

Anleitung für Szene-Start, verfasst von SMARTPHONE

Inhaltsverzeichnis:

- Schritt 1: Verschlüsselten Ordner mit VeraCrypt erstellen (S. 02)
- Schritt 2: Firefox Portable zum anonymen Surfen einrichten (S. 08)
- Schritt 3: VPN zur Verschlüsselung der IP einrichten (S. 11)
- Schritt 4: Electrum zum Verwalten von Bitcoins einrichten (S. 12)
- Schritt 5: Exodus zum Verwalten von Kryptos einrichten (S. 19)
- Schritt 6: Feather zum Verwalten von Monero einrichten (S. 20)
- Schritt 7: Kryptowährungen exchangen mit FixedFloat (S. 21)
- Schritt 8: Bitcoins mit Paysafecards erwerben (S. 22)
- Schritt 9: VSIM-Anbieter für SMS-Verifikationen nutzen (S. 24)
- Schritt 10: Bilder anonym versenden mit Exif Cleaner (S. 25)
- Schritt 11: Hardware ID ändern mit MAC Address Changer (S. 26)

Link-Sammlung:

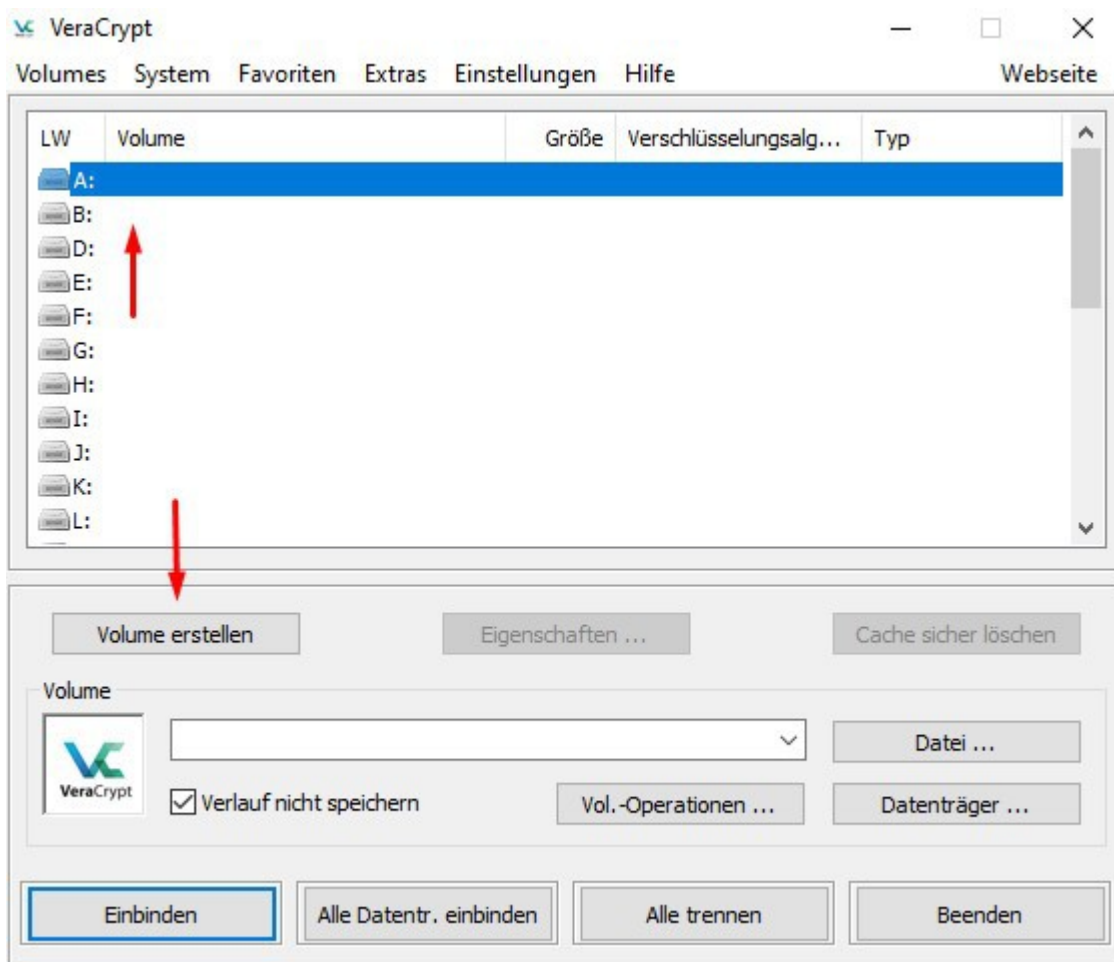
- VeraCrypt: <https://www.veracrypt.fr/en/Downloads.html>
- Firefox Portable: https://portableapps.com/de/apps/internet/firefox_portable
- Mullvad: <https://mullvad.net/de/>
- OVPN: <https://www.ovpn.com/de>
- Whoer: <https://whoer.net/de>
- Electrum: <https://electrum.org/>
- Exodus: <https://www.exodus.com/download/>
- Feather: <https://featherwallet.org/download/>
- Blockchain Explorer: <https://www.blockchain.com/explorer>
- FixedFloat: <https://fixedfloat.com/>
- Changelly: <https://changelly.com/de>
- Paysafecard kaufen: <https://dundle.com/de/paysafecard/>
- Bitcoins kaufen und einlösen: <https://www.mmoga.de/> | <https://cryptovoucher.io/>
- Autofications: <https://autofications.com/>
- SMS-Activate: <https://sms-activate.org/en>
- Exif Cleaner: <https://www.verexif.com/> | <https://www.metadata2go.com/>
- MAC Address Changer: <https://technitium.com/tmac/>

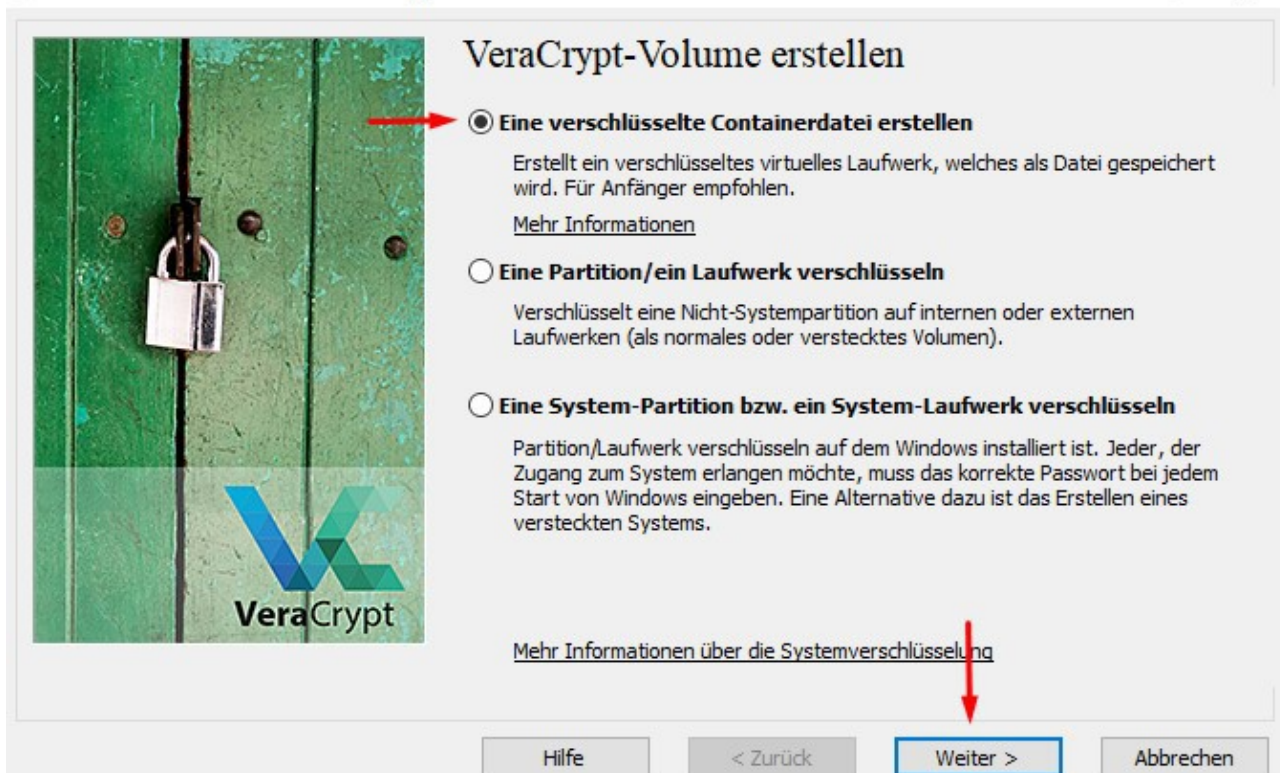
Schritt 1: Verschlüsselten Ordner mit VeraCrypt erstellen

Bevor man sensible Daten auf seinem Rechner speichert, sollte man erstmal einen gesicherten Ort haben, damit die Daten auch vor fremdem Zugriff geschützt sind. Dazu müsst ihr VeraCrypt auf eurem Rechner installieren. Über eine Google-Anfrage zu "VeraCrypt Download" erhaltet ihr die aktuellen Download-Links, ansonsten habe ich hier einmal die offizielle Download-Seite für euch:

<https://www.veracrypt.fr/en/Downloads.html>

Mithilfe von VeraCrypt könnt ihr einen verschlüsselten Ordner auf eurem Rechner erstellen, der nur mit eurem eigenen Passwort entschlüsselt werden kann. Nach der Installation startet ihr VeraCrypt und wählt zunächst einen beliebigen Buchstaben aus, der als Speicherort für die neue Containerdatei gelten wird. Dann klickt ihr auf "Volume erstellen" und folgt den weiteren Grafiken.





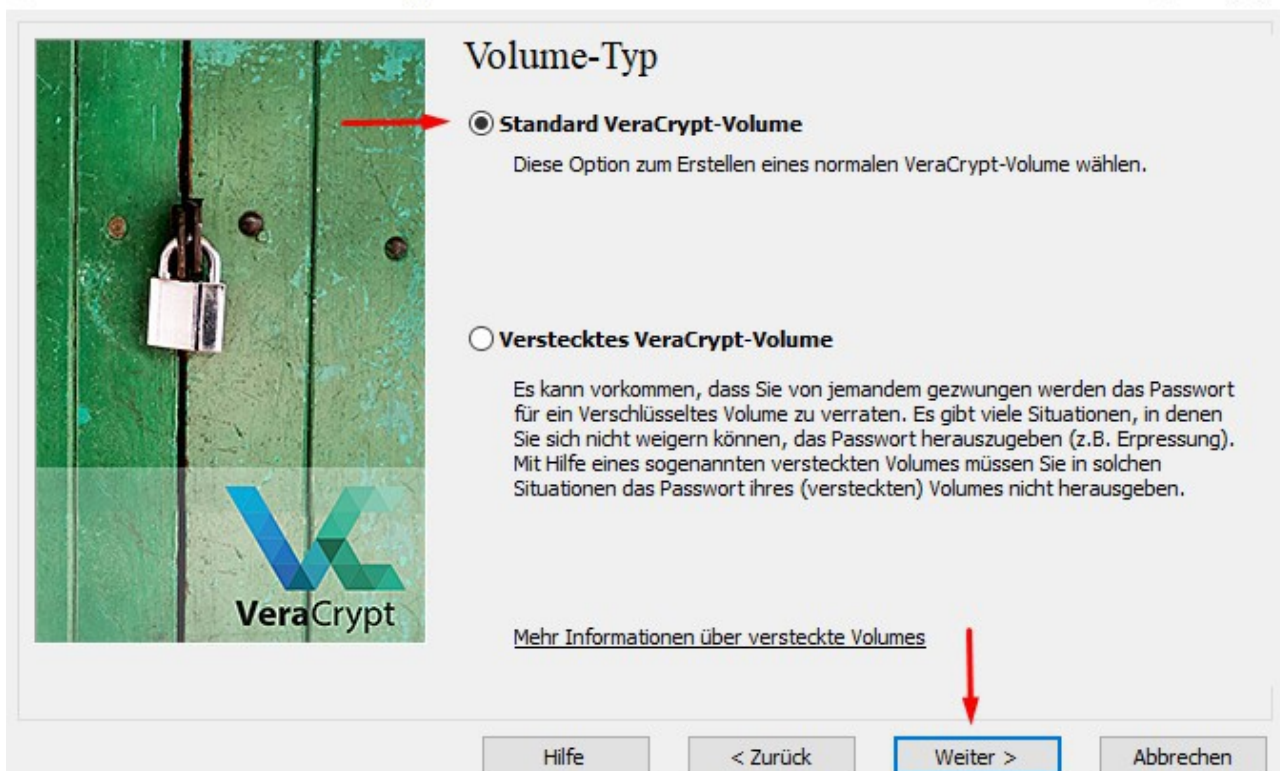
VeraCrypt-Volumen erstellen

Eine verschlüsselte Containerdatei erstellen
Erstellt ein verschlüsseltes virtuelles Laufwerk, welches als Datei gespeichert wird. Für Anfänger empfohlen.
[Mehr Informationen](#)

Eine Partition/ein Laufwerk verschlüsseln
Verschlüsselt eine Nicht-Systempartition auf internen oder externen Laufwerken (als normales oder verstecktes Volumen).

