

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus

8. Januar 2018

Sie verbraucht mehr Energie als Irland und verändert gerade die Welt: Nimm dir endlich Zeit, die Blockchain zu verstehen.

Der US-Amerikaner Erik Finman kaufte im Jahr 2011 Bitcoins ^{*1} – damals für 12 Dollar pro Stück, heute ist er Millionär. ^{#1} Mittlerweile ist jeder einzelne Bitcoin über 12.000 Euro wert ^{*2} und die digitale Währung wird sogar ^{*3} an der Börse gehandelt. ^{#2}

Heute gibt es Marktplätze, ^{#3} Online-Casinos, ^{*4} Magazine, Foren, Ratgeber ^{#4} und Starterpakete ^{*5} für das Thema Bitcoins. Ihren ursprünglichen Sinn als Zahlungsmittel haben Bitcoins aber weitgehend verloren. ^{*6} Sie sind zum beliebten Spekulationsobjekt geworden – jeder will der nächste Erik Finman sein. Doch Finanzexperten warnen immer eindringlicher vor der Spekulationsblase. ^{#5} Viele Händler, die die Währung akzeptiert hatten, sind mittlerweile genervt von den heftigen Kursschwankungen und springen ab. ^{*7} Die Tage von Bitcoins scheinen gezählt. ^{*8}

Die Technologie hinter Bitcoins aber – die »Blockchain« – hat das Potenzial, die Welt zu verändern.

So funktioniert die Blockchain, Harry

Die Technologie hinter der Blockchain wirkt leicht wie Magie. Deshalb holen wir uns zum Verständnis Harry Potter ^{*9} zur Hilfe. Stelle dir vor:

*Harry braucht dringend einen neuen Zauberstab, hat aber kein Geld dabei und die Kobold-Bank hat gerade geschlossen. Doch in der Welt von Harry Potter ist eine Bank gar nicht mehr notwendig. Harry und der Zauberstab-Händler holen ihre magischen Bücher ^{*10} aus der Tasche und schreiben darin auf, dass Harry ihm 7 Galeonen schuldet. Den neuen Zauberstab darf er dafür direkt mitnehmen. Alle magischen Bücher sind miteinander verbunden, in jedem steht immer dasselbe. Identische Kopien liegen auch bei Hermine und Ron – die beide darin Harrys Schulden nachlesen können.*

*Später will Harry seine Schulden loswerden; er hebt Geld ab, bringt es zum Zauberstab-Händler und beide notieren das in ihren Büchern. Hermine und Ron sehen nun, dass die Schulden beglichen sind und bestätigen das. ^{*11} Damit haben alle 4 Beteiligten einen Konsens darüber, was passiert ist. Harry ist seine Schulden los und die Bücher dokumentieren den Ablauf. Hätte Harry einfach versucht, zu schummeln und allein seine Schulden zu löschen, hätte das der Zauberstab-Händler gesehen und seine Zustimmung nicht gegeben.*

Das ist natürlich nur eine grobe Analogie, die aber das Prinzip hinter Blockchain erklärt: das Verteilen von gesicherten Informationen und deren Absicherung durch Dritte. Das magische Buch ist in Wirklichkeit eine Datenbank – die als Teil eines Computer-Netzwerks ständig über das Internet aktualisiert wird. Die Kopien liegen dabei nicht in der Hand von wenigen, sondern Tausenden anderer Nutzer und sind mit kryptographischen Signaturen ^{*12} versehen gespeichert. Die Datenbank enthält alle bisherigen Transaktionen. Regelmäßig wird sie von aktiven Teilnehmern – sogenannten »Minern« – unveränderlich gespeichert ^{*13} und ein neuer Datenblock beginnt. ^{*14}

Sie erschaffen quasi das nächste Kapitel des »magischen Buchs« für alle. Die vorherigen Kapitel werden abgeschlossen und niemand kann mehr in ihnen

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

schreiben.

So entsteht mit der Zeit eine Kette von aneinander anschließenden Datenblöcken – die »Blockchain«.

