Programmiertes Vertrauen: Chancen und Risiken der Blockchain-Technologie

Kurzfassung der Studie «Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment»

Die Stiftung TA-SWISS, ein Kompetenzzentrum der Akademien der Wissenschaften Schweiz, setzt sich mit den Chancen und Risiken neuer Technologien auseinander.

Die hier vorliegende Kurzfassung basiert auf einer wissenschaftlichen Studie, die im Auftrag von TA-SWISS von zwei Projektteams unter der Leitung von Nils Braun-Dubler sowie Antoine Burret durchgeführt wurde. Die Kurzfassung stellt deren wichtigste Resultate und Schlussfolgerungen in verdichteter Form dar und richtet sich an ein breites Publikum.

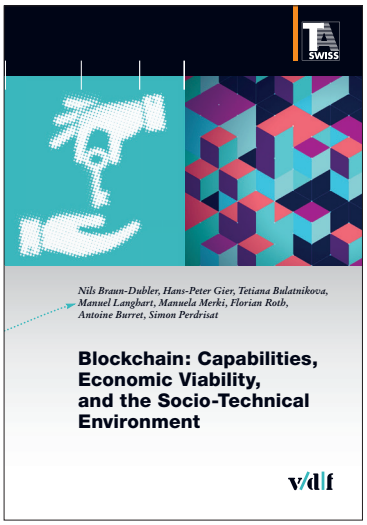
Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment

Nils Braun-Dubler, Hans-Peter Gier, Tetiana Bulatnikova, Manuel Langhart, Manuela Merki, Florian Roth, Antoine Burret, Simon Perdrisat

TA-SWISS, Stiftung für Technologiefolgen-Abschätzung (Hrsg.).
vdf Hochschulverlag an der ETH Zürich, 2020.
ISBN 978-3-7281-4016-6

Die Studie steht als eBook zum freien Download bereit: www.vdf.ch

Die vorliegende Kurzfassung ist ebenfalls online verfügbar: www.ta-swiss.ch



Eine kurze Einführung

Mit Libra, dem globalen Zahlungssystem von Facebook, hätte es endlich gelingen sollen: Erstmals würde eine Blockchain-basierte Anwendung im Alltag Einzug halten. Doch inzwischen stehen die Zeichen für den massentauglichen Durchbruch der Blockchain-Technologie eher wieder schlecht. Verschiedene der grossen, am Projekt beteiligten Player wie Visa, Mastercard oder PayPal sind noch vor dem für 2020 geplanten Start abgesprungen. Zu stark der Gegenwind, zu gross die Vorbehalte von Zentralbanken und Regierungen vor einer staaten- und bankenlosen parallelen Zahlungslösung, einer «privaten Weltwährung», die sich ihrer Kontrolle entziehen, der Geldwäscherei oder der Terrorismusfinanzierung dienen und das etablierte Finanzsystem destabilisieren könnte.

Die Schweiz – ein Blockchain-Land

Die Schweiz hat sich entschieden, auf das Potenzial der Blockchain-Technologie zu fokussieren, insbesondere was innovative Ansätze im Finanzmarkt betrifft. Und sie ist gut positioniert, um von der Blockchain-Technologie profitieren zu können. Dank ihrem liberalen Regulierungsrahmen hat sich im «Crypto-Valley» zwischen Zug und Zürich bereits eine sehr lebendige Community von Blockchain-Pionierinnen und -Pionieren etabliert. Die flexible und liberale Schweizer Schiedsgerichtbarkeit dürfte dazu führen, dass die Schweiz auch ein wichtiger Gerichtsstand für sogenannte Smart Contracts wird. Um den Blockchain-Standort zu stärken und weiter auszubauen, hat der Bund 2017 eine Taskforce ins Leben gerufen und ist bestrebt, die Rechtssicherheit rund um Blockchain-Anwendungen mit gezielten Gesetzesanpassungen zu erhöhen.

Eine Maschine, die Vertrauen fabriziert

Die Blockchain ist – stark vereinfacht gesagt – eine fälschungssichere, dezentral verwaltete Datenbank. Anstelle von klassischen Instanzen und (oft demokratisch legitimierten) Institutionen, die einen korrekten Ablauf aller Vorgänge garantieren, tritt bei der Blockchain das Vertrauen aller am System Beteiligten in ein transparentes und (theoretisch) absolut verlässliches technologisches System. Je mehr Akteure sich am Konsens beteiligen, desto mehr Vertrauen wird geschaffen und desto besser ist die Manipulationssicherheit gewährleistet. Nicht umsonst wird die Blockchain auch als eine Maschine bezeichnet, die Vertrauen herstellt. Eine Vertrauensmaschine mit dem Anspruch, das Internet zu einem «Internet der Werte» umzuwandeln, in dem auch Werte – zum Beispiel Geld, Landtitel, Versicherungsunterlagen oder Identitätsnachweise – sicher um die Welt zirkulieren.

Die virtuelle Währung Bitcoin, gefolgt von weiteren Kryptowährungen, war die erste Anwendung der Blockchain. Und gewiss auch die, die am stärksten zum zweifelhaften Nimbus der neuen Technologie beigetragen hat. Viele Digitalexpertinnen und Finanzexperten überschlugen sich schier vor Begeisterung über die Möglichkeiten dieser «wichtigsten Revolution seit Erfindung des World Wide Webs»; gleichzeitig setzte die in den dunklen Hintergassen des Internets beheimatete illegale Handelsplattform Silk Road Bitcoin als Zahlungsmittel für ihre fragwürdigen Geschäfte ein. Hinzu kamen wilde Spekulationen, Kursschwankungen und überzogene Erwartungen auf der einen und das bisherige Fehlen wirklich alltagstauglicher Anwendungen auf der anderen Seite: Das alles gehört zum Stoff, aus dem der Hype und die Legenden rund um die Blockchain geschneidert wurden. Weiter hinzu kommt die Komplexität eines informationstechnologischen Systems, das sich dem Verständnis der meisten Menschen entzieht. Und schliesslich die Tatsache, dass die grösste Stärke der Blockchain gleichzeitig auch ihre Achillesferse ist: Indem sie die herkömmlichen Kontrollinstanzen ausschaltet, wird sie letztlich nämlich selber zur Vertrauensinstanz. Aber taugt ein technisches System dazu, den Staat als «vertrauenswürdigen Dritten» zu ersetzen oder, je nach Anwendungsfeld, an Stelle der Finanzaufsicht, der Wahlbehörde oder der Notarin zu treten? Kann die Blockchain gar den Kapitalismus reformieren, wie manche ihrer heissesten Verfechter glauben? Die Antwort auf diese Frage ist gesellschaftspolitischer Art.

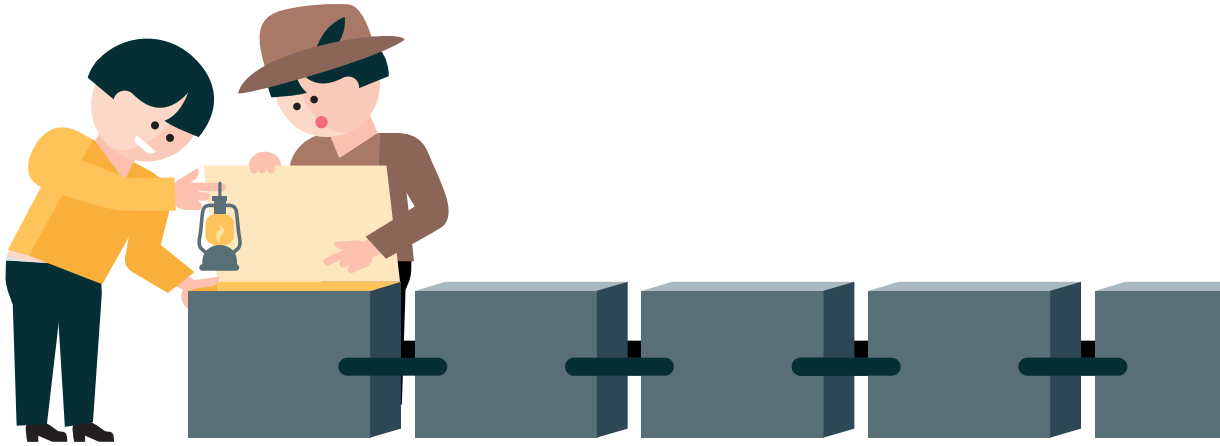
Dies die Ausgangslage, die die Stiftung für Technologiefolgen-Abschätzung TA-SWISS dazu bewegt hat, ihrem Mandat gemäss zuhanden von Politik und Öffentlichkeit eine umfassende Wissensgrundlage zu den Chancen und Risiken der Blockchain zu erabeiten.