Eine System-Partition bzw. ein System-Laufwerk verschlüsseln
Partition/Laufwerk verschlüsseln auf dem Windows installiert ist. Jeder, der Zugang zum System erlangen möchte, muss das korrekte Passwort bei jedem Start von Windows eingeben. Eine Alternative dazu ist das Erstellen eines versteckten Systems.
[Mehr Informationen über die Systemverschlüsselung](#)

Hilfe < Zurück Weiter > Abbrechen



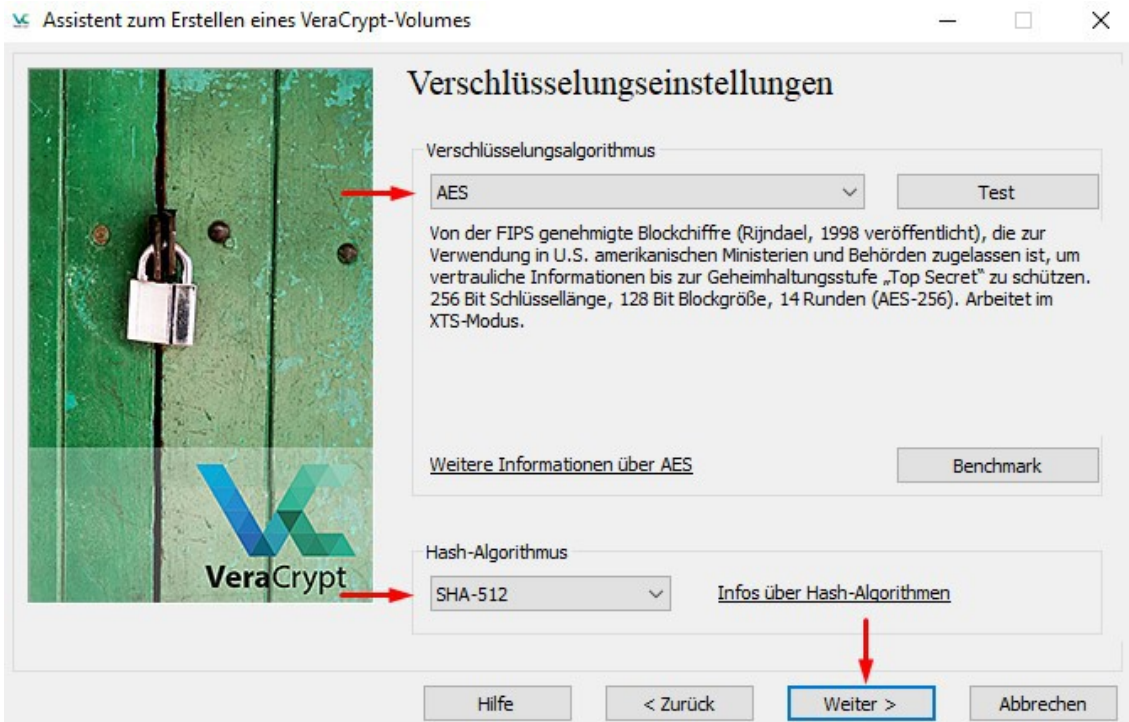
Volume-Typ

Standard VeraCrypt-Volumen
Diese Option zum Erstellen eines normalen VeraCrypt-Volumen wählen.

Verstecktes VeraCrypt-Volumen
Es kann vorkommen, dass Sie von jemandem gezwungen werden das Passwort für ein Verschlüsseltes Volumen zu verraten. Es gibt viele Situationen, in denen Sie sich nicht weigern können, das Passwort herauszugeben (z.B. Erpressung). Mit Hilfe eines sogenannten versteckten Volumens müssen Sie in solchen Situationen das Passwort ihres (versteckten) Volumens nicht herausgeben.
[Mehr Informationen über versteckte Volumens](#)

Hilfe < Zurück Weiter > Abbrechen

Dann müsst ihr der Containerdatei noch einen Namen geben und sie abspeichern. Ich würde als Speicherort vorerst den Desktop empfehlen.



Nun müsst ihr angeben, wie viel Speichervolumen ihr für den Ordner zur Verfügung stellen wollt. Für den Anfang sollten 10-100 GB völlig ausreichen. Nachdem ihr auf "Weiter" klickt, müsst ihr an dieser Stelle euer Passwort vergeben. Für maximalen Schutz vor autoritärem Zugriff empfehle ich ein Passwort aus mindestens 50 Zeichen. Der wichtigste Punkt ist, dass ihr das Passwort nirgendwo aufschreiben dürft. Ihr müsst es zwingend komplett auswendig lernen. Nur so könnt ihr euren eigenen Schutz bestmöglich garantieren. Um sich ein so langes Passwort besser merken zu können, empfehle ich ganze Sätze zu verwenden wie z.B.: "heutebinichaberwirklichbesondersgutgelaunt44444444"

Ihr bestätigt das neue Passwort dann mit "Weiter".



Volume-Format

Optionen

Dateisystem **FAT** Cluster **Vorgabe** Schnell-Formatierung Dynamisch

Zufallswerte: * . * , * / . + + + + , - - , * / + , + + - * * - . , + / / + - - ...

Kopfschlüssel: *****

Hauptschlüssel: *****

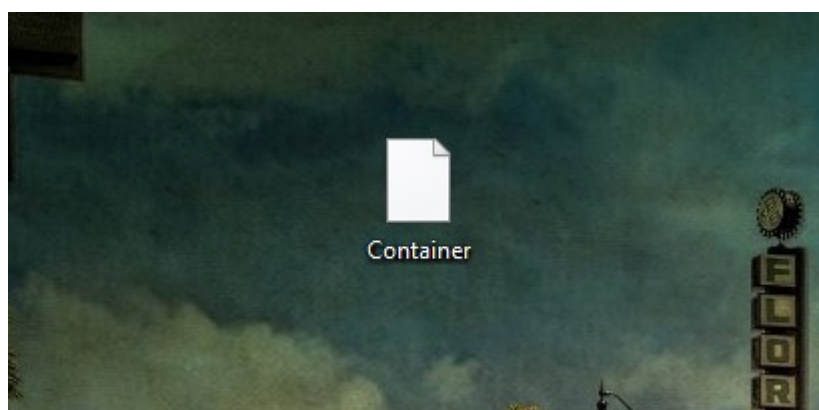
Fertig Geschw. Rest **Abbrechen**

WICHTIG: Den Mauszeiger in diesem Fenster zufällig hin- und herbewegen. Je länger (min. 30 Sek.) Sie die Maus bewegen desto besser. Dies trägt zu einer verbesserten Verschlüsselung bei. Klicken Sie auf „Formatieren“, um mit der Erstellung fortzufahren.

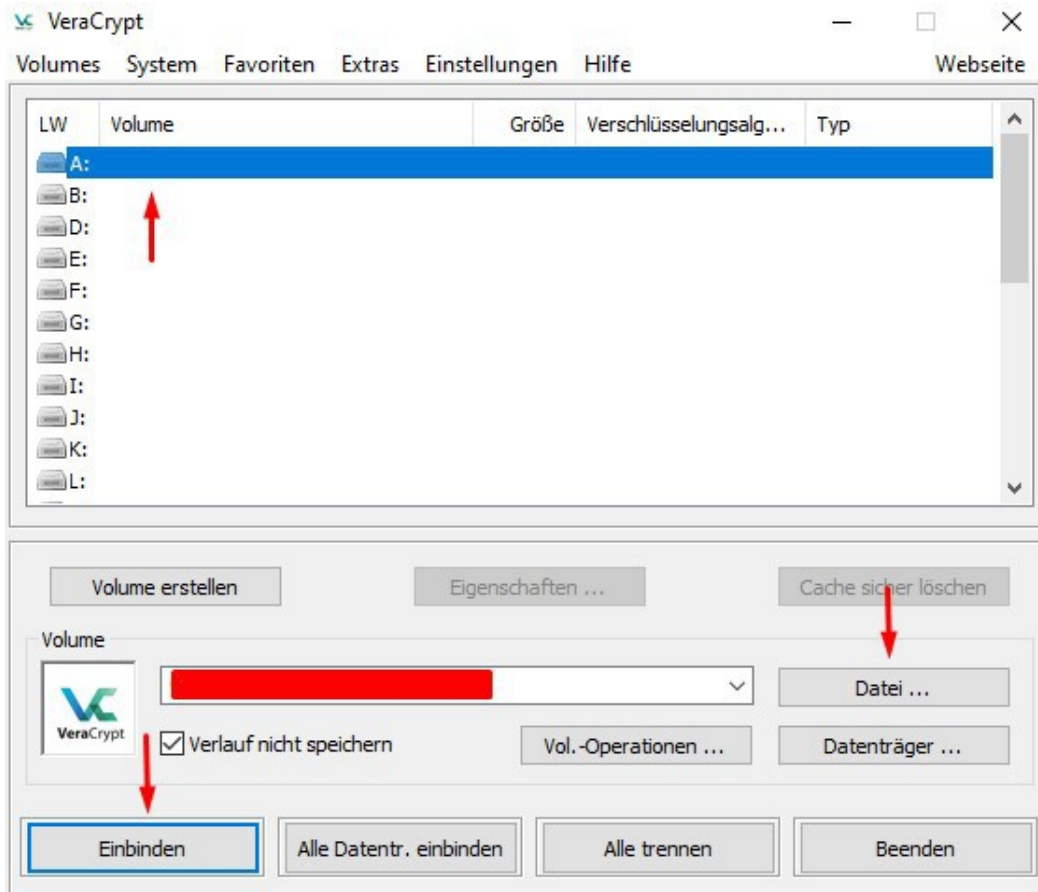
Durch Mausbewegungen gesammelte Entropie

Hilfe < Zurück **Formatieren** Abbrechen

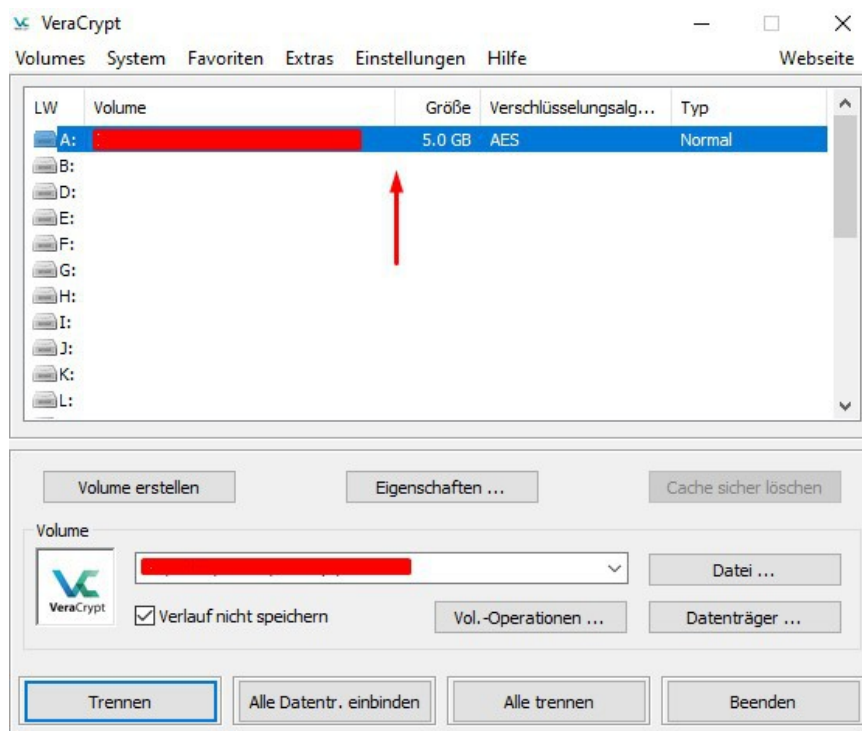
Hier müsst ihr euren Mauszeiger nun kreuz und quer durch das Fenster bewegen, bis sich der grüne Balken komplett aufgeladen hat und am besten noch 2-3 Minuten länger. Dies hilft beim Verschlüsselungsprozess des Containers. Danach bestätigt ihr das Ganze mit "Formatieren". Ihr seid jetzt mit dem Erstellen eures Containers fertig. Auf eurem Desktop befindet sich nun eine verschlüsselte Containerdatei, die nur noch mithilfe eures Passworts geöffnet werden kann. Selbst bei Zugriff durch autoritäre Institutionen halten die verschlüsselten Container oft stand, wenn das Passwort lang und stark genug ist.



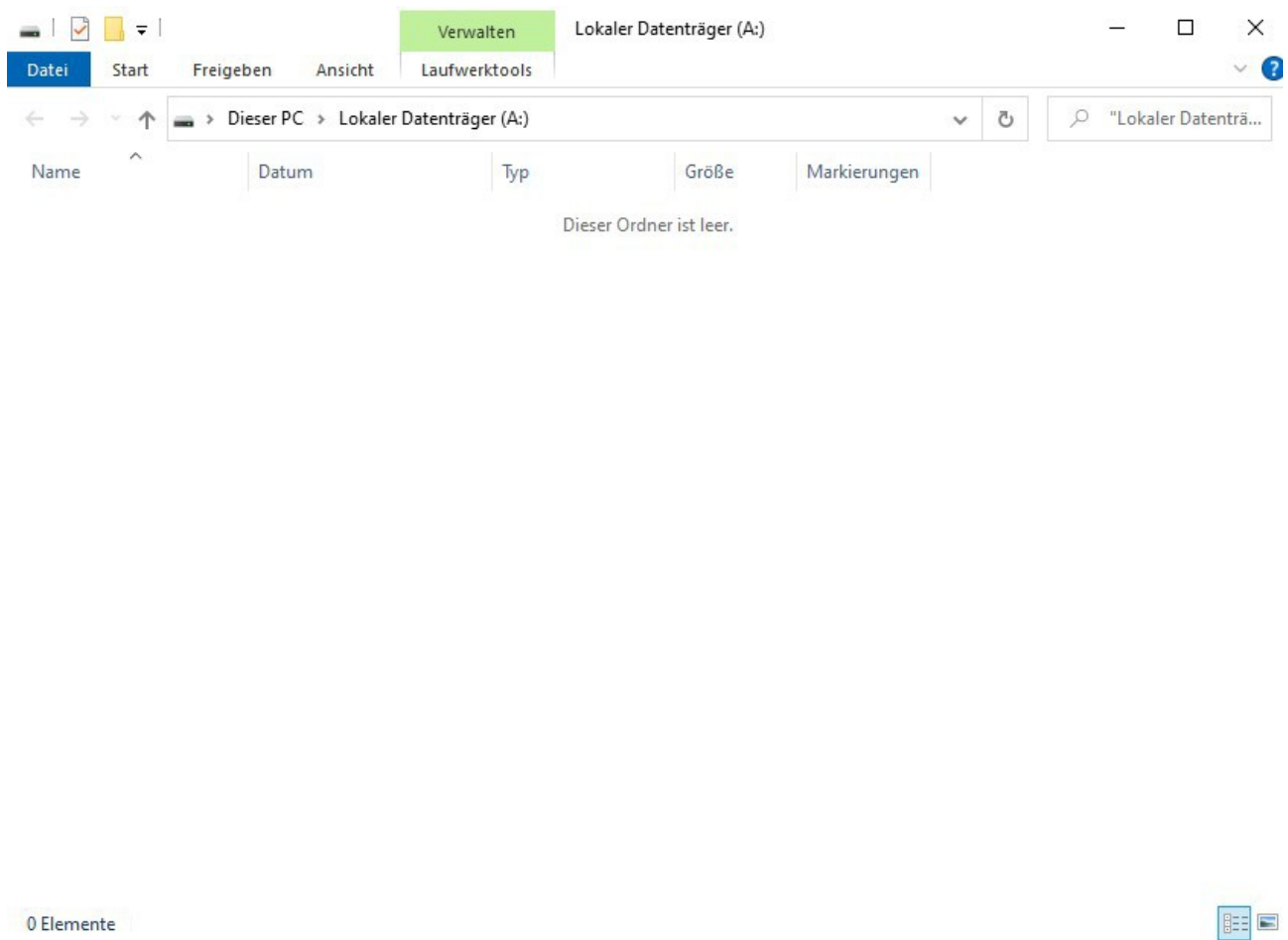
Um nun auf den Containerinhalt zugreifen zu können, startet ihr erneut VeraCrypt und wählt zuerst den Buchstaben für eure Containerdatei aus. Dann klickt ihr mittig rechts auf "Datei" und wählt eure erstellte Containerdatei aus.



