1. Grundbegriffe

1.1. Was ist Bitcoin?

Der Ausdruck „Bitcoin“ bezeichnet zwei Dinge:

- einerseits eine Währung und
- andererseits das dazugehörige Zahlungssystem.

Im Gegensatz dazu ist zB der Euro nur eine Währung bzw sind VISA, PayPal oder SWIFT nur Zahlungssysteme. Im Englischen hat es sich eingebürgert, dass „bitcoin“ (kleingeschrieben) verwendet wird, wenn die Währung gemeint ist, und „Bitcoin“ (großgeschrieben) verwendet wird, wenn das Zahlungssystem gemeint ist. Im Deutschen besteht diese Unterscheidung nicht.

1.2. Was ist eine Adresse?

Eine Adresse ist eine Kombination aus Buchstaben und Ziffern, wie beispielsweise 1F9cZYh3ZB6gdF9mnzLgFn6yqnFvpP9iHn. Bitcoins (→ 1.1) werden sozusagen an einer Adresse gespeichert. Die Adresse ist somit vergleichbar mit der IBAN eines Bankkontos (zB AT843400000000062679), auf dem Euro gespeichert sind. Eine Adresse kann man ruhig bekannt geben; man muss sie sogar bekannt geben, wenn man eine Bitcoin-Zahlung erhalten will.

1.3. Was ist ein geheimer Schlüssel?

Ein geheimer Schlüssel ist ebenfalls eine Kombination aus Buchstaben und Ziffern, wie zB 5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF. Zu jeder Adresse (→ 1.2) gibt es einen geheimen Schlüssel. Mit dem geheimen Schlüssel kann man über die auf der Adresse gespeicherten Bitcoins (→ 1.1) verfügen. Der geheime Schlüssel ist somit vergleichbar mit einem PIN-Code (zB 83puWz), mit dem man auf ein Bankkonto und das darauf vorhandene Euro-Guthaben zugreifen kann. Technisch gesprochen wird der geheime Schlüssel dazu verwendet, eine Transaktion (→ 1.5) zu signieren. Einen geheimen Schlüssel darf man niemand anderem bekannt geben; wer nämlich den geheimen Schlüssel kennt, kann eine Bitcoin-Zahlung von der Adresse vornehmen, zu welcher der geheime Schlüssel gehört.

1.4. Was ist eine Wallet?

Eine Wallet (Brieftasche oder Geldbörse) ist eine Software – oft eine Smartphone-App (→ 11.5) –, welche Adressen (→ 1.2) und die dazugehörigen geheimen Schlüssel (→ 1.3) speichert und mit der man Bitcoins (→ 1.1) komfortabel empfangen und senden kann, ohne umständlich Buchstaben-Ziffern-Kombinationen eingeben zu müssen.

1.5. Was ist eine Transaktion?

Eine Transaktion ist die Übertragung von Bitcoins (→ 1.1) von einer Adresse (→ 1.2) an eine andere Adresse. Eine Transaktion ist somit vergleichbar mit einer Überweisung von Euro von einer IBAN an eine andere IBAN. Um eine Transaktion durchführen zu können, muss der Sender über den geheimen Schlüssel (→ 1.3) verfügen, der zu der Adresse gehört, von der die Bitcoins gesendet werden sollen – genauso wie sich der Sender bei einer Überweisung von Euro bei Online-Banking typischerweise mit einem PIN-Code ausweisen muss.

1.6. Was ist ein Block?

Mehrere Transaktionen (→ 1.5) von Bitcoins (→ 1.1) werden aus administrativen Gründen zu einem Block zusammengefasst. Ein Block ist also ein Container, in welchem Transaktionen (dh Übertragungen von Bitcoins von einer Adresse an eine andere Adresse) gespeichert sind.

1.7. Was ist eine Blockchain?

Eine Blockchain (chain of blocks) ist eine Kette aus Blöcken (→ 1.6), wobei jeder einzelne Block wiederum Transaktionen (→ 1.5) enthält. Somit ist eine Blockchain im Grunde eine Liste von Transaktionen bzw in der Sprache der Buchhaltung ein Journal. Die Blöcke einer Blockchain werden mithilfe eines mathematischen (kryptografischen) Verfahrens miteinander verkettet (→ 5.20).

1.8. Was ist ein Genesis-Block?

Der erste Block (→ 1.6) einer Blockchain (→ 1.7) wird Genesis-Block genannt. Mit diesem Block entsteht eine Blockchain (vgl das erste Buch der Bibel, die Genesis, in dem von der Erschaffung der Welt berichtet wird).