Chancen der Blockchain

- ihre Unveränderbarkeit, die durch die Kryptographie und ein intelligentes Anreizsystem sichergestellt wird. Letzteres sorgt dafür, dass alle am Netzwerk Beteiligten für die Rechtmässigkeit aller Transaktionen bürgen.
- ihre dezentrale Natur, die das ganze System manipuliersicher macht.
- ihre Fähigkeit, Vertrauen zwischen Akteuren zu schaffen, die sich nicht oder kaum kennen.
- die Möglichkeit, Eigentumsrechte oder Herkunftsnachweise digital absolut glaubwürdig zu verbürgen. Dies verleiht der Blockchain das Potenzial, den Bereich der Finanzdienstleistungen grundlegend zu erneuern.
- die Aussicht, dass Transaktionen durch das Ausschalten von Intermediären rascher, günstiger und weniger fehleranfällig werden.
- die Transparenz und Unveränderbarkeit der gesicherten Information, welche die Rechtssicherheit erhöhen. Das kann insbesondere in Ländern, denen eine vertrauenswürdige oder effiziente Zentralinstanz fehlt, ein grosser Vorteil sein.
- der Umstand, dass die Blockchain – kombiniert mit intelligenten Verträgen und mit dem Internet of Things – die Automatisierung von Überprüfungsprozessen und Gültigkeitsnachweisen ermöglicht.

Risiken der Blockchain

- dass manche der Konsensmechanismen, die in der Blockchain eine zentrale Vertrauensinstanz ersetzen, eine enorme und auf eine Vielzahl von Computern verteilte Rechenleistung erfordern und damit auch Unmengen an Energie verbrauchen.
- dass die Nutzer und Nutzerinnen an öffentlichen Blockchains anonym bzw. mit einem Pseudonym teilnehmen, was für kriminelle Zwecke missbraucht werden kann.
- dass sämtliche, jemals von einer Person getätigte Transaktionen einsehbar werden, sobald die Identität eines Pseudonyms bekannt ist.
- dass die Unveränderbarkeit der Blockchain ein Recht auf Vergessen, wie es der Datenschutz vorsieht, vollständig ausschliesst.
- dass die Blockchain zwar mehr Transparenz und gemeinsames Entscheiden verspricht, gleichzeitig ihrer Komplexität wegen für Laien aber vollständig undurchsichtig bleibt.
- dass die Blockchain weitgehend eine «Lösung ohne Problem» bleibt. Denn bislang fehlt eine «Killerapplikation», und die Blockchain kann dem Hype, der um sie gemacht wird, nicht gerecht werden.



Doppelfokus

Es ist eine zweiteilige Studie, die TA-SWISS zur Blockchain-Technologie vorlegt. Der erste, technischere Teil gibt einen fundierten Einblick in die Funktionsweise der Blockchain und analysiert ihr wirtschaftliches Potenzial. Weiter zeigt er anhand von zwölf Fallstudien, wo Blockchain-Anwendungen gegenüber herkömmlichen Anwendungen im selben Bereich tatsächlich einen Vorteil bringen und wo sie (noch) nicht wirklich überzeugen. Die Beispiele reichen von öffentlichen Grundbüchern über Zahlungssysteme in Flüchtlingslagern bis zur Energieversorgung. Durchgeführt wurde dieser erste Teil von einem Projektteam des Instituts für Wirtschaftsstudien Basel (IWSB) unter der Leitung von Nils Braun-Dubler, in Zusammenarbeit mit der Managementberatungsgesellschaft Banking Concepts und dem Anwalts-, Steuer- und Compliance Unternehmen MME. Der zweite Teil der Studie reiht die Blockchain, ihre Entstehungsgeschichte und ihre Wahrnehmung in einen soziologischen und kulturellen Kontext ein. Er untersucht dabei insbesondere, wie sich die Undurchsichtigkeit des Systems für Laien auf den gesellschaftlichen Diskurs rund um die Blockchain auswirkt und in wessen Interesse es ist, diesbezüglich einen gewissen Hype aufrechtzuerhalten. Dieser zweite Teil stammt aus der Feder der Soziologen Antoine Burret und Simon Perdrisat vom Centre Universitaire Informatique der Universität Genf.

Zusammengenommen bilden die beiden Teile eine umfassende Bestandsaufnahme. Sie soll dabei helfen, etwas Luft aus der Blase der Aufregung und der oft genauso überzogenen Erwartungen wie Befürchtungen und Abwehrreaktionen rund um die Blockchain-Technologie zu lassen und die Debatte um deren wirtschaftliche und gesellschaftliche Bedeutung sowie ihre gegenwärtigen und zukünftigen Anwendungen auf eine sachliche Grundlage zu stellen.

Ein Blick zurück

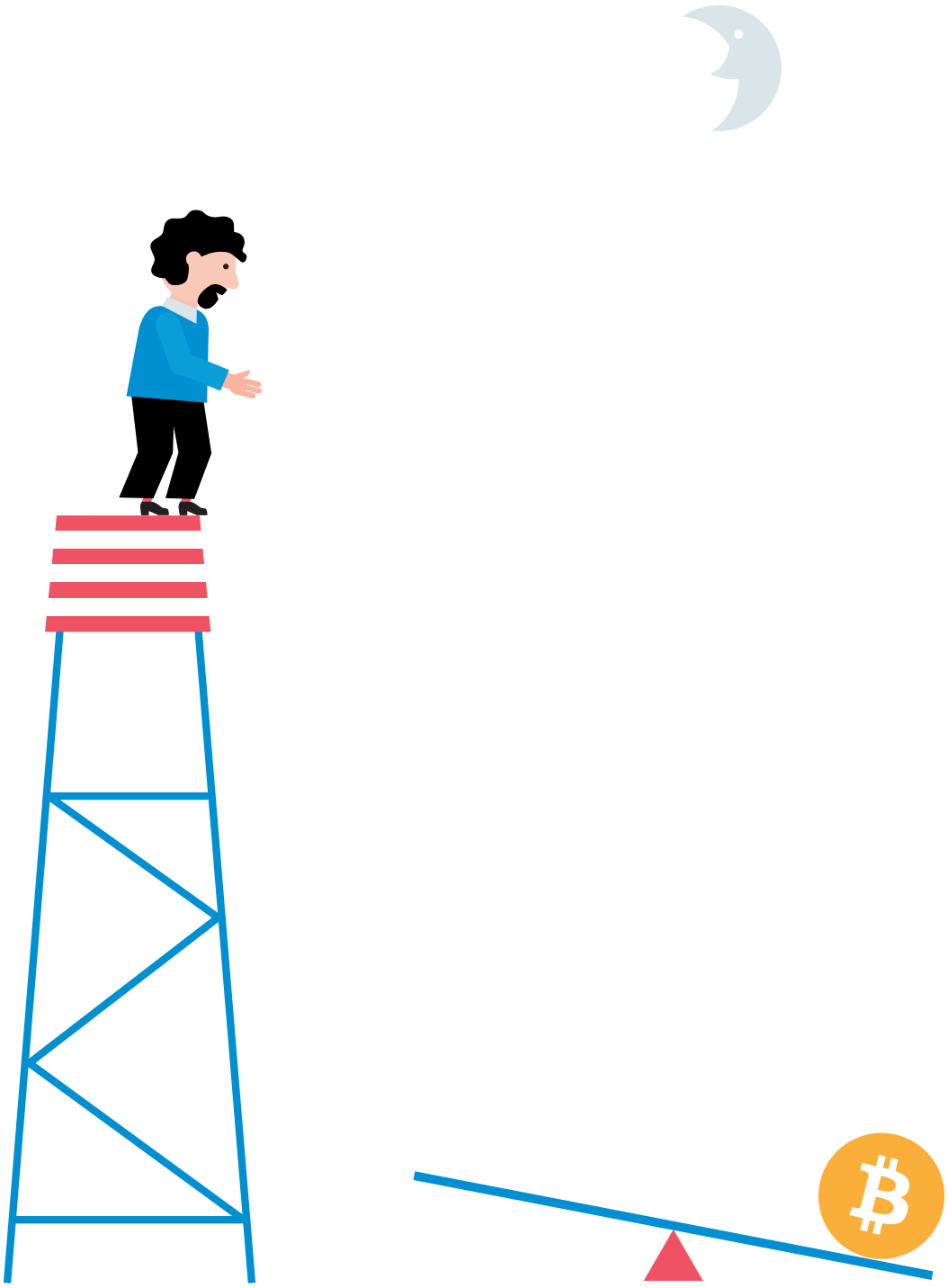
2008 publiziert ein gewisser Satoshi Nakamoto – bis heute ist nicht klar, ob sich hinter dem Namen eine einzelne Person oder ein Kollektiv verbirgt – auf einschlägigen Kryptographiekanälen einen wissenschaftlichen Aufsatz. Es geht darin um ein neues elektronisches Geldsystem, um Geldwerte innerhalb eines dezentralen Systems mithilfe einer Kette von kryptographisch versiegelten Datensätzen fälschungssicher zu übermitteln. Und zwar so, dass dabei auch das leidige Problem der doppelten Ausgabe gelöst wird, an dem bis anhin alle digitalen Währungen gescheitert waren: Ohne zentrale Kontrollinstanz zu verhindern, dass derselbe digitale Geldwert mehrmals verrechnet wird. Bitcoin, nennt Nakamoto sein System. Ein kryptographischer Beweis, an dem alle Nutzerinnen und Nutzer des Netzwerkes dank eines intelligenten Anreizsystems mitarbeiten und ihn so garantieren, ersetzt darin den vertrauenswürdigen Mittelmann. Der Artikel, nur neun Seiten lang, wird mit Begeisterung aufgenommen.