Dann klickt ihr auf "Einbinden" und gebt nun euer Passwort ein, um euren verschlüsselten Container zu entsperren. Dies dauert einige Sekunden.



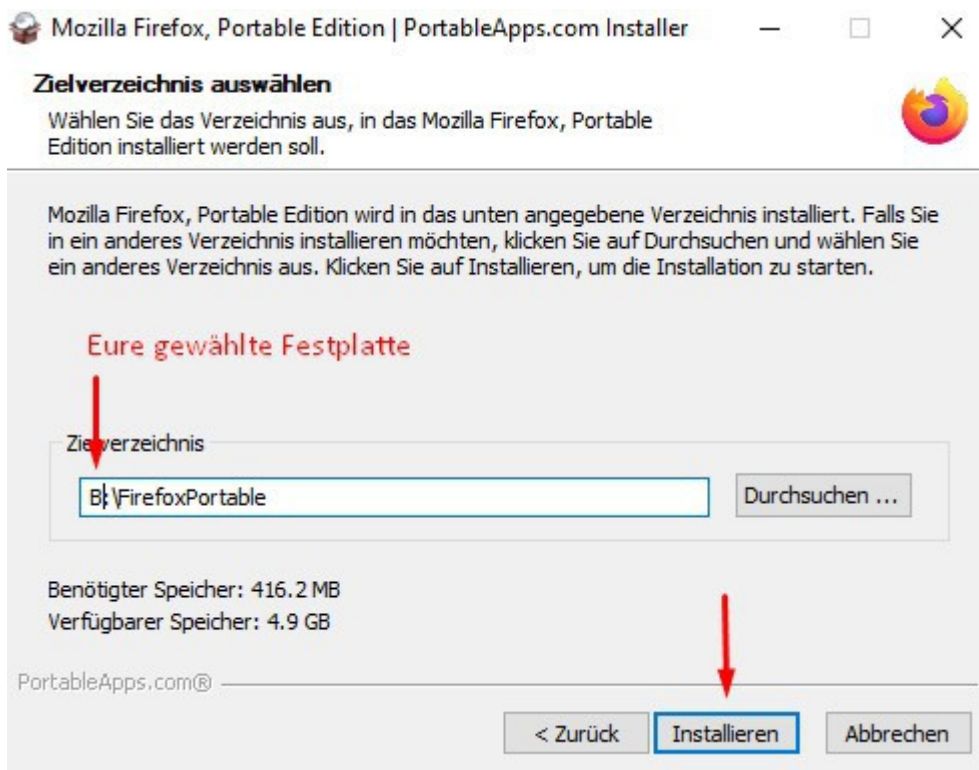
Über einen Doppelklick auf die blau gefärbte Leiste gelangt ihr nun in euren verschlüsselten Ordner, wo ihr eure Daten geschützt abspeichern könnt.



Eure Containerdatei sieht nun aus wie ein ganz normaler Ordner, aber wenn ihr bei VeraCrypt unten links auf "Trennen" geht oder euren PC ausschaltet, ist euer Ordner direkt wieder komplett verschlüsselt und nur noch über euer Passwort zu öffnen. Ihr könnt beliebig viele Containerdateien erstellen und diese z.B. auch auf USB-Sticks übertragen. Es gibt USB-Sticks, die nur einen einzigen Centimeter groß sind. Ihr könnt also vertrauliche Daten in einem Container abspeichern, diesen auf einen USB-Stick übertragen und den USB-Stick dann in irgendeiner kleinen Ritze verstecken. Somit sind eure Daten immer gesichert, wenn ihr aus irgendwelchen Gründen den Zugriff auf euren Rechner verlieren solltet.

Schritt 2: Firefox Portable zum anonymen Surfen einrichten

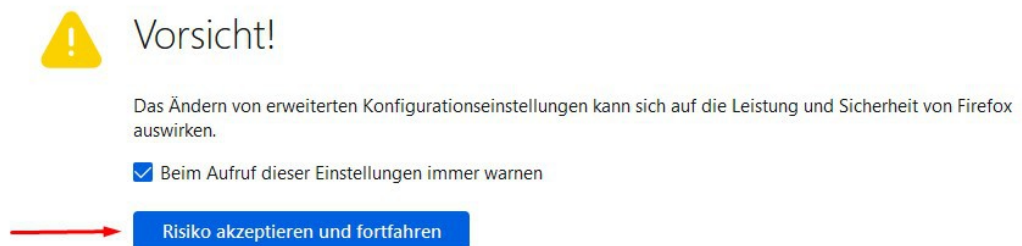
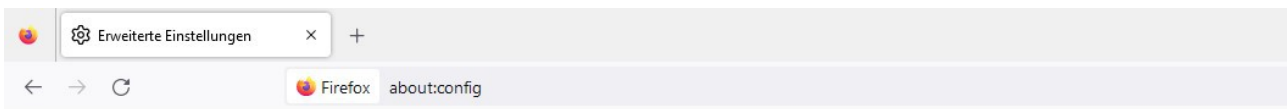
Jetzt geht es darum, den Browser einzurichten, damit ihr euch mit möglichst hoher Anonymität im Internet bewegen könnt. Mit den folgenden Einstellungen im Firefox Portable Browser sind eure Besuche auf Websites nahezu kaum zurückverfolgbar. Zuerst müsst ihr euch den Firefox Portable Browser herunterladen (über eine Google-Anfrage zu "Firefox Portable Download" oder hier: https://portableapps.com/de/apps/internet/firefox_portable) und in eurem Containerordner abspeichern. Ihr findet den Speicherort eures entsperrten Containers auf dem Rechner meistens unter "Dieser PC" und "Geräte/Festplatten". Die Installation des Programmordners von Firefox Portable führt ihr bitte auch innerhalb des Containers durch.



Nun habt ihr Firefox Portable erfolgreich installiert und könnt die Einstellungen verändern. Dazu startet ihr einmal Firefox Portable und geht oben rechts im Menü auf "Einstellungen". In den Einstellungen geht ihr dann auf der linken Seite auf "Datenschutz & Sicherheit". Als Browser-Datenschutz wählt ihr bitte die Option "Strenger Schutz". Bei der folgenden Option "Websites eine "Do Not Track"-Information senden, dass die eigenen Aktivitäten nicht verfolgt werden sollen" wählt ihr bitte "Immer". Bei der folgenden Option "Cookies und Website-Daten beim Beenden von Firefox löschen" müsst ihr unbedingt den Haken aktivieren. Bei der Option "Chronik" aktiviert ihr bitte den Modus "Immer den privaten Modus verwenden" wozu der Browser einmal neu gestartet werden muss.

Als nächstes ändern wir noch einige Konfigurationseinstellungen im Browser, um eine möglichst hohe Sicherheit beim Surfen zu gewährleisten. Was die verschiedenen

Einstellungen bewirken, könnt ihr bei Interesse gerne online nachlesen. Ihr klickt oben einmal auf die Suchleiste und gebt in dem leeren Feld "about:config" ein.



Hier könnt ihr nun die Konfigurationseinstellungen ändern. Ich habe hier eine Liste mit den effektivsten Einstellungen für anonymes Surfen zusammengestellt, die ihr bitte alle so auf euren Browser übertragen müsst, indem ihr einzeln die Einstellungen heraussucht und die jeweiligen Werte ändert:

media.peerconnection.enabled "false"

beacon.enabled "false"

geo.enabled "false"

webgl.disabled "true"

webgl.enable-webgl2 "false"

webgl.min_capability_mode "true"

webgl.enable-debug-renderer-info "false"

browser.formfill.enable "false"

extensions.formautofill.addresses.enabled "false"

extensions.formautofill.creditCards.enabled "false"

extensions.formautofill.heuristics.enabled "false"

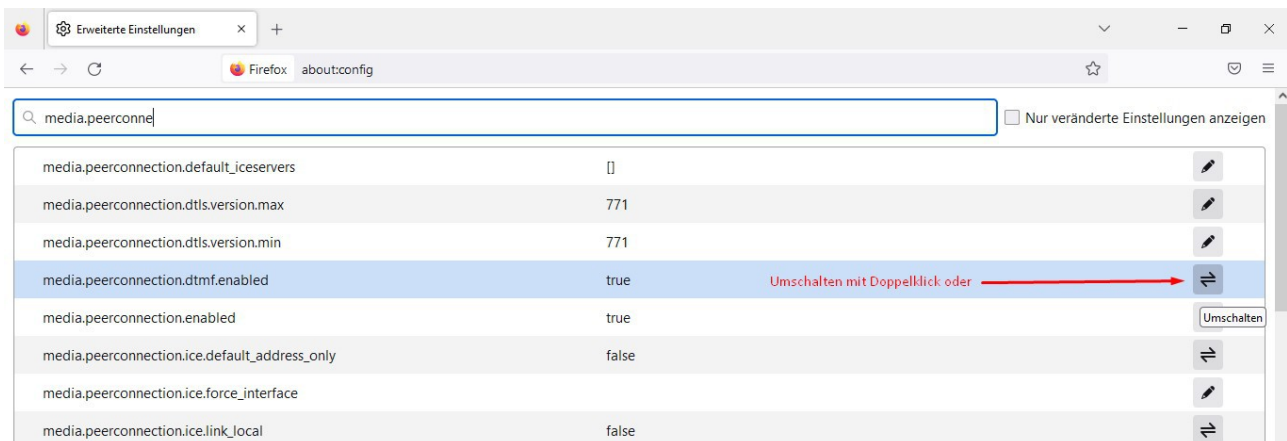
dom.enable_resource_timing "false"

dom.enable_performance "false"

dom.enable_performance_navigation_timing "false"

dom.enable_performance_observer "false"

dom.event.clipboardevents.enabled "false"
network.http.speculative-parallel-limit "0"
extensions.pocket.enabled "false"
extensions.screenshots.disabled "true"
extensions.blocklist.enabled "false"
extensions.getAddons.cache.enabled "false"
browser.safebrowsing.phishing.enabled "false"
browser.safebrowsing.malware.enabled "false"
browser.safebrowsing.blockedURIs.enabled "false"
browser.safebrowsing.downloads.enabled "false"
browser.safebrowsing.downloads.remote.enabled "false"
datareporting.policy.dataSubmissionEnabled "false"
toolkit.telemetry.unified "false"
toolkit.telemetry.archive.enabled "false"
toolkit.telemetry.updatePing.enabled "false"
browser.region.update.enabled "false"
app.normandy.enabled "false"
network.captive-portal-service.enabled "false"



Nachdem ihr alle genannten Einstellungen umgestellt habt, seid ihr nun fertig mit dem Konfigurieren eures Browsers. Solange eure IP verschlüsselt ist, wird man eure Aktivitäten im Internet an dieser Stelle praktisch kaum noch nachverfolgen oder irgendwie zuordnen können, da auch der Browserverlauf bei jedem Beenden des Browsers wieder komplett gelöscht wird. Für ein bequemes Surfen empfehle ich, die meistbesuchten Websites oben als Lesezeichen abzuspeichern, sodass man trotzdem immer direkten Zugriff auf sie hat. Wie ihr eure IP sicher verschlüsseln könnt, erfahrt ihr im nächsten Schritt.

