ZT IT-KOLUMNE

© Igor Batrakov/shutterstock.com

Bitcoin, was ist das?

Bitcoin ist eine neue digitale Währung für das Internet. Sie wird kryptografisch abgesichert und benötigt für den Wertetransfer keine Bank. Ist der Bitcoin nur ein Hype oder eine ernst zu nehmende Währung mit Zukunft? Dieser Fachartikel gibt eine fundierte Einführung in die neue Cyber-Währung.

Bitcoin kurz erklärt

Hinter „Bitcoin“ steckt eine digitale Währung, die aus der „Hackerszene“ stammt und auf einem dezentralen Buchungssystem basiert. Alle Überweisungen werden ohne Vorhandensein einer zentralen Abwicklungsstelle (Bank) in einem Netzwerk (Internet) abgewickelt. Für Desktoprechner und Smartphones gibt es kostenfreie Applikationen, die sogenannten „Bitcoin-Brieftaschen“ (engl. „Wallets“). Mit den Wallets können Bitcoins gelagert, empfangen und natürlich auch versendet werden. Nur durch Angebot und Nachfrage wird der Umrechnungskurs von Bitcoin in andere Zahlungsmittel bestimmt.

Das Konzept wurde 2008 von einem Internetnutzer unter dem Pseudonym „Satoshi Nakamoto“ vorgestellt. Wer genau dahintersteckt, weiß man bis heute nicht. Das Bitcoin-Netzwerk entstand am 3. Januar 2009 mit der Berechnung der ersten 50 Bitcoin-Blöcke und basiert auf einer von den Teilnehmern gemeinsam mithilfe einer Bitcoin-Software verwalteten dezentralen Datenbank, der sogenannten Blockchain, in der alle Transaktionen verzeichnet sind (dazu später mehr).

Bitcoin unterliegt daher keiner geografischen Beschränkung. Der Nutzer benötigt nur einen Internetzugang, und es kann länderübergreifend eingesetzt werden.

Bitcoin wird auch als „Kryptowährung“ bezeichnet, da mithilfe von kryptografischer Technik wie die „asymmetrische Verschlüsselung“ sichergestellt wird, dass die Transaktionen mit den Bitcoins nur vom jeweiligen Eigentümer vorgenommen und die Geldeinheiten nicht mehrfach ausgegeben werden können.

Bitcoin benötigt keine Banken

Der entscheidende Unterschied zu anderen Währungen ist die Dezentralität des Bitcoins. Es wird keine zentrale Institution wie z.B. eine Bank oder der Staat benötigt. Die digitale Währung wird von einem dezentralen Netzwerk an Teilnehmer/-innen selbst erzeugt. Jeder Computer, der Bitcoins errechnet und transferiert, ist Teil des Netzwerks.

Das bedeutet also: Keine Zentralbank und kein Staat steuert die Geldmenge und legt die Rahmenbedingungen fest, das Bitcoin-Netzwerk steuert sich selbst. Jede Transaktion von Guthaben von einem Sender wird direkt zu einem Empfänger ohne einer zu vertrauenden Vermittlerstelle (Bank) durchgeführt. Jede Transaktion ist vollkommen transparent von jedem Teilnehmer einsehbar und wird sogar von diesen validiert. Eine Fälschung ist unmöglich, dafür sorgt die eingesetzte Kryptografie mittels asymmetrischer Verschlüsselung.

Das Bitcoin-System ist so angelegt, dass sich maximal 21 Millionen Bitcoins im Umlauf befinden dürfen. Aktuell sind ca. 12 Millionen Bitcoins im weltweiten Handel. Die künstliche Verknappung auf maximal 21 Millionen Bitcoins schützt die Teilnehmer vor einer Inflation. Der Clou ist, dass jeder Teilnehmer sich selbst Bitcoins am eigenen Rechner erzeugen kann. Hierbei werden hochkomplexe mathematische Formeln (kryptografische Funktionen) gelöst, und das wird als Mining (deutsch: schürfen) bezeichnet. Daher kommt auch die Bezeichnung „Kryptowährung“. Für das Mining sind Computer mit extrem hoher Leistungsfähigkeit notwendig und für Bitcoin-Einsteiger deswegen eher uninteressant. Stellen Teilnehmer nun Mining-Rechner mit hoher Rechenleistung zur Verfügung, werden sie mit Bitcoins entlohnt, die in bestimmten Zeitabständen generiert und ausgeschüttet werden. Ist die maximale Anzahl der Bitcoins (21 Millionen) erreicht, werden den Teilnehmern, die Rechenleistung zur Verfügung stellen, nicht mehr mit Bitcoins entlohnt, sondern mit Transaktionsgebühren (derzeit Bruchteile von Cent-Beträgen). Bei normalen Geldwährungen streichen sich die Banken die Transaktionsgebühren ein, bei der Bitcoin-Währung sind es die Bitcoin-Teilnehmer selbst.

Was ist ein Bitcoin-Wallet?

