BITCOINEXPLAINED

HANDOUT

Teil 2

Bitcoin kaufen und verwalten

INHALT

Erste Überlegungen 1
Kaufmethoden 2
Handelsplätze 4
Gebühren 7
Wallets – Funktionsweise 8
Wallets – Sicherheit 12
Wallet-Arten 12
Wallets – Fazit 15
Funktionsweise einer Transaktion 15
Zusammenfassung/Vergleich 21
Bildquellen 23
Abschließende Bemerkungen 24

Handout zum Praxis-Kurs von BITCOINEXPLAINED.DE

Kauf und Verwaltung von Bitcoin

ERSTE ÜBERLEGUNGEN

Bitcoin bietet verschiedenste Möglichkeiten zum Kauf und zur Verwaltung. Es gibt verschiedene Wallet-Typen und verschiedene Arten von Börsen.
Alle Herangehensweisen bieten unterschiedliche Vor- und Nachteile bzw. Trade-Offs, die man kennen sollte. In diesem Handout gehen wir zuerst auf die verschiedenen Möglichkeiten und Besonderheiten beim Kauf ein und widmen uns danach der sicheren Verwaltung und Verwahrung. Die Verwaltung und Verwahrung kann zu jedem Zeitpunkt angepasst und verbessert werden. Es ist sinnvoll sich vor dem Kauf darüber Gedanken zu machen, jedoch nicht zwingend erforderlich.

Die Ausführungen in diesem Dokument stellen keine Finanzberatung dar, sondern dienen lediglich als Anleitung zum sicheren Kauf und zur Verwaltung von Bitcoin.

Dem ersten Bitcoin-Kauf sollten einige Gedanken vorausgehen:

- Wo kaufe ich?
- Auf welche Art kaufe ich?
- Welches Ziel verfolge ich?
- Was ist mir beim Kauf wichtig?
- Bin ich mir über die Gebühren im Klaren?

Für den Kauf bieten sich Börsen/Exchanges an. Weiterhin kann man auf P2P-Plattformen (peer-to-peer) kaufen oder auch Privat von Leuten, die bereits Bitcoin besitzen, Bitcoin erwerben. Hierbei ist es wichtig, die Vor- und Nachteile zu kennen und sich klar zu werden, welche Kriterien für einen selbst wichtig sind.

- Wie wichtig ist mir die Privatsphäre?
- Möchte ich Bitcoin nach dem Kauf direkt auf meiner eigene Wallet empfangen?
- Ist es mir wichtig, dass die Plattform komplett reguliert ist?
- Ist mir Kundensupport wichtig?
- Ist es mir wichtig, dass die Benutzeroberfläche auf deutscher Sprache verfügbar ist?
- Sind mir Lightning-Transaktionen wichtig?
- Möchte ich einen automatischen Sparplan anlegen oder manuell kaufen?
- Benutze ich Limit-Order oder Market-Order?
- Benötige ich zusätzliche Dokumentationen und Hilfe zur Funktionsweise und Abwicklung?

Es ergibt Sinn zuerst die eigenen Ziele zu definieren, um danach Rückschlüsse zu ziehen, welche anderen Faktoren einen hohen Stellenwert haben.
Plane ich Bitcoin nur für einen gewissen Zeitraum zu halten, um Profite in Fiatwährungen zu generieren? Oder plane ich Bitcoin für die Zukunft zu sparen, weil ich bspw. davon ausgehe, dass Bitcoin den monetären Wert der Fiatwährungen komplett verschlingt und diese letztendlich ersetzt? Je nachdem, welches Extrem als Antwort auf diese Frage gewählt wird, ergibt dies Auswirkungen auf die Methode des Kaufes, die Art der Wallet und die Wahl der Börse oder Bezugsquelle von Bitcoin-Einheiten.
Prinzipiell ist es ratsam vorerst ein Grundverständnis für Bitcoin zu entwickeln bevor erste Kaufentscheidungen getroffen werden.

ERSTE ÜBERLEGUNGEN

Bitcoin ist kein „Get rich quick scheme" (System, das einem schnellen Reichtum verspricht) sondern ein „Don´t get poor slow scheme" (Das Gegenteil: System, das einem verspricht, nicht langsam arm zu werden).
Wenn das Konzept hinter Bitcoin und die Gründe für die Dringlichkeit noch nicht bekannt sind, empfehlen wir unseren Kurs rund um das Basiswissen zu Bitcoin.

Hier klicken, um Teil 1 zu buchen

Basierend auf dem vermittelten Wissen aus unserem ersten Teil kommt man wahrscheinlich zu dem Schluss, dass die Entscheidung Bitcoin zu kaufen, langfristig ist. Nichtsdestotrotz werden wir auch die Möglichkeit der schnellen Verfügbarkeit beim Vergleich in Betracht ziehen.

KAUFMETHODEN

Bitcoin kann auf unterschiedliche Arten gekauft werden. Man kann einen Betrag direkt kaufen (Market Buy), einen Betrag in Tranchen aufteilen und entsprechende Käufe automatisch (automatisierte Limit-Order) oder manuell ausführen oder eine Art wiederkehrenden automatisierten Sparplan einrichten, der regelmäßige Käufe abwickelt.

Wenn man den Markt bereits besser versteht und weiß, welche Wechselwirkungen das Halving, die Hashrate und der Preis (gemessen in Fiat) haben dann ist es durchaus möglich, gute Einstiegspunkte zu finden. Wenn man sich also im Timing des Marktes versuchen möchte kann man per Market-Order direkte manuelle Käufe durchführen. Alternativ kann man auch eine Limit-Order für niedrigere Preise erstellen und somit darauf spekulieren, dass man letztendlich mehr Bitcoin für den Euro erhält.
Diese Methoden sind aus unserer Sicht aber eher in Ergänzung zu einem Sparplan sinnvoll denn letztendlich ist das Ziel die Menge an Satoshis zu vermehren, die man besitzt.

„Time in the market beats timing the market"

DCA steht für „Dollar Cost Average", ein regelmäßiger (meist automatisierter) Kauf, der einem Sparplan gleichkommt und den Vorteil hat, Volatilitäten im Preis auszugleichen. Weiterhin lässt DCA, bei vollautomatischer Einrichtung, keinerlei Emotionen zu. „Set and forget" - Einrichten und vergessen.
DCA macht regelmäßiges Bitcoin-Sparen möglich, um so von den hohen Preisschwankungen zu profitieren und langfristig ein stetig wachsendes Vermögen aufzubauen und zu sichern.
Ob der Sparplan vollautomatisch ist oder manuell ausgeführt wird ist eine individuelle Präferenz. Wichtig ist jedoch, die Regelmäßigkeit (bspw. monatlich oder wöchentlich) und ein gleichbleibender Betrag, der am Besten am Anfang des Monats zum Kaufen verwendet wird („Pay yourself first" - Bezahle dich selbst zuerst).Um den Effekt dieser Durchschnittskäufe zu sehen und zu errechnen, kann diese Webseite besucht werden.
Hier wird ersichtlich, welchen Effekt ein automatischer Sparplan über die letzten Jahre gehabt hat. Zeitraum, Intervall und Betrag sind einstellbar. Daher kann man sich ein sehr gutes Bild machen, wie der Betrag an Satoshis gewachsen wäre.

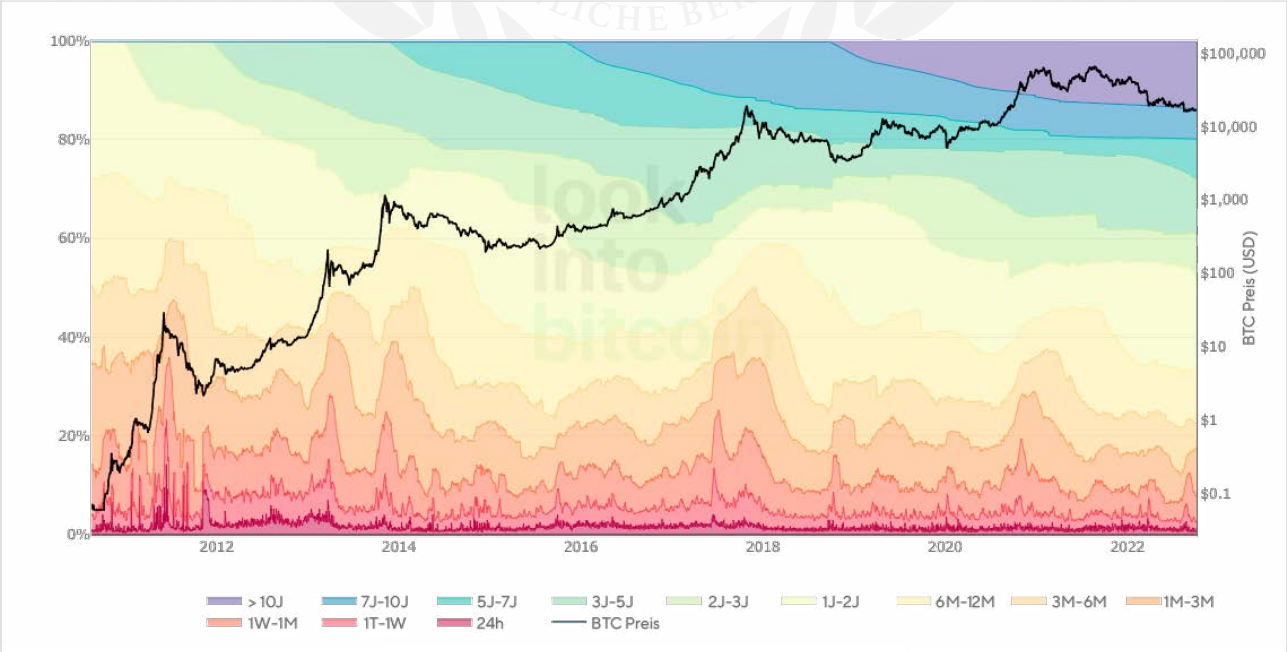
Eine langfristige Betrachtung von Bitcoin ist sinnvoll, wenn man die Volatilität (gemessen in Fiat-Währungen) berücksichtigt. Je nach Wissensstand oder Überzeugung kann es schwierig sein, den Wert auszublenden und nicht mehr in Euro oder Dollar umzurechnen.
Man muss sich aber bewusst werden, dass selbst wenn der Plan ist, später einen Verkauf zu tätigen, die Volatilität historisch eher hilfreich war.

Weiterhin kann man am 31.12.22 bei einem Preis von ca. 15.500$ pro Bitcoin feststellen, dass ein Großteil der Käufer im profitablen Bereich ist. Dies kann man am nachstehenden Chart ablesen.

KAUFMETHODEN

Der Chart zeigt die Anzahl der profitablen Tage anhand des derzeitigen Kurses. In ~83% der Fälle wäre es also profitabel gewesen Bitcoin zu kaufen. Und dies ist der Fall nachdem der Kurs, gemessen in US-Dollar, um knapp 75% eingebrochen ist.

Eine weitere Analyse entsprechender Daten zeigt, dass kurzfristiges Trading nach wie vor noch einen großen Teil des gesamten Volumens einnimmt, dies aber vor allem passiert, wenn der Preis schnell ansteigt oder abfällt. Bei massiven Preisbewegungen ist es attraktiver schnelle Trades zu platzieren, da somit potenziell ein schneller Gewinn möglich ist.
Darüber hinaus zeigt diese Grafik, dass ein Großteil an Bitcoin langfristig gehalten wird.



KAUFMETHODEN

Je nach Kaufmethode bieten sich andere Börsen an.
Wenn man größere Summen als Einzelkäufe tätigen möchte, ist es sinnvoll eine Börse zu wählen, die eine hohe Liquidität bietet, da es bei bspw. kleineren Börsen dazu kommen kann, dass diese durch die Liquidität limitiert sind. Gerade bei P2P- Börsen (peer-to-peer) bei denen man direkt von einem anderen Handelspartner kauft, ist man abhängig von den Verkäufern und der angebotenen Summe.
Einige Börsen bieten hierfür allerdings auch die Möglichkeit, dass ein größerer Kauf, welcher nicht von einem Verkäufer bedient werden kann, automatisch auf mehrere Verkäufer aufgeteilt wird, so dass die gewünschte Summe ohne Probleme erworben wird.