Aus diesen 5 Gründen gehört der Blockchain die Zukunft

Blockchain, da sind sich die meisten Nerds einig, ist für die Digitalwelt eine mindestens genauso bedeutende Erfindung wie Harry Potter für den Kosmos der Jugendliteratur. Diese 5 Eigenschaften machen die neue Technologie gemeinsam einzigartig.

- > **Dezentralität:** Das Blockchain-Protokoll ist online und dezentral, das heißt, es braucht keine Institutionen als Mittelsmann, um zu funktionieren. ^{*15} Es gibt keine Firma oder Regierung, die eine Anwendung der Blockchain wartet und kontrolliert. Das schützt vor Korruption und dem Einfluss von politischen Interessen. Fällt ein Teil des Netzwerks aus, kann der Rest der Blockchain weiterarbeiten.
- > **Sicherheit:** Durch die dezentrale Aufteilung der Daten ist es praktisch unmöglich, eine Blockchain zu manipulieren. ^{*16} Ein Hacker müsste nicht nur einen Rechner manipulieren, sondern Tausende gleichzeitig. ^{*17} Die Daten bleiben so lange archiviert, wie die Blockchain existiert. So können auch Jahre später noch Aktionen überprüft und nachvollzogen werden – aber nur von demjenigen, der im Besitz des richtigen kryptographischen Schlüssels ist. ^{*18}
- > **Datenschutz:** Was ein Nutzer tut, wird zwar in den Daten der Blockchain genau protokolliert, aber nur seine Anwendungs-Adresse ^{*20} wird gespeichert. Damit kann Blockchain für Anwendungen auch ohne persönliche Daten funktionieren – die Firmen sonst nur allzu gern abgreifen. ^{#9}

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- > **Hohe Verfügbarkeit:** Blockchain-Anwendungen sind nicht an Öffnungszeiten oder Feiertage gebunden. Und da die Anwendung ohne große Hürden jederzeit heruntergeladen werden kann, kann auch kein Mittelsmann beschränken, wer daran teilnehmen darf. So können auch Menschen zum Beispiel Bankgeschäfte tätigen, die vorher keinen Zugang hatten – etwa Geflüchtete.
- > **Open Source:** Der Programmcode für viele Blockchain-Anwendungen steht frei im Internet zur Verfügung. Damit kann jeder ^{*21} an neuen Projekten mitarbeiten und seinen Beitrag leisten. Damit ist Blockchain auch ein Jobmotor in der Tech-Szene. Es herrscht Aufbruchsstimmung.

Moment mal, wo waren die Haken – gibt es etwa keine? Gibt es doch. und lass dir die Nachteile der Blockchain anzeigen.

Zusammen genommen sind diese 5 Aspekte eine bahnbrechende Innovation: Diese ermöglicht, statt einer einzelnen Institution (und damit Menschen) zu vertrauen, ein dezentrales, datensicheres, ausfallsicheres und transparentes Netzwerk zu nutzen. Korruption und Manipulation, ob vorsätzlich oder nicht, sind damit quasi ausgeschlossen.

Bitcoins waren nur die erste Anwendung, die diese Vorteile nutzte und damit Erfolg hatte. Doch das ist nur der Anfang: Moderne Blockchain-Software wie Ethereum ^{*24} kann viel mehr und ist dabei enorm flexibel. Sie bietet einen technischen Rahmen und dient für viele moderne Blockchain-Projekte als Basis.

*>>Die Blockchain-Technologie bietet neue Möglichkeiten, die vorher noch nicht da waren. Aber sie ist auch noch in einer frühen Phase, in der vor allem viele Ideen und Konzepte entwickelt werden, während nur wenige die Technologie bereits praktisch austesten.<< – Blockchain Bundesverband ^{*25}*

Du willst Beispiele? An den folgenden 3 Anwendungen wird aktuell gearbeitet – und du hast wahrscheinlich nicht an sie gedacht!