Schritt 3: VPN zur Verschlüsselung der IP einrichten

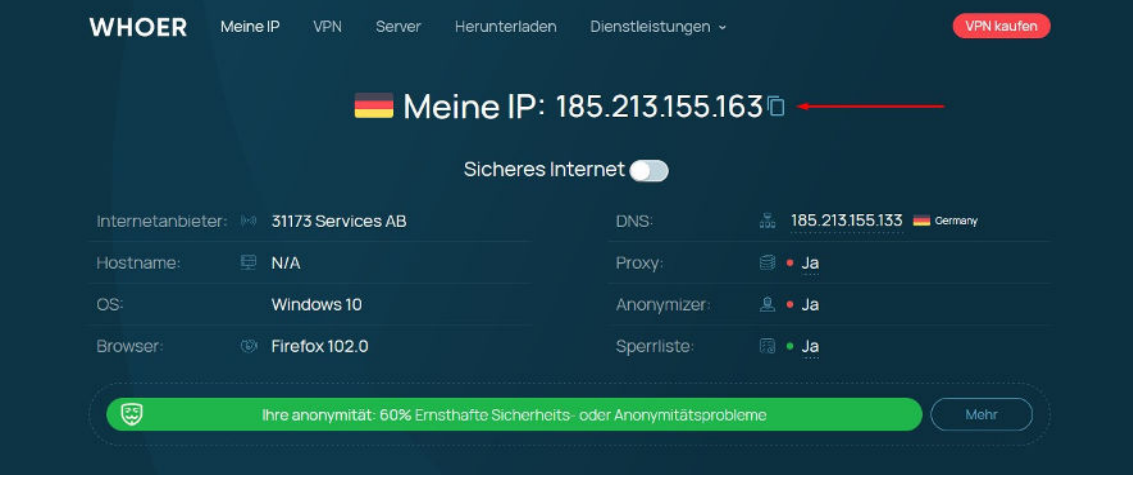
Selbst ein gut konfigurierter Browser bringt uns nichts, wenn unsere persönliche IP immer noch von den Websites ausgelesen wird, die wir besuchen. Daher müsst ihr zwingend als wichtigste Maßnahme zur eigenen Sicherheit eure IP verschlüsseln. Dies ist heutzutage sehr einfach. Meine beiden Favoriten in Sachen VPN sind:

MULLVAD: <https://mullvad.net/de/>

OVPN: <https://www.ovpn.com/de>

Bei beiden Anbietern könnt ihr **ohne Angabe einer E-Mail Adresse** direkt ein Benutzerkonto erstellen. Es gibt verschiedene Bezahlungsmöglichkeiten, unter anderem auch Bitcoins. Diese Investition von 5-10€ pro Monat für eure eigene Sicherheit ist die beste Investition, die ihr überhaupt machen könnt. Nach der erfolgreichen Bezahlung des VPN Dienstes für mindestens 1 Monat müsst ihr nur noch den VPN Client herunterladen und auf eurem Rechner installieren (diesmal nicht im Containerordner installieren). Dann startet ihr den VPN Client, loggt euch mit euren Benutzerdaten ein und klickt auf "Verbinden". Eure IP ist nun erfolgreich verschlüsselt. In den Einstellungen der meisten VPN Dienste kann man die Option "Killswitch" aktivieren, was bedeutet, dass eure Internetverbindung automatisch gekappt wird, wenn die VPN Verbindung mal aus irgendwelchen Gründen abbricht. Somit soll ein IP Leak verhindert werden. Nachdem ihr Schritt 2 und Schritt 3 erfolgreich umgesetzt habt, könnt ihr euch mit sehr hoher Anonymität im Internet bewegen. Sollte man eure Aktivitäten an dieser Stelle noch irgendwie zurückverfolgen oder zuordnen wollen, wäre dazu sehr intensive IT-Forensik notwendig, die in der Regel ohne erhebliche Gründe nicht betrieben wird. **Als letzte Maßnahme müsst ihr noch überprüfen, ob eure IP auch wirklich verschlüsselt wurde.** Dazu öffnet ihr Firefox Portable und besucht folgende Website: <https://whoer.net/de>

Hier wird nun eure VPN IP angezeigt. Ihr könnt gerne nochmal den VPN Client schliessen, um euch eure reale IP auf whoer.net anzeigen zu lassen und diese dann nach dem Starten des VPN Clients wieder mit der VPN IP zu vergleichen. Bedenkt aber, dass ihr bei jedem Wechseln eurer IP einmal den Browser neu starten müsst, damit die Anzeige auf whoer.net auch richtig übernommen wird.



The screenshot shows the WHOER website interface. At the top, there is a navigation bar with 'WHOER' and several menu items: 'Meine IP', 'VPN', 'Server', 'Herunterladen', and 'Dienstleistungen'. A red button labeled 'VPN kaufen' is in the top right corner. The main content area displays 'Meine IP: 185.213.155.163' with a German flag icon and a red arrow pointing to the IP address. Below this, there is a toggle for 'Sicheres Internet'. The interface is divided into two columns of system information:

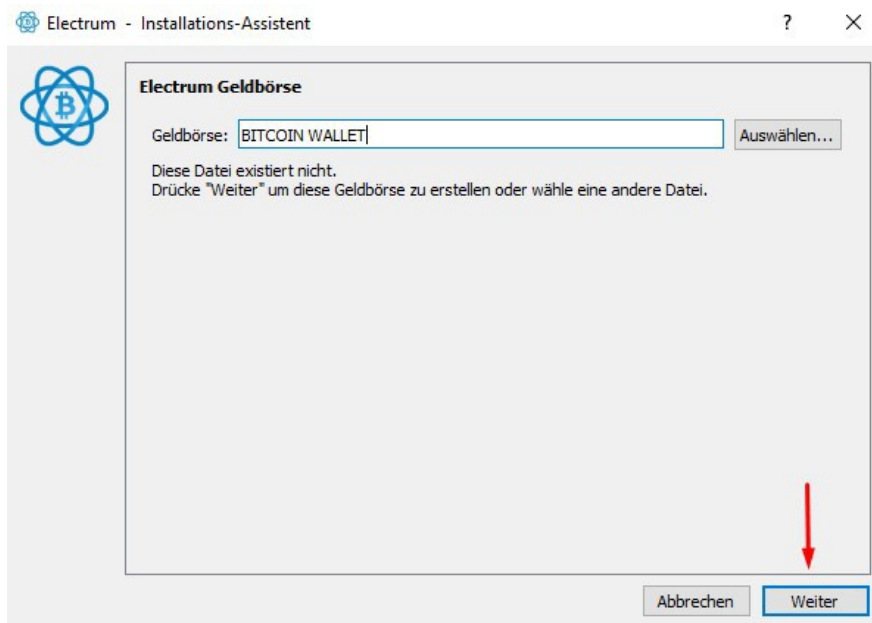
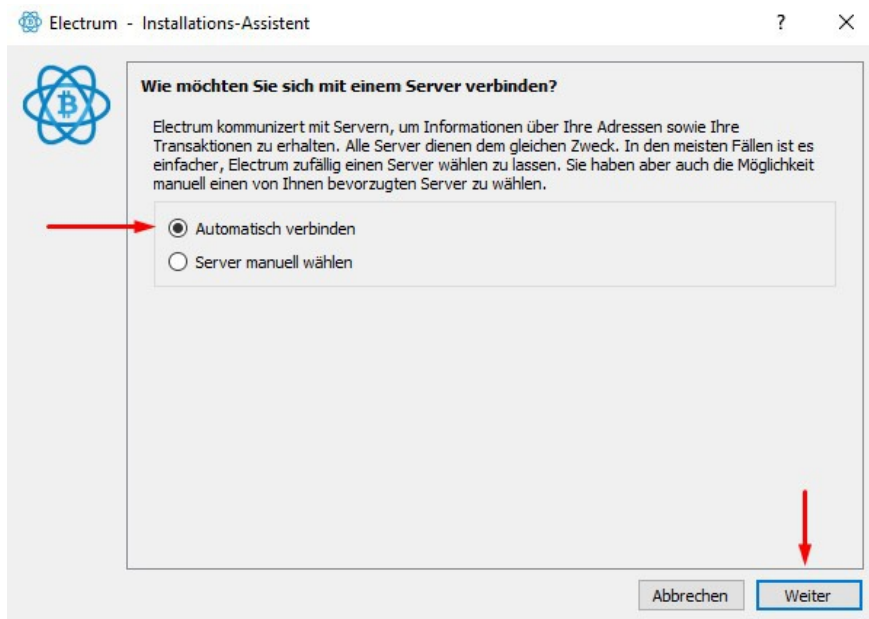
Internetanbieter: 31173 Services AB	DNS: 185.213.155.133 Germany
Hostname: N/A	Proxy: Ja
OS: Windows 10	Anonymizer: Ja
Browser: Firefox 102.0	Sperrliste: Ja

At the bottom, there is a green bar indicating 'Ihre anonymität: 60% Ernsthafte Sicherheits- oder Anonymitätsprobleme' and a 'Mehr' button.

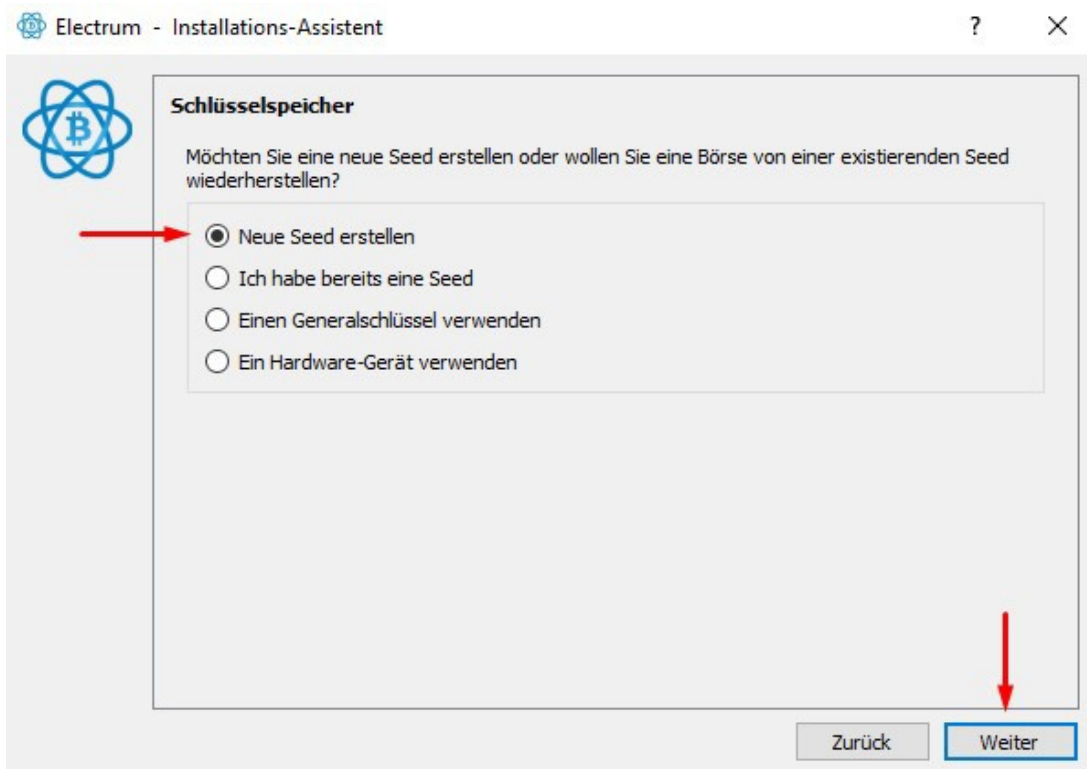
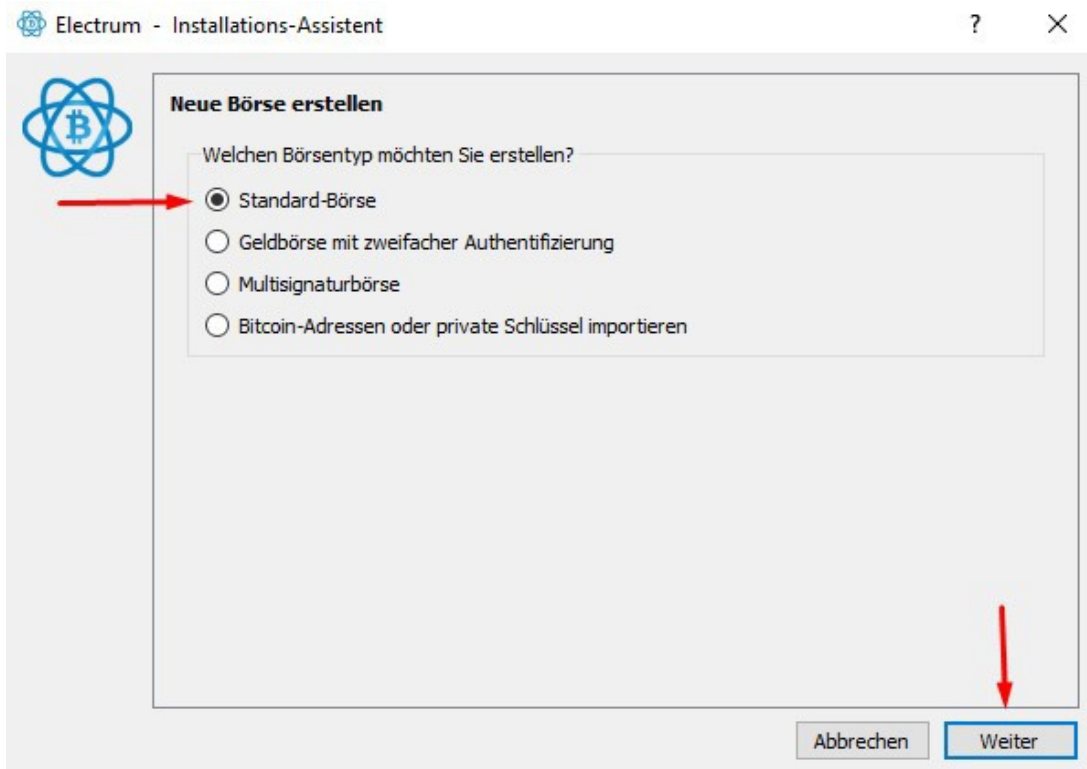
Schritt 4: Electrum zum Verwalten von Bitcoins einrichten

Ihr benötigt eine digitale Wallet, also ein digitales "Portemonnaie", um eure Bitcoins verwalten zu können. Mit dieser Bitcoin Wallet könnt ihr ganz einfach jederzeit Bitcoins empfangen oder versenden. Electrum hat sich seit Jahren als sehr zuverlässige Wallet erwiesen, daher ladet ihr euch bitte einmal die **Portable Version** der Electrum Wallet unter folgendem Link herunter und installiert das Programm **innerhalb eures Containerordners**: <https://electrum.org/>

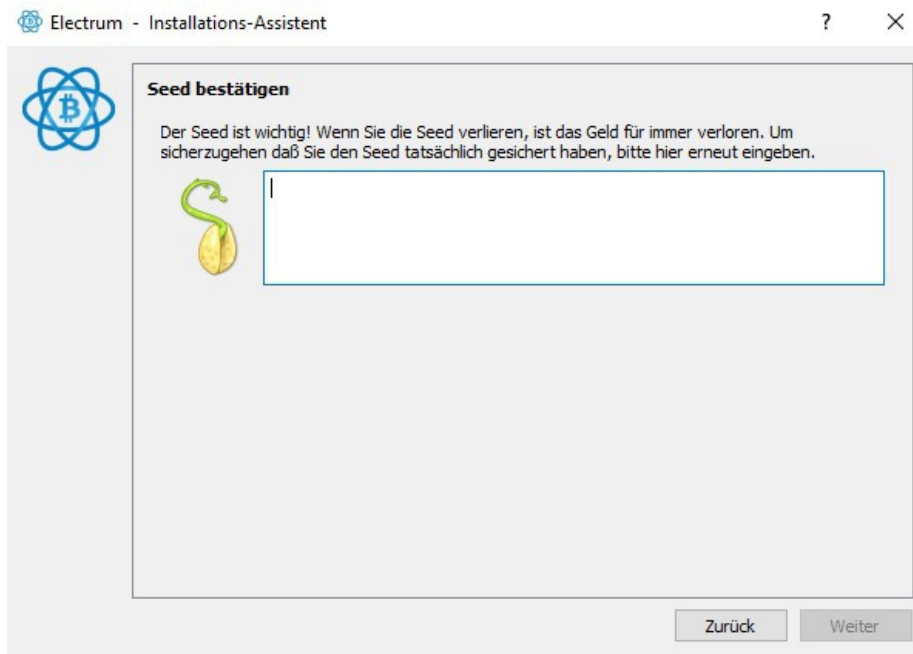
Mithilfe von Screenshots führe ich euch einmal durch die Installation sowie die Grundlagen von Electrum. Danach wisst ihr, wie ihr problemlos Bitcoins empfangen, aufbewahren und versenden könnt.