1.9. Was ist eine Kryptowährung?

Kryptowährung im engeren Sinn meint eine Währung (dh ein Zahlungsmittel), die mit kryptografischen Verfahren gesichert ist. Bitcoin (→ 1.1) ist die erste Kryptowährung; neben Bitcoin gibt es aber auch noch viele andere Kryptowährungen (→ 7.1). Kryptowährungen bestehen im Grunde aus drei Elementen:

- einem Computerprogramm (→ 2.3), das die Regeln dieser Kryptowährung aufstellt
- einer Datenbank (Blockchain; → 1.7), welche alle Transaktionen mit Einheiten dieser Kryptowährung enthält
- einem dezentralen Netzwerk (→ 5.6), welches die Datenbank betreibt und nach den Regeln des Computerprogramms periodisch ergänzt

Kryptowährung im weiteren Sinn meint jedes auf einer Blockchain gespeicherte Wirtschaftsgut, unabhängig von seiner Funktion (zB Zahlungsmittel oder Gutschein).

1.10. Was sind Krypto-Assets?

Der Begriff Kryptowährung (→ 1.9) hat sich zwar im deutschen Sprachgebrauch eingebürgert, ist aber nicht ganz passend: Einerseits (bei Kryptowährungen im engeren Sinn) liegt kein vom Staat ausgegebenes und mit Annahmezwang ausgestattetes Zahlungsmittel vor; andererseits (bei Kryptowährungen im weiteren Sinn) besteht oft gar keine Funktion als Zahlungsmittel. Besser wäre die Verwendung des Begriffs Krypto-Assets (dh Krypto-Wirtschaftsgüter), dieser hat sich aber noch nicht wirklich durchgesetzt.

Ebenfalls nicht durchgesetzt hat sich der im Geldwäscherecht definierte Begriff virtuelle Währung (→ 23.5).

2. Historische Entwicklung

2.1. Wer hat Bitcoin erfunden?

Im Oktober 2008 stellte ein gewisser *Satoshi Nakamoto* auf einem Kryptografie-Forum im Internet sein Konzept eines neuen elektronischen Geldsystems vor („*I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.*"). In seinem neunseitigen Paper „*Bitcoin: A Peer-to-Peer Electronic Cash System*" (abrufbar unter bitcoin.org/bitcoin.pdf) beschrieb er die theoretischen Grundlagen dieser neuen Kryptowährung (→ 1.9). Es handelt sich dabei sozusagen um das Gründungsmanifest der gesamten Kryptowährungs- und Blockchain-Bewegung.

2.2. Gibt es Vorläuferprojekte, auf denen Bitcoin aufbaut?

Es gab zahlreiche Vorläuferprojekte, auf denen Bitcoin (→ 1.1) aufbaute. Dazu zählen beispielsweise:

- ecash von *David Chaum*
- Hashcash von *Adam Back*
- Bit Gold von *Nick Szabo*
- b-money von *Wei Dai*

Satoshi Nakamoto (→ 2.1) kannte offensichtlich all diese Projekte und deren jeweilige Schwachstellen; darauf aufbauend entwickelte er sein eigenes elektronisches Geld.

2.3. Wann wurde Bitcoin praktisch umgesetzt?

Satoshi Nakamotos theoretisches Konzept (→ 2.1) stieß auf große Anerkennung in der Kryptografie-Community. In den nächsten Monaten programmierten er und weitere Forumsmitglieder gemeinsam die erste Version der Bitcoin-Software. Diese startete schlussendlich im Jänner 2009, was gemeinhin als die Geburtsstunde von Bitcoin (→ 1.1) angesehen wird. Zu diesem Zeitpunkt war Bitcoin nur ein Experiment, das aber im Lauf der Zeit immer größere Kreise ziehen sollte.

2.4. Wer ist Satoshi Nakamoto?

Niemand weiß, wer *Satoshi Nakamoto* (→ 2.1) wirklich ist; es handelt sich bei diesem Namen um ein Pseudonym. Seit 2009 wurden viele Versuche unternommen, um festzustellen, wer hinter diesem Pseudonym steckt. So hat man zB

- die Tageszeit seiner Postings und E-Mails analysiert, um herauszufinden, in welcher Zeitzone er sich befindet
- seine Texte mit denen anderer Mitglieder der Kryptografie-Community (→ 2.2) verglichen, um zu eruieren, ob er eine dieser Personen ist
- Stilanalysen gemacht, um zu ermitteln, ob er eher amerikanisches, britisches oder australisches Englisch verwendet

Trotz allem konnte man *Satoshi Nakamoto* bisher nicht identifizieren. Als gesichert gilt nur, dass es sich beim Erfinder von Bitcoin (→ 1.1) um eine extrem talentierte Person handeln muss, die große Expertise in den Bereichen Kryptografie (Hash-Funktionen und digitale Signaturen), Computerwissenschaft (Peer-to-Peer-Netzwerke) und Volkswirtschaft (Geldsysteme und Spieltheorie) hat. In gewisser Weise ist es sehr passend, dass eine pseudonyme Währung (→ 5.14) wie Bitcoin einen pseudonymen Gründer hat.