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

1. Die transparente Produktion für jede Pille

Jutta Steiner ist die Geschäftsführerin von Parity Technologies, einer Software-Schmiede in London und Berlin für Blockchain-Anwendungen, die zwischen Beteiligten Vertrauen und Transparenz stiften. Das Ziel ist »Polkadot«, eine Meta-Blockchain ^{*26} die es unterschiedlichen Blockchains erlaubt, zusammenzuarbeiten.

»Über Jahrhunderte haben wir in unserer Gesellschaft Institutionen geschaffen, die es uns erlaubt haben, in großem Umfang zusammenzuarbeiten. Das Blockchain-Protokoll erlaubt nun, digitale Güter und Rechte ohne solche zwischengeschalteten Institutionen zu verwalten. Das ist nicht weniger als Digitalisierung von Autorität und eine Innovation, die man nicht hoch genug einschätzen kann.« – Jutta Steiner, Geschäftsführerin von Parity Technologies

Konkret könnten so E-Books oder Musikdateien dezentral verwaltet werden. Statt bei Händlern wie Amazon liegen die Original-Dateien dann auf dem eigenen Heimrechner und die Blockchain führt Buch darüber, wem sie kopiert oder verkauft werden – eine neue Vertriebsmöglichkeit für Künstler, ohne Konzerne.

Eine andere Anwendung könnte Produktionsketten transparenter gestalten. ^{*27} Alle einzelnen Verträge und Transaktionen einer Produktion – etwa von Medikamenten – werden dann in der Blockchain abgespeichert. Diese Blockchain liegt im Unterschied zu einer normalen Excel-Tabelle bei jedem Zulieferer. Kein Einzelner kann also einfach Daten manipulieren und jeder mit Berechtigung kann die Produktionswege überprüfen.

»Geht am Ende beim Patienten etwas schief, lässt sich der Vorfall dann vollständig nachvollziehen. Aktuell ist das nahezu unmöglich. Es existiert einfach keine lückenlose Informationskette.« – Jutta Steiner, Geschäftsführerin von Parity Technologies

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

Durch die gegenseitige Kontrolle können Fehler oder Versäumnisse aber schon im Vorfeld vermieden werden. Betrug wird erschwert und offene Zusammenarbeit erleichtert. Außerdem spart eine solche Art der Dokumentation auch einen Haufen Papierkram.

2. Die eigene digitale Identität besitzen

Kai Wagner ^{*28} arbeitet für die Berliner Softwarefirma Jolocom an einer Anwendung der Blockchain für eine neue, digitale Identität.

»Mich interessiert an Blockchain vor allem das gesellschaftliche Potenzial, also eine demokratieverträglichere Digitalisierung zu ermöglichen, in der Monopole aufgelöst werden.« – Kai Wagner von Jolocom

Eine Maßnahme gegen solche Monopole könnte es sein, die persönlichen Daten aus den Händen von Internet-Unternehmen zu befreien. Statt auf den Servern von Datenkraken wie Facebook, Google oder Amazon liegen dann alle Informationen der Identität gebündelt auf dem eigenen Smartphone. ^{*29} Welche Informationen und Berechtigungen jeder Nutzer (durch die Blockchain) herausgibt, an wen, wann und wie lange, entscheidet er dann ausschließlich selbst. ^{*30}

Auch dritte Unternehmen, mit denen der Nutzer dann interagiert und bei denen er sich per »Google«-Login anmeldet, begeben sich in die Hände der Tech-Unternehmen und müssen nach deren Spielregeln spielen. Das Geschäftsmodell der Tech-Riesen ist auch für diese Firmen zum Nachteil.

Damit würde außerdem mehr Transparenz über alle eigenen Datenspuren im Netz entstehen. Als Bonus bräuchte man dann nur noch ein einziges Passwort für alles, statt sich immer neu registrieren zu müssen. Mit dieser gesicherten Identität wären sogar theoretisch Wahlen ^{#16} möglich.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

Doch Kai Wagner sieht auch Hürden, wenn Blockchain langfristig Erfolg haben soll:

»Eine Baustelle ist aktuell noch das Proof-of-Work-Konzept, also dass viele Miner quasi dasselbe tun. Hier muss für die Zukunft eine andere Lösung gefunden werden, die weniger Energie verbraucht und trotzdem die Kette gut absichert.« – Kai Wagner von Jolocom