Teilweise sucht man sich seinen Handelspartner selbst aus und teilweise wird dieser automatisch zugewiesen. Weiterhin ist der Mindesthandelsbetrag ebenso zu beachten, wie die maximale Kaufsumme. Die maximale Kaufsumme kann von den bereits abgeschlossenen Käufen auf der jeweiligen Plattform abhängen. Wenn eine gewisse Anzahl an Käufen abgeschlossen ist oder ein gewisses Level an positiven Bewertungen von direkten Handelspartnern erreicht wurde, ist es bei diesem System möglich, einen höheren Handelsbetrag freizuschalten. Dies sollte ebenfalls bei der Wahl der Börse beachtet werden, vor allem wenn einmalige, höhere Beträge vorgesehen sind.

HANDELSPLÄTZE

In diesem Kapitel widmen wir uns den verschiedenen Handelsplätzen/Börsen und Möglichkeiten, Bitcoin zu kaufen. Wir gehen dabei vorerst auf die allgemeinen Unterschiede ein und stellen später einige ausgewählte Handelsplätze mit potenziellen Vor- und Nachteilen vor.
Bitte beachte, dass dieses Kapitel nur einen Bruchteil der existierenden Börsen abdecken kann und somit nicht als Empfehlung von Handelsplätzen dient. Wir möchten lediglich verschiedene Handelsplätze vorstellen und somit auf Unterschiede in der Abwicklung, den Zahlungsmethoden oder der Benutzerfreundlichkeit hinweisen.
Allgemein kann man die Handelsplätze nach ihrer Regulierungsform unterteilen. So gibt es vollregulierte Börsen, welche oftmals auch mit Banken zusammenarbeiten und somit eine Komplettlösung anbieten. Bei diesen Börsen gilt der Grundsatz des „KYC" (Know Your Customer - Kenne deinen Kunden), wodurch nach aktueller Gesetzeslage eine vollständige Verifizierung der Person notwendig ist, welche durch den eigenen Ausweis oder Reisepass erfolgt und teilweise ebenfalls einen Adressnachweis, bspw. in Form einer Haushaltsrechnung erfordert. Es gibt ebenfalls sogenannte „KYC-Light"-Optionen, welche keine vollständige Verifizierung mit dem Ausweis verlangen, aber dennoch mit dem eigenen Bankkonto verknüpft werden. Und es gibt Handelsplätze, welche auf die Privatsphäre fokussiert sind und somit keinerlei persönliche Daten verlangen. Letzte setzen meistens aber auch ein höheres technisches Verständnis voraus bzw. könnten als weniger nutzerfreundlich angesehen werden.
Weiterhin gibt es in vielen Städten in Deutschland mittlerweile auch regelmäßige Treffen von Bitcoin-Enthusiasten bei denen oftmals auch Transaktionen stattfinden können. **Hier findest du eine Liste der Treffen.**

Regulierte Exchanges
bitcoin.de ist ein vollständig regulierter, deutscher Anbieter, welcher einen P2P-Marktplatz bietet. Das bedeutet die Plattform bringt Käufer und Verkäufer zusammen und fungiert als Mittelsmann. Verkäufer versenden hier Bitcoin an die Empfangsadresse ihres Kontos bei bitcoin.de und können diese dann anschließend zum Verkauf freigeben. bitcoin.de ist in diesem Moment Besitzer der Private Keys und kann somit die Summe, die zum Verkauf angeboten werden soll, blockieren bis entweder die Zahlung des Käufers erfolgt und eine Transaktion zur Wallet des Käufers stattfindet oder der Verkauf abgebrochen wird, wenn der Käufer bspw. nicht zahlt.
Ein Kauf funktioniert per SEPA-Transaktion vom eigenen Bankkonto. Wenn die Zahlungen über das eigene Bankkonto abgewickelt werden, erstellt man für einen Kauf eine SEPA-Überweisung an die entsprechende Bankverbindung des Verkäufers und markiert die Zahlung bei bitcoin.de als abgeschlossen. Nach Zahlungseingang tut der Verkäufer dies ebenfalls und die bisher blockierten Bitcoin-Einheiten werden der eigenen Wallet bei bitcoin.de gutgeschrieben.

HANDELSPLÄTZE

Es wird ebenfalls die Möglichkeit der Echtzeitüberweisungen angeboten, um einen schnellen Handel zu ermöglichen. bitcoin.de hat mehrere verschiedene sogenannte Trust-Level eingeführt, welche über die Handelslimits entscheiden. Beim Kauf und Verkauf kann man, basierend auf diesen Trust-Leveln, auch seine Handelspartner wählen. Weiterhin kann man Nutzer bewerten und sich somit auch über die Handelspartner informieren.
bitcoin.de ist seit 2011 am Markt und gehört somit zu einer der ältesten Börsen. Das User-Interface ist recht altmodisch aber es gibt auf der Webseite sowohl deutschen Kundensupport als auch deutschsprachige Erklärungen und Dokumentationen zu den Funktionsweisen.

kraken.com ist ebenfalls seit 2011 am Markt und gilt als sehr sicher und bewährt. Kraken hat eine hohe Liquidität und führt auf der Webseite ebenfalls einen sehr guten Hilfebereich. Dieser ist allerdings nur auf englischer Sprache verfügbar. Bei Kraken kann mit Apple Pay, Google Pay, Kredit- oder Debitkarte sowie SEPA-Zahlungen bezahlt werden. Es ist also erforderlich die entsprechende Zahlungsart mit dem Kraken-Account zu verbinden, um Handeln zu können. Weiterhin ist es unerlässlich sich bei Kraken mit seinem Ausweis zu verifizieren. Kraken unterstützt zur Auszahlung von Bitcoin sowohl On-Chain als auch in Form von Lightning-Transaktionen. Nach dem Kauf wird die entsprechende Summe direkt auf der mit dem Konto verknüpften Hot-Wallet gutgeschrieben. Eine Besonderheit bei Kraken ist, dass man selbst verifizieren kann, dass Kraken tatsächlich die Reserven hat, um eine Auszahlung von der Hot-Wallet zu gewährleisten. Dies geschieht über einen sogenannten „Proof of Reserves". Die Funktionsweise kann auf dieser Webseite nachgelesen werden. Die Prüfung geschieht über eine unabhängige, jedoch von Kraken ausgewählte Buchhaltungsfirma.
Kraken bietet weiterhin einen Sparplan zur Verfolgung der DCA-Strategie, welcher wöchentlich, alle zwei Wochen oder monatlich ausgeführt werden kann. Außerdem ist zu erwähnen, dass auch eine App existiert, welche für den Kauf genutzt werden kann.

„KYC-Light"

Im nächsten Abschnitt widmen wir uns der Möglichkeit Plattformen zu nutzen, welche die „KYC-Light"-Option anbieten. Hierbei stechen im DACH-Raum vor allem zwei Schweizer Unternehmen hervor, welche jeweils eine recht ähnliche Lösung anbieten. Beide bieten **nur** Bitcoin an, was den Kauf erleichtert und generell das Nutzen angenehmer macht.

Das eine Unternehmen heißt Relai.app, welches nur als App für das Smartphone verfügbar ist. Relai bietet eine sehr einfache Nutzeroberfläche und somit eine sehr einfache Möglichkeit, einen Kauf zu tätigen. Hierbei kann man sich entscheiden, ob man einen Einzelkauf tätigen möchte oder einen Sparplan einrichtet. Nachdem die App heruntergeladen wurde, wird eine sogenannte „Non-Custodial-Wallet" eingerichtet, bei der man die eigenen Keys verwahrt. Dies unterscheidet Relai bspw. von den eingangs beschriebenen regulierten Handelsplätzen, da es sich hierbei um eine „Custodial-Lösung" handelt, bei der man keinen Zugriff auf die Private Keys hat. Mehr dazu wird später in diesem Handout erläutert. Das Versenden und Empfangen ist ebenfalls über die App möglich und Relai bietet einen deutschsprachigen Support an. Der Mindestbetrag zum Kauf liegt bei 10 Euro und es können bis zu 1.000 Euro pro Tag gespart werden. Es ist, wie erwähnt, keine Anmeldung oder Verifizierung notwendig und die Bezahlung erfolgt über das eigene Bankkonto als (Sofort-)Überweisung oder auch per Kreditkarte sowie Apple Pay. Mit einem Empfehlungscode und dem Aufsetzen eines wiederkehrenden Sparplans von über 100 Euro kann eine Kaufgebühr von 1% erreicht werden. Zusätzlich bietet Relai ein Empfehlungsprogramm mit Umsatzbeteiligung an den geworbenen Kunden.

Das zweite Unternehmen ist Pocket,welches sowohl in einer Browserversion, als auch als App verfügbar ist. Der wesentliche Unterschied zu Relai ist, dass es bei Pocket möglich ist, seine eigene (Hardware-)Wallet zu verknüpfen. Die Auszahlung des Kaufbetrages erfolgt somit direkt zur eigenen Wallet. Die Kaufoption über Pocket ist mittlerweile auch in die BitBox-App des Hardware-Wallet-Herstellers integriert und ermöglicht so eine einfache Anbindung und macht die Notwendigkeit einer weiteren App (neben der BitBox-App) überflüssig. Es ist noch erwähnenswert, dass bei Pocket **kein** Verkauf möglich ist. Pocket benötigt ebenfalls keine Anmeldung oder Verifizierung mit einem Ausweis. Die Bezahlung erfolgt auch über das eigene Bankkonto.

HANDELSPLÄTZE

Der Support und das umfangreiche Wissenscenter sind auch auf deutscher Sprache verfügbar. Pocket ermöglicht weiterhin den Kauf und die folgende Auszahlung über das Lightning-Netzwerk, was die Netzwerkgebühren bei Auszahlungen selbstverständlich senkt. Genau wie Relai bietet Pocket durch den entsprechenden Aufbau nur Market-Order an, sprich den Kauf zum aktuellen Marktpreis und keine Möglichkeit eine Limit-Order in Auftrag zu geben. Die Verknüpfung mit Pocket kann von den meisten gängigen (Hardware-)Wallets erfolgen. Dies ist auf der Webseite auch sehr gut dokumentiert und Schritt für Schritt erklärt. Zum Kauf über Pocket in Verbindung mit der BlueWallet **haben wir auch einen Quickstart-Leitfaden geschrieben**. Pocket bietet ebenfalls ein Dashboard, welches nach Eingabe der verwendeten E-Mail Adresse eine Übersicht zu allen getätigten Transaktionen zeigt. Diese können gefiltert und exportiert werden.

Privacy-Kauf
Bitcoin ist digitales Eigentum und somit spielt die Privatsphäre für einige eine große Rolle. Daher werden wir in diesem Abschnitt einige Möglichkeiten beleuchten, die es erlauben, Bitcoin vollständig anonym zu kaufen. Bitte beachte, dass diese Methoden ein tieferes Verständnis von der Funktionsweise von Bitcoin, Transaktionen und Wallets voraussetzen und somit tendenziell nicht für Einsteiger geeignet sind, da hierbei das Risiko höher ist, Fehler zu machen. Außerdem muss man bei anonymen Plattformen damit rechnen, dass man einen höheren Preis als auf vollständig regulierten Börsen bezahlt. Wir empfehlen dazu sich vorerst näher mit der Materie zu befassen und sich mit den verschiedenen Börsen und bspw. deren Nutzer-Bewertungssystemen vertraut zu machen, um Betrug zu vermeiden. Dennoch wollen wir diese Methoden der Vollständigkeit halber aufführen und grundlegend besprechen.