Nakamotos Erfindung entsteht nicht im luftleeren Raum. Sie baut auf Konzepten und theoretischen Überlegungen aus dem Bereich der mathematischen Kryptographie und der Informatik auf und kombiniert sie mit neuen Technologien. Gleichzeitig verkörpert sie eine der tiefgreifenden Veränderungen, welche die Kommerzialisierung der Informationstechnologie mit sich gebracht hat: Verschlüsselungsmechanismen, die es erlauben, Information über das weltweite Web sicher, zuverlässig und vertraulich auszutauschen, sind nicht mehr nur Regierungen und grossen Unternehmen vorbehalten, sondern Werkzeuge geworden, welche die gesamte digitale Gesellschaft für sich beansprucht.

Am 3. Januar 2009 schürft Nakamoto den Genesis-Block der Bitcoin-Blockchain. Kurz darauf taucht er ab und überlässt die Weiterarbeit an der quelloffenen Bitcoin-Software der Community. Im allerersten Block der Kette hat der mysteriöse Urheber der Blockchain eine Schlagzeile der Londoner «Times» eingefügt, die auf die globale Bankenkrise anspielt. Damit ist von Anfang an klar, dass es beim Bitcoin-Projekt nicht allein um ein technisches, sondern auch um ein gesellschaftliches Projekt geht, das zentralen staatlichen Institutionen äusserst kritisch gegenübersteht.

Das Bitcoin-Konzept führt zu zahlreichen alternativen Kryptowährungen, auch «Altcoins» genannt, mit Namen wie Litecoin oder Peercoin. Doch bereits

2009 wird daran gedacht, die grundlegende Innovation hinter Bitcoin, die Blockchain, über alternative Währungen und Finanztransaktionen hinaus auf andere Anwendungsfelder auszuweiten: Frachtbücher, Besitzurkunden, Studienabschlüsse: In das unbestechliche digitale Registerbuch Blockchain lässt sich im Prinzip alles einschreiben, «was als Digital Asset darstellbar ist und nur eine Person auf einmal besitzen kann», schreibt der Softwareentwickler Vitalik Buterin 2013 in einem Grundlagenpapier. Aus solchen Überlegungen heraus entsteht ein paar Jahre später eine neue Plattform: Ethereum, mehr als eine Kryptowährung, leistungsfähiger als Bitcoin und in der Lage, vereinbarte Handlungen automatisch auszulösen, sobald bestimmte Bedingungen erfüllt sind – also zum Beispiel eine Zahlung auszulösen, sobald eine Lieferung eingetroffen ist. Die Smart Contracts kommen ins Spiel.

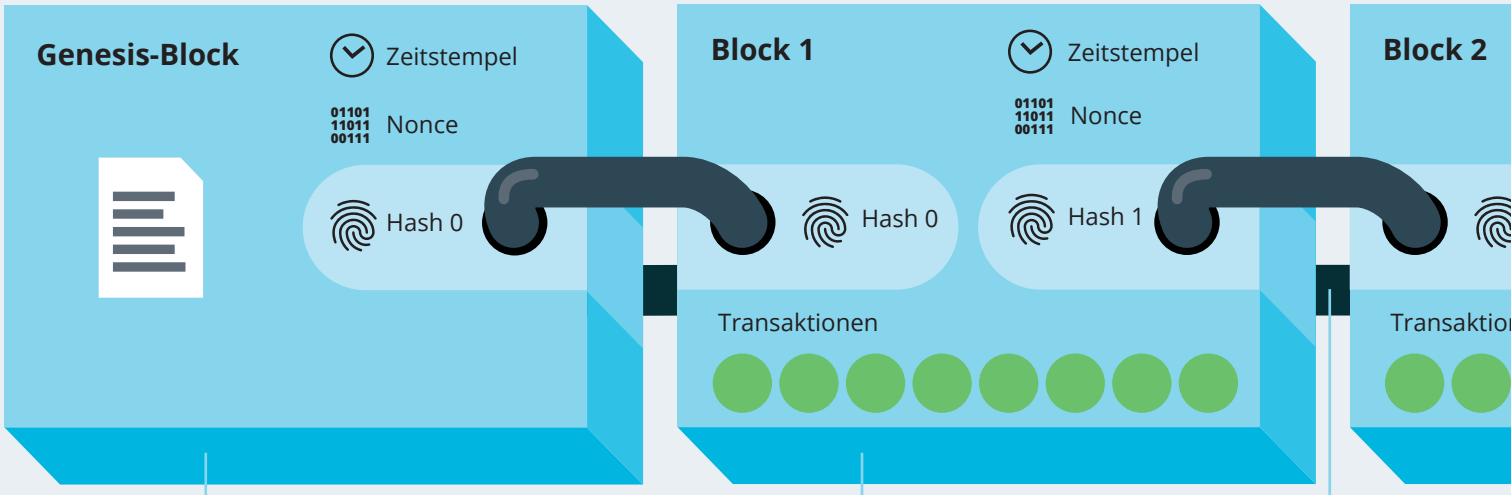


Die Glieder der Kette

Blockchain: Ein unbestechliches, digitales und dezentral gespeichertes Kontenbuch. Es besteht aus einer Abfolge von chronologisch aneinandergereihten Hash-Werten, von denen jeder auf den ihn vorangehenden Bezug nimmt. Blöcke nachträglich zu ändern oder unrechtmässig in die Kette einzuschmuggeln, ist deshalb nicht möglich.

Ein bisschen Kryptographie

Kryptographie: Zielt darauf ab, Datenbestände und sensible Informationen in einer bestimmten Form zu sichern und so zu übermitteln, dass Unbefugte keinen Zugriff darauf haben oder sie nicht verstehen können (Vertraulichkeit). Gleichzeitig sollen die Identität der Absenderin und des Empfängers unmissverständlich feststehen (Authentifizierung). Die Information darf während der Übermittlung oder der Speicherung nicht unbemerkt verändert werden können (Integrität), und schliesslich soll es nicht möglich sein, dass der Sender die Echtheit der übermittelten Information nachträglich bestreitet (Nichtabstreitbarkeit). Zum Verschlüsseln und Entschlüsseln der Information wird ein geheimer Schlüssel verwendet. Bei der symmetrischen Verschlüsselung verwenden Absender und Empfängerin denselben Schlüssel. Bei der asymmetrischen Verschlüsselung ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht, den nur eine der beiden Parteien besitzt. In beiden Fällen dient ein Schlüssel dazu, die Originalnachricht wiederherzustellen.



Genesis-Block (Schöpfer-Block): Der erste Block in einer Blockchain. Im Schöpfer-Block ist auch das Konsensprotokoll definiert. Es legt fest, wer Blöcke validieren darf und welche Aufgabe dafür zu erfüllen ist, wie oft ein neuer Block in die Kette eingeschrieben wird und wie gross er sein kann, d.h. wie viele Transaktionen darin gespeichert werden.

Block: Der Inhalt jedes Blocks besteht aus dem Hash-Wert aller im Block gespeicherten signierten Transaktionen, einem Zeitstempel und einer Zufallszahl (Nonce), die zur Validierung des Blocks benötigt wird. Dazu kommt der Hash-Wert des vorhergehenden Blocks. Aus all diesen Werten wird der Hash-Wert des neuen Blocks berechnet.

Kette: Die einzelnen Blöcke sind mittels Kryptographie verknüpft. Da jeder Block den Hash des vorhergehenden Blocks enthält, formen die Blöcke eine Kette, in der alle Transaktionen seit Beginn der Blockchain aufgezeichnet sind.

Hashfunktion: Ein kryptographisches Verfahren, das im Gegensatz zur Verschlüsselung nicht umkehrbar ist. Eine Hashfunktion ist ein Algorithmus, der eine Datei beliebiger Länge und Komplexität (z.B. einen Grundbucheintrag, ein Foto oder auch ein Audiofile) in eine Zeichenfolge mit fixer Länge umwandelt. Bei SHA-256, dem in der Blockchain-Welt meistgenutzten Algorithmus, sind das 256 bit oder Zeichen oder, anders gesagt, eine Folge von 256 Nullen und Einsen. Hashing-Mechanismen spielen in der Blockchain eine zentrale Rolle.

