensbereiche, veränderten diese teils grundlegend und eröffneten darüber hinaus noch völlig neue, zuvor nur schwer vorstellbare Möglichkeiten.

Mit Bitcoin erblickte vor elf Jahren vielleicht eine Technologie ähnlichen Ausmaßes das Licht der Welt. Bitcoin wurde als neue,

dezentralisierte Währung erdacht und erfüllt diese Funktion bis heute zuverlässig. Es ist eine neue Form des Geldes und stellt für sich genommen bereits eine große technische Neuerung dar.

Doch ähnlich zu Dampfmaschine und Internet steht hinter Bitcoin eine Erfindung, die womöglich noch weit umfassendere Auswirkungen auf unsere Gesellschaft haben wird. Diese neue Erfindung heißt Blockchain. Sie verspricht eine neue Art, wie wir einander vertrauen können.

Eine neue Art von Supercomputer

Das Prinzip der Blockchain habe ich bereits in einem vorigen Artikel ausführlich vorgestellt. Zusammengefasst beschreibe ich die Blockchain darin als digitales Register mit besonderen Eigenschaften. In diesem Register können praktisch alle Formen von digitalen Daten verlässlich, transparent und dezentral abgespeichert und verändert werden. Bei dezentralisierten Währungen wie Bitcoin werden hauptsächlich Daten über Kontostände und deren Veränderungen durch Transaktionen im Register der Blockchain gespeichert.

Auf neueren, Blockchain-basierten Plattformen können wesentlich mehr — eigentlich praktisch alle — Arten von digitalen Daten gespeichert werden und sie bieten eine Vielzahl an Möglichkeiten, mit diesen Daten zu arbeiten. Während Bitcoin nur simple Rechenoperationen wie Addition und Subtraktion beherrscht, beherrschen neuere Blockchain-basierte Plattformen wie Ethereum nahezu alle Rechenoperationen, die auf einem normalen Computer auch möglich sind.

Der Begriff Supercomputer bezeichnet üblicherweise Großrechner, die ganze Hallen füllen und ihrerseits teils aus tausenden,

miteinander verschalteten Komponenten bestehen. Im Verbund agieren alle Bestandteile eines solchen Supercomputers wie ein einziger Rechner, der über ein Vielfaches der Ressourcen gewöhnlicher Computer verfügt und somit rechenintensive Aufgaben schnell erledigen kann.

So wie alle Blockchain-basierten Systeme basiert auch Ethereum auf einer dezentralen Architektur. Viele einzelne Rechner, verteilt über die ganze Welt, sind über das Internet miteinander verbunden und bilden das Ethereum-Netzwerk. Sie kommunizieren auf eine bestimmte, festgelegte Weise miteinander und agieren dadurch — ähnlich wie klassische Supercomputer — im Verbund wie ein einziger Großrechner. Auch hinsichtlich ihrer Rechenleistung sind Blockchain-Systeme mit Supercomputern vergleichbar und übertreffen sie teils deutlich.

So verfügt das Bitcoin-Netzwerk über etwa dreihundertmal mehr Rechenleistung als der schnellste Supercomputer der Welt. Kein anderes Blockchain-Netzwerk vereint soviel Rechenleistung auf sich, wie Bitcoin. An zweiter Stelle folgt Ethereum, das immer noch etwa achtmal mehr Rechenkapazität besitzt, als sein schnellster, zentralisierter Kollege. Leider fordert hohe Leistung ihren Tribut häufig in Form großen Energiebedarfs. Hierauf komme ich später noch einmal zurück.

> ***Blockchain-Netzwerke können also aus vielerlei Hinsicht als Supercomputer angesehen werden. Anders als bei ihren traditionellen Pendants dient ihre Rechenleistung jedoch nicht der schnellen Bearbeitung von aufwendigen Modellrechnungen, sondern der Sicherung des Netzwerkes.***

Wie bereits erwähnt, folgt die Kommunikation der Rechner innerhalb des Netzwerkes bestimmten Regeln. Anders ausgedrückt, halten sich alle Netzwerkteilnehmer an ein bestimmtes Protokoll,

das vorgibt, wie innerhalb des Netzwerkes kommuniziert wird. Dieses Protokoll wird Konsens-Protokoll oder auch Konsens-Mechanismus genannt. Der Name kommt daher, dass die Kommunikationsregeln dazu dienen, Einigkeit, also einen Konsens, unter allen Teilnehmern des Netzwerkes darüber herzustellen, welche Berechnungen des Netzwerkes als valide akzeptiert werden.

