Bitcoin verstehen

Ein kurzer Leitfaden für jeden, der es wissen will

Von ultimocafe

Version 2024_09_11

Zuallererst

Dass es Bitcoin gibt war mir schon seit einigen Jahren bekannt. So richtig ernst habe ich das ganze aber nicht genommen. Als vor wenigen Jahren der Börsenbrief, den ich regelmäßig lese, in sein Musterdepot neben Aktien auch Bitcoin aufnahm wurde ich mit einem Schlag wach: Was war da los, wenn jetzt auch traditionell verankerte Analysten sich damit beschäftigen? Da müsste mehr dahinterstecken. So begann die Reise, die mich immer weiter in die spannende Materie eintauchen ließ.

Ich hatte Gespräche mit Freunden, die von mir wissen wollten, was es mit Bitcoin auf sich hat und musste also selber einige Ordnung in meine Gedanken und meine Kenntnisse diesbezüglich bringen. Schließlich kam ich auf die Idee, das was ich mir bisher aus verschiedenen Quellen so zusammengelesen hatte in diesen Leitfaden zu packen um es anderen Interessierten ebenso zugänglich zu machen.

Das Ziel dieser Seiten soll sein, dass jeder Leser auch ohne mathematische Kenntnisse ein gutes Verständnis von Bitcoin, seiner Konstruktion, seinen Abläufen und Möglichkeiten und dem ganzen Rest kriegt, dass er sagen kann: „Ja, das ist mir jetzt so klar und deutlich, dass ich direkt loslegen kann. Ich weiß, worum es geht!“

Ganz klar, dass damit sehr viele Ungenauigkeiten und sogar Fehlerhaftigkeit im Detail vorkommen. Das sollte aber für das Erreichen des Ziels keine Rolle spielen. Das Internet bietet endlose Möglichkeiten, sich da weiterzuarbeiten. Besonders möchte ich auf eine Webseite hinweisen, die da in allen Lebenslagen, Bitcoin betreffend sehr gut weiterhilft: **www.blocktrainer.de**

Zu guter Letzt: Diese Seiten sollen zum technischen Verständnis von Bitcoin für jedermann beitragen und enthalten deshalb starke Vereinfachungen und teilweise unkorrekte Darstellungen. Sie stellen keine Anlageempfehlung dar. Ich selber habe mir das Folgende auch zusammengelesen, es spiegelt mein persönliches aktuelles Verständnis des Themas wieder. Bitte seien Sie sich bewußt, dass ich mich irren kann.

Dank an Satoshi Nakamoto, wer oder was auch immer das ist.

Das Schwierigste zuerst

1. Die Hashfunktion

Die Hashfunktion „SHA256“ erzeugt aus einem Text (auch mit Zahlzeichen) beliebiger Länge seinen Hashwert, einen eindeutigen „Fingerabdruck“ aus 64 Zeichen.

Beispiele:

Text	Hashwert
E	a9f51566bd6705f7ea6ad54bb9deb449f795582d6529a0e22207b8981233ec58
Heute hat Sabine Geburtstag	ec8eead30a43cf088695e6f53ea3775e556dad0fb3d2e1847fd67b6809e4152b
4501Abc	5b3702cbdf18469cbf7f1c8c702e29b07feed8a799f0db85476bce4e3279248a
0501Abc	407c93700e569f29ef182140a3558e3bfd084b3cc84b2b886930037ea27ee338

Sie können diese Hashes im Internet probehalber selber erzeugen. Zum Beispiel auf https://emn178.github.io/online-tools/sha256.html

Das Besondere an diesen Hashwerten ist:

Sie liefern bei geringfügigen Änderungen des Quelltextes komplett andere Werte. Siehe die beiden letzten Beispiele „4501Abc“ und „0501Abc“

Verschiedene Texte liefern zuverlässig unterschiedliche Hashwerte. Die Gefahr, dass gleiche Hashwerte auftreten ist tatsächlich so gut wie ausgeschlossen. Eher hat ein Mensch 100 mal hintereinander „sechs Richtige“ im Lotto, als dass so ein Fall auftritt.

Aus einem Hashwert den zugrundeliegenden Text zu entschlüsseln ist nicht möglich.

Anmerkung: So funktionieren auch Passwörter, zum Beispiel bei Ihrem e-Mail-Provider oder Online-Händler. Wenn Sie da ein Passwort anlegen, wird das dort nicht als Klartext gespeichert, sondern Ihr Passwort wird „gehasht“ und der Hashwert beim Händler gespeichert. Der Händler kennt damit das eigentliche Passwort nicht. Wollen Sie sich mit Ihrem Passwort einloggen, wird wieder gehasht und die Hashwerte verglichen. Stimmen sie überein, ist alles in Ordnung. Damit ist auch klar, dass der Händler nicht gezwungen werden kann, Ihr Passwort an interessierte Stellen herauszugeben. Es geht schlicht und einfach nicht.