2.5. Wer könnte Satoshi Nakamoto sein?

Es gibt jede Menge Mutmaßungen, wer *Satoshi Nakamoto* (→ 2.1) sein könnte, und auch ein paar originelle Verschwörungstheorien dazu:

- Die Zeitschrift *Newsweek* zB hat im Jahr 2014 einen Ingenieur in Kalifornien mit dem Namen *Dorian Satoshi Nakamoto* ausfindig gemacht, der aber letztlich dementiert hat, der Bitcoin-Gründer zu sein (vgl bit.ly/2qaIlZT).
- Viele der sogenannten „Cypherpunks" aus der Kryptografie-Community (→ 2.2) werden als mögliche Gründer von Bitcoin geführt, wie zB *Nick Szabo*, dessen Initialen denen von *Satoshi Nakamoto* entsprechen. Auch *Hal Finney*, der die erste Bitcoin-Zahlung von *Satoshi Nakamoto* erhalten hat, wird in diesem Zusammenhang oft erwähnt.
- Der Australier *Craig Wright* – der sich selbst als *Satoshi Nakamoto* geoutet hat, ohne aber Beweise dafür zu erbringen – wird dagegen vielfach für einen Betrüger gehalten.
- Weiters gibt es eine Theorie, dass *Satoshi Nakamoto* ein Akronym aus Samsung, Toshiba, Nakamichi und Motorola ist; dieser Theorie folgend verbirgt sich also keine Einzelperson hinter dem Pseudonym.
- Behauptet wurde auch, dass die US-amerikanische National Security Agency Bitcoin entwickelt hat (siehe zB bit.ly/2CBNxxv).
- Das jüngste Gerücht besagt, dass ein gewisser *Ilya Zhitomirskiy* Bitcoin erfunden haben soll, aber bereits mit 22 Jahren Selbstmord begangen hat (vgl zB bit.ly/2D4LvHd).
- Angeblich soll die US-amerikanische Central Intelligence Agency wissen, wer *Satoshi Nakamoto* ist (vgl bit.ly/2AtqROB). Auch dies erscheint zweifelhaft.

Es wird sich wahrscheinlich nie herausfinden lassen, wer hinter dem Pseudonym steckt.

2.6. Wann gab es den letzten Kontakt mit Satoshi Nakamoto?

Mitte 2010 zog sich *Satoshi Nakamoto* (→ 2.1) weitestgehend aus dem Projekt zurück und übergab die Website bitcoin.org sowie die Kontrolle über den Source Code von Bitcoin (→ 1.1) an mehrere prominente Mitglieder der Bitcoin-Community, die fortan Bitcoin weiterentwickelten. Im April 2011 verschickte er eine E-Mail zum Abschied („*I've moved on to other things. It's in good hands with Gavin and everyone.*"). Nach dem Bericht in *Newsweek* (→ 2.5) im Jahr 2014 kam dann die offenbar letzte Nachricht („*I am not Dorian Nakamoto*.").

2.7. Ist es bedeutsam, wann Bitcoin vorgestellt wurde?

Es ist bedeutsam, dass *Satoshi Nakamotos* Paper (→ 2.1) im Herbst 2008 vorgestellt wurde, nämlich auf dem Höhepunkt der globalen Banken- und Finanzkrise. Nach der Insolvenz von *Lehman Brothers* war das allgemeine Vertrauen in Banken auf einem Tiefpunkt. *Satoshi Nakamoto* stellte zu diesem Zeitpunkt ein neues Geldsystem vor, welches Intermediäre (dh Banken; → 3.4) überflüssig macht. Im Genesis-Block (→ 1.8) der Bitcoin-Blockchain hinterlegte er die folgende Nachricht: „*Chancellor on brink of second bailout for banks.*" Dieser Satz, welcher die Schlagzeile der englischen Tageszeitung *The Times* am 3.1.2009 war, kann als Kampfansage von *Satoshi Nakamoto* an die Banken gewertet werden.

