Bitcoin: Geldverkehr ohne Banken

Kryptografie wird Währung

Das Internet hat bereits zahlreiche Bereiche des täglichen Lebens komplett umgekrempelt. Da liegt es nahe, auch Währungs- und Geldverkehrssysteme neu zu überdenken. Mit Bitcoin hat sich in nur wenigen Jahren ein sehr vielversprechendes, globales Zahlungsnetzwerk etabliert, das nun bereits an einigen Stellen seine Integration ins praktische Leben beginnt. Anders als alle anderen digitalen Zahlungssysteme ist es Open-Source-basiert und damit anbieterneutral. Das Verständnis für Bitcoin erfordert jedoch tatsächlich intensive Beschäftigung – vielleicht der Hauptstolperstein für ein größer angelegtes Roll-out.

„Es gibt nichts Neues mehr. Alles, was man erfinden kann, wurde bereits erfunden." Charles Duell, der Leiter des US-Patentamtes, konnte 1899 ja noch nicht wissen, dass nicht nur die elektrische Zahnbürste folgen sollte, sondern eine mengenmäßig kaum fassbare Anzahl an Innovationen, die die Welt von Grund auf verändern sollten. Also Erfindungen, die, dem lateinischen Wortursprung folgend, wirklich etwas erneuern – und nicht bloß die x-te Abart des Vorhandenen sind. Tatsächlich fällt der Ausblick auf die nächsten echten Innovationen heute genauso schwer wie vor 114 Jahren: seien sie technisch, strukturell, gesellschaftlich – oder auch finanzpolitisch. Vieles klingt einfach zu verrückt, und im ursprünglichsten Sinne ist es das auch, denn es verrückt unser Bild von der Welt. Der Begriff der Internetwährung Bitcoin ist so ein Thema, weil hier mit einer zunächst abstrakten Idee das komplette Geld- und Finanzsystem auf den Kopf gestellt werden könnte.

Nichts als Mathematik

Zugegeben: Wollen wir das auf den ersten Blick durchaus irritierende Bitcoin-System verstehen, müssen wir uns auf eine anspruchsvolle Logik-Spielwiese begeben. Die Funktionsweise des Bitcoin-Systems stellt sicher, dass es in ein paar Jahrzehnten maximal 21.000.000 Bitcoins weltweit geben wird, aktuell sind etwas mehr als die Hälfte „geschürft" worden.

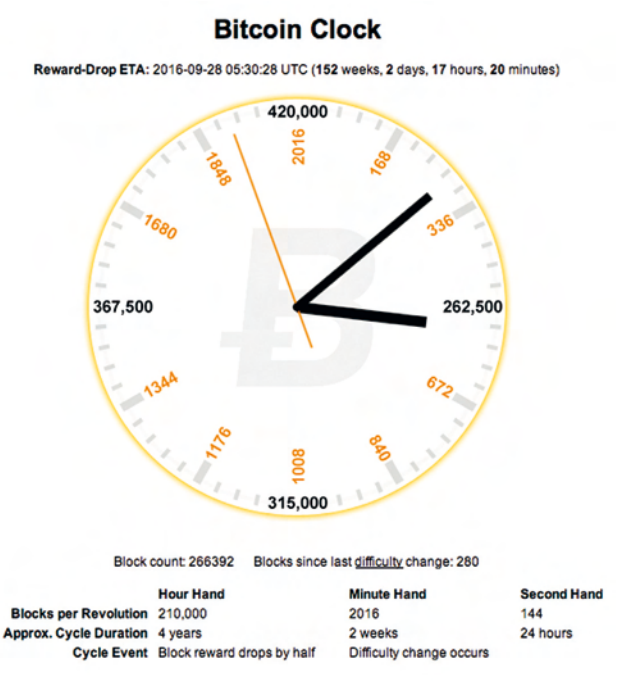
Skeptiker steigen bereits aus, wenn sie einen Bitcoin (BTC) beispielsweise mit einem Euro gleichsetzen. In diesem Fall wäre die maximale Kapazität einer ganzen Währung tatsächlich zu begrenzt. Doch Bitcoins sind keine 1:1-Währung, sie sind vor allem ein mathematisches Konstrukt, das problemlos in kleinere Einzelteile geteilt werden kann. Aktuell ist die kleinste Einheit eines Bitcoin 1 Satoshi und entspricht 0,00000001 BTC. Dies ist eine Hommage an den Erfinder Satoshi Nakamoto, der mit seinem Whitepaper 2009 den Grundstock für die Peer-to-Peer-Währung Bitcoin gelegt hat.