Wichtige Aufgabe - ein Türöffner zum weiteren Verständnis!!!!
Öffnen Sie einen Hash-Generator (zB. im Web den obengenannten https://emn178.github.io/online-tools/sha256.html) und erzeugen Sie einen Hashwert aus einem beliebigen Text (beispielsweise „Das Wetter wird schön“). Der Output liefert:
6bca1c77fdfe39a6eb4d129d7654d3161e1fa5f40722b644c35ea19d51da618a
Hängen Sie jetzt an den Input-Text willkürlich Ziffern an, beispielsweise „Das Wetter wird schön**1**“

oder „Das Wetter wird schön**12**“ und beobachten den Output.

Probieren Sie solange bis einmal am Anfang des Outputs eine 0 steht, so wie
0adb0857888986dc4d3bce4a1b0089aa652d0ab6e17c2ab4f080eb238a40fba5
Sollte in überschaubarer Zeit gehen, oder?

Machen Sie weiter, bis am Anfang zwei Nullen stehen, so wie
00d842ef7c0474289426cb70d0df3fdc35ef5a6e21715e281cede8feba9bdbee
Das dauert schon deutlich sehr viel länger. Und wenn’s Ihnen zu langweilig wird, einfach sein lassen und glauben, dass die Nullen schon mal daherkommen.

Es ist schon ersichtlich, dass es wenig Sinn hat, mehr als zwei Nullen vorne auf diese Weise hinkriegen zu wollen.

2. Die Verschlüsselung

Verschlüsseln ist ein anderes Thema, als einen Hashwert zu erzeugen. Wie eben erwähnt läßt sich der Hashwert nicht rückwärts entschlüsseln. Das Verschlüsselungsverfahren, das im Zusammenhang mit Bitcoin steht, verwendet zum Verschlüsseln einer Nachricht einen öffentlichen („**Public-Key**“) und zum Entschlüsseln der Nachricht, einen privaten, geheimen Schlüssel (“**Private-Key**”).

Zur Annäherung an die Idee ein Beispiel: An Rande eines Blumenfelds hat der Eigner eine Kasse aufgestellt, dahinein können Passanten das Entgelt für die selber geschnittenen Blumen werfen. Abends öffnet er mit seinem (Metall-) Schlüssel die Kasse und entnimmt das Geld. Hier entspricht der Metallschlüssel dem Private-Key. Die Kasse wäre der Public-Key (der Eigentümer veröffentlicht diesen, jeder hat Zugang dazu und kann ihn verwenden – sprich Geld einwerfen). Niemand kann mit dem Public-Key etwas anfangen außer einzahlen, solange er nicht den Private-Key hat (daher hütet ihn der Eigentümer sehr sorgfältig).

Im Verschlüsselungssystem des Bitcoin erzeugt jeder Nutzer seinen eigenen, individuellen privaten Schlüssel selber. Der liegt dann sicher beim Nutzer verborgen und besteht aus einer ellenlangen Zeichenfolge. Aus diesem privaten Schlüssel kann der Nutzer dann je nach Bedarf beliebig viele öffentliche Schlüssel – auch als Adressen bezeichnet - herstellen (ebenfalls ellenlange Zeichenfolgen) und im Bitcoin-Netzwerk oder im Internet verteilen.

An so eine öffentliche Adresse kann jemand Bitcoin schicken und nur derjenige, der den zugehörigen privaten Schlüssel hat, kann über diese Bitcoin verfügen.

Der mathematische Hintergrund von all dem ist recht komplex, spielt aber für den Normalanwender keine Rolle. Es reicht, das beschriebene Konzept zu verstehen.

Und jetzt zum Einfachen, dem Bitcoin

1. Die Blockchain

Die einzelnen Blöcke sind mit den Transaktionen der Teilnehmer gefüllt. Eine Transaktion hält fest, wer wieviel an wen zahlt (genaueres später). Die gesamte Bitcoingeschichte, also alle jemals durchgeführten Transaktionen, ist in diesen Blöcken erhalten. Wenn neue Transaktionen da sind, werden sie von speziellen Teilnehmern des Bitcoin-Netzwerkes, den Minern, in neuerzeugte Nachfolgeblöcke (Mining) aufgenommen. Die maximale Blockgröße beträgt 4 Megabyte. Weitere Transaktionen kommen dann in die danach folgenden Blöcke. Ein Block wird an den vorhergehenden angehängt, es bildet sich eine Kette, die Blockchain. Die kann in ihrem Fortschreiten direkt im Internet besichtigt werden: https://mempool.space/de/mempool-block/0 Rechts in der Kette stehen in blau die fertigen, angefügten Blöcke der Chain, links die in Vorbereitung befindlichen, die noch nicht gültig gemint sind.