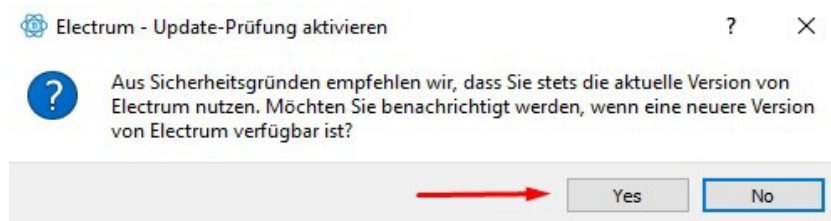
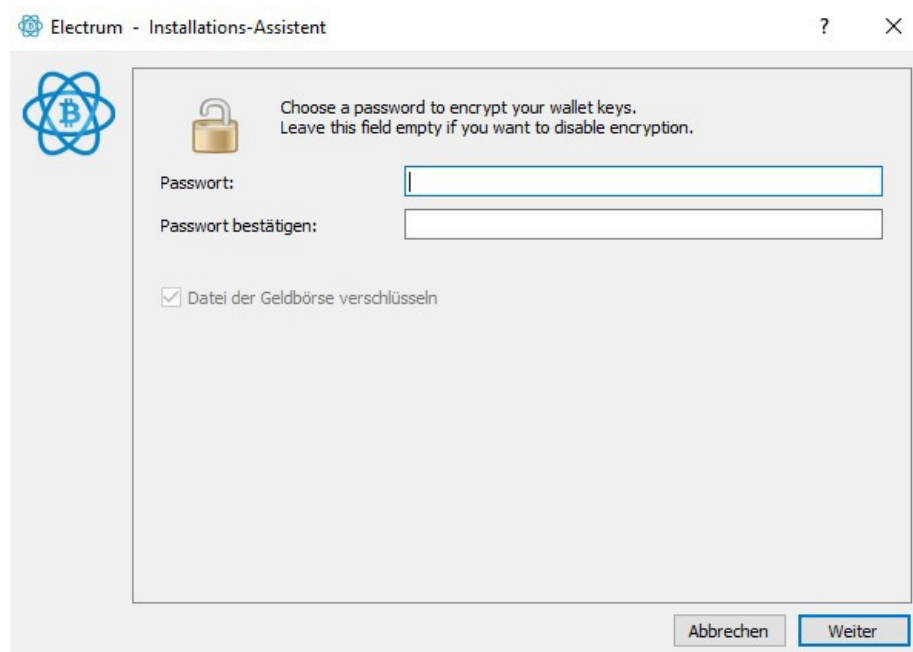
Hier könnt ihr eurer Wallet einen Namen geben sowie den Speicherort auswählen.



An dieser Stelle erhaltet ihr von Electrum einen "Seed" bestehend aus 12 Wörtern, die ihr euch unbedingt notieren müsst. Bewahrt den Seed sicher auf, denn damit könnt ihr von überall auf der Welt aus auf eure Bitcoins zugreifen, indem ihr bei der letzten Grafik einfach "Ich habe bereits einen Seed" anklickt und mit den 12 Wörtern wieder den vollständigen Zugriff auf eure Bitcoins wiederherstellt. Daher darf der Seed auf keinen Fall an andere weitergegeben werden!

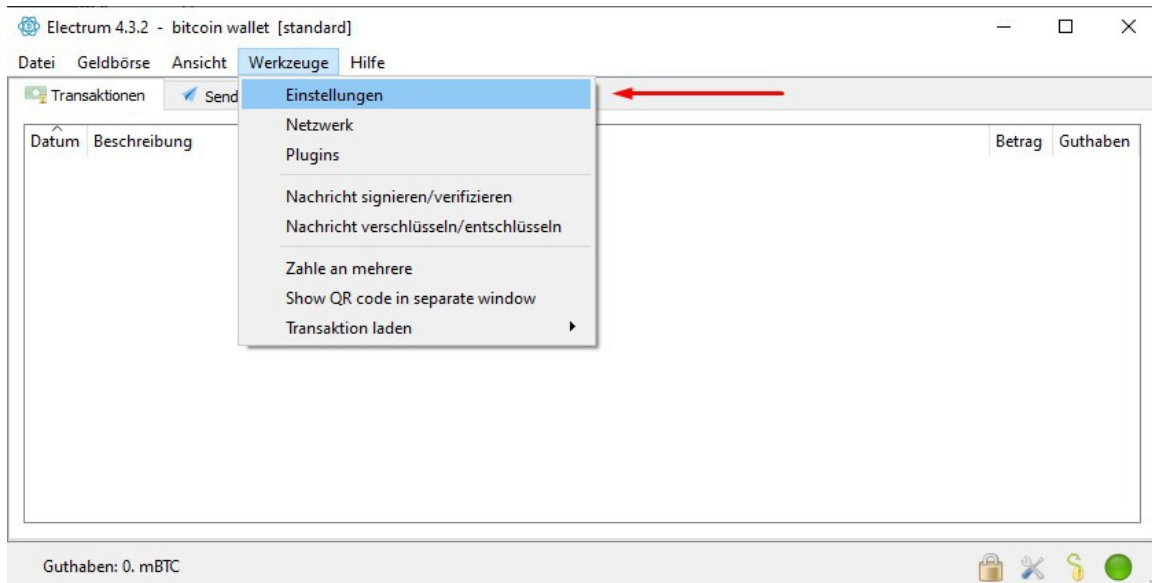


Danach müsst ihr den Seed zur Bestätigung einmal erneut eingeben.

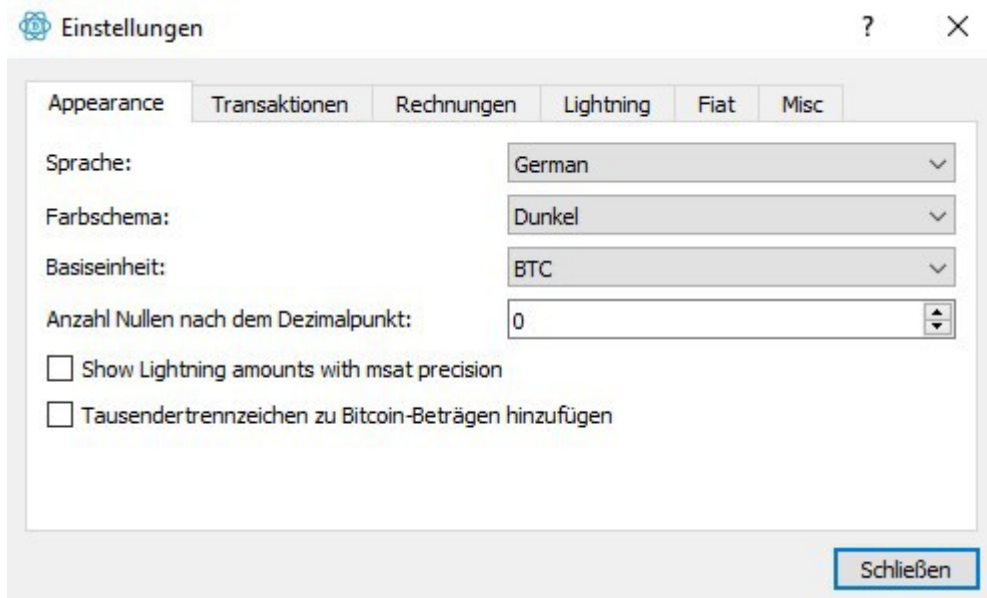


Zum Schluss der Installation vergebt ihr noch ein Passwort und bestätigt die Update-Prüfungsmeldung mit "Yes", um immer die aktuellste und sicherste Version zu nutzen.

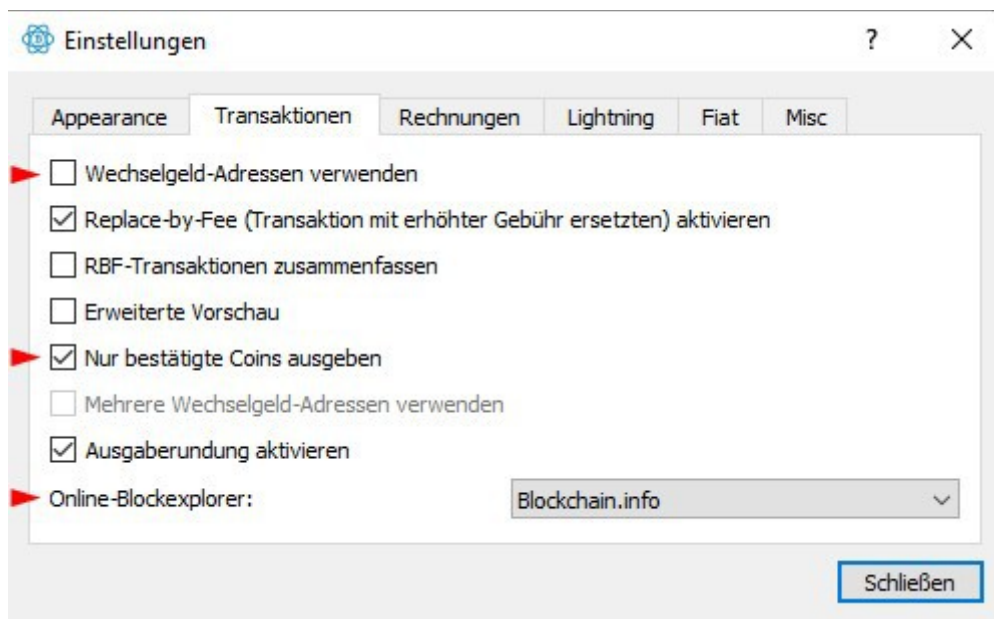
Nun konfigurieren wir noch kurz einige Einstellungen, um euch die Nutzung von Electrum so angenehm wie möglich zu gestalten. Dazu öffnet ihr die Einstellungen.



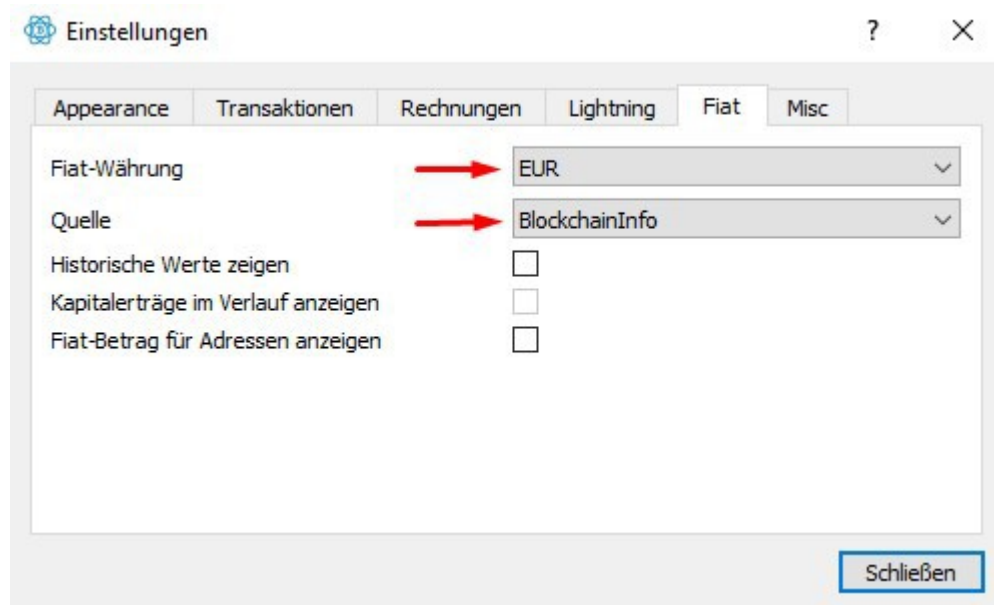
Als Farbschema finde ich das dunkle Design wesentlich angenehmer und als Basiseinheit nehmt ihr bitte "BTC".