Die Verwendung von Konsens-Protokollen, ist für die sehr hohe Verlässlichkeit von Blockchain-basierten Systemen essentiell. Ebenso wichtig hierfür ist, dass kein einzelner Akteur im Netzwerk den Konsens-Mechanismus eigenmächtig ändern kann und Veränderungen für jeden frühzeitig und transparent nachvollziehbar sind.

So ermöglichen Plattformen wie Ethereum etwas, das im englischen häufig „Trusted Computing" genannt wird und übersetzt etwa bedeutet: Vertrauenswürdiges oder verlässliches Berechnen. Das wirklich Neue daran ist, dass diese Systeme ihre Vertrauenswürdigkeit im Prinzip aus der Abwesenheit von Vertrauen erzeugen. Darauf komme ich später noch einmal zurück.

Digitales Öl

Eine Blockchain abzusichern benötigt viele Ressourcen und verursacht damit hohe Kosten. Daher bieten Blockchain-basierte Systeme wie Bitcoin und Ethereum Anreizsysteme in Form von Verdienstmöglichkeiten für jeden, der Rechenleistung zur Absicherung ihrer Netzwerke bereitstellt. Ethereum ermöglicht dazu eine Vergütung in einer eigenen Währung, die Ether genannt wird. Wie Bitcoin ist Ether eine sogenannte Kryptowährung. Das ist der Sammelbegriff für alle Währungen, die auf der Blockchain-Technologie basieren und er rührt daher, dass Kryptographie — also Verschlüsselungstechniken — eine wesentliche Rolle bei dieser

Technologie spielen.

Wenn man Bitcoin mit digitalem Gold vergleicht, dann ist Ether so etwas wie digitales Öl, denn es ist gewissermaßen der Treibstoff von Etherum. Alle Berechnungen, die das Ethereum-Netzwerk ausführt, müssen in der Währung Ether bezahlt werden. Die Höhe des Preises richtet sich nach dem Aufwand, den die angeforderte Aktion für das Netzwerk bedeutet.

Die Kosten für Rechenoperationen auf den neuen Supercomputern übersteigen diejenigen bei klassischen Computern um ein Vielfaches. So kostet es beispielsweise etwa 17.500 Ether, um ein Gigabyte an Daten auf der Ethereum-Blockchain zu speichern. Das entspricht bei einem Preis von derzeit circa 500 Euro pro Ether knapp neun Millionen Euro für die Datenmenge eines zehn-minütigen Videos. Ethereum und andere Blockchain-basierte Systeme sind somit nicht für die gleichen Aufgaben geeignet wie klassische Computer.

Die Erträge aus den Gebühren werden an diejenigen ausgezahlt, die Rechenleistung zur Absicherung des Netzwerkes bereitstellen. So entsteht ein stabiler Wirtschaftskreislauf, in dem die Ether-Coins ständig zwischen denjenigen zirkulieren, die die technische Infrastruktur für Ethereum bereitstellen, und den Nutzern der Plattform. Dieser Kreislauf sorgt dafür, dass das Netzwerk aufrechterhalten wird und verfügbar bleibt. Doch wozu?

Intelligente Verträge

Für den Einsatz der Blockchain eignen sich vor allem Vorgänge von relativ geringem Rechenaufwand, die zuverlässig, vorhersehbar und überprüfbar ablaufen müssen. Die gleichen Anforderungen finden sich bei einer zivilisatorischen Errungenschaft, die unser Leben bis

heute entscheidend prägt: Verträge.