3. Die Blockchainisierung der Welt

Fabian Vogelsteller arbeitet am Herzen von Ethereum, dem aktuell vielversprechendsten Protokoll ^{*31} für Blockchain-Anwendungen. Er hat 2 der wichtigeren Anwendungen für Ethereum bisher programmiert, mit denen jeder die Ethereum-Blockchain nutzen kann. ^{#17}

»Wer der Erste ist und mitmacht, wird natürlich Vorteile haben. Das verstehen auch viele heutzutage. Damals beim Internet haben noch alle gelacht, dann hat es alles verändert. Blockchain fühlt sich jetzt ähnlich an und niemand will am Ende der Dumme sein.« – Fabian Vogelsteller, Entwickler bei Ethereum

Fabian baut an einer Welt, in der klassisches Vertrauen zu Unternehmen nicht mehr nötig ist, da alles transparent über das Ethereum-Protokoll abgewickelt wird. Das kann in Zukunft zu einer ganz neuen Infrastruktur führen – zu welcher genau, ist auch für viele Blockchain-Profis noch nicht ganz klar.

»Das Potenzial ist einfach so groß, dass wir heute noch nicht absehen können, was es alles verändern wird.« – Fabian Vogelsteller, Entwickler bei Ethereum

Aktuell arbeiten Fabian und seine Kollegen daran, einzelne Anwendungen und ganze Blockchains miteinander zu einem gemeinsamen Ökosystem zu verschränken. Je mehr Bereiche unseres Lebens wir ins Digitale verlagern, desto mehr praktische Anwendungen von Blockchain sind denkbar – als virtueller Gläubiger bei Vertragsschlüssen, als sicherer Speicher für sensible Daten, zum Nachprüfen von Produktionswegen oder

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

doch am Ende als digitale Währung über Ländergrenzen und Bankinteressen hinweg.

In einem sind sich aber alle einig, die heute am Thema Blockchain arbeiten: Die Technologie wird der nächste Meilenstein der Digitalisierung sein. Vieles spricht dafür, wenn Programmierer Wege finden, die Nachteile der Technologie auszubügeln.

Und dabei besteht die Chance, die Fehlentwicklungen des Internets auszugleichen und zurück zu einer dezentralen, demokratischeren Struktur zu finden. Da heute Tech-Giganten wie Google oder Facebook große Teile der digitalen Welt unter sich aufgeteilt haben, ^{#18} wäre dezentrale Konkurrenz sicher nicht verkehrt.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