Hashwert der Eingabe:
Hello World

```
10100101100100011010011011
01010000001011111101000010
00000100000001001010000000
01000101110011001111001111
10110111101100011001000011
01011000101100011001011011
11110000101111001101101000
11001010110101011110110010
01110111110110011010110110
01111100010100011101110
```

Hashwert der Eingabe:
Hello, World

```
00000011011001110101101011
00010100111111111110011100
11010001010100110101110011
00110001111101111111001101
11111010001011000100010110
00110001010010000110000011
01110001111101000001100011
01110000010011011011110010
11010001100110101100000111
11101111101000101001O1
```

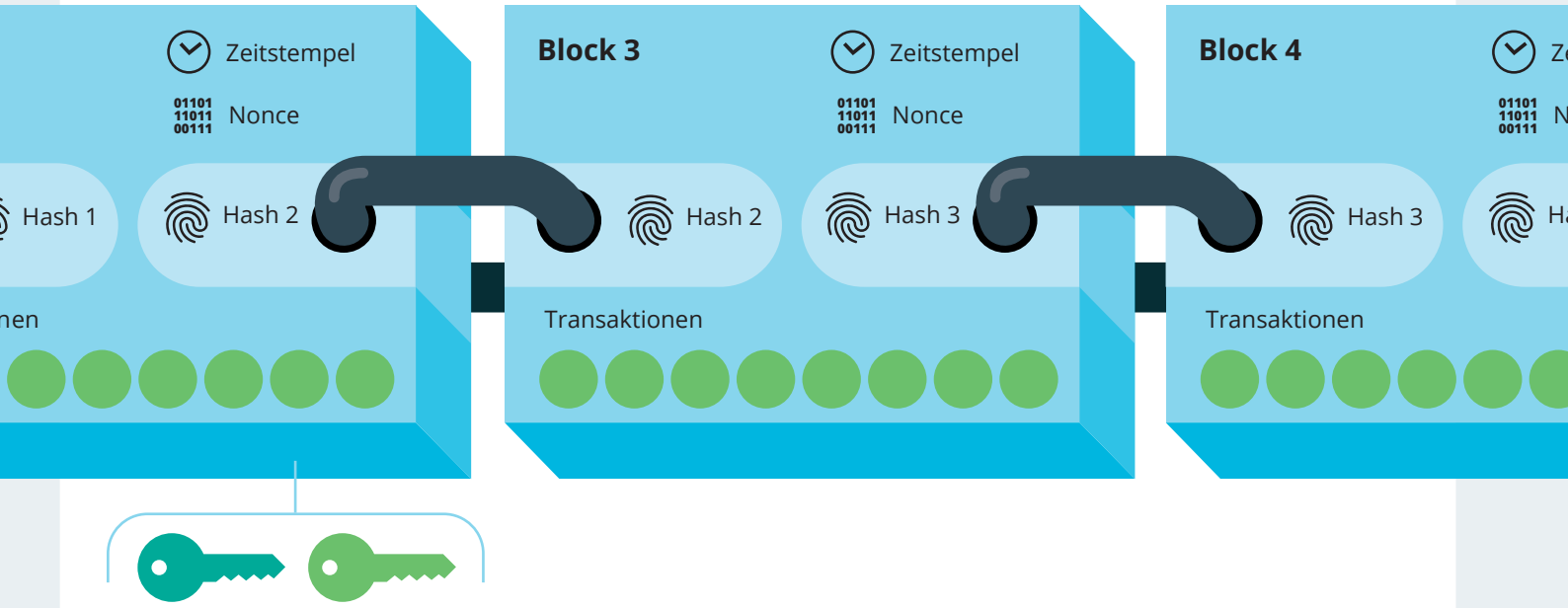
Ein Hash, auch Prüfzahl genannt, hat drei wichtige Eigenschaften:

1. Er ist unumkehrbar, d.h. es ist unmöglich, vom Output zurückzurechnen und herauszufinden, welche Input-Datei ihn erzeugt hat. Ein «gehashtes» Dokument ist also aus seinem Hash-Wert nicht rekonstruierbar. Ändern könnte sich das allenfalls, sobald ein leistungsfähiger Quantencomputer zur Verfügung steht. Das mühselige Zerlegen grosser Zahlen in ihre Primfaktoren, an dem heute noch die besten Supercomputer scheitern, würde er in Windeseile erledigen.

2. Die kleinste Änderung bei der Eingabe ergibt einen völlig anderen Hash-Wert: Es kann also überprüft werden, ob ein Datensatz abgeändert wurde. Hash-Werte ermöglichen somit das Aufdecken von Manipulationen.

3. Dieselbe Eingabe ergibt immer denselben Output. Der Hash-Wert wird deshalb auch als «digitaler Fingerabdruck» bezeichnet. Fällt das Resultat anders aus, bedeutet das in jedem Fall, dass der Eingabewert verändert wurde.

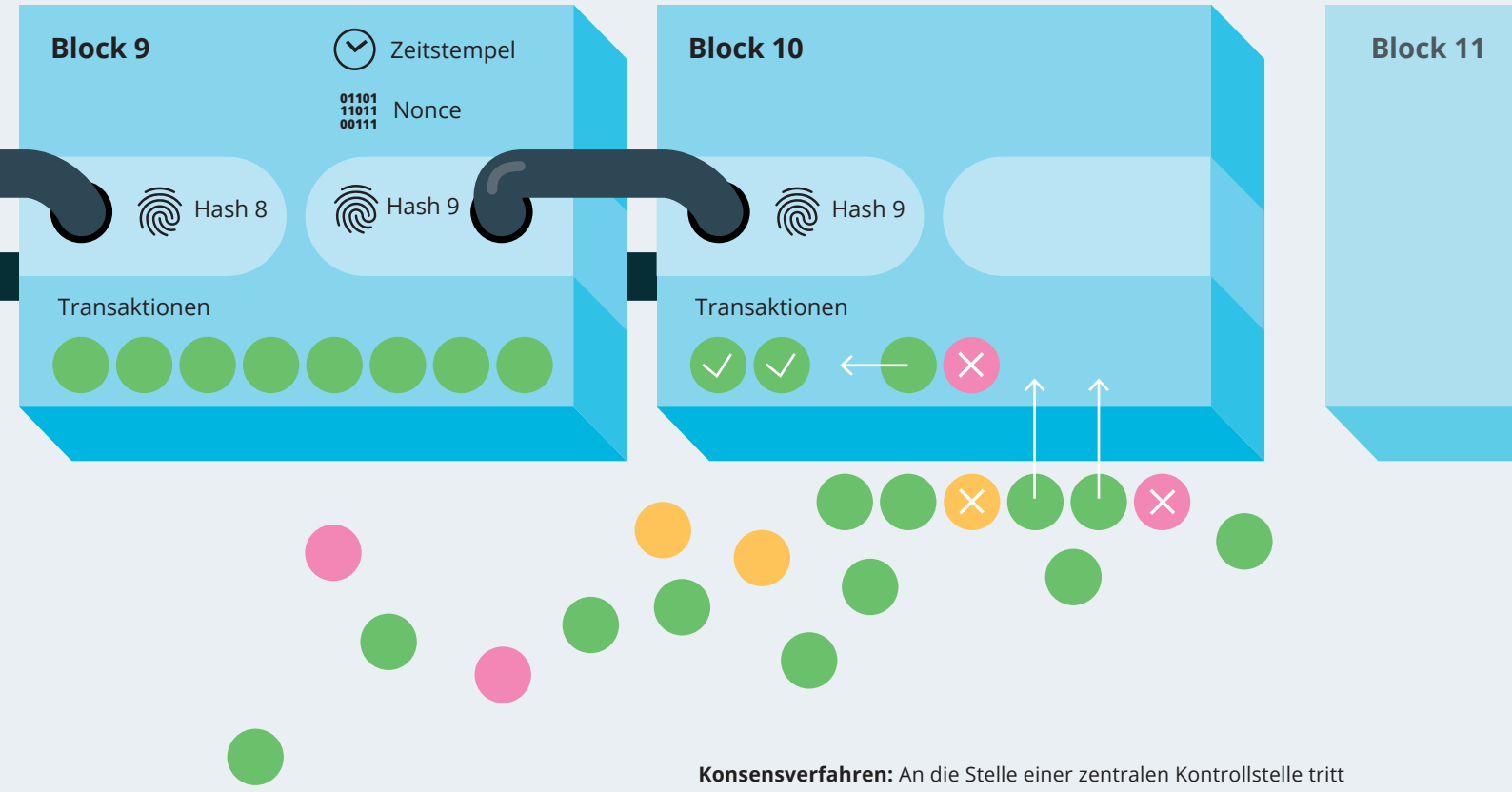
Die Macht der grossen Zahl: Rein theoretisch ist, was unter Punkt 3 steht, nicht immer richtig: Es ist möglich, dass unterschiedliche Datensätze durch denselben Hash-Wert abgebildet werden. Doch die Wahrscheinlichkeit für eine solche «Kollision» ist so klein, dass wir sie gleich wieder vergessen können: Sie entspricht der Chance, den Euromillions-Jackpot neun Mal nacheinander zu knacken. Genauso geht beispielsweise die Wahrscheinlichkeit, dass zwei Blockchain-Nutzern derselbe Hashwert als Kontonummer zugewiesen wird, gegen null.