Bisq bietet eine dezentralisierte Peer-to-Peer-Handelsplattform, auf welche über eine Software zugegriffen werden kann. Um Bisq zu benutzen ist daher zuerst der Download des Programms auf den eigenen Computer oder Laptop notwendig. Wenn der Download und die Installation abgeschlossen sind, erhält man ohne weitere Anmeldung oder Verifizierung, Zugriff zur Plattform und den potenziellen Handelspartnern. Die eigenen Daten verlassen den eigenen Computer nicht, da durch die dezentrale Struktur keine Verbindung zu einem zentralen Server notwendig ist. Die Verbindung erfolgt über das Tor-Netzwerk und der Source-Code für die Bisq-Software ist Open-Source und somit von jedem verifizierbar oder sogar selbst nutzbar, da die Lizenz öffentlich ist. Bisq ermöglicht den Nutzern ihre bevorzugte Währung und Zahlungsmethode zu wählen (je nach gewählter Fiat-Währung ist es möglich, dass mehr oder weniger Handelspartner vorhanden sind). Als Bezahlmethode kann also neben vielen weiteren Möglichkeiten bspw. eine Überweisung an den Handelspartner oder die Bezahlung durch Amazon-Gutscheine gewählt werden. Dadurch ist nicht zurückverfolgbar, dass man im Gegenzug Bitcoin erhalten hat. Bisher musste man, um auf Bisq handeln zu können vor einem Trade allerdings ebenfalls eine gewisse Summe an Bitcoin an die über Bisq erstellte Non-Custodial-Wallet transferieren. Bei einem Handel wird eine gewisse Summe von Bitcoin durch Nutzung einer sogenannten Multisig-Lösung „eingefroren" und erst wieder freigegeben wenn der Handel abgeschlossen ist und beide Seiten dies signalisieren. Dies verhindert den Anreiz für betrügerische Handlungen und sichert vor allem die Verkäufer ab. Nach erfolgreichem Trade wurde der Bitcoin-Betrag selbstverständlich wieder freigegeben. Gerade wenn einem die Privatsphäre wichtig ist, so ist an dieser Stelle erwähnenswert, dass die Bitcoin, welche für den Handel hinterlegt werden, ebenfalls bereits anonymisiert sein sollten. Dies kann bspw. über einen sogenannten „Coinjoin" geschehen. Auf die Möglichkeit der Anonymisierung und weiterer Privatsphäre-Aspekte gehen wir in unserem „Teil 3 - Für fortgeschrittene Nutzer" ein. Seit 2024 bietet Bisq aber auch eine stark vereinfachte Variante des Handels an, für die keine Bitcoin vorhanden sein müssen. Über Bisq kann ein eigenes Angebot für einen Kauf erstellt werden oder ein bestehendes Angebot angenommen werden. Je mehr Trades man selbst eingeht, desto öfter und länger Bisq benutzt wird, desto mehr Vertrauen haben andere Nutzer und Bisq belohnt dies ebenfalls durch mehr Möglichkeiten und Handelspartner. Bisq bietet insgesamt eine übersichtliche Software und eine gute Dokumentation und Hilfestellung in englischer Sprache.

Eine weitere Plattform ist HodlHodl, welche auf Peer-to-Peer-Basis funktioniert. Auf der Webseite ist es notwendig sich mit einem Pseudonym und einer E-Mail-Adresse zu registrieren. HodlHodl fungiert als Treuhandservice und ist zu keiner Zeit in vollständigem Besitz der Keys. Es wird ebenfalls wieder mit einer Multisig-Lösung gearbeitet, wodurch die Zustimmung aller Beteiligten erforderlich ist, um das Guthaben freizugeben.

HANDELSPLÄTZE

Sollte etwas schief laufen so ist die Plattform als Mediator zu verstehen, dem von beiden Seiten die Situation geschildert wird und der entsprechend fallabhängig entscheidet. Eine saubere Dokumentation ist hierbei also wichtig. Auf der Internetplattform kann, ähnlich wie bei Bisq, ein Angebot von anderen angenommen oder ein eigenes Angebot eröffnet werden. Bevor ein Angebot angenommen und bezahlt wird, sollte man sich unbedingt über den Nutzer informieren. Dies kann über das entsprechende Profil geschehen. Anhand der Bewertungen, des Profils und der Historie kann man abschätzen, ob der Nutzer vertrauenswürdig ist. HodlHodl bietet, ähnlich wie Bisq, sehr viele Zahlungsmöglichkeiten. Während des Bezahlvorgangs wird eine Art Treuhand-Wallet erstellt, welche beide Seiten bestätigen. Der Verkäufer sendet Bitcoin an die entsprechende Wallet und der Käufer bestätigt, dass die Zahlung mit der gewählten Methode gesendet wurde. Nachdem der Verkäufer den Eingang der Zahlung bestätigt hat, wird die Bitcoin-Transaktion an die Wallet des Käufers freigegeben. Während des Vorgangs kann mit dem Handelspartner über ein Chatfenster kommuniziert werden. HodlHodl bietet auf der Webseite auch ein „Testnet" an, um den Umgang mit der Plattform zu üben. Die Dokumentation und Hilfe ist nur in englischer Sprache verfügbar.

Die letzte Alternative, die wir vorstellen möchten ist **Robosats**. Vermutlich ist sie, was die Privatsphäre angeht, am Ehesten in Betracht zu ziehen. Robosats bietet eine **Clearnet-Adresse** an, empfiehlt aber eine Verbindung über den Tor-Browser herzustellen. Dieser sollte daher vor der Benutzung heruntergeladen werden. Adressen im Tor-Browser sehen etwas anders aus als herkömmliche Internetadressen im Clearnet. Die entsprechende „Onion-Adresse" kann über die Webseite von Robosats oder über die **Github-Seite** des Projektes gefunden werden. Neben dem Tor-Browser wird weiterhin eine Lightning-fähige Wallet benötigt, da alle Transaktionen bei Robosats über das Lightning-Netzwerk abgewickelt werden. Als letztes zusätzliches Programm kann Telegram installiert werden. Durch einen Bot können hierüber Nachrichten zu den eigenen Angeboten empfangen werden, da es dazu kommen kann, dass man mit längeren Wartezeiten rechnen muss, bis der Handelspartner bspw. das Angebot annimmt, ähnlich wie bei HodlHodl. Sobald die Webseite über den Tor-Browser aufgerufen wird, generiert sie automatisch ein anonymes Profil. Das erneute Laden der Webseite führt zu einem neuen Profil und so weiter. Dies ist wichtig, da man jedes generierte Profil nur für einen Handel benutzen sollte. Die Informationen zu dem Profil können aber in Form eines Tokens, bspw. in einer geöffneten Textdatei für die Zeit des Handels zwischengespeichert werden, damit diese nicht verloren gehen sollte bspw. der Browser die Verbindung verlieren. Wir empfehlen generell die Textdatei nur zu öffnen und den Sicherheitstoken nicht zu speichern. Wenn man ganz sicher sein möchte sollte man sich den Token lieber handschriftlich notieren. Bei Robosats ist es möglich, eigene Angebote zu erstellen oder bestehende Angebote anzunehmen. Wie ehemals bei Bisq ist es notwendig einen sehr geringen Betrag in Bitcoin über das Lightning-Netzwerk „einzufrieren", um sogenanntes Spoofing (das füllen des Orderbuches mit vielen Angeboten, die nicht bedient werden sollen) zu verhindern. Der Betrag liegt zwischen 3% und 15% des Ordervolumens. Es ist daher notwendig bereits eine Wallet mit einem gewissen Betrag bereitzuhalten. Hierbei ist zu empfehlen, dass das Guthaben, welches eingefroren wird, ebenfalls bereits vorher anonymisiert wurde. Auch bei Robosats ist es möglich mit dem Handelspartner über ein Chatfenster zu kommunizieren, während die Zahlungen abgewickelt werden. Es sind sehr viele Bezahlmöglichkeiten geboten und die Webseite kann auf Deutsch eingestellt werden. Die Dokumentation und Hilfeseiten sind sehr umfangreich, bisher jedoch nur auf Englisch verfügbar.

Neben den Methoden, online anonym Bitcoin zu kaufen, gibt es selbstverständlich auch die Möglichkeit im eigenen Wohnort **Bitcoin-Meetups** zu besuchen. Mittlerweile gibt es bereits deutschlandweit organisierte und regelmäßige Meetups für Gespräche unter Gleichgesinnten. Bei einem solchen Treffen kann man erfragen, ob jemand Bitcoin verkauft. Die Bezahlung kann in Bargeld erfolgen und man kann eine Lightning-Wallet für einen schnellen Ablauf verwenden. Als positiven Nebeneffekt kann man gute Gespräche führen und vielleicht sogar ein Netzwerk aufbauen.

GEBÜHREN

In den vorherigen Ausführungen wurden bereits die Gebühren angesprochen. Vor einem Kauf sollte man sich immer mit den entsprechenden Gebühren der Handelsplattform vertraut machen, um Überraschungen zu

GEBÜHREN

vermeiden. Je nach Plattform fällt die Berechnung der Gebühren unterschiedlich aus. Meistens ist es aber ein bestimmter Prozentsatz des Handelsvolumens. Man sollte darauf achten, ob sich die Gebühren durch die Zahlungsart ändern. So ist es möglich, dass höhere Gebühren bei der Zahlung mit einer Kreditkarte anfallen. Außerdem ist es notwendig, den Mindest- und Maximalhandelsbetrag zu kennen, bevor man sich für eine Börse entscheidet. Oftmals bieten Börsen auch Anreize in Form von Verkaufsaktionen, Empfehlungen oder der Erfüllung bestimmter Bedingungen, um den Handel attraktiver zu machen. Der Kauf bei anonymen Plattformen ist meistens, wie schon angesprochen, durch ein Aufgeld auf den Wechselkurs höher. Bei der Auszahlung von der Plattform zur eigenen Wallet, fallen immer die aktuellen Netzwerkgebühren an. Wenn über das Lightning-Netzwerk gehandelt wird, sind diese allerdings aktuell nahezu nicht existent.

WALLETS - FUNKTIONSWEISE

Bei der Wahl der geeigneten Wallet muss man sich erneut überlegen, welches Ziel verfolgt wird und welche Kompromisse man bereit ist, einzugehen. Mit einer höheren Sicherheit der Wallet, geht ebenfalls eine höhere Eigenverantwortung einher. Weiterhin muss über die Schnelligkeit des Zugriffs nachgedacht werden. Möchte man also bspw. regelmäßige Zahlungen tätigen oder aber mit Bitcoin sparen. Oftmals ist auch der Wert entscheidend, der gespeichert wird. Je mehr Kapital vorhanden ist, desto mehr Eigenverantwortung kann für einige Personen gewünscht sein. Für andere Personen kann genau das Gegenteil zutreffen. Generell kann man eine Analogie zur Entscheidungshilfe hinzuziehen: Ein Fahrradschloss sollte nicht mehr als 10% des Kaufpreises des Fahrrads kosten. Ähnlich kann man es auch mit einer Wallet halten.
Nicht zu vergessen ist auch, dass man jederzeit die Möglichkeit hat, von einer Lösung zu einer anderen zu wechseln oder etwas an der Verwahrmethode zu ändern.

Doch was tun Wallets genau und warum sind sie wichtig?
Der Begriff Wallet (dt. Brieftasche) kann zu Missverständnissen führen, da man denken könnte, dass eine Wallet ein Speicherplatz für Kryptowährungen ist. Eigentlich übernimmt die Wallet jedoch die Verwaltung der privaten und öffentlichen Schlüssel („Private Keys“ und „Public Keys“) und die Generierung von Empfangsadressen. Eine Wallet speichert also keine Bitcoin, sondern die Private Keys, die es erlauben Signaturen zu erstellen, um letztendlich die Macht zu haben, Bitcoin zu versenden bzw. auszugeben. Die Private Keys müssen daher sicher bleiben, was der hauptsächliche und wichtigste Zweck einer Wallet ist. Die Private Keys werden digital versteckt und gesichert.
Die Adresse benötigt man, um Bitcoin zu **empfangen**, den privaten Schlüssel, um die Bitcoin auf der Adresse **auszugeben** und den öffentlichen Schlüssel, um zu **beweisen**, dass der private Schlüssel auch wirklich zu dieser Adresse gehört.
Der Private Key ist im ersten Stadium eine randomisierte binäre Zahlenfolge (bestehend aus 0 und 1), eine sehr große Zufallszahl. Zu dieser Zufallszahl wird eine sogenannte „Checksum“, eine Prüfsumme, hinzugefügt, welche mathematisch berechnet ist. Der Prüfsumme liegt die Zufallszahl zu Grunde. Die randomisierte Zahl besteht aus 264 binären Ziffern (24 Gruppen à 11 Ziffern), wovon die letzten 8 Ziffern die mathematische Prüfsumme darstellen. Die Prüfsumme ist da, um Fehler bei der Eingabe zu vermeiden. Wenn eine Ziffer in den zufälligen Zeichen geändert wird, ändert sich auch die Prüfsumme.
Da solch lange Zahlenfolgen für Menschen sehr schwer sind, fehlerfrei zu übertragen oder sogar auswendig zu lernen, wird diese Zahlenfolge im Anschluss in das Dezimalsystem umgerechnet. Das bedeutet, dass jede Gruppe der Zufallszahl, bestehend aus 11 Ziffern, in das Dezimalsystem übersetzt wird.