Zusätzliche Informationen

- *1 Bitcoins entstanden Ende 2008. Damals veröffentlichte jemand unter dem Pseudonym Satoshi Nakamoto in der »Cryptography Mailing List« ein Paper, in dem er das Konzept einer elektronischen Währung vorstellte, die auf einem kryptographischen Beweis beruht. Bis heute ist Satoshi Nakamoto ein Unbekannter. Einen Monat später, Anfang 2009, veröffentlichte Nakamoto die Software. Nakamoto besitzt 980.000 Bitcoins, was [ihn heute durch den Wertanstieg zu einer der reichsten Personen der Welt macht. \(englisch\)](#)
- *2 Allein im vergangenen Jahr stieg der Kurs um 500% und mehr an. Da ist es kein Wunder, dass Bitcoins heute auch Hedgefonds interessieren, die den Kurs durch Millionen-Investitionen in die Höhe treiben. Kurz nach dem Start der Bitcoin-Futures kratzte die Kryptowährung sogar an der 20.000-Dollar-Marke, fiel dann aber wieder stark ab. Generell ist der Wert von Bitcoins starken Schwankungen unterworfen.
- *3 Bitcoin-Handel gibt es bisher erst an wenigen Börsen, etwa an der Chicago Mercantile Exchange (CME), per Future – einem standardisierten Terminkontrakt. Ein Vertragspartner verpflichtet sich dadurch, eine Menge eines Finanztitels zu einem festen Preis zu einem bestimmten Zeitpunkt zu liefern. Die Abnahme ist dabei ebenfalls vertraglich festgelegt. Futures werden an eigenen Terminbörsen gehandelt.
- *4 Bitcoin-Casinos lassen die Spieler mit Bitcoins bezahlen und sind häufig auf mobiles Spielen unterwegs ausgelegt.
- *5 [Starterpakete](#) versprechen den schnellen Einstieg in die Bitcoin-Thematik. Dazu gibt es meist Erklärvideos, Zugang zu Ressourcen sowie E-Books und eine App für das Smartphone, um Bitcoins leicht zu kaufen und zu verkaufen.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *6 Dennoch ermöglichen viele große Firmen mittlerweile, dass man bei ihnen mit Bitcoins einkauft; darunter Amazon, Edeka oder Starbucks.
- *7 Darunter etwa der Online-Spieledienst [Steam \(englisch\)](#) oder Computerriese [Dell \(englisch\)](#). Denn durch die heftigen Schwankungen der Währung müssen die Händler die Preise ständig anpassen. Dazu kommen steigende Transaktionsgebühren, eine hohe Transaktionszeit von teilweise über 4 Stunden und geringe Nachfrage als Zahlungsmittel.
- *8 Das ist jedenfalls die Meinung der meisten Experten. Tatsächlich sind Bitcoins auch technisch gezählt: Regelmäßig schafft das Bitcoin-Netzwerk durch sogenannte »Miner« neue Bitcoins – eine Arbeit, die vor allem viel Rechenpower benötigt. Etwa alle 4 Jahre halbiert sich aber rechnerisch die Anzahl an neuen Bitcoins, die ins System kommen. Der unbekannte Entwickler der Bitcoins, der unter dem Pseudonym Satoshi Nakamoto bekannt ist, legte dies parallel zur Schürfrate von Gold fest. Die Zahl an Bitcoins ist insgesamt auch auf 21 Millionen limitiert. [Der letzte Bitcoin wird vermutlich um das Jahr 2140 herum gehoben werden. \(englisch\)](#)

Doch schon lange vorher dürfte die Technologie an ihre Grenzen stoßen. Der Grund liegt darin, dass jeder beteiligte Rechner die gesamte Blockchain speichern muss. Die Bitcoin-Chain ist aktuell etwas über 100 Gigabyte groß und wächst immer schneller – zwar noch langsamer als die Speicherkapazität moderner Computer. Brechen aber die beteiligten Rechner weg, kann Bitcoin nicht mehr aufrechterhalten werden.

- *9 Harry Potter von J.K. Rowling ist längst keine Jugendbuch-Reihe mehr, sondern ein Kulturphänomen. Die Kurzfassung: Der Waisenjunge Harry Potter lernt an der Magier-Schule Hogwarts die Zauberei, seine Freunde Ron und Hermine sowie seinen Rivalen Draco Malfoy kennen. Die ständige Bedrohung der Buchreihe ist der finstere Magier Voldemort, der ein faschistisches Regime errichtete und Harrys Eltern ermordete.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *10 Harry wäre in diesem Beispiel ein »Node«, also ein Nutzer des Blockchain-Netzwerks. Sein magisches Buch wäre eine Blockchain-Datei auf einem Rechner (»ledger«) und Teil eines »peer-to-peer«-Netzwerks.
- *11 Das Bestätigen nennt man »Proof of Work«-Prinzip. Dazu müssen die Teilnehmenden die Informationen wie die Identität von Harry oder den Gegenstand der Transaktion (den Zauberstab) nicht einmal kennen – sie müssen nur bestätigen, dass die Regeln des Systems eingehalten wurden.
- *12 Diese Verschlüsselung schützt die Daten effektiv vor Mitlesern. Dabei handelt es sich um eine sogenannte »Asymmetrische Verschlüsselung« – die Daten werden mit einem mathematischen Schlüssel verschlüsselt (der kann sich aber nicht entschlüsseln) und mit dem anderen entschlüsselt (der kann aber nicht verschlüsseln). Das ganze Blockchain-System hängt von der Sicherheit dieser Verschlüsselung ab. Die kryptographischen Signaturen erlauben damit schnelle und eindeutige Verifikation der gesamten Historie. [Hier](#) findest du einen tieferen Einstieg in die dahinterstehende Mathematik.
- *13 Um einen solchen Speichervorgang durchzuführen und einen Datenblock zu erzeugen, muss der Rechner des Teilnehmers ein mathematisches Rätsel lösen – das immer schwieriger wird, je länger die Blockchain ist. Ist der Speichervorgang erfolgreich, schickt der »Miner« den Block an alle Empfänger der Blockchain. Als Belohnung erhält er sogenannte »Coins« der jeweiligen Blockchain, die ganz allgemein als Währung dienen können. Bei Bitcoin ist diese Währung der Hauptzweck und die Blockchain dient ihrer Aufrechterhaltung und Verwaltung.