Bei einer derzeitigen Weltbevölkerung von geschätzten 7.155.058.300 Menschen und zurzeit 11.906.050 nutzbaren Bitcoins könnten pro Mensch genau 166.400 Satoshi verwaltet werden. Sollte dieser Wert noch nicht ausreichen, können die Entwickler des Open-Source-Projektes – die andernorts unter anderem das LINUX-Betriebssystem fortentwickeln – die kleinste Einheit um eine 10er Potenz vergrößern. Bitcoins sind aus Mathematik gemacht, und weil Mathe seit jeher eine begrenzte Aufmerksamkeit erfährt, setzt sich auch nur eine begrenzte Anzahl von Menschen mit dem Thema Bitcoin auseinander. Erschwert wird das Verständnis des Bitcoin-Systems durch komplexe Verschlüsselungstechniken, die die Erschaffung von Bitcoins in wachsenden Peer-to-Peer-Netzwerken überhaupt erst ermöglichen.

Jeder Mensch kann Teil dieses Bitcoin-Netzwerkes werden, in der er seine Rechenkapazität wie bei SETI@Home dem Bitcoin-Netzwerk zur Verfügung stellt. Im Gegenzug bekommt er anteilig zu der eingebrachten CPU-Leistung Bitcoins überwiesen. Nebenbei bemerkt: Die Rechenkapazität dieses sehr speziellen Bitcoin-Netzwerks übertrifft die Leistung der addierten TOP-500-Supercomputer dieser Welt bereits um den Faktor acht.

Funktionsprinzip

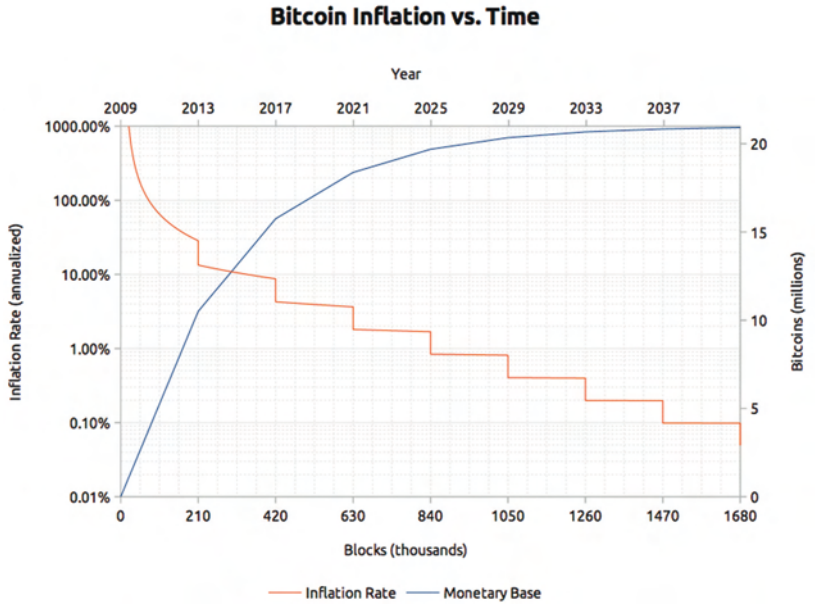
Ein Bitcoin-Konto zu eröffnen, ist einfach. Dazu lädt sich eine Person ein Wallet (elektronische Geldbörse) auf ihren Computer oder ihr Smartphone und erzeugt ein asymmetrisches Schlüsselpaar. Da es kein zentra-