Wichtige Bestandteile eines Blocks sind:
Der Hashwert des jeweils vorherigen Blocks der Kette (da die Blöcke aus Textzeichen bestehen, kann ein Hashwert gebildet werden), die Transaktionen und ein Zahl-Element (natürlich in Textform), das als **nonce** bezeichnet wird.

Einen neuen Block (Anwärterblock) finden und anhängen („minen“):
Der Miner d.h., sein Computer – befüllt nun den Anwärterblock. Für das Element „Hashwert des vorherigen Blocks“ verwendet er den Hashwert des letzten Blocks der Kette. Für das Element „Transaktionen“ bedient er sich aus der Liste der anstehenden neuen Transaktionen und trägt diese ein.

Jetzt beginnt die eigentliche Arbeit. Im Element „nonce“ wird eine Ziffer eingetragen und der Hashwert des Anwärterblocks ermittelt. Die Bitcoin-Vorschrift (das **Bitcoin-Protokoll**) fordert, dass dieser Hashwert am Anfang führende Nullen haben muß, so wie in der Aufgabe oben. Allerdings sind das nicht nur zwei sondern beispielsweise gleich 20 (im Block Nummer 859730 beginnt der Hash so: **00000000000000000000**665b1...). Passt die nonce-Zahl nicht, wird sie durch eine höhere ersetzt und der Hash erneut gebildet. Das geht so lange, bis eine nonce-Zahl gefunden ist, welche die führenden Hash-Nullen liefert. Man kann sich nach den Erfahrungen aus der obigen Aufgabe leicht vorstellen, dass das extrem schwierig ist. In der Tat erfordert das eine gewaltige Rechenleistung, die nur von den leistungsstärksten spezialisierten Computern in vernünftiger Zeit zu bewältigen ist. Der erfolgreiche Miner gibt dann sofort dem Bitcoin-Netzwerk den neuen Block bekannt, der als gültig bezeichnet wird, da er den Regeln des Bitcoinprotokolls entspricht. Damit ist jetzt der bisherige Anwärterblock neuer Bestandteil der Blockchain und zusammen mit ihm auch die enthaltenen Transaktionen. Auf der Mempool-Seite im Internet sieht man einen neuen blauen, gültigen Block erscheinen. Sofort nach dieser Veröffentlichung beginnt die Suche nach einem neuen Anwärterblock: Darin wird für das Element „Hashwert des vorherigen Blocks“ der Hashwert des eben angehängten Block eingetragen und so weiter...

Wozu aber der ganze Aufwand? Sollte irgendwer irgendetwas in einem früheren gültigen Block verändern, den gezahlten Betrag einer Transaktion vielleicht, würde sich der Hashwert dieses

Blocks verändern und mit ihm die Gültigkeit erlöschen (keine 20 Nullen am Anfang). Da der Hashwert im jeweils nächsten Block enthalten ist, würden nach gleichem Muster sofort alle folgenden Blöcke d.h deren Hashwerte ungültig. Die einzige Möglichkeit wäre, alle folgenden Blöcke der Reihe nach schnell neu zu minen. Leicht zu sehen, der Arbeitsaufwand wäre immens und wahrscheinlich unter Einsatz der gesamten weltweit verfügbaren Energie (Computer brauchen Strom) und aller Computer nicht zu bewältigen. Auf diese Weise ist der Bitcoin bombenfest abgesichert durch den sogenannten „**proof of work**“, die beim Mining geleistete Arbeit, d.h. die hineingesteckte Energie.

Die geforderten 20 Nullen bilden die sogenannte „**difficulty**“, die Schwierigkeit, neue gültige Blöcke zu finden. Und die wird von Zeit zu Zeit angepasst. Meist wird sie größer und es werden vielleicht 21 oder mehr Nullen vorneweg verlangt. Den Grund dafür erfahren Sie jetzt.

Es gibt weltweit eine Menge Miner und alle konkurrieren darin, den jeweils nächsten gültigen Block zu finden, so wie eben beschrieben. Ist einer gefunden, verlängert der betreffende Miner die Blockchain mit diesem Block. Alle anderen kriegen das ziemlich schnell mit (siehe unten) und beginnen sofort, den nächsten auf den eben gefundenen Block zu minen.