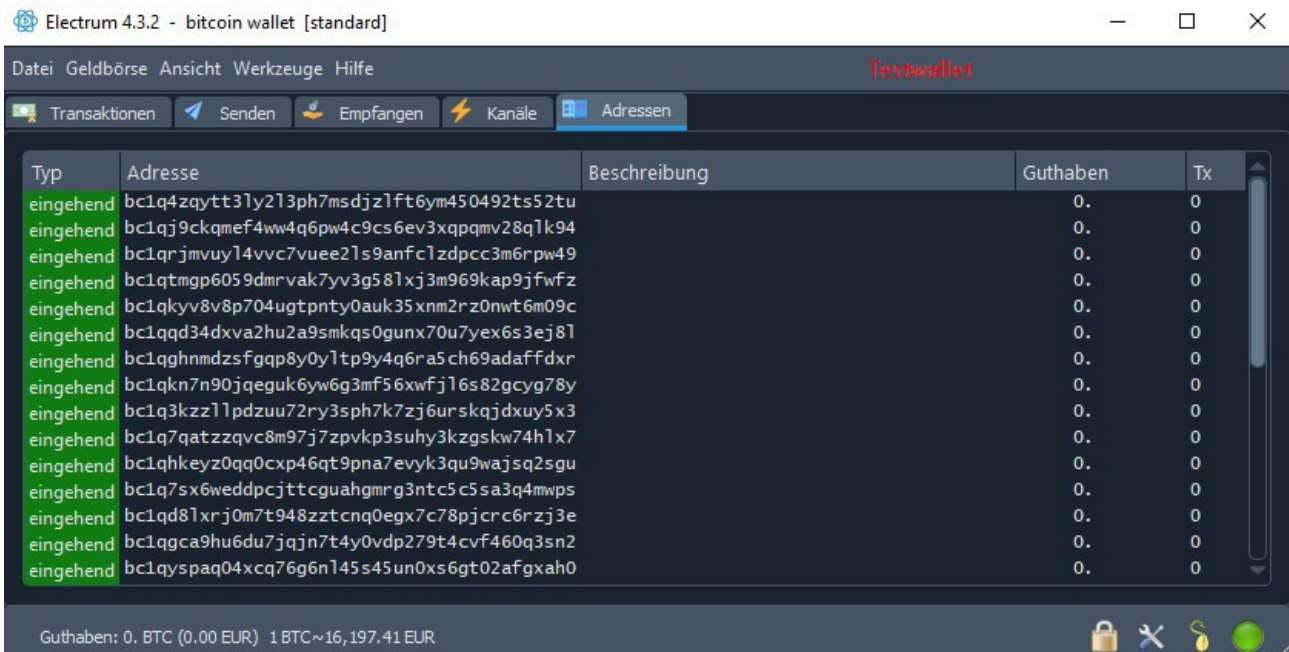
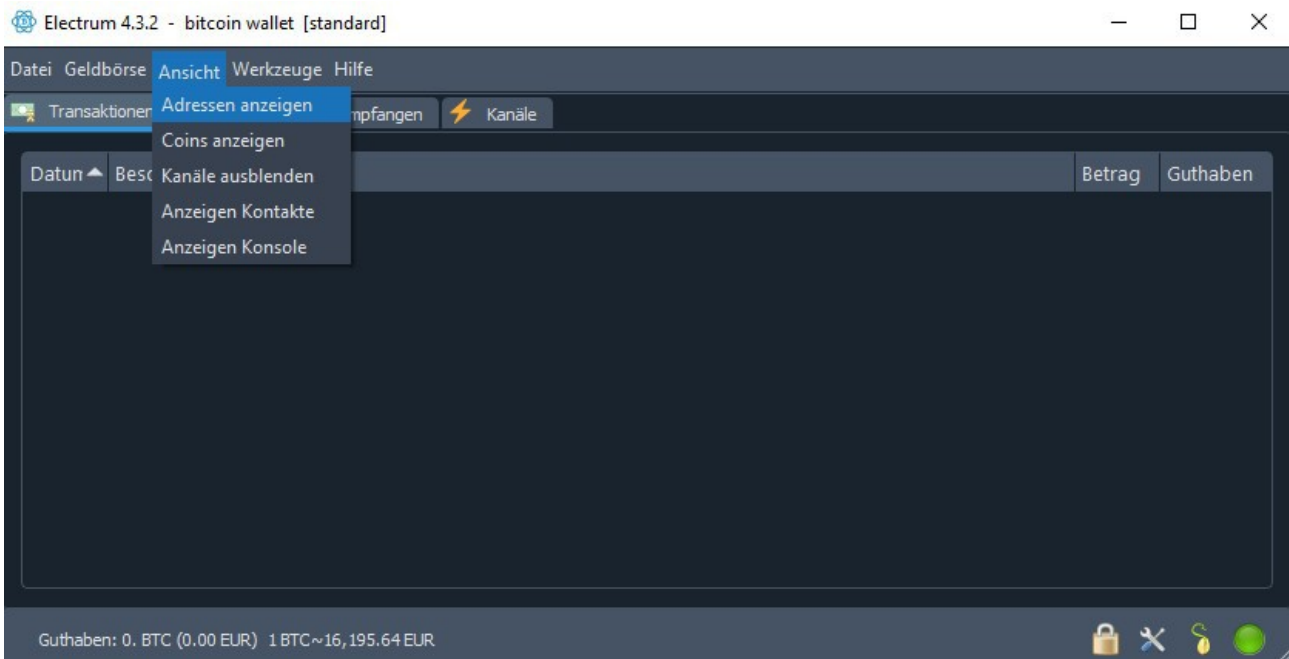
Im nächsten Reiter "Transaktionen" übernehmt ihr bitte die Einstellungen so wie sie auf dem folgenden Bild zu sehen sind. Wir wollen keine Wechselgeld-Adressen verwenden, weil dadurch sonst die Bitcoins nach jeder Zahlung auf eine neue Wallet Adresse von euch übertragen werden, was ziemlich nervig ist. Ohne diese Option verbleiben eure Bitcoins immer auf derselben Wallet Adresse, was die Nutzung nicht so kompliziert gestaltet und von mir bevorzugt wird.



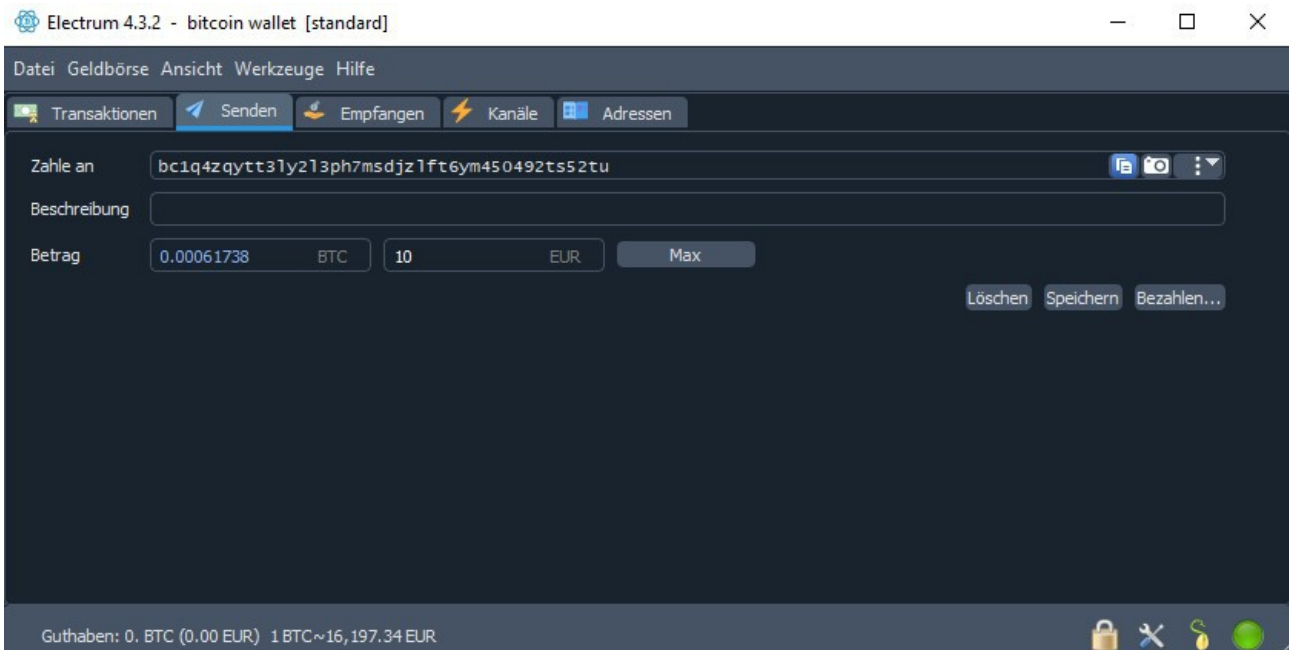
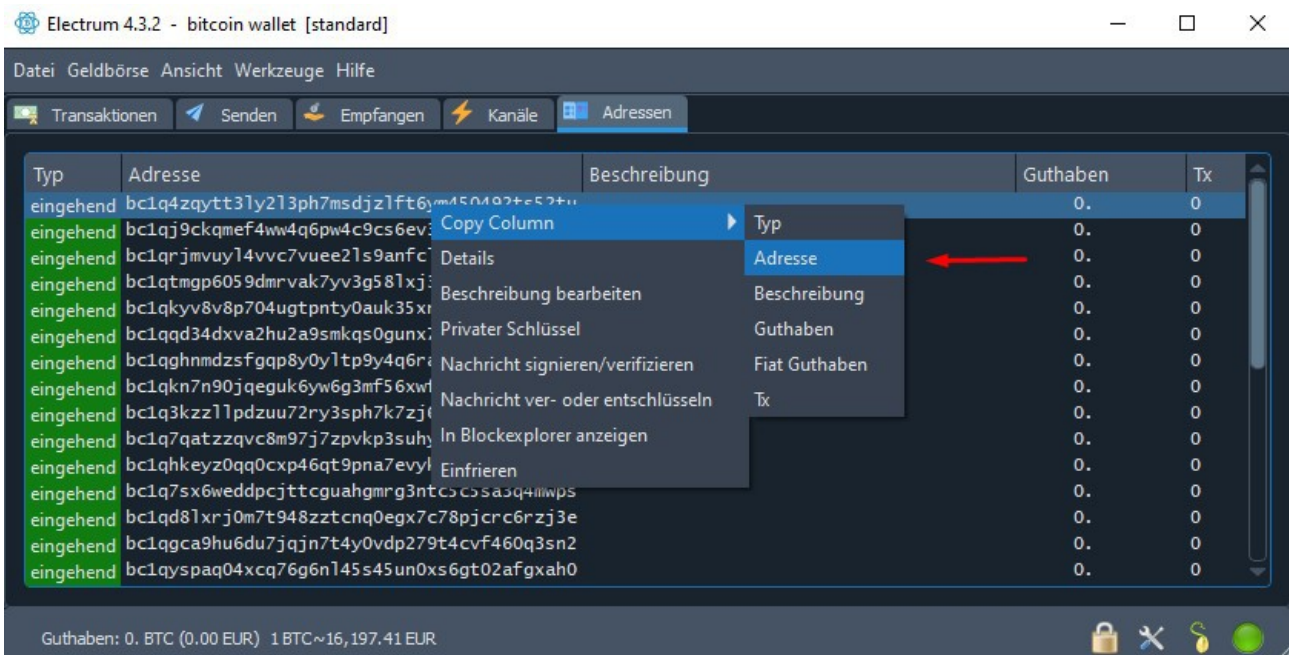
Auf dem folgenden Bild wählt ihr den Reiter "Fiat" an, um eure bevorzugte Währung sowie die Quelle der angezeigten Bitcoin Preise auszuwählen. Hier nehmt ihr bitte "EUR" für Euro und als Quelle wählt ihr BlockchainInfo (bzw. blockchain.info), weil dies in meinen Augen eine sehr authentische Quelle zum Anzeigen der Preise ist.



Nun müsst ihr Electrum einmal neu starten, damit die Einstellungen auch übernommen werden. Nach dem Neustart wird nun auch das für mich angenehmere dunkle Design angezeigt. Als nächstes erkläre ich euch, wie ihr Bitcoins selbstständig empfangen und versenden könnt. Dazu müsst ihr zuerst einmal oben auf "Ansicht" klicken und dann auf "Adressen anzeigen". Dies müsst ihr aber nur einmalig machen, weil ihr ab jetzt permanent auf alle eure Wallet Adressen zugreifen könnt unter dem neu hervorgerufenen Reiter "Adressen".



Unter dem Reiter "Adressen" bekommt ihr nun dutzende Bitcoin Wallet Adressen angezeigt. Diese Bitcoin Adressen gehören alle euch! Alle diese Bitcoin Wallets gehören zu eurer einen "Electrum Wallet" und können von euch genutzt werden, um Bitcoins zu empfangen oder zu versenden. Ihr könnt eine Bitcoin Adresse von euch rauskopieren, indem ihr einfach einen Rechtsklick drauf macht, dann auf "Copy Column" klickt und dann auf "Adresse" so wie im folgenden Bild angezeigt. Nun könnt ihr diese Bitcoin Adresse jemandem schicken, um darauf Bitcoins zu erhalten. Als Letztes zeige ich euch noch, wie ihr Bitcoins selber versenden könnt.



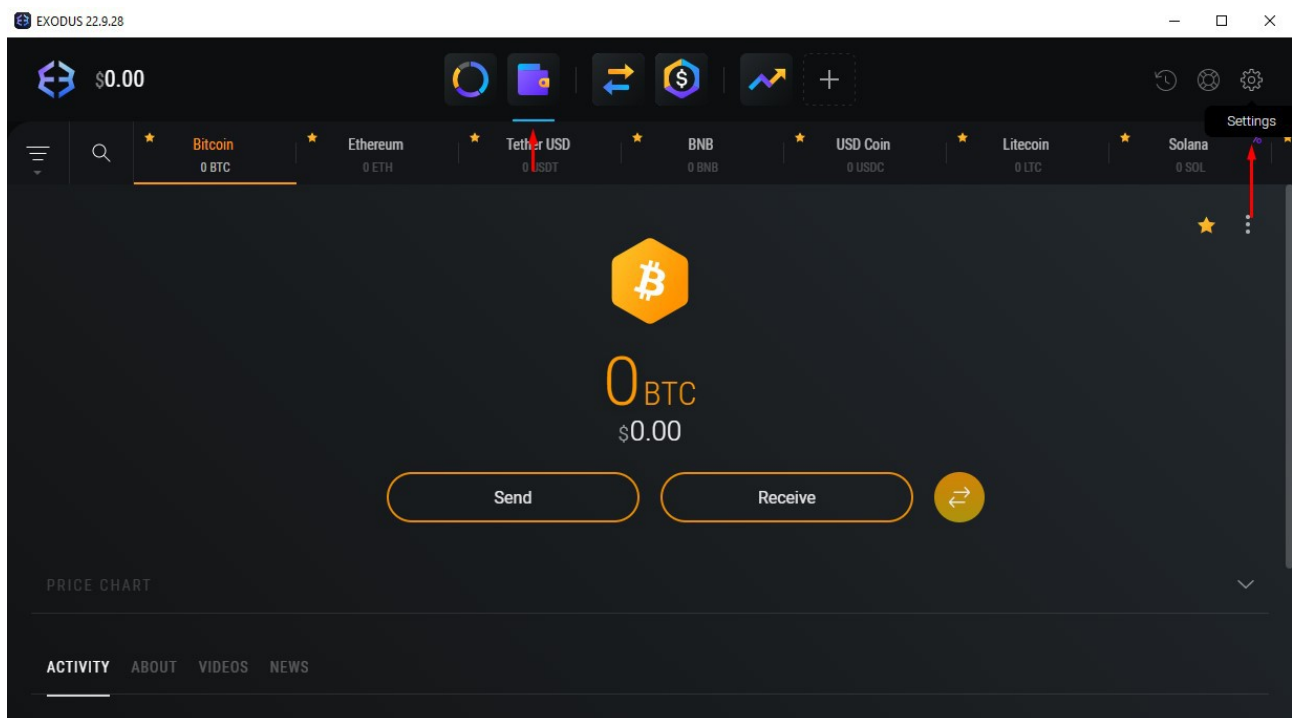
Um Bitcoins zu versenden, müsst ihr auf den Reiter "Senden" klicken. Dort gebt ihr dann als erstes eine Bitcoin Adresse ein, die eure Zahlung erhalten soll. Danach könnt ihr den Zahlungsbetrag in Euro oder BTC angeben. Mit einem Klick auf "Max" wird automatisch euer maximales Guthaben aus allen Wallets für die Zahlung verwendet. Nun klickt ihr auf "Bezahlen", wo ihr im letzten Schritt noch eine Transaktionsgebühr festlegen müsst und die Zahlung dann final bestätigt. Je niedriger die festgesetzte Gebühr ist, desto länger wird es dauern, bis eure Zahlung vom Bitcoin Netzwerk (nennt sich Blockchain) bestätigt wird. Man kann ungefähr sagen, dass alle 10 Minuten ein neuer "Bitcoin Block" bestätigt wird. Damit eure Zahlung also innerhalb von ein bis zwei Stunden bei eurer Zielperson ankommt, solltet ihr eine Gebühr festlegen, bei der die Zahlung bereits nach maximal 5 oder 10 Blöcken bestätigt wird.