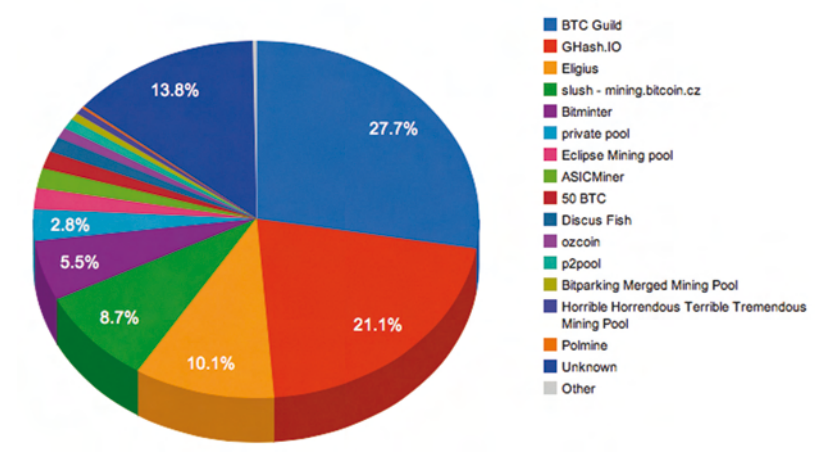
Bitcoin Clock, Quelle: http://bitcoinclock.com

les Verzeichnis gibt, muss dieses Bitcoin-Konto nirgendwo registriert oder vergeben werden. Kollisionen sind nahezu ausgeschlossen, da es bedeuten würde, dass zwei Personen unabhängig voneinander dasselbe Schlüsselpaar erzeugen. Der Public Key entspricht der Kontonummer und mit dem Private Key werden Transaktionen signiert, um Guthaben auf diesem Bitcoin-Konto an eine andere Adresse zu überweisen. Eine solche Transaktion wird in das Peer-to-Peer-Netzwerk eingestellt und landet auf diese Weise bei den Minern, die das Bitcoin-Netzwerk mit ihren Servern betreiben. Ein Miner sammelt alle Transaktionen und arbeitet an einer kryptografischen Aufgabe. Vergleichbar mit einem Bergarbeiter, der nach Gold schürft, suchen Miner mit ihrer Rechenkapazität passende Zufallszahlen. Dazu werden die Transaktionen mit einem Hash-Wert versehen. Ein Hash-Wert ist eine mathematische Einwegfunktion und produziert zufällige Ergebnisse. In diesem Fall muss der Hash-Wert aber einem Kriterium genügen, beispielsweise mit einer bestimmten Anzahl von Nullen beginnen. Bei Hash-Wert-Verfahren ist es praktisch nicht möglich, Hash-Werte rückwärts zu berechnen, dementsprechend ist die einzige Möglichkeit ein ständiges Ausprobieren per Brute-Force.

Der Schwierigkeitsgrad dieser Aufgabe wird alle 2.016 Blöcke – das entspricht etwa zwei Wochen – immer so angepasst, dass die Rechenkapazität des gesamten Bitcoin-Netzwerkes gerade so groß ist, dass rein statistisch alle zehn Minuten ein Miner eine Lösung findet.