Das Bitcoin-Protokoll verlangt, dass die Blockchain durchschnittlich alle 10 Minuten um einen neuen gültigen Block verlängert wird. Das erreicht man durch Justierung der Difficulty. Die Rechenleistung der Computer nimmt ja ständig zu und auch die Anzahl der Miner, also der rechnenden Computer kann steigen. Damit werden natürlich insgesamt gesehen schneller gültige Blöcke gefunden. Jetzt wird einfach die Difficulty genau um soviel erhöht, dass es wieder durchschnittlich 10 Minuten sind. Natürlich kommt es vor, dass mal eine Stunde kein Block gefunden wird, dafür sind es aber bei den folgenden vielleicht einigemale nur 3 Minuten. Es zählt eben der Durchschnitt.

Umgekehrt geht es aber auch. Vor einigen Jahren verbot China das Mining (heute scheint sich das allerdings wieder zu relativieren) und das dortige Mining ist in andere Teile der Welt gezogen. Es stand also plötzlich erheblich weniger Rechenleistung zur Verfügung und der 10-Minuten-Takt verlängerte sich erheblich und unerwünscht. Also wurde die Difficulty verringert (weniger führende Nullen) und sofort waren die verbliebenen Miner wieder in der Lage, den Takt zu gewährleisten, solange bis die vertriebenen Miner wieder aktiv wurden und die Difficulty wieder heraufgesetzt wurde. Das war ein Paradebeispiel dafür, wie robust das Bitcoin-Netzwerk auf Störungen reagiert.

2. Der Bitcoin (BTC)

Warum minen die Miner eigentlich und wo bleibt denn nun der Bitcoin? Einen Bitcoin als Entität gibt es nicht, es gibt keinen Gegenstand oder kein Element im Computerbereich der die Funktion einer „Münze“ übernimmt, die von einer Hand zur anderen wandert. **Wirklich alles was es gibt sind Transaktionen**, die einen Sender und einen Empfänger haben und in der Blockchain verewigt sind. Bis auf eine Ausnahme: Die erste Transaktion eines jeden geminten Blocks, die sogenannte **Coinbase** hat nur einen Empfänger, nämlich den Miner des betreffenden Blocks. Und der Wert, der in diese Transaktion nach Bitcoin-Protokoll eingetragen wird, ist gegenwärtig (im September 2024) 3,125. Der Miner, der diesen gültigen Block gefunden hat trägt also diese Coinbase in den Block ein, mit sich selbst als Empfänger, und hat damit 3,125 „Bitcoin“ verdient und neu erzeugt

(ausserdem erhält er von jeder Transaktion einen Anteil, die Transaktionsgebühr). Im Laufe der Zeit wird er diese Bitcoin – oder Teile davon - veräußern (d.h. eine oder mehrere Transaktionen an andere Empfänger anstoßen). Damit verteilen sie sich nach und nach in die Welt des Bitcoin-Netzwerks. Die kleinste Einheit des Bitcoin ist übrigens 0,00000001 BTC.

Diese Belohnung (**reward**) für das Mining ist ebenfalls nicht fix, denn alle 210.000 Blöcke halbiert sich diese Bitcoin-Zahl. Alle 10 Minuten wird ein neuer Block hinzugefügt, das bedeutet, dass etwa alle vier Jahre dieses **halving** stattfindet. Zu Beginn des Bitcoin-Netzwerks im Jahr 2009 betrug der reward 50 BTC. Man kann damit ausrechnen, wieviele Bitcoin heute in Umlauf sind (etwa 19,75 Millionen) und wieviele es jemals geben wird. Die Rechnung ergibt **21 Millionen Bitcoin** die schließlich maximal zur Verfügung stehen und die sich alle Interessierten teilen müssen. Mehr gibt es nicht und mehr wird es nicht geben, basta. Das wird auch nicht zum Problem, da BTC fast unbegrenzt unterteilbar ist; jeder Bitcoin wird im Laufe der Zeit einfach mehr wert, das Interesse der Menschen vorausgesetzt. Damit hat Bitcoin die wichtigste Eigenschaft guten Geldes unverrückbar eingebaut: Die Knappheit. Kein Staat kann beschließen, einfach im Übermaß Bitcoin so wie Geld zu drucken und den Samen einer hohen Inflation zu säen. Warum keine Institution oder Person Einfluß nehmen kann, sei sie noch so mächtig, zeigt der folgende Abschnitt.

3. Das Bitcoin-Netzwerk

Die Transaktionen und der Bitcoin stecken also in der Blockchain, aber wo steckt die Blockchain? Bei den Kontobewegungen Ihres Bankkontos ist es klar: Alles ist zentral auf einem Server der Bank gespeichert und fleißige Bankangestellte stellen sicher, dass alles seinen geordneten Gang geht und überwachen, dass alle Regeln eingehalten werden.