Jeder Bitcoin-Teilnehmer benötigt eine digitale Geldbörse (englisch: Wallet), um eine Transaktion zu einem anderen Bitcoin-Teilnehmer durchzuführen. Die Bitcoin-Wallet lässt sich mit einer echten Geldbörse vergleichen, bei der ja auch bei einem Warenkauf Geld entnommen und weitergereicht wird. Die digitale Bitcoin-Wallet ist eine sehr lange Zeichenkette; es gibt sie für jeden Teilnehmer nur einmal. In dieser Wallet wird das eigene Guthaben gespeichert und ist mit einem Passwort geschützt. Jede Bitcoin-Wallet ist anonym und es werden keine persönlichen Daten gespeichert. Sie kann wie eine normale Datei auf dem Rechner eines Teilnehmers kopiert und gesichert werden.

Wie nutze ich eine Bitcoin-Wallet?

Das Erstellen und Nutzen einer Bitcoin-Wallet ist relativ simpel. Zuerst müssen Sie sich entscheiden, ob Sie die Wallet auf Ihrem Smartphone bzw. Tablet oder auf Ihrem Desktop nutzen möchten. Außerdem gibt es noch reine Online-Wallets oder sogenannte Hardware-Wallets. Diese sind eine Art USB-Stick, auf dem die Wallet gespeichert wird.

Auf der deutschen Bitcoin-Seite gibt es eine große Auswahl an verschiedenen Wallets für die jeweiligen Systeme. Suchen Sie sich eine dieser Wallets heraus und installieren Sie diese. Nach der Installation können Sie Bitcoins zu Ihrer Wallet hinzufügen.

Legale Online-Währung

Bitcoins sind eine ganz legale Online-Währung und man kann mittlerweile in vielen Onlineshops und Geschäften mit Bitcoins einkaufen. In Japan hat der Bitcoin seit dem 1. April 2017 den offiziellen Status als Zahlungsmittel erlangt, ist somit also ein ganz legales Zahlungsmittel. Für die Finanzdienstleister und Börsen bedeutet das, dass sie sich an die gleichen Regeln und Auflagen wie bei den normalen Währungen halten müssen.

Die wesentlichen Merkmale von Bitcoin

1. Bitcoin basiert auf dezentraler Steuerung, es wird keine zentrale Institution, wie z.B. eine Bank, benötigt. Der Wertetransfer geht direkt von Teilnehmer A zu Teilnehmer B.
2. Jeder Bitcoin-Teilnehmer kann Bitcoins „schürfen“ (englisch: Mining) und sich an den Transaktionen beteiligen.
3. Die Transaktionen laufen prinzipiell schneller im dezentralen Netzwerk ab, und das ohne hohe Transaktionsgebühren.
4. Bitcoin basiert auf der Blockchain-Technologie (siehe nächsten Abschnitt) mit extrem sicheren kryptografischen Verschlüsselungsverfahren. Die Blockchain mit den kryptografischen Verschlüsselungsverfahren ist absolut sicher und nicht zu hacken (siehe nächsten Abschnitt).
5. Die Bitcoin-Währung ist durch die künstliche Verknappung auf 21 Millionen vor Inflation geschützt und hat somit ähnliche Eigenschaften wie die Edelmetalle Gold und Silber.
6. Für die Bitcoin-Teilnehmer ist eine Transaktion mittels dafür geeigneter Software sehr einfach durchzuführen.

Was ist die Blockchain?

Blockchain (deutsch: Blockkette) ist die Technologie hinter Bitcoin, d.h. mittels Blockchain werden alle Bitcoin-Transaktionen gesteuert. Im Prinzip beinhaltet die Blockchain unterschiedliche Blöcke, die in einer Kette miteinander gekoppelt sind. Man kann sie mit einem Journal in der Buchführung gut vergleichen. Die Blockchain ist eine dezentrale Datenbank, in der ein Datensatz durch die

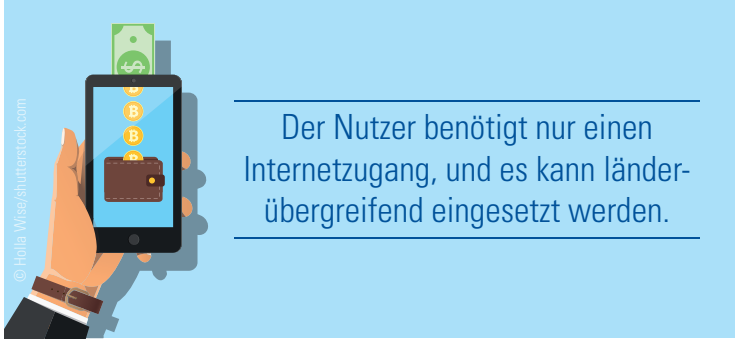
Speicherung des Hashwertes des vorangehenden Datensatzes gesichert wird. Der Hashwert ist ein kryptografischer Daumenabdruck, der für jeden Datensatz eindeutig ist und sich somit bestens für eine Integritätsprüfung eignet. Mit diesem Verfahren, mit dem die Datensätze kryptografisch und aufeinander aufbauend gespeichert werden, ist eine nachträgliche Änderung der Datensätze nicht möglich, ohne die Integrität des Gesamtsystems zu beschädigen. Man kann hier gut erkennen, dass sich die Blockchain als dezentralen Kontrollmechanismus selbst schützt. Die Integrität, also die Unversehrtheit, wird somit automatisch und selbstständig gewährleistet. Eine weitere Instanz, z. B. eine Bank, ist für die Absicherung (Bestätigung der Integrität) der Transaktionen nicht mehr notwendig.