Bitcoin Inflation, Quelle https://bitcointalk.org/index.php?topic=130619.0/Whitslack



Bitcoin Mining Pools

Gewinnung von Bitcoins

Der Miner mit der korrekten Lösung nimmt die unbestätigten Transaktionen, die er gesammelt hat und bündelt diese in einen Block. Dieser Block fügt sich nahtlos an die sogenannte Blockchain an, die alle jemals durchgeführten Transaktionen enthält. Ein Block kann nicht beliebig groß sein, im Moment gibt es ein Limit von 1 Megabyte, damit die Blockchain durch Spam-Transaktionen nicht inflationär groß wird. Diese Regelung bedeutet aber auch, dass ein Miner, der den Hashwert trifft, es in der Hand hat, alle oder nur eine Teilmenge der Transaktionen zu berücksichtigen. Ein Kriterium kann zum Beispiel die Transaktionsgebühr sein, von der Miner – nachdem alle Bitcoins geschürft wurden – ihre Kosten (Strom, Hardware und Internetverbindung) bezahlen. Ein anderes Kriterium könnte sein, dass bestimmte Anwendungen wie Glücksspiele von einem Mining Pool nicht berücksichtigt werden, so wie dies in der Vergangenheit auch einzelne Pools im Falle der Glückspielplattform Satoshi Dice gehandhabt haben. Dafür, dass ein Miner einen Block gefunden und Transaktionen bestätigt hat, darf er sich zurzeit 25 neue Bitcoins gutschreiben. Auf diese Weise entstehen alle zehn Minuten neue Bitcoins, aktuell 3.600 am Tag. Da sich diese Belohnung alle 210.000 Blöcke – das entspricht etwa vier Jahren – halbiert, werden bis ins Jahr 2040 hinein noch rund 9.000.000 Bitcoins bis zu einer theoretischen Obergrenze von maximal 21.000.000 erzeugt.

Erste Fußspuren in der realen Welt

Bitcoin ist keineswegs nur ein Thema der ewigen IT-Nerd. Bereits heute bezahlen Menschen mit Bitcoins ihre Burger im „Room77" in Berlin, kaufen in einem von 10.000 Shops im Internet ein oder reservieren ihren Tennisplatz mit der virtuellen Währung. Tatsächlich springen mittlerweile auch weitere Anbieter auf den Zug der Internetwährungen. Amazon kreiert seinen eigenen Coin und auf der Xbox werden Spiele und downloadable Contents mit Microsoft Points bezahlt. John Donahoe, CEO von eBay sagte dem Wall Street Journal: „Bitcoin ist eine disruptive Technologie, also klar, wir schauen uns Bitcoin genau

an, vielleicht gibt es Wege, ihn in PayPal zu integrieren." Facebook im Gegenzug verabschiedete sich bereits 2012 von seinen Credits. Wichtig zu wissen: Die digitalen Währungen einzelner Anbieter werden allesamt zentral ausgegeben und verwaltet und dienen ausschließlich zum Zahlungsverkehr im jeweiligen Ökosystem dieses Anbieters. Nur Bitcoins sind anbieterneutral und unabhängig von einem bestimmten Marktplatz. Und: Bitcoin ist sehr gut abgesichert.

Sicherheit auf SSL-Niveau

Der grundlegende Unterschied zwischen Bitcoin und anderen digitalen Währungen ist sein Peer-to-Peer-Ansatz. Es gibt keine zentrale Instanz wie beispielsweise PayPal oder die Deutsche Bank. Doch wie wird ein Konsens in einem verteilten Netzwerk erzielt, bei dem die einzelnen Teilnehmer per Definition nicht vertrauenswürdig sind? Eine Transaktion zu fälschen, das heißt, ohne den Private Key eine gültige Transaktion zu erzeugen und so von einem beliebigen Konto Bitcoins zu transferieren, kann praktisch ausgeschlossen werden. Dies würde bedeuten, dass man grundsätzlich von einem Public Key aus auf einen Private Key schließen kann. Wäre dies möglich, wäre auch jedwede SSL-Verbindung nicht mehr sicher. Über einen Zeitraum von 20 oder 40 Jahre betrachtet, mag das sicherlich irgendwann der Fall sein, aber da Bitcoin ein Open-Source-Projekt ist, besteht jederzeit die Möglichkeit, die verwendeten Algorithmen auszutauschen oder Schlüssellängen anzupassen und so die Sicherheit geänderten Situationen anzupassen. Dennoch sind verschiedene Betrugsszenarien möglich.

