Blockchain: Eine verschlüsselte Kette für sämtliche Transaktionen. Bild: istock

Blockchain für Anfänger

«Block.... Hä?» – Es vergeht kein Tag, ohne dass man diesem Begriff, der übersetzt «Blockkette» bedeutet, begegnet. Experten erklären, dass diese Kette die Welt verändern wird und die liechtensteinische Regierung will ein Gesetz dazu machen. Trotzdem verstehen die meisten nur Bahnhof. Ein Erklärungsversuch.

VON JÖRG EUGSTER*

Hand aufs Herz: Wissen Sie, was die Blockchain ist? Könnten Sie es Ihrer Grossmutter erklären, sodass sie es versteht? Und dabei vergeht kaum ein Tag, an dem man nicht einen Artikel über die Blockchain lesen könnte. Doch leider wird die Blockchain immer viel zu technisch erklärt. Wichtig ist, dass wir deren Konzept und Nutzen verstehen. Letztlich nützt die beste Technologie nichts, wenn wir keinen Nutzen daraus ziehen können. Ich versuche in diesem Artikel, die Blockchain so zu erklären, dass der Nutzen daraus folgerichtig erkannt wird.

Blockchain ist nicht Bitcoin

Bestimmt haben Sie schon von Bitcoin gehört oder gelesen. Das wäre auch fast ein Wunder, wenn dem nicht so wäre, denn das Thema Bitcoin ist sehr omnipräsent. Zuerst einmal müssen wir den Unterschied der beiden festhalten:

- Blockchain ist eine Basistechnologie, auf der man entsprechende Anwendungen entwickeln kann.
- Bitcoin ist eine solche Anwendung, die auf dem Blockchain-Konzept bzw. auf der Blockchain-Technologie basiert. Bitcoin wird auch als Kryptowährung bezeichnet.

Was ist die Blockchain?

Blockchain ist eine dezentrale, hoch verschlüsselte Datenbank. Das tönt auf den ersten Eindruck etwas langweilig, doch versteckt sich dahinter eine der grössten Entwicklungen unserer Zeit.

Stellen Sie sich vor, Sie leihen einem Freund 100 Franken. Nach einem Monat möchten Sie Ihre 100 Franken wieder zurück. Doch Ihr Freund meint, es seien nur 50 Franken gewesen. Doch Sie sind ganz sicher, dass es 100 Franken waren. Wer ist im Recht? Haben Sie einen mündlichen oder schriftlichen Vertrag abgeschlossen? Wurde dieser vom Notar beglaubigt? Wohl kaum. So haben Sie ein Vertrauensproblem Ihrem Freund gegenüber. Künftig werden Sie das bestimmt schriftlich abwickeln. Und vermutlich ist er danach nicht mehr Ihr Freund. Ihr Vertrauen hat er verspielt.

Und dabei ist das eine ganz normale Transaktion, wie sie häufig vorkommt. Wenn Sie das mit einer Bank gemacht hätten, hätte diese die Transaktion in ihrer Datenbank gespeichert und hätte Ihnen eine Quittung gegeben. Doch könnte der Bankserver oder Ihr Online-Zugang dazu gehackt werden. Keine Transaktion ist sicher. Je nach Medium kann sie gehackt, vergessen oder gestohlen werden.

Und genau hier setzt das Konzept der Blockchain auf. Sie ist sicherer, weil sie die Transaktionen dezentral und verschlüsselt speichert. Die gleiche Transaktion wie oben: Sie leihen Ihrem Freund 100 Franken aus. Im Raum sitzen 200 Zeugen, die die Transaktion notieren: A leiht B 100 Franken am xx.xx.xx um yy:yy Uhr aus. Jetzt wird diese Transaktion mit einem Algorithmus mit der vorhergehenden Transaktion verschlüsselt. Sobald 101 Zeugen, also mehr als die Hälfte, die Transaktion notieren und mit der vorherigen verschlüsselt haben, gilt diese als bestätigt.