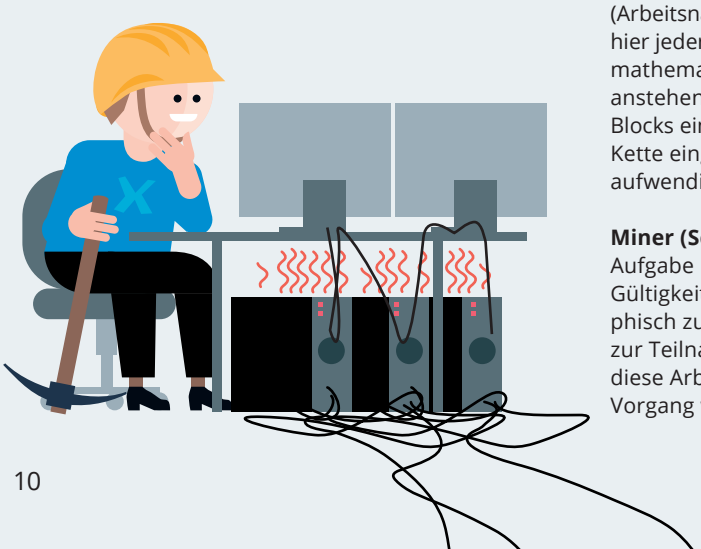
Asymetrische Verschlüsselung: Sie kommt bei der Blockchain für die Sicherung der Zugangsdaten und die Verifikation von Eigentumsrechten zum Einsatz. Jeder Nutzer erhält eine willkürliche Zahlenkombination als Private Key zugewiesen. Daraus werden ein Public Key und aus diesem wiederum eine Kontonummer (Public Address) berechnet. Mit dem Private Key kann eine Nutzerin nachweisen, einzige berechtigte Besitzerin eines Kontos zu sein. Sie muss zudem jede Transaktion, die sie auf ihrem Konto ausführt, mit ihrem privaten Schlüssel signieren. Durch die mathematische Verknüpfung zwischen den beiden Schlüsseln, kann mit dem öffentlichen Schlüssel geprüft werden, ob eine Transaktion korrekt vorgenommen wurde und eine Signatur gültig ist. Verliert der Kontoinhaber den privaten Schlüssel, kann er nicht mehr an seine Daten gelangen. Zwischen drei und fünf Millionen Bitcoins sollen so für immer verloren sein.

Pseudo-Anonymität (Pseudonymität): Weil die Blockchain transparent ist, können alle Transaktionen jederzeit verfolgt werden und sind einer öffentlichen Adresse zugeordnet. Um die Privatsphäre der Nutzerinnen schützen zu können, ist der Public Key nicht mit dem Namen sondern mit einem Pseudonym verbunden, das keine Rückschlüsse auf die reale Person dahinter zulässt. Weil trotzdem nicht auszuschliessen ist, dass jemand die Identität eines Nutzers anhand seiner Transaktionsbewegungen erraten kann, wird von Pseudo-Anonymität gesprochen.

Zero-Knowledge-Proof: Ein mathematisch ungeheuer komplexes kryptographisches Verfahren, bei dem eine Partei der anderen beweist, dass sie ein Geheimnis kennt, ohne das Geheimnis selber preisgeben zu müssen. Zero-Knowledge-Protokolle können die Anonymität auf der Blockchain stärken.



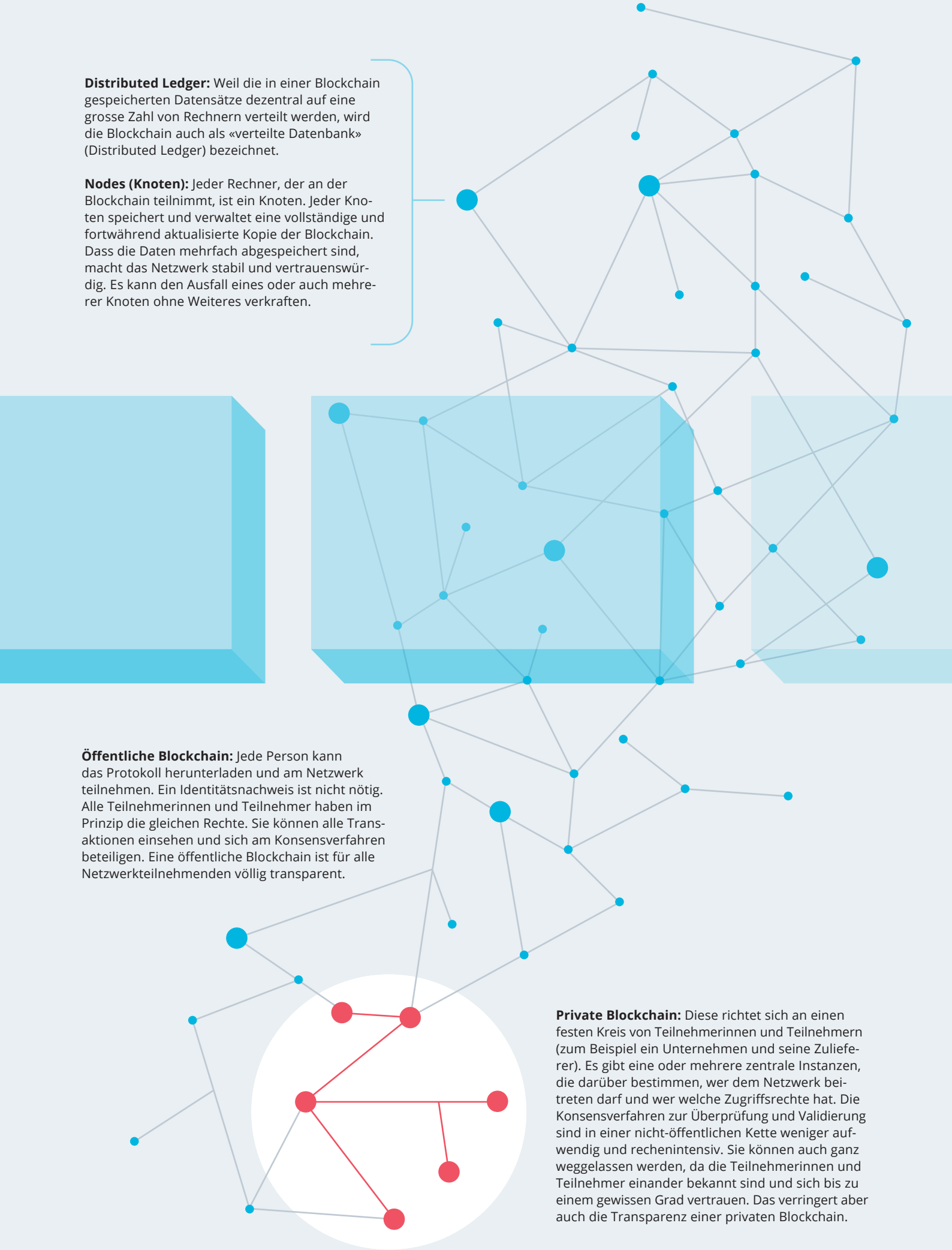
Konsensverfahren: An die Stelle einer zentralen Kontrollstelle tritt bei der Blockchain ein Abstimmungsmechanismus, mit dessen Hilfe alle Teilnehmenden darüber entscheiden, welche Transaktionen gültig sind und in welcher Reihenfolge sie in die Kette eingereiht werden. Der Konsens wird nicht bei allen Blockchain-Anwendungen gleich hergestellt. Das meistgenutzte Konsensverfahren heisst Proof of Work (Arbeitsnachweis). Es nimmt enorm viel Rechenpower in Anspruch, weil hier jeder Node im Wettstreit mit den anderen versucht, ein komplexes mathematisches Rätsel zu lösen. Die Aufgabe besteht darin, aus den anstehenden Transaktionen und dem Hash-Wert des vorhergehenden Blocks einen eigenen Hash für den neuen Block zu berechnen, der in die Kette eingereiht werden soll. Andere Konsensverfahren sind weniger aufwendig und verbrauchen dementsprechend weniger Energie.



Miner (Schürfer): Ein Teil der Nodes sind als Validatoren tätig. Ihre Aufgabe ist mit der eines Buchhalters zu vergleichen: Sie prüfen die Gültigkeit neuer Transaktionen, bündeln sie und reihen sie, kryptographisch zu einem neuen Block versiegelt, in die Kette ein. Um die Nodes zur Teilnahme am Verifikationsprozess zu bewegen, werden sie für diese Arbeit entlöhnt. Bei Bitcoin erhalten die Miner neue Bitcoins. Der Vorgang wird deshalb mit dem Schürfen von Gold verglichen.

Distributed Ledger: Weil die in einer Blockchain gespeicherten Datensätze dezentral auf eine grosse Zahl von Rechnern verteilt werden, wird die Blockchain auch als «verteilte Datenbank» (Distributed Ledger) bezeichnet.

Nodes (Knoten): Jeder Rechner, der an der Blockchain teilnimmt, ist ein Knoten. Jeder Knoten speichert und verwaltet eine vollständige und fortwährend aktualisierte Kopie der Blockchain. Dass die Daten mehrfach abgespeichert sind, macht das Netzwerk stabil und vertrauenswürdig. Es kann den Ausfall eines oder auch mehrerer Knoten ohne Weiteres verkraften.



Öffentliche Blockchain: Jede Person kann das Protokoll herunterladen und am Netzwerk teilnehmen. Ein Identitätsnachweis ist nicht nötig. Alle Teilnehmerinnen und Teilnehmer haben im Prinzip die gleichen Rechte. Sie können alle Transaktionen einsehen und sich am Konsensverfahren beteiligen. Eine öffentliche Blockchain ist für alle Netzwerkteilnehmenden völlig transparent.

Private Blockchain: Diese richtet sich an einen festen Kreis von Teilnehmerinnen und Teilnehmern (zum Beispiel ein Unternehmen und seine Zulieferer). Es gibt eine oder mehrere zentrale Instanzen, die darüber bestimmen, wer dem Netzwerk beitreten darf und wer welche Zugriffsrechte hat. Die Konsensverfahren zur Überprüfung und Validierung sind in einer nicht-öffentlichen Kette weniger aufwendig und rechenintensiv. Sie können auch ganz weggelassen werden, da die Teilnehmerinnen und Teilnehmer einander bekannt sind und sich bis zu einem gewissen Grad vertrauen. Das verringert aber auch die Transparenz einer privaten Blockchain.