Beim Bitcoin ist das komplett anders. Sämtliche Regeln, Algorithmen, Abläufe des Bitcoins (die Transaktionen, das Mining, Halving, das Zusammenspiel der Abläufe, die konstanten Werte, also einfach alles, was den Bitcoin funktionieren lässt) bilden das sogenannte **Bitcoin-Protokoll** in Software gegossen.

Es gibt ein Netzwerk aus zahllosen weltweit verteilten Knotenpunkten, den **nodes**. Jeder Knoten ist ein größerer oder kleinerer Computer samt Festplatte. Auf jeder Node läuft dieses Bitcoin-Protokoll, auf jeder dazugehörenden Festplatte ist die gleiche, gesamte Blockchain gespeichert. Jede Node sucht sich eine Anzahl von Nachbar-Nodes, mit denen sie im dauernden Austausch steht. Jede Node ist gleichberechtigt zu allen anderen.

Bei der Inbetriebnahme einer Node lädt sie die gesamte Blockchain von den Nachbarnodes und prüft Block für Block selber, ob alle Vorschriften des Bitcoinprotokolls vom allerersten bis zum aktuellsten Block bis ins kleinste Detail eingehalten sind. So sind alle gespeicherten Blockchains auf der ganzen Welt konsistent und ohne Fehler. Kein Betrug, keine Änderung ist möglich.

Wird die Blockchain verlängert, ist also ein neuer gültiger Block dazugekommen und erfährt eine Node davon, überprüft sie selbständig, ob alles gültig ist, also dem Bitcoinprotokoll entspricht. Dann aktualisiert sie die auf ihrer Festplatte gespeicherte Blockchain und informiert sofort ihre Nachbarnodes. Diese führen die gleiche Arbeit aus und innerhalb überschaubar kurzer Zeit ist im gesamten Netz, bei allen Nodes, die Blockchain aktualisiert. Beachten Sie, jede Node prüft nach

dem Bitcoinprotokoll, niemand kann aus der Reihe tanzen. Ein Fehler, ein Betrug würde sofort auffallen und von jeder Node als ungültig verworfen.

Es gibt spezielle Nodes, die mehr können, außer dem eben Beschriebenen. Die werden von den Minern betrieben und da kommen natürlich die neuen gültigen Blöcke rein und werden ins Netz gespeist. Ansonsten funktionieren sie aber wie alle anderen.

Weitere Nodes werden von Wallet-Anbietern betrieben, über die Sie Ihre Transaktionen (Zahlungen) ins Netzwerk schleusen können. Die meisten Nodes allerdings werden von Privatpersonen betrieben (über die diese ebenfalls ihre Transaktionen einschleusen können). Jeder kann so eine Node ohne großen Aufwand selber einrichten - wie demokratisch ist das denn? Damit kann man seine Transaktionen selber direkt ins Bitcoin-Netzwerk einspeisen ohne die Vermittlung von Wallet-Anbietern. Das wichtigste beim Betrieb einer eigenen Node ist allerdings, dass man zur Stabilität des Bitcoins beiträgt. Die zehntausende miteinander kommunizierenden Nodes, die bisher in Betrieb sind, können kaum angegriffen werden. Das Bitcoin-Netzwerk ist mittlerweise für einen derartigen Angriff einfach viel zu groß. Das macht Bitcoin einzigartig in der Welt der Crypto-Währungen.

4. Die Transaktionen

Achtung, im folgenden wird mit starken Vereinfachungen gearbeitet. Aber zum Verständnis des Prinzips sollte es erstmal genügen.

Wie schon erwähnt beinhalten die Transaktionen verschlüsselt den Sender (**Input**), den Betrag und den Empfänger (**Output**). Soll eine Zahlung als Transaktion angelegt werden, benötigt der Sender einen öffentlichen Schlüssel vom Empfänger (denken Sie an die Kasse im Beispiel). Der Empfänger erzeugt den mithilfe seines geheimen Private-Keys, einer ellenlangen Zeichenfolge, bei sich im Stillen (es können, je nach Bedarf beliebig viele verschiedene Public-Keys mit dem einen Private-Key erzeugt werden). Dann sendet er den so geschaffenen Public-Key, ebenfalls eine ellenlange Zeichenfolge an den Absender der Bitcoin. Ob auf dem Weg andere Leute diesen Public-Key mitlesen ist vollkommen egal. Das einzige, was sie machen könnten, wäre, ebenfalls Geld einzuzahlen – der Empfänger könnte sich bedanken.