Ein realistischeres Szenario ist ein sogenannter Double Spend, der wie folgt funktioniert: Man stellt eine gültige Transaktion ein, die zum Beispiel 1 BTC von A nach B transferiert. Sobald diese von einem Miner in einem Block – nennen wir ihn BlockAB – bestätigt wurde, ist diese Transaktion in der Blockchain und gilt als durchgeführt. Ein Händler kann nun die Ware verschicken. Da aber zurzeit über 10.000 Nodes an der Blockchain arbeiten, kann es theoretisch passieren, dass ein Angreifer Blöcke berechnet, die eine alternative Blockchain darstellen. Hierbei ist wichtig zu wissen, dass die längste Kette die jeweils gültige ist. Das Konzept dahinter nennt Satoshi Nakamoto „Proof of Work".

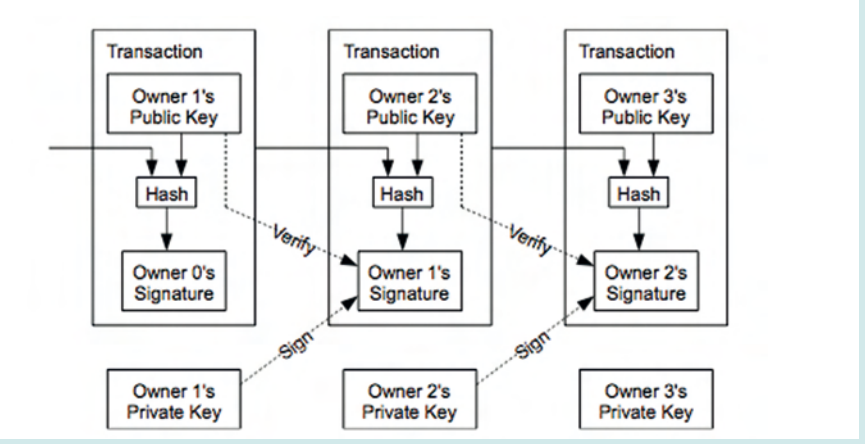
Möchte ein Angreifer, dass seine Transaktion statt von seinem Konto A zum Händler B nun zum Konto C überwiesen wird, muss er den BlockAB in Form von BlockAC neu berechnen. Damit dies von der Mehrheit des Netzwerkes akzeptiert wird, muss er auch die Folgeblöcke BlockAC1, BlockAC2 etc. berechnen, und zwar so lange, bis die Mehrheit des Netzwerks „glaubt", dass diese Version der Blockchain die längste und somit die gültige ist. Gewinnt einer der anderen Server das Rennen um den nächsten Block, wird er auf BlockAB aufsetzen und somit die Blockchain in Richtung BlockAB1, BlockAB2 usw. verlängern. Der Angreifer muss also über mehrere Blocks hinweg über mehr Rechenkapazitäten verfügen als die Mehrheit des Netzwerks. Diese Rechenkapazität liegt aktuell bei 3,5 Petahashes, und am Tag werden – rein rechnerisch – über 8.000.000 Dollar in Form von Strom und Ressourcen für dieses

Byzantinische Blockchain

Im November 2008 hat Satoshi Nakamoto auf der Mailing List, auf der er sein Whitepaper veröffentlicht hat, erklärt, welche Funktion die Blockchain hat. Letztlich geht es um die Fragestellung, wie in einer Gruppe, deren Mitglieder per Definition nicht vertrauenswürdig sind, alle unabhängig voneinander zu dem gewünschten Ergebnis kommen. Mögliche Verräter, die sich unter die Gruppe mischen, dürfen das System nicht zu Fall bringen. In der Wissenschaft ist dieses Problem als das der „Byzantinischen Generäle" bekannt:

Eine Gruppe von Generälen hat eine Stadt umstellt. Der Angriff auf diese Stadt kann nur erfolgreich sein, wenn alle gleichzeitig angreifen. Doch wie kann man die Angriffszeit an die anderen übermitteln, wenn man nicht weiß, ob es unter den Generälen Verräter gibt, die verhindern wollen, dass der Sturm auf die Stadt erfolgreich ist? So könnte ein Verräter eine falsche Uhrzeit weiterleiten, und loyale Generäle könnten diese erst einmal nicht von der korrekten unterscheiden.

