GEBÜHREN-CHEAT-SHEET

Was sind Gebühren?

Zum Versenden von Bitcoin wird immer eine Gebühr fällig, die **zusätzlich** zur Summe, die man versenden möchte im Netzwerk bekannt gegeben wird. Die Gebühr wird im Regelfall **vom Sender bezahlt** und festgelegt.

Das Bitcoin-Netzwerk nutzt Transaktionsgebühren, die bei jeder Transaktion anfallen und somit einen zusätzlichen Anreiz für die Miner schaffen, um das Fortbestehen des Netzwerks zu sichern.

Der **Blockspace**, die verfügbare Speichergröße eines jeden Blocks, welcher der Timechain hinzugefügt wird, ist begrenzt. Durch die freie Wahl bei der Höhe der Gebühren entsteht ein **freier Markt** zwischen allen Netzwerkteilnehmern, bei dem um den verfügbaren Platz im (nächsten) Block gehandelt wird. Für die Miner besteht der Anreiz die Transaktionen mit den höchsten Gebühren in den aktuellen Block zu integrieren.
Soll eine Transaktion schnell ausgeführt werden, ist es daher sinnvoll eine höhere Gebühr als die Durchschnittsgebühr zu wählen. Wenn man es nicht so eilig hat, kann man die Gebühr niedrig ansetzen, wodurch es länger dauert, bis sie ausgeführt bzw. bestätigt wird.

Die Gebühren werden in **Satoshi per vByte** (Virtual Byte oder auch vB) bemessen. 1 Satoshi ist die kleinste Bitcoin-Einheit und die Maßeinheit vB entscheidet über die Speichergröße, die im Block für die Transaktion aufgewendet werden muss.
Wenn zu Stoßzeiten oder allgemein viele Netzwerkteilnehmer Bitcoin versenden wollen, kann es daher zu **sehr hohen** Gebühren kommen.

Aus diesem Grund ist es sinnvoll die Gebühren **bereits vor** der Transaktion zu kalkulieren.

Die Größe einer Bitcoin-Transaktion wird nicht dadurch bestimmt, wie viel Bitcoin (im monetären Sinne) bewegt wird. Stattdessen wird die Größe durch technische Faktoren bestimmt, bspw. wie viele Signaturen oder Inputs und Outputs die Transaktion hat. Weiterhin ist das Adressformat entscheidend.

Die Datenmenge in den Blöcken ist auf maximal 4.000.000 WU (Weight Units) begrenzt, was sich in 1.000.000 vB übersetzt, da 1 vB = 4 WU.
Daher zahlen größere Transaktionen mehr Gebühren.

Wie kalkuliert man Gebühren?

Durch Weiterentwicklung des Bitcoin-Protokolls sind über die Zeit verschiedene Adressformate und Transaktionsmöglichkeiten entstanden, die auf die Größe der Transaktion in vB Einfluss haben.

So gibt es u.a. MultiSig-Transaktionen (Multisignatur), Legacy-Adressen, Segwit-Adressen und Taproot-Adressen. Hinzu kommt, dass es, vor allem durch das Segwit-Upgrade, verschiedene Skripte gibt, die ebenfalls einen Einfluss auf die Transaktionsgröße bzw. das Transaktionsgewicht haben.

Grundsätzlich wird die Größe der Transaktion **folgendermaßen berechnet**:

Transaction Size
Transaktionsgröße

Die gesamte **Größe**, die die Transaktion benötigt, wird in Weight Units angegeben und entscheidet über die Gebühren, die zur Ausführung notwendig sind.

=

Input Size
Größe der Eingabe

Jedes UTXO der Transaktion wird **geordnet** und eindeutig zuordenbar gemacht.
Hinzu kommen die Daten zur **Signatur**.
Pro Input:
Legacy: **148** Bytes
Segwit: **68,5** Bytes

+

Output Size
Größe der Ausgabe

Die **monetäre Anzahl** an Satoshis/Bitcoin wird festgehalten.
Hinzu kommen Daten zu evtl. **Bedingungen** (Skripte) zur Ausgabe.
Pro Output:
Legacy: **34** Bytes
Segwit: **31** Bytes

+

Overhead
Weitere Daten

Weitere Metainformationen zur Transaktion, wie **Locktime** oder die **Segwit Flag**, die zeigt, dass es keine Legacy-Transaktion ist.
Konstante:
Legacy: **10** Bytes
Segwit: **10,5** Bytes

Beispiele zur Kalkulation

Exkurs: **Adressformate**
Da sich Bitcoin über die Zeit weiterentwickelt hat, haben sich die Adressformate geändert. Um die Rückwärtskompatibilität zu erhalten, gibt es daher verschiedene Formen, die sich leicht voneinander unterscheiden lassen.