Verträge beinhalten eine oder mehrere Bedingungen, die erfüllt werden müssen, um bestimmte Folgeereignisse auszulösen. Ein Beispiel ist ein Grundstückskaufvertrag, bei dem die Bedingung für den Eigentümerwechsel eines Grundstücks der Eingang eines festgelegten Betrages auf ein bestimmtes Konto ist. Sobald das Geld auf das entsprechende Konto eingegangen ist, folgt in der Regel zwingend der Übertrag des Grundstückes auf den Käufer.

Prinzipiell ist dies ein rein datenbasierter Vorgang, der im Kern nur die Veränderung zweier Informationszustände umfasst. Erstens muss der Kontostand des bestehenden Eigentümers um den Kaufbetrag ansteigen und zweitens muss daraufhin der Name des bestehenden Eigentümers im Grundbuch durch den des neuen Eigentümers ersetzt werden. Zusätzlich werden noch ein oder mehrere vertrauenswürdige Akteure benötigt, die beide Operationen verlässlich durchführen können.

Grundstücksübertragungen sind gewöhnlich mit hohen Kosten verbunden. Nach anfallenden Steuern machen Gebühren für Notar und Grundbuchamt häufig den größten Anteil der Kaufnebenkosten aus. Im Prinzip fallen diese Gebühren nur an, weil der Vorgang möglichst zuverlässig, vorhersehbar und überprüfbar ablaufen muss. Alle Aufgaben des Grundbuchamtes sowie des Notars können von einem Supercomputer wie Ethereum übernommen werden, der dabei viel schneller arbeitet, und das bei gleich bleibender Sicherheit und zu einem Bruchteil der Kosten.

Aus technischer Sicht ist es leicht möglich, die Eigentumsverhältnisse von Grundstücken an Datensätze in einer Blockchain zu binden und in diesem Feld sind bereits einige Unternehmen aktiv. Ethereum übernimmt dabei die Verwaltung aller relevanten Daten und führt alle nötigen Prozesse automatisiert aus. Operationen wie das Überprüfen von Kontoständen und das

Ändern von Einträgen in digitalen Grundbucheinträgen benötigen sehr wenig Rechenleistung und ihre Kosten auf der Blockchain bewegen sich typischerweise im Bereich von wenigen Cent bis zu ein paar Euro. Einen auf einer Blockchain abgeschlossenen Vertrag kann keine Partei eigenmächtig ändern, alle relevanten Informationen sind jederzeit für alle einsehbar und der Supercomputer garantiert die Erbringung der vereinbarten Leistung und führt sie automatisiert aus.

Am Beispiel des Grundstückseigentümerwechsels wird das Potenzial Blockchain-basierter Systeme deutlich. Die typischerweise anfallenden Gebühren in Höhe von etwa zwei Prozent des Grundstückskaufpreises verringern sich auf wenige Euro und der nötige Aufwand schrumpft auf ein Minimum.

Blockchain-basierte Plattformen können Verträge automatisiert und in Echtzeit verwalten, überprüfen und ausführen. Verträge dieser Art werden daher „Smart Contracts" genannt, was mit „intelligente Verträge" übersetzt werden kann. Im Prinzip handelt es sich bei intelligenten Verträgen um vollständige Computerprogramme mit der Eigenschaft, dass sie besonders zuverlässig und transparent ausgeführt werden. Diese Programme können genauso komplex gestaltet werden, wie wir es von unseren Computern kennen. Sie werden dezentralisierte Applikationen oder "dApps" genannt, da sie auf dezentralisierten Systemen ausgeführt werden und viele Eigenschaften ihrer Plattformen erben.

Mehr als nur Verträge

Smart Contracts und dApps erschaffen viele neue Anwendungsbereiche und besitzen das Potenzial, ganze Wirtschaftsbereiche zu transformieren. Die wohl am weitesten entwickelten, dezentralisierten Applikationen gehören zu einem

Bereich, der dezentralisiertes Finanzwesen oder kurz „DeFi" genannt wird.

Das neue, dezentralisierte Finanzwesen bietet alle wesentlichen Funktionen des klassischen zentralisierten Finanzwesens. Dort ist es möglich, Kredite aufzunehmen, in Fonds und Projekte zu investieren, Werte zu handeln und noch einiges mehr.