Nach einem Monat möchten Sie Ihre 100 Franken wieder zurück. Nun kann Ihr Freund nicht mehr behaupten, es wären nur 50 Franken gewesen, denn nun haben Sie 200 Zeugen, die diese Transaktion notiert und bestätigt haben. Das ist so, wie wenn Sie 200 Notare diese Transaktion haben bestätigen lassen. Ihr Freund müsste jetzt mindestens 101 der Zeugen, also mehr als die Hälfte, gleichzeitig dazu bringen, auszusagen, dass es nur 50 Franken gewesen seien. Wenn diese Zeugen nun nicht mehr im gleichen Raum sind und über die ganze Welt verteilt sind, wird diese Aufgabe ungleich schwieriger. Wenn Ihr Freund die Datenbanken der Zeugen hacken wollte, wäre das noch viel schwieriger, denn er müsste mindestens 101 dieser Datenbanken gleichzeitig hacken, die ja zudem hoch verschlüsselt sind.

Blockchain heisst es deshalb, weil die Transaktionen blockweise gespeichert werden. Und Kette heisst es darum, weil ein Block immer mit dem vorher- und nachherfolgenden Block verschlüsselt und gespeichert wird und so eine Kette bildet. Die Speicherung erfolgt blockweise in einer Kette und genau darum heisst dieses Konzept Blockchain.

Das Wichtigste kommt aber jetzt. Es braucht keinen Intermediär bzw. Zwischenhändler mehr, um eine Transaktion abwickeln zu können. Wenn Sie mit Franken bezahlen, ist immer eine Bank beteiligt. Die Notenbank eines Landes druckt das Geld, das von den Geschäftsbanken in Umlauf gebracht wird. Privatpersonen können bei Geschäftsbanken ein Konto unterhalten und damit bezahlen. Mit Bitcoin oder einer anderen Kryptowährung ist das nicht mehr nötig. Dazu mehr im nächsten Abschnitt über die Kryptowährungen.

Wenn Sie im obigen Fall Ihrem Freund nun Bitcoin statt Franken leihen würden, wäre diese Transaktion auf der Blockchain verewigt. Da die Bitcoin-Blockchain über 100 000 Nodes umfasst, so werden die Datenbanken und Server der Zeugen bezeichnet, müssten gleichzeitig über 50 000 Nodes gehackt werden. Die Blockchain selber gilt heute als nicht hackbar. Der Aufwand wäre zu gross und zu kostspielig; es würde sich schlicht nicht rechnen. Gehackt werden kann allerdings nur das Wallet. Dazu mehr im nachfolgenden Kapitel über die Kryptowährung.

> «Das Wichtigste: Es braucht keinen Zwischenhändler mehr, um die Transaktion abzuwickeln.»

Was ist eine Kryptowährung?

Bitcoin ist eine Kryptowährung, die auf der Blockchain-Technologie basiert. Um jemandem Bitcoin zu überweisen, braucht es keine Bank mehr.

So könnte man bezahlen. Bild: iStock

Die Transaktion wird auf der Blockchain gespeichert. Dazu hat jeder Teilnehmer eine Kontonummer, die einer IBAN-Kontonummer ähnlich ist.

Ich besitze mehrere solcher Accounts, die im Fachjargon auch Wallets genannt werden. Einer meiner Wallets für die Kryptowährung Ether lautet wie folgt:

0xC8d64Ce63D77b6B2fB52aD8cc5568D126455c634

Sie dürfen gerne auf mein Wallet Ether überweisen. Dagegen hätte ich nichts. Ether ist nebenbei gesagt die zweitbedeutendste Kryptowährung, die auf der Ethereum-Blockchain gespeichert ist.

Die Überweisung von Kryptowährungen erfolgt von Wallet zu Wallet mit einem öffentlichen Schlüssel. Zugang zur Blockchain bekommt man mit dem Private Key. Nur wer den Private Key kennt, hat Zugang zur Blockchain und zu den Transaktionen. Das ist mit dem Passwort fürs E-Banking vergleichbar. Bei der Blockchain genügt der Private Key, um über die Kryptowährung auf der entsprechenden Blockchain verfügen zu können. Hat man sein Wallet bei einer Kryptobörse gehostet, so empfiehlt es sich, den Zugang wie zum E-Banking ebenso mit den höchsten Sicherheitsstandards zu sichern. Wenn in der Vergangenheit Blockchains gehackt wurden, dann war es nicht die Blockchain selber, sondern das Wallet oder die Kryptobörse. Journalisten machen da bei der Berichterstattung oft keinen Unterschied. Dann gelangt der Hacker an den Private Key und Ihre Bitcoins & Co. sind weg.