2.8. Wie war die weitere Entwicklung in den Anfangsjahren von Bitcoin?

Die wichtigsten Meilensteine in den Anfangsjahren von Bitcoin (→ 1.1), als diese neue Währung nur einer ganz kleinen Gruppe von Kryptografie-Experten bekannt war, waren folgende:

- Im Mai 2010 erfolgte der erste dokumentierte Kauf, bei dem Bitcoins als Zahlungsmittel eingesetzt wurden: Jemand erwarb zwei Pizzen für 10.000 Bitcoins. Damit wurde zum ersten Mal ein Bezug dieser virtuellen Währung zur realen Welt hergestellt.
- In der kleinen Bitcoin-Community wurden Bitcoins regelmäßig gegen Geld getauscht, wobei der Bitcoin-Kurs im Februar 2011 einen Wert von USD 1 erreichte. Dies wurde als ein ganz besonderer Höhepunkt angesehen.
- Im Juni 2011 wurde die Whistleblowing-Plattform WikiLeaks offenbar auf Betreiben der US-Regierung von Zahlungssystemen wie VISA und PayPal boykottiert. WikiLeaks entschied sich daraufhin, Spenden in Form von Bitcoins anzunehmen (vgl shop.wikileaks.org/donate). Dadurch wurde ein etwas größerer Personenkreis auf Bitcoin aufmerksam.

- Im Oktober 2013 wurde *Ross Ulbricht*, der Betreiber des im Darknet operierenden illegalen Marktplatzes „Silk Road", verhaftet. Im Zuge dessen wurden vom US-amerikanischen Federal Bureau of Investigation ca 144.000 Bitcoins sichergestellt. Auch diese Zeitungsmeldung machte einen größeren Personenkreis mit Bitcoin bekannt.
- Im Februar 2014 stellte Mt. Gox (mtgox.com) einen Insolvenzantrag in Tokio. Es handelte sich um die damals größte Bitcoin-Börse (→ 12.1), über die ca 70 % des gesamten Bitcoin-Handels abgewickelt wurden. Nach Berichten waren offenbar 850.000 Bitcoins verloren gegangen.

2.9. Wann wurde Bitcoin in der Öffentlichkeit bekannt?

Erst im Jahr 2017 ist das Thema Bitcoin (→ 1.1) endgültig im Mainstream angekommen. Dies zeigt sich zB in der Anzahl an Google-Suchanfragen (siehe dazu bit.ly/2O7U1WS), an durchgeführten Transaktionen und an Berichten in den Medien während dieses einen Jahres, welches mit einem Kurs von ca USD 20.000 schloss (wobei der Kurs im Februar 2018 dann schnell wieder auf ca USD 7.000 fiel).

3. Vergleich von Bitcoins mit konventionellem Geld

3.1. Welche Unterschiede bestehen betreffend die ausgebende Stelle?

Konventionelles Geld – aufgrund des „Fiat" (lateinisch: „es geschehe") des Staates geschaffenes Geld wird oft auch als Fiatgeld bezeichnet – wird zentral von einer Notenbank ausgegeben.

Bitcoins (→ 1.1) werden dagegen von einem dezentralen Netzwerk geschaffen und ausgegeben (→ 6.1).

3.2. Welche Unterschiede bestehen betreffend die Steuerung der Geldmenge?

Bei konventionellem Geld beruht die Bestimmung der Geldmenge auf einer diskretionären (politischen) Entscheidung.

Bei Bitcoins (→ 1.1) hingegen beruht die Bestimmung der Geldmenge auf einem Algorithmus: Bitcoins werden nach einem festgelegten System ausgegeben, wobei die Anzahl der jeweils ausgegebenen Bitcoins im Lauf der Zeit sinkt (→ 6.9).

3.3. Welche Unterschiede bestehen betreffend die Begrenztheit der Geldmenge?

Konventionelles Geld kann beliebig vermehrt werden. Passiert dies, kann es eines Tages wertlos sein. *Satoshi Nakamoto* (→ 2.1) wies anschaulich auf dieses Hauptproblem von konventionellem Geld hin: Von einer Zentralbank ausgegebenes Geld funktioniere nur, wenn man vertrauen kann, dass es nicht entwertet wird; die Geschichte sei aber voll von diesbezüglichen Vertrauensbrüchen.

Ein Wesensmerkmal von Bitcoin (→ 1.1) ist dagegen seine Begrenztheit: Es kann maximal 21 Mio Bitcoins geben. Durch die Begrenzung der Geldmenge wird ein Inflationsschutz geschaffen. Insgesamt wurden seit Gründung bis heute schon ca 17,5 Mio der möglichen 21 Mio Bitcoins ausgegeben (→ 6.11), das sind also mehr als 80 % aller Bitcoins, die es je geben wird.