Die Blockchain im Test der Anwendungen

Staatliche Register – digital verbürgte Eigentumsrechte

Als unbestechliches und völlig transparentes digitales Registerbuch scheint die Blockchain auf den ersten Blick insbesondere für staatliche Register wie das Grundbuch geeignet. Auf viele Rechner verteilt garantiert ein Blockchain-basiertes Register die Unveränderbarkeit der darin hinterlegten Informationen und bietet mehr Sicherheit als eine auf einem zentralen Server gespeicherte Datenbank. Abläufe werden schneller und effizienter. Eine zentrale Instanz ist nicht nötig. Das kann in einem Land mit schwachen Institutionen ein grosser Vorteil sein.

Und in der Schweiz? Hier hält, als Beispiel für ein staatliches Register, das Grundbuch fest, welche Rechte an einem Grundstück bestehen. Jede Änderung, sei es der Verkauf des Grundstücks oder seine Überschreibung an einen neuen Besitzer, muss notariell beglaubigt ins Grundbuch eingetragen werden. In der Schweiz sind es die Kantone, die im Auftrag des Bundes das Grundbuch führen und dafür bürgen, dass alle Einträge korrekt sind. Ein gesamtschweizerisches zentrales Grundbuch gibt es nicht. Das Grundbuch ist öffentlich – jedermann kann zum Beispiel Auskunft darüber verlangen, wem ein bestimmtes Grundstück gehört. Der Grundstücksmarkt ist deshalb weitgehend transparent. Viele der Stärken der Blockchain scheint das herkömmliche System also bereits zu besitzen.

Dazu kommt, dass das Recht auf den Schutz der Privatsphäre die Einsicht ins Grundbuch beschränkt. Es liegt im Ermessen der Grundbuchverwalterinnen, Personen, die ein besonderes Interesse glaubhaft machen können, weitergehende Einsichten zu gewähren. Ohne das Gesetz zu verändern, könnte dieser Umstand nur mithilfe einer privaten Blockchain mit genau definierten Zugriffsrechten abgebildet werden. Das Vertrauen in die kantonale Grundbuchbehörde würde dann durch das Vertrauen in eine Gruppe von Genehmigungsinstanzen ersetzt.

Ein staatliches Register vollständig auf die Blockchain zu übertragen, macht wenig Sinn. Interessanter sind Teillösungen, wie sie beispielsweise der Kanton Genf testet. Dort werden von Bürgerinnen und Bürgern angeforderte Grundbuchauszüge gleichzeitig auch auf der Blockchain hinterlegt. Die Empfänger können so nachprüfen, dass das ihnen zugeschickte Dokument mit dem Original übereinstimmt und somit gültig ist. Denselben Zweck könnte allerdings auch der bereits existierende – und rechtsgültige – elektronische Identitätsnachweis SuisseID erfüllen. Vielversprechender scheint der Ansatz, ein Blockchain-basiertes Register durch die Funktionalität smarter Verträge zu erweitern: Grundbuchänderungen würden dann zum Beispiel erst gültig, wenn bestimmte Bedingungen erfüllt sind.

Kryptowährungen – im Tal der Enttäuschung

2017 explodierte der Wert von Bitcoin, der wichtigsten Digitalwährung, um mehr als 1800 Prozent und erreichte Ende Jahr ein Rekordhoch von knapp 20 000 US-Dollar. Auch andere Kryptowährungen – rund 3000 gibt es heute davon – kennen solche, von tiefen Kursstürzen gefolgte Höhenflüge. Ähnlich volatil ist die Haltung von Öffentlichkeit, Finanzmärkten und Regierungen dieser neuen Asset-Klasse gegenüber. Manchmal wird ihr eine grosse Zukunft vorausgesagt sowie das Potenzial, das gesamte Geldbankensystem umzukrempeln und die Macht ihrer klassischen Institutionen zu brechen. Technologieaffine Länder wie Japan haben sie als Teil der aufstrebenden Fintech-Industrie akzeptiert, und auch in der Schweiz hat die Eidgenössische Finanzmarktaufsicht (FINMA) bereits zwei Krypto-Banken die Banklizenz erteilt. Andere warnen vor einer klassischen Spekulationsblase, sehen eine Bedrohung für die Finanzstabilität und den Versuch, Notenbanken und Regulierungsbehörden im grossen Stil zu umgehen.

Bei nüchterner Betrachtung schneiden aber gerade virtuelle Währungen eher bescheiden ab. Als Alternative zu klassischen Währungen sind sie bisher kaum geeignet: der durchschnittliche tägliche Transaktionswert um mehrere Grössenordnungen kleiner, die Wertstabilität miserabel, als alltägliches Zahlungsmittel noch kaum akzeptiert. Auch beim Versuch, traditionelle Systeme des Zahlungsverkehrs zu ersetzen, überzeugen sie nicht. Mit Bitcoin beispielsweise lassen sich weltweit nur etwa sieben Transaktionen pro Sekunde ausführen, während Zahlungen mit PayPal praktisch augenblicklich erfol-

gen. Als Wertspeicher schliesslich sind Kryptowährungen, die im Gegensatz zu Gold keinen intrinsischen Wert haben, viel zu volatil.

Die Blockchain-Community arbeitet daran, das Kryptowährungssystem gezielt zu verändern und weiterzuentwickeln. So setzt sich etwa die Bitcoin Foundation dafür ein, die Verwendung von kryptographischem Geld weltweit zu standardisieren, zu schützen und zu fördern. Doch vorläufig bleibt die Feststellung: Ihren eigenen Ansprüchen sind die Blockchain-basierten Währungen bisher nicht gerecht geworden.

Initial Coin Offering (ICO) – der virtuelle Börsengang

Die Kapitalbeschaffung kann für Start-ups ein langwieriges und schwieriges Unterfangen sein. Im Umfeld der Blockchain ist nun eine Finanzierungsmöglichkeit entstanden, welche die Blockchain-Technologie mit Crowdfunding kombiniert. Anders als beim klassischen Börsengang (Initial Public Offering oder IPO) werden hier nicht Unternehmensanteile gegen Risikokapital verkauft, sondern gegen Tokens. Das sind digitale Einheiten einer Kryptowährung, die eigens für das Projekt geschaffen wird. Die FINMA unterscheidet drei Kategorien von Blockchain-basierten Tokens: Solche, die einen Geldwert haben (Zahlungs-Tokens), solche, die Zugang zu einer Dienstleistung geben (Nutzungs-Tokens), und schliesslich solche, die einen Vermögenswerte repräsentieren (Anlage-Tokens). Der Käufer spekuliert darauf, dass der zukünftige Erfolg des unterstützten Projektes den Wert der erworbenen Tokens vervielfachen wird. Weltweit finden ICOs riesigen Anklang und verzeichnen regelmässig Rekorde bezüglich ihres Emissionsvolumens. Ein ICO ermöglicht es, eine zündende Idee zu finanzieren, die noch ganz am Anfang steht. Das kann eine unglaubliche Chance sein, um eine Innovation rasch umzusetzen – aber auch eine Masche, um gutgläubigen Anlegern Geld aus der Tasche zu ziehen.

Während ein klassischer Börsengang mindestens fünf Monate Zeit in Anspruch nimmt, mit hohen Kosten und viel bürokratischem Aufwand verbunden ist, strengen Vorschriften genügen muss sowie die Vermittlerdienste mindestens einer Bank voraussetzt, ist der Prozess beim ICO vergleichsweise einfach, schnell und günstig. Insbesondere in der Schweiz, wo Risikokapital nicht im Überfluss vorhanden ist, haben ICOs Jungunternehmen im Fintech-Bereich einen starken Schub gegeben. Dass die Schweiz inzwischen zu einer der wichtigsten Drehscheiben für ICOs geworden ist, lässt sich hauptsächlich auf günstige rechtliche und steuerliche Rahmenbedingungen, eine lebendige Fintech-Szene und einen bemerkenswerten Talentpool im Bereich der Hochschulforschung zurückführen. Um dem Missbrauchsrisiko entgegenzuwirken, welches die spekulative Natur der ICOs mit sich bringt, hat die FINMA eine Wegleitung publiziert, die Klarheit schaffen und die Integrität des Finanzplatzes schützen soll, ohne das innovative Potenzial der virtuellen Börsengänge zu schmälern.