Vom klassischen Finanzwesen unterscheidet sich das dezentralisierte Finanzwesen vor allem in zwei Punkten: Erstens können dort bisher hauptsächlich Blockchain-basierte Währungen und Werte gehandelt werden. Und zweitens interagieren Käufer und Verkäufer auf dezentralisierten Marktplätzen direkt miteinander statt durch Mittelsmänner wie Banken oder Handelsbörsen.

Die Rolle der Vermittler übernehmen dezentralisierte Applikationen, die auf den neuen Supercomputern wie Ethereum ausgeführt werden. Abgesehen von möglichen, unentdeckten Programmierfehlern verhalten sich diese dezentralisierten Applikationen absolut vorhersehbar und verlässlich. In diesem Sinne gleicht ihr Verhalten mehr dem von Maschinen als demjenigen von Organisationen oder Institutionen, die von menschlichen Entscheidungen gesteuert werden. Damit erhalten sie den Charakter von Werkzeugen, die es Marktteilnehmern ermöglichen, miteinander in Austausch zu treten, ohne sich gegenseitig vertrauen oder auch nur kennen zu müssen.

Das Prinzip der direkten Interaktion gilt sowohl für dezentrale Handelsplätze als auch das digitale Kreditwesen, das es Besitzern von Kryptowährungen erlaubt, diese gegen einen Zins zu verleihen. Ein Smart Contract verwaltet die zugrunde liegende Sicherheit des Kreditnehmers treuhänderisch und garantiert dem Kreditgeber, dass er sein Geld zurückerhält.

> ***Die verlässliche und automatisierte Ausführung von Finanzgeschäften ohne Mittelsmänner zwischen Marktteilnehmern ist das zentrale Merkmal des dezentralen Finanzwesens.***

Durch das Wegfallen der Mittelsmänner entfallen auch etwaige Zugangshürden, die durch Finanzinstitutionen der zentralisierten Finanzwelt auferlegt werden. Bereits bestehende, dezentralisierte Finanzapplikationen ermöglichen schon heute, jedem, mit nur wenigen Euro, zum Kreditgeber zu werden oder in Start Ups zu investieren, ohne dass jemand sie oder ihn davon abhalten könnte. Bei vielen Finanzmarktprodukten des klassischen sowie des dezentralen Finanzsystems handelt es sich zwar im Wesentlichen um Wetten mit bestenfalls zweifelhaftem Nutzen für die Gesellschaft und deren Verbreitung sollte nicht zusätzlich durch neue Technologien gefördert werden.

Dennoch erachte ich dezentralisierte Finanzapplikationen als eine grundlegend positive Entwicklung. Sie ermöglichen erstmals praktisch jedem Zugang zu Finanzgeschäften, die zuvor nur wenigen vorbehalten waren. Welche Folgen das haben wird, ist schwer vorauszusehen. Ein Finanzwesen, das ohne Vertrauen in Mittelsmänner auskommt und zudem noch für jeden mit einem Smartphone zugänglich ist, scheint mir jedoch beachtliches Potenzial zu haben.

Probleme und Fragen

Gemessen an den Trillionen des klassischen Finanzsystems ist der Bereich dezentralisierter Finanzen noch klein. Dennoch werden schon jetzt Werte von über 700 Millionen US-Dollar pro Tag auf dezentralisierten Marktplätzen gehandelt, Tendenz stark steigend. Dabei ist der Finanzsektor nur einer von vielen, die sich durch Blockchain-Technologien stark verändern könnten. Das *Forbes*

Magazin veröffentlichte bereits im Jahr 2018 eine Liste mit zehn Bereichen, die möglicherweise davon betroffen sein werden. Unter ihnen finden sich neben dem Bank- und Immobiliensektor auch Bereiche wie Politik, Rechtswesen, Gesundheitswesen und Bildung.