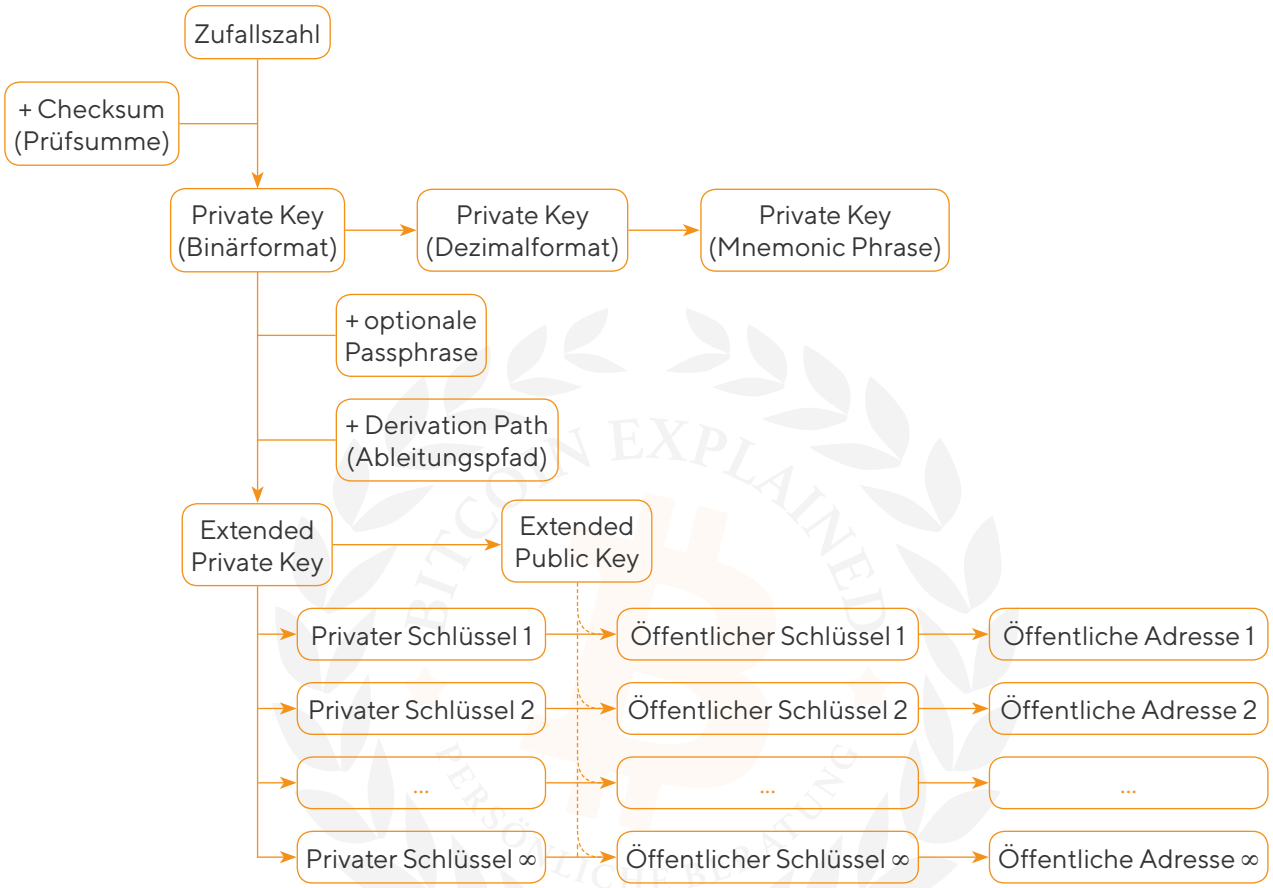
00000000000 = 0
11111111111 = 2047

Die größte Zahl, die im Dezimalsystem auf diese Art und Weise zu Stande kommen kann ist die Zahl 2047. Mit den entsprechenden Zahlen und einer in Bitcoin implementierten Wortliste (implementiert durch: Bitcoin Improvement Proposal 39, kurz: BIP 39) kann man nun den Private Key in eine Liste aus 24 Wörtern übersetzen. Diese Möglichkeit nennt sich Mnemonic- oder Seed Phrase. Diese „Seeds“ bestehen aus 12 bis 24 Wörtern, aus

WALLETS - FUNKTIONSWEISE

denen sich dann der zugehörige private Schlüssel ableiten lässt. Da diese Herleitung sehr abstrakt ist, erklären wir diese an Hand eines Schaubilds und eines Beispiels.

Die Struktur der Ableitung aus der Zufallszahl funktioniert wie folgt:



Für ein besseres Verständnis haben wir nachfolgend eine Wallet **über diese Webseite**,welche sich gut zum Üben eignet, kreiert und die entsprechenden Daten erklärt. Zuerst wird die **Zufallszahl** im Binärformat erstellt:
10110011111 11001110001 01000000001 10001010110 00001100001 11001001111 10100110001 10100100110 01010011111 01110000110 11000010010 11100001011 11111100011 10111100000 00011101001 11101110110 01101010111 01001111010 00101001000 10101000000 00010111110 11010001111 10000100100 101

Hinzu kommt die **Prüfsumme**:
11111100

Der Private Key im **Binärformat** lautet also:
10110011111 11001110001 01000000001 10001010110 00001100001 11001001111 10100110001 10100100110 01010011111 01110000110 11000010010 11100001011 11111100011 10111100000 00011101001 11101110110 01101010111 01001111010 00101001000 10101000000 00010111110 11010001111 10000100100 10111111100

Nun können die Gruppen von jeweils 11 Ziffern in das **Dezimalformat** übersetzt werden:
1439, 1649, 513, 1110, 97, 1615, 1329, 1318, 671, 902, 1554, 1803, 2019, 1504, 233, 1910, 855, 634, 328, 1344, 190, 1679, 1060, 1532

WALLETS - FUNKTIONSWEISE

Mit der weiter oben verlinkten **Wortliste** können nun die entsprechenden Wörter herausgesucht werden: die mnemonische Phrase (Seedphrase). Hierbei ist zu beachten, dass die Wortliste bei „1" anfängt, was ein Fehler ist, da sich der Binärcode „00000000000" in „0" übersetzt und nicht in „1". Der Binärcode für „1" lautet „00000000001". Das erste Wort auf der Liste ist „abandon", welches somit an Stelle „1" statt an Stelle „0" steht. Dadurch sind alle Wörter jeweils um 1 höher gekennzeichnet, als die Zahl, die sie codieren. Das erste Wort ist laut unseren Dezimalzahlen die Nummer 1439 - „record" (Binärcode: 10110011111).
Dadurch, dass die Nummer um 1 zu hoch ist, suchen wir aber eigentlich Nummer 1440 - „recycle".

Nachfolgend alle generierten Wörter:
recycle **soda** dizzy **member** around **size** plate **pill** fault **ignore** seat **thumb** wise **rose** brush **uphold** helmet **exercise** cinnamon **pool** blind **spin** loyal **sauce**

Übrigens ist die Wortliste so erstellt, dass die ersten 4 Buchstaben jedes Wortes ausreichen, um ein Wort eindeutig zu identifizieren. Auf dieser Webseite findet sich eine druckbare Version der Liste.

Die **optionale Passphrase** kann als zusätzlicher Sicherheitsfaktor hinzugefügt werden. Man kann es sich als eine Art Passwort vorstellen, welches dazu führt, dass eine von der eigentlichen mnemonischen Phrase komplett unabhängige Wallet mit eigenen privaten und öffentlichen Schlüsseln, sowie eigenen öffentlichen Adressen erzeugt wird. Je nachdem welche Passphrase verwendet wird, oder ob überhaupt eine eingegeben wird, gelangt man jedes Mal in eine andere Wallet mit eigenen Schlüsseln und Adressen. Der Ausgang und somit die einzige Gemeinsamkeit ist die mnemonische Phrase, auf welche aus kryptographischen Gründen aber nicht zurück geschlossen werden kann. Jede Wallet hat einen eigenen sog. Fingerprint, wodurch man später sehen kann, ob man beispielsweise seine Passphrase korrekt eingegeben hat oder nicht.
Wer Zugriff auf die 12 bzw. 24 Wörter (= Seedphrase oder mnemonische Phrase) hat, hat auch die Macht die entsprechenden Bitcoin zu versenden. Die Verwendung einer zusätzlichen Passphrase schafft Abhilfe, da man ohne die optionale Passphrase nicht auf das Guthaben zugreifen kann, selbst wenn die mnemonische Phrase in die falschen Hände geraten ist. Wichtig ist, dass der Umgang und die Einrichtung einer Passphrase nur mit fortgeschrittenem Wissensstand erfolgt, da ein Fehler im schlimmsten Falle zum Verlust der eigenen Bestände führen kann.

Der „**Derivation Path**" oder Ableitungspfad ist im Prinzip ein Wegweiser, da alle Schlüssel in direkter Beziehung zueinander stehen hilft dieser dabei einen Standard zu schaffen, um bspw. nach der Generierung von neuen öffentlichen Schlüsseln und somit Empfangsadressen einen Rückschluss treffen zu können, ob man das Guthaben tatsächlich ausgeben kann. Der Grund dafür, dass ein Wegweiser benötigt wird, ist der, dass man über die mnemonische Phrase theoretisch beliebig viele (öffentliche) Schlüssel und Adressen generieren kann. Um etwas ausgeben zu können muss ich aber den exakten Pfad zu der entsprechenden Adresse kennen, von der ich Guthaben ausgeben möchte. Der im BIP 44 festgelegte Standard für einen Ableitungspfad lautet: „m/44'/0'/0'/0/0".
Der Ableitungspfad wird von der genutzten Wallet festgelegt und man sollte an diesem nichts ändern, da sich sonst, wie bei der Änderung der Passphrase, der gesamte Adressstamm ändert (sichtbar am Fingerprint der Wallet). Es ist allerdings sinnvoll sich den von der Wallet genutzten Pfad zu notieren. Weitere Ausführungen zum Ableitungspfad würden an dieser Stelle zu weit führen.

Mit diesen Informationen wird dann der „**Extended Private Key**" (xPrv) errechnet. Dieser ist verantwortlich für die Produktion aller Adressen und ebenfalls verantwortlich für die Fähigkeit, Bitcoin von diesen Adressen auszugeben. Wie weiter oben im Diagramm zu sehen ist, werden von diesem Extended Private Key die weiteren Private Keys abgeleitet. Spätestens hier wird klar, warum der Ableitungspfad wichtig ist.
Eine Ableitung erfolgt immer über das folgende Schema, niemals andersherum, da es kryptografisch nahezu unmöglich ist, zurückzurechnen:

Seedphrase → Private Key → Public Key → Public Address

WALLETS - FUNKTIONSWEISE

Das Wichtigste ist, wie bereits erwähnt, der **Private Key**. Denn aus diesem lässt sich wiederum der Public Key ableiten. Bei der Erstellung einer Empfangsadresse wird der Public Key zusätzlich nochmals gehasht, wodurch sich die Public Address, die eigentliche Empfangsadresse, ergibt. Für einen potenziellen Angreifer ist es durch die Hashing-Funktion (Stichwort: Trapdoor-Funktion, siehe **Handout zu Teil I**) nahezu unmöglich die Empfangsadresse, den Hash des Public Key, in diesen zurückzurechnen und danach den Private Key abzuleiten.

Die Schlüssel bestehen aus einer langen Zeichenfolge. Der Extended Private Key für unser Beispiel lautet ausgeschrieben:
xprv9yt6aLtZpf2BrJTyUy7sHTDxoXQEbJ4ppCBMep3cGF38Jn9gbTN4UnUkzprEqfc3obDaddBC-BGmwHpFML6aToAqQWvokYRJqmf3tdsxSybR

Anhand der langen Buchstaben- und Zahlenfolge sieht man, weshalb die mnemonische Phrase (12-24 Wörter) so wichtig ist. Es ist weitaus komfortabler, sich diese Wörter zu merken, als diese lange Zeichenfolge.
Weiterhin kann an Hand des ersten Buchstabens xprv... festgestellt werden, um welche Adressform es sich handelt, bzw. welche Adressform aus diesem Schlüssel abgeleitet werden. Je nach Adressform ändert sich übrigens auch der Ableitungspfad.
Die Adressformen in Bitcoin lauten wie folgt:

xprv oder xpub	„Legacy Addressen" oder auch P2PKH (pay to public key hash)	beginnen immer mit „1"
yprv oder ypub	P2SH (pay to script hash)	beginnen immer mit „3"
zprv oder zpub	„Segwit Adressen" oder auch Bech32	beginnen immer mit „bc1q"

Sowohl der Extended Private Key als auch der „**Extended Public Key**" (xPub) starten mit dem entsprechenden Buchstaben. Wenn ein Großbuchstabe (X,Y,Z) am Anfang steht, so deutet dies darauf hin, dass es sich um eine Multisignatur-Wallet handelt.
Prinzipiell sind alle Adressformate untereinander kompatibel. Man braucht sich also keine Sorgen zu machen, mit welcher Adressform man operiert. Es ist allerdings zu sagen, dass durch die technische Struktur die „Segwit-Adressen" meistens geringere Gebühren aufweisen, wodurch diese Adressform vorherrschend ist. Je nach Börse, ist es auch möglich, dass gerade die Legacy-Adressen nicht akzeptiert werden auf Grund derselben Thematik.