Die Lösung ist, eine Uhrzeit zum Angriff festzulegen, einen Prozess zu starten, der auf diesem Zeitpunkt aufsetzt und mit so viel Arbeit verbunden ist, dass man frühestens nach zehn Minuten zu einem Ergebnis kommt. Alle Generäle arbeiten nun an dieser Fragestellung und derjenige, der als erster die Lösung findet, publiziert diese an alle anderen Generäle. Sobald es eine korrekte Lösung gibt – die jeder unabhängig voneinander überprüfen kann – muss auf dem vorherigen Arbeitsergebnis aufgesetzt werden und wiederum eine Lösung gefunden werden. Nach zwei Stunden ist davon auszugehen, dass zwölf aufeinanderfolgende Lösungen (Blöcke) gefunden wurden. Jeder General kann sich nun diese Lösung anschauen, überprüfen, wie viel Arbeit in diese Lösungen gesteckt wurde und schauen, auf welche Uhrzeit im ersten dieser zwölf Blöcke verwiesen wurde. Solange die Mehrheit, also mindestens 51 Prozent des Netzwerks, loyale Generäle sind, kann man davon ausgehen, dass das Ergebnis korrekt ist.



Blockchain Funktionsweise

Quellen: http://bit.ly/blockchain, http://bitcoin.org/bitcoin.pdf

Bitcoin-Netzwerk bereitgestellt. So ist es für einen Angreifer wahrscheinlich lukrativer, seine Ressourcen nicht dafür einzusetzen, Blöcke zu fälschen, sondern gültige Blöcke zu berechnen und sich auf diese Weise friedlich an der Infrastruktur zu beteiligen. Händler können auf der anderen Seite einfach eine gewisse Anzahl von Bestätigungen abwarten. So geht man davon aus, dass nach sechs Bestätigungen ein Angreifer das Rennen um eine längere Blockchain nicht mehr gewinnen kann.
Betriebswirtschaftlich macht auf Grund der exponentiell gewachsenen Rechenkapazität das Mining als einzelne Personen keinen Sinn. In der Regel schließt man sich deshalb einem Mining Pool an und bekommt anteilig an seiner eingebrachten CPU-Leistung entsprechend Bitcoins ausbezahlt.

Zukunftsperspektiven

Die Kritiker mahnen vor Geldwäsche und subversiven Mächten, die Befürworter sprechen vom Gold 2.0 und von der inflationssicheren Währung. Beide haben grundsätzlich Recht! Eine spannende juristische Betrachtung hat Rechtsanwalt Julian Schneider auf der 1. Bitcoin-Konferenz.de am Startplatz in Köln vorgenommen. So hat die Bundesregierung auf die Anfrage des FDP-Politikers Frank Schäffler Bitcoin als „privates Geld" anerkannt. Aus einer weiteren Anfrage ging hervor, dass Kursgewinne für Privatpersonen nach einem Jahr steuerfrei sind. Das alles sind Impulse, die dafür sorgen, dass Bitcoin Schritt für Schritt ernst genommen wird.