Einzelne Analysten identifizieren über fünfzig Gesellschaftsbereiche, denen aufgrund der Blockchain tiefgreifende Veränderungen bevorstehen und im Januar 2021 kürte das auf Geschäftskontakte ausgerichtete, soziale Netzwerk *LinkedIn* Blockchain-Entwicklung zur wichtigsten Fähigkeit für 2020. Viele Anzeichen deuten derzeit darauf hin, dass die Verbreitung von Blockchain-Technologien in den kommenden Jahren stark zunehmen und Einzug in immer mehr Lebensbereiche halten wird.

Obwohl in einigen Bereichen schon heute gut funktionierende, dezentralisierte Anwendungen existieren, sind bis zur Massenverbreitung noch einige Probleme zu lösen und Fragen zu beantworten.

So gibt es häufig kaum oder gar keine gesetzliche Regulierung und auch kaum Garantien oder Rückversicherungen bei der Nutzung von Blockchain-Technologien. Zwar garantieren die neuen Supercomputer die Ausführung von intelligenten Verträgen exakt so, wie deren Programmierung es festschreibt. Sind die Verträge jedoch selbst bereits fehlerhaft programmiert, existiert derzeit meist keine Möglichkeit, dadurch entstandene Schäden zu kompensieren. Zahlreiche Beispiele von digitalen Diebstählen, bei denen Diebe Schwachstellen in der Programmierung von Smart Contacts ausbeuteten, um das von Smart Contracts verwaltete Vermögen zu entwenden, zeugen von den teils hohen Risiken dieser neuen Technologie in ihren Kinderschuhen.

In solchen Fällen wird eine große Innovation der Blockhain-Technologie zum Nachteil. Viele dezentrale Systeme verfügen nicht über Autoritäten, die in Prozesse eingreifen oder sie rückgängig

machen könnten. Für Betroffene bedeutet das in der Regel den Totalverlust ihrer eingezahlten Beträge.

Zukünftige Regulierungen und technische Weiterentwicklungen werden dieses Problem wahrscheinlich lösen. So verkündete der Finanzminister der USA, Steven Mnuchin, dass er noch vor Ende der Legislaturperiode ein Gesetz verabschieden möchte, das eine staatliche Registrierung der bisher praktisch völlig anonymen Kontoadressen von Kryptowährungen in bestimmten Fällen vorschreibt. Offiziell möchte die US-amerikanische Regierung damit zur Bekämpfung illegaler Aktivitäten beitragen. In Wirklichkeit geht es dabei wohl ebenso sehr um die Ausdehnung staatlicher Kontrolle auf diesen neuen und noch ungezähmten Bereich. Die entstehende regulatorische Sicherheit wird sich wohl dennoch positiv auf Akzeptanz und Verbreitung der neuen Technologie auswirken.

Dennoch bringt die von Blockchain-basierten Systemen gebotene Autonomie auf absehbare Zeit ein erhöhtes Maß an Eigenverantwortung mit sich. Ein gewisser Wissensstand und Sicherheit im Umgang mit der Technologie sind daher Voraussetzung, um Schäden zu vermeiden. Zwar ist die Nutzung dezentraler Finanzapplikationen prinzipiell kinderleicht mit dem Smartphone möglich. Nötig ist dazu nur eine entsprechende App, in der man mit wenigen Eingaben Kryptowährungen gegeneinander umtauschen kann. Um jedoch nicht den Gefahren von Betrug und anderen Möglichkeiten des Verlustes zu erliegen, ist ein tieferes Verständnis der zugrunde liegenden Technologien und Abläufe sehr ratsam.

Entsprechende Bildungsangebote sind zahlreich im Internet vorhanden, selten jedoch in deutscher Sprache und häufig ausgerichtet auf ein junges und Technologie-affines Publikum. Jeder der das dezentralisierte Finanzwesen nutzen möchte, sollte daher eine große Bereitschaft mitbringen, sich in das Thema einzuarbeiten.

Kinderkrankheiten

Frühe Anwendungen neuer Technologien leiden häufig an Kinderkrankheiten. Bitcoin gehört zur ersten Generation Blockchain-basierter Systeme und obwohl es stets weiterentwickelt wird, ist seine Technologie in gewisser Weise bereits veraltet und im Vergleich zu neueren Blockchain-Systemen langsam, behäbig und unausgereift. So kann das Bitcoin-Netzwerk nur etwa sieben Transaktionen pro Sekunde verarbeiten und liegt damit weit entfernt von der Kapazität des Kreditkartenunternehmens Visa mit über fünfzigtausend Transaktionen pro Sekunde.