- „Legacy“ Adressen beginnen immer mit „1“
  - Skript: P2PKH (pay to public key hash)
  - lässt keine zweideutigen Zeichen, wie Buchstabe O und Zahl 0 zu
  - am Ende der Adresse steht die Prüfsumme, womit Tippfehler ausgeschlossen werden
- „Nested Segwit“ Adressen beginnen immer mit „3“
  - Skript: P2SH (pay to script hash)
  - erweiterte Legacy-Adresse, vor allem für komplexere Methoden, wie Multisig verwendet
  - Vorteil von niedrigen Gebühren durch Segwit wird genutzt
- „Native Segwit“ Adressen beginnen immer mit „bc1q“
  - Skript: P2WPKH (pay to witness public key hash)
  - lagert Signaturdaten aus dem eigentlichen Block aus, wodurch mehr Platz für Transaktionen ist
  - verweist auf die angehängten Daten, was im Sinne der Speichergröße platzsparender ist
  - reduziert die Transaktionsgröße und somit die Gebühr
  - aktueller Standard bei gängigen Plattformen und Wallets
- „Taproot“ Adressen beginnen immer mit „bc1p“
  - Skript: P2TR (pay to taproot)
  - das Taproot-Update bringt vor allem ein höheres Maß an Privatsphäre
  - reduziert die Transaktionsgröße bei z. B. Multisig-Transaktionen
  - bisher noch nicht weit verbreitet

Es sei gesagt, dass alle Adressformate **untereinander kompatibel** sind. Durch den Aufbau und die technische Struktur sind Transaktionen mit Segwit-Adressen allerdings **günstiger**, als z. B. eine Transaktion mit Legacy-Adressen. Die meisten Plattformen nutzen daher momentan voreingestellt „bc1q“-Adressen.

Nachstehend haben wir **Formeln**, sowie einige **Beispiele** zur Berechnung von Transaktionsgebühren zusammengestellt:

Adressformate	vB pro Input	vB pro Output	Overhead in vB	1 Input; 2 Output	2 Input; 1 Output
Legacy	148	34	10	226 vB	340 vB
Nested Segwit	91	32	10	165 vB	224 vB
Native Segwit	68,5	31	10,5	141 vB	178,5 vB
Taproot	57,5	43	10,5	154 vB	168,5 vB

Nachdem wir nun das Gewicht bzw. die Größe der Transaktion in vB berechnet haben können wir das Ergebnis mit der **aktuellen Gebühr** des Bitcoin-Netzwerks in sat/vB multiplizieren.
Die aktuellen Netzwerkgebühren findet man in sog. Blockchain-Explorern, wie mempool.space. Diese werden, wie im Bild (zur Blockhöhe 855827 aufgenommen) dargestellt. Hierbei wird eine Schätzung durchgeführt, wie viel Gebühren zu zahlen sind, um beispielsweise mit hoher Priorität in den nächsten Block aufgenommen zu werden.
Anhand dieser Schätzung kann nun das Ergebnis der ersten Rechnung mit dem tatsächlichen Gebührenpreis in Satoshis multipliziert werden.
Günstigste Transaktion mit Segwit (1 Input, 1 Output) bei **1 sat/vB**: 109,5 vB * 1 Satoshi = **110 Satoshi**
1 Input, 2 Outputs bei **4 sat/vB**: 141 vB * 4 Satoshi = **564 Satoshi**
1 Input, 2 Outputs bei **100 sat/vB**: 141 vB * 100 Satoshi = **14.100 Satoshi**
Fazit: Zum einen können die Gebühren am Markt steigen, da der Blockspace momentan begehrt ist, zum anderen kann aber auch die Transaktionsgröße erheblichen Einfluss auf die Gebühren nehmen.

GEBÜHREN-CHEAT-SHEET

Weitere Begriffserklärungen

Die Abkürzung UTXO steht für „Unspent Transaction Output“. UTXOs beschreiben immer das Guthaben einer Wallet. Alle vom Private Key abgeleiteten Empfangsadressen mit Beträgen zusammengenommen stellen somit das Gesamtguthaben der Wallet dar.
So könnte es sein, dass das Gesamtguthaben 2 Bitcoin beträgt, aber auf 4 unterschiedliche UTXOs aufgeteilt ist:

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

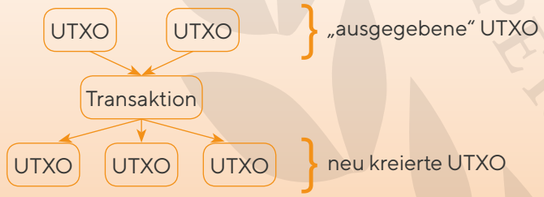
Nun sollen 1,3 BTC von der eigenen Wallet „A“ an eine andere Person „B“ gesendet werden. Die Wallet würde nun also die passenden UTXOs mit den entsprechenden Empfangsadressen heraussuchen und die Transaktion signieren. Es wäre möglich die 1,1 BTC und die 0,2 BTC zu versenden aber es wäre genau so möglich, dass 1,1 BTC und 0,6 BTC zusammengefasst und dann wieder 0,4 BTC auf eine neue Empfangsadresse („Change-Address“) der eigenen Wallet gutgeschrieben werden.
Sollte dies der Fall sein würde das Gesamtguthaben 0,7 BTC betragen und sich wie folgt 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 zwei Inputs (1,1 BTC und 0,6 BTC) und zwei Outputs: 1,3 BTC als Zahlung und 0,4 BTC als „Wechselgeld“ zur sog. **Change-Address**.