Schritt 5: Exodus zum Verwalten von Kryptos einrichten

Exodus ist ebenfalls eine sehr empfehlenswerte und sichere Wallet, mit der man hunderte von Kryptowährungen gleichzeitig verwalten kann. Ihr könnt mit der Wallet auch problemlos eure Bitcoins verwalten, jedoch bevorzuge ich explizit für Bitcoins lieber Electrum, aber das ist jedem selbst überlassen. Die Installation von Exodus verläuft extrem ähnlich wie die Installation von Electrum. Ihr erhaltet beim Erstellen eurer Wallet einen Seed bestehend aus 12 Wörtern, mit dem ihr von jedem Rechner aus auf eure Exodus Wallet zugreifen könnt. Diesen Seed müsst ihr wieder unbedingt an einem sicheren Ort notieren und auf keinen Fall weitergeben. Nach der Installation habt ihr beim Starten von Exodus unter "Settings" und danach "Backup" die Möglichkeit, ein Passwort für eure Wallet zu vergeben. Mit einem Klick auf das "Wallet" Symbol könnt ihr dann auf alle verfügbaren Kryptowährungen zugreifen. Unter folgendem Link könnt ihr Exodus herunterladen:

<https://www.exodus.com/download/>

Beachtet bitte, dass es auch bei Exodus manchmal einige Sekunden oder Minuten dauern kann, bis die Wallet sich mit den verschiedenen Blockchains der Kryptowährungen "synchronisiert" hat.

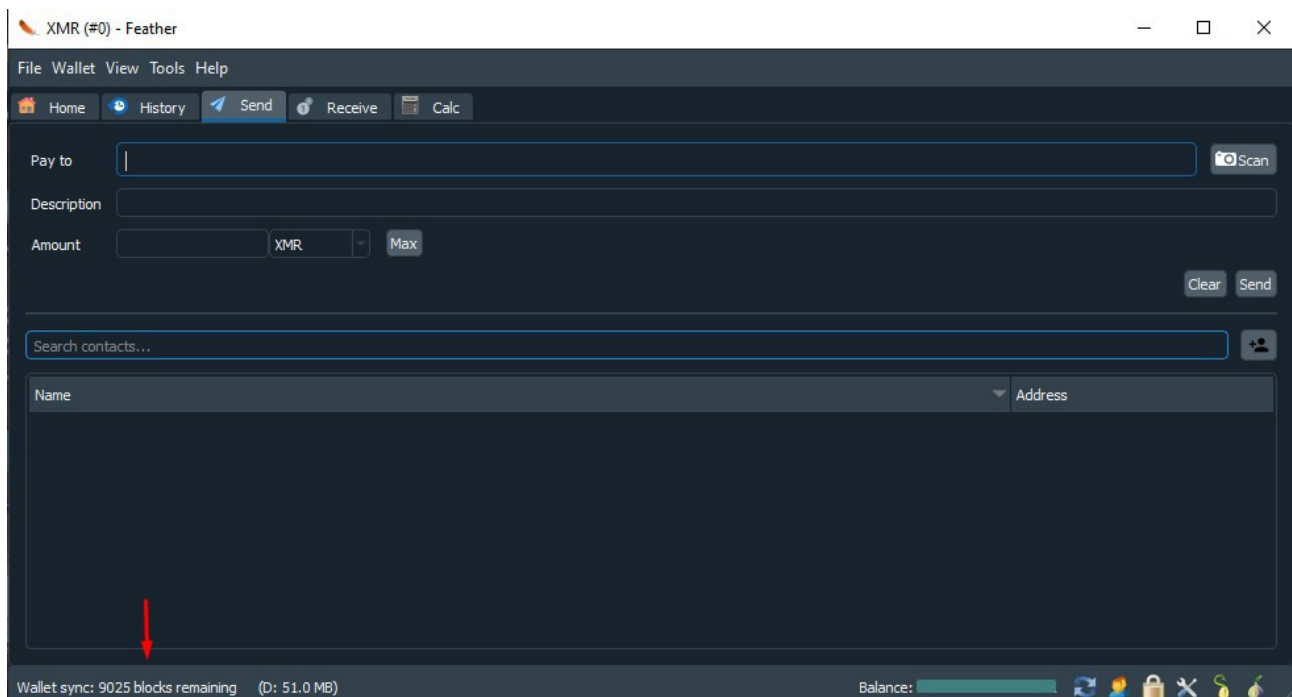


Schritt 6: Feather zum Verwalten von Monero einrichten

Zum Verwalten der Kryptowährung Monero (Abkürzung XMR) würde ich explizit die Feather Wallet empfehlen. Monero ist eine Kryptowährung mit einer extrem hohen Anonymität, weil Transaktionen **nicht** wie bei Bitcoins öffentlich von allen in der Blockchain nachgesehen werden können (unter <https://www.blockchain.com/explorer>). Die Installation von Feather verläuft wieder extrem ähnlich wie die Installation von Electrum. Ihr erhaltet einen Seed bestehend aus 16 Wörtern, den ihr an einem sicheren Ort notieren müsst, um von jedem Rechner aus auf eure Feather Wallet zugreifen zu können. Unter "Send" habt ihr die Möglichkeit XMR zu versenden und unter "Receive" könnt ihr euch eure Monero Adressen anzeigen lassen, wo euch andere Leute XMR draufsenden können. Ein Vorteil bei Monero ist, dass die Transaktionsgebühr immer unter 1 Cent beträgt und die Transaktionen auch immer innerhalb von wenigen Minuten vom Netzwerk bestätigt werden. Ich habe hier einmal den Download-Link der Feather Wallet für euch:

<https://featherwallet.org/download/>

Wichtig: Bei jedem Neustart von Feather muss die Wallet sich einmal mit der Monero Blockchain "synchronisieren". Ich habe dies auf dem folgenden Bild mit dem roten Pfeil markiert. Dies dauert immer einige Minuten, also nicht darüber wundern.



Schritt 7: Kryptowährungen exchange mit FixedFloat

Nun beherrscht ihr den Umgang mit den verschiedenen Wallets und seid bereit für das nächste coole Feature: <https://fixedfloat.com/>

FixedFloat ist ein sehr zuverlässiger Krypto Exchanger, dem ihre eure Coins anvertrauen könnt. Auf fixedfloat.com könnt ihr die meisten gängigen Kryptowährungen für eine niedrige Gebühr gegeneinander exchange, also austauschen. Die Exchangegebühr beträgt in der Regel nur maximal 1%, jedoch kann sie bei kleinen Beträgen und bestimmten Coins eventuell auch ein wenig höher ausfallen. Genaue Informationen über den ganzen Ablauf könnt ihr euch auf der Website im FAQ einholen. Die Benutzung der Website ist im Endeffekt sehr einfach: Auf der linken Seite wählt ihr die Kryptowährung aus, die ihr gerne versenden möchtet und auf der rechten Seite wählt ihr die Kryptowährung aus, die ihr im Gegenzug gerne dafür erhalten möchtet. Euch wird direkt beim Eingeben des Betrags bereits angezeigt, welchen Gegenwert an Coins ihr dafür erhalten werdet, also könnt ihr schon vor dem Exchange ausrechnen, wie viel Minus ihr an den Gebühren machen werdet, aber wie gesagt sind das in der Regel nur ca. 1% vom Gesamtwert. Danach müsst ihr noch eine Wallet Adresse für den Empfang der ausgetauschten Kryptowährung eingeben und bestätigt das Ganze mit "Jetzt austauschen". Es öffnet sich dann ein neues Fenster mit eurer Bestellung/Order. Ihr speichert an dieser Stelle bitte sofort den Link oben in der Browserleiste ab, damit ihr bei Problemen mit dem Exchange auch den Support kontaktieren könnt, falls ihr aus Versehen den Browser schliessen solltet. Der Link sieht z.B. so aus: fixedfloat.com/order/XYZXYZ

Bei jeder Order läuft ein Timer von 30 Minuten, um die Coins auf die angezeigte Wallet einzuzahlen, aber ihr braucht euch keine Sorgen zu machen, wenn der Timer mal abgelaufen ist, bevor ihr die Coins versendet habt. Sobald die 30 Minuten abgelaufen sind, erscheint bei jeder Order eine Meldung, dass ihr die Order mit einer entsprechenden Bestätigung auf 24 Stunden verlängern könnt, sodass der Exchange immer noch vollautomatisch ausgeführt wird, wenn ihr die Coins innerhalb von 24 Stunden auf die angezeigte Wallet sendet. Sollte FixedFloat einmal nicht funktionieren, habe ich hier eine zweite seriöse und zuverlässige Alternative für euch, wo man Kryptowährungen aller Art exchange kann: <https://changelly.com/de>

Nehmt euch unbedingt vor Fake-Seiten in Acht! Hier seht ihr einmal FixedFloat:

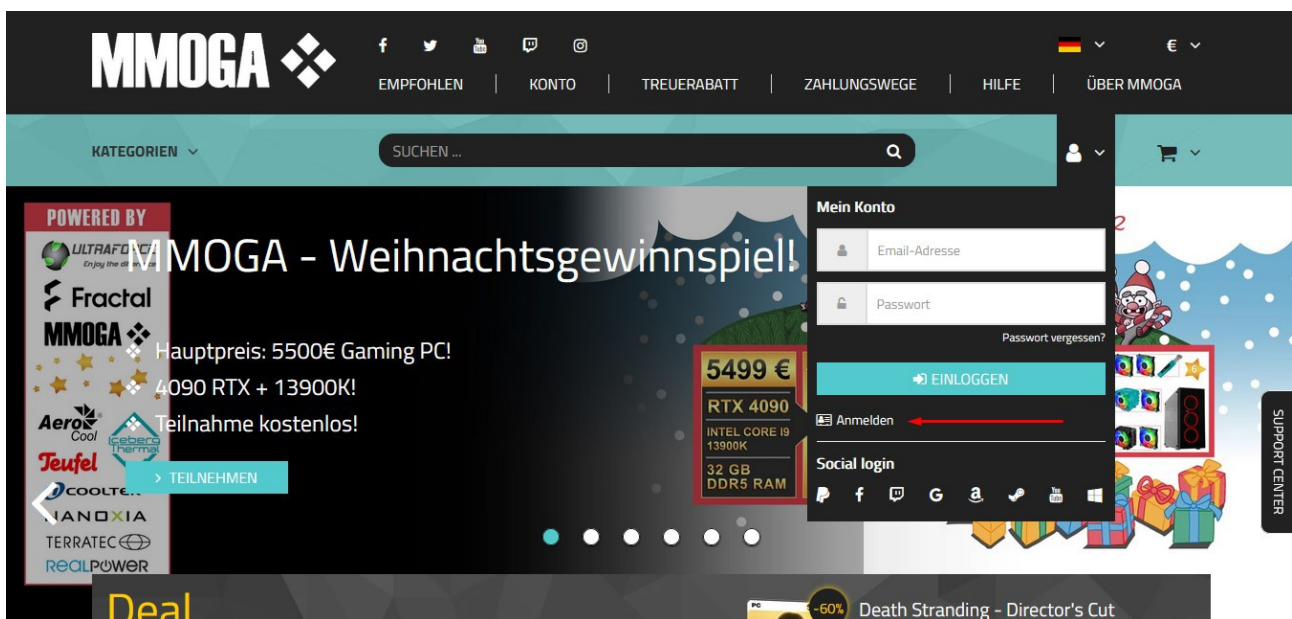


Schritt 8: Bitcoins mit Paysafecards erwerben

Im Folgenden erkläre ich euch eine effektive Methode, um mithilfe von Paysafecards schnell und stressfrei an Bitcoins zu kommen. Am Ende bleiben euch ca. 75% des Werts eurer Paysafecards erhalten, das heisst, ihr erhaltet 75% in Bitcoins vom Gesamtwert eurer Paysafecards. Paysafecards kann man online erwerben, z.B. auf:

<https://dundle.com/de/paysafecard/>

Dazu kann man Paysafecards an jeder Tankstelle und in den meisten Supermärkten kaufen. Im ersten Schritt geht ihr auf <https://www.mmoga.de/> und erstellt euch einen neuen Benutzeraccount. Dies dauert nur 2 Minuten und es wird auch keine besondere Kontoverifikation benötigt. Ihr müsst nur die Anmeldung einmal mit dem versendeten Link in eurem E-Mail Postfach bestätigen.