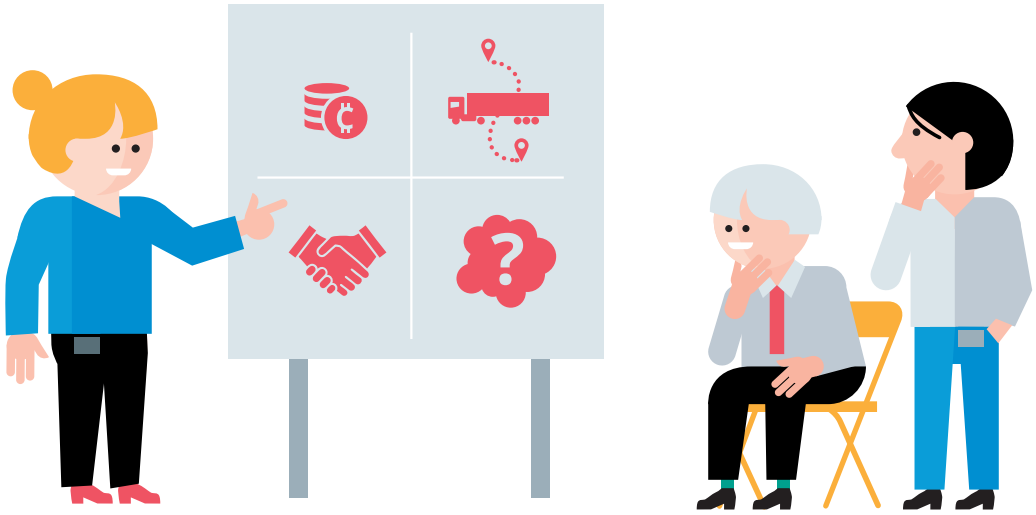
Private Payment Systems – Einkauf im Flüchtlingslager

Im Flüchtlingscamp Azraq in der jordanischen Wüste läuft ein vielbeachtetes Blockchain-Projekt. Das Welternährungsprogramm der Vereinten Nationen (WFP) setzt dort die Blockchain-Technologie ein, um rund 10'000 syrischen Flüchtlingen Lebensmittel zu verteilen. Seit etwa zehn Jahren gibt das WFP Essensrationen nicht mehr direkt ab. Stattdessen erhalten die Geflüchteten Geld oder Prepaid-Karten, damit sie selber einkaufen können. Das gibt ihnen ein Stück Selbstbestimmung und Würde zurück und führt interessanterweise auch dazu, dass sie sich ausgewogener ernähren. Darüber hinaus kurbeln diese «Cash Based Transfers» die lokale Wirtschaft an und sparen Logistikkosten. Aber Food-Voucher können verloren gehen, gestohlen, gehortet oder mit Profit weiterverkauft werden. Im Supermarkt im Azraq-Camp kommt seit Mai 2017 ein Blockchain-basiertes Verfahren zum Einsatz, das den Ablauf sicherer und effizienter macht und weitgehend vor Manipulationen schützt. Wer einkaufen will, identifiziert sich durch einen Iris-Scan. Die Daten werden mit der Datenbank des WFP verglichen. Dort sind alle Angaben zum Konto, zur Identität und zur Einkaufsgeschichte aller Flüchtlinge als verschlüsselte Datensätze sicher in der Blockchain hinterlegt. Die Bank als Vermittlerin entfällt, an ihre Stelle tritt das WFP als die zentrale Autorität, die ganz allein die Abwicklung der Zahlungen und die Buchhaltung übernimmt. Das macht den ganzen Prozess effektiver und günstiger, da keine Gebühren anfallen.

Was in Azraq zum Einsatz kommt, ist ein rudimentäres privates Blockchain-Netzwerk mit nur einem Node. Die Blockchain-Technologie wird hier hauptsächlich dafür verwendet, sensible Daten fälschungssicher zu speichern. Doch es bleibt die Möglichkeit bestehen, das sehr erfolgreiche Projekt dezentral auszubauen und damit das ganze Potenzial der Blockchain zu erschliessen: Sie könnte dazu dienen, Einkäufe und Ausgaben für verschiedene Lager und vielleicht sogar die Dienstleistungen weiterer Hilfsorganisationen in einem einzigen dezentral verwalteten System transparent abzuwickeln – Missbrauch von Spenden, ihr Versickern in der Tasche korrupter Zwischeninstanzen oder der zweckentfremdete Einsatz von Hilfsgeldern wären dann nicht mehr möglich.

Herkunftsnachweise – vom Meer bis auf den Teller

Mithilfe der Blockchain lassen sich auch die Lieferwege von Konsumgütern oder Lebensmitteln über komplizierte Lieferketten hinweg besser nachvollziehen. Das britische Start-up Provenance beispielsweise nutzt die Ethereum-Blockchain, um die Herkunft von fair gefischtem Thunfisch aus Indonesien zu dokumentieren. Das fängt damit an, dass die im System eingetragene lokale Fischerin Gewicht und Qualität ihres Fangs per SMS registriert. Welchen Kriterien der Fisch entsprechen muss, um als nachhaltig zu gelten, hat eine unabhängige Zertifizierungsstelle zuvor klar definiert und diese Kriterien ebenfalls in der Blockchain hinterlegt. Aus all diesen Informationen wird ein Token erstellt, das den Fang eindeutig identifiziert. Dieser «digitale Fingerabdruck» begleitet den Fisch auf jeder Station seines Wegs, vom Dock über die Fabrik und den Gross- bis zum Einzelhändler, wird dabei jedes Mal registriert und aktualisiert und ans nächste Glied in der Lieferkette weitergegeben. So gelangt er am Ende zum Kunden, der seinerseits einen QR-Code



scannen, die gespeicherten Informationen zurückverfolgen und somit genau wissen kann, was auf seinem Teller landet. Weiter verbessert werden kann das Supply-Chain-Management, wenn Smart Contracts und das Internet der Dinge mit der Blockchain kombiniert werden: Sensoren könnten dann beispielsweise überwachen, dass die Temperatur während des Transports im vereinbarten Bereich liegt oder die transportierte Ware nicht manipuliert wurde und im Bedarfsfall automatisch eine vorher definierte Aktion auslösen. Dadurch lässt sich die Produktqualität gewährleisten.

Die Überwachung und Sicherung von Lieferketten ist auch ohne Blockchain möglich, doch Blockchain-basierte Lösungen optimieren die Verfolgbarkeit der Güter und den korrekten Prozessablauf. Fehler sind auch hier nicht ausgeschlossen: So könnte im Fall des Thunfisches die Instanz, die damit beauftragt ist zu kontrollieren, ob die Fischer die Nachhaltigkeitskriterien tatsächlich einhalten, schlechte Arbeit machen. Das Vertrauen in die Garanten des Systems wird also weiterhin vorausgesetzt – ein gänzlich «vertrauensloses» System, d.h. ein System, in dem das Vertrauen in Intermediäre durch ein dezentrales, öffentliches und transparentes Netzwerk vollständig ersetzt wird, ist die Blockchain also auch in diesem Fall nicht.

Smartes Energiemanagement – die Sonne über Brooklyns Dächern

Die beschriebenen Beispiele zeigen, dass Stärken der Blockchain heute vor allem dort sinnvoll zum Einsatz kommen, wo die Blockchain eine Lücke füllt. Dort also, wo das Vertrauen, das die Basis jedes Leistungstransfers ist, nicht gegeben oder schwierig herzustellen ist, sei es, weil eine vertrauenswürdige zentrale Instanz fehlt oder weil zu viele fehleranfällige Zwischeninstanzen beteiligt sind. Ob beim staatlichen Register, dem Einkauf im Flüchtlingslager oder dem genau dokumentierten Lieferweg fair gefischter Thunfische: In all diesen Fällen agiert die Blockchain eher als Ergänzung bestehender analoger oder digitaler Verfahren. Oft überzeugt sie auch erst dort, wo sie auf einen lokalen Kontext begrenzt bleibt. So ein Beispiel findet sich auf den Dächern von Brooklyn.

Auf einer Reihe von Brownstones im Brooklyner Quartier Park Slope hat sich eine Gruppe von Nachbarinnen und Nachbarn zu einem dezentralen Mikro-Stromnetz zusammengeschlossen. Sie produzieren Sonnenenergie für den Eigenverbrauch, möchten Energieüberschüsse aber auch zu möglichst fairen Preisen ins Netz einspeisen und bestimmen können, welchen Strompreis sie zu zahlen bereit sind, wenn sie selber Strom von ihren Nachbarn benötigen. Das gelingt mithilfe des Brooklyn Microgrids, einer mit Smart Contracts kombinierten privaten Blockchain-Plattform, die die Stromverteilung gemäss Angebot und Nachfrage steuert. Die Preise werden mithilfe von Smart Contracts in automatischen Auktionen bestimmt; sie richten sich nach dem Höchstpreis, den ein ans Mikronetz angeschlossener Konsument zu zahlen bereit ist, und nach dem Mindestpreis, zu dem ein Stromproduzent willens ist zu verkaufen. Die Plattform umfasst Kontroll- und Steuersysteme, Konverter, Smart Meter und Energiespeicher in Form von Lithium-Ionen-Batterien. Strom wird in diesem Netz also direkt zwischen den Erzeugerinnen und Endkunden gehandelt und abgerechnet, ein dazwischengeschalteter Energieversorger ist nicht nötig. Allerdings ist das Brooklyn Microgrid nicht völlig vom Stromnetz abgekoppelt. Im Bedarfsfall können die Anwohner weiterhin Strom aus dem öffentlichen Netz beziehen.