Der Absender legt nun die Transaktion an, indem er den gewünschten Betrag in Bitcoin einträgt und als Output den Public-Key des Empfängers. Dann wird die gewünschte Transaktion an eine x-beliebige Node übergeben, von wo aus sie sich im Bitcoin-Netzwerk schnell verbreitet und bald von den Minern aufgesammelt wird um schließlich in einem Block der Blockchain zu landen.

Dort fristet sie ihr Dasein als **UTXO**. Die Abkürzung für „Unspent Transaction Output“, was übersetzt heißt „Nicht ausgegebener Transaktions-Output“.

Denn jetzt hat der Empfänger allein mithilfe seines Private-Keys die Verfügungsgewalt über diese Bitcoin-Zahl in dieser Transaktion in diesem Block der Bloickchain. Niemand sonst hat Zugriff. Genau genommen, hat nicht der Empfänger die Kontrolle, sondern der Private-Key. Sobald jemand anderes diesen Key hat, hat er uneingeschränkten Zugriff auf alle Bestände, die damit verbunden sind. Nicht umsonst gibt es in der Bitcoin-Welt den Spruch „**Not your keys, not your coins**“. Denn

auch bei Verlust des Private-Keys oder Vergessen gibt es keine, wirklich keine Möglichkeit der Wiederherstellung. Das Vermögen ist unwiederbringlich verloren!

Diese seine UTXO kann nun vom Empfänger, der in diesem Fall zum Sender mutiert, verwendet werden, um eine neue Transaktion an jemand anderen als Empfänger anzustoßen. Dabei verwendet er seinen Private-Key, um sein Eigentum an dieser UTXO zu beweisen. Gleichzeitig verliert diese Transaktion ihren Status als „nicht ausgegeben“. Doppelte Ausgaben ein und derselben Transaktion sind damit zuverlässig ausgeschlossen.

5. Die Wallet

Wie genau eine Transaktion neu angelegt wird ist im Bitcoin-Protokoll festgelegt und ziemlich kompliziert. Glücklicherweise gibt es sogenannte Wallets, die das und einiges andere für uns übernehmen. Die gibt es als reine Softwarelösung, also Apps und als Hardware die über USB-Kabel an den Computer angeschlossen wird .

Zuallererst müssen wir unseren Kontostand kennen. Wie jetzt schon deutlich ist, gibt es keine Bitcoin im Sinne einer symbolischen Münze (so wie den Euro). Wir erinnern uns, es gibt ausschließlich Transaktionen in der Blockchain, die Bitcoin-Beträge enthalten, unter anderem die Coinbase, die den initialen Bitcoin-Betrag beim Mining enthalten. Und speziell gibt es die UTXOs, die noch nicht ausgegebenen.

Was damit in keinem Fall in der Wallet enthalten ist sind unsere Bitcoin! Die Wallet durchsucht hingegen mit Hilfe des Private-Keys die Blockchain nach unseren UTXOs (die wir mittels unseres Private-Keys kontrollieren) und zeigt diese an. Sie bildet auch die Summe und präsentiert den Kontostand. So ist nun auch klar, dass die Wallet der Ort ist, wo unser Private-Key haust und diesen niemals, unter keinen Umständen verlassen darf. Klar, dass damit Hardware-Wallets um Lichtjahre sicherer als Software-Wallets sind; ein Muß bei größeren Beständen.

Soll eine Transaktion, also eine Zahlung durchgeführt werden, teilen wir der Wallet die Adresse (Public-Key) des Empfängers und den Betrag mit und klicken auf „Senden“. Das ist alles, die Wallet kümmert sich dann um den ganzen Rest, so wie im Abschnitt „Transaktionen“ beschrieben.

6. Vierundzwanzig Wörter

Hier folgt nun das Praxiskapitel für den Benutzer. So kompliziert sich das ganze bis jetzt dargestellt hat, so einfach ist die Anwendung.

Sie benötigen eine Wallet und einen Computer oder ein Handy. Die Wallet können Sie entweder als App installieren (Software-Wallet) oder erwerben (Hardware-Wallet).