Der Extended Public Key sieht dem Extended Private Key in ausgeschriebener Form sehr ähnlich:
xpub6CsSyrRTf2aV4nYSazesebAhMZEizkngBR6xTCTDpaa7BaUq8zgK2aoEr8SSk3Ach2MynrhRWKeVVa-mYaz1b3zNSxAufFr28cCpJdCang3s

Wenn man sich das Schaubild genauer ansieht, stellt man fest, dass der Besitz des Extended Public Key die Generierung derselben öffentlichen Schlüssel und somit Adressen erlaubt, wie der Extended Private Key. Der Unterschied ist jedoch, dass Ausgaben nur erfolgen können, wenn die Adressen über den Extended Private Key generiert wurden.
Das Generieren derselben Adressen mit einem xPub erlaubt es, eine sogenannte „**Watch-Only-Wallet**" einzurichten. Diese Funktion kann bspw. auf einem nicht sicheren Endgerät verwendet werden, um in der Lage zu sein über dieses Gerät das Guthaben abzurufen oder jemanden eine Adresse für eine eingehende Zahlung zu senden. Das Ausgeben von Guthaben wäre auf diese Art jedoch nicht möglich.

Die Sicherheit des xPub ist dennoch nicht zu unterschätzen, denn wer Zugriff darauf hat kann das gesamte Guthaben und alle Adressen einsehen, die verwendet werden. Dies ist demnach auch für zukünftige Adressen und Bestände zutreffend. Der xPub ist vergleichbar mit einem Kontoauszug.
Die Privatsphäre rund um das finanzielle Guthaben sollte durchaus ernst genommen und geschützt werden. Noch besser sollten die Zugänge zu den Finanzen (Private Keys) geschützt werden. Weitere Hinweise dazu im nächsten Abschnitt.

WALLETS - SICHERHEIT

Die Seed-Phrase, also der in 12 bzw. 24 übersetzte Private Key, ist immens wichtig. Es kann nicht oft genug betont werden, dass dieser sicher verwahrt werden muss und mit äußerster Vorsicht behandelt werden sollte. Wenn diese Informationen verloren gehen oder in falsche Hände geraten bedeutet dies, dass das Guthaben auf ewig verloren ist!

Bitcoin hat keinen Kundenservice oder Ansprechpartner, welcher Transaktionen rückgängig machen kann oder die eigenen Keys ebenfalls gespeichert hat. Bitcoin bedeutet Eigenverantwortung!

Dies zu verstehen ist absolut essenziell. Einige der folgenden Maßnahmen mögen auf den ersten Blick sehr radikal wirken, allerdings kann mit einem Fehler oder dem Vertrauen in die falsche Person das gesamte Guthaben gefährdet oder sogar unwiederbringlich verloren sein. Daher möchten wir für gewisse Dinge sensibilisieren.
Es ist immer ratsam, eine Kopie der Wörter in sicherer Verwahrung zu haben. Die Informationen sollten niemals auf einem Endgerät gespeichert werden, welches eine Verbindung zum Internet hat. Stattdessen kann man die Verwahrung auf Papier oder eine Gravur in Metall in Betracht ziehen. Ebenfalls kann man die Wörter in einem Buch chiffrieren oder sie können sich als „Brain-Wallet" (Gehirn-Wallet) gemerkt werden. Das Merken der Wörter birgt aber natürlich auch hohe Risiken. Aber generell kann auf diese Arten verhindert werden, dass die Information einem Hacker in die Hände fallen. Wichtig ist auch das Backup der Wörter durch eine Test-Transaktion zu überprüfen, um sicherzustellen, dass kein Fehler vorliegt (bspw. vertauschte Wörter).
Egal wie sicher man sich mit einem Virenschutz auf dem Computer fühlt, sollten die Private Keys niemals auch nur an einem mit dem Internet verbundenen Computer eingegeben oder erstellt werden.

Weiterhin muss man immer achtsam sein, was Versuche von Betrügern angeht, Zugang zu den Keys zu bekommen. Mehr Informationen zum Erkennen von betrügerischen Aktivitäten finden sich auf unserer Webseite im Artikel zum Thema Sicherheit. Generell gilt, dass egal wer fragt, die Keys nicht herausgegeben werden. Man sollte sich selbst überlegen, ob man sie mit einem Familienmitglied teilt, oder lieber eine Anleitung anlegt, welche den Zugang im Todesfall erklärt.

Bei der Erstellung einer Wallet sollte ebenfalls darauf geachtet werden, dass niemand den Vorgang einsehen, abhören oder auf andere Art beobachten kann. Eine Wallet kann theoretisch durch das Werfen von Würfeln erstellt werden, indem bspw. jeweils drei Seiten des Würfels entweder eine „0" oder „1" als Codierung zugeteilt werden. Die entsprechenden Würfe werden dann in einen Binärcode übersetzt und später wird, wie oben beschrieben, die mnemonische Phrase daraus erstellt. In unserem Leitfaden zum Erstellen einer Wallet durch Würfeln gehen wir auf die Methodik des Würfelns in Verbindung mit einer Hardware-Wallet ein. Hierbei empfiehlt es sich die Wallet alleine einzurichten, eventuell darauf zu achten, dass man nicht vor einem Fenster sitzt und bei der Einrichtung kein Handy, Tablet oder Laptop in der Nähe hat. Die Erstellung kann aber auch randomisiert durch eine Hardware-Wallet erfolgen.

Im Allgemeinen sollte man nie darüber sprechen, wie viel Bitcoin man besitzt oder, dass man Bitcoin besitzt. Außerdem können Mittel und Wege in Betracht bezogen werden, das eigene Guthaben zu anonymisieren, um sich bspw. staatlichen/räuberischen Übergriffen auf das eigene Vermögen gegenüber abzusichern.

Es ist wichtig, sich mit den getroffenen Maßnahmen wohl zu fühlen. Verbesserungen sind auch im Nachhinein meist noch möglich. Vorsicht ist immer geboten.
Im nächsten Abschnitt stellen wir verschiedene Wallet-Arten vor und beleuchten die Unterschiede und worauf man bei der Auswahl achten sollte.

WALLET-ARTEN

Grundlegend unterscheidet man zwischen Hot- und Cold-Wallets und Custodial bzw. Non-Custodial-Wallets. Weiterhin wird danach zwischen Software- und Hardware-Wallets differenziert.

WALLET-ARTEN

Wir beginnen mit dem Unterschied „Hot" und „Cold"-Wallets:

Hot-Wallets = dauerhafte Internetverbindung vorausgesetzt
Cold-Wallets = benötigen keine Verbindung zum Internet

Hot-Wallets werden bspw. bei Handelsplattformen, wie bitcoin.de oder Kraken im eigenen Nutzerkonto verwendet. Zum Senden und Empfangen ist bei den Börsen meistens eine Hot-Wallet verknüpft, da diese einfach einzurichten sind, meistens eine bessere Nutzerfreundlichkeit bieten und das Guthaben schneller zugänglich ist. Generell besteht bei Hot-Wallets allerdings die Gefahr, dass Hacker Zugang zu den Private Keys erhalten.
Cold-Wallets hingegen benötigen keine Verbindung zum Internet. Es wird stattdessen ein physisches Medium benutzt, um die Private Keys sicher offline verwahren zu können. Dazu gehören bspw. Hardware-Wallets. Dazu später mehr.

Die weitere wichtige Kategorisierung ist zwischen „Custodial" und „Non-Custodial". Custodial ist der englische Begriff für „Obhut" oder „Vormundschaft" und im Zusammenhang mit Wallets wird er benutzt, um zu beschreiben, wer die Wallet verwaltet und Zugriff auf die Private Keys hat.

Custodial = eine dritte Partei sichert die Private Keys
Non-Custodial = die Private Keys sind im eigenen Besitz und ermöglichen volle Kontrolle & Eigentum

Für **Custodial-Wallets** kann ebenfalls wieder das Beispiel eines Handelsplatzes genutzt werden. Die Plattform sichert das Guthaben für einen selbst ab. Sollte die Plattform allerdings Schwachstellen haben und ein Hacker kann sich Zugang verschaffen dann ist es für diesen leicht die Private Keys zu stehlen.
Non-Custodial-Wallets hingegen werden von einem selbst verwaltet. Dies kann auch bei Börsen funktionieren, indem man selbst die Private Keys hält, die Börse ebenso. Dies wird dann als 2/2-Multisig bezeichnet, da man selbst die volle Kontrolle hat aber zum Ausgeben/Versenden trotzdem den zweiten Key der Börse benötigt. Dadurch, dass man selbst den Private Key hält kann man jederzeit seine Wallet wiederherstellen und bei einer Multisig-Lösung werden beide Keys benötigt, um das Guthaben zu versenden.

Custodial-Lösungen nehmen einem viel Arbeit und Verständnis ab. Sie haben den Vorteil, dass man die Private Keys nicht verlieren kann oder einen Fehler bei Handhabung der Wallet machen kann. Sie haben aber den oben beschriebenen Nachteil, dass durch einen Hack das Guthaben verloren ist. Weiterhin ist es denkbar, dass eine Plattform in betrügerischer Absicht handelt und man dieser in dem Szenario ausgeliefert ist. Außerdem ist die tatsächliche Liquidität der Plattform schwer nachprüfbar. Sollte es also zu einer Art Bank-Run auf die Plattform kommen, ist es möglich, dass mehr ausgegeben wurde als die Plattform tatsächlich hält (ähnlich wie im Fractional Reserve Banking). Theoretisch hält eine Plattform nichts davon ab, mehr Bitcoin auf den Konten der Kunden auszuschreiben, als tatsächlich vorhanden sind. Sogenannte „Paper-Bitcoin" könnten zu einem Problem werden, da in einem Szenario in dem viele Kunden ihr Guthaben von der Plattform abziehen möchten, eventuell gar nicht ausgezahlt werden können. Mit der Custodial-Lösung kommt gleichzeitig wieder das „Oracle-Problem" zu tragen und somit ist immer ein massiver Vertrauensvorschuss vorausgesetzt.

Um sich über den Besitz sicher zu sein, muss man daher die Verantwortung über die Schlüssel übernehmen. „Not your keys, not your coins" – „Nicht deine Schlüssel, nicht deine Bitcoin" ist ein berühmter Leitspruch in der Szene. Das Vertrauen in eine zentrale Partei beim Nutzen einer Custodial-Lösung entspricht auch nicht der eigentlichen Grundidee von Bitcoin, seine eigene Bank zu sein.
Non-Custodial-Lösungen setzen selbstverständlich mehr Eigenverantwortung voraus, denn wenn die Keys verloren gehen, sie nicht korrekt aufbewahrt, aufgeschrieben oder erstellt werden, kann das Guthaben von niemanden wiederhergestellt werden. Allerdings kann bei korrekter Handhabung auch niemand anderes auf das Guthaben zugreifen. Zugegebenermaßen ist es eine Grundsatzdiskussion und eine sehr individuelle Entscheidung. Wir empfehlen allerdings immer die Private Keys selbst zu halten und sie nicht aus der Hand zu geben.

WALLET-ARTEN

Hot-Wallets sind in den meisten Fällen sogenannte **Software-Wallets**. Diese können wiederum als Web-Variante, als Desktop-Wallet oder in einer mobilen Version installiert und genutzt werden. Ein Internetzugang ist, wie oben beschrieben, für den vollen Funktionsumfang unerlässlich.

Web-Wallets
Diese Art Wallet ist direkt in die Browseroberfläche integriert und in den meisten Fällen wird direkt im Browser über ein Plug-In eine neue Wallet mit einem Passwort angelegt. Einige Anbieter speichern allerdings auch den eigenen Private Key, haben also Zugang zum eigenen Guthaben.