Haben 2 Miner gleichzeitig Erfolg, kommt es selten zu einer kurzfristigen Teilung der Blockchain – einem sogenannten »Fork«. Die Kette wird an beiden Blöcken solange fortgeführt, bis ein Zweig länger ist als der andere. Die Blöcke im kürzeren Zweig werden dann gelöscht und die darin gebundenen Transaktionen wieder dem Pool der unbestätigten Transaktionen hinzugefügt.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *14 Die Größe eines durchschnittlichen Datenblocks liegt etwa bei der Bitcoin-Chain **bei 1,07 Megabyte**. Jeder Datenblock enthält eine Auflistung aller kürzlich erfolgten Datenveränderungen (zum Beispiel Transaktionen) und eine eindeutige Referenz zum vorherigen Block als Prüfsumme. Neue Datenblöcke werden von sogenannten »Minern« erstellt, also Teilnehmern im Netzwerk, die aktiv mitarbeiten und ihre Rechenleistung zum Aufrechterhalten der Blockchain zur Verfügung stellen. Ihre Rechner lösen dazu eine mathematische Aufgabe, deren Antwort in jedem Block unterschiedlich ist. Neue Blöcke werden vom Netzwerk nur akzeptiert, wenn sie die richtige Antwort enthalten. Damit entsteht allerdings auch ein Wettbewerb zwischen Minern, denn wer die Aufgabe zuerst löst und an das Netzwerk schickt, wird akzeptiert. Die erfolgreichen Miner erhalten dafür eine Belohnung, etwa im Fall der Bitcoin-Chain eben eine Anzahl der Kryptowährung Bitcoin.
- *15 Natürlich müssen sie erst einmal programmiert werden, weshalb aktuell so viele Blockchain-Start-ups aufgebaut werden. Jeder möchte derjenige sein, der die Anwendung schafft, die demnächst einen Standard definiert.
- *16 Theoretisch wäre es denkbar, das System zu manipulieren, wenn sich über 51% der aktiven Miner zusammenschließen. Wenn 2 Blöcke gleichzeitig entstehen, entscheidet nämlich die Mehrheit der Teilnehmer darüber, welcher Block die Kette fortführt. Er könnte so einen vorher erstellten Blockchain-Teil anfügen, der ihn begünstigt. Doch das ist unwahrscheinlich, da es einen sehr hohen logistischen Aufwand benötigt. Blockchain-Programmierer nennen diesen theoretischen Fall die »51-Percent-Attack«. Bei Bitcoins ist die Gefahr dadurch höher, dass **ein Großteil der »Miner« sich in großen Pools zusammenschließen** und dazu noch alle in demselben Land – China – sitzen.
- *17 Dazu existieren einzelne Blöcke in einer festen Reihenfolge, verbunden durch ihre Prüfsumme. Je tiefer ein Datenblock in der Blockchain sitzt, desto unwahrscheinlicher ist es, dass ein möglicher Hacker es schafft, diese Blockchain bis zum Datenblock zurück zu entschlüsseln.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *18 Damit wird der größte Schwachpunkt eines jeden traditionellen Computersystems obsolet gemacht: der Mensch in Form des Administrators, der am Ende des Tags Systeme durch Social Engineering angreifbar macht.
- *19 Wenn nur 10% der Weltbevölkerung eine Blockchain-Technologie nutzen, würden dafür rund 1/4 der weltweiten Stromproduktion in Anspruch genommen. Mit der aktuellen Blockchain-Technologie ist also derzeit keine Flächendeckung möglich.