Um zu einem Teilnehmer am weltweiten Bitcoin-Netzwerk zu werden, richten Sie die Wallet entsprechend der Anbieterangaben ein. Im Verlauf dessen werden 24 Wörter erzeugt (per Zufall aus einer international einheitlichen Liste von 2048 englischen Begriffen), die Ihnen zur Kenntnisnahme präsentiert werden. Die haben es wirklich in sich, passen Sie da gut auf! Denn mithilfe dieser Wörter erzeugt die Wallet Ihren hochgeheimen Private-Key. **Wer diese Wörter**

kennt, hat sofort Zugriff auf Ihr Bitcoin-Vermögen. Dieser Private-Key wohnt ab jetzt in Ihrer Wallet, gut verborgen, eingesperrt und abgeschirmt bei Hardware-Wallets und vermutlich ganz gut geschützt bei Software-Wallets. Ab jetzt ist Ihre Wallet „scharf“ und Sie können über sie Transaktionen vornehmen und Ihren Kontostand sehen. Bei all diesen Tätigkeiten gelangt der Private-Key niemals aus der Wallet hinaus in den Computer, das Handy oder gar das Internet. Aber darüber müssen Sie sich dann keine Gedanken mehr machen.

Und der Clou an der ganzen Sache ist: Solange Sie Ihre 24 Wörter kennen können Sie sich überall auf der Welt eine jungfräuliche Wallet besorgen und bei der Einrichtung Ihre persönlichen 24 Wörter angeben anstatt neue Wörter erzeugen zu lassen. Das kann so gut wie jede verfügbare Wallet, es muß nicht die gleiche sein, die Sie bei der Erzeugung der Wörter verwendet haben. Und innerhalb kürzester Zeit haben Sie die volle Verfügungsgewalt über Ihr Bitcoin-Vermögen, ohne Gebühren, Wartezeiten oder dass irgendjemand anders, eine Bank oder ein Service zum Geldtranfer benötigt würde. Welches andere Geld bietet denn solche Möglichkeiten?

Verwahren Sie also Ihre 24 Wörter sorgfältig. Und merken Sie sie sich. Wie meinen? 24 Wörter merken sei für Ihr Gedächtnis kaum möglich? Lesen Sie den Anhang, ich zeige Ihnen da einen simplen Trick, wie das ganz leicht geht. Ganz wichtig: Unter keinen Umständen allein auf’s Merken verlassen! Vergessen wäre fatal. Also immer ein oder zwei sichere Stellen der Verwahrung parat haben.

Anmerkung: Wer ganz sicher gehen will, kann sich die 24 Wörter auch selber aus der ganzen Liste verfügbarer Wörter zusammenwürfeln. Da gibt es Anleitungen.

7. Das hat man nun davon (vom Bitcoin)

Ein gutes Geld

- das niemanden zur Überwachung oder zum Transfer benötigt, keine Bank und keinen Dienstleister (es überwacht sich durch das verteilte Netzwerk und das Bitcoinprotokoll selber) und vollkommen dezentral ist (im Gegensatz zum Zentralbankgeld und anderen Kryptowährungen). Es kann nicht manipuliert werden, weder durch Betrüger noch durch wohlmeinende Zentralbanken oder Regierungen.
- in dem unbeschwert gespart werden kann, weil es knapp ist und knapp bleibt.
- das in der absoluten Verantwortung des Inhabers liegt.
- das bereits die weltweit größte Akzeptanz mit gewaltigem Abstand zu allen konkurrierenden Kryptowährungen gefunden hat.
- das liquide und augenblicklich transferierbar ist.

8. Der benötigte Strom

Der Stromverbrauch des Bitcoin-Netzwerks dient nicht zum “Finden neuer Bitcoins” und er ist unabhängig von der Anzahl der Teilnehmer oder Transaktionen. Er dient ausschließlich zum Finden gültiger Blöcke im 10-Minuten-Takt (die Schaffung neuer Bitcoin ist nur ein Nebeneffekt). Damit ist er kein Fehler, sondern die wichtigste Funktion um die Sicherheit und Stabilität des Netzwerkes und aller Transaktionen zu garantieren.

Gutes Geld, so wie es Bitcoin darstellt - und es gibt so kein zweites – ist eine der Säulen einer Zivilisation. Dafür könnte man durchaus ausreichend Energie zur Verfügung stellen.

Jedenfalls kann der Stromverbrauch des Mining zur Stabilität des Stromnetzes aus erneuerbaren Energien beitragen. Es ist gängige, verbreitete Praxis, dass Miner gerade dann Strom abnehmen, wenn zuviel davon da ist, bei knappem Angebot dagegen wird einfach das Mining zurückgefahren. Ein Großteil der Mining-Hardware wird sowieso schon durch erneuerbare Energien betrieben.