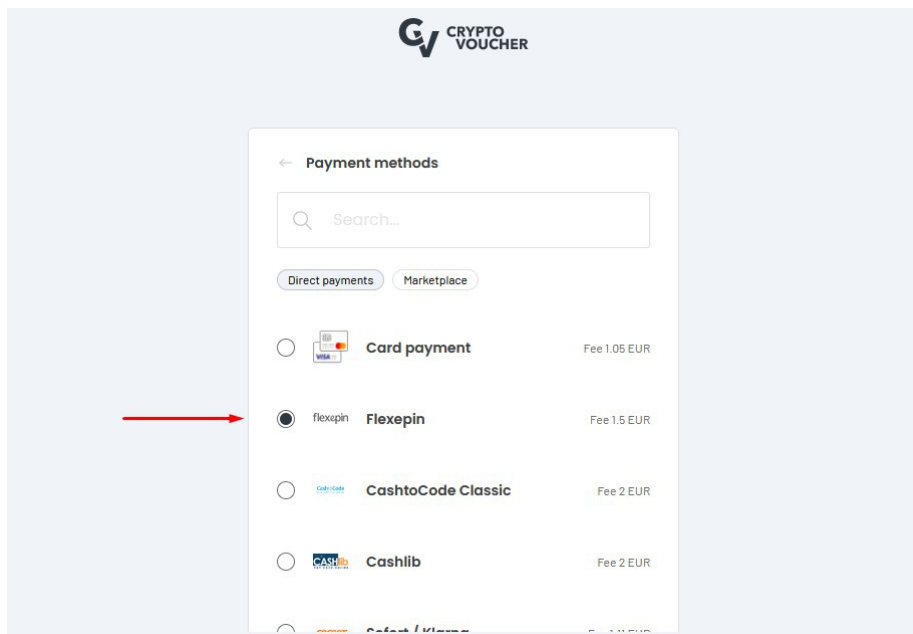
Danach könnt ihr direkt in der Suchleiste nach "Bitcoin" suchen und bekommt die verfügbaren Bitcoin Guthabekarten angezeigt. Um nicht in die manuelle Sicherheitsüberprüfung zu geraten, empfehle ich als erste Bestellung auf keinen Fall die 100€ Guthabekarte zu bestellen, sondern erstmal mit der 50€ Guthabekarte oder besser nur der 25€ Guthabekarte anzufangen. Bedenkt bitte, dass auf den angezeigten Betrag im Warenkorb beim Auschecken noch 7% Gebühren für die Zahlung mit Paysafecards draufkommen! Pro Account gibt es ein monatliches PSC Limit von 500€, ihr könnt also monatlich nur 500€ mit Paysafecards einzahlen. Dazu kann man bei MMOGA nur Paysafecard Codes mit einem Maximalwert von 50€ aufladen. Ihr könnt also keine PSC Codes mit einem Wert von 100€ bei MMOGA aufladen, sondern **pro jeweilige Aufladung immer nur maximal 50€**.

Eine weitere sehr wichtige Information: Ihr dürft beim Einlösen des PSC Codes auf gar keinen Fall eine VPN IP verwenden! Das System von Paysafecard erkennt automatisch, wenn man eine VPN IP verwendet und sperrt dann den eingegebenen Paysafecard Code weg, sodass er völlig unbrauchbar wird! Bitte aufpassen!

Nachdem ihr die Bitcoin Guthabekarte erfolgreich bezahlt habt, wird euch der Code in der Regel bereits nach wenigen Minuten in euren Bestellungen angezeigt und zusätzlich noch an eure E-Mail Adresse versendet. Mit diesem Code könnt ihr euch nun auf folgender Website eure Bitcoins abholen:

<https://cryptovoucher.io/>

Dazu wählt ihr zuerst den gewünschten Betrag und bestätigt das Ganze mit "Buy". Als Nächstes wählt ihr als Bezahlungsoption die Option "Flexepin" aus. Nun gebt ihr euren Code sowie eure E-Mail Adresse ein und im Anschluss könnt ihr direkt die Kryptowährung auswählen, die ihr gerne erhalten möchtet und eure Wallet Adresse für den Empfang der Coins eingeben. Nach der finalen Bestätigung erscheinen die Coins dann innerhalb von einigen Minuten auf eurer Wallet, sodass ihr nun frei darüber verfügen könnt. Speichert bitte noch oben den Link von eurer CryptoVoucher Bestellung ab, solange die Coins noch nicht bei euch angekommen sind (für Support).



Redeem your voucher to your preferred cryptocurrency. Easy, simple and secure.

1 Redeem 2 Transaction summary 3 Transaction completed

Enter the code (Crypto Voucher or Flexepin)

E-mail

Select all terms

* I acknowledge that I have read and fully agree to Crypto Voucher's Terms & Conditions.

I agree to receive marketing emails from Crypto Voucher.

CONTINUE

Schritt 9: VSIM-Anbieter für SMS-Verifikationen nutzen

Viele Websites fordern heutzutage eine zusätzliche Kontobestätigung in Form von SMS-Codes an euer Handy. Wenn man nun einen zweiten Account auf einer solchen Website erstellen möchte und keine zweite SIM-Karte zur Hand hat, steht man oft vor großen Problemen. Manchmal möchte man bestimmten Websites auch einfach nicht seine echte Handynummer preisgeben. Aus diesen Gründen gibt es zahlreiche VSIM-Anbieter, die uns bei der Überwindung dieses Hindernisses helfen. Meine beiden Favoriten sind diese beiden Anbieter:

<https://autofications.com/>

<https://sms-activate.org/en>

Mit einer Google-Suche findet ihr jedoch zahlreiche weitere Anbieter. Die Funktionsweise ist immer gleich: Ihr erstellt euch einen Account, ladet euer Guthaben mithilfe einer verfügbaren Zahlungsmethode mit 5-10\$ auf und könnt dann mehrere SMS-Verifikationen für alle möglichen Websites & Anbieter empfangen. Die Preise richten sich immer nach den jeweiligen Anbietern und betragen meistens 1-3\$ pro SMS. Beachtet jedoch, dass es sich immer nur um eine einmalige SMS-Verifikation handelt! Bei autofications.com werden verwendete Nummern in eurer Profilhistorie gespeichert und können manchmal sogar ein zweites Mal benutzt werden für einen weiteren SMS-Empfang vom gleichen Anbieter. Bei Google Accounts z.B. muss man nach einiger Zeit beim Login immer wieder seine hinterlegte Handynummer bestätigen, sodass Google Accounts auf diese Weise nicht für immer verifiziert und genutzt werden können.

SMS Verification Real Virtual

United Kingdom	United States
France	Hong Kong
China	Germany
Netherlands	Malaysia
Brazil	Indonesia
Russia	Ukraine
Spain	Philippines
India	New Zealand
Vietnam	Argentina
Poland	Sweden
Portugal	Romania
Turkey	Estonia

[Show all countries](#)

Amazon	\$1.5
Twitter	\$1.2
Plenty Of Fish	\$2
Discord	\$0.8
Microsoft/Hotmail	\$1.2
Instagram	\$1.5
Microsoft Azure	\$1.2
WeChat	\$1.5
Uber	\$1.2
Vinted	\$2
Netflix	\$3

Schritt 10: Bilder anonym versenden mit Exif Cleaner

Ihr solltet immer die EXIF-Daten aus euren Bildern entfernen, bevor ihr sie an jemanden online versendet! Die EXIF-Daten kann man auch als Metadaten bzw. Eigenschaften von Bildern bezeichnen. Das sind z.B. Angaben zu eurem Standort und zum verwendeten Gerät. Diese Daten werden von manchen Endgeräten automatisch zusammen mit jedem neuen Bild gespeichert! Das heisst, dass jede Person aus dem Internet theoretisch personenbezogene Daten von euch auslesen kann, wenn ihr die EXIF-Daten nicht vorher aus den Bildern entfernt! Daher müsst ihr zum anonymen Verschicken von Bildern immer vorher die EXIF-Daten entfernen, was zum Glück ein relativ einfacher Prozess ist. Dazu besucht ihr folgende Website:

<https://www.verexif.com/>

Wenn die Website mal nicht gehen sollte, könnt ihr gerne andere "Exif Cleaner" auf Google suchen. Auf verexif.com könnt ihr immer nur ein Bild einzeln umwandeln. Das heisst, ihr klickt auf "Durchsuchen" und wählt zuerst euer Bild aus. Dann klickt ihr auf "Quitar Exif" und wartet dann einige Sekunden, während die Website die EXIF-Daten aus eurem Bild entfernt. Nach ein paar Sekunden erscheint dann automatisch ein neues Download-Fenster, wo ihr euer umgewandeltes Bild wieder herunterladen und abspeichern könnt. Nun habt ihr erfolgreich die EXIF-Daten bzw. die Metadaten aus eurem Bild entfernt.

Übrigens kann man mit solchen Exif Cleanern auch die EXIF-Daten von PDF-Dokumenten entfernen. Hier habe ich zwei weitere Anbieter für euch, mit denen man die EXIF-Daten aus PDF-Dokumenten entfernen kann:

<https://www.metadata2go.com/>

<https://www.sejda.com/de/edit-pdf-metadata>

ELIGE TU FOTO

Selecciona la foto a la que quieres ver o quitar el Exif

Sube una foto: Keine Datei ausgewählt.

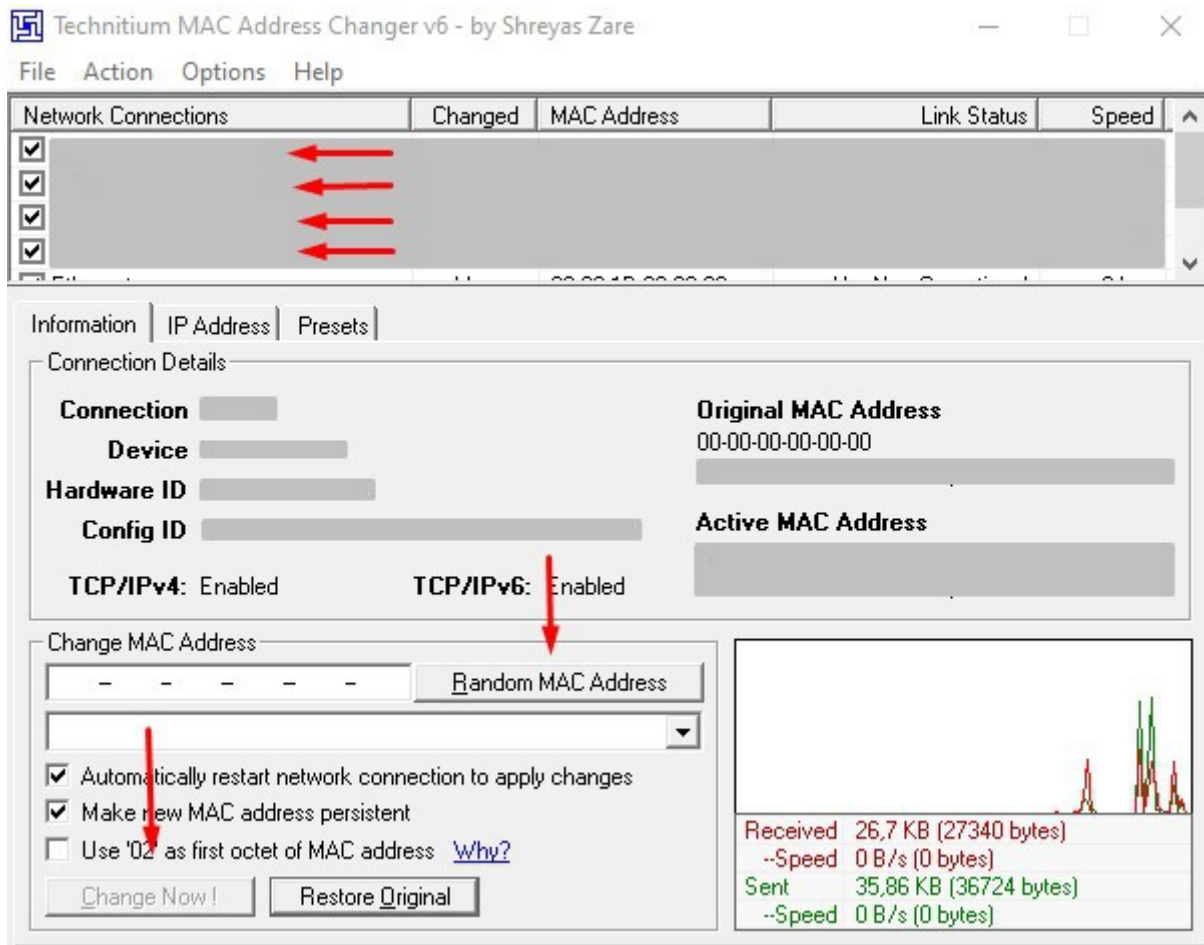
O pega la dirección de una foto en Internet:

- Para poder ver una foto online debe de ser pública. Si está en una web que requiere validación, como algunas redes sociales, deberás descargarla y subirla aquí.
- El tamaño máximo de la foto a subir son 20MB
- No conservamos copia de ninguna foto.

Schritt 11: Hardware ID ändern mit MAC Address Changer

Die MAC-Adresse bzw. Hardware ID ist die Nummer eines Gerätes auf einer Datenverbindung. Anhand dieser Nummer werden über die Verbindung laufende Daten den Geräten zugeordnet. Die MAC-Adresse dient quasi als eindeutiger Identifikator eures Geräts in einem Rechnernetz. Daher solltet ihr unbedingt **einmalig** die MAC-Adresse eures Rechners ändern, um eure Sicherheit beim Surfen zu erhöhen. Dazu ladet ihr euch bitte den folgenden MAC Address Changer herunter:

<https://technitium.com/tmac/>



Nun klickt ihr die Verbindungen jeweils einzeln an, geht dann auf "Random MAC Address" und bestätigt das Ganze dann mit einem Klick auf "Change Now!". Ihr könnt dann direkt in dem Fenster sehen, ob eure MAC-Adresse auch wirklich geändert wurde. Ab jetzt kann eure ursprüngliche Hardware ID nicht mehr ausgelesen werden.

Ihr seid nun am Ende des Tutorials angelangt. Ich bedanke mich fürs Lesen und hoffe, dass jeder einige wichtige Sachen für sich mitnehmen konnte. Viel Erfolg!