- *20 Bei Bitcoins »Digital Wallet« genannt. Das ist eine einfache App auf einem Heimrechner oder Smartphone, die mit der jeweiligen IP-Adresse versehen ist. Moderne Blockchains erstellen für jede Transaktion eine neue Anwendungs-Adresse und sind damit sogar noch sicherer.
- *21 An aktuellen Blockchain-Lösungen arbeitet derzeit eine Gemeinschaft von Start-ups, einzelnen Programmierern und Stiftungen weltweit in einer sogenannten »Open-Source-Environment«. Der Programmcode ist dabei von allen einsehbar. Die Lizenzen erlauben es, Codestücke von anderen wiederzuverwenden – über Unternehmensgrenzen hinweg.
- *22 Eine Plattform für die Entwicklung von Open-Source-Anwendungen, an der jeder teilhaben kann.
- *23 Eine Übersicht über die aktuellen Kryptowährungen und ihren Kurs bei [CoinGecko](#). Natürlich entspricht das der »Fail-better«-Mentalität von Start-ups und durch das Open-Source-Prinzip können Projekte Lösungen von anderen Projekten verwenden. Damit wächst die Blockchain-Technologie insgesamt auch mit Fehlschlägen. Verwirrend ist dies nur für die Endnutzer.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *24 Im Gegensatz zur Bitcoin-Chain kann Ethereum über vollzogene Transaktionen mit der Blockchain statistische Informationen hinzufügen, interaktive Objekte oder intelligente Kontakte – die alle vorher programmierten Regeln entsprechen müssen. Außerdem sind die Ether-Coins nicht fest auf eine Zahl limitiert, wie etwa Bitcoins, sondern werden stattdessen mit einem jährlichen Maximum erzeugt. Beliebt ist Ethereum vor allem bei Start-ups, die sich damit mit Kapital versorgen und die strengen Prozesse bei der Kapitalvergabe von Banken umgehen.
- *25 Der [deutsche Blockchainverband](#) besteht aus Vertretern von Unternehmen, die im Bereich Blockchain arbeiten. Dazu kommen Vertreter von allen großen Parteien der letzten Legislaturperiode plus der FDP. Das Ziel des Verbandes ist es, für Deutschland Rechtssicherheit im Bereich Blockchain zu schaffen und den Standort für Entwicklungen in dem Bereich zu verbessern.
- *26 Die Meta-Blockchain könnte damit Anwendungen erlauben, die selbst mit heutigen Blockchains schwer umgesetzt werden können.
- *27 Jutta Steiner verfolgt dieses Ziel als Mitgründerin des Londoner Start-ups Project Provenance Ltd. Produktionsketten sind dabei technisch sogenannte »Mehrstufentransaktionen«.
- *28 Außerdem ist er Mitglied bei Perspective Daily!
- *29 Wird das Smartphone verloren oder gestohlen, ist das kein Beinbruch. Der darauf abgespeicherte »Datentresor« kann beliebig als Backup gespeichert werden. Wird das Passwort vergessen, können nahe Freunde und Mitglieder der Familie benannt werden, die dann die Identität bestätigen und ermöglichen, den Passwortschlüssel neu zu generieren.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- *30** Aktuell begibt sich der Nutzer für seine digitale Identität noch ganz in die Hände von solchen Tech-Unternehmen. Diese nutzen dann die gesammelten Daten zur Analyse des Nutzerverhaltens und zur Optimierung von Werbung. Außerdem behalten sich die Unternehmen stets per AGB vor, das Nutzer-Konto »ohne Angabe von Gründen« jederzeit zu löschen.