Alle Transaktionen auf der Blockchain sind für alle offen einsehbar. Nur weiss man nicht, wer dahintersteckt. Sie dürfen das gerne bei meinem oben genannten Konto machen. Sie können dort auf der Website von https://etherscan.io/ alle meine Transaktionen abrufen. Es kann nichts passieren, denn den Private Key halte ich unter Verschluss.

Was ist ein Token?

Es gibt grundsätzlich drei Arten von Kryptowährungen:

Zahlungs-Token sind mit reinen «Kryptowährungen» gleichzusetzen, ohne mit weiteren Funktionalitäten verknüpft zu sein. Token können die Akzeptanz als Zahlungsmittel entwickeln. Bitcoin ist ein solcher Zahlungs-Token, der bereits über eine grosse Akzeptanz verfügt. Man kann mit Bitcoins keinen weiteren Nutzen generieren. Der Wert hängt alleine von Angebot und Nachfrage ab.

Das italienische Restaurant Made in Italy an der Herrengasse 9 in Vaduz nimmt Bitcoin als Zahlung (siehe Abbildung).

«bitcoin accepted» in Vaduz. Bild: Jörg Eugster

Nutzungs-Token sind Token, die Zugang zu einer digitalen Nutzung oder Dienstleistung vermitteln sollen. Die oben genannte Kryptowährung Ether von der Ethereum Foundation stellt einen Nutzen dar. Ethereums Spezialität sind Smart Contracts. Smart Contracts sind Verträge, die aufgrund einer erfüllten Bedingung ausgeführt werden. Nutzungs-Token werden auf Englisch Utility Token genannt.

Im E-Commerce haben wir z. B. das Vertrauensproblem zwischen Handel und Kunden. Der Handel möchte für sein Paket bezahlt werden und der Kunde möchte für sein Geld die Ware bekommen. Ein Smart Contract kann das Problem lösen. Beim Kauf wird der Betrag auf der Blockchain, analog einer Hotelreservation mit der Kreditkarte, reserviert. Sobald der Kunde dem Paketdienstleister bestätigt, dass das Paket angekommen ist, wird der reservierte Betrag unverzüglich und ohne manuelles Auslösen dem Händler gutgeschrieben.

Ein weiteres Beispiel eines Smart Contracts zeigt die Versicherung Axa, die mit ihrer Flugverspätungsversicherungspolice genau dieses Konzept verfolgt. Der Versicherungsnehmer schliesst diese Police auf einen Flug ab. Ist der Flug um mehr als x Stunden verspätet, bekommt der Versicherungsnehmer seine Entschädigung, ohne dass ein Schadensachbearbeiter diese Zahlung auslösen muss.

Ich selber besitze über 30 Kryptowährungen. Vorwiegend habe ich in Nutzungs-Token investiert. Es gibt hier so viele gute und einleuchtende Konzepte mit einem hohen Mehrwert und Nutzen. Doch würde es den Rahmen dieses Artikels sprengen, mehr darüber zu schreiben. Vielleicht ein anderes Mal in einem Folgeartikel?

Patrick Eugster @Patrick_Eugster · 19 h
Das Internet hat die Art und Weise wie wir miteinander kommunizieren verändert; die #Blockchain verändert die Art und Weise wie wir einander vertrauen

Quelle: https://twitter.com/Patrick_Eugster/status/978929525894631424

Anlage-Token repräsentieren Vermögenswerte wie Anteile an Realwerten, Unternehmen, Erträgen oder einen Anspruch auf Dividenden oder Zinszahlungen. Der Token ist damit hinsichtlich seiner wirtschaftlichen Funktion wie eine Aktie, Obligation oder ein derivatives Finanzinstrument zu werten.