In diesem Beispiel wurden die Netzwerkgebühren bewusst nicht beachtet.
Nach Bestätigung einer Transaktion stehen die an Empfänger B versendeten Inputs ihm selbst wieder als UTXO und somit als Input für seine nächste Transaktion zur Verfügung.

Der eigene Bitcoin-Bestand besteht daher 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.



- 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 **im Ganzen konsumiert**, das „Wechselgeld“ der eigenen Wallet gutgeschrieben
- jedem UTXO kann eine Public Address (öffentliche Empfangsadresse) zugeordnet werden
- der Private Key zu einer UTXO ist immer sicher zu verwahren - Not your Keys, not your Coins

---

Die Einheit Virtual Byte (vB) wurde durch das Segwit-Update (Segregated Witness) eingeführt, da die **Signaturdaten** durch Veränderung der Transaktionsstruktur ausgelagert wurden und somit mehr Platz für Transaktionen in den einzelnen Blöcken geschaffen wurde. Die Gewichtseinheiten des „normalen“ Teil des Blocks werden mit **Faktor 4** bemessen, die ausgelagerten Daten im „Witness“-Teil des Blocks (Signaturdaten) werden einfach hinzuaddiert.
So würden aus 40 Byte im normalen Block und 2 Byte im Witness also 162 **Weight Units** (WU) werden.
Aus 2 Byte im normalen Block und 40 Byte im Witness würden 48 WU werden.
Die maximale Größe eines Blocks beträgt **4.000.000 WU** und nicht mehr, wie vor Segwit, 1.000.000 Byte. Die Einheit vB berechnet den zusätzlichen Speicherplatz des ausgelagerten Witness mit ein.

Probleme bei hohen Gebühren

Wenn die Gebühren im Netzwerk sehr hoch sind, kann es vorkommen, dass **UTXOs wertlos** werden, da diese nicht mehr bewegt werden können. Wenn beispielsweise die Gebühren höher sind als der Betrag, der beim speziellen UTXO hinterlegt ist dann ist es ökonomisch nicht sinnvoll diesen zu bewegen.

Gerade, wenn man durch einen **DCA-Sparplan** („Dollar-Cost-Average“) regelmäßig Bitcoin-Käufe tätigt, sammeln sich viele UTXOs an. Teilweise bieten Börsen tägliche oder sogar stündliche Ausführung des Sparplans an, wodurch die Gefahr steigt, dass diese UTXOs irgendwann unbrauchbar werden.

Die **Konsolidierung**, also Zusammenführung vieler kleiner UTXOs zu einem größeren brauchbaren UTXO, kann sehr schnell sehr teuer werden (s. Berechnungen umseitig).

Lösungen bei hohen Gebühren

Eine einfache Lösung ist es, den DCA auf **längere Zeiträume** zu strecken und somit auch den **monetären Wert pro Kauf erhöhen**. Statt beispielsweise täglicher einzelner Käufe à 10€ kann man auch einmalig im Monat einen größeren Kauf tätigen. Man umgeht somit auch später bei einer möglichen Konsolidierung den Zwang viele Inputs verwenden zu müssen.

Bei der Konsolidierung werden mehrere Inputs zu einem Output. Hierzu lohnt es sich in Phasen, in denen das Netzwerk besonders belastet ist, zu warten, bis die **Gebühren wieder niedriger** sind. Da die Kennzahl sat/vB letztendlich der entscheidende Faktor ist und über die Höhe der Gebühr entscheidet sollte man sich **bereits im Vorfeld Gedanken machen**, welche UTXO-Größen für einen selbst sinnvoll sein könnten.
Kleinere UTXOs können sinnvoll sein, wenn man regelmäßig mit Bitcoin bezahlt, umgekehrt können größere UTXOs sich besser für Leute eignen, die nicht planen ihre Bitcoin in naher Zukunft zu bewegen. Hier gibt es allerdings keine Faustregel und auch kein richtig oder falsch. Wichtig ist dennoch sich über die Problematik bewusst zu sein und darüber nachzudenken, **wie man individuell verfahren möchte**.

Beim Bekanntgeben von Transaktionen im Netzwerk („broadcasten“) bieten einige Wallet-Softwares auch an, dass man die Gebühr in sat/vB selbst festlegt. Hier sollte man bedenken, dass es möglich ist, dass bestimmte Nodes **die eigene Transaktion ablehnen**, da die hinzugefügte Transaktionsgebühr zu niedrig ist.

Weiterführende Links

Nodesignal Podcast:	https://tinyurl.com/Nodesignal-EP-144
Blockchain Academy:	https://tinyurl.com/Blockchain-Academy
Learn Me A Bitcoin:	https://tinyurl.com/learnmeabitcoin
Gebührenrechner:	https://tinyurl.com/Bitcoinops

MADE WITH ❤ BY
WWW.BITCOINEXPLAINED.DE

- Seminare
- Einzelberatungen
- Individuelle Themen
- Freie Inhalte und Artikel