- *31** Die bekannteste Anwendung von Ethereum ist Ether, eine Kryptowährung. Sie könnte Bitcoins beerben.

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

Quellen und weiterführende Links

- #1** Erik Finmans Geschichte bei CNBC (englisch, 2017)
 <https://www.cnbc.com/2017/06/20/bitcoin-millionaire-erik-finman-say-s-going-to-college-isnt-worth-it.html>

- #2** Der Start des Future-Handels für Bitcoins auf der Börse CME im Dezember
 (2017)
<https://deutsche-wirtschafts-nachrichten.de/2017/12/18/boerse-cme-eroeffnet-future-handel-fuer-bitcoin/>

- #3** Ein Überblick über die gängigsten Bitcoin-Handelsplattformen beim
 Krypto-Magazin (2017)
<https://www.krypto-magazin.de/krypto-boersen-vergleich/>

- #4** Das Bitcoin-Handbuch von Felix Mago (2016)
 https://www.buch7.de/store/product_details/1026341994

- #5** Eine Analyse der Bitcoin-Blase auf börse.ard.de (2017)
 <https://boerse.ard.de/boersenwissen/boersenwissen-fuer-fortgeschrittene/wehe-wenn-die-bitcoin-blase-platzt100.html>

- #6** Die Alternative ist eine Teil-Abspaltung wie bei Bitcoin Cash im August
 2017. Die Meldung dazu bei der österreichischen Innovationsplattform
>>der Brutkasten<<
<https://www.derbrutkasten.com/a/abspaltung-tag-der-entscheidung-fuer-bitcoin/>

- #7** Der Bitcoin Energy Consumption Index bei Digiconimist.net
- <https://digicono.net/bitcoin-energy-consumption>

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- #8** Die HuffPost erklärt hier, warum Bitcoins auch noch in China beliebt sind
 und die chinesische Regierung dagegen vorgeht (2017)
http://www.huffingtonpost.de/robert-brungert/darknet-wahrung-bitcoin-z_b_18021328.html
- #9** In diesem Text erkläre ich dir, warum Daten viel wert sind und die Krake
 nicht alles wissen muss
<https://perspective-daily.de/article/65>
- #10** Diese Studie untersuchte die Warenwege im Darknet (englisch, 2017)
 <http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085>
- #11** Ewald Nowotny, Präsident der Österreichischen Notenbank, findet, dass
 Bitcoins auch Kriminellen helfen (2018)
<http://www.sueddeutsche.de/wirtschaft/kryptowaehrung-bitcoin-hilft-kriminellen-1.3811342?reduced=true>
- #12** Der Trojaner CryptoShuffler stiehlt Bitcoins im Wert von 140.000 Dollar;
 die Meldung von Kaspersky-Labs (2017)
<https://www.kaspersky.de/blog/cryptoshuffler-bitcoin-stealer/15144/>
- #13** Ein Vergleich der Transaktionen pro Sekunde von Blockchains, Paypal und
 VISA (2017)
<http://www.altcointoday.com/bitcoin-ethereum-vs-visa-paypal-transactions-per-second/>
- #14** Forscher der Universität Sydney haben eine Blockchain entwickelt, die
 7-mal schneller als VISA ist (englisch, 2017)
<http://redbellyblockchain.io/>
- #15** Viele Blockchain-Projekte scheiterten – die Meldung auf CNBC (englisch,
 2017)
<https://www.cnn.com/2017/11/09/just-8-percent-of-open-source-blockchain-projects-are-still-active.html>

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N

- #16** David Ehl erklärt, wie die Blockchain eine sichere und geheime Wahl gestalten kann
 <https://perspective-daily.de/article/90/>
- #17** Link zum Ethereum-Wallet und dem Mist-Browser (englisch)
- <https://daowiki.atlassian.net/wiki/spaces/DAO/pages/1212461/Mist>
- #18** Das Ranking der weltweit größten Medien bei Zenith (englisch, 2017)
 <https://www.zenithmedia.com/google-facebook-now-control-20-global-adspend/>

Dirk Walbrühl

Neben dieser Technik sehen Bitcoins alt aus
perspective-daily.de/article/429/SXhop59N