Desktop-Wallets
Eine Desktop-Wallet ist eine Software, welche auf dem eigenen Computer als ausführendes Programm installiert wird. Da das Programm lokal ausgeführt wird, ist zu beachten, dass bei der Erstellung einer Wallet immer eine Datei (z. B. mit dem Namen „wallet.dat“) auf deinem Computer gespeichert wird. Diese Datei enthält den Private Key. Es ist daher sinnvoll diese Datei nochmals zusätzlich mit einem Passwort zu sichern oder anderweitig zu verschlüsseln. Bekannte Desktop-Wallets sind Exodus, Electrum, Sparrow, Specter und Wasabi

Mobile-Wallets
Über diese Art von Wallet kann das eigene Smartphone schnell Bitcoin empfangen und senden. Auch bei diesem Typ Wallet ist es ratsam, sie, wenn möglich, mit einem Passwort abzusichern, weil andernfalls der Private Key ungeschützt auf dem Smartphone gespeichert ist. Grundsätzlich gilt diese Art Wallet als sehr unsicher und man sollte als Faustregel darüber nachdenken, nur so viel Guthaben hier zu verwalten, wie man bspw. Bargeld im Portemonnaie bei sich tragen würde. Bekannte Mobile-Wallets sind: Wallet of Satoshi, BlueWallet, Samourai, Zeus, Muun und Breez

Cold-Wallets sind in den meisten Fällen sogenannte **Hardware-Wallets**. Dies sind physische Geräte, welche entweder selbstständig offline einen Private Key über eine Zufallszahl erzeugen oder einen eigenständig erzeugten Private Key speichern. Dabei verlässt der Private Key niemals das Gerät, weshalb das Guthaben dort drauf als sehr sicher betrachtet werden kann. Dies gilt sogar, wenn man das Gerät an einen kompromittierten Computer anschließt. Die Verbindung erfolgt in der Regel über ein USB-Kabel oder auch über sogenannte „Partially Signed Bitcoin Transactions“. Bei dieser Art der Transaktion wird die gewünschte Summe, die Empfangsadresse und die Netzwerkgebühr auf einem Computer voreingestellt und danach als Datei exportiert. Diese exportierte Datei wird dann mittels einer SD-Karte in der Hardware-Wallet geladen und durch den Private Key auf dem Gerät signiert. Danach wird die signierte Transaktion mittels der SD-Karte wieder über den Computer im Netzwerk bekannt gegeben. Generell sind Hardware-Wallets nie direkt mit dem Internet verbunden und somit eine der sichersten Methoden, einen Private Key zu sichern. Sie bieten eine technisch vereinfachte und haptische Lösung, um auf die eigene Wallet zuzugreifen und Transaktionen mittels des eigenen Private Key zu signieren, man könnte die Geräte daher auch als **Signiergeräte** bezeichnen. Beim Kauf eines solchen Gerätes ist darauf zu achten diese direkt vom Hersteller zu beziehen und nicht über einen Reseller, wie Amazon, Ebay etc., da sonst die Gefahr besteht, dass das Gerät manipuliert wurde.
Bei der Bestellung ist in Betracht zu ziehen, ob man das gerät an ein Postfach schicken lässt und somit anonym bleibt oder zumindest im Nachhinein die Daten bei dem Unternehmen löschen lässt. Wenn das Paket ankommt sollte man überprüfen, ob von außen erkennbar ist, dass eine Hardware-Wallet verschickt wurde. Sollte dies erkennbar sein, dann weiß theoretisch die gesamte Lieferkette, dass man sich ein solches Produkt bestellt hat und wo man wohnt. Dies ist aus Gründen der Privatsphäre inakzeptabel. Weiterhin sollte man sich vergewissern, dass keine Fremdeinwirkung stattgefunden hat. Die meisten Hersteller haben auf ihren Webseiten genaue Anweisungen auf was zu achten ist, wenn das Gerät ausgepackt wird. Viele Hersteller verschicken ihre Geräte bspw. in manipulationssicheren Sicherheitstaschen. Den Anweisungen des Herstellers zur Inspektion des Gerätes und zum öffnen des Paketes, sollte Folge geleistet werden, da hierbei eine mögliche Fremdeinwirkung ausgeschlossen werden kann.
Bekannte Hardware-Wallets sind: BitBox02, Ledger, Trezor, ColdCard, SeedSigner, Keystone, Jade

WALLETS - FAZIT

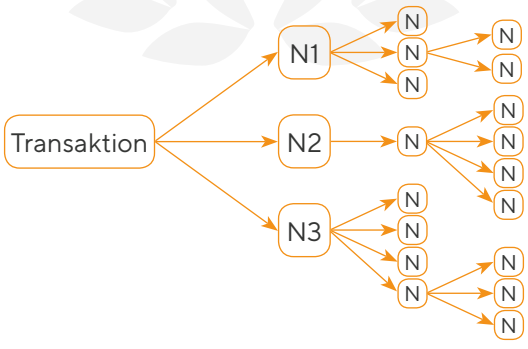
Wie in den vorangegangenen Abschnitten beschrieben gibt es verschiedene Arten von Wallets und somit auch keine Universal-Lösung. Grundsätzlich würden wir empfehlen, die Kontrolle über die eigenen Keys zu übernehmen und sich am besten eine Hardware-Wallet zuzulegen. Dadurch ist man auf der sicheren Seite, vor allem langfristig.

Allerdings hängt die Wahl der Wallet auch wieder davon ab, welche Pläne man verfolgt und welche Funktionen einem wichtig sind. Unterschiedliche Wallets bieten auch unterschiedliche Services, wie Multisig, Einrichtung einer Passphrase, Unterstützung von Legacy-Adressen, die Möglichkeit zum Coinjoin oder auch Lightning-Unterstützung.
Bei kleineren Beträgen oder kurzfristigen Anlagen könnte man auf Grund der einfacheren Einrichtung und als kostenlose Wallet-Alternative auch eine Hot-Wallet benutzen oder vorerst das Guthaben bei der Börse belassen.

FUNKTIONSWEISE EINER TRANSAKTION

In diesem Kapitel gehen wir auf die Funktionsweise einer Bitcoin-Transaktion ein und erklären, welche Rolle eine Wallet darin spielt. Wir setzen für dieses Kapitel ein Grundverständnis voraus, welches bereits in unserem „Teil 1 - Basiswissen“ vermittelt wurde.

Eine Transaktion wird aus folgenden Bestandteilen von der Wallet konstruiert: Sendeadresse, Empfangsadresse, Betrag und Signatur. Die Transaktion kann aus akkumulierten Beständen zusammengesetzt werden. Darauf gehen wir später genauer ein. Wenn die Transaktion (durch den Private Key) signiert ist, wird sie von der eigenen Wallet zu anderen Netzwerk-Knotenpunkten (Nodes) übermittelt, welche mit dem eigenen Knotenpunkt, in diesem Fall der Wallet, verbunden sind. Die Nodes können andere Wallets, Mining-Nodes und auch Full-Nodes von Handelsplätzen, Unternehmen oder Privatpersonen sein. Sobald eine Transaktion bei einer Node eingeht wird diese validiert. Das bedeutet, dass geprüft wird, ob alle Parameter stimmen. Es wird also unter anderem geprüft, ob die Netzwerkgebühr hoch genug ist, ob die Beträge stimmen oder versucht wird einen bestimmten Betrag doppelt auszugeben, ob die Größe der Transaktion korrekt ist, ob das korrekte Skript für die Transaktion verwendet wurde und ob die Signatur valide ist. Nach diesem Schritt wird die Transaktion von diesen Nodes entsprechend wiederum weitergeleitet. Dieser Vorgang passiert so lange, bis das gesamte Netzwerk über die Transaktion informiert wurde, geschieht aber innerhalb weniger Augenblicke.
Aus dem Grund, dass jede Transaktion über diesen Weg übermittelt wird, ist es für einen Teilnehmer unmöglich zu sagen, von welchem Knotenpunkt die Transaktion ausgelöst wurde.



Ähnlich, wie in dem Schaubild, wird die Transaktion also validiert und dann von Node zu Node weitergeleitet. Jede Node hat eine Ansammlung von Transaktionen, welche validiert aber unbestätigt sind. Diese Ansammlung nennt man Mempool. Der Mempool ist also ebenfalls über alle Nodes verteilt, da alle Nodes ja über jede Transaktionen informiert werden. Es kann trotzdem sein, dass der Mempool unterschiedlicher Nodes nicht zu 100% identisch ist. Gründe hierfür sind Unterschiede in der Verteilung über die Nodes oder die zeitliche Ab-

FUNKTIONSWEISE EINER TRANSAKTION

folge zu der eine Transaktion empfangen wird. Davon abgesehen ist die Synchronität über alle Nodes zu ca. 99% sichergestellt. Es wäre also denkbar, dass einige Transaktionen in einer anderen Reihenfolge bei einigen Mempools vorhanden sind. Dies ist aber nicht weiter schlimm, da es erstmal nur wichtig ist, dass sie empfangen werden.

Mining-Nodes spielen eine wichtige Rolle, da sie die Transaktionen aus dem Mempool bestätigen. Betrachten wir nun den Ablauf aus Sicht einer dieser Mining-Nodes und beleuchten das Szenario, in dem gerade ein neuer Block errechnet und der Blockchain hinzugefügt wurde. Für die Miner bedeutet dies, dass nun der Wettbewerb um die nächste Blockbelohnung von Neuem beginnt. Um die Belohnung zu erhalten muss der Proof-of-Work für den Block errechnet werden. Die Miner beginnen mit einem leeren Block, welcher die Verlinkung über den Hash des vorangegangenen Blocks und einige weitere Informationen enthält. Die erste Transaktion, die hinzugefügt wird ist die sogenannte Coinbase-Transaktion, welche den Miner selbst bezahlt. Sie enthält entsprechend die Empfangsadresse des Miners. Bisher ist der Block allerdings noch nicht valide, da der Proof-of-Work noch fehlt. Ebenso fehlen Transaktionen, welche aus dem Mempool gewählt werden. Die Transaktionen mit den höchsten angehangenen Netzwerkgebühren werden als erste ausgewählt, um den Profit der Miner zu maximieren. Der Block wird als „Candidate Block" bezeichnet, da dieser noch nicht bestätigt ist. Erst wenn durch die Arbeitsleistung und nach dem Generieren von Milliarden an Hashes eine gültige Nonce gefunden wird, kann der Miner dem Netzwerk mitteilen, dass er einen gültigen Block gefunden hat. Dies geschieht über denselben Weg, über den eine neue Transaktion im Netzwerk bekannt gegeben wird. Der Miner propagiert die Nachricht zu allen Nodes mit denen er verbunden ist, welche die Nachricht wieder weitertragen bis das gesamte Netzwerk die Nachricht empfangen hat. Alle Miner, die diesen Block empfangen, überprüfen und validieren diesen Block so schnell sie können und starten dann mit dem Proof-of-Work wieder von vorne mit dem gerade validierten Block als Ausgangsposition. Alle anderen Nodes empfangen den neuen Block ebenfalls und gleichen die Transaktionen innerhalb des Blockes mit dem eigenen Mempool ab. Jede Transaktion, welche in den Block aufgenommen wurde, wird also aus dem Mempool gelöscht und als bestätigt angesehen. Dieser Prozess passiert natürlich auch bei der eigenen Wallet, was wiederum bedeutet, dass die Wallet nun weiß, dass die gesendete Transaktion eine Bestätigung auf der Blockchain hat. Durchschnittlich 10 Minuten später hat sich der Prozess mit einem neuen Block wiederholt und dieselbe von uns ausgelöste Transaktion hat nun bereits zwei Bestätigungen und so weiter.

Sobald nun also jede Node entsprechend kommuniziert hat, können die Bestände des Absenders und des Handelspartners als Empfänger aktualisiert werden. In diesem Video wird die Thematik beispielhaft erklärt.

Mittlerweile gibt es für die Einsicht der Transaktionen auf der Blockchain bereits visuell ansprechende Tools, sogenannte Blockchain-Explorer. Eine dieser Webseiten auf denen man Transaktionen nachverfolgen, Bestände von Wallets einsehen und bspw. Gebühren prüfen kann ist mempool.space.
Diese Webseiten machen es einfach, das vorher beschriebene darzustellen.

Auf der Webseite sieht man Linkerhand oben die unbestätigten Transaktionen, den Mempool und auf der rechten Seite die letzten gefundenen Blöcke mit der entsprechenden Blockhöhe (fortlaufende Nummerierung der einzelnen Blöcke), den Informationen wann sie gefunden wurden, wie viele Transaktionen sie beinhalten und auch welche Netzwerkgebühr durchschnittlich gezahlt wurde.