9. Die bösen Buben?

Wer mit Bitcoin arbeitet, ist keineswegs anonym. Mittlerweile sind fast alle Anbieter über die man Bitcoin erwerben oder verkaufen kann in Europa und zunehmend auch im Rest der Welt reglementiert. Man muß da ein Verifizierungsverfahren mit Ausweis und Kontodaten durchführen, so ähnlich wie bei der Kontoeröffnung bei einer Bank. Erst dann erhält man Zugang. Diese Anbieter sind die Schnittstelle des traditionellen Geldsystems zum Bitcoin. Es gibt da zum Beispiel Kryptobörsen bei denen der Handel mit Bitcoin und Euro oder US-Dollar so ähnlich wie bei Aktien stattfindet. Wichtig zu wissen: In dieser Funktion sind sie nicht Teil des Bitcoin-Netzwerkes, sondern externe Anbieter. Wenn jemand also einen größeren Bitcoin-Betrag in Euro wandeln will, weiß der Staat Bescheid. Geldwäsche und jede andere Form der Geldkriminalität sind daher ähnlich schwierig oder leicht zu bewerkstelligen, wie bei den traditionellen Systemen zum Geldtransfer. Die Handlungen Krimineller können beim Bitcoin sogar leichter zurückverfolgt werden als beim Bargeld. Der Großteil der Nutzer sind heute ehrliche Bürger und legale Institutionen. Sogar große Firmen wie PayPal oder BlackRock setzen mittlerweile auf Bitcoin.

Der Crypto Crime Report 2024, vom Analyseunternehmen Chainalysis herausgegeben, meldet insgesamt einen Rückgang der illegalen Aktivitäten am Kryptomarkt. Während Chainalysis den Anteil an illegalen Transaktionen im Jahr 2022 noch mit 0,42% angab, betrug dieser für das Jahr 2023 nur 0,34%! In jeder anderen Währung ist dieser Anteil vermutlich wesentlich höher.

Transparenz ist eine wichtige Eigenschaft der Blockchain. Alle jemals getätigten Transaktionen beginnend mit der allerersten Bitcoin-Transaktion sind öffentlich einsehbar (z.B. hier https://mempool.space/de/mempool-block/0). Behörden oder darauf spezialisierte Unternehmen (z.B. Chainalysis) können da natürlich sehr leicht herausfinden, welche Transaktion von wem an wen ging .

Und das war’s dann auch schon. Vielleicht ist das für Sie der Beginn einer spannenden Entdeckungsreise in die Welt des Bitcoin. Ich wünsche jedenfalls viel Erfolg!

Anhang

Ein einfaches System, sich seine 24 Wörter zu merken (vorausgesetzt Sie können Englisch)

Achtung!!!!!!! Sichern Sie die Wörter unbedingt auch anderweitig, denn wenn Sie die vergessen, können Sie auch Ihre Bitcoin-Bestände vergessen. Die Wörter im Kopf zu haben, kann aber in misslichen Situationen die Rettung sein, denn mit ihnen sind Sie immer handlungsfähig.

Nehmen wir an, die ersten 12 Wörter (hier zufällig aus den 2048 Wörtern ausgewählt) wären

1 upper	2 salt	3 marriage
4 breeeze	5 allow	6 candy
7 poem	8 input	9 achieve
10 guitar	11 cash	12 point

Unterteilen Sie die Wörter in vier Grupen zu je drei Wörtern. Zu jeder Gruppe überlegen Sie sich eine Geschichte oder ein Bild. Um so abstruser oder wilder die Phantasie, umso besser und wirkungsvoller. Beispiele dafür wären folgende:

upper salt marriage: Ein Berg aus Salz, oben tanzt ein Brautpaar

breeeze allow candy: Eine leicht Brise streicht um den geöffneten Mund und säuselt „jaaaa“. Dann verschwindet ein Bonbon im Mund.

poem input achieve: Man versucht, ein Gedicht auf Papier zusammenzufalten und in eine winzige Dose zu stecken. Schließlich gelingt es.

guitar cash point: Eine automatisch spielende Gitarre, davor ein Hut, in den Geld geworfen wird. Schließlich schnurrt der Hut zu einem Punkt zusammen.

Visualisieren Sie Geschichten und wiederholen damit die Wörter jeden Tag, solange, bis es von selber abläuft. Man kann das in „unproduktive“ Zeiten schieben (im Bad, im Wartezimmer und so weiter). Sie werden sehen, wie es immer leichter geht, bis es schließlich wie am Schnürchen läuft. Als interessanten Nebeneffekt können Sie die Funktionsweise Ihres Gehirns beobachten, wie die Gedächtnisinhalte in andere Bereiche mit unterschiedlichen Arten der Speicherung wandern.

Wenn die ersten 12 Wörter sitzen, nehmen Sie sich die zweite Hälfte der 24 Wörter auf gleiche Weise vor. Das Gedächtnis so zu trainieren macht ausserdem richtig Spaß.