Wie funktioniert die Blockchain?

Unser Beispiel: Eine Person A (Bitcoin-Teilnehmer) möchte einer Person B (Bitcoin-Teilnehmer) 100 Bitcoins überweisen. Genau diese Bitcoin-Transaktion wird nun als neue Transaktion in die Blockchain gespeichert. Die Blockchain ist prinzipiell auf allen Rechnern der Teilnehmer weltweit verteilt und liegt nicht zentral irgendwo auf nur einem Rechner. Sogenannte Miner „schnüren" dabei die Transaktionsblöcke, in dem sie ihre Rechenkapazität zu Verfügung stellen. Der nun erstellte Transaktionsblock wird mit einer digitalen Signatur versiegelt und bezieht sich dann immer auf den vorherigen erstellten Block. Eine nachträgliche Manipulation innerhalb der Blockchain ist somit nicht mehr möglich. Ein böswilliger Hacker müsste nicht nur den entsprechenden Transaktionsblock für einen Wertetransfer von Person A nach Person B hacken, sondern auch alle anderen Blöcke, also die gesamte Kette. Das ist absolut nicht möglich.
Alle Transaktionen in der Blockchain werden transparent für alle Teilnehmer gespeichert, d. h. jeder Teilnehmer kann alle Transaktionen einsehen, jedoch weiß man nicht, welcher Teilnehmer hinter einer Transaktion steckt.

Wie funktioniert eine Bitcoin-Transaktion genau?

Beispiel: Bitcoin-Teilnehmer A versendet zum Bitcoin-Teilnehmer B einige Bitcoins. Die entsprechende Bitcoin-Transaktion beinhaltet folgende Informationen:



1. Input: Eine Aufzeichnung darüber, welche Sender-Adresse zuvor einem anderen Bitcoin-Teilnehmer diese Bitcoins geschickt hat.
2. Anzahl Bitcoins: Anzahl der Bitcoins, die Teilnehmer A an Teilnehmer B sendet
3. Output: Bitcoin-Adresse von Teilnehmer B

Für eine Bitcoin-Transaktion werden eine Bitcoin-Adresse und ein privater Schlüssel benötigt. Wenn Teilnehmer A nun die Bitcoins an Teilnehmer B versenden will, wird der private Schlüssel verwendet, um eine Nachricht mit der vorigen Bitcoin-Transaktion, der Anzahl von Bitcoins und der Bitcoin-Adresse von Teilnehmer B zu signieren. Jetzt versendet Teilnehmer A die Bitcoins aus seinem Wallet an das Bitcoin-Netzwerk. Im Netzwerk verifizieren Bitcoin-Miner die Transaktion, schreiben sie in den Transaktionsblock und lösen sie eventuell auf.
Für die erfolgreiche Verbreitung einer Zahlung im Bitcoin-Netzwerk wird ein spezieller mathematischer Algorithmus verwendet. Bei diesem Algorithmus sendet der Client von Teilnehmer A die Transaktion an alle ihm bekannten Clients. Erhält ein Client eine neue Transaktion, beginnt er deren Signatur zu verifizieren und prüft, ob die Zahlung gültig ist. Erhält Teilnehmer B nun ein positives Ergebnis, sendet er die Transaktion an alle ihm bekannten Clients weiter. Dieser Vorgang wird solange wiederholt, bis das gesamte Bitcoin-Netzwerk mit der Transaktion „geflutet" wurde und diese jedem Bitcoin-Teilnehmer des Netzwerks bekannt ist. Während dem „Flooding" befindet sich die Zahlung noch in der Schwebe, d. h. sie könnte verloren gehen oder auch durch konkurrierende Zahlungen ersetzt werden.

Ausblick

Prinzipiell steht dem Erfolg von Kryptowährungen wie der Bitcoin nichts entgegen. Die Hintergrundtechnologie Blockchain wird definitiv auch für andere Bereiche, wie z. B. Industrie 4.0, Einzug erhalten. Der Wettbewerb wird wohl entscheiden, ob sich Bitcoin gegenüber dem heutigen Fiat-Geld (Geld, das nicht durch reale Vermögenswerte gedeckelt ist) durchsetzen wird. In der Geldtheorie steht Bitcoin auf jeden Fall ganz weit oben und könnte auch zum allgemein akzeptierten Tauschmittel aufsteigen. ZT

Infos zum Autor

ZT Adresse

Thomas Burgard, Dipl.-Ing. (FH)
Softwareentwicklung & Webdesign
Bavariastraße 18 b
80336 München
Tel.: 089 540707-10
info@burgardsoft.com
www.burgardsoft.de