FUNKTIONSWEISE EINER TRANSAKTION

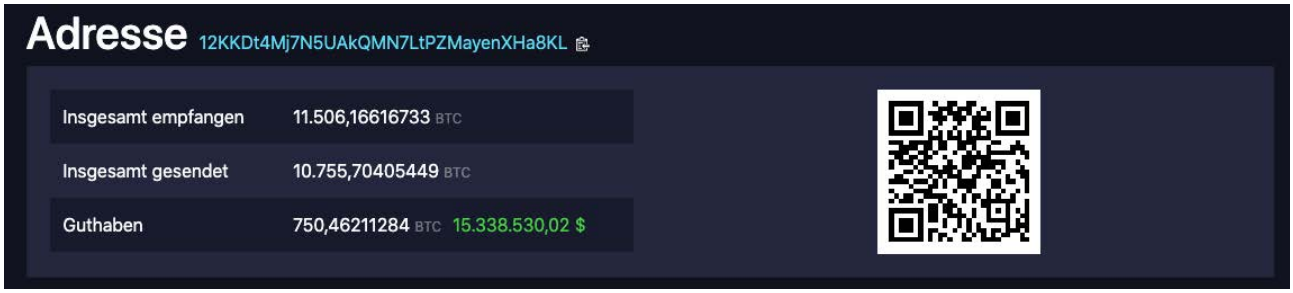
So kann man einzelne Blöcke anklicken und sieht die Zusammensetzung, welcher Miner den Block gefunden hat, wie viele Gebühren akkumuliert ausbezahlt wurden und einige weitere Informationen.

Die Visualisierung auf der rechten Seite verdeutlicht, welche Transaktionen mehr Speicherplatz benötigen und welche weniger. Eine Transaktion benötigt mehr Speicherplatz wenn es mehr Inputs und Outputs gibt, es eine sog. Multisig-Transaktion ist oder ein älteres Adressformat benutzt wird. Größere Transaktionen (virtuelle Größe gemessen in vB, also „Virtual Bytes") zahlen insgesamt mehr Gebühren, da die Blockgröße begrenzt ist. Die Färbung der Quadrate zeigt die anteilige Höhe der Gebühren (in sat/vB) an. Rote Quadrate haben anteilig Gebühren weit über dem Median gezahlt. Ganz links unten in der Ecke ist immer ein tiefgrünes Quadrat, welches die Coinbase-Transaktion zeigt. Wenn man mit der Maus über die Quadrate fährt werden einem weitere Informationen zur Transaktion angezeigt, mit einem Klick kommt man zur Übersichtsseite der entsprechenden Transaktion. Wichtig ist der Hash des Blocks, welcher oben links angezeigt wird. Dieser ist für jeden Block individuell und somit kann ein bestimmter Block immer wiedergefunden werden.

Weiter unten auf der Webseite findet man die Liste mit allen Transaktionen (in diesem Block sind es insgesamt 3.101 Transaktionen), angefangen bei der Coinbase-Transaktion. Diese zeigt also die Adresse des Miners, der den Block gefunden hat. Im Jahr 2022 gibt es für jeden gefundenen Block eine Belohnung von 6,25 Bitcoin und zusätzlich die im Block enthaltenen Gebühren, wodurch der Wert von ~6,4 Bitcoin zu Stande kommt.

FUNKTIONSWEISE EINER TRANSAKTION

Nun kann man sich ebenfalls die Adresse in der Einzelübersicht ansehen, indem man den Link anklickt. So kann

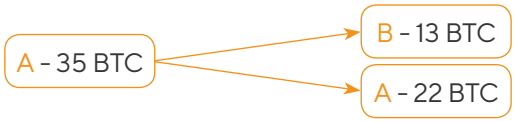


man alle getätigten Transaktionen nachvollziehen, in die diese Adresse, seit Erstellung, involviert war.
Diese Adresse stammt von einem großen sogenannten Mining-Pool (Zusammenschluss von Minern) und hat dementsprechend schon viele Transaktionen getätigt und ein hohes Guthaben angesammelt. Alle Transaktionen dieser speziellen Adresse werden darunter wieder in Listenform dargestellt.
Zurück in der Block-Übersicht kann man auch jede herkömmliche Transaktion einsehen. So beinhaltet Block Nummer 761143 bspw. folgende Transaktion:

Oben sieht man wieder einen Hash, welcher diesmal die einzelne Transaktion eindeutig kennzeichnet. Weiterhin sieht man auf der linken Seite die Adresse, von der die Transaktion gestartet wurde und auf der rechten Seite die Adresse der Gegenpartei und einen Wert, welcher sich „**Unspent Transaction Output**“ (kurz UTXO) nennt. Weiterhin sieht man die Gebühr und an Hand der Farbe der Pfeile kann man erkennen, ob sich ein Guthaben auf den jeweiligen Adressen befindet. Rot ist ein Indikator, dass kein Guthaben vorhanden ist und grün bedeutet, dass die Adresse ein positives Guthaben aufweist.

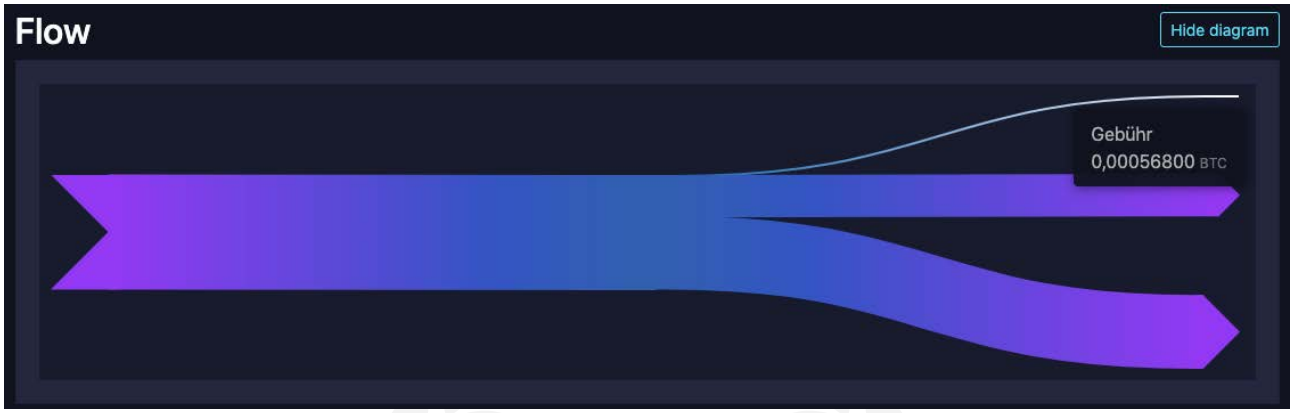
Doch was ist ein UTXO?

Dieser technische Terminus ist besonders am Anfang verwirrend, beschreibt jedoch einen logischen Vorgang. Um das Konzept besser zu verstehen hilft es sich Bitcoin für den Moment als tatsächlich physisch trennbare Einheit vorzustellen. Wie bspw. ein Goldbarren mit einem bestimmten Gewicht. Wenn man bei dem Beispiel der obigen Transaktion bleiben möchte, so kann man also sagen, dass der Sender „A“ einen Goldbarren von, der Einfachheit halber, 35g besitzt. Nun möchte A einen Teil von 13g an den Empfänger „B“ als Zahlung für eine Leistung oder Ware übergeben bzw. übersenden. Physisches Gold müsste man nun einschmelzen und aufteilen. Zum einen in einen 13g-Barren und einen 22g-Barren. Der erste Barren wird als Bezahlung benutzt und der zweite bleibt weiterhin im Besitz von A.
Bei Bitcoin ist es ähnlich. Wenn man 35 Bitcoin empfängt ist dies ein einzelner UTXO. Wenn man diese Summe ausgeben möchte „schmilzt“ man den gesamten Betrag zuerst ein und kann ihn danach durch eine Transaktion beliebig aufteilen. Das heißt man kann eine beliebige Summe an beliebig viele Adressen senden. Man kann es im Bezug auf die eigene Adresse also als eine Art „Wechselgeld“ betrachten. Es gibt also einen Input und zwei Outputs. Für das Beispiel oben sieht das vereinfachte Schaubild daher folgendermaßen aus:

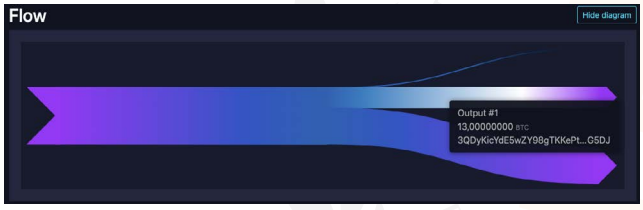


FUNKTIONSWEISE EINER TRANSAKTION

Nun können A und B noch die entsprechenden Empfangsadressen zugeordnet werden und es entsteht ein ähnliches Bild, wie im Blockchain-Explorer.
Auf der Webseite kann nach anklicken des Hashes einer Transaktion auch nochmal eine bessere Übersicht in Form eines Flow-Diagrammes finden.



Der erste Geldfluss zeigt die Gebühr, der zweite zeigt den ersten Output an B und der dritte den zweiten Output an den Sender A und somit an eine neue Adresse seiner eigenen Wallet.



UTXOs beschreiben immer ein Guthaben der eigenen Wallet. Wie oben beschrieben können theoretisch von jeder Zufallszahl, bzw. von jedem Extended Private Key unendlich viele Public Adresses abgeleitet werden. Im Normalfall wird bei jeder Interaktion einer Wallet, sprich bei jedem Empfang von Guthaben, auch eine neue Empfangsadresse erstellt. All diese Empfangsadressen mit Beträgen durch Empfangen von Guthaben oder dem Kauf von Bitcoin stellen letztendlich das Gesamtguthaben dar.
So könnte es also sein, dass das Gesamtguthaben 2 Bitcoin beträgt, aber auch 4 unterschiedliche UTXOs aufgeteilt ist:

- 0,2 BTC
- 0,6 BTC
- 1,1 BTC
- 0,1 BTC

Nun sollen 1,3 BTC an eine andere Person gesendet werden. Die Wallet würde nun also die passenden UTXOs mit den entsprechenden Empfangsadressen heraussuchen und die Transaktion signieren. Es wäre möglich die 1,1 BTC und die 0,2 BTC zu versenden aber es wäre genau so möglich, dass 1,1 BTC und 0,6 BTC zusammengefasst und dann wieder 0,4 BTC auf eine neue Public Address der eigenen Wallet gutgeschrieben werden.
Sollte dies der Fall sein würde das Gesamtguthaben 0,7 BTC betragen und sich folgendermaßen verteilen:

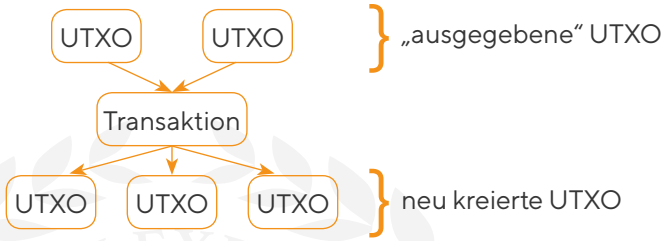
- 0,2 BTC
- 0,4 BTC
- 0,1 BTC

Die beiden UTXOs mit 0,1 BTC und 0,2 BTC würden in diesem Beispiel völlig unberührt bleiben. Die Zahlung hätte wieder zwei Outputs: 1,3 BTC als Zahlung und 0,4 BTC als „Wechselgeld".
In diesem Beispiel wurden die Netzwerkgebühren bewusst nicht beachtet.

FUNKTIONSWEISE EINER TRANSAKTION

Einige Wallets bieten sogenanntes „UTXO-Management“ an. Dies kann sinnvoll sein, wenn man sich sicher sein möchte, welche einzelnen Guthaben wo herkommen und wo sie hingehen. Dies kann man dann entsprechend als Notiz kennzeichnen. Vor allem in Hinblick auf die Privatsphäre ist dies ein nützliches Werkzeug, um bspw. zu wissen welcher Betrag von einer Handelsplattform kommt und welcher bspw. durch einen Coinjoin anonymisiert wurde.

Der eigene Bitcoin-Bestand besteht tatsächlich aus (mehreren) UTXOs, welche durch den Private Key nutzbar gemacht werden können. Jeder UTXO verweist auf den Herkunftspfad, welcher hierarchisch in der Blockchain abgebildet und gespeichert ist. Sobald ein UTXO benutzt wird, gilt dieser als „ausgegeben“ und es werden entsprechend neue UTXO an dieser Stelle erstellt.