Vielleicht haben Sie schon den Begriff ICO gehört. ICO heisst Initial Coin Offering. Hier geht es um Crowdfunding, also um die Schwarmfinanzierung von Projekten oder Firmen. Statt dass man Wertpapiere herausgibt, gibt man Token oder Coins heraus. Das lässt sich einfacher durchführen als ein IPO. Der IPO, Initial Public Offering, ist die Geldaufnahme über die Börse. Man sagt auch Börsengang. Der Begriff ICO lehnt sich an sein Vorbild, den IPO an.

Der digitale Tsunami kommt

Kürzlich hat mein Sohn Patrick wie folgt getwittert: «Das Internet hat die Art und Weise wie wir miteinander kommunizieren verändert; die #Blockchain verändert die Art und Weise wie wir einander vertrauen.»

Er trifft es auf den Punkt. Dank der sicheren und dezentralen Speicherung der Transaktionen können wir einander besser vertrauen. Ihr Freund – wenn er dann noch Ihr Freund ist – wird dank der Blockchain nicht mehr etwas Unwahres behaupten, denn er weiss, dass die Blockchain nicht hackbar ist und die Wahrheit sagt.

Die grössten Innovationen

In einem Artikel auf cointelegraph.com wurde die Blockchain zu den fünf grössten Innovationen der Menschheit gezählt.

Neben dem Buchdruck, der Elektrizität, dem Radio und dem Internet wird die Blockchain bereits heute in einer Reihe genannt. Wir können aber wohl erst in rund 20 Jahren überprüfen, ob die Blockchain gleichbedeutend ist wie die anderen vier grossen Innovationen.

Ich bin überzeugt, dass das so kommen wird. Wir können vermutlich heute noch nicht einmal im Ansatz erahnen, in welche Richtung uns die Blockchain führen wird. Ich vergleiche das mit der Zeit, als die ersten Personalcomputer aufkamen. Damals fragte man sich ernsthaft, was man mit einem Computer zu Hause machen könne. Wir dachten, dass wir den Weinkeller so verwalten könnten. Doch das tut heute niemand, bestimmt nicht den privaten Weinkeller. Und genau so wird es mit der Blockchain sein. Ich denke nicht, dass uns die Entwicklung des Bitcoins zu neuen Erkenntnissen führen wird, die Blockchain aber ganz sicher, dank Smart Contracts und des Internets der Dinge. Denn die Blockchain ermöglicht neue Geschäftsmodelle. Zum Beispiel könnte Road Pricing oder Parkgebühren automatisch dank Sensoren und einer internen Kryptowährung erfolgen.

In 20 Jahren wird unsere Welt ganz anders aussehen und viele Vorteile bieten, und das nicht zuletzt wegen der Blockchain. Die Blockchain wird ähnlich weitreichende Auswirkungen haben wie seinerzeit das Internet. Ich freue mich darauf.

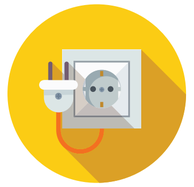
***Über den Autor**

Jörg Eugster ist Internetunternehmer aus Leidenschaft seit 1998. Er hat als Internet-Pionier mehrere Start-ups gegründet und zwei an Medienunternehmer verkaufen können. Er ist Zukunftsbotschafter, Keynote Speaker, Autor, Dozent, Berater und Verwaltungsrat (unter anderem bei der Vaduzer Medienhaus AG). Im vergangenen Jahr hat er ein Buch mit dem Titel «Übermorgen – Eine Zeitreise in unsere digitale Zukunft» veröffentlicht.
https://eugster.info

Fünf bahnbrechende Innovationen in der Menschheitsgeschichte

Die Blockchain wird von Experten bereits zu den fünf grössten Innovationen der Menschheit gezählt. Offen ist, ob und bis wann sie so selbstverständlich ist wie heute das Internet. Auch die Meinungen, in welchen Bereichen sich die Blockkette durchsetzen wird, gehen noch auseinander.

Buchdruck
1436



Elektrizität
1879

Radio
1901

Internet
1960

Blockchain
um 2008