Als Vertreter der zweiten Generation Blockchain-basierter Netzwerke bietet Ethereum nicht nur mehr Funktionen als Bitcoin, kann auch beinahe doppelt so viele Transaktionen pro Sekunde bearbeiten. Jedoch reicht auch dieser Wert nicht für eine Massenverbreitung aus.

Der Grund für die Transaktionskapazitäten früher Blockchain-Systeme liegt in deren Konsens-Mechanismen. Erinnern wir uns: Die Konsens-Mechanismen oder Konsens-Protokolle geben Kommunikationsregeln vor, mit deren Hilfe alle Teilnehmer der dezentralisierten Netzwerke Einigkeit darüber erlangen, welche Berechnungen und Ergebnisse sie als valide ansehen und welche nicht.

Ältere Konsens-Protokolle, wie die von Bitcoin und Ethereum, setzen auf ein Verfahren, das „Proof of Work" — zu deutsch etwa: Nachweis geleisteter Arbeit — genannt wird. Sie beruhen darauf, dass alle Akteure, die ein Netzwerk absichern, gleichzeitig an der Lösung desselben mathematischen Rätsels arbeiten. Die hierfür notwendigen Rechenoperationen erfordern eine bestimmte Menge an Arbeit oder Energie. Jede vorhandene Lösung ist daher ein Nachweis darüber, dass die entsprechende Energie aufgebracht

wurde, um sie zu finden. Im nächsten Schritt nutzt das Netzwerk solche Lösungen als Zertifikate, um die Echtheit von neuen Einträgen in das Register der Blockchain zu bestätigen.

Ein Paket von Einträgen in die Blockchain und ihr zugehöriges Zertifikat wird Block genannt. Neue Blocks werden kontinuierlich erzeugt und an die bereits bestehenden angehängt. So entsteht eine, sich ständig verlängernde, Kette von Blocks, also eine Blockchain.

Arbeit gegen Bürgschaften

Bitcoin und Ethereum verwenden den Hauptanteil ihrer Rechenleistung zur Berechnung der Zertifikate, die die Echtheit ihrer Daten garantieren. Dieses Verfahren bietet ein sehr hohes Maß an Sicherheit, führt jedoch auch dazu, dass wenig Kapazität für die eigentlichen Programme der dezentralisierten Supercomputer übrig bleibt. Das macht sie zwar sicher, aber auch langsam.

Findige Entwickler erkannten dieses Problem schon früh und fragten sich, wie ein größerer Teil der verfügbaren Rechenleistung für die Ausführung von Programmen genutzt werden könnte. So entstand eine neue Form von Konsens-Protokollen oder Konsens-Mechanismen, die „Proof-of-Stake" — zu deutsch etwa „Nachweis einer Einlage" — genannt werden.

Der Hauptunterschied zwischen Proof-of-Stake und Proof-of-Work basierten Blockchains besteht in dem Verfahren, mit dessen Hilfe die Zertifikate zur Verifizierung der Registereinträge erzeugt werden. Statt mit hohem Energieaufwand werden Blocks des neuen Typs durch Bürgschaften abgesichert. Die neuen Zertifikate entstehen, indem sie von Prüfern unterschrieben werden, die mit einem Teil ihres Vermögens für die Korrektheit ihrer Unterschrift

bürgen. Signieren sie gefälschte oder anderweitig fehlerhafte Einträge, wird, je nach Schwere des Vergehens, automatisch ein bestimmter Betrag des eingelegten Vermögens als Strafe eingezogen. Zur Gegenleistung erhalten sie eine Rendite auf ihr gebundenes Kapital.