Um solche Projekte gesetzkonform in der Schweiz implementieren zu können und beispielsweise ganze Städte über eine öffentliche, dezentrale Peer-to-Peer-Plattform mit Energie zu versorgen, ohne dass der Energieversorger eine Rolle als Intermediär spielt, müssten zuerst die Strukturen des heutigen Strommarktes aufgebrochen werden – mit den aktuell in der Energiewirtschaft geltenden Vorschriften ist das nicht möglich: In der Schweiz mit ihrem noch nicht vollständig geöffneten Strommarkt, dürfen Kleinverbraucherinnen und Kleinverbraucher bisher am Markt gar nicht teilnehmen. Zudem sind die Kosten für die Nutzung des Netzes stark geregelt und dürfen nicht gesenkt werden, wenn der Strom aus der Nachbarschaft kommt.

Die Suche nach der Killerapplikation

Noch fehlt der grosse Wurf: Die Anwendung, die der Blockchain zum Durchbruch verhilft. Noch gibt es für die meisten ihrer Anwendungen bereits bestens funktionierende Alternativen. Und manch innovative Blockchain-Anwendung würde ohne Blockchain genauso überzeugen. Allerdings hat das oft weniger mit der Technologie selber zu tun als damit, dass die Blockchain in ihrer reinsten Form als dezentrale, öffentliche, völlig transparente und vertrauenswürdige Datenbank den bestehenden Rechts- und Regulierungsrahmen sprengt – und damit bestehende Wirtschaftsstrukturen sowie die Rolle einer ganzen Reihe von privaten und staatlichen Institutionen in Frage stellt.

Die Blockchain als Katalysator

Noch mag der Gebrauch der Blockchain marginal sein, als soziales Phänomen ist sie nicht kleinzureden. Technisch hochkomplex und für Laien kaum verständlich, ist sie zu einer Projektionsfläche geworden, die verschiedene Akteure mit unterschiedlichen Motiven eifrig polieren, insbesondere im Bereich der Kryptowährungen. Ein Beispiel sind die oft in undurchdringlichem Tech-Sprech verfassten White Papers, mit denen ICOs lanciert werden. Sie haben oft mehr mit Marketing zu tun als mit fundierter Information für potenzielle Anleger – und dienen wohl eher dazu, den tatsächlichen Endnutzungswert des lancierten Produkts zu verschleiern und die Verantwortung für technische Probleme von vornherein abzuschieben.

Vertrauen, Kontrolle und Verantwortung

Von Anfang an als libertärer Gegenentwurf zu einer Welt konzipiert, in der nationale Staaten als zentrale Steuerungsinstanzen wirken, sprengt die Blockchain nicht nur in vielen Bereichen den akzeptierten regulatorischen und rechtlichen Rahmen, sondern stellt auch eine ganze Reihe von gesellschaftlichen und politischen Werten in Frage. Ihre Verfechterinnen träumen nicht selten von der Abschaffung staatlicher und marktwirtschaftlicher Strukturen, in der Hoffnung, die Welt Blockchain-basiert und dezentral organisiert effizienter und gerechter ordnen zu können.

So ersetzt die Blockchain das Vertrauen in eine Kontrollinstanz, die dafür bürgt, dass alle Abläufe korrekt sind, mit dem Vertrauen in ein komplexes kryptographisches System und in einen von allen Akteuren gemeinsam getragenen Überprüfungsmechanismus. Die Wahrscheinlichkeit, dass im System Fehler auftreten, wird als vernachlässigbar gering eingestuft. Sollte dies dennoch geschehen, gibt es keine Stelle, die die Verantwortung für die Fehlfunktion des Systems übernimmt.

Transparenz versus Privatsphäre

Ihre völlige Transparenz ist der Blockchain grosse Stärke. Das gilt zum Beispiel wenn es darum geht, Lieferketten lückenlos zu dokumentieren, um die Lebensmittelsicherheit zu verbessern. Der Preis für diese Transparenz ist jedoch, dass die Identität und die Privatsphäre der Nutzerinnen und Nutzer nicht ausreichend geschützt sind. Jeder, der im Besitz des öffentlichen Schlüssels eines Nutzers ist, kann all dessen Transaktionen verfolgen. Und er kann durch die Verknüpfung von Gewohnheitsmustern mit anderen Datensätzen möglicherweise herausfinden, wer hinter einem Pseudonym steckt. Da die Blockchain darauf ausgelegt ist, Daten unlöschbar und vor Manipulation geschützt zu speichern, kennt sie auch kein Recht auf Vergessen.

Den Tiger zähmen – aber gemeinsam

Dass die Blockchain ganz ohne vertrauenswürdige Dritte auskommt, fordert all jene Institutionen heraus, die diese Vermittlerrolle bisher wahrgenommen haben und nun ihre Bedeutung in Frage gestellt sehen. Insbesondere Kryptowährungen sind weltweit ins Visier der Regulierungsinstanzen gekommen, manche Länder haben sie bereits verboten. Anderswo wird auf «Regulatory Sandboxes» gesetzt, wo Kryptowährungen mit sanftem Druck und ohne die Innovation zu gefährden in geordnete Bahnen gelenkt werden sollen. Das World Wide Web Consortium arbeitet seinerseits daran, die Rahmenbedingungen für den Einsatz von Blockchain-Anwendungen mittels internationaler Standards zu klären.

Aber nicht nur über Regulierung und Standardisierung wird versucht, die Blockchain zu zähmen. Die grossen Industrie- und Finanzakteure haben längst damit begonnen, die Technologie, die ihr angestammtes Geschäftsmodells bedroht, ihren eigenen Zielen und Zwecken gemäss umzubauen. So sind die privaten Blockchains mit Zulassungsbeschränkungen entstanden, die inzwischen auch von öffentlichen Verwaltungen übernommen wurden. Manche Länder denken gar daran, eine nationale Kryptowährung zu lancieren.

Es ist wichtig, dass solche Normalisierungsversuche nicht durch die Interessen, Begehrlichkeiten und Befürchtungen von Akteuren dominiert werden, die dazu demokratisch gar nicht legitimiert sind. Wie der Einsatz einer hochinnovativen Technologie gestaltet werden soll, die so viel in Frage stellt, muss – jenseits von jedem Hype – im Interesse der Allgemeinheit breit und mit Bedacht diskutiert werden. Diesem Zweck dient der zweiteilige Bericht, den TA-SWISS nun vorlegt.

Mitglieder der Begleitgruppe

- Dr. Olivier Glassey, Leiter der Begleitgruppe und Mitglied des Leitungsausschusses von TA-SWISS, Universität Lausanne
- Raphael Bucher, Bundesamt für Umwelt (BAFU)
- Prof. Christian Cachin, Universität Bern
- Hannes Gassert, crstl
- Anja Wyden Guelpa, civiclab
- Dr. Uwe Heck, Informatiksteuerungsorgan des Bundes (ISB)
- Luzius Meisser, meissereconomics
- Marine Pasquier-Beaud, Bundesamt für Energie (BFE)
- Martin Rindlisbacher, UBS
- Dr. Fabian Schnell, Avenir Suisse
- Antoine Verdon, Swiss Legal Tech Association

Projektleitung bei TA-SWISS

- Dr. rer. soc. Elisabeth Ehrensperger, Geschäftsführerin
- Dr. Catherine Pugin, Projektleiterin

Impressum

Programmiertes Vertrauen:
Chancen und Risiken der Blockchain-Technologie
Kurzfassung der Studie «Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment»
TA-SWISS, Bern 2020
TA 73A/2020

Autorin: Christine D'Anna-Huber, Wissenschaft im Text, Paradiso
Produktion: Fabian Schluep, TA-SWISS, Bern
Gestaltung und Illustrationen: Hannes Saxer, Bern
Druck: Jordi AG – Das Medienhaus, Belp

TA-SWISS – Stiftung für Technologiefolgen-Abschätzung

Neue Technologien bieten oftmals entscheidende Verbesserungen für die Lebensqualität. Zugleich bergen sie mitunter aber auch neuartige Risiken, deren Folgen sich nicht immer von vornherein absehen lassen. Die Stiftung für Technologiefolgen-Abschätzung TA-SWISS untersucht die Chancen und Risiken neuer technologischer Entwicklungen in den Bereichen «Biotechnologie und Medizin», «Informationsgesellschaft» und «Mobilität / Energie / Klima». Ihre Studien richten sich sowohl an die Entscheidungstragenden in Politik und Wirtschaft als auch an die breite Öffentlichkeit. Ausserdem fördert TA-SWISS den Informations- und Meinungsaustausch zwischen Fachleuten aus Wissenschaft, Wirtschaft, Politik und der breiten Bevölkerung durch Mitwirkungsverfahren. Die Studien von TA-SWISS sollen möglichst sachliche, unabhängige und breit abgestützte Informationen zu den Chancen und Risiken neuer Technologien vermitteln. Deshalb werden sie in Absprache mit themenspezifisch zusammengesetzten Expertengruppen erarbeitet. Durch die Fachkompetenz ihrer Mitglieder decken diese Begleitgruppen eine breite Palette von Aspekten der untersuchten Thematik ab.

Die Stiftung TA-SWISS ist ein Kompetenzzentrum der Akademien der Wissenschaften Schweiz.

TA-SWISS
Stiftung für Technologiefolgen-Abschätzung
Brunngasse 36
CH-3011 Bern
info@ta-swiss.ch
www.ta-swiss.ch

mitglied der
akademien der wissenschaften schweiz