Eine Transaktion kann man sich daher als eine abstrakte „Aktion“ vorstellen, die das Freischalten früherer UTXOs und gleichzeitig das Erzeugen neuer UTXOs definiert. Die Summe aller „freigeschalteten“ UTXOs wird immer gleich sein mit der Summe der neu kreierten UTXOs, wodurch die zirkulierende Summe an Bitcoin immer konstant bleiben wird. Weiterhin kann dadurch jeder einzelne Satoshi auf der Blockchain auch bis zu seinem Ursprung, der Coinbase-Transaktion, zurückverfolgt werden.
Die Historie aller UTXOs nennt sich auch das „UTXO-Set“ oder „Chainstate“. Diese Historie wird immer von den einzelnen Nodes im Netzwerk auf dem neuesten Stand gehalten. Die Chainstate-Datei aktualisiert sich immer, wenn ein neuer Block im Netzwerk akzeptiert wird. Die Liste der letzten Transaktionen in dem neuesten Block definiert welche UTXOs als „ausgegeben“ gekennzeichnet werden und welche neu kreiert wurden. Jede Full-Node im Netzwerk wird immer exakt dieselbe Kopie der Chainstate im lokalen Speicher haben. Technisch gesehen bedeutet dies, dass jeder alle UTXOs und deren Historie in dieser Datei hat. Ohne den entsprechenden Private Key ist es aber unmöglich, diese nutzbar zu machen.
Da das Konzept ziemlich abstrakt ist, finden sich hier die wichtigsten Stichpunkte:

- UTXOs sind verschlüsselte Bitcoin-Beträge
- mit dem richtigen Private Key können diese Beträge genutzt werden
- wenn eine Transaktion durchgeführt wird, werden einige UTXOs „konsumiert“ und neue kreiert
- UTXO werden immer im Ganzen konsumiert und das „Wechselgeld“ wird automatisch der eigenen Wallet gutgeschrieben
- jeder UTXO kann eine Public Address (öffentliche Adresse) zugeordnet werden
- der Private Key zu einer UTXO ist immer sicher zu verwahren - **Not your Keys, not your Coins**

Zusammenfassend hat also jede Transaktion sogenannte Inputs (das Guthaben, welches versendet wird) und Outputs (die neue Verteilung der Summen). Wie beschrieben, bleibt die Anzahl der Satoshis gleich, aber die Verteilung ändert sich auf den involvierten Empfangsadressen. Nach Bestätigung einer Transaktion stehen die versendeten Inputs dem Empfänger selbst wieder als UTXO und somit als Input für seine nächste Transaktion zur Verfügung.

ZUSAMMENFASSUNG/VERGLEICH

Kaufmethode
Die Kaufmethode ist stark von der eigenen Risikobereitschaft und eventuell Liquidität abhängig. Grundsätzlich erachten wir regelmäßige Käufe als sinnvoll, da somit der durchschnittliche Kaufpreis niedrig bleibt und man auf langfristige Sicht mehr Satoshis für weniger Euro einkaufen kann. Das Ziel ist es die eigene Ansammlung von Satoshi zu vergrößern.

Handelsplattform
Bei der Wahl der richtigen Plattform für den Kauf sind im Prinzip zwei Fragen entscheidend:

- Wie wichtig ist mir meine Privatsphäre
- Möchte ich manuell kaufen oder einen regelmäßigen Sparplan einrichten?

Je nachdem, wie man sich diese Fragen beantwortet kann man viele Plattformen ausschließen oder muss eventuell überlegen, welche Antwort Priorität hat und dann einen Kompromiss eingehen.

Plattform	Auto-DCA	Non-Custodial	Anonymität	Gebühr	Zahlungsmethode
bitcoin.de	✗	✗	--	0,3% - 0,5%	SEPA & Sofortüberweisungen
Kraken	✗	✗	--	1,5% - 5,25%	SEPA, Kredit-/Debitkarte, Apple & Google Pay
Relai	✓	✓	-	< 2,5%	SEPA, Kredit-/Debitkarte, Apple & Google Pay
Pocket	✓	✓	-	1,5%	SEPA & Sofortüberweisungen
Bisq	✗	✓	+	0,7% + höherer Marktpreis	SEPA, Online-Banken, Bargeld u.a.
HodlHodl	✗	✓	+	0,3% + höherer Marktpreis	SEPA, Online-Banken, Gutscheinkarten u.a.
Robosats	✗	✓	++	0,175% + höherer Marktpreis	SEPA, Online-Banken, Gutscheinkarten u.a.
in Person	✗	✓	++	individuell	individuell

Viel wichtiger, als die Auswahl der Handelsplattform, ist die Wahl der Wallet, welche später genutzt werden soll. „Wie verwahre ich meine Keys?" sollte die essenzielle Frage für jeden sein, der Bitcoin kauft.

Wallet
Die Wahl der Wallet und vor allem das Verwahren des Backups sind Themen, mit denen sich jeder Bitcoiner beschäftigen muss. Man kann nicht auf alle Eventualitäten vorbereitet sein und es gibt mit jedem Setup Verbesserungspotenzial, Besonders, da ständig neue Möglichkeiten auf dem Markt angeboten werden. Man sollte also ein Setup finden, mit dem man sich selbst wohl fühlt.
Wir sind der Überzeugung, dass eine Hardware-Wallet und ein Backup der mnemonischen (Seed-)Phrase (12-24 Wörter), bspw. in Stahl, ein sehr guter Weg ist, um den eigenen gespeicherten Wert zu schützen.
Am wichtigsten ist es unserer Meinung nach allerdings, sein Guthaben von Börsen oder Handelsplattformen zu transferieren. Diese Drittparteien bieten immens viel Angriffsflächen und sind immer mit großen Risiken behaftet. Ob man selbst nun für den Anfang eine Software-Wallet oder direkt eine Hardware-Wallet wählt, kann diskutiert werden. Aber zumindest der Schritt dorthin, seine eigenen Keys zu verwahren, sollte gemacht werden.

Ein Backup der Keys sollte, wie beschrieben, in möglichst robuster Form vorhanden sein, um den Verlust des Backups minimieren zu können.
Einsteigerfreundliche Software-Wallets sind bspw. BlueWallet und Muun. Beide funktionieren sowohl auf Android als auch auf iOS und erlauben dem Nutzer die volle Kontrolle über die Keys, sind also Non-Custodial. Eine sehr einfache Custodial-Lösung ist die Wallet of Satoshi. Wir würden empfehlen, auf einer Custodial-Wallet niemals hohe Beträge zu halten.
Als Hardware-Wallet eignet sich die BitBox02 (Bitcoin-Only Edition) für Einsteiger. Eine Alternative für Fortgeschrittene ist die ColdCard-Wallet.

ZUSAMMENFASSUNG/VERGLEICH

Sowohl die BitBox02, als auch die ColdCard bieten eine sehr gute Dokumentation auf der jeweiligen Webseite und erklären die Einrichtung Schritt für Schritt. Bei beiden ist es ebenso möglich, eine gewisse Anzahl der mnemonischen Wörter zu erwürfeln. Die restlichen werden von der Wallet, basierend auf einem Zufallsgenerator hinzugefügt. Dies geschieht, da es sehr schwierig ist die Checksum für eine komplett selbst generierte Wallet zu errechnen. Weiterhin lassen sich beide Wallets auch mit einer eigenen Full-Node verbinden, wodurch man noch unabhängiger ist.
Wenn es gewünscht ist, eine eigene Node zu betreiben, dann gibt es auch für die Mobile-Wallets bessere Alternativen, wie bspw. Zeus. Die BlueWallet bietet ebenfalls die Möglichkeit seine eigene Node zu verbinden. Wenn fortgeschrittenere Anwendungsbereiche (Coinjoin, Einrichtung von Multisig-Wallets, Verbindung mit der eigenen Node etc.) mit der Zeit interessanter werden, ist ein Wechsel zu einer Desktop-Wallet recht wahrscheinlich, da diese sehr viel mehr Funktionen bieten und sich wiederum mit der eigenen Hardware-Wallet verbinden lassen.

Fortgeschrittene Themen besprechen wir in unsere Beratung für Fortgeschrittene, in der nochmals näher auf die Themen Privatsphäre, Timelocks, das Lightning-Netzwerk und das Thema Full-Node eingegangen wird.

Hier klicken, um Teil 3 zu buchen

Sollte dir ein beschriebenes Produkt oder eine Dienstleistung besonders gefallen, würden wir uns freuen, wenn du einen unserer Affiliate-Links zur Registrierung bzw. beim Abschluss des Kaufs benutzt.

Pocket
Zum einfachen Kauf von Bitcoin
5€ in Bitcoin geschenkt ab 500€ Transaktionsvolumen
https://pocketbitcoin.com/?ref=bitcoinexplained

BitBox 02
Hardware-Wallet zur sicheren Verwahrung
5% Rabatt-Code: BITCOINEXPLAINEDDE
https://bitbox.shop/?ref=bitcoinexplained

Seedor
Stanzen des Seeds in Stahl leicht gemacht
5% Rabatt-Code: BITCOINEXPLAINED
https://www.seedor.io/

Vielen Dank für deine Unterstützung!

BILDQUELLEN

Seite 3

Bitcoin Profitable Days (Stand 31.12.2022)
https://www.lookintobitcoin.com/charts/bitcoin-profitable-days/

Bitcoin HODL Waves (Stand 31.12.2022)
https://www.lookintobitcoin.com/charts/hodl-waves/

Seite 9

Erstellung und Ableitung einer Wallet
eigene Darstellung nach dem Vorbild armantheparman
https://armantheparman.com/public-and-private-keys/

Seite 16

Funktionsweise einer Transaktion (Stand 31.10.22)
https://mempool.space/

Seite 17, Seite 18

Funktionsweise einer Transaktion
https://mempool.space/de/block/000000000000000000376b2c45428f7c5d479b47e8fa06c-19900d7ceb18be27

Seite 18

Funktionsweise einer Transaktion (Stand 31.10.22)
https://mempool.space/de/address/12KKDt4Mj7N5UAkQMN7LtPZMayenXHa8KL

Seite 19

Funktionsweise einer Transaktion
https://mempool.space/de/tx/d052ddda5ad48b7a722fb7afc55e0d07717387e25699683544b-0cc3dba5cc86c

ABSCHLIESSENDE BEMERKUNGEN

Bitcoin ist generell ein komplexes Thema und der Umgang mit eigenen Werten sollte immer mit Bedacht durchgeführt werden. Gerade die technische Seite von Bitcoin auch nur im Ansatz zu verstehen, erfordert viel Recherche und natürlich Interesse.

Es ist möglich, dass sich gewisse Funktionen im Laufe der Zeit verändern und einige der hier festgehaltenen Informationen damit ungültig werden. Wir versuchen unsere Materialien ständig auf dem aktuellsten Stand zu halten. Bevor mögliche finanzielle Entscheidungen getroffen werden oder Werte gesichert bzw. transferiert werden, sollte immer nochmals geprüft werden, ob sich bspw. die Funktionsweise geändert hat oder technische Neuerungen entstanden sind.

Wir empfehlen allen Anwendern weiterhin, sich immer erst mit einer Wallet oder einer Handelsplattform vertraut zu machen, bevor tatsächlich Transaktionen durchgeführt werden und eigene Werte (Bitcoin) gesichert werden. Weiterhin empfehlen wir selbst dann, bei den ersten Versuchen **immer erst mit einem kleinen Anteil zu starten** und sowohl das Versenden, Empfangen und Wiederherstellen im Falle einer Wallet oder das Kaufen und Verkaufen im Falle einer Handelsplattform auszuprobieren.
Generell ist es sinnvoll mit Summen zu starten, die man bereit ist zu verlieren, um sich mit der gesamten Funktionsweise der verschiedenen Technologien vertraut zu machen.

Unsere Materialien werden nach dem besten Wissen und Gewissen erstellt. Wir übernehmen allerdings keinerlei Haftung für verlorene Schlüssel, Codes oder Passwörter. Weiterhin übernehmen wir keinerlei Haftung für sich ändernde Funktionen in der beschriebenen Software, Webseiten oder Bitcoin-Applikationen.

Jeder Nutzer ist verantwortlich, die hier beschriebenen Informationen selbst zu prüfen.

Dieses Handout dient daher nicht als finanzielle Beratung. Wir haben hier unsere eigenen Erfahrungen und Praktiken dargelegt.