So wird nur ein Bruchteil der Rechenleistung für die Zertifizierung aufgewendet und sowohl Transaktionskapazität als auch Energiebedarf verbessern sich um mehr als das Tausendfache. Erkauft werden diese Vorteile durch ein verringertes Maß an Sicherheit. Wie viel Sicherheit dabei für Geschwindigkeit und Energieeffizienz tatsächlich geopfert wird, lässt sich nur schwer beziffern und ist Gegenstand lebhafter Debatten unter Entwicklern. Fest steht jedoch, dass neuere Blockchains fast ausschließlich auf Proof-of-Stake basieren und die gebotene Sicherheit für die meisten Anwendungsfälle auszureichen scheint.

Mit den neuen, auf Bürgschaften basierenden Zertifikaten werden zwanzigtausend Transaktionen pro Sekunde möglich. Blockchain-basierte Netzwerke erreichen somit etwa die Kapazität des Kreditkartenanbieters Visa.

Wo geht die Reise hin?

Wie wir gesehen haben, können mithilfe der Blockchain neue Supercomputer erschaffen werden. Sie bieten neue Werkzeuge, mit deren Hilfe zwei oder mehr Parteien verbindlich miteinander in Austausch treten können. Dazu müssen sie sich weder gegenseitig kennen oder vertrauen, noch benötigen sie Mittelsmänner.

Wie sich diese neuen Werkzeuge langfristig auf unsere Gesellschaft auswirken werden, ist schwer abzuschätzen. Auch das volle Potenzial der Dampfmaschine musste allmählich entdeckt werden.

Vor ihrem Aufkommen dachte kaum jemand darüber nach, was man mit so einer Maschine anfangen könnte. Entsprechend brauchte es Zeit, Ideen zu entwickeln und umzusetzen. Ähnlich verlief die Geschichte des Internets.

Diese zunächst unspektakulär anmutende Verbindung von Computern hat viele Bereiche unserer Gesellschaft in wenigen Jahrzehnten umgeformt oder überflüssig gemacht. Dafür wurden mit ihrer Hilfe neue Felder geschaffen, die zuvor kaum denkbar schienen. Große Innovationen finden ihre Anwendungsmöglichkeiten oft erst allmählich.

Die Blockchain schafft eine neue Art, Vertrauen zu schaffen. Durch sie können wir Vertrauen gegenüber Autoritäten durch Vertrauen zu bestimmten, mathematischen Gesetzmäßigkeiten ersetzen.

An die Stelle des Vertrauens gegenüber einer Bank tritt eine Art des Vertrauens wie zu einem Tresor. Ein Tresor ist möglicherweise leicht zu knacken oder weist andere Mängel auf. Er wird jedoch sicher niemals Einlagen veruntreuen oder seine Machtposition missbrauchen. Darauf ist Verlass.

Viele Anwendungsfälle für die Blockchain sind schon erdacht, einige bereits umgesetzt und ein paar wenige erfreuen sich breiter Nutzung. Viele Anwendungsmöglichkeiten müssen jedoch erst noch erdacht, entwickelt und eingesetzt werden, bevor das wahre Potenzial der Blockchain erkennbar wird. Welche Auswirkungen sie haben wird, müssen wir abwarten. Fest steht, dass sie uns neue, bisher unbekannte Werkzeuge an die Hand gibt. Was wir aus ihnen machen, liegt an uns.

Quellen und Anmerkungen:

Dieser Artikel erschien im **Tageslicht Magazin** (https://www.tageslicht-magazin.de/) unter dem Titel „**Die Besonderheit der Blockchain** (https://www.tageslicht-magazin.de/artikel/die-besonderheit-der-blockchain/)“.

Dieser Artikel erschien bereits auf www.rubikon.news.

Dharmendra Laur, Jahrgang 1991, ist studierter Physiker, politischer Aktivist bei der ganzheitlichen politischen Bewegung MENSCHLICHE WELT und Redakteur beim unabhängigen Magazin TAGESLICHT. Nach seinem Studium machte er die Spiritualität zu seinem Lebensmittelpunkt. Die systematische Entwicklung des eigenen Bewusstseins ist für ihn der beste Weg zu individueller und gesellschaftlicher Freiheit. Daran arbeitet er durch tägliche spirituelle Praxis und ganzheitliches, gesellschaftliches Engagement.