Dabei kann es durchaus erschrecken, wie lässig dieses Zahlungssystem auf die weltweit in der Dauerkritik befindlichen Banken verzichtet, weil die Zahlungen einzig zwischen den Protagonisten im Peer-to-Peer-Netzwerk verlaufen – eben ohne zentrale Institutionen. Dass dies so funktioniert, liegt zum einen an den zugrunde liegenden kryptografischen Verfahren und zum anderen an vielen tausend Menschen, die sich aktiv in das Open Source-Projekt einbringen und es weiterentwickeln. Man kann deshalb Bitcoin durchaus mit Wikipedia vergleichen. Ob Banken den Weg des Brockhaus-Verlages nehmen oder sich aber mit der digitalen Währung arrangieren, wird die Zukunft zeigen.

Das Institut für Internet-Sicherheit ist gerade dabei, ein Bitcoin-System aufzubauen, um Erfahrungen zu sammeln und die notwendigen Anforderungen an einer breit genutzten digitalen Währung pragmatisch umzusetzen. ■

Ein Bitcoin Wallet enthält die privaten Schlüssel und somit den Zugriff auf die Bitcoin-Guthaben zu den dazugehörigen öffentlichen Schlüsseln. Wenn zum Beispiel durch einen Festplattencrash diese Schlüssel verloren gehen, sind auch die dazugehörigen Bitcoins unwiderruflich verloren. Dementsprechend ist immer auch das Risiko des Verlusts und des Diebstahls des Private-Key einzukalkulieren – analog zu Bargeld, das gestohlen oder verloren gehen kann.

Desktop Wallet
Der offizielle Client von Bitcoin.org heißt Bitcoin-Qt und ist ein sogenannter Full Client. Das bedeutet, dass er die gesamte Blockchain herunterlädt und somit die Gültigkeit von Transaktionen selbst prüfen kann. Da die Blockchain im Moment 12 Gigabyte groß ist, wird entsprechend viel Speicherplatz benötigt, und es kann ein wenig dauern, bis alle Blöcke heruntergeladen und der Client einsetzbar ist. Multibit (multibit.org) ist ein leichtgewichtiger Desktop Client für Windows-, Macintosh- und Linux-Rechner. Er synchronisiert sich mit dem Bitcoin-Netzwerk und ist deshalb in wenigen Minuten einsetzbar.

Mobile Wallet
Bitcoin bietet sich als Bezahlverfahren für mobile Endgeräte an. Dementsprechend gibt es insbesondere für die Android-Plattform eine Vielzahl von Bitcoin-Wallet-Apps, eine der populärsten ist die von Andreas Schildbach. Für die iOS-Plattform wird lediglich die Hybrid-App von Blockchain.info angeboten.

Web-Wallet
Bei einem Web-Wallet werden die privaten Schlüssel zu den eigenen Bitcoins bei dem Anbieter des jeweiligen Dienstes gelagert. Der Vorteil liegt darin, dass man keine Software installieren muss und praktisch von jedem Ort der Welt mit einer Internetverbindung aus in der Lage ist, Transaktionen durchzuführen. Coinbase.com ist beispielsweise ein solcher Anbieter. Laut eigenen Angaben werden etwa 90 Prozent der Guthaben auf Offline-Wallets offline in einer Bank gelagert. Allerdings kann der Schutz nur so gut sein wie der Passwortschutz und die Vertrauenswürdigkeit des Bitcoin-Systemadministrators.

Offline-Wallet
Offline-Wallets funktionieren ohne eine Online-Verbindung und werden deshalb auch „Cold Storage" genannt. Der private Schlüssel wird zum Beispiel auf einem USB-Stick gespeichert oder in Form eines 2D-Barcodes auf Papier ausgedruckt und an einem sicheren Ort hinterlegt. Auf brainwallet.org können Nutzer sich einen Satz ausdenken, der als Grundlage für die Generierung des asymmetrischen Schlüsselpaares dient. Armory ist beispielsweise ein Desktop Wallet, das auch Offline-Funktionen bereitstellt.

Quelle: http://bitcoin.org/en/choose-your-wallet

Christian Kammler,
Mobile Entrepreneur und freier Berater, engagiert sich für bitcoin-konferenz.de und twittert über Bitcoin unter @ck9

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen