Manual für Electrum Bitcoin Wallet für Windows

Christopher Yoon

yoondeveloping@outlook.com

14. März 2024

Inhalt

Inhaltsverzeichnis

1 Einleitung

Das vorliegende Manual beinhaltet eine detaillierte Anleitung zur Installation, Konfiguration, Sicherung und Nutzung einer persönlichen Bitcoin Wallet für das langfristige Sparen und Investieren.[1] Darüber hinaus umfasst das Manual einen Überblick über die Grundlagen von Bitcoin, wie die Funktionen und Auswirkungen von Bitcoin, Marktdynamiken, die technischen Eigenschaften sowie die Sicherheit des Netzwerks.

Das Manual richtet sich primär an Bitcoin-Einsteiger und Interessierte, die ihr Vermögen langfristig sparen und anlegen möchten. Die technische Anleitung ist in einer Art und Weise gestaltet, dass auch Personen ohne technischem Hintergrundwissen den Ausführungen folgen können. Die technische Anleitung erklärt die Einrichtung und Nutzung der Wallet Schritt für Schritt mit Screenshots und detaillierten Beschreibungen. Tauchen bei der Einrichtung der Wallet Fragen oder Probleme auf, ist der Autor des Manuals per Email erreichbar.[2]

Im Vordergrund des Manuals steht keine Wallet für die tägliche Verwendung von Bitcoin, wie für die Bezahlung des Starbucks Kaffees oder anderer Ausgaben, sondern für die langfristige Aufbewahrung. Für Lösungen mit Fokus auf die alltägliche Verwendung wird man eher eine bequemere Konfiguration mit einem geringeren Sicherheitsaufwand implementieren. Auch die kurzfristige Spekulation mit Kryptowährungen ist nicht Teil des Manuals. Für solche Verwendungszwecke wird empfohlen, sich auf Krypto-Tauschbörsen anzumelden oder auf andere Lösungen zu setzen. Stattdessen wird die Verwahrung so konfiguriert, dass die Nutzer die vollständige Kontrolle über ihre eigene Wallet haben und die Wallet höchst mögliche Sicherheitsstandards erfüllt.

Für die Lösung im vorliegenden Manual wird die Open Source Wallet *Electrum* verwendet, die ausschließlich Bitcoins (BTC) verwaltet. Um einen hohen Sicherheitsstandard zu erfüllen, stützt sich die Lösung im vorliegenden Manual auf die Kombination mehrerer Konzepte und Sicherheitsmaßnahmen:

- Self-Custody (Selbstaufbewahrung)
- Cold-Storage (Offline-Aufbewahrung)
- 2-Faktor Authentifizierung (2FA)
- kryptographische Verschlüsselung

Darüber hinaus skizziert das Manual eine Strategie zur sicheren Aufbewahrung der Wiederherstellungsschlüssel. Dies inkludiert unter anderem eine Beschreibung der wichtigsten Risiken und Lösungsansätze zur Aufbewahrung der Schlüssel sowie eine konkrete Anleitung zur Nutzung eines Passwort-Managers. Zudem beinhaltet das Manual einige konkrete Tipps zur Sicherung des persönlichen Computers.

Bevor die Bitcoin-Wallet eingerichtet wird, empfiehlt es sich die Funktionen von Bitcoin und die technischen Begriffe und Grundlagen durchzulesen, um sich einen Überblick über das Bitcoin-Netzwerk zu verschaffen.

[1] Der Autor dieses Manuals übernimmt keinerlei Haftung für finanzielle Verluste, Verlust der Bitcoins, Verlust von Daten oder für die Beschädigung technischer Geräte. Auch für Folgeschäden und andere etwaige Schäden übernimmt der Autor keine Haftung. Dieses Manual dient der reinen Informationsweitergabe für den Privatbereich. Jeder Nutzer dieses Manuals ist dazu angehalten, die Informationen dieses Manuals selbst oder durch externe Experten zu überprüfen. Der Autor verfolgt keinerlei finanzielle Motive mit der Weitergabe des Manuals. Die Informationen wurden nach Anfrage von Freunden und Bekannten gesammelt und dokumentiert.

[2] yoondeveloping@outlook.com

2 Aufbau der Manuals

Das Manual besteht aus mehreren Teilen. In Kapitel 2 **Technische Voraussetzungen** wird ausgeführt, welche technischen Voraussetzungen für die Einrichtung der Wallet erforderlich sind, um dem Manual folgen zu können.

Kapitel 3 **Was ist Bitcoin?** befasst sich mit den Funktionen und Auswirkungen von Bitcoin aus ökonomischer, gesellschaftlicher, politischer und technologischer Sicht. Dieses Kapitel richtet sich vor allem an Einsteiger und Interessierte, die sich mit Bitcoin noch kaum beschäftigten. Hier stehen die Fragen im Mittelpunkt, welche Funktionen Bitcoin erfüllt und warum Bitcoin als eine disruptive Technologie betrachtet werden muss.

In Kapitel 4 **Begriffe und Grundlagen** befindet sich ein Überblick über die zentralen Begriffe und Themen im Bitcoin Space. Dazu zählen unter anderem Themen wie die Unterscheidung zwischen Bitcoin und Kryptos, die technischen Komponenten des Bitcoin-Netzwerks oder die Sicherheit des Bitcoin-Netzwerks.

Das Kapitel 5 **Grundlagen und Sicherheit der Wallet** gibt einen Überblick über verschiedene Arten von Wallets und deren Konfigurationen. Darüber hinaus wird das Sicherheitskonzept für die Wallet im vorliegenden Manual erläutert.

In Kapitel 6 **Erstinstallation von Electrum** beginnt der praktische Teil des Manuals, in dem wir Schritt für Schritt den USB-Stick verschlüsseln und die Wallet runterladen, installieren, konfigurieren und mit dem USB-Stick verlinken.

Kapitel 7 **Neuinstallation von Electrum** beschreibt die Verfahrensschritte, wenn der USB-Stick zwar noch intakt ist, allerdings sich das Electrum Programm nicht mehr auf dem Computer befindet. Dies kann dann der Fall sein, wenn der Computer neu aufgesetzt, ein neuer Computer gekauft oder das Programm deinstalliert wurde.

Das Kapitel 8 **Wiederherstellung der Wallet** umfasst eine detaillierte Anleitung zur Wiederherstellung der Wallet mithilfe der Seed Phrase (Wiederherstellungsschlüssel). Dies kann z.B. bei einem technischen Gebrechen des USB-Sticks der Fall sein, bei Diebstahl oder Verlust des USB-Sticks oder wenn man das Passwort für den Zugriff zur Wallet vergessen hat.

Im darauffolgenden Kapitel 9 **Aufbewahrung der Wiederherstellungsschlüssel** geht es um die sichere Verwahrung der Seed Phrase, mit der wir die Wallet bei Verlust, Diebstahl oder technischem Gebrechen wiederherstellen können. Die sichere Aufbewahrung der Wiederherstellungsschlüssel ist primär eine persönliche Angelegenheit und kann individuell gestaltet sein, allerdings werden im Kapitel allgemeine Risiken und Lösungsvorschläge diskutiert.

Das Kapitel 10 **Nutzung eines Passwort-Managers** beinhaltet eine Anleitung zur Installation, Konfiguration und Nutzung eines Passwort-Managers, mit dem wir Passwörter sowie die Seed-Phrase der Wallet verschlüsselt aufbewahren und verwalten können.

In Kapitel 11 **Sicherheit des Computers** wird eine Reihe an Risiken und Lösungsansätze der Cyber-Sicherheit diskutiert. Das Kapitel umfasst einerseits Maßnahmen zur technischen Sicherung des persönlichen Computers, andererseits Tipps zum sicheren Online-Verhalten.

Abschließend wird in Kapitel 12 **Nutzung der Wallet** beschrieben, wie Bitcoins empfangen, versendet, gekauft und verkauft werden können. Zudem gibt das Kapitel einen Überblick über ein paar wichtige Einstellungen der Wallet.

3 Technische Voraussetzungen

Für die Installation, Konfiguration, Sicherung und Nutzung der Bitcoin Wallet im vorliegenden Manual bedarf es einer Reihe an technischen Voraussetzungen. Folgende Voraussetzungen sind für die Einrichtung der Wallet erforderlich:

- Computer (Laptop oder PC)
- Windows Betriebssystem (Version 10 oder höher)
- Handelsüblicher USB-Stick oder externe Festplatte (ohne Daten)
- Internetverbindung
- Mobile Phone (Smart Phone)

Wer keinen freien externen Datenträger zur Verfügung hat oder lediglich eine Wallet einrichten möchte, die nicht offline auf einem USB-Stick gespeichert wird, kann dem Manual auch ohne USB-Stick folgen.

Um auch die Schlüssel für die Wiederherstellung der Wallet im Falle eines Verlustes des USB-Sticks sicher aufzubewahren, sollten weitere Voraussetzungen erfüllt sein, wie z.B. zusätzliche externe Datenträger oder sichere physische Aufbewahrungsmittel.

Sollten momentan keine weiteren externen Datenträger zur sicheren Aufbewahrung der Wiederherstellungsschlüssel zur Verfügung stehen, können die Wiederherstellungsschlüssel kurzfristig auch auf einem Blatt Papier festgehalten und aufbewahrt werden, um die Wallet einzurichten. Allerdings wird bei höheren Sparsummen davon abgeraten den Schlüssel auf Papier aufzubewahren. Siehe Kapitel 10 für eine Aufbewahrungsstrategie der Wiederherstellungsschlüssel.

4 Was ist Bitcoin?

Viele Menschen begegnen Bitcoin mit Skepsis und Unwissenheit. Wenn man sich allerdings mit dem Thema näher auseinandersetzt, kommt man zur Überzeugung, dass es sich bei Bitcoin um eine disruptive Technologie handelt, um die langfristig kein Weg vorbeiführt. Dies liegt nicht nur daran, dass Bitcoin eine *digitale* Form von Geld darstellt. Die Bedeutung von Bitcoin geht weit darüber hinaus.

Der folgende Abschnitt beschreibt die zentralen Funktionen und Auswirkungen von Bitcoin und beantwortet die Fragen, warum Bitcoin eine disruptive Technologie ist und warum es unausweichlich ist, sich mit Bitcoin auseinanderzusetzen.

Bitcoin ist ein digitales Tauschmedium

Grundsätzlich ist Bitcoin eine neue und bessere Form von Geld. Nun stellt sich die Frage: *Was ist Geld?* Geld ist eine Technologie, die das Problem der *Coincidence of Wants* (Koinzidenz von Bedürfnissen) der Tauschwirtschaft löst. Das Problem der *Coincidence of Wants* beschreibt die Herausforderung, dass ein Gegenüber das anbietet, was man selbst nachfragt und zugleich das nachfragt, was man selbst anbietet.

Um dieses Problem zu lösen, entwickelten sich im Laufe der Geschichte Tauschmedien, die den wirtschaftlichen Austausch effizienter machten und eine komplexere Arbeitsteilung ermöglichten. Erst durch Geld kann ein ökonomisches System von der Dimension einer kleinen Kommune zu einer globalen, komplexen Arbeitsteilung skaliert werden. Geld erleichtert also die räumliche Übertragung von Eigentum und den Austausch von Gütern.

Bitcoin ist eine vielfach bessere Technologie für die räumliche Übertragung von Eigentum als bisherige Tauschmedien. Eine der Funktionen des Bitcoin-Netzwerks ist es, weltweite finale Zahlungsausgleiche (Settlements) und die Übertragung von Eigentum sicher abzuwickeln und zwar in Lichtgeschwindigkeit und zu geringen Kosten, ohne auf riskante Transportwege oder Geschäfts- und Zentralbanken angewiesen zu sein. Bitcoins können fast überall auf der Welt empfangen und in lokale Währungen oder in andere Assets umgetauscht werden.

Kapitalverkehrskontrollen oder Transaktionsobergrenzen sind gegen Bitcoin wirkungslos. Bitcoins können rund um die Uhr und sieben Tage die Woche weltweit im Sekunden- oder Minutentakt versendet oder empfangen werden. Der Base Layer von Bitcoin dient als unmittelbarer Clearing Mechanismus für Zahlungsausgleiche, Second-Layer-Lösungen wie das Lightning-Netzwerk oder Third-Layer-Applikationen wie die Cash App ermöglichen kostengünstige Transaktionen im Alltag in Sekundenschnelle. Insgesamt ist Bitcoin ein mächtiges, monetäres Netzwerk für die räumliche Übertragung von Eigentum und den ökonomischen Austausch.

Bitcoin ist ein digitales Wertaufbewahrungsmittel

Die zweite Funktion von Geld ist die Funktion der Wertaufbewahrung – also die zeitliche Übertragung von Eigentum aus der Gegenwart in die Zukunft. Im letzten Jahrhundert wurden nominelle Vermögen wie fixe Gehälter, Bargeldreserven oder Versicherungs- und Pensionskassen von den Machthabern mehrmals vernichtet, indem die Geldmenge dauerhaft ausgedehnt und die Währungen zunehmend entwertet wurden. Dies gilt nicht nur für Papiergeldwährungen. Auch Gold oder Silber werden jedes Jahr in größeren Mengen gefördert.

Bitcoins hingegen sind nicht vermehrbar. Keine Person, kein Unternehmen oder kein politischer Machthaber hat die Möglichkeit, die Spielregeln zu ändern, die Geldmenge auszuweiten und somit Vermögen zu entwerten. Das Bitcoin-Protokoll definiert eine Obergrenze von 21 Mio. Bitcoins und ist in seinen Grundeigenschaften konservativ. Für die Integrität des Bitcoin-Protokolls sorgt die dezentrale Struktur des Netz-

werks, welches von 50.000 bis 80.000 Computern (Nodes) und tausenden von Rechenzentren (Minern) kryptographisch und unter dem Einsatz elektrischer Energie und Rechenleistung geschützt wird.

Bitcoin ist zudem kaum konfiszierbar oder zensierbar. Eigentum kann mithilfe von Bitcoin über Staatsgrenzen oder durch Kontrollen an Flughäfen in Sicherheit gebracht werden, ohne Gefahr zu laufen, enteignet zu werden. Immobilien, Aktien, Kunstgegenstände oder andere physische Wertaufbewahrungsmittel hingegen können ohne weiteres besteuert oder direkt konfisziert werden. Da Bitcoin eine Obergrenze von 21 Mio. Coins hat und nicht leicht konfisziert werden kann, ist Bitcoin auch eine um vielfaches bessere Technologie als konventionelle Wertaufbewahrungsmittel.

Bitcoin ist ein Investment

Die Attraktivität der Technologie, die disruptive Macht des Netzwerks und die interne, ökonomische Anreizstruktur führen dazu, dass wöchentlich 3 Mio. neue Nutzer dem Netzwerk beitreten. Zudem wird Bitcoin mithilfe von Second-Layer- und Third-Layer-Lösungen in zunehmendem Ausmaß in verschiedenste Applikationen integriert, wodurch eine wachsende Anzahl an Transaktionen auf das Bitcoin-Netzwerk verlagert werden. Aufgrund der steigenden Nachfrage, der wachsenden Anzahl an Applikationen, das zunehmende Transaktionsvolumen und der Obergrenze von 21 Mio. Bitcoins ist ein langfristiger Preisanstieg zu erwarten. Durch den langfristigen Preisanstieg verstärkt sich die Sogwirkung von Bitcoin noch zusätzlich.

Bis dato umfasst das Bitcoin-Netzwerk einen Anteil der ökonomischen Energie von weniger als 1% am weltweiten Gesamtvermögen. Allerdings ist zu erwarten, dass konventionelle Vermögensklassen wie Edelmetalle, Staatsanleihen und Aktien zunehmend demonetarisiert und auf das Bitcoin-Netzwerk umgeschichtet werden. Bei Gold ist die Demonetarisierung durch Bitcoin bereits beobachtbar. Darüber hinaus wurden im Jänner 2024 von der amerikanischen Aufsichtsbehörde Bitcoin-ETFs zugelassen, wodurch mehrere 1.000 Milliarden US-Dollar in den nächsten zehn bis fünfzehn Jahren in das Netzwerk fließen sollen.

Bitcoin bedeutet Fairness

Das Fiatgeldsystem schafft dauerhafte Gewinner und Verlierer und ist einer der Haupttreiber der wachsenden Schere zwischen Arm und Reich - ein Effekt, der auch als Cantillon-Effekt bekannt ist. Jene Akteure, die der „Druckerpresse“ nahestehen, wie staatliche Organisationen, staatsnahe Betriebe, Großbanken oder andere Finanzinstitutionen zählen zu den dauerhaften Gewinnern dieses Systems, da sie die Möglichkeit haben, Geld aus dem Nichts zu schaffen und diese ökonomische Energie (Geld) in politische Energie (Macht) zu transformieren.

Jene Menschen hingegen, denen der Zugang zur Druckerpresse verwehrt bleibt, gehören zu den dauerhaften Verlierern des Systems. Ihnen wird mit der ständigen Geldmengenausdehnung und der Entwertung des Geldes nach und nach der Sauerstoff entzogen. Im Jahr 2020 wurde der Cantillon-Effekt anschaulich dargestellt. Wallstreet machte im Jahr 2020 durch die Geldmengenausdehnung um 30% mehr Gewinn als im Vorjahr ohne einen Finger zu rühren, während „Mainstreet“ – also einfache Bürger und Klein- und Mittelbetriebe – durch die Geldentwertung Einkommens- und Vermögensverluste von bis zu 30% erleiden musste.

Bitcoin ist eine Alternative zum konventionellen Fiatgeldsystem, bringt Fairness in das System und zwingt die Machthaber zur Haushaltsdisziplin. Bitcoin sorgt dafür, dass das Geld entpolitisiert und die Politik demonetarisiert wird. Politisches Geld wird durch eine Engineering Lösung ersetzt, bei der sich alle an die selben Regeln halten müssen.

Bitcoin bedeutet Frieden

Die Geschichte des 20. Jahrhunderts belegt, dass Staaten die Druckerpresse ständig missbrauchten, um verheerende Kriege zu finanzieren. Sämtliche Kriege des 20. Jahrhunderts wurden mit der Druckerpresse in die Länge gezogen bis das gesamte Kapital der Gesellschaft vernichtet war. Es ist kein Zufall, dass das 20.

Jahrhundert sowohl das Jahrhundert des Fiatgeldes als auch das Jahrhundert des totalen Krieges war.

Bis zum Ersten Weltkrieg bestand das Geldsystem aus einem Goldstandard, wodurch Staaten zur Haushaltsdisziplin gezwungen wurden. Allerdings implizierte der Goldstandard den Nachteil, dass sich der Transport und die Zahlungsausgleiche zwischen den Banken sehr unsicher und teuer gestalteten und daher Zentralbanken erforderlich waren, in denen das Gold gelagert und die Ausgleichszahlungen durchgeführt wurden. Die zentrale Lagerung des Goldes ermöglichte es aber, dass Staaten mit einem Federstrich den Goldstandard abschaffen und das Gold konfiszieren konnten. Wer zuvor sein Gold zur Bank brachte, um es gegen eine Banknote einzutauschen, hatte nun Papier in der Hand statt Gold.

Ähnliches geschah vor Ausbruch des Zweiten Weltkrieges. Ob es Hitler oder Stalin war, die Machthaber nutzten ihr Geldmonopol und die Druckerpresse, um ihre mörderischen Regime zu finanzieren. Später wurde der Goldstandard unter dem Bretton Woods System aufgrund des Vietnam-Krieges aufgegeben. Seit 1971 ist das vorherrschende Geldsystem ein reines Fiatgeldsystem, das auch die Kriege danach finanzierte. Irak I, Afghanistan, Irak II, Libyen, Syrien, Jemen oder Somalien – keiner dieser Kriege wurde mit Steuererhöhungen finanziert, sondern mit der Druckerpresse.

Zukünftig wird der Bitcoin-Standard die Staaten in ihre Schranken weisen. Bitcoins werden nicht in einer zentralen Institution aufbewahrt, sondern sind in der Blockchain gespeichert, die auf zigtausenden Computern auf der ganzen Welt dezentral verteilt liegt. Wer unter einem Bitcoin-Standard einen Krieg führen möchte, muss mit seinen Steuerzahlern erst verhandeln. Ob die Bürger bereit sind, sinnlose Kriege mitzutragen und die Kosten für die irrationalen Machtinteressen der Politiker zu übernehmen, kann bezweifelt werden. Politiker werden damit gezwungen, an den Verhandlungstisch zu treten und Lösungen für Konflikte auf diplomatischem Wege zu erarbeiten.

Bitcoin ist Inklusion

Hunderten Millionen von Menschen ist gegenwärtig der Zugriff auf Bankkonten, Vermögensassets oder Fremdwährungen verwehrt. Entwicklungsländer leiden oftmals an Hyperinflation und können nicht auf Fremdwährungen ausweichen, da sie meist nicht in das internationale Geld- und Finanzsystem integriert sind. Verliert ein Bürger eines Hyperinflationslandes den Job, geht es oftmals um Leben oder Tod.

Bitcoin ist inklusiv, da es Zugang zum internationalen Finanzsystem schafft und die Möglichkeit zur Wertaufberwahrung bietet. Jeder Mensch kann sich ein Bitcoin-Konto eröffnen unabhängig von Geschäfts- und Zentralbanken und sein Einkommen vor der Hyperinflation schützen – eine Entwicklung, die bereits seit einiger Zeit in Ländern wie Simbabwe, Nigerien oder Libanon beobachtbar ist.

Aber auch im Westen wird es durch die Geldmengenausweitung und Inflation für jüngere Menschen immer schwieriger sich etwas aufzubauen. Die Kaufkraft der nominellen Einkommen und Vermögen schmilzt und immer mehr junge Menschen haben es schwer, ihre Karriereziele zu erreichen, für die Zukunft vorzusorgen, sich ein Eigenheim zu leisten oder eine Familie zu gründen.

Oftmals bleibt jungen Menschen nichts anderes übrig als sich bis auf die Knochen zu verschulden, um größere Investitionen tätigen zu können, wodurch sie jahrzehntelang in Kreditverträgen gefangen sind. Mit Bitcoin besteht nun die Möglichkeit, Einkommen zu sparen und die Kaufkraft ihres aufgebauten Vermögens über den Zeitverlauf zu steigern, ohne dass es durch Inflation entwertet wird.

Bitcoin ist eine Rückkehr zur Enthaltsamkeit und Sittlichkeit

Das Anreizsystem im Fiatgeldsystem führt dazu, dass gesellschaftliche Werte erodieren. Nicht nur haben Politiker mit dem Fiatgeld einen erheblichen Anreiz zur Zerstörung, da sie die Kosten ihres destruktiven Verhaltens auf die Allgemeinheit abwälzen können, auch auf gesellschaftlicher Ebene führt das Fiatgeldsystem zu selbstzerstörerischen Tendenzen.

Das Fiatgeld und die damit einhergehende Inflation tragen dazu bei, dass Menschen immer weniger Anreiz haben, sparsam mit ihrem Geld umzugehen, für die Zukunft vorzusorgen und auf Konsum zu verzichten. Zugleich steigen die Vermögenspreise, sodass Menschen kaum mehr in der Lage sind, sich Vermögen anzueignen. Anstelle des Sparens und der Enthaltsamkeit tritt Verschuldung und Überkonsum.

Bitcoin ändert die Anreizstruktur um 180 Grad. Wer regelmäßig seine Ersparnisse in Bitcoin tauscht und Jahr für Jahr sein Vermögen vermehrt, denkt über jede Konsumausgabe mindestens zweimal nach. Mit EUR 100.- in der Geldbörse steht man oftmals vor der Entscheidung, ob man diese EUR 100.- sofort verkonsumiert oder in Bitcoin umtauscht, um in einem Jahr Bitcoin im Wert von EUR 250.- in den Händen zu halten. Spart man Bitcoin, sind Preise deflationär und nicht inflationär.

In vielen Fällen fällt die Entscheidung für Bitcoin aus und man verzichtet auf den Konsum. Bald befindet man sich in einer Anreizstruktur, die frövelhaftes Verhalten mit Opportunitätskosten belegt und dadurch den Konsumverzicht gegenüber den Überkonsum fördert. Kapitalakkumulation ist nicht nur möglich, sondern sogar wahrscheinlich, womit sich auch die Prioritäten und Werte verschieben und es zu einer Rückkehr zur Enthaltsamkeit und Sittlichkeit kommt.

Bitcoin ist digitale Energie und Knappheit

Albert Einstein entdeckte mit seinem Äquivalenzprinzip, dass Masse und Energie zwei Seiten einer Medaille sind. Verbrennt man ein Stück Kohle, das sich aus Atomen mit einer bestimmten Masse zusammensetzt, wird die Materie in Wärme- und Lichtenergie transformiert. Geld kann als monetäre Energie betrachtet werden, da es in andere Energieformen oder in Materie umgewandelt werden kann. Geld kann bspw. für Arbeitskraft eingetauscht werden oder in chemische Energie, indem man Erdöl kauft. Oder man wandelt es in Materie um, indem man bspw. ein Haus kauft. Allerdings galt für die konventionellen Tauschmedien nicht das thermodynamische Prinzip der Energieerhaltung, da Geld dauerhaft entwertet wurde und die ökonomische Energie im Zeitverlauf verloren ging.

Ähnliches galt für die erste Welle der Digitalisierung, in der primär Informationen digitalisiert wurden, wie Bücher, Dokumente, Musik, Videos oder geographische Karten. Bis zum Aufkommen von Bitcoin konnten digitale Informationen ähnlich wie das Fiatgeld endlos kopiert werden, wodurch die Informationen an ökonomischer Energie verloren.

Bitcoins hingegen können aufgrund der Eigenschaften des Netzwerks nicht beliebig vermehrt werden, wodurch die ökonomische Energie erhalten bleibt. Es gilt also das thermodynamische Prinzip der Energieerhaltung. Bitcoin ist eine Engineering-Lösung für ein ökonomisches Problem basierend auf den Gesetzmäßigkeiten der Physik und der Mathematik und ist im Unterschied zum Fiatgeld kein politisches System, welches die physikalischen und mathematischen Gesetzmäßigkeiten missachtet.

Bitcoin bedeutet die Monetarisierung periphärer Energie

Bitcoin führte zu einer Revolution im Energiesektor, da das Bitcoin-Netzwerk periphäre Energiequellen weit weg von Ballungszentren monetarisiert. In vielen Ländern existieren Unmengen an Energie, die für den Menschen nicht nutzbar sind, da die Kosten für den Transport der Energie aus der Periphärie in die Ballungszentren zu hoch sind. Mit einem einfachen Satellitenanschluss und Bitcoin Mining Equipment kann das Bitcoin-Netzwerk die periphäre Energie monetarisieren und für jedermann nutzbar machen. Die Nutzung von Energie für das Bitcoin Mining zählt heute zu den lukrativsten Anwendungen von Energie.

Die Monetarisierung periphärer Energie ist eine Folge der ökonomischen Dynamik des Bitcoin-Netzwerks. Bitcoin Mining erfolgt hauptsächlich an jenen Orten, an denen ausreichend Energie zur Verfügung steht und die Kosten für Energie dementsprechend niedrig sind. Bitcoin monetarisiert somit nicht nur periphäre Energie, sondern ist auch keine Konkurrenz zum Energiebedarf in den Ballungszentren. Die Energie für das Bitcoin-Netzwerk ist Off-Grid und hat dadurch keinen Einfluss auf die Energiekosten der Allgemeinheit.

Bitcoin ist eine disruptive Technologie

Die Geschichte zeigt, dass sich bessere Technologien in der Regel gegen schlechtere Technologien durchsetzen. Bronze wurde durch Eisen abgelöst und Eisen durch Stahl. Steinwaffen wurden von Speeren abgelöst, Speere von Pfeil und Bogen, Pfeil und Bogen vom Schießpulver und Schießpulver von Atomwaffen. Auch in der Mobilität war die disruptive Macht der Technologie zu beobachten. Das Ruderboot wurde vom Segelschiff abgelöst, Segelschiffe von Dampf-betriebenen Schiffen und Dampf-betriebene Schiffe von Stahlfrachtern mit Dieselmotoren.

Bitcoin ist in allen Dimensionen eine bessere Technologie als vorherige Tauschmedien und Wertaufbewahrungsmittel und muss somit als disruptive Technologie eingeschätzt werden, die die alten Technologien zunehmend ablöst. Dass die Staaten ein Interesse daran haben, ihr Geldmonopol und den Zugang zur Druckerpresse aufrechtzuerhalten, ist verständlich. Auch die Kerzenhersteller lehnten elektrisches Licht ab und die Pferdezüchter das Automobil. Letztlich setzten sich aber die besseren Technologien durch. Bitcoin ist wie das Feuer oder die Mathematik. Es ist außerordentlich nützlich, anderen Technologien überlegen und verbreitet sich in rasanter Weise.

Wer sich in der Geschichte weigerte, das Schießpulver als eine überlegene Technologie gegenüber Pfeil und Bogen anzuerkennen, der musste mit seinem Leben bezahlen. So ähnlich ist es mit Bitcoin. Entweder man ignoriert Bitcoin und verarmt langfristig durch die Inflation oder man macht es sich zu Nutze und profitiert davon.

5 Begriffe und Grundlagen

5.1 Bitcoin versus Krypto

Im allgemeinen Sprachgebrauch wird Bitcoin als Kryptowährung bezeichnet und mit anderen Kryptos in einen Topf geworfen. Allerdings gibt es einen deutlichen Unterschied zwischen Bitcoin und Kryptowährungen, der sich in der Unterscheidung zwischen Property (Eigentum) und Security (Wertpapier) widerspiegelt. Bitcoin ist ein digitales Asset, welches allgemein als Eigentum eingestuft wird, wohingegen Kryptos in der Regel als Securities gelten. Die Unterscheidung zwischen Property und Security ist nicht unwichtig.

Der Bitcoin Supply hat eine maximale Obergrenze von 21 Mio. Coins und kann praktisch nicht verändert werden. Darüber hinaus ist das Bitcoin-Netzwerk weltweit dezentral auf tausenden Computern verteilt und wird von keiner zentralen Instanz oder von keiner einzelnen Person kontrolliert oder herausgegeben. Zudem bedeutet Eigentum, dass eine eindeutige Eigentumsbeziehung zwischen dem Inhaber und dem Asset besteht. Der Inhaber einer Bitcoin Wallet kontrolliert seinen eigenen Schlüssel, um auf sein Bitcoin Konto zuzugreifen und die Eigentumsbeziehung ist auf tausenden von Computern verteilt auf der Blockchain festgeschrieben und unveränderbar. Mit diesen Eigenschaften gelten Bitcoins als Eigentum.

Kryptos hingegen gelten als Securities und sind eine Art Wertpapier, aber ohne die rechtliche Absicherung und Transparenz eines öffentlichen Unternehmens an der Börse. Kryptos werden in der Regel von einer zentralen Entität wie einem Unternehmen oder einer Einzelperson herausgegeben und kontrolliert. Oftmals besteht zwar ein Netzwerk, welches zur Validierung der Transaktionen beiträgt, allerdings sind die Netzwerke um ein Vielfaches kleiner als das Bitcoin-Netzwerk und in der Regel kann das Protokoll vom Herausgeber der Coins mithilfe eines Schlüssels unilateral verändert werden. Somit sind nicht alle Teilnehmer des Netzwerks gleich. Im Unterschied zu Bitcoin können Krypto-Unternehmen die Transaktionen auf ihrer Blockchain rückgängig machen, die Geldmenge ausweiten, die Consensus-Parameter ändern, die Coins und deren Nutzen reprogrammieren oder Teilnehmer des Netzwerkes ausschließen und zensieren.

Bitcoin und Kryptos unterscheiden sich auch hinsichtlich ihrer Funktionen und ihrem Nutzen. Bitcoin gilt in der Regel als ein Wertaufbewahrungsmittel für langfristige Sparer und Investoren, die sich für die Zukunft absichern möchten. Da sich immer mehr Cash Balances aufbauen, kann Bitcoin auch zunehmend als Tauschmedium verwendet werden. Bitcoin hat ein eher geringes Risikoprofil. Kryptos hingegen sind eher kurzfristige Spekulationsobjekte und werden in der Regel lediglich auf Tauschbörsen akzeptiert. Kryptos haben daher ein eher hohes Risikoprofil.

5.2 Bitcoin-Netzwerk

Das Bitcoin-Netzwerk ist ähnlich wie das TCP Internet-Protokoll ein Open Source Protokoll, welches den Base Layer des Netzwerks konstituiert. Das Bitcoin-Protokoll ist eine Art genetischer Code des Netzwerks und definiert die Regeln und die Funktionsweise des Netzwerks. Jeder, der das Bitcoin Protokoll auf seinem Computer installiert hat und über einen Internetzugang verfügt, kann sich mit dem Bitcoin-Netzwerk verbinden. Alle Teilnehmer des Netzwerks sind gleichwertig und müssen sich denselben Regeln unterwerfen. Open Source bedeutet dabei, dass der Code des Protokolls für jedermann einsehbar ist und somit durch viele Programmierer-Augen auf Sicherheitslücken kontrolliert werden kann. In diesem Sinne ist das Bitcoin-Netzwerk egalitär und offen.

Das Protokoll ist in seinen Grundeigenschaften nur schwer veränderbar. Um ein Upgrade des Protokolls durchzuführen, bedarf es einer Zustimmung der Nodes und der Mehrheit der gesamten Rechenleistung

(Hashrate), die für das Netzwerk eingesetzt wird. Für Veränderungen des Protokolls braucht es also einen breiten Konsens, der abseits der grundsätzlichen Instandhaltung nur schwer zu erreichen ist. In diesem Sinne ist das Bitcoin-Netzwerk also konservativ.

Insgesamt setzt sich das Bitcoin-Netzwerk aus drei unterschiedlichen Typen von Teilnehmern zusammen: User, Nodes und Miners. Die User sind die Teilnehmer des Netzwerks, die das Bitcoin-Netzwerk für sich nutzen. Dies umfasst das Senden, Empfangen und Halten von Bitcoins. Die User interagieren mit dem Netzwerk in der Regel über eine Wallet oder indirekt über eine Applikation.

Die Nodes (Knoten) sind Computer oder Server, auf denen eine Kopie der Blockchain gespeichert ist und die in der Validierung von Transaktionen, der Einhaltung der Consensus Parameter und der Blockchain beteiligt sind. Meist werden die Nodes von Unternehmen betrieben, die Bitcoin handeln oder akzeptieren, aber auch Einzelpersonen betreiben Nodes. Weltweit wird eine Zahl zwischen 50.000 und 80.000 Nodes geschätzt.

Die Miners (Mienenarbeiter) bezeichnen leistungsstarke Rechner, die die Schwerarbeit der Validierung und Sicherung des Netzwerks übernehmen. Die Miners fassen die Transaktionen in einen Block zusammen und stehen im Wettbewerb zueinander, um für jeden Block ein mathematisches und kryptographisches Puzzle zu lösen. Ist das Puzzle von einem Miner gelöst, wird das Ergebnis von den Nodes kontrolliert. Der erste Miner, der den Block kryptographisch validiert, erhält vom Netzwerk eine Belohnung in Form der Transaktionsgebühren. Wofür diese kryptographischen Puzzles dienlich sind, wird im nächsten Abschnitt erklärt. Sowohl die Nodes als auch die Miners sind wichtige Komponenten zur Sicherung der Integrität des Netzwerkes.

5.3 Blockchain und Proof-of-Work

Ein zentraler Begriff des Bitcoin-Netzwerks ist die sogenannte Blockchain-Technologie. Die Blockchain ist die Datenbank, in der die Transaktionen und Eigentumsverhältnisse festgeschrieben werden. Die Blockchain ist also eine Art dezentrales Grundbuch, was auch der Grund ist, warum eine Blockchain als *Distributed Ledger* (Verteiltes Grundbuch) bezeichnet wird. Allerdings ist die Blockchain keine zentrale Datenbank auf einem Server, wie bei herkömmlichen Websites, sondern liegt auf zigtausenden Nodes auf der gesamten Welt verteilt, die ständig synchronisiert werden. Bei einer Blockchain werden die Transaktionen zu einem Block zusammengefasst. Jeder neue Block wird an den vorherigen Block angehängt. Im Bitcoin-Netzwerk ist die Anordnung der Blockchain aus kryptographischen Gründen und der Rechenleistung praktisch nicht veränderbar.

Die Nodes, die auf tausenden von Computern liegen und eine volle Version der Blockchain gespeichert haben, sind vernetzt und kommunizieren miteinander. Die Nodes spielen eine zentrale Rolle im laufenden Betrieb des Bitcoin-Netzwerks, da sie die Bitcoin-Transaktionen verarbeiten, vermitteln, validieren und schließlich an die Blockchain hinzufügen. Zudem sind die Nodes die Hüter des Protokolls und sind für die dezentrale Struktur des Netzwerks verantwortlich. Verarbeitet werden diverse Informationen einer Transaktion, wie die Adresse des Senders, die Adresse des Empfängers sowie die Transaktionshöhe. Auf den Nodes werden neue Transaktionen in einem sogenannten Mempool temporär gespeichert. Der Mempool beschreibt eine Art Warteschlange von Transaktionen, die erst validiert und an die Blockchain hinzugefügt werden müssen.

Doch bevor die Transaktionen an der Blockchain hinzugefügt werden, findet ein sogenanntens Mining (Schürfen/Mienenarbeit) statt. Dabei werden zuerst die Transaktionen von einem Miner eingesammelt und zu einem Block zusammengefasst. Um die Transaktionen zu validieren und an die Blockchain final hinzuzufügen, müssen die Miner eine Zahlenkombination (Nonce) finden und aus dieser Zahlenkombination gemeinsam mit anderen Informationen mithilfe eines kryptographischen Algorithmus einen sogenannten Hash berechnen. Dieser Hash muss niedriger sein als ein vom Protokoll festgelegter Zielwert. Erst wenn

dieser Hash vom Miner gefunden wurde, kann das Bitcoin-Netzwerk sicher gehen, dass physische Energie und Rechenleistung für das Mining eingesetzt wurde. Im Bitcoin-Netzwerk wird dieser Prozess auch als Proof-of-Work (POW) bezeichnet.

Der POW-Prozess beginnt mit der Festlegung eines nummerischen Zielwertes durch das Bitcoin-Protokoll. Der Zielwert wird durch eine 256-Bit Nummer repräsentiert und bestimmt den Schwierigkeitsgrad des kryptographischen Puzzles. Teil der Festlegung des Zielwertes ist das sogenannte Difficulty Adjustment (Schwierigkeitsadjustierung). Beim Difficulty Adjustment wird der Schwierigkeitsgrad des kryptographischen Puzzles je nach Geschwindigkeit der Miner angepasst. Werden die Blöcke zu schnell gemined, wird vom Protokoll der Schwierigkeitsgrad erhöht, sind die Miners zu langsam, wird der Schwierigkeitsgrad gesenkt. Unterm Strich wird der Zielwert so angepasst, dass in etwa alle 10 Minuten ein neuer Block gemined wird.

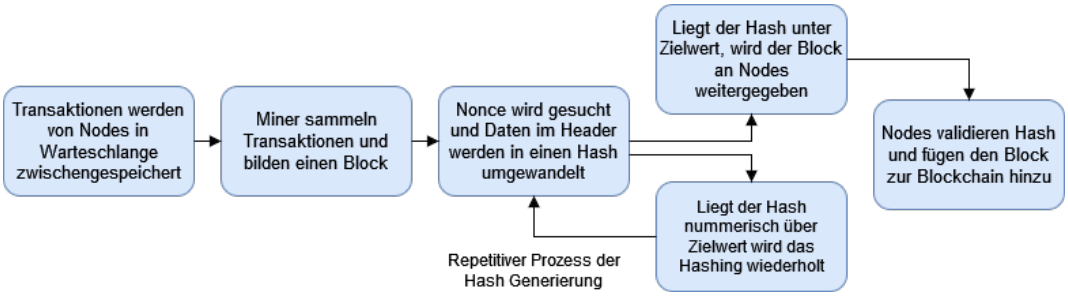


Abbildung 1: High-Level Prozess des Minings (Quelle: Eigene Darstellung)

Auf Seiten der Miners beginnt der Mining Prozess mit der Erstellung eines Block-Templates, das die Transaktionen und eine Kopfzeile (Header) mit Meta-Daten beinhaltet. In der Kopfzeile befinden sich verschiedene Informationen, wie ein Zeitstempel, der kryptographische Hash des vorherigen Blocks und eine kryptographische Nonce (32-Bit Nummer), die zu Beginn des Mining-Prozesses eine leere Variable darstellt und für das Lösen des Puzzles wichtig ist. Zuerst wählt der Miner eine Nonce und setzt diese in die Kopfzeile ein. Die Informationen in der Kopfzeile werden zusammengefügt und mithilfe des SHA-256d Algorithmus in einen Hash umgewandelt. Der Output des Hashing Algorithmus ist eine Zahlen- und Buchstabenkombination mit einer fixen Länge, die als Zahl ausgedrückt werden kann. Liegt der Hash nummerisch unter dem Zielwert, der vom Protokoll vorgegeben wurde, so wird der Block validiert. Liegt der Hash über dem Zielwert, ändert der Miner die Nonce im Block Header und wandelt die Sequenz im Header erneut in einen Hash um. Die Nonce wird im Rahmen eines Trial-and-Error Prozesses solange geändert und gemeinsam mit den anderen Informationen in einen Hash umgewandelt bis der Output des Hashing Algorithmus nummerisch unter dem vorgegebenen Zielwert des Protokolls liegt. Wurde eine Nonce gefunden und ein Hash generiert, der unter dem Zielwert liegt, wird der Block zurück an die Nodes gesendet, die den Block und den Hash validieren und an die bestehende Blockchain anhängen.

Der POW-Prozess ist einer der wichtigsten Komponenten für die Integrität des gesamten Netzwerks. Der POW-Algorithmus ist eine Schnittstelle zwischen der physischen und digitalen Welt. Die Genialität dahinter ist, dass der POW-Algorithmus einen *physischen* Cyber-Security-Layer bildet, der Angreifern hohe Kosten in Form von Energie und Rechenleistung auferlegt. Je mehr Rechner am Mining Prozess teilnehmen, desto mächtiger ist das Netzwerk und desto schwieriger ist es, das Netzwerk anzugreifen. Der POW-Algorithmus stellt hiermit sicher, dass keine zentrale Instanz das Netzwerk übernehmen und die Blockchain manipulieren kann. Der Proof-of-Work Algorithmus ist Teil der sogenannten Consensus Parameter, die festlegen, wie das gesamte Netzwerk einen Konsens erreicht und wie die Transaktionen und die Blockchain validiert werden.

5.4 Sicherheit des Netzwerks

Das Bitcoin-Netzwerk operiert seit 2009 in reibungsloser Art und Weise und demonstrierte eine einzigartige Resilienz und Robustheit, wodurch Bitcoin zu den sichersten Netzwerken der Welt zählt, die jemals vom Menschen geschaffen wurden. Mehrere Komponenten und Eigenschaften des Netzwerks sorgen für die Sicherheit des Netzwerks. Dazu zählen (1) die dezentrale Struktur des Netzwerks, (2) die kryptographische Sicherung, (3) die eingesetzte Energie und Rechenleistung, (4) die Größe des Netzwerks sowie (5) die ökonomischen und logistischen Anreize für die redliche Teilnahme am Netzwerk.

In der Theorie wurden verschiedene Angriffsvektoren identifiziert, über die das Netzwerk potentiell attackiert werden könnte. Allerdings sind die Angriffsszenarien eher theoretischer Natur, da in der Praxis erfolgreiche Attacken äußerst unwahrscheinlich sind. Ein bekannter Agriffsvektor ist eine sogenannte 51% Attacke, die sich dadurch charakterisiert, dass ein einzelner Miner oder eine Gruppe an Minern mehr als 50% der Hashrate (Rechenleistung) des gesamten Netzwerks kontrolliert. Wäre dies erreicht, hätten die Angreifer die Möglichkeit, die Blockchain zu manipulieren, Transaktionen rückgängig zu machen oder einzelne Bitcoins doppelt auszugeben.

Eine weitere Angriffsstrategie sind sogenannte Sybil-Attacken, bei der ein Angreifer mehrere Fake Identitäten kreiert und die Kontrolle über einen Teil der Nodes übernimmt. Aber auch Sybil-Attacken sind aufgrund der dezentralen Struktur des Netzwerks, den kryptographischen Mechanismen und den dafür eingesetzten Ressourcen unwahrscheinlich. Um Sybil-Attacken erfolgreich durchzuführen, bedürfte es einer Mehrheit der Hashrate des gesamten Netzwerks. Zudem sind Sybil-Attacken auch nur dann effektiv, wenn es im Netzwerk zentrale Instanzen gibt.

In der Praxis sind derartige Attacken aus mehreren Gründen äußerst unwahrscheinlich. Die Rechenleistung des Bitcoin-Netzwerks stützt sich auf ungefähr 12-15 Gigawatt an elektrischer Energie und um die 600 Exahash an Rechenleistung. Die Abbildung unten zeigt die Entwicklung der Hashrate, also der Rechenleistung, die das Netzwerk vor Angriffen schützt.

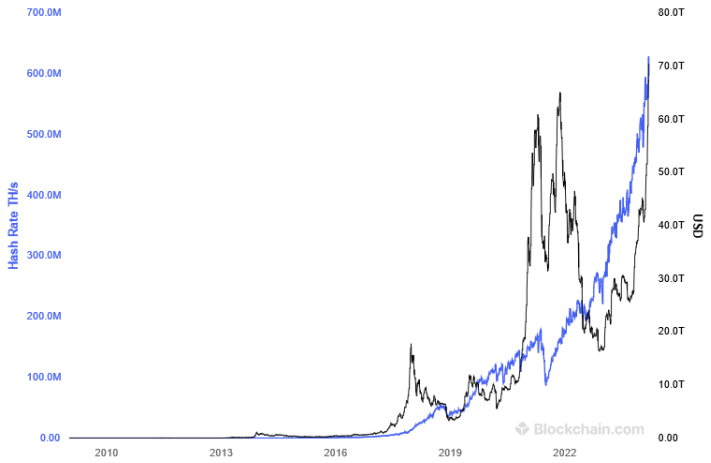


Abbildung 2: Entwicklung der Hashrate (blau) und Bitcoin Preises (black) (Quelle: https://blockchain.com)

Doch was bedeuten diese Zahlen konkret? Oftmals wird argumentiert, dass sich das Dollar-System auf die Macht der US-Navy stützt. Die US-Navy besteht aus 53 Virgina-class U-Booten mit jeweils 30 Megawatt (1590 Megawatt), 14 Ohio-class Ballistic Missile U-Booten mit jeweils 45 Megawatt (630 Megawatt), 11

nuklearbetriebene Flugzeugträger mit jeweils 195 Megawatt (2145 Megawatt), 17 Cruisers mit jeweils 60 Megawatt (1020 Megawatt) und 62 Destroyers mit 30 Megawatt (1860 Megawatt). Insgesamt stützt sich die Sicherheit des Bitcoin Netzwerks also auf doppelt soviel Energie wie der gesamte Energiebedarf der US-Navy. Darüber hinaus ist die benötigte Energie dezentral auf der gesamten Welt verteilt und hat keinen Single Point of Failure.

Doch Energie alleine reicht nicht. Die Energie muss auch in Rechenleistung transformiert werden. Im Bitcoin-Netzwerk werden die 15 Gigawatt Energie in 600 Exahash an dezentraler Rechenleistung von Sillicon Asics Rechnern umgewandelt, die durchschnittlich um das vielfache besser sind als Personal Computer. Angesichts dieser Dimensionen ist es unwahrscheinlich, dass eine 51%-Attacke in der Praxis realisierbar ist, da das Netzwerk mittlerweile zu groß und zu stark ist, um von Angreifern übernommen zu werden.

Eine Befürchtung ist, dass sich die Miners zu größeren Pools zusammenschließen und gemeinsam das Netzwerk attackieren. Allerdings ist zu berücksichtigen, dass die einzelnen Miners aufgrund der ökonomischen Anreizstruktur und aus spieltheoretischen Gründen kein Interesse haben, das Netzwerk zu attackieren. Warum sollte man hohe Summen in Energie und Rechenleistung investieren und die Integrität des Netzwerks zerstören, wenn eine redliche Teilnahme am Mining Prozess hohe Returns abwirft? Es macht also aus ökonomischer Sicht keinen Sinn für Angreifer, das Netzwerk zu korrumpieren. Bereits mehrmals in der Geschichte des Bitcoin Minings erreichten Mining Pools beinahe mehr als 50% der Rechenleistung und starben in weiterer Folge, da die Miners den Pool wechselten. Dennoch ist die Zentralisierung der Mining Pools eine legitime Befürchtung, an der zukünftig gearbeitet werden muss, wie etwa durch die Dezentralisierung der Template Konstruktion.

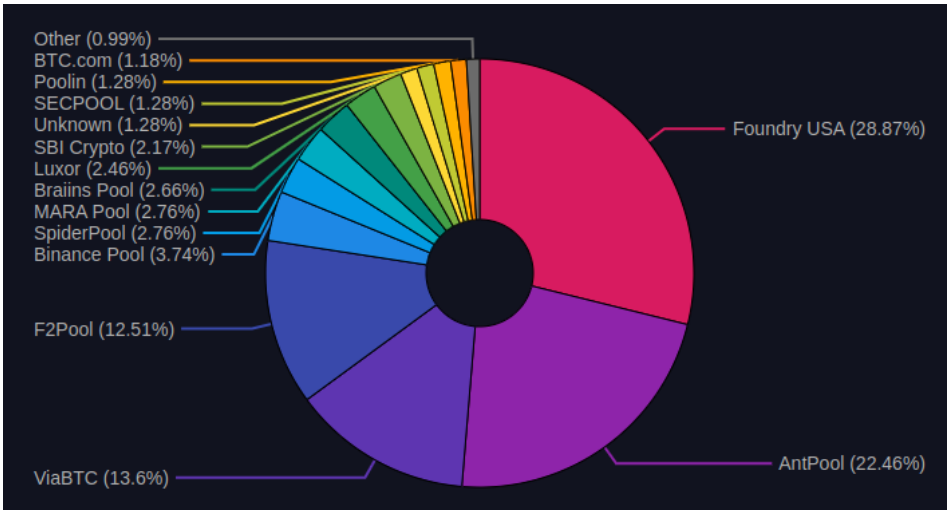


Abbildung 3: Bitcoin Mining Pools (Quelle: https://mempool.space/graphs/mining/pools)

Eine Problematik, die in der Bitcoin-Szene diskutiert wird, ist die Entwicklung von Quantencomputern, deren Rechenleistung gegenwärtige kryptographische Methoden leicht durchbrechen könnten. Quantencomputer können nicht nur eine Bedrohung für das Netzwerk selbst sein, sondern auch für die Elliptic Curve Cryptography (ECC), die für digitale Signaturen von Wallets eingesetzt wird. Allerdings ist Bitcoin das sicherste Netzwerk im Cyberspace und bevor Quantencomputer eine Bedrohung für das Bitcoin-Netzwerk darstellen, werden Netzwerke wie Google, Facebook oder Amazon attackiert.

Auch wenn die Zukunft der Quantencomputer ungewiss ist und die derzeitigen Prototypen noch ganz am Anfang stehen, wird unter Bitcoin-Entwicklern bereits diskutiert, wie das Netzwerk vor Angriffen durch

Quantencomputer geschützt werden kann. In der Kryptographie wird heute an kryptographischen Ansätzen gearbeitet, die zukünftig auch gegen Quantencomputern resistent sein sollen, allerdings weisen diese Ansätze derzeit noch Probleme hinsichtlich ihrer Effizienz und Skalierbarkeit auf.

Das Bitcoin-Netzwerk bietet die Flexibilität das Bitcoin-Protokoll zu aktualisieren, um sich gegen potentielle Quantencomputer zu schützen, allerdings muss dafür ein Konsens zwischen den Nodes erreicht werden. Die Nodes-Betreiber und Miners sind grundsätzlich konservativ gegenüber Veränderungen des Base Layers, jedoch ist zu erwarten, dass es im gemeinsamen Interesse liegt, das Netzwerk vor Bedrohungen durch Quantencomputer zu schützen.

Ein entscheidender Faktor für die Sicherheit des Bitcoin-Netzwerks ist, dass Bitcoin zu den innovativsten Industrien zählt. Die Bitcoin Industrie tätigte von Anbeginn hohe Investitionen in bessere Technologien. Zu Beginn verwendeten Miners noch CPU-Prozessoren, später zählten Bitcoiners zu den ersten, die GPU-Prozessoren für das Mining verwendeten. Mittlerweile nutzen Miners hochentwickelte Silicon Asics Rechner, die zu den stärksten Rechnern der Welt zählen. Alle Teilnehmer des Netzwerks haben ein Interesse, die Integrität des Netzwerks zu gewährleisten, da sie „Skin in the Game“ haben. Das heißt, sowohl die Nutzer als auch die Nodes und Miners stecken ihr Kapital in das Netzwerk und setzen alle Hebel in Bewegung, um das Netzwerk zu schützen.

Das Bitcoin-Netzwerk wurde in den letzten 15 Jahren mehrmals attackiert, allerdings ohne signifikante Auswirkungen. Insgesamt ist die Sicherheit des Netzwerks mit kaum etwas vergleichbar. Weder China noch Russland waren in der Lage, Bitcoin abzuschalten. Die dezentrale Struktur des Netzwerks in Kombination mit dem 15 Gigawatt Energie-Wall, der 600 Exahash Rechenleistung modernster Silicon Asics Rechenmaschinen, den kryptographischen Methoden sowie der Open Source Natur des Bitcoin Protokolls machen das System unvergleichbar robust und resilient. Darüber hinaus ist zu erwarten, dass sich der Trend der letzten Jahre fortsetzt und das Netzwerk weiter wächst, wodurch das Netzwerk auch immer stärker und sicherer wird.

5.5 Multi-Layer Modell

Immer wieder hört man von Kritikern von Bitcoin, dass das Bitcoin-Netzwerk zu langsam sei, um alle Transaktionen, die weltweit über Bankinstitute oder Kreditkarteninstitute durchgeführt werden, abzuwickeln, da im Schnitt lediglich 200 bis 300 Transaktionen pro Sekunde auf der Blockchain verzeichnet werden können. Hierbei handelt es sich allerdings um einen Vergleich zwischen Äpfel und Birnen. Das Bitcoin-Netzwerk ist ein Base Layer, auf dem unmittelbare finale Zahlungsausgleiche (Settlements) durchgeführt werden. Vergleicht man die Geschwindigkeit der Zahlungsausgleiche des konventionellen Geldsystems mit dem Final Settlement des Bitcoin-Netzwerks, ist das Bitcoin-Netzwerk um ein vielfaches schneller. Im konventionellen Geldsystem kann zwar schnell bezahlt werden, die Finalisierung der Zahlungsausgleiche zwischen den Banken und Kreditkarteninstituten allerdings findet lediglich alle paar Wochen oder Monate im Hintergrund statt. Die Banken, Kreditkarteninstitute und andere Zahlungsdienstleister wie PayPal bilden also einen höheren Layer, der auf dem Fiatgeld-System aufgebaut ist.

Im Gegensatz dazu können auf dem Bitcoin Base Layer finale Settlements je nach Anzahl der Validierungen bereits in wenigen Minuten bis zu einer Stunde finalisiert werden. Zugleich können auf den Base Layer ähnlich wie im Gold-Standard oder Fiatgeldsystem weitere Layer aufgebaut werden. Bitcoin ist daher ein Multi-Layer Netzwerk. Nicht alle Transaktionen müssen auf dem Base Layer stattfinden. Gegenwärtig bildet das sogenannte Lightning-Netzwerk den zweiten Layer von Bitcoin, um auch kleinere Transaktionen durchzuführen mit nur 1 oder 2 Cent Gebühr pro Transaktion und in Sekundenschnelle. In Zukunft können noch weitere Second Layer Lösungen hinzukommen. Um das Lightning-Netzwerk nutzen zu können, braucht man spezielle Lightning-Wallets. Die Electrum Wallet im vorliegenden Manual ermöglicht sowohl Transaktionen über den Base Layer als auch über das Lightning Netzwerk.

Darüber hinaus gibt es Third- oder Fourth-Layer-Lösungen. Von Third-Layer-Lösungen spricht man dann,

wenn es sich um Tauschbörsen wie Coinbase, Bitcoin ATMs oder Bezahlapps wie die Cash App von Jack Dorsy handelt. Meist sind die Third-Layer-Lösungen bestimmte Apps, hinter denen ein Bitcoin-Unternehmen steckt. Fourth-Layer-Lösungen wären bspw. Bitcoin ETFs, die von Investmentbanken gehandelt werden und auch von Nutzern ohne Wallet gehalten werden können.

Die verschiedenen Layer können in der persönlichen Nutzung unterschiedliche Funktionen ausüben. So würde man bspw. höhere Transaktionssummen, die vom Savings-Account (Sparkonto) auf eine andere Wallet überwiesen werden, wie z.B. für den Umtausch höherer Summen in Fiatgeld oder für den Kauf einer Wohnung, auf dem Base Layer abwickeln, da dieser eine hohe Sicherheit gewährleistet und man die Transaktionskosten dafür in Kauf nimmt. Zugleich würde man für niedrigere Transaktionssummen, wie für die Bezahlung eines Starbucks-Kaffees, das Lightning Netzwerk nutzen, das zwar ein etwas höheres Sicherheitsrisiko impliziert, dafür aber niedrige Transaktionskosten und eine hohe Effizienz aufweist.

Die Skalierung des Bitcoin-Netzwerkes erfolgt also nicht über den Base-Layer, der grundsätzlich eher konservativ und ineffizient ist, dafür aber ein hohes Sicherheitsbedürfnis gewährleistet. Stattdessen erfolgt die Skalierung über Second-Layer und Third-Layer Lösungen, die Effizienz und Flexibilität bieten.

5.6 The Block Size War

Der sogenannte Block Size War (Krieg über die Blockgröße) ist ein zentrales Ereignis in der Geschichte des Bitcoin-Netzwerks und beschreibt eine hitzige Debatte zwischen zwei Camps unter Bitcoin-Entwicklern, Minern, Nodes-Betreibern, Unternehmen und Nutzern, die zwischen 2015 und 2017 ausgetragen wurde. Der Block Size War war ein bedeutsames Ereignis, nicht nur aus technischen Gründen zur Weiterentwicklung des Netzwerks, sondern auch aus Gründen der Integrität des Netzwerks.

An der Oberfläche ging es in der Debatte um die Größe der Blöcke auf der Blockchain und um die zukünftige Skalierung des Netzwerks. Satoshi Nakamoto, der anonyme Entwickler von Bitcoin, legte im ursprünglichen Protokoll eine Blockgröße von 1 MB fest. Da die Blockgröße mit dem zunehmenden Transaktionsvolumen zu Engpässen führte und die Transaktionskosten in die Höhe schossen, entfachte sich eine Debatte über die Vergrößerung der Blockgröße. Eine Seite der Debatte setzte sich für eine signifikante Veränderung des Bitcoin-Protokolls (Hard-Fork) ein und für eine deutliche Erhöhung der Blockgröße, um die Engpässe zu minimieren und die Transaktionskosten auf dem Base Layer zu senken.

Die Gegenseite lehnte eine grundsätzliche Veränderung des Protokolls (Hard-Fork) ab und setzte sich stattdessen für eine sogenannte Soft-Fork-Lösung ein – also ein Upgrade des Protokolls mit nur leichten Veränderungen, welches eine Rückwärtskompatibilität mit dem ursprünglichen Protokoll ermöglicht. Ein wesentliches Gegenargument war, dass die Blockgröße bei einer Skalierung auf dem Base Layer zuviel Speicherplatz benötigen würde und herkömmliche Computer folglich keine Node mehr betreiben könnten. Um die Engpässe in den Griff zu bekommen, schlug die Gegenseite das sogenannte SegWit (Segregated Witness) Upgrade vor, welches die Blockgröße effektiv auf 4 MB erhöhte, allerdings das grundsätzliche Protokoll nicht veränderte. Zudem wurden mit dem SegWit Upgrade Second Layer Lösungen wie das Lightning Netzwerk ermöglicht. Grundsätzlich ging es also um die Frage, in welche Richtung das Bitcoin Netzwerk geht und ob die Skalierung über den Base Layer erfolgt oder über Second- und Third-Layer Lösungen.

Da die Befürworter der Hard Fork mit der vorgeschlagenen Lösung der Gegenseite nicht zufrieden war, kam es zu einer Abspaltung von Bitcoin in Bitcoin Core (BTC) und Bitcoin Cash (BCH). Nur eine kleine Minderheit schloss sich der Hard-Fork an und wechselte zu Bitcoin Cash. Die Gegenseite hingegen, die gegen die grundsätzliche Veränderung des Protokolls war, setzte sich durch. Das dominante Netzwerk gemessen an der Marktkapitalisierung und der Anzahl der Nutzer ist heute das Bitcoin Core (BTC) Netzwerk.

Der Block Size War war eine grundlegende Auseinandersetzung über die Zukunft des Netzwerks und dessen Skalierungsmethode. Mit dem SegWit Upgrade zeigte die Bitcoin-Szene, dass das Netzwerk einerseits

genügend Flexibilität besitzt, um konkrete Probleme wie die Skalierbarkeit zu adressieren, und andererseits, dass eine hohe Bereitschaft besteht, die Integrität des Netzwerks und des Base Layers aufrechtzuerhalten.

Der Block Size War führte zwar zu Verwerfungen und Abspaltungen innerhalb der Bitcoin-Community, die große Mehrheit der Bitcoiners allerdings hielt an der Integrität des Protokolls fest und stärkte das Vertrauen in das Netzwerk. Zudem gab der Block Size War den Anstoß für das Lightning-Netzwerk und für die Möglichkeit zur Skalierung in Form der Second-Layer Lösungen.

5.7 Volatilität und „Hodling“

Ein zentraler Begriff, der oftmals als Kritik gegen Bitcoin angeführt wird, ist der Begriff der Volatilität. Der Bitcoin Preis unterliegt sehr starken Schwankungen, was bei vielen Einsteigern oftmals für Nervosität sorgt und zu Panikverkäufe führt. Die Volatilität des Bitcoin Preises ist in erster Linie ein Ausdruck der Menge an ökonomischem Kapital, welches im Netzwerk steckt, im Vergleich zu anderen Vermögensklassen. Bitcoin steht noch ganz am Anfang und beinhaltet weniger als 1% des weltweiten Gesamtvermögens. Wenn Elon Musk bspw. einen großen Teil an Bitcoins verkauft, wirkt sich dies stärker auf den Bitcoin Preis aus als bei anderen Vermögensklassen. Da aber die Cash Balances im Bitcoin-Netzwerk wachsen und immer mehr Vermögen in das Bitcoin-Netzwerk fließt, wird die Volatilität des Bitcoin-Preises zukünftig zurückgehen.

Bitcoin-Profis lassen sich von der Volatilität nicht beirren. Im Gegenteil: man nutzt die Volatilität zum eigenen Vorteil aus. Sinkt der Preis stark, nutzt man die Gelegenheit und kauft antizyklisch mehr Bitcoin nach. Steigt der Preis stark an, kann man einen Teil seiner Bitcoin Cash-Balances liquidieren, um bspw. einen Kredit bei der Bank zurückzuzahlen oder eine Konsumausgabe zu tätigen.

Aufgrund der Volatilität des Bitcoin Preises ist es unter Bitcoinern üblich, dass man sich eher an der log-linearen Skala (blaue Kurve) orientiert anstelle der linearen Skala (schwarze Kurve). Die log-lineare Skala erlaubt eine klarere Perspektive, da sie die starken Preisschwankungen glättet und ein deutlicheres Muster der Schwankungen und Zyklen zeigt.

Abbildung 4: Log-linear und linear skalierte Entwicklung des Bitcoin Preises (Quelle: https://blockchain.com)

Wichtiger als die vorteilhafte Nutzung der Volatilität ist die langfristige Perspektive. Das letzte Hoch eines Zyklus war bisher immer höher als das vorletzte Hoch und das letzte Tief eines Zyklus war bisher immer höher als das vorletzte Tief. Das heißt, Sparen und Investieren in Bitcoin bedürfen einer langfristigen Perspektive. Zwar gibt es im Bitcoin-Markt auch Trader, die die Volatilität für die kurzfristige Spekulation nutzen, allerdings kennzeichnen sich Bitcoiner durch eine andere Mentalität. Bitcoin-Profis nehmen eine langfristige Perspektive ein und zählen sich grundsätzlich zu den sogenannten *Hodlers*.

Der Ursprung des Begriffs *Hodling* liegt in einem Internet-Witz, als ein Bitcoin-Inhaber in einem Online-Forum versehentlich *Hodling* anstelle von *Holding* (Halten) schrieb. Der Begriff *Hodling* wurde in weiterer Folge in der Bitcoin-Szene übernommen und steht für das (ewige) Halten der Bitcoins. Der Begriff *Hodling* beschreibt also eine bestimmte Investment-Philosophie, die einen langfristigen Zeithorizont einnimmt. Verkonsumiert wird primär das inflationierte Fiatgeld, Bitcoins hingegen sind Eigentum und werden bis in die Ewigkeit gehalten und gespart, auch wenn der Preis einmal stärker fällt.

Hodling ist eine Strategie, die sich nicht auf Bitcoiners beschränkt, sondern eine Philosophie, die in der Regel von den vermögendsten Familien der Welt gelebt wird. Vermögende werden nicht vermögend, indem sie ihren Besitz verkaufen, sondern indem sie ihren Besitz langfristig halten und gegebenenfalls als Kreditsicherheit (Collateral) einsetzen, um sich mit zusätzlichen Assets einzudecken. Bitcoin-Hodlers lassen sich von Preisschwankungen nicht beirren, sondern nehmen eine langfristige Perspektive ein und sitzen die Preisschwankungen ab.

6 Grundlagen und Sicherheit der Wallet

Während das Bitcoin-Netzwerk insgesamt zu den sichersten Systemen der Welt zählt, ist die Sicherheit der persönlichen Wallet eine zentrale Herausforderung. Die Herausforderung bei der Sicherung der Wallet ist nicht nur technischer Natur. Je höher die Sicherheit der Wallet, desto aufwändiger ist auch die Einrichtung und Nutzung der Wallet. Das heißt, es gibt einen Trade-off zwischen Sicherheit und Bequemlichkeit.

Der Begriff *Wallet* bedeutet übersetzt *Geldbörse* und kann im Bitcoin Jargon als ein Bitcoin-Konto verstanden werden, mit dem Bitcoins empfangen, versendet und gehalten werden können. In der Wallet selbst sind die Bitcoins nicht gespeichert, denn diese liegen auf der Blockchain auf der ganzen Welt verteilt. Stattdessen befindet sich in der Wallet der Schlüssel, der den Inhaber authorisiert auf die Bitcoins zuzugreifen.

Es gibt verschiedene Arten von Wallets. Eine Wallet kann auf einer Tauschbörse erstellt oder direkt auf dem Computer installiert werden. Beide Arten von Wallets können je nach Nutzertyp unterschiedliche Vor- und Nachteile aufweisen. Zudem stellt sich die Frage, wofür man die Wallet nutzen möchte, denn je nach Use Case wird man unterschiedliche Sicherheitsmaßnahmen implementieren. Möchte man Bitcoin primär als Tauschmedium im Alltag nutzen, so würde man eher kleinere Beträge in der Wallet halten und mehr Wert auf Bequemlichkeit legen. In einem solchen Fall würde sich eine Mobile App mit Zugang zum Lightning Netzwerk anbieten mit schnellen Transaktionen und niedrigen Transaktionskosten. Möchte man hingegen Bitcoin als Wertaufbewahrungsmittel halten und die Wallet als Sparkonto nutzen, wird man eher weniger häufig Bitcoins versenden und nach gewisser Zeit höhere Beträge in der Wallet halten, wodurch der Sicherheitsaspekt eher priorisiert wird und die Bequemlichkeit in den Hintergrund rückt.

Im vorliegenden Manual geht es um die Installation und Konfiguration einer Wallet für das langfristige Sparen und Investieren, für die man selbst die Verantwortung trägt und für die ein hoher Sicherheitsstandard erfüllt sein soll. Dafür wird die Open Source Bitcoin Wallet *Electrum* installiert. Für die Sicherheit der Wallet sind zwei Risiken zu beachten: (1) Bedrohungen durch unauthorisierte Zugriffe und (2) Verlust der Seed Phrase, mit der die Wallet bei einem Hardware-Gebrechen oder bei Verlust wiederhergestellt werden kann. Während die Bedrohung eines unauthorisierten Zugriffs in erster Linie technisch gelöst wird, ist die Aufbewahrung der Seed Phrase eher eine logistische bzw. organisatorische Herausforderung.

Für die Wallet im vorliegenden Manual werden vier Konzepte und Sicherheitsmaßnahmen kombiniert:

- Self-Custody (Selbstaufbewahrung)
- Cold Storage (Offline-Aufbewahrung)
- kryptographische Verschlüsselung
- 2-Factor Authentication (2FA)

Self-Custody heißt übersetzt *Selbstaufbewahrung* und bedeutet, dass man zwar die absolute Kontrolle über die Wallet hat und nicht von Drittparteien abhängig ist, allerdings für die Wallet und deren Sicherheit selbst verantwortlich ist. Nutzt man eine App oder eine Hardware Wallet, stellt sich die Frage, wie sehr man den Anbieter der App vertraut (Stichwort: Trustless). Die Selbstaufbewahrung kann bei korrekter Anwendung auch ein Vorteil in Punkto Sicherheit sein. Hält man eine Wallet bei einer Tauschbörse, ist man auf die technische Sicherheit des Anbieters angewiesen. Zugleich werden Tauschbörsen von Hackern oftmals ins Visier genommen, da dort mehr zu holen ist als beim „kleinen Sparer“. Zudem besteht das Risiko, dass eine Tauschbörse insolvent geht und man seine Ersparnisse verliert. Dazu kommt, dass Selbstaufbewahrung nicht das Risiko einer Teilreserve (Fractional Reserve) impliziert.

Der zweite zentrale Begriff ist *Cold Storage*, der eine Konfiguration beschreibt, bei der die Wallet offline gespeichert wird und nicht mit dem Internet verbunden ist. Cold Storage impliziert eine höhere Sicherheit

und einen besseren Schutz vor Hackern. Das vorliegende Manual erklärt, wie eine Self-Custody Wallet als Cold Storage installiert und konfiguriert werden kann. Somit hat man einerseits die volle Kontrolle über die Wallet, ohne Tauschbörsen bzw. Drittparteien vertrauen zu müssen, andererseits erfüllt die Wallet einen hohen Sicherheitsstandard. Für die Offline-Speicherung der Wallet im vorliegenden Manual wird ein handelsüblicher USB-Stick eingesetzt.

Das dritte Konzept ist die kryptographische Verschlüsselung. Nicht nur wird die Wallet selbst kryptographisch verschlüsselt, sondern auch der USB-Stick, sodass beim Öffnen des USB-Sticks ein Passwort eingegeben werden muss. Des Weiteren soll nach der Einrichtung der Wallet auch der Wiederherstellungsschlüssel mithilfe eines Passwort-Managers kryptographisch gesichert werden.

Das vierte Konzept zur Sicherung der Wallet ist die 2-Factor Authentifizierung. Eine Wallet mit 2FA erfordert ein Mobile Phone mit der Google Authenticator App, welche beim Senden von Bitcoins einen Code generiert und in der Wallet zur Bestätigung eingegeben werden muss. Die 2FA wird bei der Electrum Wallet von Trusted Coin zur Verfügung gestellt.

Eine Bitcoin Wallet ist in der Regel mit vier Informationen verknüpft:

- Persönliches Passwort, um die Wallet und die Signatur-Schlüssel zu sichern
- Seed Phrase, um eine Wallet bei Verlust oder Hardware-Gebrechen wiederherzustellen
- Schlüssel (Keys), um das Senden von Bitcoins kryptographisch zu signieren
- Bitcoin Adresse (Kontonummer), auf die die Bitcoins beim Empfangen von Bitcoins transferriert werden.

Das Passwort, die Seed Phrase und die Keys sollten mit niemandem geteilt werden. Besonders wichtig ist die sichere Verwahrung der Seed Phrase, die aus insgesamt zwölf zufälligen Wörtern besteht und für die Wiederherstellung der Wallet eingesetzt wird, wie etwa bei einem technischen Gebrechen der Hardware, bei Diebstahl oder bei Verlust des Wallet-Passwortes.

Die Electrum Wallet bietet noch weitere Sicherungsmaßnahmen, wie Multi-Signatur oder eine Watch-Only Wallet. Bei der Multi-Signatur werden Transaktionen mit zwei oder mehr getrennten Schlüsseln signiert. Dies kann vor allem dann nützlich sein, wenn zwei oder mehr Personen über eine Wallet verfügen. Bei der Watch-Only Wallet werden zwei Wallets eingerichtet: eine Watch-Only Wallet, die auf einem Online Computer gespeichert ist und lediglich das Abfragen des Kontostandes und das Empfangen von Bitcoins erlaubt und eine Offline Wallet, die auf einem Computer ohne Internetverbindung liegt und mit der Zahlungsausgänge signiert werden.

7 Erstinstallation von Electrum

Nach der Einführung in die Theorie, beginnt ab jetzt der praktische Teil. Um dem Manual folgen zu können und die Electrum Wallet erfolgreich zu installieren und zu konfigurieren, sollte überprüft werden, ob alle technischen Voraussetzungen erfüllt sind (Siehe Kapitel 3). Sollte kein USB-Stick zur Verfügung stehen oder möchte man lediglich eine Wallet einrichten, die nicht offline auf einem externen Datenträger gespeichert wird, können Schritt 1 und Schritt 6 übersprungen werden. Der High-Level Prozess der Installation und Konfiguration besteht aus mehreren Etappen:

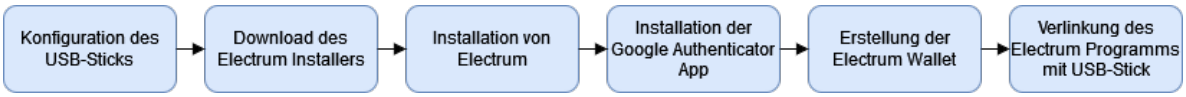


Abbildung 5: Verfahrensschritte zur Einrichtung der Wallet

- In Schritt 1 wird der USB-Stick für die Cold-Storage Aufbewahrung konfiguriert, indem der USB-Stick formatiert und verschlüsselt wird.
- In Schritt 2 wird der Installer von der Electrum Website runtergeladen.
- In Schritt 3 wird das Electrum Programm auf dem Computer installiert.
- In Schritt 4 installieren wir die Google Authenticator App auf dem Mobile Phone.
- In Schritt 5 erstellen und konfigurieren wir die Electrum Wallet.
- Im letzten Teil erfolgt der anspruchvollste Schritt der Installation, nämlich die Verlinkung des Electrum Programms auf dem Computer mit der Wallet-Datenbank auf dem USB-Stick.

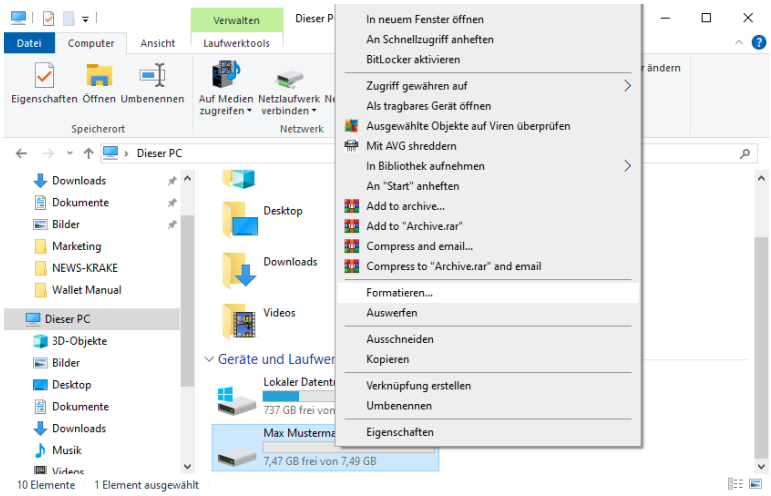
7.1 Konfiguration des USB-Sticks

Um die Wallet offline (Cold Storage) zu speichern, benötigen wir einen USB-Stick oder eine externe Festplatte. Zwar kann der USB-Stick nach der Installation der Wallet für die Datenspeicherung im Alltag genutzt werden, allerdings wird empfohlen, dass der USB-Stick ausschließlich für die Wallet verwendet wird, um die Wallet nicht unnötig zu exponieren oder die Wallet-Daten nicht unabsichtlich zu löschen oder zu verändern. Darüber hinaus sollte man den USB-Stick an einem sicheren Ort verwahren. Wie bereits oben erwähnt, kann die Wallet bei einem Hardware-Gebrechen oder bei Verlust des USB-Sticks mithilfe der Seed Phrase wiederhergestellt werden.

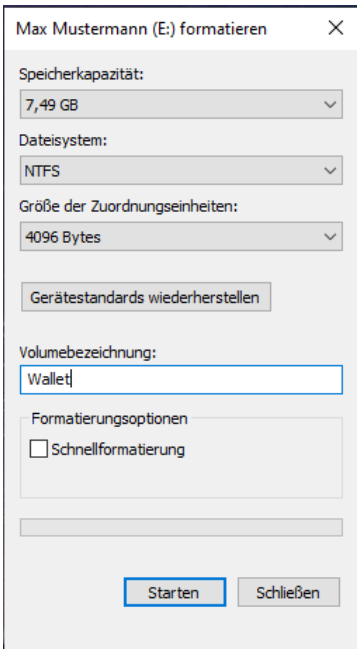
Um sicher zu gehen, dass sich auf dem USB-Stick kein Schadcode befindet oder beschädigt ist, wird der USB-Stick zuerst formatiert. **ACHTUNG! Bei der Formatierung des USB-Sticks werden alle gespeicherten Daten vom USB-Stick gelöscht. Befinden sich auf dem USB-Stick noch Daten, sollten die Daten vorher gesichert werden.**

Für die Formatierung des USB-Sticks öffnet man zuerst die Ordner Übersicht (Explorer), indem man mit der rechten Maustaste auf das *Start* Symbol in der Taskleiste klickt und die Option *Explorer* auswählt. Danach navigieren wir zu *Dieser PC*, wo sich unter der Rubrik *Geräte und Laufwerke* der USB-Stick befindet. Nachdem der korrekte Datenträger identifiziert wurde, klickt man mit der rechten Maustaste auf den USB-Stick und wählt die Option *Formatieren* aus. **ACHTUNG! Man sollte überprüfen, ob der richtige**

Datenträger ausgewählt wird, da die Daten vom Laufwerk bei der Formatierung gelöscht werden. Zudem sollten die Daten auf dem USB-Stick vorher gesichert werden.

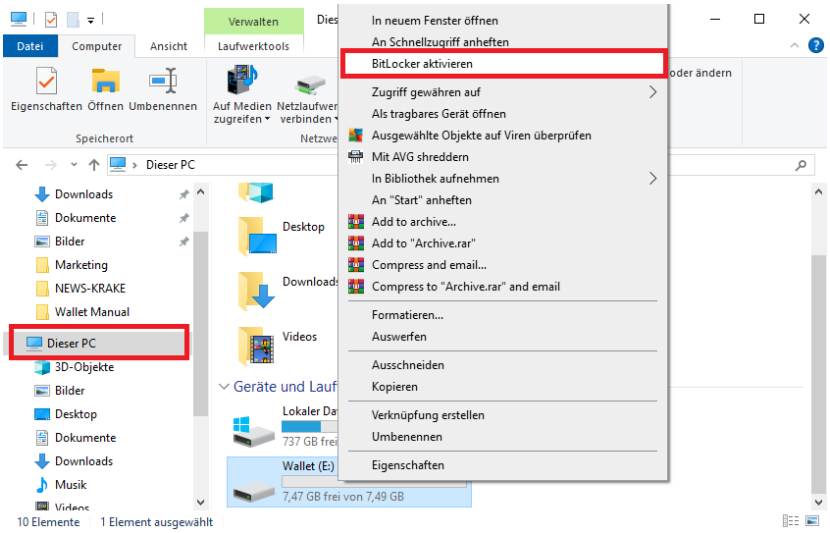


Nun sollte sich ein Fenster öffnen, in dem verschiedene Parameter konfiguriert werden können. Verwendet man den USB-Stick auf einem Windows-Rechner, wählt man das Windows Dateisystem NTFS aus, wobei auch FAT32 reibungslos funktionieren sollte. Bei der Volumebezeichnung wird eine Bezeichnung für den USB-Stick eingegeben. Bei der Schnellformatierung wird das Häkchen entfernt, wodurch man sicherstellt, dass auch die sogenannten schlechten Sektoren (Bad Sectors) des Datenträgers gescannt werden. Nach der Einstellung der Parameter klicken wir auf *Starten*.

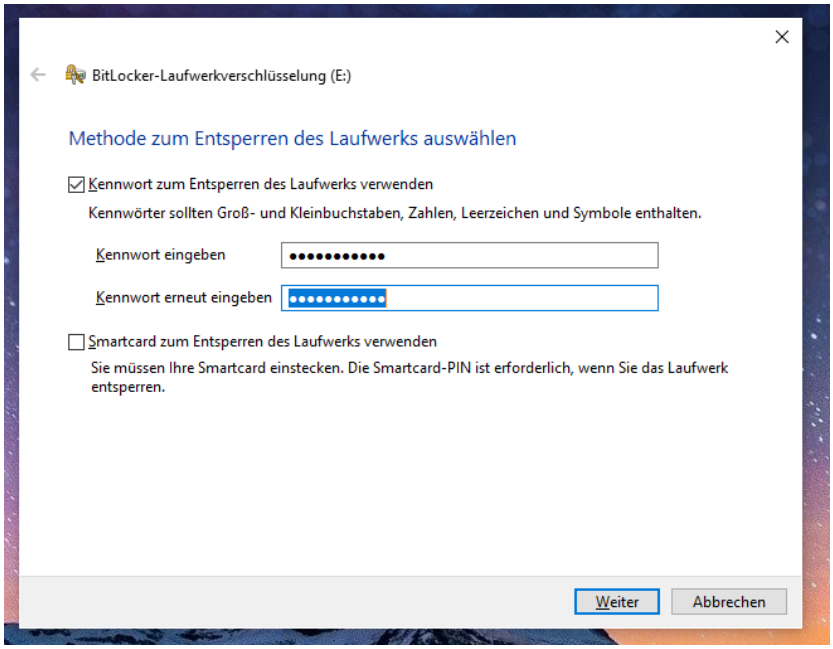


Der Formatierungsprozess kann je nach Speichergröße einige Minuten dauern. Nach Ende der Formatierung öffnet sich ein Fenster mit dem Hinweis, dass die Formatierung erfolgreich abgeschlossen wurde. Sowohl das Hinweisfenster als auch das Formatierungsfenster können geschlossen werden.

Im nächsten Schritt verschlüsseln wir den USB-Stick mit einem Passwort. Hierfür geht man zurück zu *Dieser PC*, klickt mit der rechten Maustauste auf den USB-Stick und wählt die Option *BitLocker aktivieren* aus. Bitlocker ist das Windows Verschlüsselungsprogramm, es können aber auch andere Programme für die Verschlüsselung verwendet werden, wie bspw. VeraCrypt, die mehr Konfiguration ermöglichen.

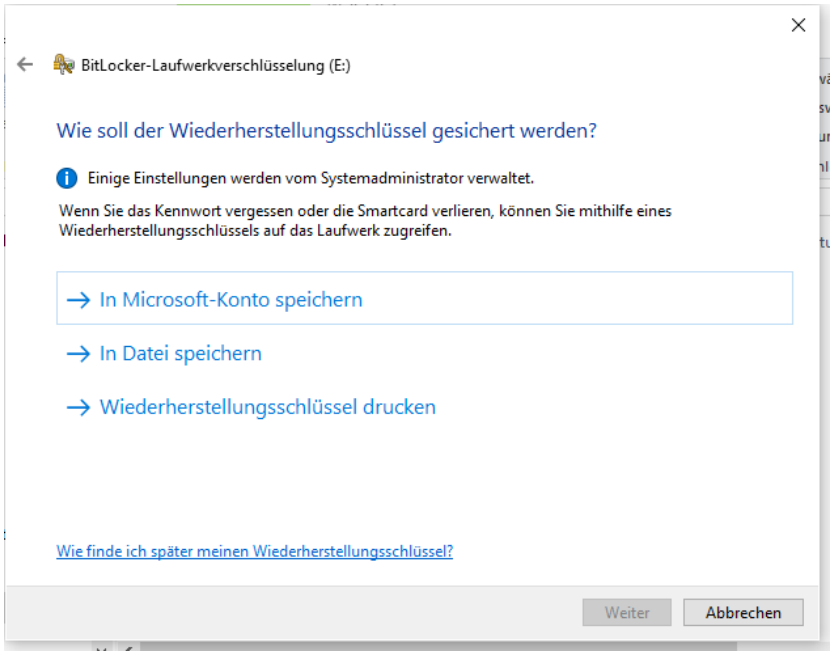


Nun sollte sich das Bitlocker Fenster öffnen und das Laufwerk initialisieren bis die Seite *Methode zum Entsperren des Laufwerks auswählen* erscheint. Hier wählen wir die erste Option *Kennwort zum Entsperren des Laufwerks verwenden* und definieren das Passwort für den USB-Stick. Danach klicken wir auf *Weiter*.

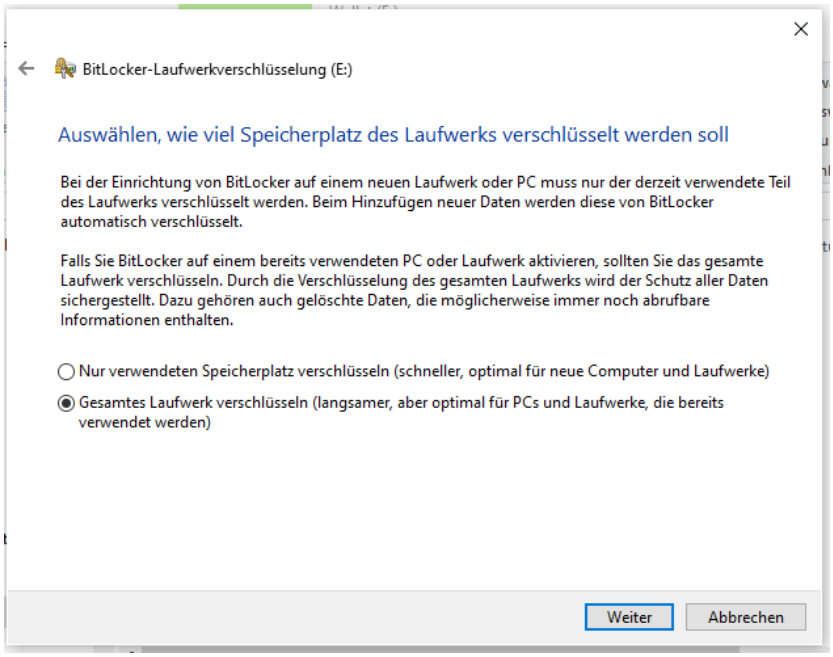


Im nächsten Schritt fragt Bitlocker, wie man den Wiederherstellungsschlüssel sichern möchte. Mit dem Wiederherstellungsschlüssel kann das Laufwerk wiederhergestellt werden, sollte man das Passwort für den USB-Stick vergessen.

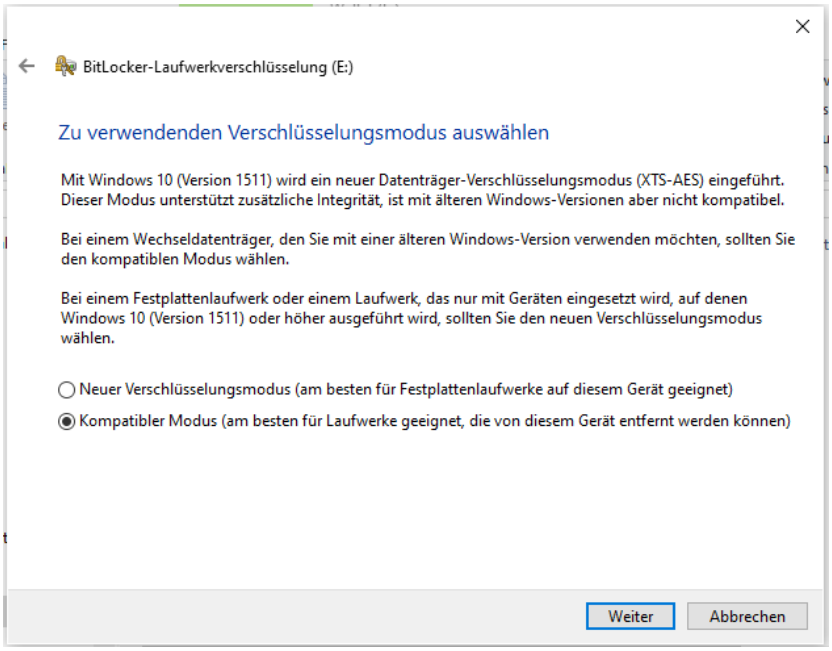
Für die vorliegende Konfiguration klicken wir auf *Wiederherstellungsschlüssel drucken* und drucken den Schlüssel in ein PDF. Steht ein Drucker zur Verfügung, kann der Schlüssel auch auf Papier ausgedruckt werden. Später in Kapitel 10 werden wir uns genauer damit befassen, wie wir den Wiederherstellungsschlüssel sicher verwahren können. Nachdem der Wiederherstellungsschlüssel gedruckt wurde, klicken wir auf *Weiter*.



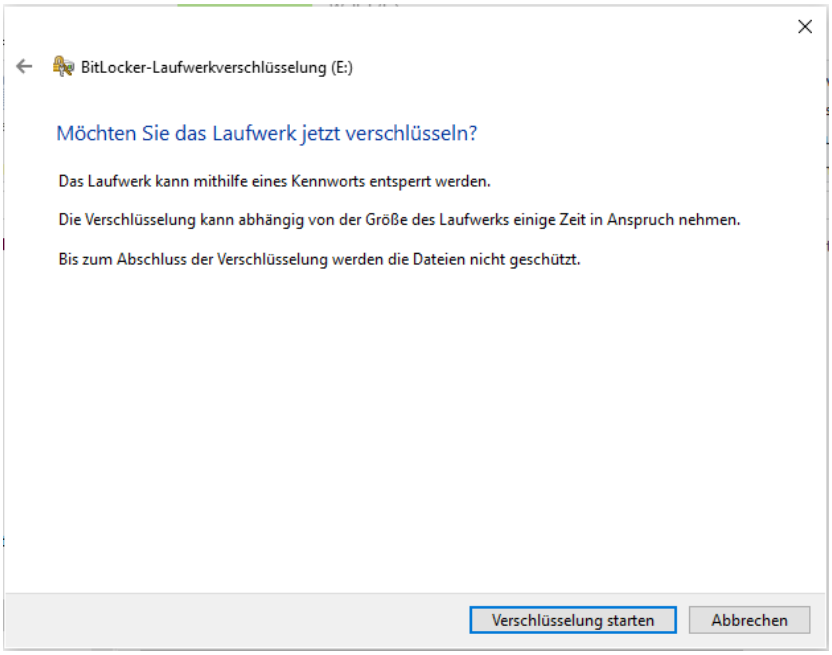
Im nächsten Schritt wählen wir aus, ob das gesamte Laufwerk verschlüsselt werden soll oder nur der verwendete Speicherplatz. In dem Fall wählen wir die Option *Gesamtes Laufwerk verschlüsseln* aus.



Im nächsten Schritt wählen wir den kompatiblen Modus für die Verschlüsselung aus. Der kompatible Modus eignet sich für externe Datenträger, die vom Computer entfernt werden können. Nach Auswahl des kompatiblen Modus, klicken wir auf *Weiter*.



Im letzten Schritt klicken wir auf *Verschlüsselung starten*, womit die Verschlüsselung des USB-Sticks beginnen sollte. Nachdem die Verschlüsselung erfolgreich durchgeführt wurde, kann das Fenster geschlossen werden. Der USB-Stick kann ab sofort nur von jenen Personen geöffnet werden, die im Besitz des korrekten Passworts oder des Wiederherstellungsschlüssels sind.

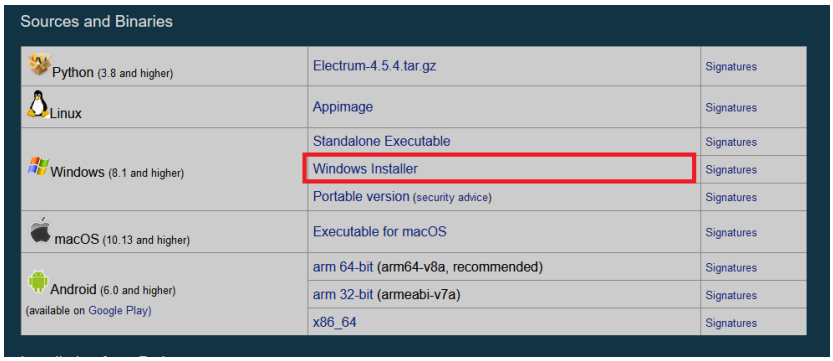


Abschließend führen wir einen Test durch, ob die Verschlüsselung erfolgreich war, indem der USB-Stick abgesteckt und neu angeschlossen wird. Nach Anschluss an den Computer sollte Windows nach ein Passwort fragen oder gibt rechts unten einen Hinweis, dass der Datenträger entsperrt werden muss.

Mit einem Klick auf den Hinweis öffnet sich ein Fenster mit einem Eingabefeld für das Passwort. Zudem sollte im Folder *Dieser PC* beim Laufwerk ein kleines Schloss erscheinen. Nun geben wir das Passwort ein und überprüfen, ob Bitlocker das Laufwerk korrekt verschlüsselt hat. Öffnet sich nach Eingabe des Passworts der USB-Stick, war die Verschlüsselung erfolgreich und der erste Schritt ist erfolgreich abgeschlossen.

7.2 Download Electrum Installer

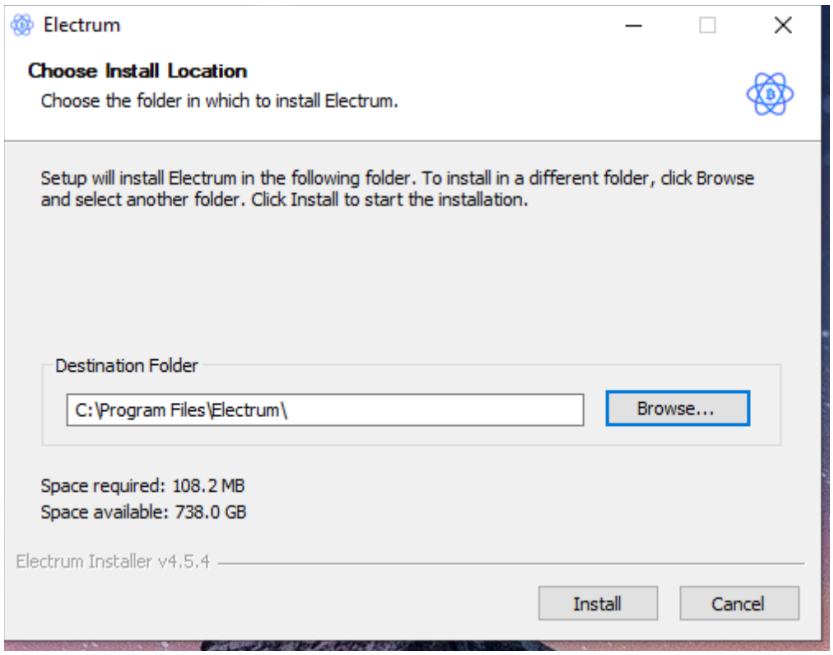
Bevor wir Electrum auf dem Computer installieren, laden wir den Installer von der Electrum Website runter. Die Website von Electrum lautet `https://electrum.org`, von der im Menü Punkt *Download* der Windows Installer runtergeladen werden kann. Für Windows gibt es drei Download Möglichkeiten: (1) Standalone Executable, (2) Windows Installer und (3) Portable Version. Für das vorliegende Manual klicken wir auf (2), womit der Download des Electrum Installers starten sollte.



Der Installer sollte sich nun im *Downloads* Ordner befinden.

7.3 Installation von Electrum

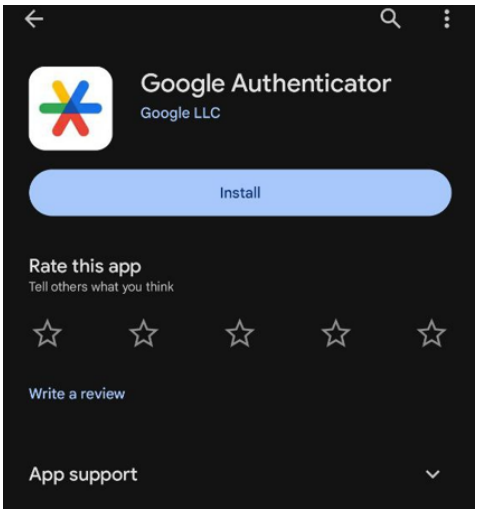
Nach dem Download des Installers kann die Installation mit einem Doppelklick auf die runtergeladene Datei gestartet werden. Im ersten Schritt des Installers kann unter *Browse* der Ordner ausgewählt werden, in dem das Programm installiert werden soll. In der Regel werden die Programm Dateien im `C:\` Datenträger im Ordner *Programme* (`C:\Program Files`) gespeichert. Im Normalfall ist der korrekte Ordner bereits voreingestellt und muss nicht manuell ausgewählt werden.



Ist der Zielordner korrekt, klicken wir auf *Install*, um die Installation zu starten. Nachdem die Programm Dateien installiert wurden, kann der Installer geschlossen werden.

7.4 Installation der Google Authenticator App

Um eine Wallet mit 2-Factor Authentifizierung einzurichten, benötigen wir die Google Authenticator App, die wir auf dem Mobile Phone installieren. Dafür gehen wir in den App Store (PlayStore auf Android, Apple Store auf iPhone), suchen nach Google Authenticator und installieren die App. Nach der Installation öffnen wir die App.



Um die App zu verwenden, benötigen wir nicht notwendigerweise einen Google Account, allerdings können

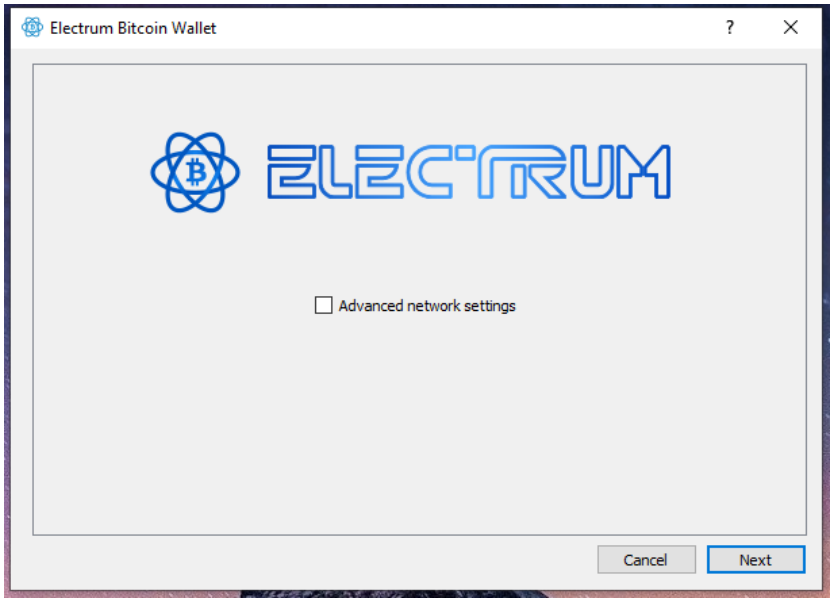
mit einem Google Account die verknüpften Apps im Falle eines neuen Mobile Phones leicht wiederhergestellt werden. Möchten wir keinen Google Account nutzen, können wir als Alternative einen QR-Code erstellen, mit dem wir später die verknüpften Apps auf einem neuen Mobile Phone importieren können.

Dafür klicken wir in der App auf das Menü oben, navigieren in den Reiter *Transfer accounts*, klicken auf *Export accounts*, wählen die verknüpften Apps aus, klicken auf *Next* und erstellen im letzten Schritt einen Screenshot des QR-Codes. Für diesen Screenshot sollte ein Backup erstellt werden, falls wir das Mobile Phone verlieren. Doch bevor wir einen Screenshot des QR-Codes erstellen und diesen sichern, sollten wir zuvor die Wallet mit dem Google Authenticator verknüpfen, was wir im nächsten Abschnitt in Angriff nehmen. **ACHTUNG! Können wir im Falle eines neuen Mobile Phones die verknüpften Apps nicht in die Google Authenticator App importieren, müssen wir die Bitcoin Wallet mit der Seed Phrase wiederherstellen.**

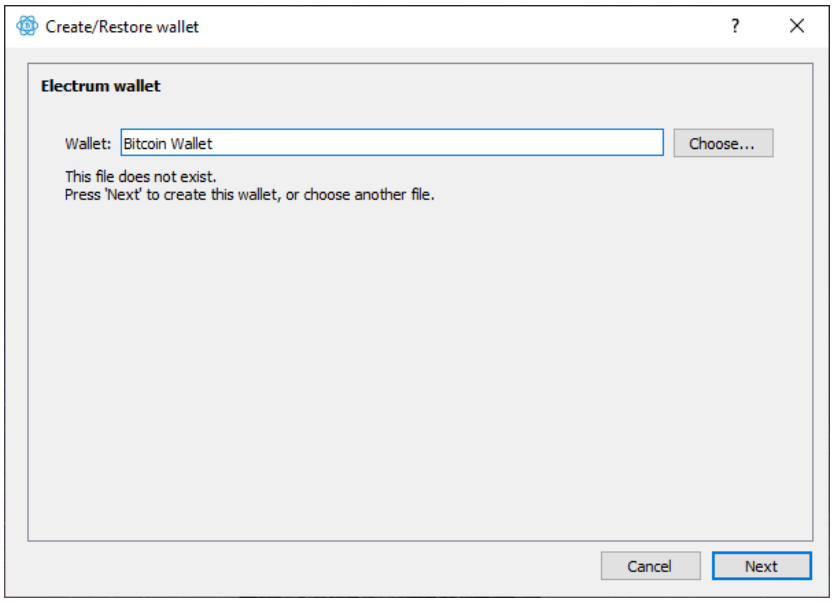
7.5 Erstellung der Wallet

Electrum sollte nun auf dem Computer installiert sein und wir können mit der Erstellung der Bitcoin Wallet beginnen. Nach Abschluss der Installation sollte sich auf dem Desktop eine Electrum Verknüpfung befinden. Um die Wallet zu erstellen, starten wir Electrum mit einem Doppelklick auf die Electrum Verknüpfung.

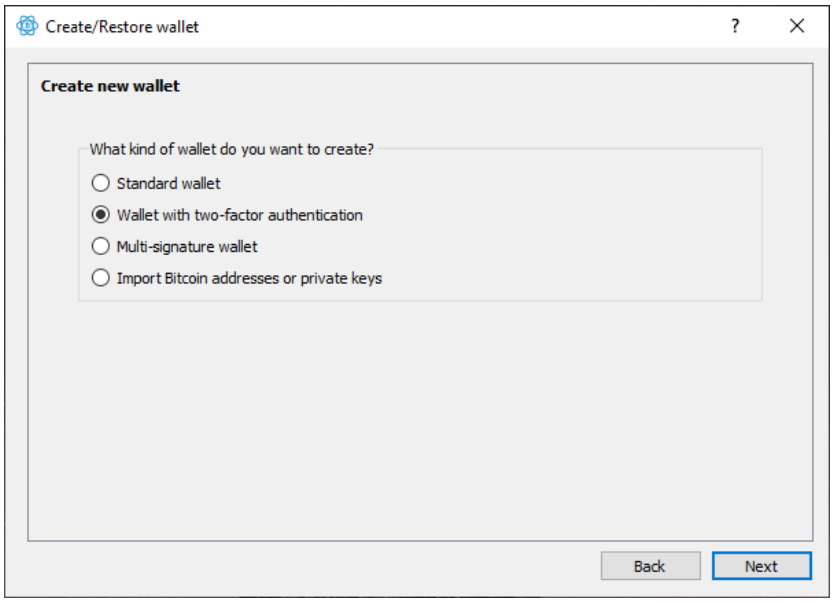
Bei *Advanced network settings* wird kein Häkchen gesetzt, da wir keinen Proxy Server oder Server einrichten. Das heißt, einfach auf *Next* klicken.



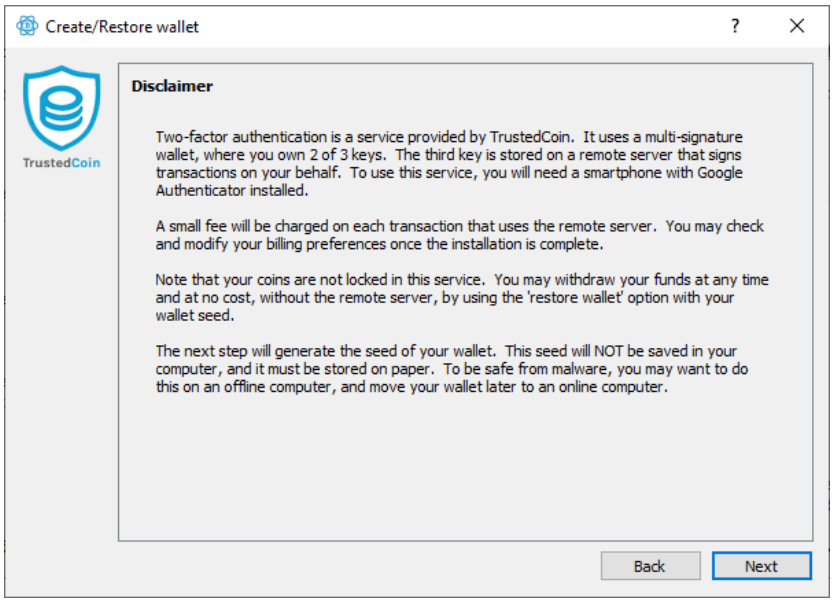
Im nächsten Schritt definieren wir einen Namen für die Wallet. Standardmäßig steht im Eingabefeld *default_wallet*. Möchte man mehrere Wallets im Laufe der Zeit erstellen, sollte der Name so gewählt werden, dass wir die verschiedenen Wallets eindeutig voneinander unterscheiden können. Danach klicken wir auf *Next*.



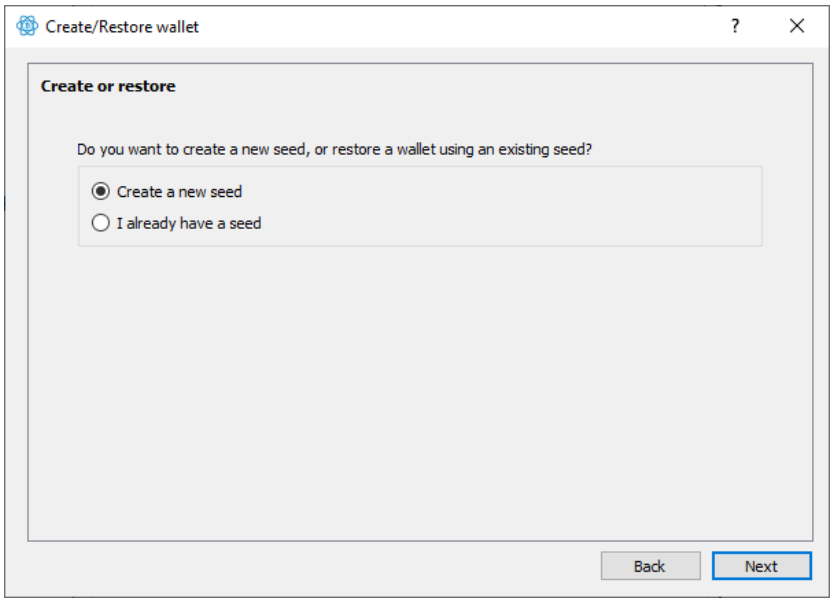
Als nächstes wählt man aus, welche Art von Wallet erstellt werden soll. Für das vorliegende Manual wird eine Wallet mit 2FA erstellt. Nach Auswahl der Option *Wallet with 2-factor authentication* klickt man wieder auf *Next*.



Im nächsten Schritt lesen wir den Disclaimer der 2FA-Wallet. Wichtig zu erwähnen ist, dass das Service bei jeder gesendeten Transaktion eine kleine Gebühr abzweigt.

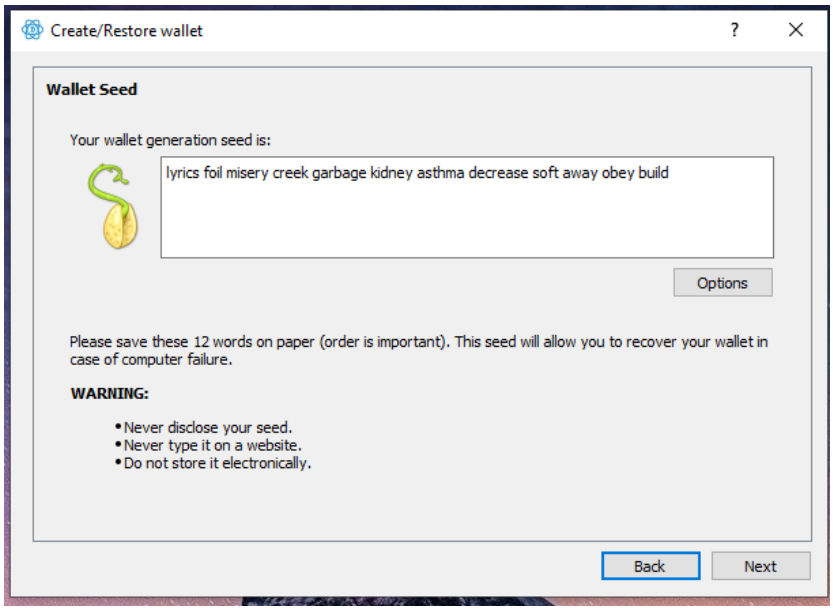


Nun wählen wir die Option *Create a new seed* aus und klicken wieder auf *Next*.

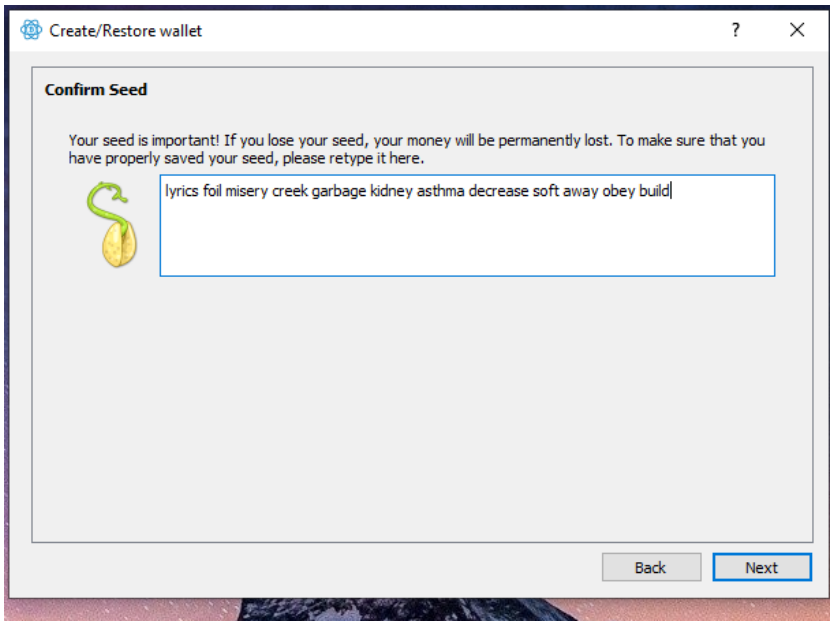


Nun wurde für unsere Wallet eine Seed Phrase kreiert, die aus zwölf Wörtern besteht und sicher aufbewahrt werden sollte. Mit der Seed Phrase kann die Wallet später bei Verlust des USB-Sticks oder bei technischem Versagen wiederhergestellt werden. Dieser Seed sollte mit niemandem geteilt werden, da sich jede Person im Besitz der Seed Phrase Zugriff auf die Wallet verschaffen kann.

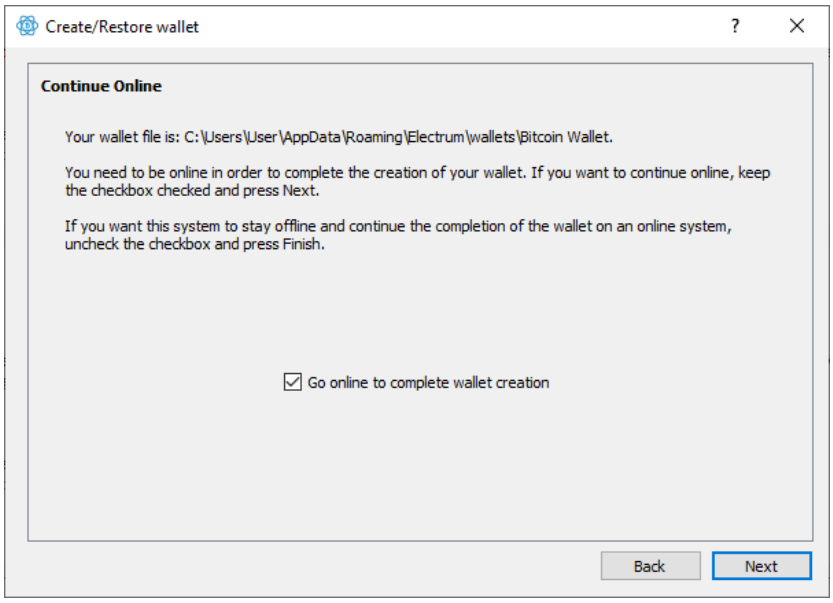
Fürs erste sollte die Seed Phrase auf einem Blatt Papier aufgeschrieben oder in einer Word- oder Textdatei abgespeichert werden. Wie man die Seed Phrase sicher aufbewahrt, wird später in Kapitel 10 näher diskutiert.



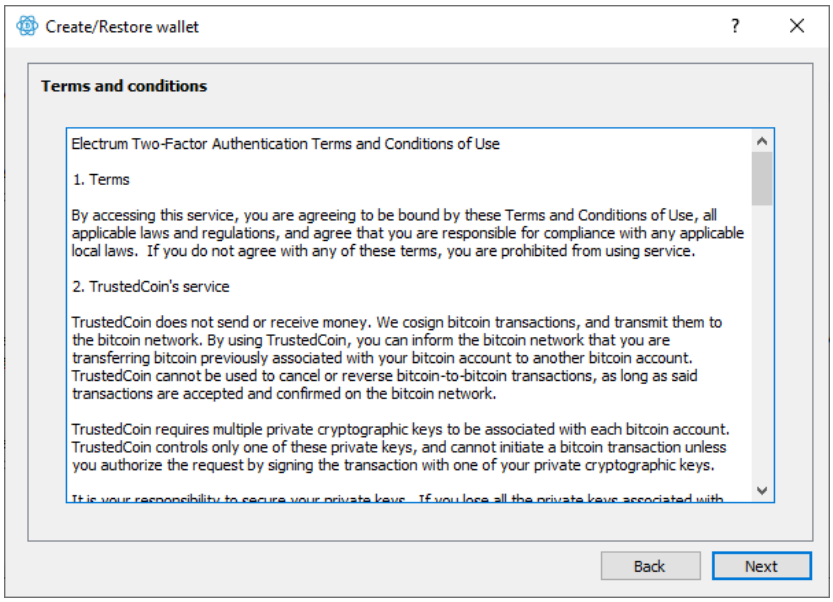
Im nächsten Schritt muss die Seed Phrase nochmals eingegeben und bestätigt werden. Nach Eingabe der Seed Phrase klicken wir auf *Next*.



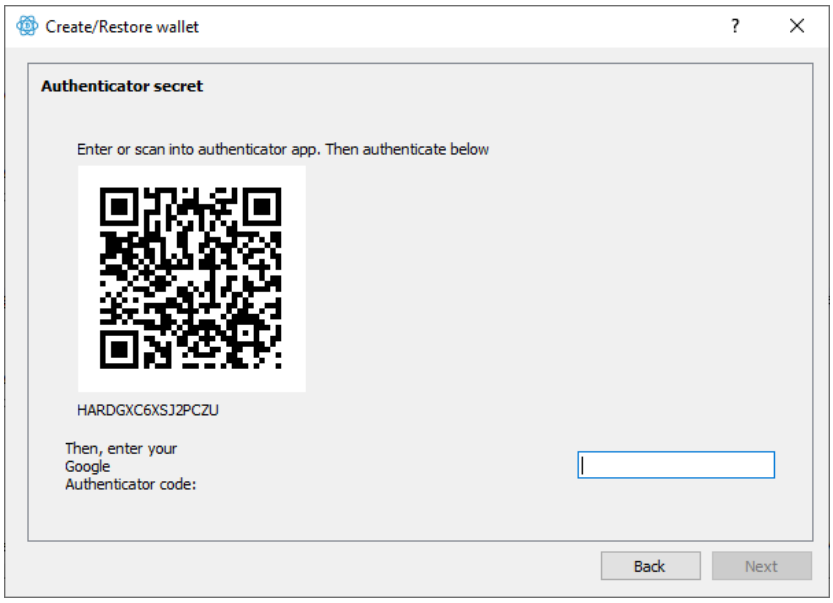
Als nächstes wird uns der Hinweis gegeben, dass für die weitere Einrichtung der Wallet eine Internetverbindung bestehen sollte. Ist die Internetverbindung aktiv, klicken wir auf *Next*.



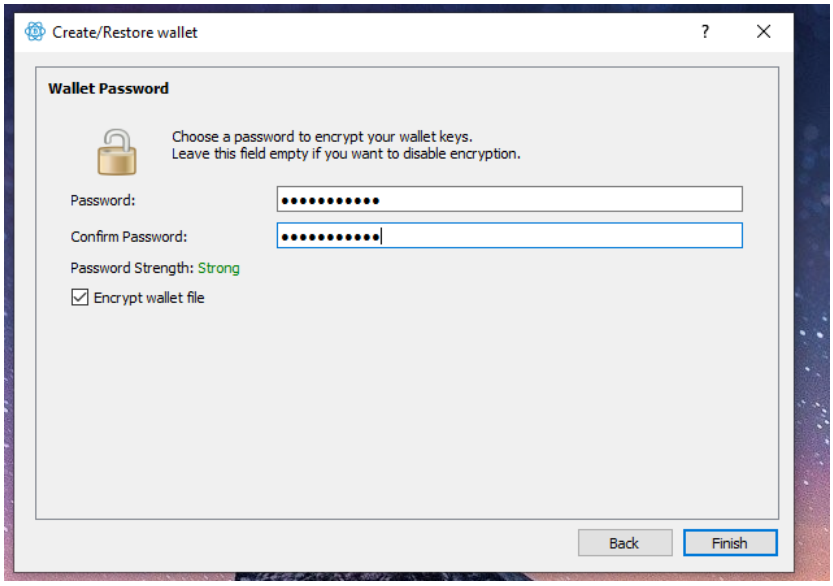
Im nächsten Schritt befinden sich die Nutzungsbedingungen der 2FA API von Trusted Coin. Nachdem wir die Nutzungsbedingungen durchgelesen haben, klicken wir wieder auf *Next*.



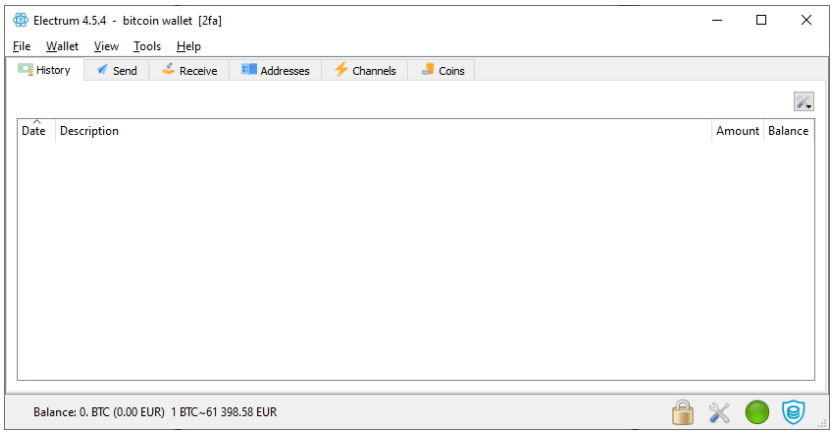
Nun sollte sich ein QR-Code im Fenster befinden, mit dem wir die Google Authenticator App verknüpfen. Dafür öffnen wir die Google Authenticator App, klicken auf das Plus-Zeichen, wählen die Option *Scan a QR code* und geben dann den Code ein, den die Google Authenticator App für die Wallet generiert. Dieser Code ist nur für eine gewisse Zeit gültig, bevor ein neuer Code generiert wird. Danach klicken wir wieder auf *Next*.



Im nächsten Schritt wird ein Passwort für die Wallet definiert, um die Wallet zu verschlüsseln. Um die Sicherheit zu erhöhen, kann/sollte dieses Passwort ein anderes Passwort sein als für den USB-Stick. Später in Kapitel 11 wird noch näher ausgeführt, wie wir die Passwörter und die Seed Phrase in einem Passwort-Manager speichern können.



Nach Festlegung des Passworts klickt man auf *Finish*, wodurch die Wallet erstellt wird und sich automatisch öffnen sollte. Electrum fragt noch nach, ob man über Updates informiert werden möchte. Es macht Sinn, die Electrum Wallet zu aktualisieren, da die Open Source Community von Electrum ständig daran arbeitet, die Sicherheit der Wallet zu erhöhen und die Funktionalitäten auszubauen. Zu beachten ist, dass Electrum aus Sicherheitsgründen keine Built-In Update Funktion implementiert hat. Das heißt, bei einem Update muss Electrum deinstalliert und neu installiert werden. Wie man ein Update durchführt, wird in Abschnit 13.6 beschrieben.



Im nächsten Schritt verlinken wir das Electrum Programm mit dem USB-Stick. Sollte kein USB-Stick für die Cold-Storage Aufbewahrung zur Verfügung stehen, ist die Konfiguration beendet und der nächste Schritt kann übersprungen werden.

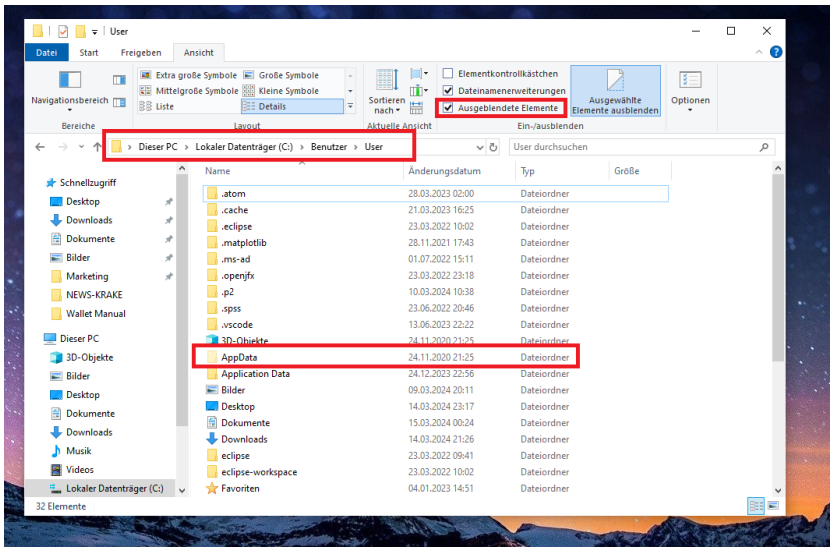
7.6 Verlinkung von Electrum mit USB-Stick

Im letzten Schritt werden nun die App Daten der Wallet auf den USB-Stick übertragen und mit dem Electrum Programm am Computer verknüpft. Das heißt, die Programm Dateien von Electrum bleiben auf dem Computer, lediglich die sensiblen Daten wie die Schlüssel der Bitcoin Wallet werden auf dem USB-Stick gespeichert.

Im Zuge der Installation der Electrum Wallet wurden vom Installer nicht nur die Programm Files im Ordner *Programme* erstellt, sondern auch ein weiterer Ordner mit den App Daten. Dieser Ordner befindet sich im Dateipfad `C:\Users\<Usernme>\AppData\Roaming`. Um in diesen Ordner zu gelangen, öffnen wir erneut den Explorer, indem man mit der rechten Maustaste auf das *Start* Symbol in der Taskleiste klickt und die Option *Explorer* auswählt. Um zum besagten Ordner zu gelangen, navigieren wir durch folgenden Pfad:

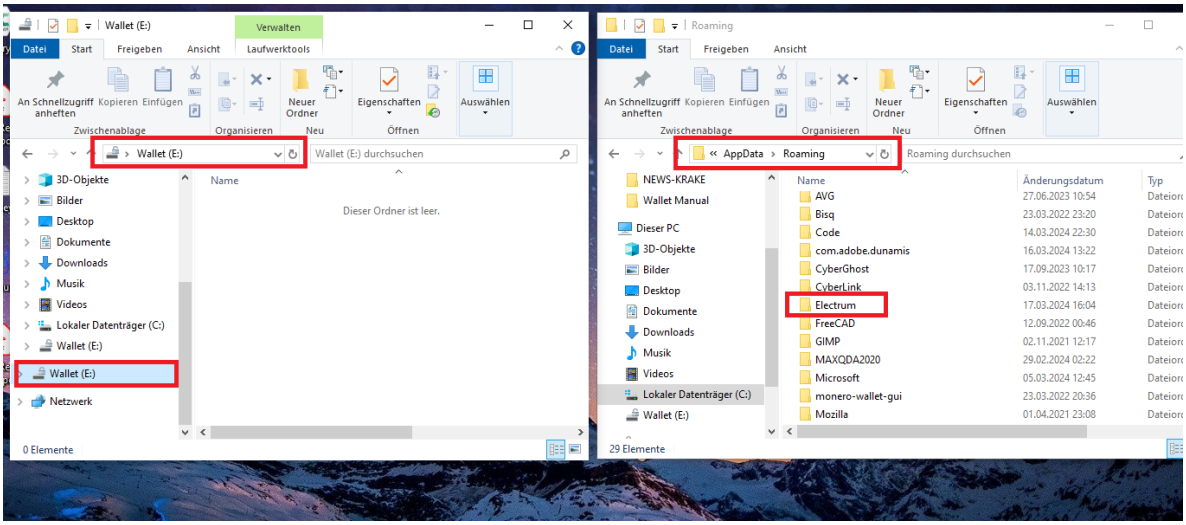
`Lokaler Datenträger (C:)` → `Benutzer` → `<Username>` (Benutzername am Computer) → `AppData` → `Roaming`

Beachtet werden muss, dass der *AppData* Ordner ein versteckter Ordner sein kann. Falls dieser Ordner nicht angezeigt wird, klickt man im Ordner `<Username>` (Benutzername am Computer) auf den Reiter *Ansicht* oben im Fenster und setzt einen Haken bei *Ausgeblendete Elemente*. Mit der Aktivierung des Häkchens sollten die versteckten Ordner angezeigt werden.



Im *Roaming* Ordner sollte sich ein Ordner mit dem Namen *Electrum* befinden, in dem sich die Wallet Datenbank und die App Daten befinden. Diese Datenbank wurde bei der Installation von Electrum neu angelegt und wird in den nachfolgenden Schritten auf den USB-Stick übertragen. Damit die Electrum Wallet weiß, dass sie auf die Datenbank auf dem USB-Stick zugreifen soll und nicht auf den *Electrum* Ordner im *Roaming* Ordner, muss der *Roaming* Ordner mit dem USB-Stick verlinkt werden. Folgende Schritte sind dafür durchzuführen.

Im ersten Schritt schließen wir die Wallet, falls sie noch geöffnet ist. Danach wird der USB-Stick an den Computer angeschlossen, das Passwort für Entschlüsselung des USB-Sticks eingegeben und der USB-Stick geöffnet. Im Optimalfall verwendet man zwei verschiedene Explorer Fenster. In einem Fenster befindet man sich im Verzeichnis des USB-Sticks (siehe unten links), im anderen Fenster befindet man sich im *Roaming* Ordner (siehe unten rechts).

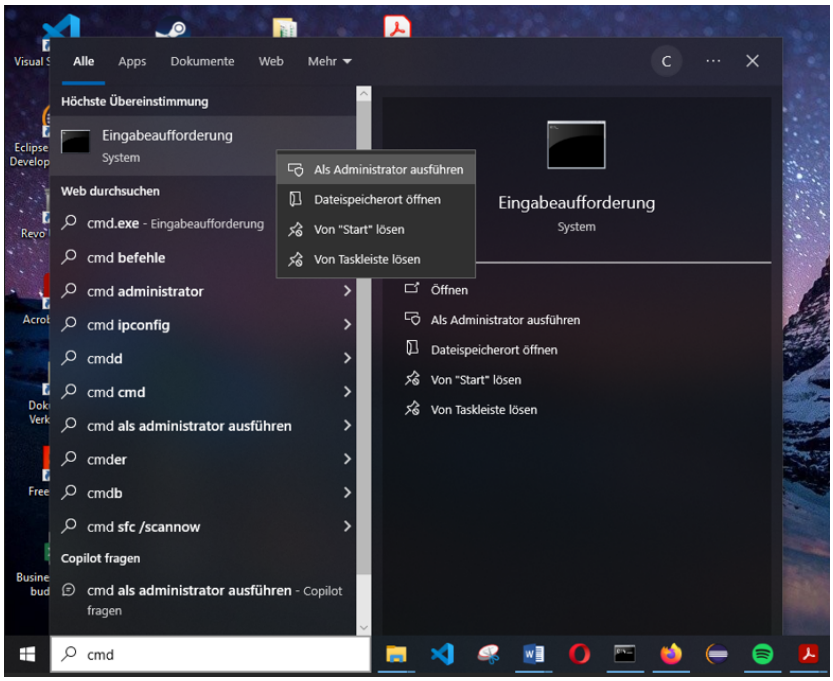


Zunächst kopieren wir den *Electrum* Ordner im *Roaming* Ordner und fügen ihn auf dem USB-Stick ein. Wurde der *Electrum* Ordner auf den USB-Stick kopiert, löschen wir den ursprünglichen *Electrum* Ordner

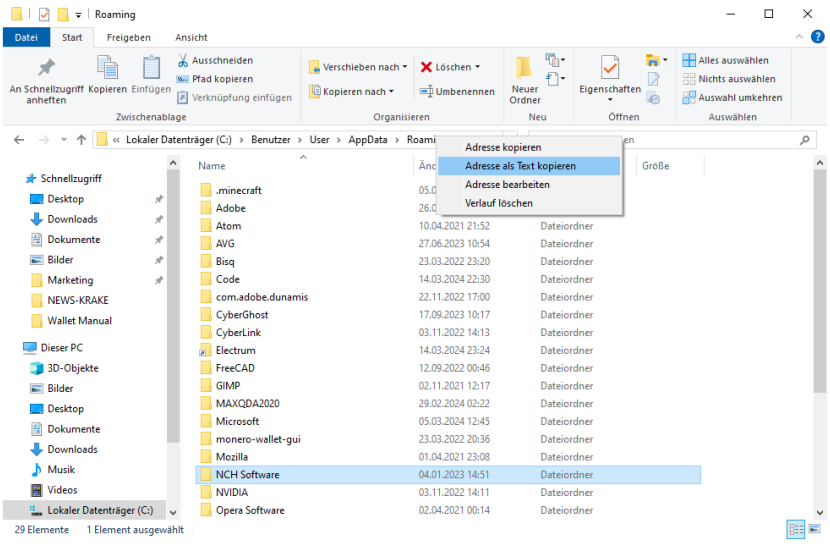
im *Roaming* Ordner. Wurde der *Electrum* Ordner aus dem *Roaming* Ordner einfach gelöscht, sollte man sicherstellen, dass man den Ordner auch aus dem Papierkorb entfernt.

Im nächsten Schritt wird die *Eingabeaufforderung* geöffnet, indem folgende Schritte durchgeführt werden:

Klick auf *Start* Symbol in der Taskleiste → `cmd` eintippen bis die *Eingabeaufforderung* erscheint → mit rechter Maustaste auf *Eingabeaufforderung* klicken → *Als Administrator ausführen* klicken. Siehe Abbildung unten.



Nun sollte sich die Windows Command Line öffnen. Bevor der *Roaming* Ordner mit dem USB Stick verlinkt wird, sollte zunächst der Pfad des *Roaming* Ordners als Text kopiert werden. Der Pfad des *Roaming* Ordners kann kopiert werden, indem im Explorer Fenster (siehe Abbildung unten) mit der rechten Maustaste im Pfad oben auf *Roaming* geklickt wird und dann die Option *Adresse als Text kopieren* ausgewählt wird.



Danach wechseln wir zur Eingabeaufforderung (Windows Command Line) und navigieren in der Command Line zum *Roaming* Ordner. Dies geschieht mit dem Command `cd <Pfad des Roaming Ordners>` (siehe Command unten). Der Pfad kann mit `STRG + V` eingefügt werden, da er im vorigen Schritt oben kopiert wurde. `cd` steht für *Change Directory* und der Pfad ist der Pfad des *Roaming* Ordners. Nach Eingabe des Commands, muss die `ENTER`-Taste gedrückt werden, um den Command auszuführen. Der eingegebene Command sieht so aus wie der Command unterhalb, lediglich der Username des Benutzers am Computer im Pfad wird sich unterscheiden.

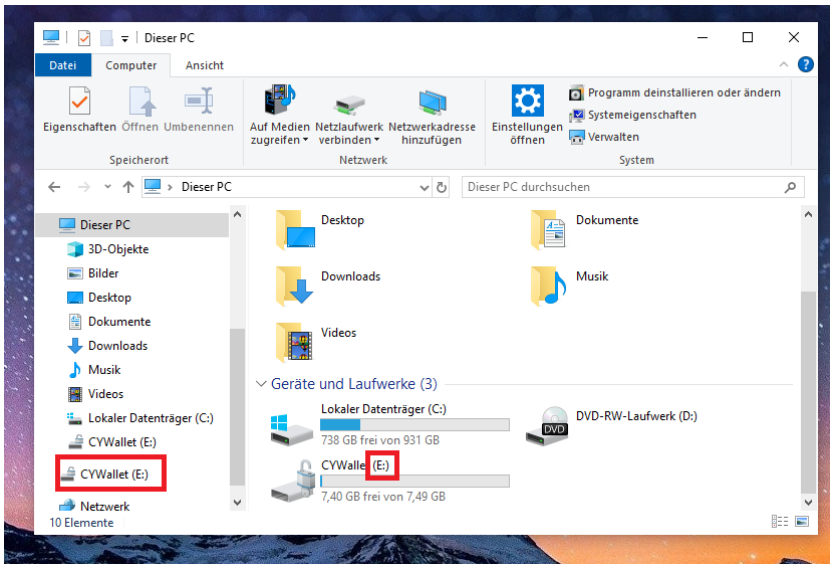
```
cd C:\Users\User\AppData\Roaming
```

Danach sollte sich der Prompt der Command Line ändern und den Pfad anzeigen, in dem sich der Cursor in der Command Line gerade befindet. In diesem Fall befindet sich der Cursor nun im *Roaming* Ordner.

Im nächsten Schritt erstellen wir einen symbolischen Link in der Command Line, der den *Roaming* Ordner mit dem *Electrum* Ordner auf dem USB-Stick verbindet. Dafür wird der Command unterhalb eingegeben, allerdings sollte der Buchstabe für die Laufwerksbezeichnung des USB-Sticks angepasst werden. In diesem Fall ist es das E-Laufwerk. Welcher Buchstabe für das USB-Stick Laufwerk verwendet wird, kann aus dem Explorer Fenster abgelesen werden (siehe Abbildung unten).

```
mklink /D Electrum E:\Electrum
```

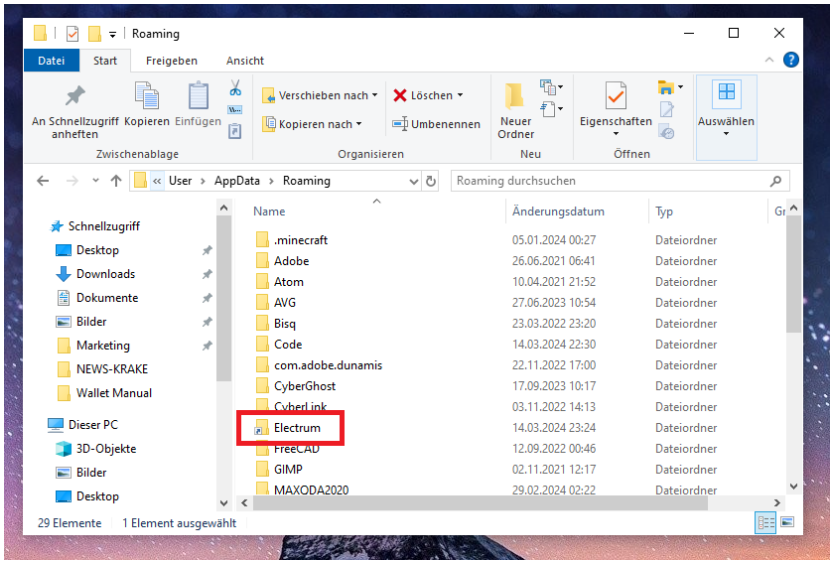
`mklink` steht für *make link*, `\D` steht für *Link zu Directory*, `Electrum` steht für den Ordnername und `E:\Electrum` steht für den Pfad des *Electrum* Ordners auf dem USB-Stick.



Nachdem der Command `mklink /D Electrum E:\Electrum` eingegeben wurde, muss die Enter-Taste gedrückt werden und der folgende Output sollte in der Command Line erscheinen:

```
symbolische Verknüpfung erstellt für Electrum <<===>> E:\Electrum
```

Nun sollte der *Roaming* Ordner mit dem USB-Stick verlinkt sein und die Electrum Wallet kann geöffnet werden. Im *Roaming* Ordner sollte nun ein neuer *Electrum* Ordner mit einem kleinen Pfeil angelegt worden sein (siehe Abbildung unten).



Damit wurde die Verlinkung des Electrum Programms mit der Datenbank auf dem USB-Stick konfiguriert. Ist der USB-Stick am Computer angeschlossen und mit dem Passwort entschlüsselt, kann die Electrum Wallet nun auf den USB-Stick zugreifen und die Wallet öffnen.

Bevor wir fortfahren, überprüfen wir, ob die Konfiguration korrekt durchgeführt wurde. Bevor man den

USB-Stick entfernt, sollte man die Wallet ordnungsgemäß schließen und den USB-Stick sicher auswerfen, indem man mit der rechten Maustaste auf den USB-Stick klickt und die Option *Auswerfen* wählt.

Nachdem die Wallet geschlossen und der USB-Stick entfernt wurde, können wir zuerst überprüfen, ob sich der *Electrum* Ordner im *Roaming* Ordner und die Electrum Wallet am Desktop öffnen lassen, wenn der USB-Stick nicht angesteckt und entschlüsselt wurde. Weder die Electrum Wallet noch der *Electrum* Ordner mit dem Pfeil im *Roaming* Ordner sollten sich öffnen lassen.

Nun überprüfen wir, ob sich die Wallet öffnen lässt, wenn der USB-Stick angesteckt und entschlüsselt wurde. Dafür schließen wir den USB-Stick an und geben das Passwort ein. Im nächsten Schritt öffnen wir mit einem Doppelklick auf die Electrum Verknüpfung am Desktop das Programm. Nun sollte das Electrum Programm starten und wir sehen die Wallet, die zuletzt geöffnet wurde. Abschließend geben wir das Passwort für die Wallet ein und klicken auf *Finish*. Die Wallet sollte sich nun öffnen.

Bevor wir mit dem Sparen und Investieren beginnen, sollte man sich um die sichere Aufbewahrung der Seed Phrase kümmern. Die Seed Phrase ist der Wiederherstellungsschlüssel, der es ermöglicht, die Wallet bei Verlust oder technischem Gebrechen wiederherzustellen. Eine ausführliche Diskussion zur Aufbewahrung der Wiederherstellungsschlüssel befindet sich in Kapitel 10.

8 Neuinstallation von Electrum

Im vorherigen Kapitel wurde eine neue Wallet erstellt und mit einem USB-Stick verknüpft. Im folgenden Kapitel werden die Verfahrensschritte beschrieben, wenn zwar der USB-Stick intakt ist, allerdings sich das Electrum Programm nicht mehr auf dem Computer befindet. Dies kann dann der Fall sein, wenn man sich einen neuen Computer zugelegt hat, das Betriebssystem neu aufgesetzt wurde oder das Electrum Programm deinstalliert wurde.

Dafür muss das Electrum Programm neu auf dem Rechner installiert werden. Zu beachten ist, dass bei der ursprünglichen Erstinstallation zwar die Programm Files auf dem Computer lokal gespeichert wurden, allerdings nicht die Datenbank der Wallet und die App Daten. Die Datenbank der Wallet wurde bei der Erstinstallation aus Sicherheitsgründen auf dem verschlüsselten USB-Stick gespeichert, um die Wallet im Cold Storage (Offline) aufzubewahren und vor Hacker-Angriffen zu schützen.

Damit die Wallet wieder auf die Datenbank auf dem USB-Stick zugreifen kann, muss nach einer Neuinstallation das Programm wieder mit dem Electrum Ordner auf dem USB Stick verlinkt werden. Grundsätzlich wurde dieser Vorgang bereits bei der Erstinstallation einmal durchgeführt, allerdings fallen einige Schritte weg. Die Neuinstallation der Electrum Wallet ist nachfolgend Schritt für Schritt beschrieben.

Abbildung 6: Verfahrensschritte bei einer Neuinstallation des Programms

- In Schritt 1 wird der Electrum Installer von der Electrum Website runtergeladen.
- In Schritt 2 wird das Programm auf dem Computer installiert.
- In Schritt 3 wird der *Roaming* Ordner mit dem USB-Stick verlinkt.

8.1 Download Electrum Installer

Siehe Kapitel 7 Abschnitt 7.2.

8.2 Installation Electrum Installer

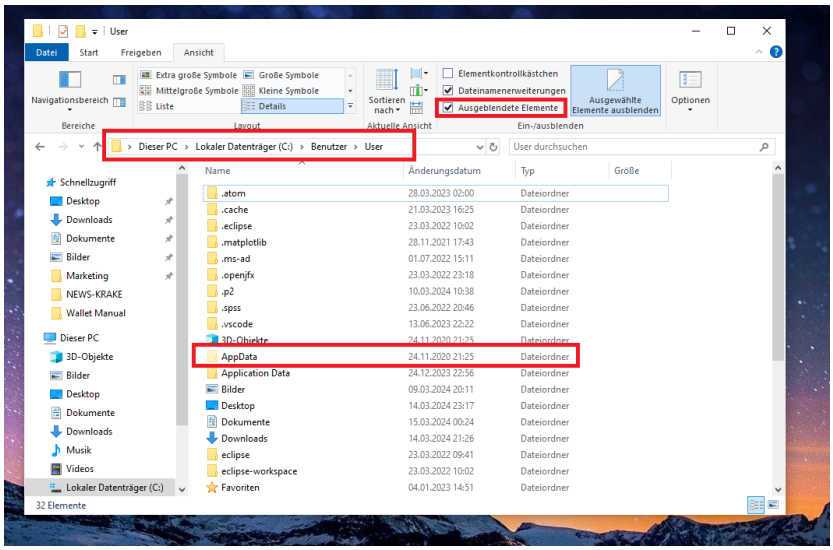
Siehe Kapitel 7 Abschnitt 7.3.

8.3 Verlinkung der App Daten mit USB

Im Zuge der Installation der Electrum Wallet wurden vom Installer nicht nur die Programm Files im Ordner *Programme* erstellt, sondern auch ein weiterer Ordner namens *Electrum*, in dem sich die App Daten und die Datenbank befinden. Dieser Ordner befindet sich im Dateipfad `C:\Users\User\AppData\Roaming`. Um in diesen Ordner zu navigieren, folgen wir den Pfad unten:

`Lokaler Datenträger (C:)` → `Benutzer` → `<Username>` (Benutzername am Computer) → `AppData` → `Roaming`

Es kann sein, dass der *AppData* Ordner versteckt ist. Falls dieser Ordner nicht angezeigt wird, können wir im Ordner `<Username>` (Benutzername am Computer) auf den Reiter *Ansicht* oben im Fenster klicken und dann einen Haken bei *Ausgeblendete Elemente* setzen. Mit diesem Schritt sollten die versteckten Ordner angezeigt werden.



Im *Roaming* Ordner, der sich im *AppData* Ordner befindet, sollte sich nach der Neuinstallation ein Ordner mit dem Namen *Electrum* befinden, in dem sich die Wallet Datenbank und die App Daten befinden. Diese Datenbank wurde neu angelegt, allerdings befindet sich unsere Datenbank bereits auf dem USB-Stick. Damit die Electrum Wallet weiß, dass sie auf die Datenbank auf dem USB-Stick zugreifen soll und nicht auf den neu erstellten *Electrum* Ordner im *Roaming* Ordner, muss der *Roaming* Ordner mit dem USB-Stick verlinkt werden. Folgende Schritten sind dafür durchzuführen:

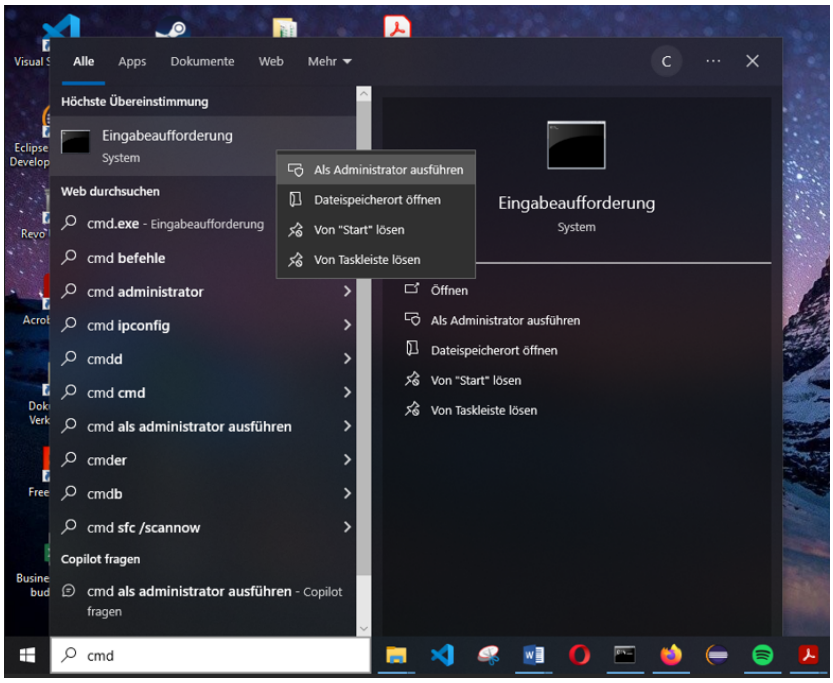
Um den *Roaming* Ordner mit dem USB-Stick zu verlinken, wird im ersten Schritt der *Electrum* Ordner aus dem *Roaming* Ordner gelöscht (rechte Maustaste auf Ordner Electrum → Löschen).

Danach schließen wir den USB-Stick an den Computer an und entschlüsseln den USB-Stick mit dem Passwort.

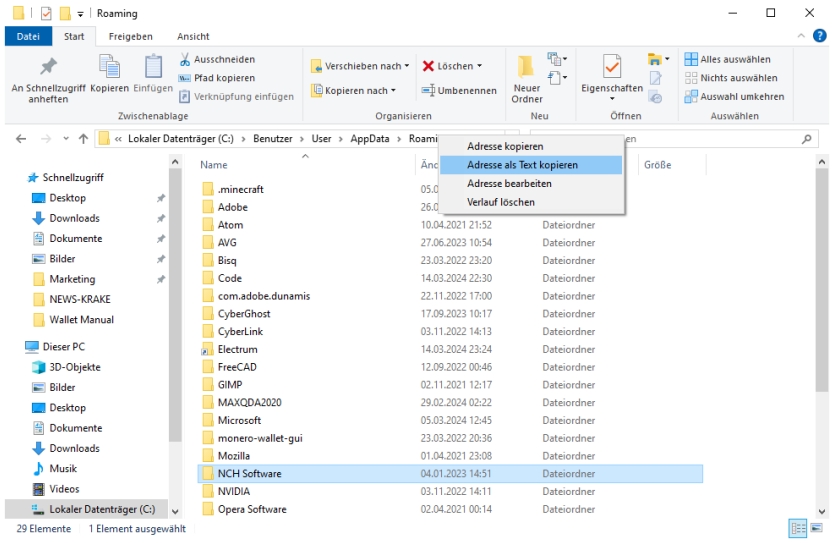
Im nächsten Schritt muss die *Eingabeaufforderung* geöffnet werden, indem folgende Schritte durchgeführt werden:

Klick auf *Start* Symbol → `cmd` eintippen bis die *Eingabeaufforderung* erscheint → rechte Maustaste auf *Eingabeaufforderung* → *Als Administrator ausführen* klicken.

Damit sollte sich die Windows Command Line öffnen.



Bevor der *Roaming* Ordner mit dem USB-Stick verlinkt wird, sollte zunächst der Pfad des *Roaming* Ordners als Text kopiert werden. Der Pfad des *Roaming* Ordners kann kopiert werden, indem wir im Explorer Fenster (siehe unten) mit der rechten Maustaste im Pfad oben auf *Roaming* klicken und dann die Option *Adresse als Text kopieren* auswählen.



Danach wechseln wir zur *Eingabeaufforderung* (Windows Command Line). In der Command Line navigieren wir nun zum *Roaming* Ordner. Dies geschieht mit dem Command `cd` und dem Pfad des *Roaming* Ordners. Der Pfad kann mit `Strg + V` eingefügt werden, da wir ihn im vorigen Schritt kopierten. `cd` steht für *Change Directory*. Der Command sollte so aussehen wie die Eingabe unten, außer dass der Username im Pfad abweicht.

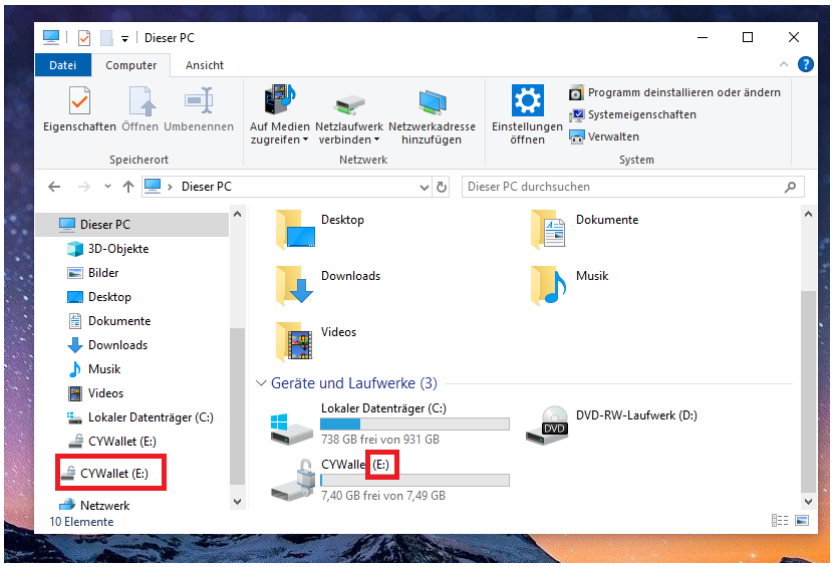
`cd C:\Users\User\AppData\Roaming`

Danach wird die ENTER-Taste gedrückt, um den Command auszuführen. Wurde der Command ausgeführt, sollte sich der Prompt der Command Line ändern und den Pfad anzeigen, indem sich der Cursor gerade befindet. In diesem Fall befindet sich der Cursor nun im *Roaming* Ordner.

Im nächsten Schritt erstellen wir einen symbolischen Link in der Command Line, der den *Roaming* Ordner mit dem *Electrum* Ordner auf dem USB-Stick verlinkt. Dafür geben wir den Command unten ein, allerdings muss möglicherweise der Buchstabe (Laufwerksbezeichnung) des USB-Sticks angepasst werden. In diesem Fall ist es das E-Laufwerk. Welcher Buchstabe für das USB-Stick Laufwerk verwendet wird, kann aus dem Explorer Fenster abgelesen werden (siehe Abbildung unten).

`mklink /D Electrum E:\Electrum`

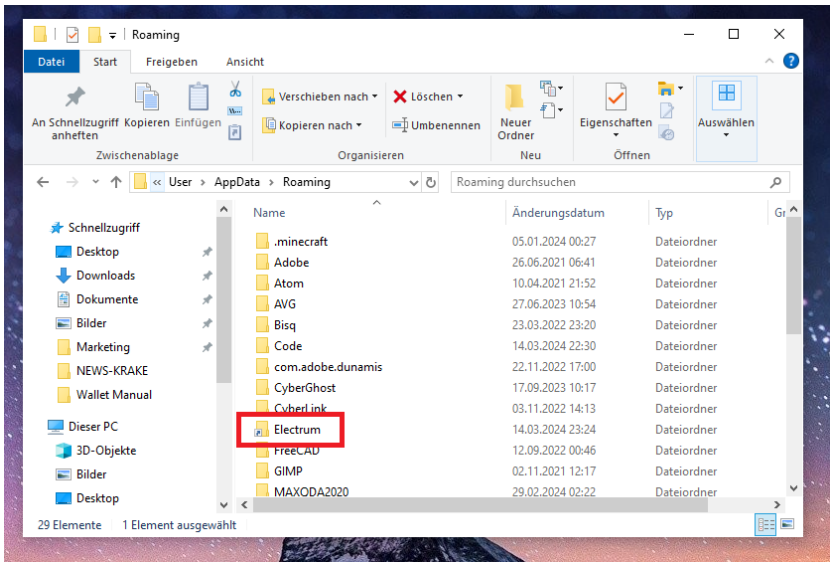
`mklink` steht dabei für *make link*, `\D` steht für *Link zu Directory*, `Electrum` steht für den Ordnernamen und `E:\Electrum` steht für den Pfad des *Electrum* Ordners auf dem USB-Stick.



Nachdem der Command `mklink /D Electrum E:\Electrum` eingegeben wurde, muss die ENTER-Taste gedrückt werden und der folgende Output sollte in der Konsole erscheinen:

`symbolische Verknüpfung erstellt für Electrum <<===>> E:\Electrum`

Nun sollte der *Roaming* Ordner mit dem USB-Stick verlinkt sein und die Electrum Wallet kann geöffnet werden. Um zu überprüfen, ob der Vorgang korrekt ausgeführt wurde, kann man zurück zum *Roaming* Ordner navigieren und kontrollieren, ob nun ein neuer *Electrum* Ordner mit einem kleinen Pfeil angelegt wurde (siehe Abbildung unten). Ist der USB-Stick nun angeschlossen und mit dem Passwort entschlüsselt, so kann die Electrum Wallet auf die Datenbank des USB-Sticks zugreifen und die Wallet öffnen.



Zusätzlich kann überprüft werden, ob sich der *Electrum* Ordner im *Roaming* Ordner oder das Electrum Programm öffnen lässt, wenn der USB-Stick nicht angesteckt ist. Weder das Programm noch der Ordner sollten sich dabei öffnen lassen.

Nach diesen Schritten sollte die Electrum Wallet wieder wie gewohnt nutzbar sein und auf die Electrum Datenbank auf dem USB-Stick zugreifen können. **ACHTUNG! Es ist möglich, dass die Verlinkung bei einer neueren Version von Electrum nicht funktioniert, da die Entwickler von Electrum die Ordnerstruktur der App Daten änderten. Ist dies der Fall, müssen wir die Wallet mithilfe der Seed Phrase wiederherstellen.**

9 Wiederherstellung der Wallet

Im vorigen Kapitel ging es um die Verfahrensschritte, wie man im Falle eines Verlustes des Programms am Computer vorgeht, um die Wallet wieder einzurichten, wie z.B. wenn man sich einen neuen Computer zulegt oder wenn man das Betriebssystem neu aufsetzt.

Im vorliegenden Kapitel geht es um die Wiederherstellung der Wallet mithilfe der Seed Phrase, wenn z.B. der USB-Stick durch ein technisches Gebrechen der Hardware ausfällt, durch Verlust oder Diebstahl des USB-Sticks oder wenn man das Wallet-Passwort vergessen hat.

Für einen solchen Fall haben wir die Seed Phrase aufbewahrt, mit der wir die Wallet wiederherstellen können. Die Seed Phrase besteht aus den zwölf Wörtern, die uns bei der Erstinstallation zugewiesen wurden. Im folgenden Abschnitt wird das Verfahren für die Wiederherstellung der Wallet beschrieben. Folgende Schritte sind dabei durchzuführen:

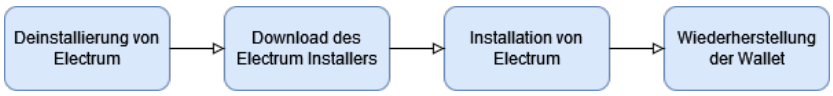


Abbildung 7: Verfahrensschritte bei der Wiederherstellung der Wallet

- In Schritt 1 wird zuerst das Programm vom Computer deinstalliert.
- In Schritt 2 wird der Electrum Installer von der Website runtergeladen.
- In Schritt 3 wird das Electrum Programm installiert.
- In Schritt 4 stellen wir die Wallet wieder her.

9.1 Deinstallierung von Electrum

Sollte das Electrum Programm noch auf dem Computer installiert sein und lediglich der USB-Stick ausgefallen sein, muss vor der Wiederherstellung der Wallet das Programm vom Computer deinstalliert werden. Sind sowohl der USB-Stick als auch der Computer ausgefallen, kann dieser Schritt übersprungen werden.

Für die Deinstallierung von Electrum klickt man unten links auf das *Start* Symbol in der Taskleiste und sucht nach der Electrum Software. Hat man die Electrum App im Startmenü gefunden, klickt man mit der rechten Maustaste auf die App und wählt die Option *Deinstallieren* aus. Damit öffnet sich ein Fenster mit einer Liste an Applikationen, die man markieren und deinstallieren kann.

Befindet sich die App nicht in der Liste, obwohl das Programm installiert ist, gibt es noch eine weitere Möglichkeit die Software zu entfernen. Dafür klickt man erneut auf das *Start* Symbol in der Taskleiste und tippt *Software* ein. Im Menü sollte nun die Option *Programme hinzufügen oder entfernen* erscheinen, die man mit einem Klick öffnet. Im Reiter *Apps und Features* erscheint eine Liste mit allen Apps, die auf dem Computer installiert sind. In dieser Liste sucht man die Electrum Software, klickt auf den Listeneintrag und klickt auf *Deinstallieren*.

Nun sollte das Programm deinstalliert sein, allerdings befindet sich noch im *Roaming* Ordner der verlinkte *Electrum* Ordner für die Wallet Datenbank auf dem USB-Stick. Dieser Ordner muss gelöscht werden, bevor man Electrum erneut installiert. Den Ordner findet man über den Pfad:

`Lokaler Datenträger C:` → `Benutzer` → `<Username>` (Benutzername am Computer) → `AppData` → `Roaming`

Der *AppData* Folder kann ein versteckter Ordner sein. Um ihn sichtbar zu machen, klickt man im `<Username>` Folder (Benutzername am Computer) auf *Ansicht* im Menüpunkt oben und aktiviert das Häkchen *Ausgeblendete Elemente*. Nun sollte der *AppData* Ordner aufscheinen.

Im *Roaming* Ordner sollte sich der verlinkte *Electrum* Ordner mit einem kleinen Pfeil befinden, den wir nun löschen.

9.2 Download Electrum Installer

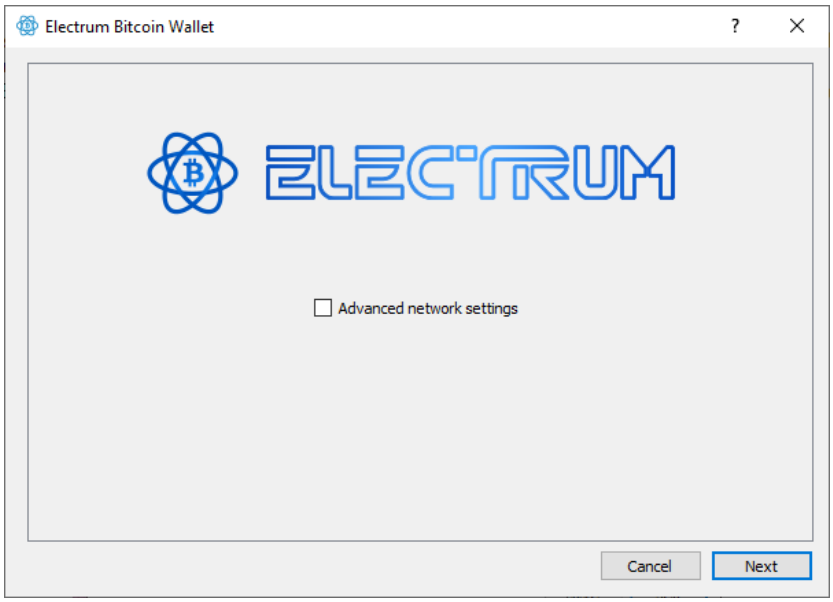
Siehe Kapitel 7 Abschnitt 7.2

9.3 Installation von Electrum

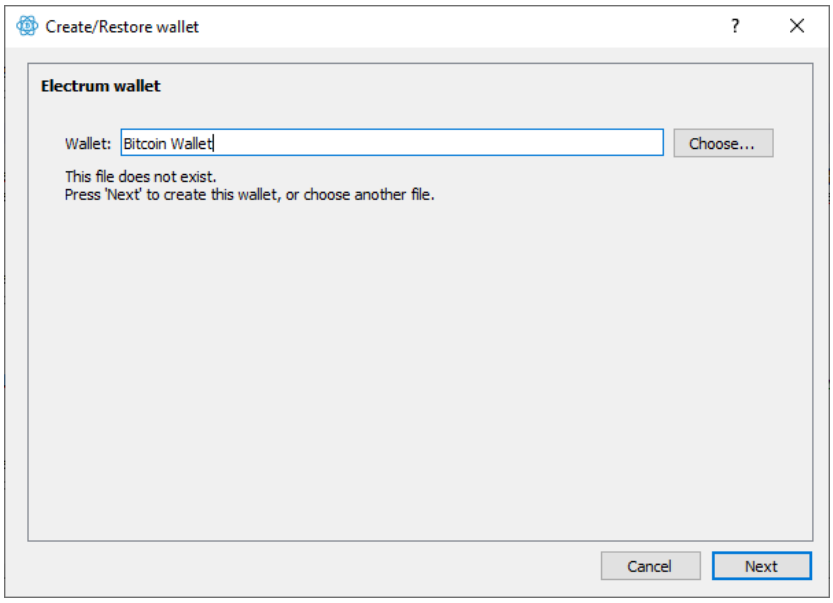
Siehe Kapitel 7 Abschnitt 7.3

9.4 Wiederherstellung der Wallet

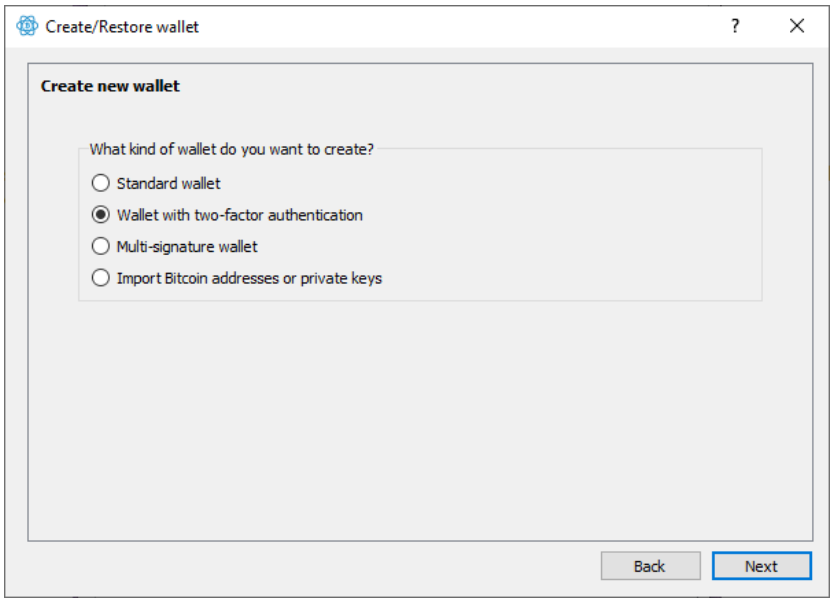
Nach der Installation von Electrum sollte sich wieder ein Electrum Icon auf dem Desktop befinden. Mit einem Doppelklick auf die Electrum Verknüpfung am Desktop öffnet sich der Konfigurationsguide von Electrum. Hier klicken wir auf *Next*, ohne einen Haken bei Netzwerkeinstellungen zu setzen.



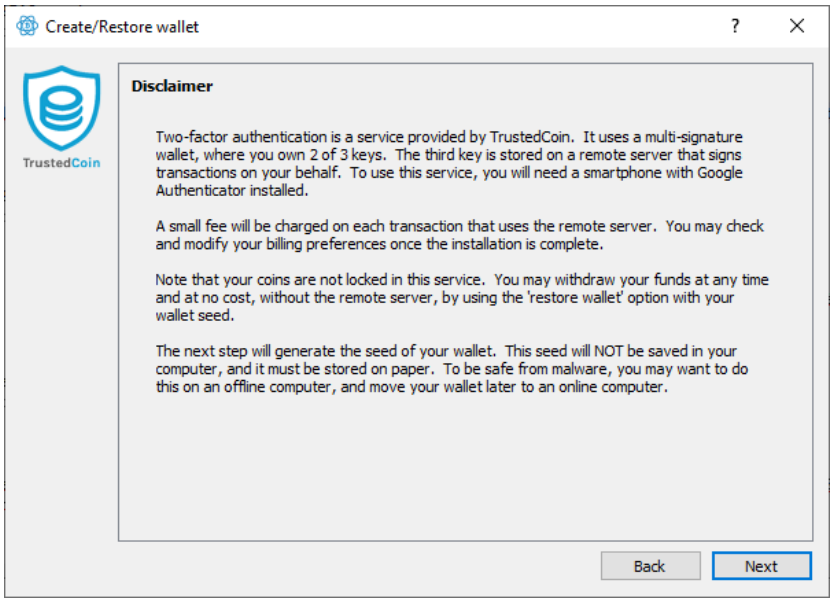
Im nächsten Schritt befindet sich ein Eingabefeld für die Bezeichnung der Wallet. Standardmäßig steht hier *default_wallet*. Nach Eingabe der Bezeichnung der Wallet, klicken wir auf *Next*.



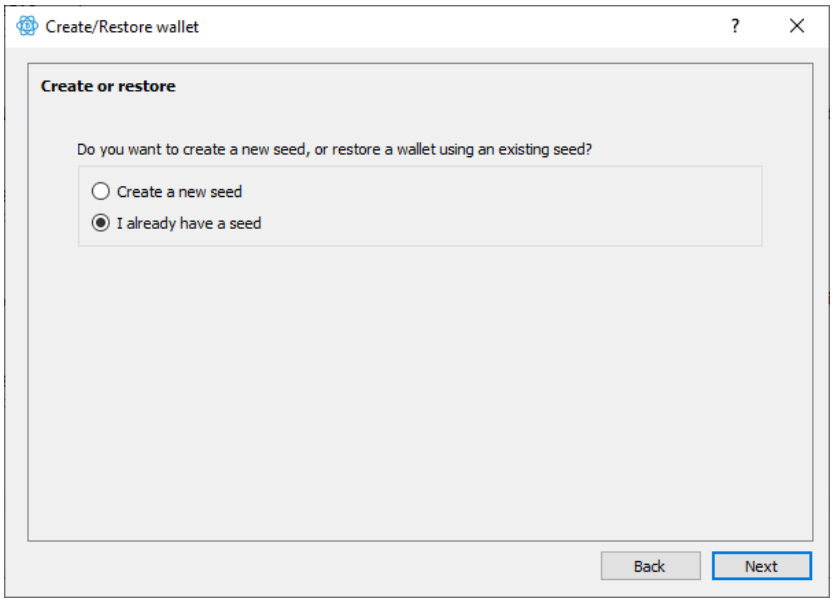
Im nächsten Schritt wählen wir aus, welche Art von Wallet man erstellen möchte. Wir wählen hier die Option *Wallet with two-factor authentication* aus und klicken auf *Next*.



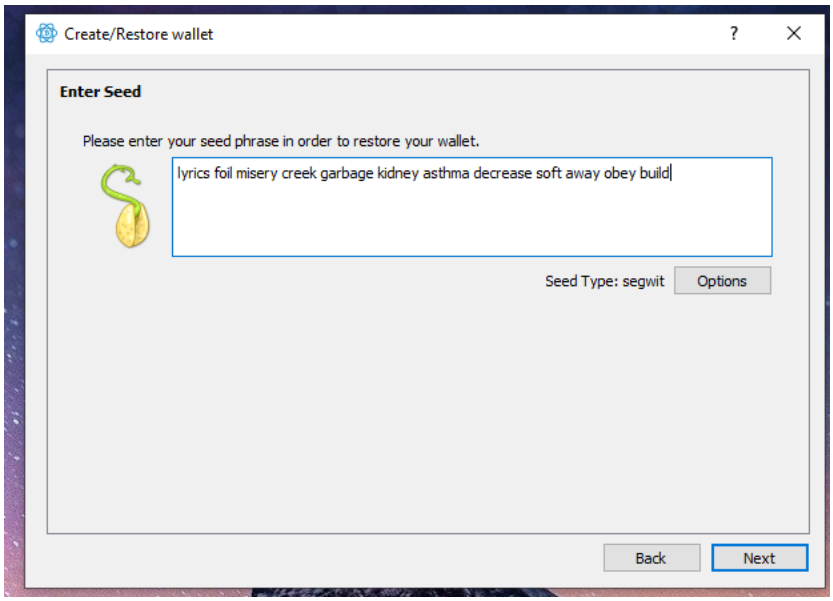
Danach erscheint der Disclaimer der 2FA API von Trusted Coin. Nachdem wir den Disclaimer durchgelesen haben, klicken wir auf *Next*.



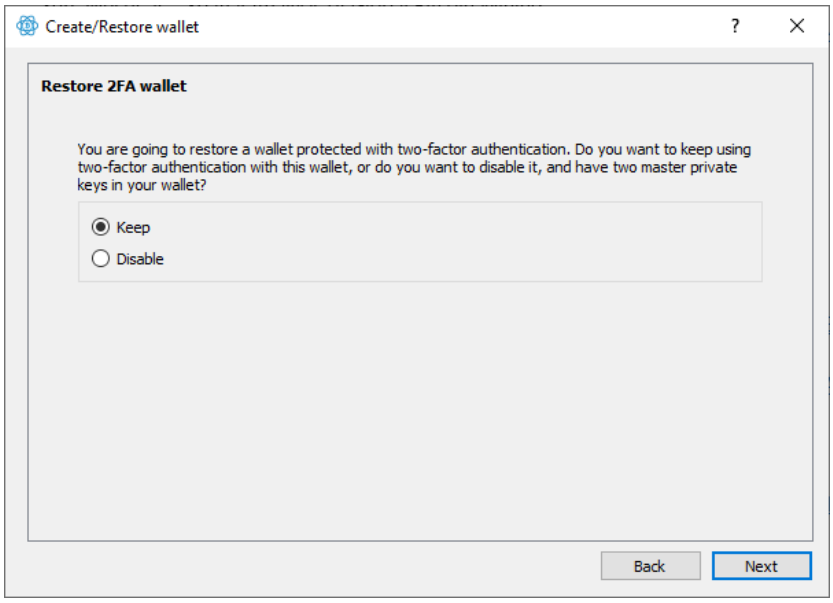
Im nächsten Schritt wählen wir aus, ob wir eine neue Wallet errichten oder eine alte Wallet wiederherstellen möchten. Hier wählen wir die Option *I already have a seed* und klicken auf *Next*.



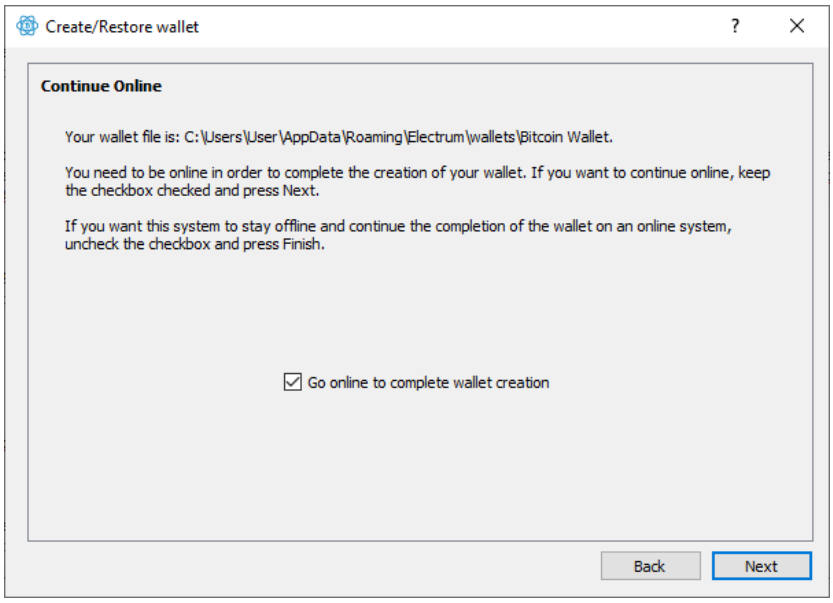
Im nächsten Fenster befindet sich ein Eingabefeld, in das wir die Seed Phrase eingeben oder reinkopieren. Die Seed Phrase ist der Schlüssel aus den zwölf Wörtern für die Wiederherstellung. Hier muss beachtet werden, dass die Reihenfolge der Wörter eingehalten wird und die Wörter mit einem Leerzeichen getrennt werden.



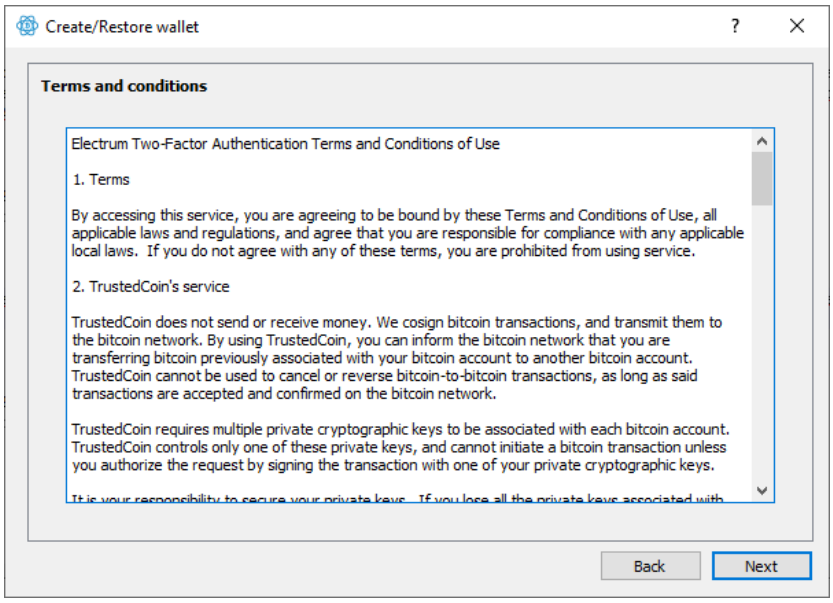
Danach werden wir gefragt, ob wir die 2-Factor Authentication, die mit der Wallet bei der Erstinstallation verknüpft wurde, beibehalten möchten. Möchte man die 2-Factor-Authentication deaktivieren, wechselt man praktisch zu einer Multi-Sig Wallet mit zwei Private Keys in der Wallet. In diesem Fall verknüpfen wir die Wallet erneut mit der Google Authenticator App.



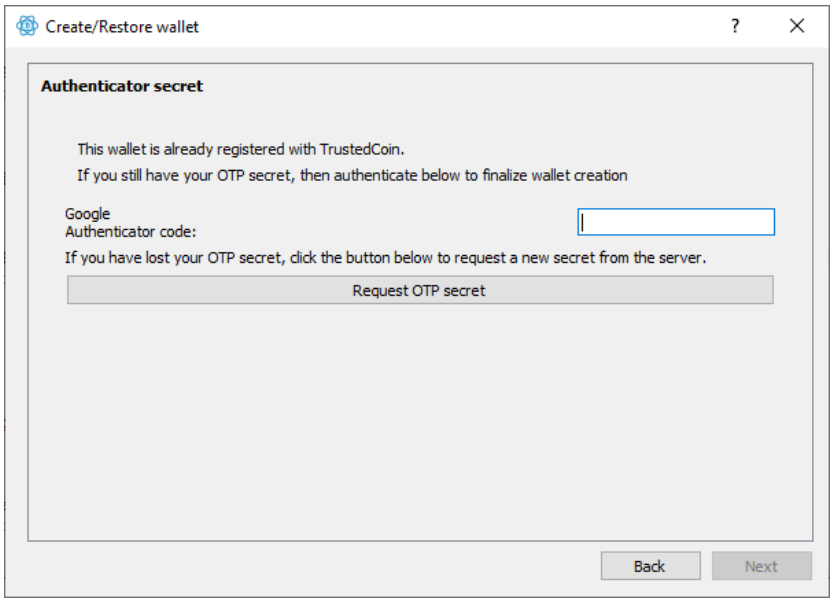
Nachdem wir auf *Next* klicken, erscheint ein Hinweis, dass wir für die Fertigstellung der Wallet eine Internetverbindung benötigen, um die Wallet mit der Google Authenticator App zu verknüpfen. Nun klicken wir wieder auf *Next*.



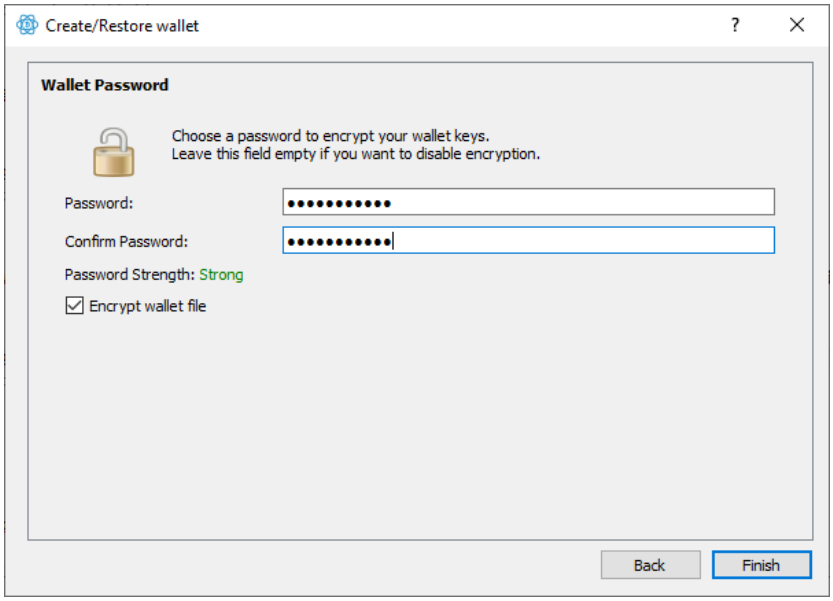
Im nächsten Schritt lesen wir die Nutzungsbedingungen und klicken wieder auf *Next*.



Nun öffnen wir die Google Authenticator App und geben den Code ein, den die App für die Bitcoin Wallet generiert. Danach klicken wir auf *Next*.



Im letzten Schritt definieren wir ein Passwort für die Wallet. Klickt man nun auf *Finish*, ist die Wiederherstellung abgeschlossen und die Wallet sollte sich öffnen.



Um nun die Wallet wieder mit einem hohen Sicherheitsstandard einzurichten, kann man die Schritte in Kapitel 7 wiederholen. Die offenen Schritte für die ursprüngliche Konfiguration wären:

- Konfiguration des USB-Sticks (Abschnitt 7.1)
- Verlinkung der Wallet App Daten mit USB-Stick (Abschnitt 7.6)

ACHTUNG! Bei Verlust oder Diebstahl des USB-Sticks, wird empfohlen, nach der Wiederherstellung der Wallet die Bitcoins auf eine neu errichtete Wallet zu transferrieren. Dafür öffnen wir nach

der Wiederherstellung der Wallet das Electrum Programm mit einem Klick auf die Electrum Verknüpfung am Desktop und klicken im Startbildschirm auf den Button *Create new wallet*. Danach erstellt man eine neue Standard Wallet mit einer neuen Seed Phrase. Wurde die neue Wallet mit der neuen Bitcoin Adresse erstellt, öffnen wir die alte Wallet und senden die Bitcoins auf die neue Adresse.

10 Aufbewahrung der Wiederherstellungsschlüssel

Im Rahmen der Installation und Konfiguration der Bitcoin Wallet wurde ein Wiederherstellungsschlüssel (Seed Phrase) generiert, der aus zwölf Wörtern besteht und mithilfe dessen die Wallet wiederhergestellt werden kann. Eine Wiederherstellung der Wallet kann verschiedene Gründe haben, wie etwa der Verlust des USB-Sticks, ein technisches Gebrechen der Hardware oder bei Diebstahl. Zudem kann es passieren, dass man das Wallet Passwort oder das Passwort für den USB-Stick vergisst. Für all diese Fälle können wir auf die Seed Phrase zurückgreifen.

Allerdings stellt sich die Frage, wie man die Seed Phrase sicher aufbewahrt und vor unterschiedlichen Risiken schützt. Jede Person im Besitz der Seed Phrase kann die Wallet wiederherstellen und auf die Ersparnisse zugreifen. Die Seed Phrase sollte daher an niemandem weitergegeben werden. Im folgenden Abschnitt wird eine Reihe an Szenarien und Risiken diskutiert, die bei der Aufbewahrung der Seed Phrase berücksichtigt werden sollten. Zudem werden Lösungen vorgeschlagen, die das Risiko eines Verlustes auf ein Minimum reduzieren.

Die Umsetzung einer konkreten Strategie wird umso wichtiger, je mehr Bitcoins über die Zeit gespart wurden. Investiert man sofort eine höhere Summe in Bitcoin, sollte man ohne zu zögern eine geeignete Aufbewahrungsstrategie entwickeln und implementieren. Geht man eher langsamer vor und investiert in regelmäßigen Abständen kleinere Summen, kann man vorrübergehend die Seed Phrase auf Papier aufschreiben und an einem sicheren Ort verwahren. Allerdings wird empfohlen, dass man sich zeitnah um eine geeignete Lösung kümmert.

Eine sichere und zuverlässige Strategie zur Aufbewahrung der Seed Phrase involviert die Kombination von drei Konzepten: (1) Redundanz, (2) Security Layer und (3) kryptographische oder physische Verschlüsselung.

10.1 Redundanz

Redundanz bedeutet, dass man die Seed Phrase nicht nur an einem Ort und mithilfe einer einzigen Methode aufbewahrt, sondern dass man mehrere Backups hat und wenn möglich an unterschiedlichen Orten. Damit bedient man sich der Strategie der Diversifizierung und setzt nicht alles auf eine Karte. Sollte eine Aufbewahrungsmethode ausfallen, hat man noch immer eine zweite oder eine dritte Möglichkeit, auf die Seed Phrase zuzugreifen und die Wallet wiederherzustellen.

Bei der Aufbewahrung der Schlüssel auf einem digitalen Datenträger sollte ein zweites Backup erstellt werden, falls ein Datenträger durch technisches Gebrechen nicht mehr verwendbar sein sollte.

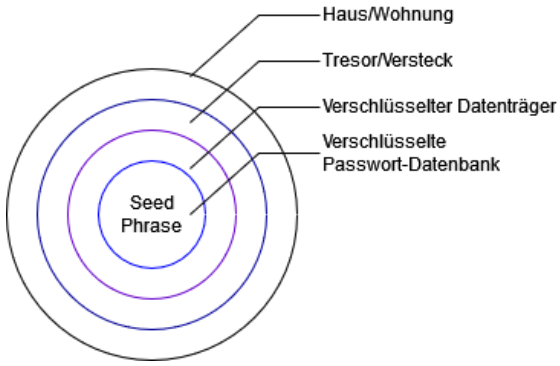
Redundanz ist vor allem dann gegeben, wenn die Seed Phrase an mindestens zwei unterschiedlichen, physisch getrennten Orten aufbewahrt wird. Man nehme an, die Seed Phrase wurde auf zwei digital verschlüsselten Datenträgern gespeichert, die beide im eigenen Haus oder in der Wohnung aufbewahrt werden. Zwar kann bei Ausfall eines einzelnen Datenträgers auf den zweiten Datenträger ausgewichen werden, allerdings bleiben dabei mögliche Risiken unberücksichtigt, wie Wohnungseinbrüche und Diebstahl, Feuer- und Wasserschäden oder Zerstörungen durch Erdbeben, Tsunamis oder Erdrutsche.

Redundanz bedeutet auch, dass eine weitere Vertrauensperson, wie etwa ein Ehepartner, Kinder oder ein Elternteil im Todesfall Zugang zur Seed Phrase erhält und die Ersparnisse weitervererbt werden können. Daher sollte eine Aufbewahrungsstrategie auch den digitalen Nachlass berücksichtigen, insbesondere wenn es sich um höhere Summen handelt, die im Laufe der Jahre angespart wurden.

10.2 Security Layer

Ein weiterer Ansatz, der mit der Redundanz kombiniert werden sollte, ist die Verwendung mehrerer Security Layer. Die Verwendung mehrerer Security Layer bedeutet, dass man als Angreifer oder Dieb nicht nur eine einzige Barriere zu überwinden hat, sondern mehrere Layer, bis man zur Seed Phrase gelangt. Damit erhöht man nicht nur die Kosten für einen Angreifer, um einen Angriff präventiv zu verhindern, sondern man verschafft sich im Falle des Falles auch Zeit, um auf einen Diebstahl zu reagieren und die Bitcoins auf eine neue Wallet zu transferrieren.

Security Layer können sowohl aus digitalen als auch aus physischen Barrieren bestehen. Zudem können digitale und physische Layer kombiniert werden. Z.B. kann man die Seed Phrase in einer Passwort Datenbank speichern und verschlüsseln, die auf einem verschlüsselten externen Datenträger gespeichert ist, der wiederum in einem verschlüsselten Tresor aufbewahrt wird.



Security Layer können auch so implementiert werden, dass sie für den digitalen Nachlass geeignet sind. Z.B. kann man das Passwort für die Passwort-Datenbank mit einer Vertrauensperson teilen, die aber erst im Todesfall Zugang zum physischen Security Layer erhält, wie etwa zu einem Schließfach.

10.3 Verschlüsselung

Neben der physisch getrennten Aufbewahrung der Seed Phrase sollte auch dafür gesorgt werden, dass die beiden Aufbewahrungsorte sicher sind, um einen unauthorisierten Zugriff zu verhindern. Wird die Seed Phrase bspw. auf einen digitalen Datenträger verwahrt, sollte der Datenträger oder die Passwort-Datenbank verschlüsselt sein.

Neben USB-Sticks und externen Festplatten nutzen viele Menschen Cloud-Services. Allerdings sind Cloud-Lösungen mit Risiken verbunden. Einer der wichtigsten Gründe, der gegen Cloud-Services spricht, ist, dass Clouds permanent mit dem Internet verbunden sind und somit von Hackern angegriffen werden können. Darüber hinaus muss man dem Betreiber der Cloud ein hohes Vertrauen entgegen bringen.

Auch für die physische Aufbewahrung der Seed Phrase sollte sichergestellt werden, dass ein unauthorisierter Zugriff verhindert wird. Bei der physischen Aufbewahrung wird oftmals auf ein Versteck zurückgegriffen. Allerdings können Verstecke auch Tücken und Risiken aufweisen, wie z.B. dass man über die Zeit vergisst, wo sich die Seed Phrase befindet, oder dass man bei einem Umzug vergisst das Versteck zu räumen. Darüber hinaus kann ein Versteck gefunden oder durch physischen Einfluss zerstört werden.

Ähnlich wie bei digitalen Datenträgern sollte die Seed Phrase auch bei einer physischen Aufberwahrung verschlüsselt werden, wie etwa mithilfe eines Tresors. Allerdings involvieren Tresore im Haus Risiken. Handelt

es sich um einen relativ kleinen Tresor, der nicht ausreichend am Ort befestigt ist, können Diebe den Tresor stehlen. Ist man bspw. für mehrere Tage oder Wochen auf Reisen, haben Diebe alle Zeit der Welt den Tresor mitzunehmen und in einer Werkstatt zu öffnen, insbesondere wenn man keine Alarmanlage installiert hat, die direkt mit einer Polizeiwache verbunden ist.

Eine der besten Lösungen für eine physische Aufbewahrung ist ein Schließfach bei einer Bank oder einem Tresordienstleister. Die Tresore bestehen in der Regel aus dicken und hitzeresistenten Stahlwänden, die nicht nur schwer für Diebe zu durchdringen sind, sondern auch einen hohen Feuerschutz bieten. Zudem nutzen Tresordienstleister mehrere technische Security Layers und sind oftmals mit Sicherheitspersonal ausgestattet. Darüber hinaus bieten Schließfächer auch Platz für weitere Wertgegenstände, wie Edelmetalle, Schmuck, Uhren, Datenträger, wichtige Dokumente oder andere Gegenstände. Zudem wird bei der Anmietung eines Schließfaches meist auch eine Versicherung mitabgeschlossen. Schließfächer können ab ca. EUR 200.- pro Jahr je nach Größe des Schließfaches angemietet werden.

10.4 Beispiel einer Aufbewahrungsstrategie

Die folgende Strategie beschreibt eine mögliche Methode zur Sicherung der Seed Phrase. Folgende Zielsetzungen verfolgt die Strategie:

- Eine sichere Aufbewahrung
- Eine praktikable Aufbewahrung
- Ein günstiger Lösungsansatz
- Zugang zur Wallet für Familienmitglieder im Todesfall

Um diese Zielsetzungen zu erreichen, werden die Ansätze Redundanz, Security Layer und Verschlüsselung miteinander kombiniert. Folgende Strategie könnte konkret implementiert werden:

- Die Seed Phrase wurde in einem ersten Schritt auf zwei unterschiedlichen USB-Sticks (Datenträger A und Datenträger B) gespeichert.
- Auf beiden Datenträgern befindet sich eine Datenbank eines Passwort-Managers. Als Passwort-Manager wurde in beiden Fällen das Open-Source Programm KeePass2 verwendet (Siehe Kapitel 11). Beide KeePass2-Datenbanken sind mit unterschiedlichen Master-Passwörtern verschlüsselt.
- Bei Datenträger A ist nicht nur die KeePass2 Datenbank verschlüsselt, sondern auch der Datenträger selbst. Das Passwort für die Entschlüsselung von Datenträger A und das Master-Passwort für die KeePass2 Datenbank unterscheiden sich voneinander.
- Bei Datenträger A, bei dem nicht nur die KeePass2-Datenbank verschlüsselt ist, sondern auch der Datenträger selbst, wird zuhause aufbewahrt und erlaubt einen schnellen Zugriff auf die Seed Phrase im Falle des Falles. Der USB-Stick wird in der Wohnung so verstaut oder versteckt, dass er im Falle eines Wohnungseinbruchs nicht auffällt oder gefunden werden kann. Im besten Fall wird er physisch mit einem Schlüssel versprerrt, z.B. in einem Tresor oder in einem Schreibtischfach.
- Datenträger B, auf der lediglich die KeePass2 Datenbank verschlüsselt ist und nicht der Datenträger selbst, wird in einem Schließfach bei einem Tresordienstleister verwahrt. Das Passwort zur Entschlüsselung der KeePass2-Datenbank auf Datenträger B wurde einer Vertrauensperson weitergegeben, die im Todesfall verständigt wird und physischen Zugang zum Schließfach erhält.

Mit dieser Strategie wird die Redundanz sichergestellt, indem zwei Datenträger verwendet werden und beide an zwei physisch voneinander getrennten Orten aufbewahrt werden. Fällt ein Datenträger aufgrund eines technischen Gebrechens oder einer physischen Zerstörerung aus, kann man auf den zweiten Datenträger zurückgreifen. Darüber hinaus erhält im Todesfall eine Vertrauensperson Zugang zum Datenträger im Schließfach.

Beide Datenträger sind zudem mithilfe mehrerer Security Layers gesichert. Datenträger A befindet sich in einem guten Versteck oder in einem Tresor verschlossen in der Wohnung, der Datenträger selbst ist verschlüsselt sowie die KeePass2-Datenbank wurde verschlüsselt. Somit wurde er mit drei Security Layer gesichert. Datenträger B beinhaltet die verschlüsselte KeePass2-Datenbank und wird in einem Schließfach in einem Tresor aufbewahrt, der zudem durch mehrere technische und physische Layer des Tresordienstleisters geschützt ist. Für beide Datenträger sind also mehrere Hürden zu überwinden, um zur Seed Phrase zu gelangen.

In beiden Fällen werden zudem kryptographische Methoden in Form von Passwort-Managern eingesetzt und beide Datenträger werden offline aufbewahrt, sodass sie vor Hacker-Angriffen geschützt sind.

10.5 Weitere Aufbewahrungsmethoden

Um die Seed Phrase sicher zu verwahren, gibt es noch weitere Aufbewahrungsmethoden und Strategien. Folgende gängige Methoden können noch genannt werden:

- **Paper Backup:** Hierbei wird die Seed Phrase auf einem Blatt Papier aufgeschrieben und das Blatt Papier sicher verwahrt. Grundsätzlich sollte sichergestellt werden, dass das Blatt Papier sicher vor Feuer- oder Wasserschäden, Schimmel oder Diebstählen aufbewahrt wird.
- **Metall Backup:** Bei Metall Backups wird die Seed Phrase auf einer Metallplatte (Stahl) eingraviert oder mit eingestampften Löchern auf der Platte gespeichert, um es vor Wasser, Feuer oder anderen Risiken zu schützen. Ein Beispiel dafür ist die Firma BlockPlate `https://blockplate.com`
- **Digitales Backup:** Beim digitalen Backup wird die Seed Phrase auf einem digitalen externen Datenträger gespeichert, auf dem die Seed Phrase mithilfe eines Passwort-Managers verschlüsselt wird. Bei digitalen Datenträgern sollte ein digitales oder physisches Backup aufbewahrt werden.
- **Unauffälliges Versteck:** Mit einem unauffälligen Versteck ist gemeint, dass die Seed Phrase auf eine schlaue Art und Weise verwahrt wird, sodass sie nicht gefunden werden kann.

11 Nutzung eines Passwort-Manager

Der folgende Abschnitt beinhaltet eine Anleitung zur Installation und Konfiguration des KeePass2 Passwort-Managers, mit dem die Seed Phrase für die Bitcoin Wallet gespeichert und verschlüsselt werden kann. Die Seed Phrase ist zentral, um bei einem Verlust oder technischen Gebrechen der Hardware die Wallet wiederherstellen zu können. Im Zuge der Erstinstallation der Wallet wurde zusätzlich zur Seed Phrase auch ein Bitlocker Wiederherstellungsschlüssel generiert, um das Passwort des USB-Sticks wiederherzustellen. Beide Schlüssel können mithilfe des KeePass2 Passwort-Managers gesichert werden.

Ein Passwort-Manager verwendet kryptographische Verschlüsselungen, um verschiedene Passwörter mit einem einzelnen Master-Passwort zu speichern und zu verwalten. Der KeePass2 Passwort-Manager ist nicht nur zur Sicherung der Seed Phrase für Bitcoin geeignet, sondern auch für andere Passwörter. Der Vorteil dabei ist, dass man für verschiedene Verschlüsselungen und Accounts unterschiedliche komplexe Passwörter verwenden kann, zugleich man sich aber nur ein einzelnes Master-Passwort merken muss. Zusätzlich kann man sich vom Passwort-Manager auch starke Passwörter generieren lassen.

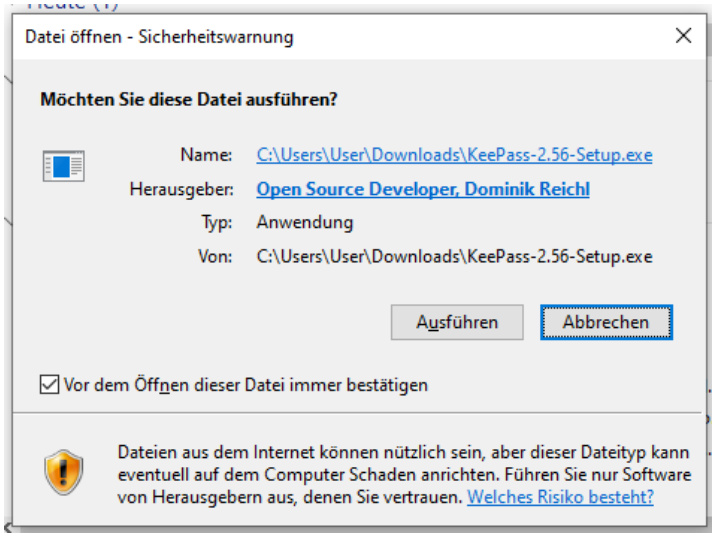
KeePass2 ist ein OpenSource Verschlüsselungsprogramm und Passwort-Manager, der lokal am Computer installiert wird. Mit dem Passwort-Manager legt man eine KeePass2-Datenbank an, in der die Passwörter gespeichert und verschlüsselt werden. Die Datenbank kann in weiterer Folge auf einem externen Datenträger gespeichert werden. Es macht Sinn, auch ein Backup der Datenbank anzulegen, indem man die Datenbank einfach kopiert und auf einem weiteren Datenträger speichert. Möchte man eine Datenbank einsehen, öffnet man den KeePass2 Passwort-Manager und wählt die entsprechende Datenbank aus.

11.1 Installation von KeePass2

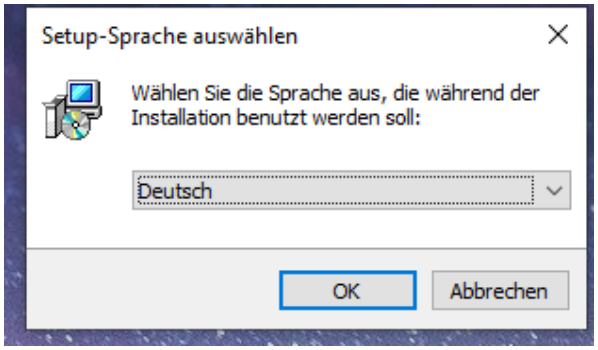
Im ersten Schritt wird der KeePass2 Passwort-Manager von der Website `https://keepass.info/download.html` runtergeladen. Für den Windows Installer wählen wir die .exe Setup Datei. Mit einem Klick auf den *Download-Now* Button wird man auf SourceForge umgeleitet, wo der Download nach wenigen Sekunden automatisch startet. Der Installer sollte sich nach dem Download im *Downloads* Ordner befinden.

Mit einem Doppelklick auf die Setup-Datei öffnet sich ein Fenster mit den Buttons *Ausführen* und *Abbre-*

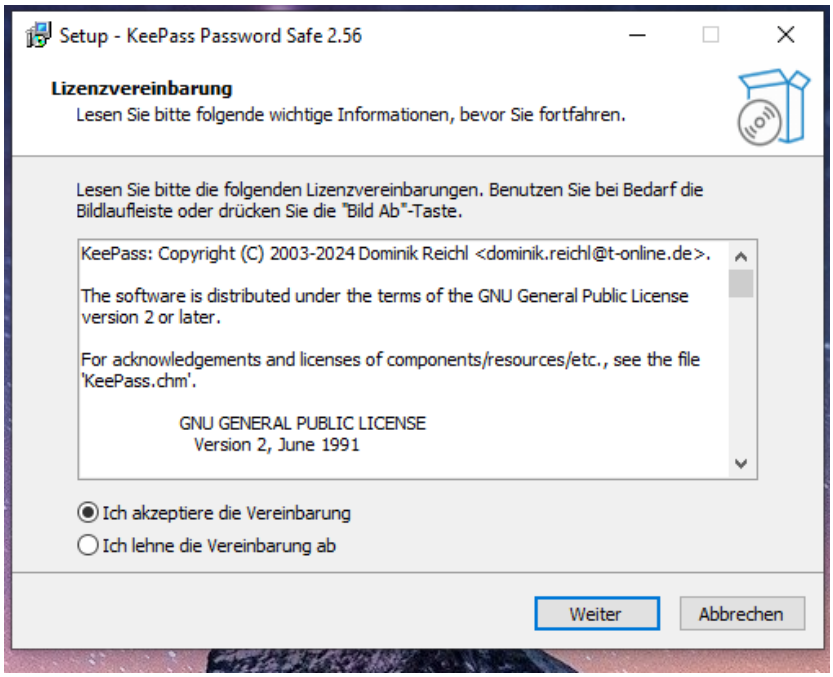
chen. Um die Installation zu starten, klicken wir auf *Ausführen*.



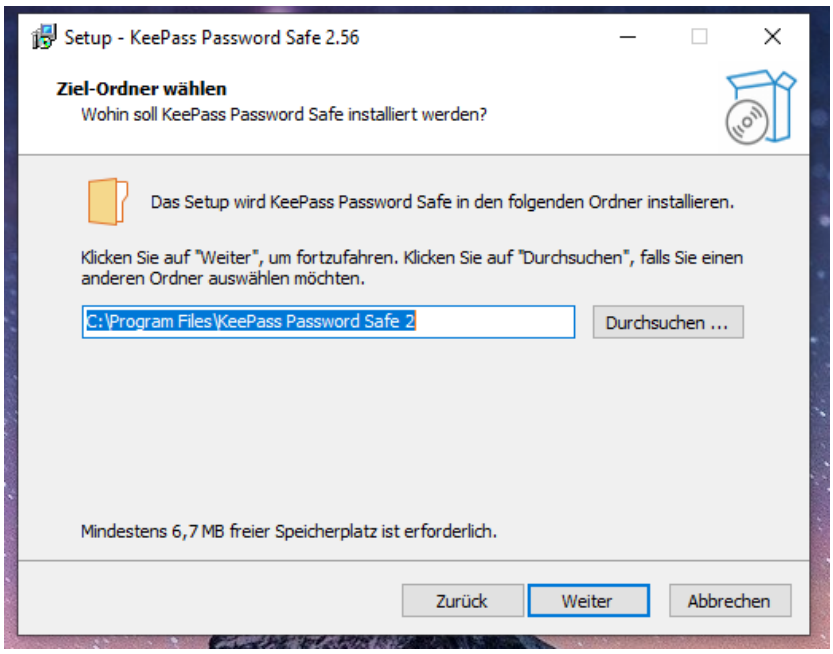
Danach wählen wir die Sprache des Installers aus und klicken auf *OK*.



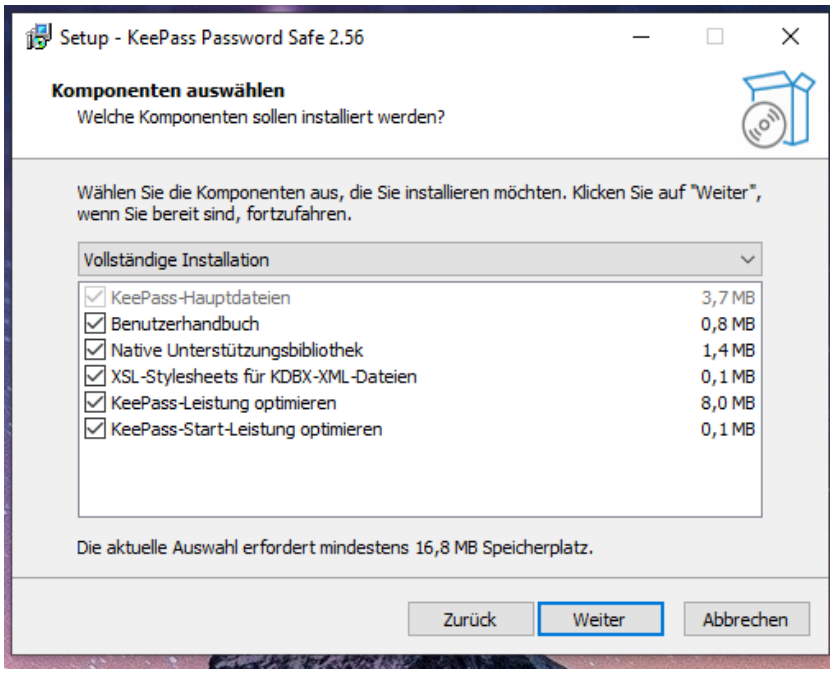
Im nächsten Schritt akzeptieren wir die Lizenzvereinbarungen und klicken auf *Weiter*.



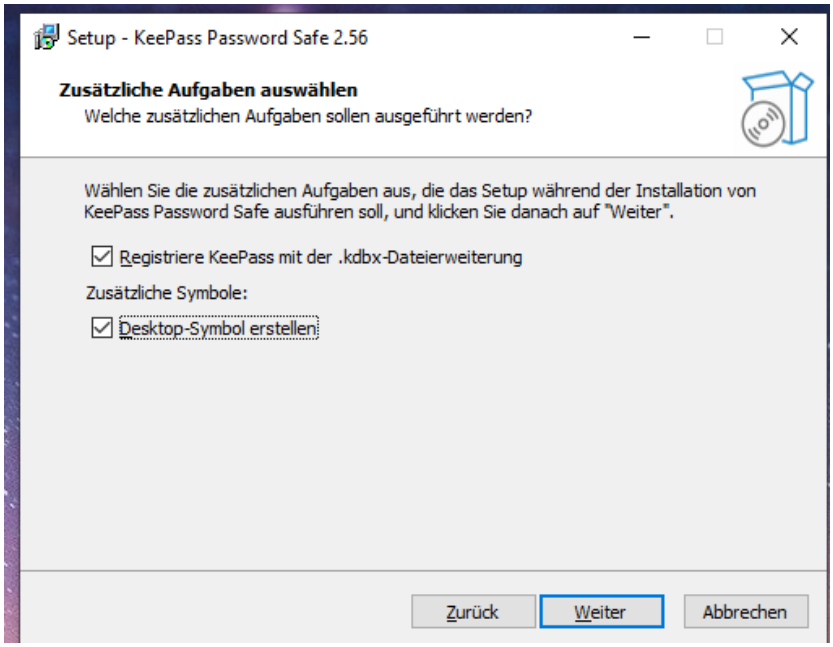
Abschließend wird der Zielordner des Programms definiert, wohin der Installer die Dateien entpacken soll. In der Regel ist der Ordner für die Programm Dateien bereits voreingestellt. Nach Überprüfung des Pfads, klicken wir auf *Weiter*.



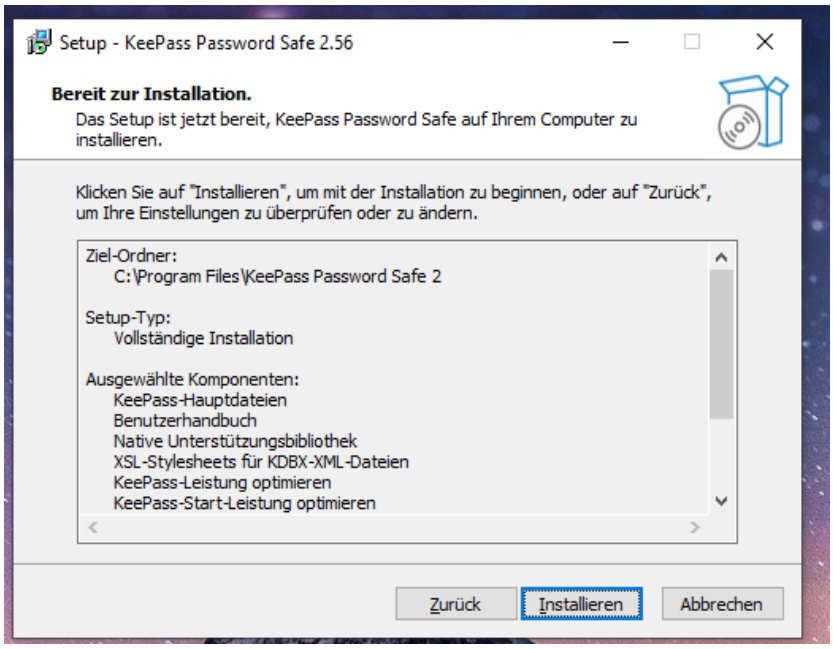
In einem weiteren Schritt wählen wir aus, welche Dateien und Features im Rahmen der Installation installiert werden und klicken auf *Weiter*.



Abschließend fragt KeePass2, welche zusätzlichen Aufgaben von KeePass2 ausgeführt werden soll und ob man eine Verknüpfung am Desktop erstellen möchte. Möchte man eine Desktop Verknüpfung erstellen, sollte die Option *Desktop-Symbol erstellen* aktivieren. Nach Auswahl der Optionen, klickt man auf *Weiter*.



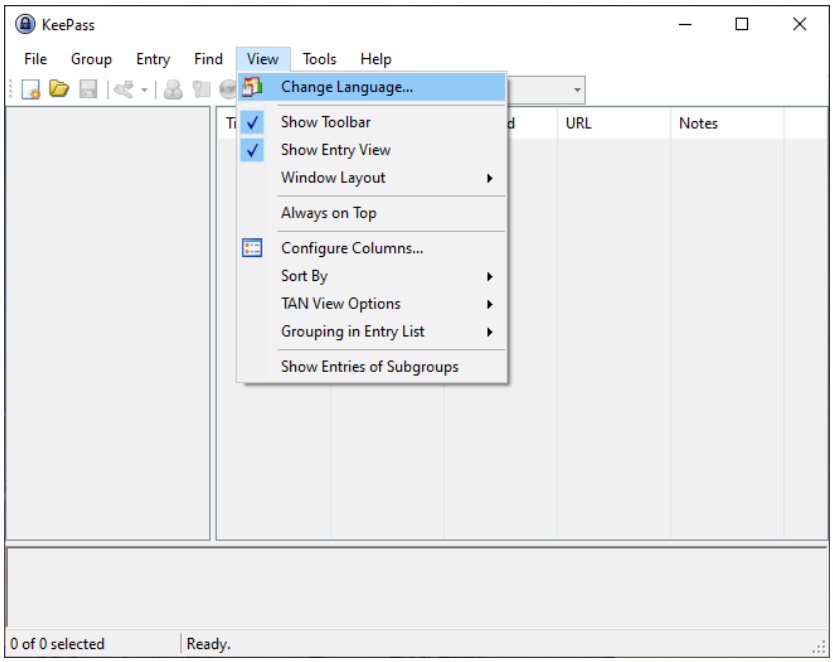
Abschließend klickt man auf *Installieren*, um die Installation von KeePass2 zu starten. Nach Abschluss der Installation kann das Fenster geschlossen und KeePass2 gestartet werden.



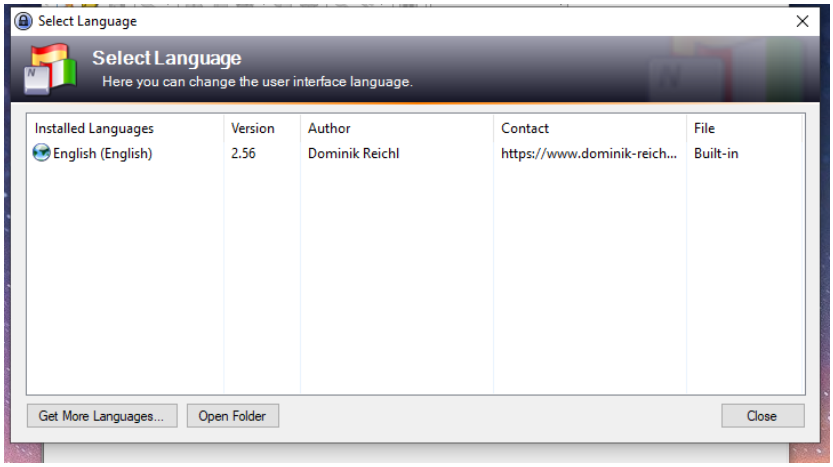
Beim erstmaligen Starten fragt KeePass2, ob man über Updates informiert werden möchte. Es wird empfohlen, dies zu bestätigen, da die Open Source Community das Programm ständig weiterentwickelt. Danach öffnet sich der KeePass2 Passwort-Manager.

11.2 Änderung der Sprache auf Deutsch

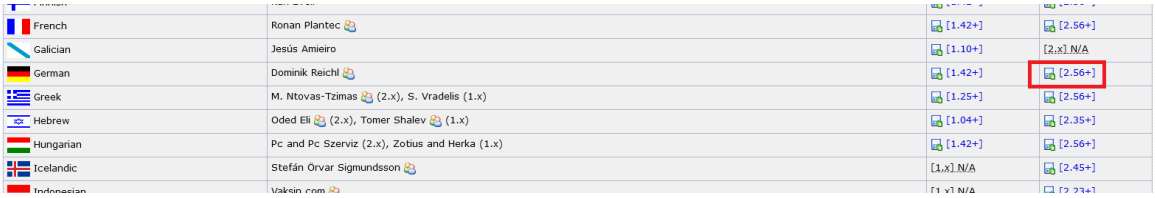
Die Standardeinstellung der Sprache des KeePass2 Passwort-Managers ist Englisch. Möchte man die Sprache auf Deutsch ändern, muss noch ein Zwischenschritt durchgeführt werden, bevor wir die Datenbank aufsetzen und die Bitcoin Seed Phrase sichern. Dafür klicken wir zuerst auf *View* oben in der Menü Leiste und wählen die Option *Change Language*.



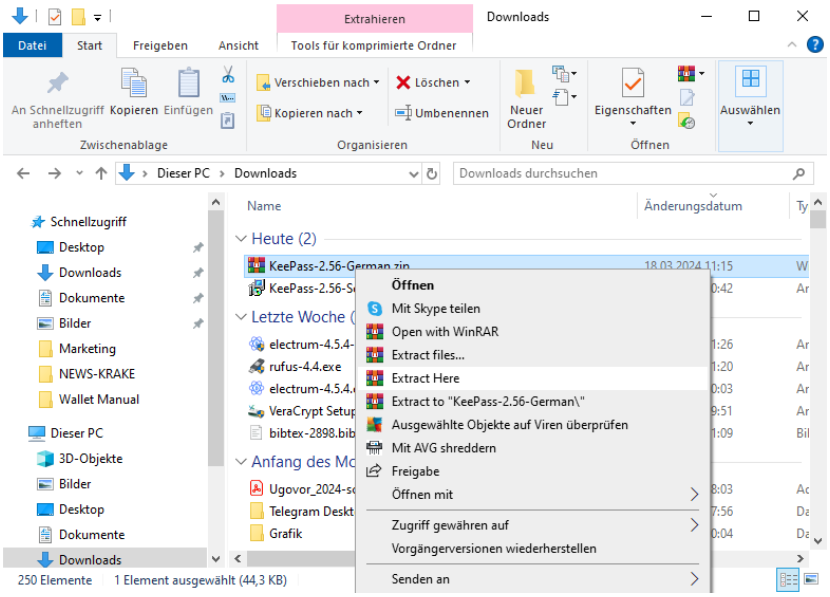
Nun öffnet sich ein Fenster mit den vorhanden Sprachen. Da die deutsche Sprache nicht mitinstalliert wurde, klicken wir unten auf den Button *Get More Languages*.



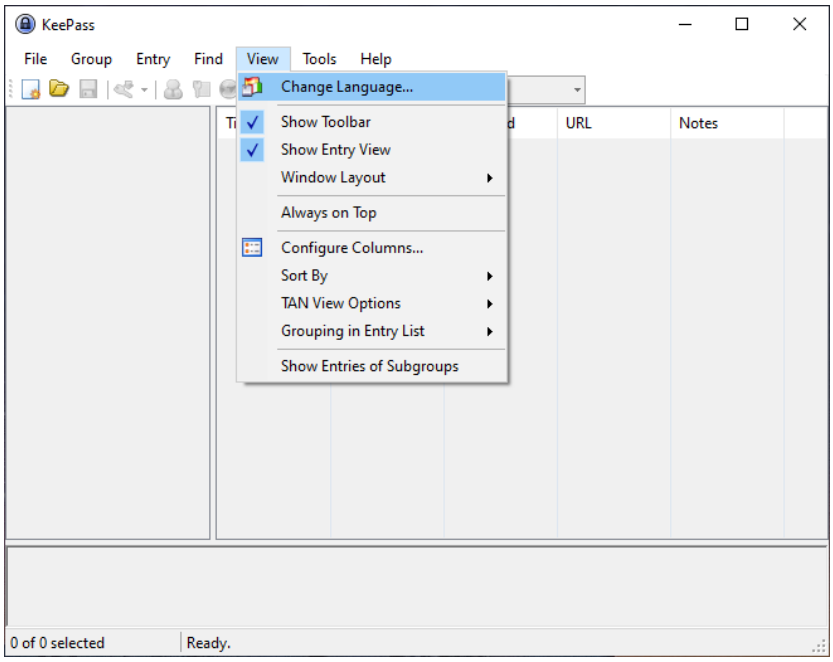
Danach öffnet sich die Website von KeePass mit einer Liste an Sprachen. Für jede Sprache gibt es ein eigenes Sprachpackage. Dabei muss beachtet werden, dass wir das Sprachpackage für die richtige Version installieren. In unserem Fall klicken wir auf den Link für das Sprachpackage [2.56+].



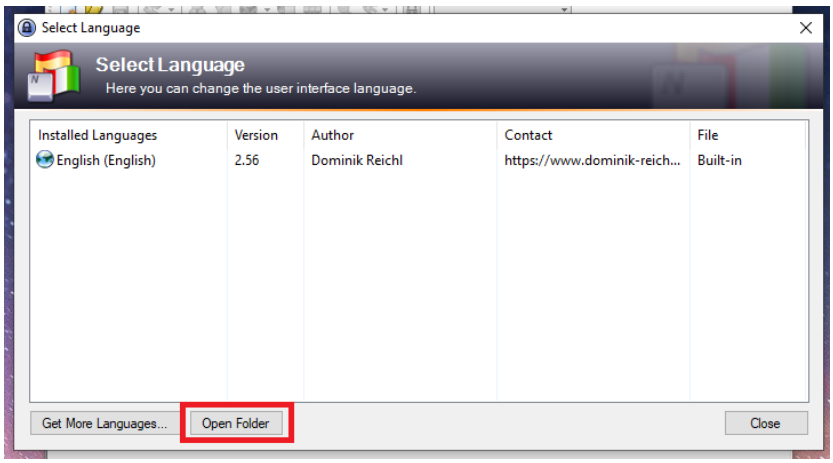
Danach sollte man erneut auf die SourceForge Website weitergeleitet werden, wo der Download nach wenigen Sekunden automatisch startet. Im nächsten Schritt bewegen wir uns in den *Downloads* Ordner und extrahieren die .zip Datei direkt im *Downloads* Ordner. Dafür klickt man mit der rechten Maustaste auf das Sprachpaket und wählt die Option *Extract Here*.



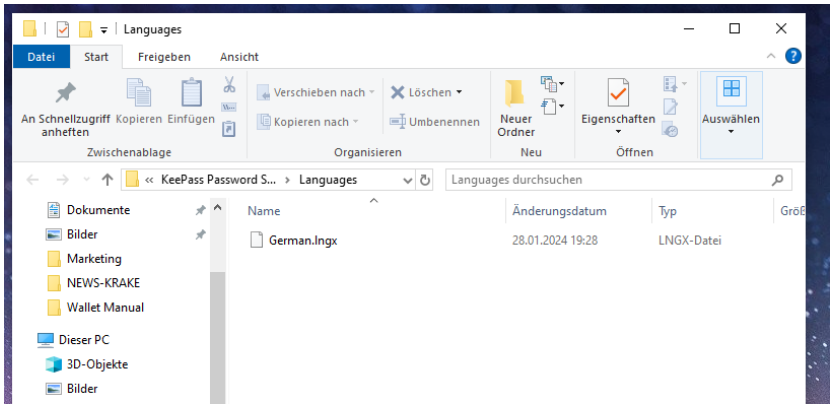
Nun sollte sich das Sprachpaket im *Downloads* Ordner befinden. Ist die Liste der Dateien nach dem Änderungsdatum geordnet, kann sich die entpackte Datei auch weiter unten befinden. Nun wechseln wir zurück zum KeePass2 Fenster, wo wir erneut auf *View* in der Menü Leiste des Passwort-Managers klicken und die Option *Change Language* auswählen.



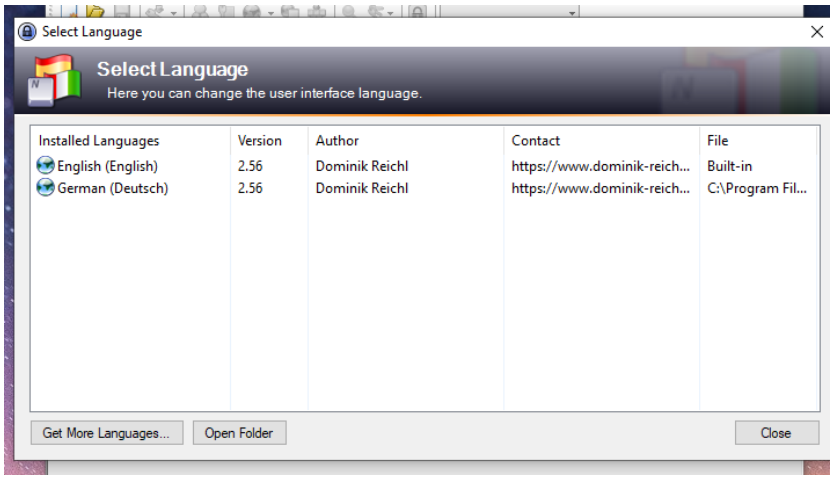
Damit öffnet sich wieder das Fenster mit den Sprachen. Dieses Mal klicken wir aber auf *Open Folder*, wodurch KeePass2 einen Ordner im Programm Ordner mit dem Namen *Languages* öffnet.



Im nächsten Schritt wird die entpackte Datei German.lngx im *Downloads* Ordner in den Ordner *Languages* kopiert oder verschoben. Windows möchte dabei eine Authorisierung durch den Administrator. Dafür klickt man auf *Fortsetzen*. Nun sollte sich das Sprachpackage im Ordner *Languages* befinden und wir können im KeePass2 Passwort-Manager die Sprache auswählen.



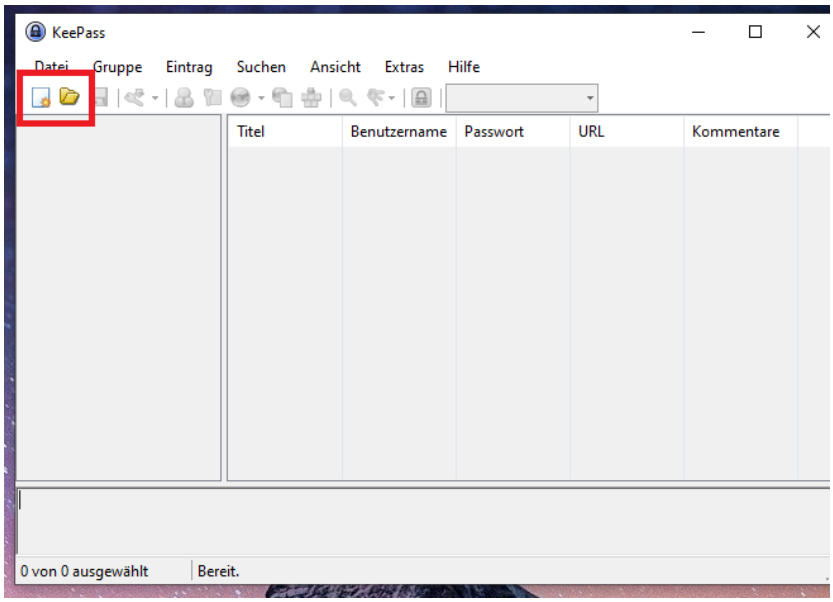
Im letzten Schritt klicken wir im Menü des KeePass2 Passwort Managers auf *View* und wählen erneut die Option *Choose languages* aus. Damit wird erneut das Fenster mit den verfügbaren Sprachen geöffnet und Deutsch sollte sich nun in der Liste befinden. Um die Sprache Deutsch zu aktivieren, klicken wir auf den Listeneintrag *Deutsch* und starten KeePass2 neu.



Nach dem Neustart sollten die Spracheinstellungen übernommen sein und wir können mit der Erstellung unserer Passwort-Datenbank beginnen.

11.3 Erstellung der Passwort-Datenbank

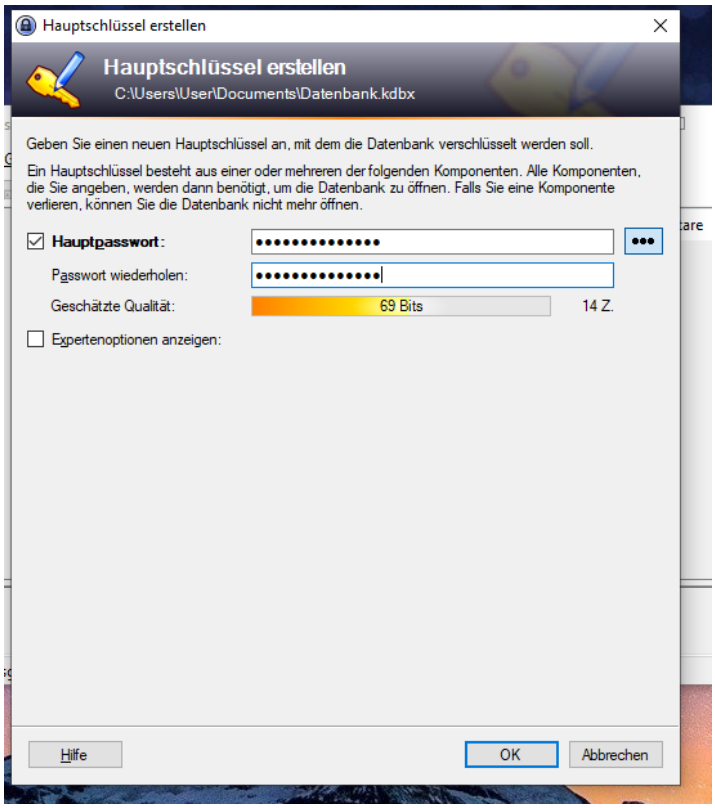
Oben in der Icon-Leiste befinden sich die wichtigsten Funktionalitäten des Passwort-Managers. Mit dem Icon ganz links außen kann eine neue Datenbank erstellt werden. Mit dem zweiten Icon kann eine bestimmte Datenbank geöffnet werden. Im ersten Schritt klicken wir auf *Neue Datenbank*.



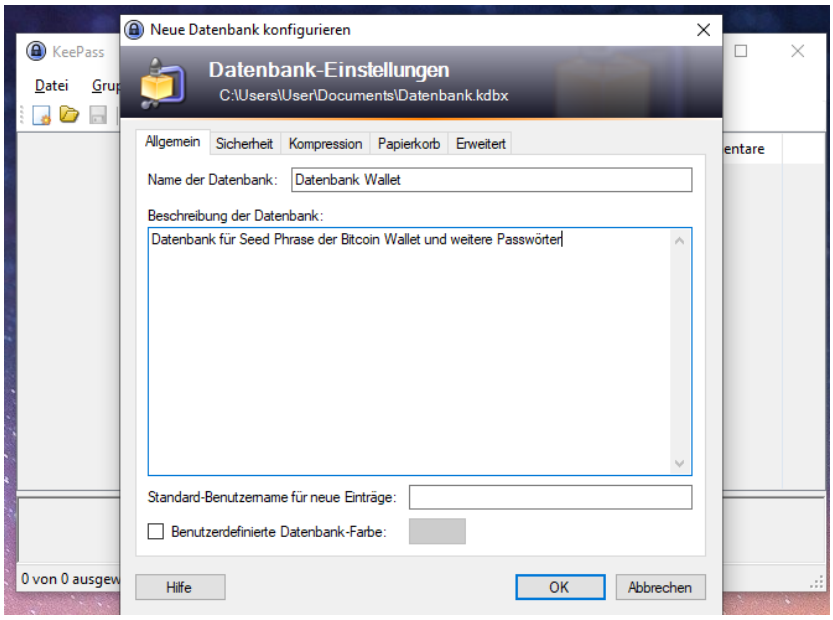
Dabei öffnet sich ein Fenster, welches uns darauf hinweist, dass wir uns den Ort, an dem wir die Datenbank speichern, merken und regelmäßig ein Backup der Datenbank erstellen sollten. Wir nehmen den Hinweis zur Kenntnis und klicken auf *OK*. Entweder schließt man sofort einen verschlüsselten externen Datenträger an und wählt diesen als Speicherort für die Datenbank oder man wählt vorrübergehend einen anderen Ordner,

wie den *Dokumente* Ordner und kopiert die Datenbank später auf einen oder mehr externe Datenträger (je nach Aufbewahrungsstrategie). Nach Auswahl eines Speicherortes klicken wir auf *Speichern*.

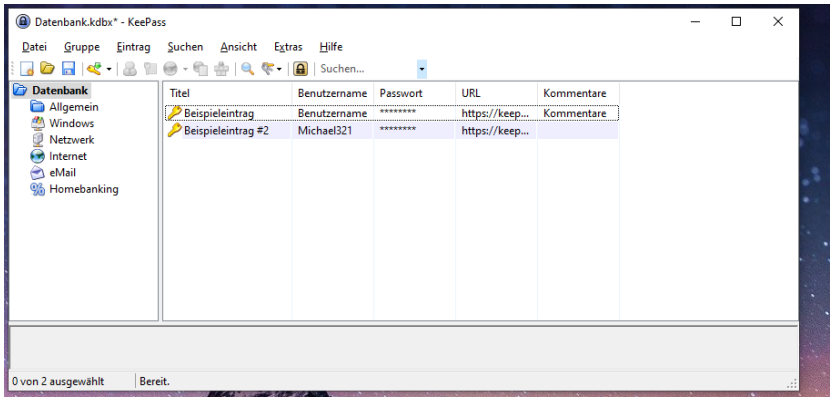
Als nächstes definieren wir ein Master-Passwort. Dieses Master-Passwort dient für die Entschlüsselung der KeePass2-Datenbank. KeePass2 gibt uns einen Hinweis über die Sicherheit des Passworts. Die Sicherheit des Passworts ist zwar wichtig, zugleich sollte aber die Merkfähigkeit des Passworts nicht unbeachtet bleiben. Hat man ein Passwort ausgewählt, klickt man auf *OK*.



Im nächsten Schritt definieren wir einen Namen für die Datenbank. Bei Bedarf kann man auch eine Beschreibung der Datenbank einfügen oder weitere Einstellungen konfigurieren. Z.B. kann man im Reiter *Papierkorb* einstellen, ob ein gelöschter Eintrag in den Papierkorb verschoben oder ganz von der Festplatte gelöscht werden soll. Zudem kann auch der Verschlüsselungsalgorithmus ausgewählt werden. Im vorliegenden Manual belassen wir es bei der Standardeinstellung und klicken nach der Eingabe der Datenbank-Bezeichnung auf *OK*.



Danach gibt KeePass2 einen Hinweis und bietet die Möglichkeit ein sogenanntes Notfallblatt zu drucken. Steht kein Drucker zur Verfügung, kann das Blatt auch vorrübergehend als PDF abgespeichert (Microsoft Print to PDF) und später ausgedruckt werden. Das Notfallblatt beinhaltet eine Reihe an Informationen, wie der Speicherort der Datenbank, ein Pfad, wo sich die Backup-Datei befindet oder Angaben zum Master-Passwort. Zu beachten ist, dass nicht das Master-Passwort auf dem ausgedruckten Blatt notiert wird, sondern lediglich Hinweise, aus welchen Komponenten das Passwort besteht. Nun sollte eine neue Datenbank angelegt sein.



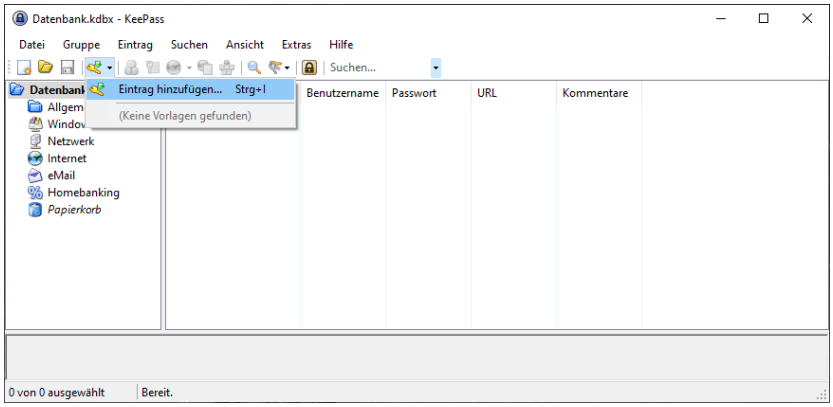
11.4 Löschen eines Eintrages

Nach der Erstellung der Datenbank beinhaltet die Datenbank zwei Beispieleinträge. Mit einem Doppelklick auf einen Eintrag, kann der Passwort Eintrag eingesehen werden. Da wir unsere eigenen Einträge erstellen und die Beispieleinträge nicht benötigen, nutzen wir die Gelegenheit, um den Löschvorgang eines Eintrages kennenzulernen.

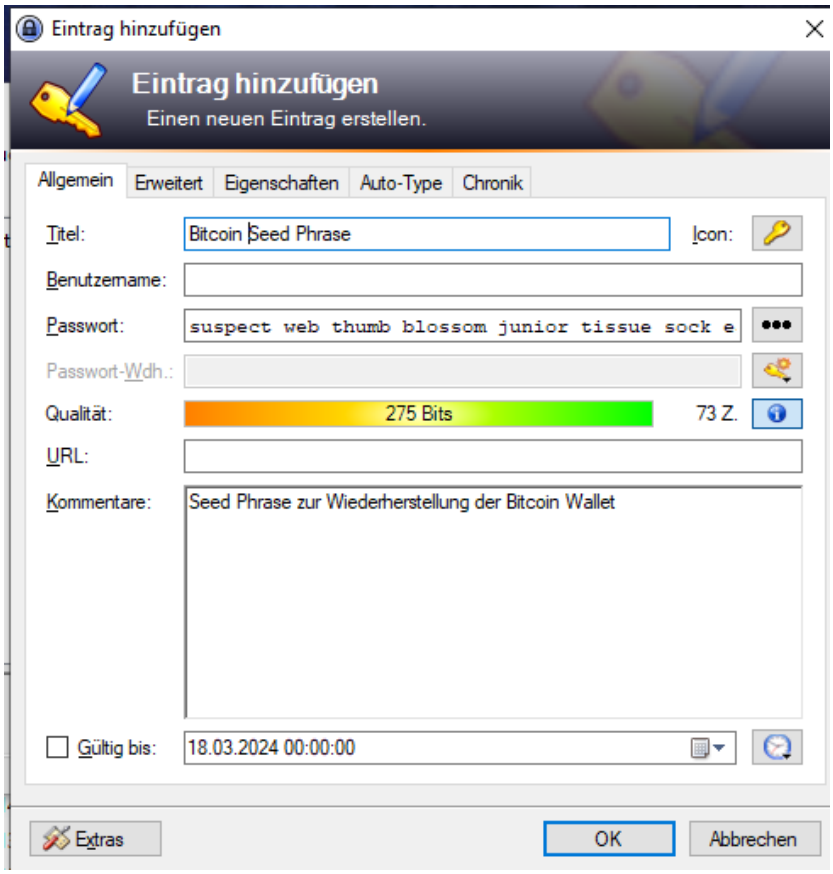
Gelöscht werden Einträge, indem man mit der rechten Maustaste auf einen Eintrag klickt und die Option *Eintrag löschen* klickt. Nachdem der Eintrag gelöscht wurde, sollte man auf das dritte Icon *Datenbank speichern* klicken, damit die Einträge übernommen werden. **ACHTUNG! Die Datenbank muss nach Änderungen immer gespeichert werden! Dies gilt auch für neu hinzugefügte oder geänderte Einträge.**

11.5 Erstellung eines neuen Eintrages

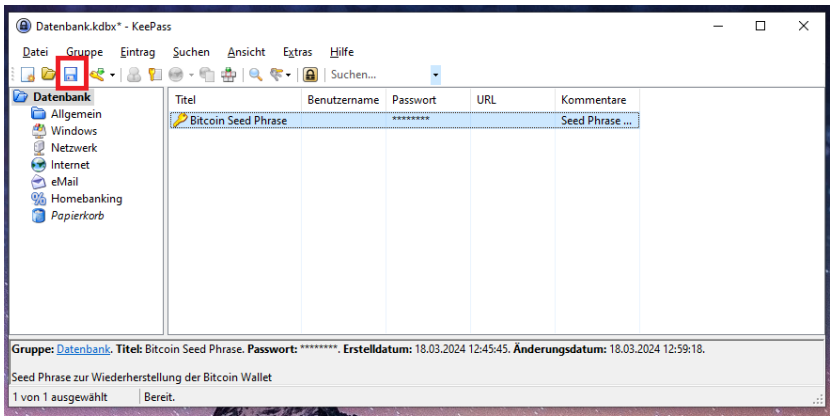
Um einen neuen Eintrag hinzuzufügen, klickt man auf das Icon *Eintrag hinzufügen*.



Damit sollte sich ein Fenster öffnen, mit dem wir einen neuen Eintrag hinzufügen können. Im *Titel* Eingabefeld geben wir eine Bezeichnung für den Passwort-Eintrag ein. In diesem Fall wurde die Bezeichnung *Bitcoin Seed Phrase* gewählt. Im Kommentarfeld unten wurde eine kurze Beschreibung des Eintrages formuliert. Verwendet man mehrere Bitcoin Wallets können bei Bedarf im Kommentarfeld weitere Informationen eingetragen werden, wie etwa die Bitcoin-Adresse und der Name der Wallet. Nun fügen wir die Bitcoin Seed Phrase in das Passwort-Eingabefeld ein, die wir uns bei der Errichtung der Wallet notiert haben und klicken auf *OK*.



Nun sollte sich in der Datenbank ein neuer Eintrag befinden. **ACHTUNG! Es ist wichtig, dass wir nach dem Hinzufügen oder bei Änderung eines Eintrages die Datenbank speichern, indem wir auf das Icon Datenbank speichern in der Icon Leiste klicken**.



Dieser Vorgang kann nun mit dem BitLocker Schlüssel, den wir im Zuge der Konfiguration des USB-Sticks in Abschnitt 7.1 erstellt haben, wiederholt werden. Wurden die Schlüssel in die Datenbank eingetragen und die Datenbank gespeichert, können wir die Datenbank auf einen oder mehrere Datenträger übertragen. Wichtig ist, dass man eine Backup-Datei der Datenbank erstellt, um bei einem technischen Gebrechen oder

bei Verlust des Datenträgers auf eine Ersatzdatenbank ausweichen zu können. Ein weiteres Backup empfiehlt sich vor allem dann, wenn die Seed Phrase nicht zusätzlich in physischer Form aufbewahrt wird. Dafür kann die Datenbank einfach kopiert werden. Möchte man für das Backup ein anderes Passwort verwenden, sollte eine neue Datenbank angelegt werden. Möchte man seine Bitcoins im Todesfall weitervererben, sollte sichergestellt werden, dass eine Vertrauensperson das Master-Passwort für die KeePass2-Datenbank kennt und somit Zugang zur Seed Phrase erhält.

12 Sicherheit des Computers

In einer vernetzten Welt spielt die Sicherheit des Computers eine zunehmend wichtige Rolle. Banken werden heute kaum noch physisch ausgeraubt, sondern sind regelmäßig Zielobjekt von Hacker-Angriffen. Auch beim Handling der Bitcoin Wallet sollte man sich um die Sicherheit des persönlichen Computers kümmern.

Die äußere Sicherheit des Computers ist ein wichtiger Layer der Sicherheitsarchitektur zum Schutz der persönlichen Bitcoin-Ersparnisse und zur Risikominimierung eines Verlustes. Dies umfasst einerseits die technische Sicherung, andererseits aber auch das persönliche Verhalten. Sogenannte Brute Force Attacken, bei denen sich Hacker über technische Sicherheitslücken Zugriff zum Computer verschaffen und die Kontrolle übernehmen, sind heute relativ selten, insbesondere dann, wenn der Computer ausreichend gewartet wird. Ein wesentlich höheres Risiko stellen heute sogenannte Social Engineering Attacken dar, mit denen Hacker über eine listige Art und Weise versuchen, den Nutzer eines PCs zu einem bestimmten Verhalten zu bewegen, welches die Sicherheit des Computers untergräbt.

Eine detaillierte Anleitung sämtlicher Bedrohungen und Lösungsstrategien für die Sicherung des persönlichen Computers würde den Rahmen dieses Manuals sprengen, allerdings sollten für Computer-Laien ein paar Grundsätze erörtert werden, die das Risiko bereits auf ein Minimum reduzieren. In den folgenden Abschnitten werden zwei Aspekte der Cyber-Sicherheit angesprochen: (1) die technische Sicherung und (2) ein sicheres Online-Verhalten. Beide Aspekte dienen primär der Prävention. Wurde der Computer bereits gehackt bzw. mit Schadcode befallen, sollte man sich professionelle Hilfe von IT-Experten holen.

12.1 Technische Sicherung

Um einen Hacker-Angriff präventiv zu verhindern, zielen technische Sicherheitsmaßnahmen in erster Linie darauf ab, die Kosten eines Angriffes zu erhöhen. Das heißt, je leichter es einem Hacker gemacht wird, desto eher wird man Opfer einer Cyber-Attacke. Um die Kosten eines Angriffes für den Hacker zu erhöhen, reicht oftmals eine Kombination einfacher Maßnahmen aus. Allerdings werden auch diese einfachen Maßnahmen von vielen Menschen ignoriert.

Eine erste wichtige Grundregel zur technischen Sicherheit ist, dass das Betriebssystem auf den neuesten Stand gebracht wird. In der Regel bieten Software-Anbieter wie Microsoft eine Zeit lang Updates auch für veraltete Betriebssysteme an. Nach einer gewissen Zeit allerdings läuft der Support für ein Betriebssystem aus und man sollte ein Upgrade des Betriebssystems durchführen.

Des Weiteren ist die Nutzung einer Anti-Virus Software von zentraler Bedeutung. Standardmäßig verwendet Windows den Windows Defender. Grundsätzlich ist der Windows Defender die erste Wahl, da Microsoft selbst vermutlich am besten weiß, wie es einen Windows-Rechner schützen kann. Allerdings können auch andere Anti-Virus Programme verwendet werden, wie McAfee oder AVG, die zusätzliche Funktionalitäten bieten. Es sollte regelmäßig überprüft werden, ob die Anti-Virus Software auch tatsächlich aktiviert ist und nicht unabsichtlich deaktiviert wurde.

Eine weitere wichtige Grundregel ist, dass am Computer eine Firewall aktiviert ist. Eine Firewall ist ein weiterer Security Layer, der den Datenverkehr zwischen Computer und Internet überwacht und filtert. In der Regel ist die Firewall standardmäßig aktiviert, dennoch lohnt sich eine Überprüfung, ob die Firewall auch tatsächlich aktiv ist und nicht unabsichtlich deaktiviert wurde.

Darüber hinaus ist die Verwendung von starken Passwörtern ein wesentlicher Aspekt der Cyber-Sicherheit. Die Passwörter sollten nicht zu kurz, zu einfach oder zu vorhersehbar sein. Es empfiehlt sich, dass für unterschiedliche Accounts verschiedene Passwörter verwendet werden, die in regelmäßigen Abständen geändert

werden. Um die Passwörter nicht zu vergessen oder durcheinander zu bringen, bieten sich Passwort-Manager an. Eine weitere wichtige Grundregel bei der Wahl eines Passwortes ist, dass das Passwort nicht auf persönliche Merkmale zurückzuführen ist, wie das Geburtsdatum oder der Name. Zudem sollten keine gängigen Phrasen oder Sprichwörter verwendet werden, die mithilfe von sogenannten Dictionary Attacken geknackt werden können. Wenn möglich sollte eine 2-Factor-Authentication genutzt werden.

Eine weitere Maßnahme, die einen zusätzlichen Security-Layer bietet, ist die Nutzung eines VPN (Virtual Private Network). Bei der Nutzung eines VPN wird der Datenverkehr verschlüsselt, wodurch sogenannte Man-in-the-Middle Attacken verhindert werden. Darüber hinaus kann mit einem VPN die IP-Adresse des Computers maskiert werden, sodass die eigene IP-Adresse für Hacker nicht einsehbar ist. Insbesondere wenn man sich in öffentliche WiFi-Netzwerke einloggt, wie etwa am Flughafen oder in Cafes sind VPN-Zugänge besonders nützlich. Als VPN kann bspw. der VPN Service *Cyberghost* oder andere Services verwendet werden, die über eine App einen einfachen, sicheren und günstigen VPN-Zugang zur Verfügung stellen.

12.2 Sicheres Verhalten

Zusätzlich zu den technischen Sicherheitsmaßnahmen spielt heute vor allem das persönliche Verhalten im Internet eine zentrale Rolle. Bei sogenannten Social Engineering Attacken werden Nutzer dazu gebracht, ein bestimmtes Verhalten zu setzen, welches Schadcode auf dem Computer installiert oder Sicherheitslücken für Hacker öffnet. Um diese Attacken zu verhindern oder abzuwehren, sollte man gewisse Regeln beim Online-Verhalten einhalten.

Zunächst sollte sichergestellt werden, dass keine verdächtigen Dateien vom Internet runtergeladen und geöffnet werden, insbesondere wenn es sich um sogenannte Executables (.exe-Dateien) handelt. Executables sind grundsätzlich nicht vermeidbar, da man mit .exe-Files auf Windows Rechnern Programme installiert bzw. ausführt. Daher sollte man sicherstellen, dass die runtergeladenen exe-Files vertrauenswürdig sind. Bei der Neuinstallation einer Software empfiehlt es sich daher das Programm immer von der offiziellen Website des Anbieters runterzuladen und nicht von Drittanbietern.

Dies gilt auch für Email-Anhänge. Hacker nutzen oftmals Emails als Angriffsvektor und hängen Schadcode als Attachment an. Schadcode in Email Anhängen muss nicht notwendigerweise in Form von .exe Dateien verbreitet werden, sondern können auch in anderen Dateiformaten, wie PDFs, Multimedia-Dateien, etc. versteckt sein. Aus diesem Grund sollte man sich vor Download und Öffnung eines Email Attachments vergewissern, dass es sich um einen vertrauenswürdigen Absender handelt. Zu beachten dabei ist, dass Hacker oftmals Emails und Anhänge so gestalten, dass diese vertrauenswürdig wirken. Dasselbe gilt auch für Links. Oftmals fügen Hacker Links in Emails ein, die bei einem Klick einen automatischen Download starten. Aus diesem Grund sollten keine Links von verdächtigen Emails oder Nachrichten von verdächtigen oder unbekannten Email Adressen geöffnet werden.

Eine weitere Angriffsstrategie von Hackern ist, dass man dazu aufgefordert wird, Zugangsinformationen wie Passwörter oder Benutzernamen preiszugeben. Diese Attacken werden auch als Phishing-Attacken bezeichnet und können via Email oder per Telefon durchgeführt werden. Meist gestalten die Hacker das Email so, dass es den Eindruck eines offiziellen Emails vermittelt. Häufig befinden sich in den Emails auch Links, die zu nachgebauten Websites führen und wie eine offizielle Website wirken. Die wichtigste Grundregel lautet: Offizielle Website Betreiber senden keine Emails, die dazu auffordern, ein Passwort oder einen Benutzernamen zu ändern oder preiszugeben. Wenn im Posteingang eine derartige Email auftaucht, kann man diese Email getrost löschen. Generell sollten keine Zugangsdaten preisgegeben werden unabhängig vom Kontext.

In letzter Zeit kam es häufig vor, dass Hacker einen Nutzer dazu bringen ein Software-Update durchzuführen und dabei im Hintergrund Schadcode installieren. Hierfür werden unterschiedliche Strategien eingesetzt. Eine mögliche Strategie ist, dass eine bestimmte App bzw. ein Programm gratis zur Verfügung gestellt wird. Zum

Zeitpunkt des Downloads befindet sich kein Schadcode im Programm, sodass das Anti-Virus-Programm nicht anschlägt. Im Laufe der Zeit werden die Nutzer dieser Software in der App dazu aufgefordert ein Software-Update durchzuführen. Im Rahmen dieses Software-Updates ist es nun einfacher, einen Schadcode zu installieren. Ein bekannt gewordenes Beispiel einer solchen Attacke war ein QR-Code Scanner für das Android Mobilephone, welcher sich über ein Update Zugänge zu Krypto-Wallets verschaffte. Auch für den Google Chrome Browser oder andere Browser wurden Websites in einer Art gestaltet, dass sie wie eine offizielle Website wirkten und den Nutzer dazu aufforderten, ein Software Update für den Browser durchzuführen. Aus diesem Grund sollten Built-In Software Updates nur dann durchgeführt werden, wenn man der Quelle der App vertraut und es sich um eine offizielle Software oder Webadresse handelt. Wenn möglich, sollten Updates lediglich über die offiziellen App Stores durchgeführt werden.

Ein sicheres Verhalten in Punkto Computer-Security sollte auch im eigenen Umfeld berücksichtigt werden. Menschen mit bösartigen Intentionen könnten mithilfe von Manipulationstechniken versuchen, an persönliche Informationen zu gelangen und sich Zugang zum Computer zu verschaffen. Daher ist auch beim alltäglichen sozialen Verhalten Vorsicht geboten. Heikle Informationen sollten niemals weitergegeben werden, auch wenn Personen vertrauenswürdig wirken oder freundlich erscheinen. Zudem sollte man keine Passwörter auf Klebezettel notieren und an den Bildschirm kleben oder unter der Tastatur verstecken.

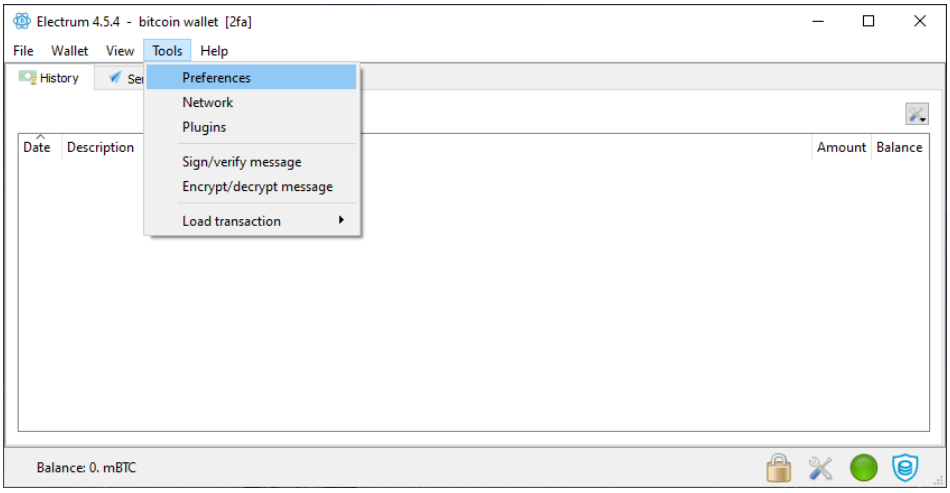
Bitcoiners kennzeichnen sich durch einen zentralen Grundsatz: *Don't trust, but verify*. Übertragen auf das Online-Verhalten bedeutet dies, dass man beim Internet-Surfen oder bei der Online-Kommunikation generell vorsichtig ist und die Authentizität und Vertrauenswürdigkeit einer Online-Quelle überprüft. Nicht jedes Email oder jede Nachricht auf sozialen Netzwerken muss geöffnet werden. Nicht jeder Link oder jedes blinkende Icon müssen angeklickt werden. Bestimmte Arten von Websites sollten generell vermieden werden. Prinzipiell sollte man sich immer vergewissern, ob es sich um offizielle Websites oder Email Adressen handelt. Darüber hinaus sollten keine verdächtigen Dateien geöffnet werden.

13 Nutzung der Wallet

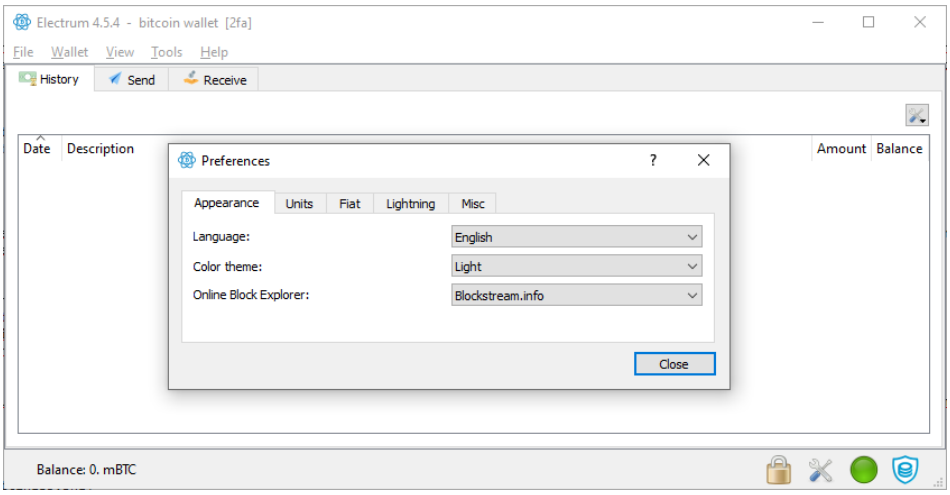
Nach der Installation der Wallet und der Sicherung der Wiederherstelllungsschlüssel, wird im abschließenden Kapitel ein Überblick über die Nutzung der Bitcoin Wallet dargelegt. Dies umfasst das Empfangen und Senden von Bitcoins sowie den Kauf und Verkauf. Darüber hinaus werden wir zu Beginn die Einstellungen der Wallet etwas näher kennenlernen.

13.1 Einrichtung der Wallet

Bevor wir Bitcoins mit unserer Wallet empfangen und senden, bietet es zunächst sich an, die Einstellungen der Wallet zu konfigurieren. Dafür öffnen wir zuerst unsere Wallet, indem wir auf die Electrum Verknüpfung am Desktop klicken, die Wallet auswählen und das Passwort eingeben. Nachdem die Wallet geöffnet wurde, klicken wir auf *Tools* in der Menü Leiste der Wallet und wählen die Option *Preferences*.



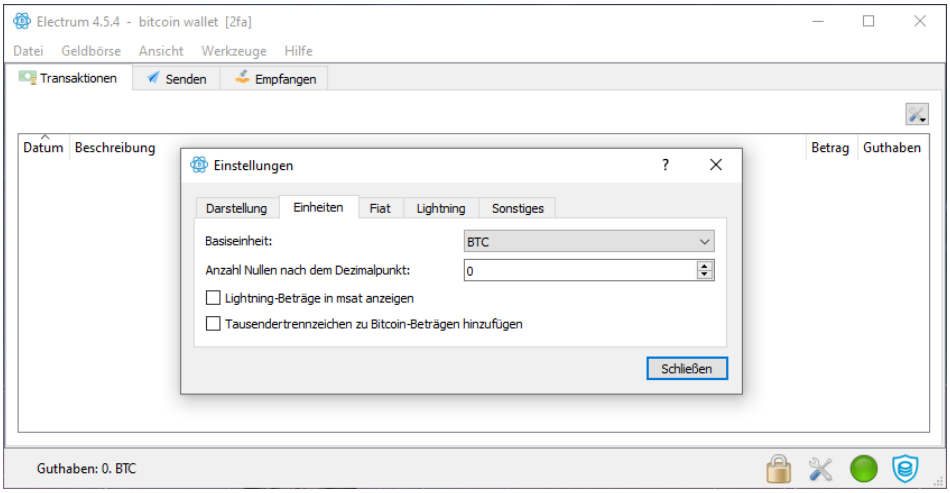
Im *Preferences* Fenster befinden sich mehrere Reiter. Im *Appearance* Reiter können wir die Sprache sowie das Farbschema der Wallet auswählen. Bei der Option *Online Block Explorer* wählt man eine Website aus, die dann geöffnet wird, wenn bestimmte Funktionen der Wallet auf Web-Informationen zugreifen. In diesem Fall wählen wir *German* als die bevorzugte Sprache aus und starten die Wallet neu.



Nach dem Neustart der Wallet sollten die Spracheinstellungen übernommen sein. Nun klicken wir auf *Werkzeuge* im Menü oben und wählen die Option *Einstellungen*. Im Reiter *Einheiten* können wir einstellen, welche Maßeinheit für die Darstellung der Beträge verwendet werden soll. Bitcoin hat vier Maßeinheiten, die zur Auswahl stehen:

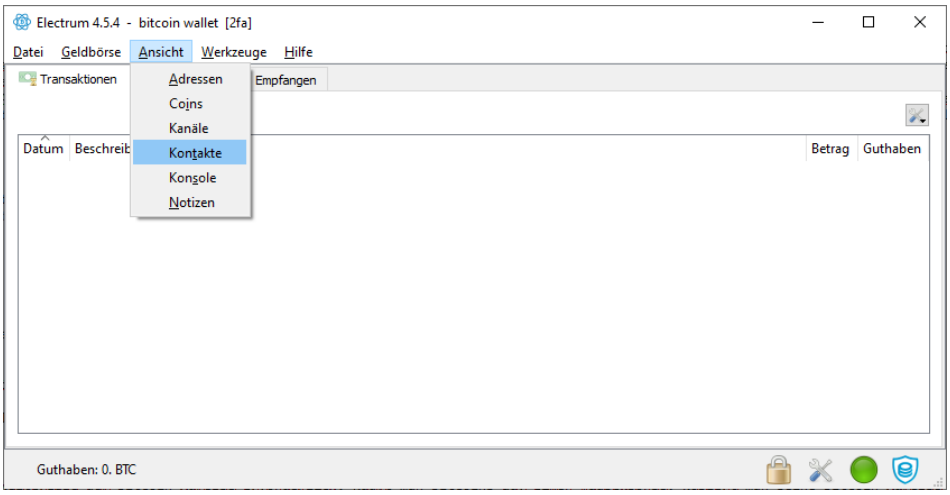
- **BTC:** BTC steht für Bitcoin und repräsentiert die Basiseinheit des Netzwerks. Insgesamt gibt es 21 Mio. Bitcoins.
- **Sats:** Sats steht für *Satoshis* und ist die kleinste Maßeinheit. Ein Bitcoin besteht aus 100 Mio. Satoshis. 1 BTC = 0.00000001 BTC
- **mBTC:** mBTC steht für MilliBitcoin und repräsentiert $\frac{1}{1.000}$ eines Bitcoins. 1 BTC = 0.001 mBTC
- **Bits:** Bits ist eine weitere Einheit und repräsentiert 100 Satoshis. 1 BTC = 0.000001 Bits

Unter dem Reiter *Fiat* kann die Währung eingestellt werden, in die die BTCs umgerechnet werden sollen. Die Einstellungen in den Reitern *Lightning* und *Sonstiges* werden belassen.



Unter dem Menü Punkt *Ansicht* können weitere Reiter zur Wallet hinzugefügt werden. Ein nützlicher Reiter ist die Ansicht *Kontakte*, in der zusätzliche Bitcoin Adressen von Kontaktpersonen hinzugefügt werden

können. Unter dem Reiter *Notizen* können Notizen in der Wallet gespeichert werden. Im Reiter *Adressen* befinden sich verschiedene Kontoadressen, die die Wallet generiert. Zwar kann man für das Empfangen von Bitcoins immer die gleiche Adresse verwenden, unter Bitcoinern ist es allerdings üblich, dass man für jede Transaktion aus Gründen der Anonymität eine neue Adresse verwendet. Bitcoins können an Adressen vom Typ *eingehend* gesendet werden. Die Adressen vom Typ *Wechselgeld* werden nicht weitergegeben, sondern lediglich intern von der Software verwendet, wenn man bspw. einen zu hohen Betrag versendet hat und man ein Wechselgeld zurückerhält. Ist man ein Bitcoin-Einsteiger und fühlt sich unsicher mit den vielen Adressen, können wir die Adressen ausgeblendet lassen. Zudem sollten Einsteiger die anderen Ansichten fürs erste ausblenden.



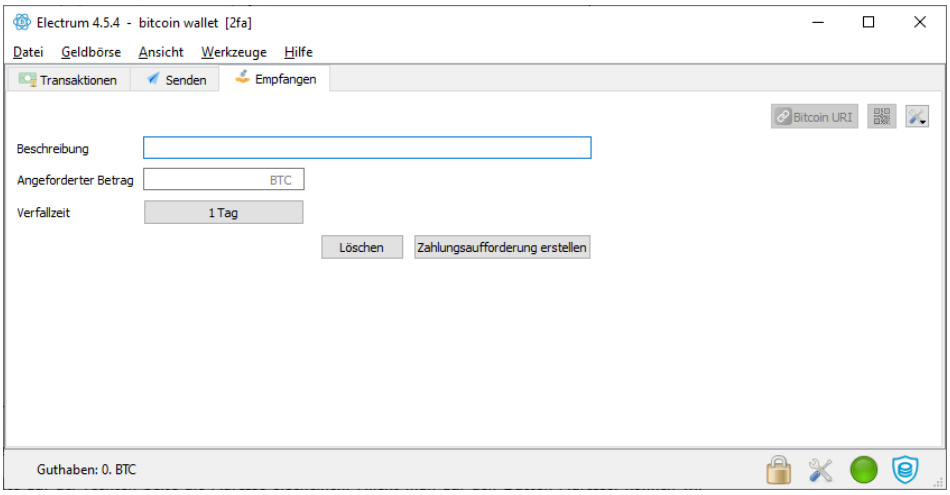
13.2 Bitcoins empfangen

Es gibt mehrere Möglichkeiten, um an Bitcoins zu gelangen:

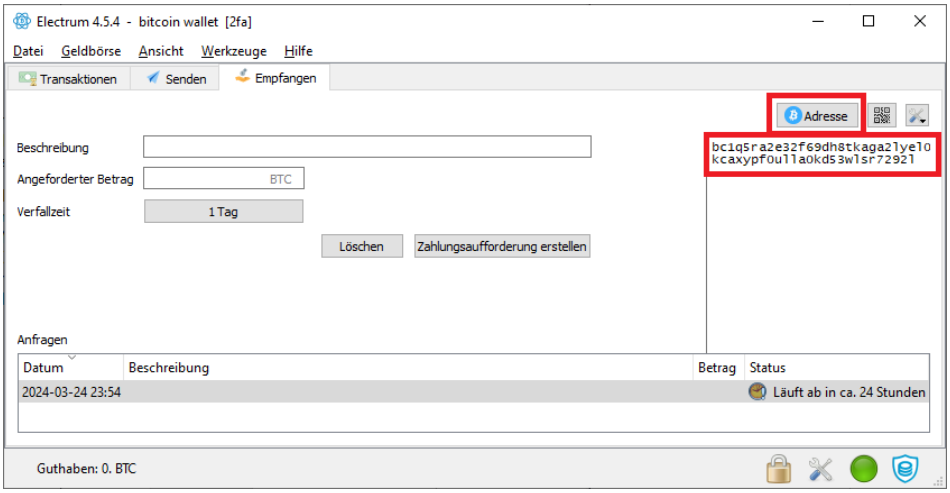
- Kauf von Bitcoins an einer Tauschbörse
- Kauf von Bitcoins bei Bitcoin ATMs (Tauschautomaten)
- Bezahlung durch Bitcoins bei Bereitstellung der eigenen Arbeitsleistung oder bei Verkauf von Waren
- Teilnahme am Netzwerk als Miner

Um Bitcoins zu empfangen, ist lediglich die Weitergabe der Bitcoin-Adresse erforderlich. Kauft man Bitcoins auf einer Tauschbörse, kopiert man die eigene Bitcoin Adresse und fügt sie beim Kauf auf der Tauschbörse ein. Möchte man sich als Selbstständiger in Bitcoin bezahlen lassen, gibt man seine Bitcoin-Adresse an den Auftraggeber weiter.

Dafür klicken wir zuerst auf den Reiter *Empfangen*. Danach klicken wir auf den Button *Zahlungsaufforderung erstellen*. Dies bietet die Möglichkeit eine Art Rechnung zu erstellen, wenn man sich bspw. als Selbstständiger von einem Auftraggeber in Bitcoins bezahlen lässt. Allerdings ist keine Erstellung einer Rechnung erforderlich um Bitcoins zu empfangen. Auch die Verfallszeit kann ignoriert werden. Die Adresse ist auch nach Ende der Verfallszeit weiterhin gültig. Wichtig ist nur, dass wir auf der rechten Seite die Adresse kopieren. Allerdings muss man hier die richtige Adresse wählen.



Standardmäßig ist die Bitcoin URI eingestellt. Klickt man auf den Button *Bitcoin URI*, können wir zwischen zwei Adresstypen wählen: *Bitcoin* und *Bitcoin URI*. *Bitcoin URI* beginnt mit *bitcoin:* und beinhaltet die Verfallzeit. *Bitcoin URI* ist eine Adresse für bestimmte Applikationen wie z.B. im E-Commerce Bereich. Die *Adresse* mit dem blauen Icon ist die herkömmliche Bitcoin Adresse, die wir im Normalfall verwenden. Darüber hinaus kann die Adresse in Form eines QR-Codes, der die herkömmliche Bitcoin Adresse beinhaltet, verwendet werden. In diesem Fall klicken wir auf *Bitcoin URI* und wechseln zur herkömmlichen Bitcoin Adresse mit dem blauen Icon (siehe Abbildung unten).

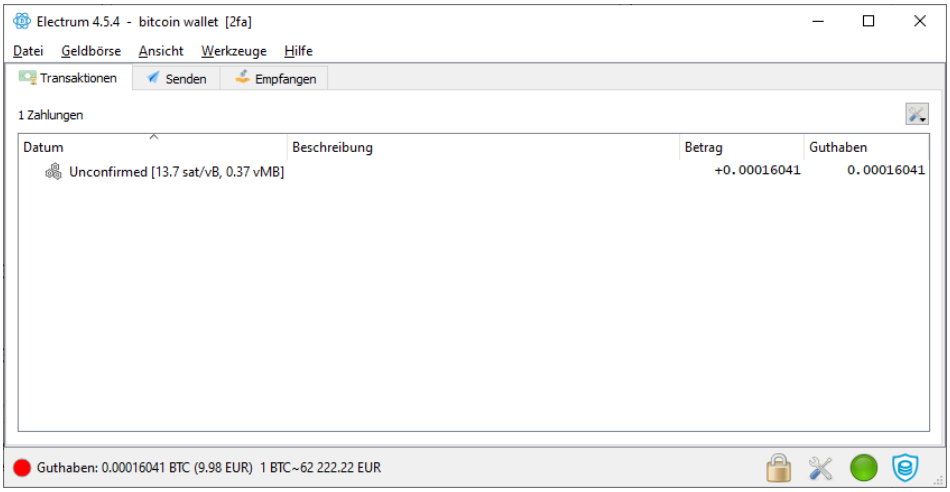


Kopiert wird die Bitcoin Adresse, indem man in das Feld mit der Adresse klickt. Danach gehen wir zur Tauschbörse, auf der wir die Bitcoins kaufen und fügen die Adresse ein. **ACHTUNG! Man sollte die Adresse nach Einfügen immer überprüfen und abgleichen. Werden die Bitcoins an eine falsche Adresse gesendet, kann die Transaktion nicht mehr rückgängig gemacht werden.**

Wurde der Kaufabschluss abgeschlossen oder von einer Gegenpartei die Bitcoins an die eigene Wallet gesendet, so sehen wir nach wenigen Minuten im Reiter *Transaktionen* die eingegangene Überweisung. Mit einem Doppelklick auf die eingegangene Transaktion können wir die Details der Transaktion einsehen.

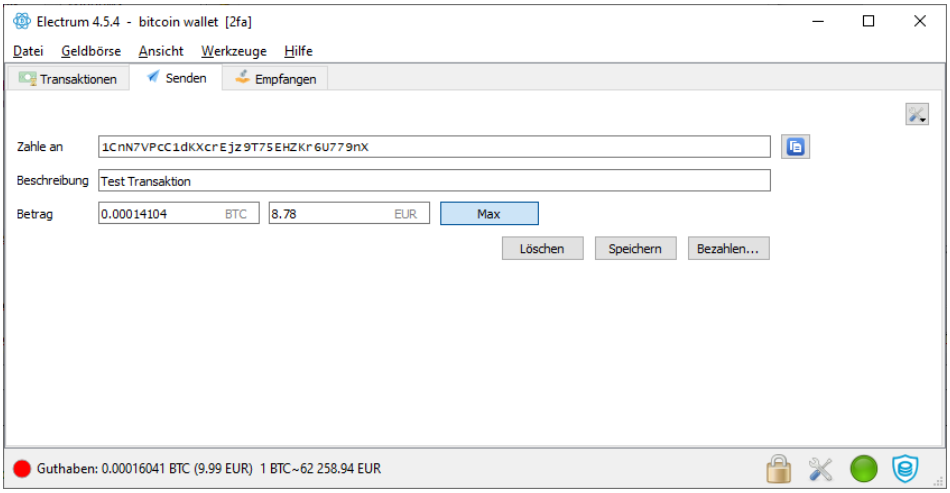
Die Transaktion scheint kurz nach Versand der Bitcoins im Reiter *Transaktionen* auf, allerdings kann es ein paar Minuten dauern bis das Bitcoin-Netzwerk die Transaktion validiert hat und sich auch das Guthaben

unten im Fenster aktualisiert.

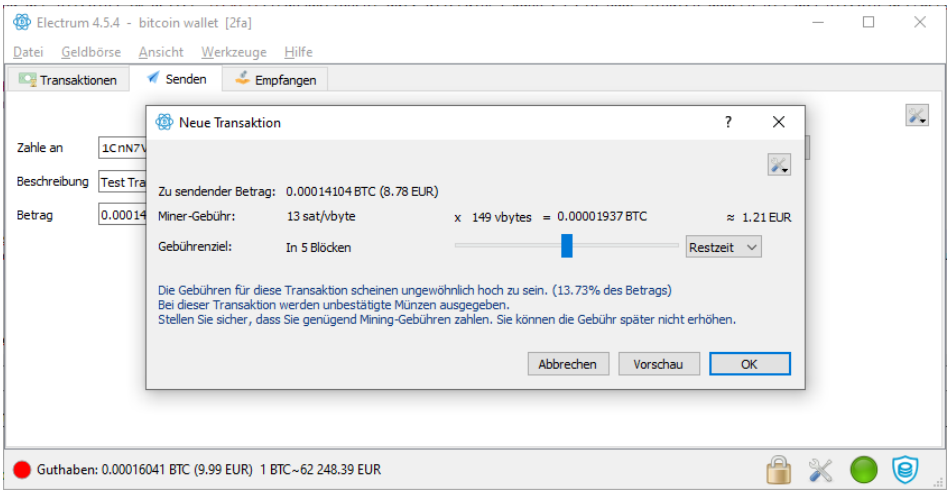


13.3 Bitcoins senden

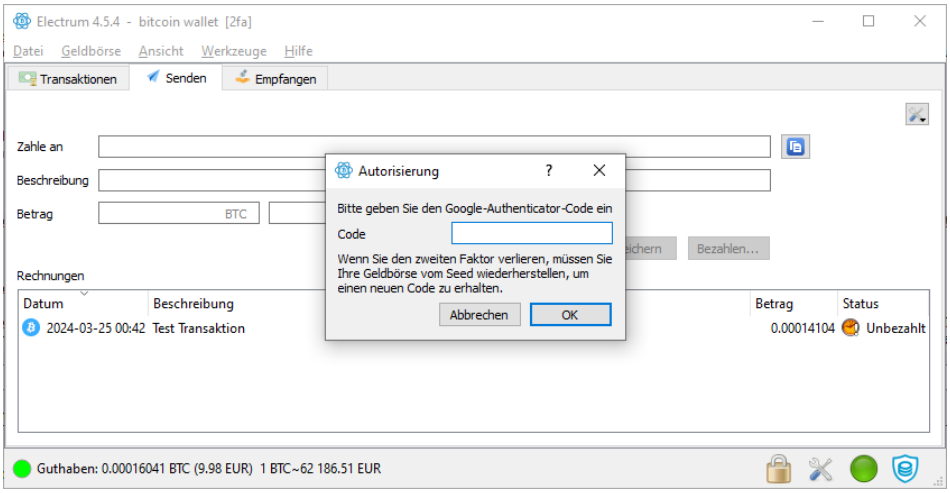
Im folgenden Abschnitt werden wir unsere erste Transaktion mit unserer neuen Wallet senden. Dafür wechseln wir zunächst zum Reiter *Senden* und fügen die Transaktionsdaten ein. Beim Feld *Zahle an* fügen wir die Bitcoin Adresse des Empfängers ein. Bei der Beschreibung können wir eine Zahlungsreferenz hinzufügen, um die Transaktion zuordnen zu können. Danach geben wir den Betrag ein und klicken auf *Bezahlen*.



Im nächsten Schritt definieren wir das sogenannte Gebührenziel. Je höher das Gebührenziel, desto höher sind die Transaktionskosten und desto schneller wird die Transaktion durchgeführt. Die Gebühren können sich je nach Auslastung des Netzwerks dynamisch verändern. Danach klicken wir auf *OK*. **ACHTUNG! Es sollten mit einer Adresse nicht zu häufig kleine Beträge gesendet werden, da man relativ schnell hohe Transaktionskosten bezahlt. Dies hängt mit den sogenannten UTXOs zusammen. Möchte man häufig kleinere Beträge senden, sollte man sich eine Lightning Wallet einrichten.**



Bevor die Transaktion gesendet wird, fragt die Wallet nach dem Wallet Passwort und dem Code der Google Authenticator App. Nach Eingabe des Passwortes öffnen wir die Google Authenticator App, geben den Code der Google Authenticator App ein und klicken auf *OK*.



Ist der Code korrekt, sollte die Transaktion nun gesendet und im Reiter *Transaktionen* gelistet werden.

13.4 Bitcoins kaufen

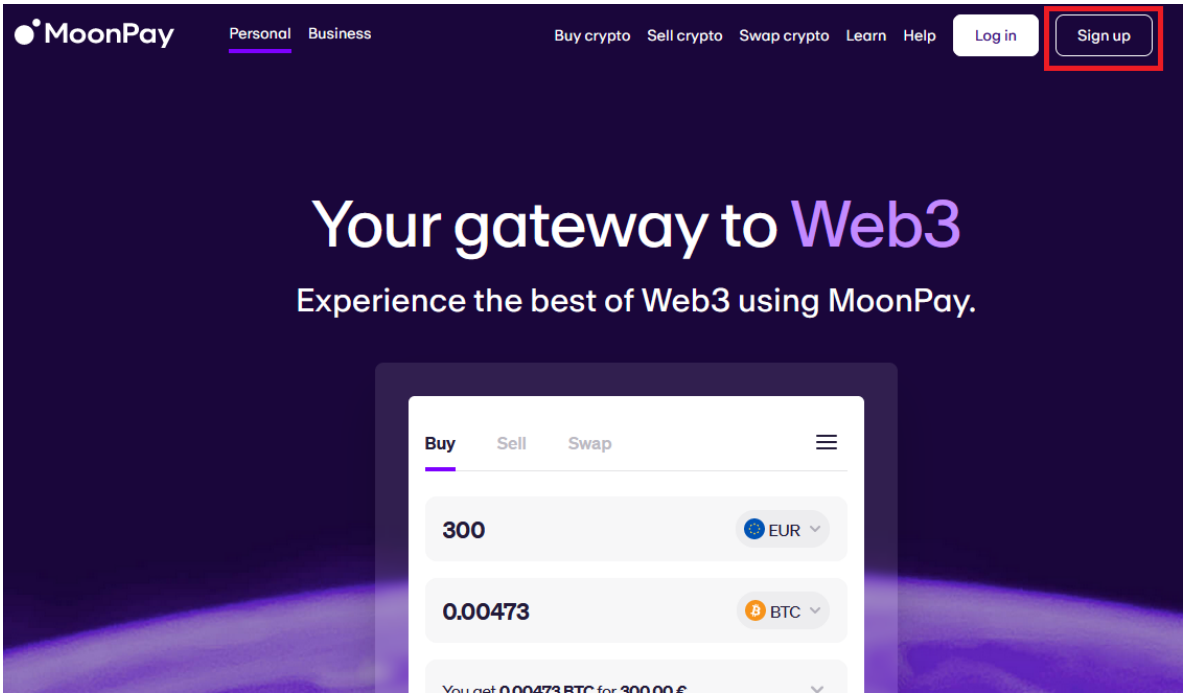
Möchte man Bitcoins kaufen, wird man sich in der Regel auf einer Tauschbörse anmelden und dort die Bitcoins erwerben. Es gibt weltweit sehr viele verschiedene Tauschbörsen. Eine Liste mit Tauschbörsen geordnet nach einem Vertrauensindex findet sich auf https://www.coingecko.com/en/exchanges. Zu den bekanntesten und populärsten Tauschbörsen zählen Coinbase, Binance oder Kraken.

Im Normalfall muss man sich für den Kauf auf einer Tauschbörse mit einer Email Adresse registrieren. In den meisten Fällen ist man verpflichtet, die eigene Identität zu bestätigen, indem man einen Reisepass oder Personalausweis hochlädt. Nachdem die Identität bestätigt wurde, kann man mit einer Debit- oder

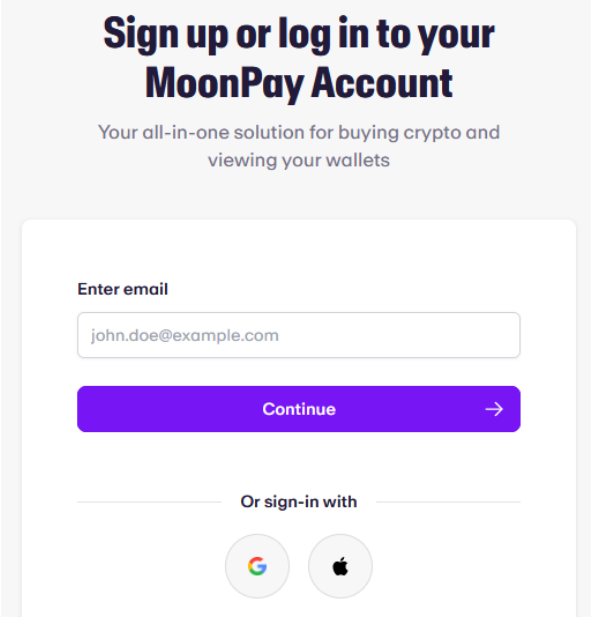
Kreditkarte die Bitcoins kaufen.

Im vorliegenden Manual wird der Kauf von Bitcoins bei `https://www.moonpay.com/` gezeigt. MoonPay bietet die Möglichkeit direkt beim Kauf die Adresse der eigenen Wallet einzugeben.

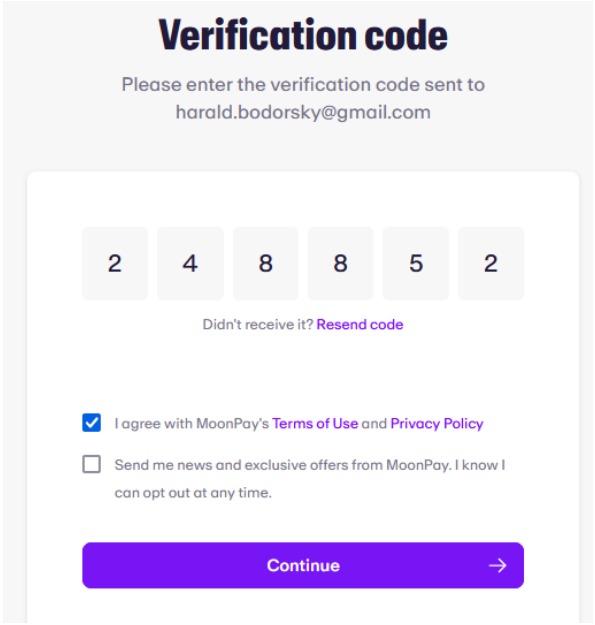
Kauft man das erste Mal auf MoonPay, müssen wir uns zunächst registrieren. Dafür gehen wir auf die MoonPay Website und klicken rechts oben auf *Sign up*.



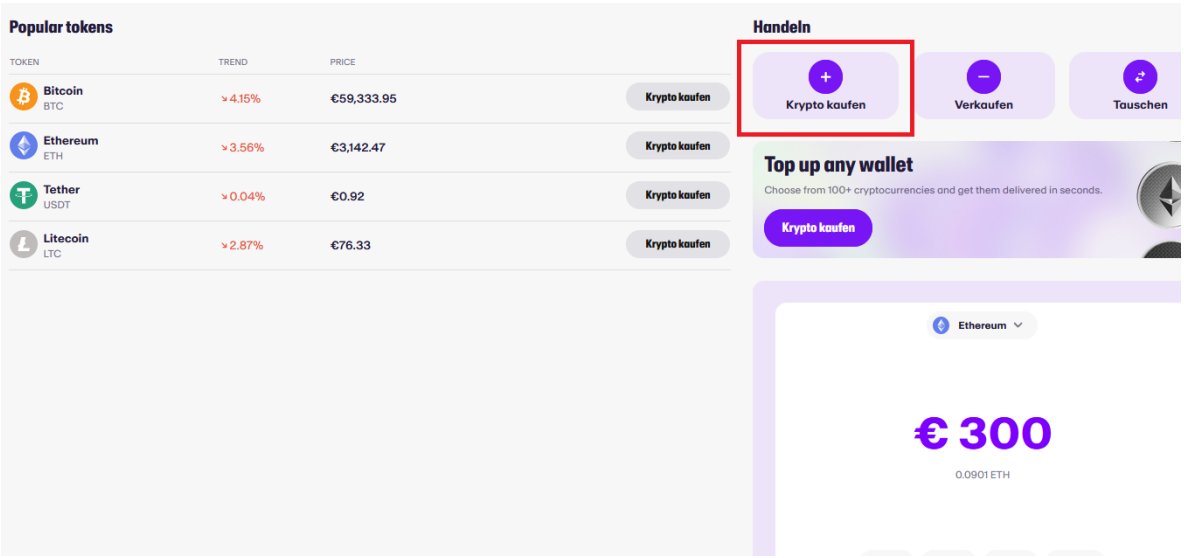
Danach geben wir unsere Email Adresse ein, mit der wir uns auf der MoonPay Website registrieren.



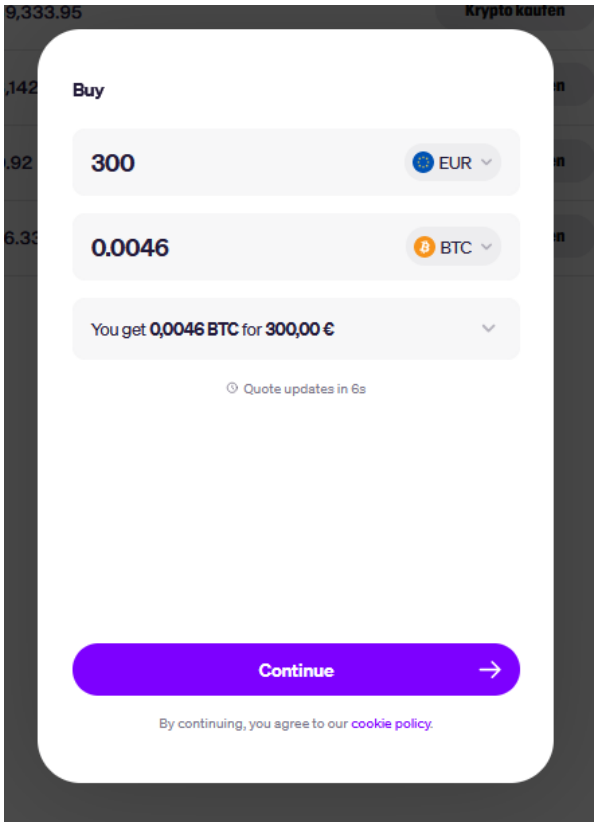
MoonPay sendet in weiterer Folge einen Verifizierungscode an die Email Adresse, mit dem wir unsere Email Adresse bestätigen. Zudem müssen hier die Nutzungsbedingungen akzeptiert werden.



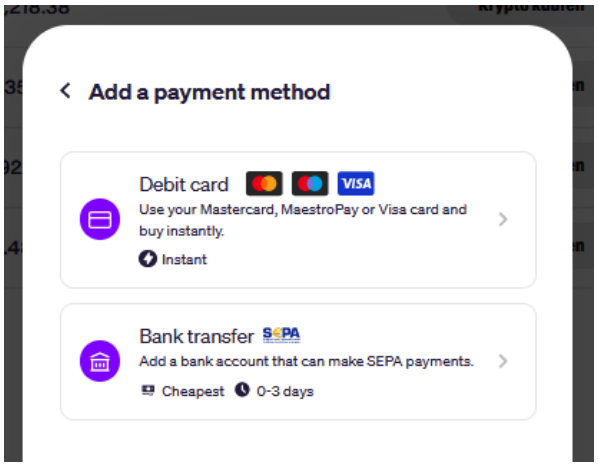
Nach der Bestätigung landen wir in der *Home* Area der Website und können dort Bitcoins kaufen oder verkaufen. Um unsere ersten Bitcoins zu kaufen, klicken wir oben rechts auf *Krypto kaufen*.



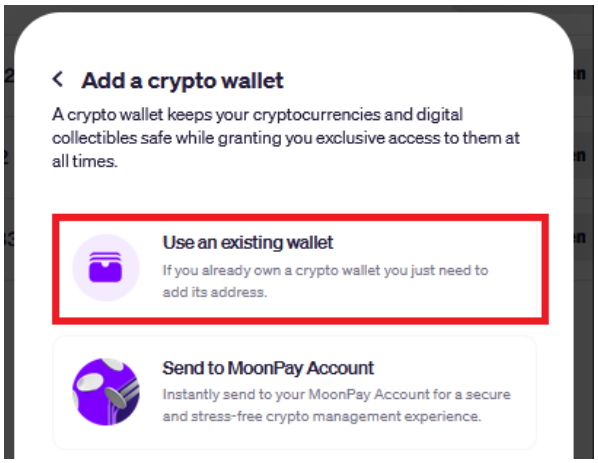
Damit sollte sich ein Fenster öffnen, in dem wir eingeben, wieviel BTC wir erwerben möchten. BTC sollte bereits voreingestellt sein. **ACHTUNG! MoonPay erlaubt uns hier, auch andere Kryptowährungen auszuwählen. Allerdings können wir keine anderen Kryptos an unsere Wallet senden, da Electrum ausschließlich für BTC entwickelt wurde.** Möchte man andere Kryptos erwerben, können wir uns diese auf den MoonPay Account senden. Nachdem ein Beitrag eingegeben wurde, klicken wir auf *Continue*.



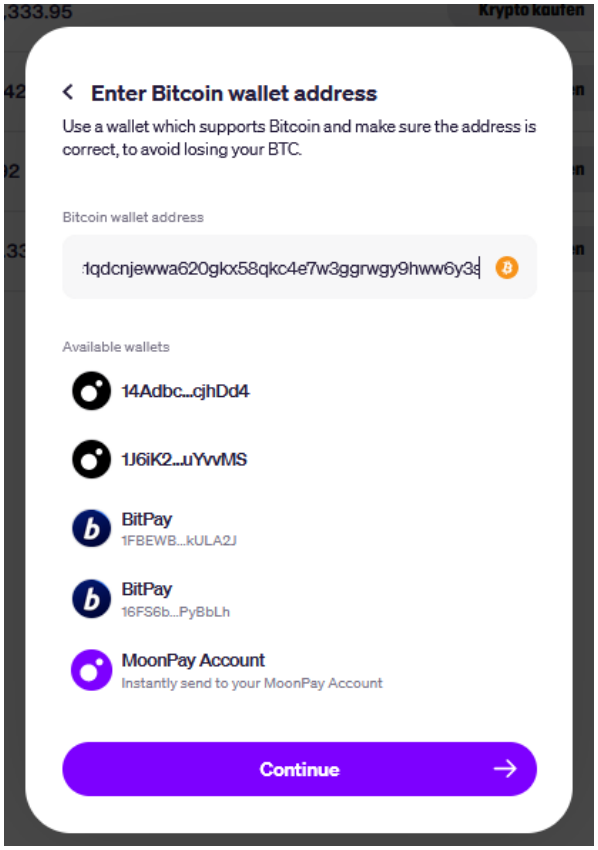
Danach müssen wir eine Zahlungsmethode hinzufügen. Zur Auswahl stehen eine Debit- und Kreditkarte oder Banküberweisung. Nach Auswahl der Zahlungsmethode müssen wir noch die Kartennummer und die restlichen Informationen ausfüllen. Wurden die Kontoinformationen eingegeben, klicken wir auf *Continue*.



Im nächsten Schritt können wir auswählen, ob wir die Bitcoins an unsere eigene Wallet senden möchten oder an den MoonPay Account. In diesem Fall senden wir die Bitcoins an die eigene Wallet und wählen die Option *Use an existing wallet*.



Im nächsten Schritt fügen wir unsere Wallet Adresse ein. Dafür öffnen wir unsere Wallet, klicken auf den Reiter *Empfangen*, klicken dann auf *Zahlungsaufforderung erstellen* und kopieren auf der rechten Seite die Bitcoin Adresse. Wichtig ist, dass wir hier die herkömmliche Bitcoin Adresse mit dem blauen Icon verwenden und nicht die Bitcoin URI Adresse. Die Adresse fügen wir dann in das Eingabefeld auf der MoonPay Website ein. Bevor wir auf *Continue* klicken, überprüfen wir nochmals die Bitcoin Adresse.

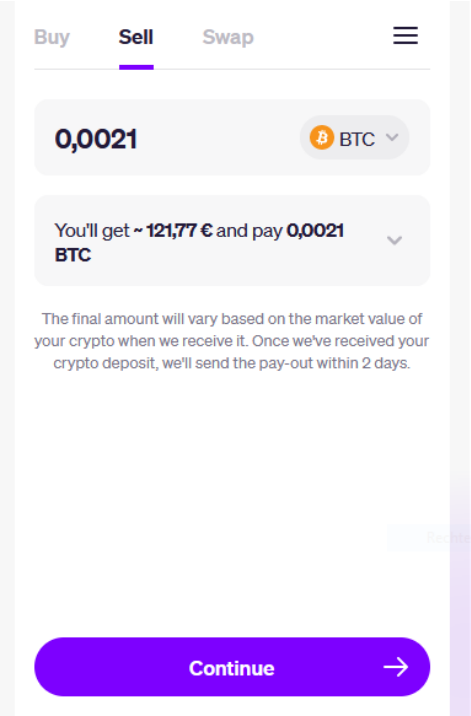


Danach überprüft man nochmals die Zahlungsinformationen und klickt auf *Check out*. Ist eine 2FA für die Debit- oder Kreditkarte aktiviert, muss die Bezahlung noch mit einem zweiten Gerät abgesegnet werden.

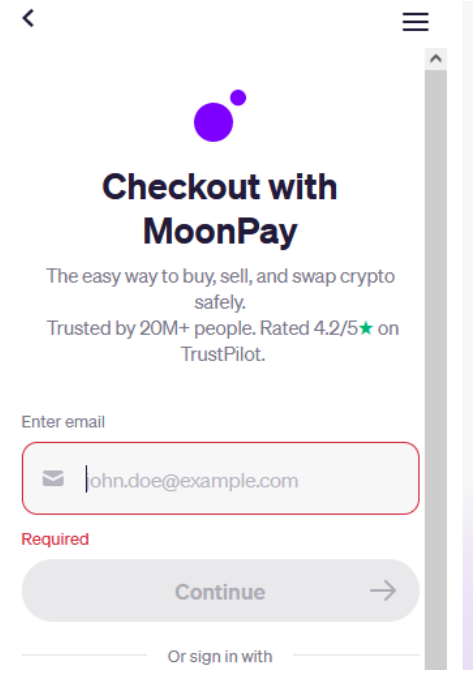
Danach wird der Kauf von MoonPay verarbeitet und in wenigen Minuten sollten die Bitcoins in der Wallet eingelangt sein.

13.5 Bitcoins verkaufen

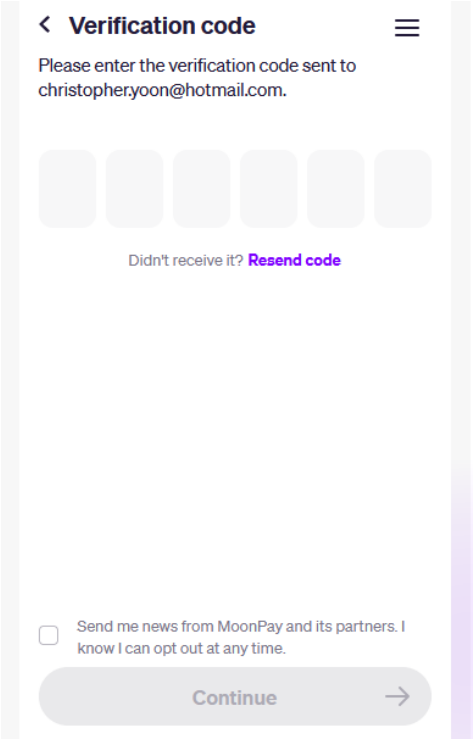
Um Bitcoins zu verkaufen, öffnen wir den Browser und die MoonPay Website https://www.moonpay.com/. Im Menü der MoonPay Website klicken wir auf die Option *Sell crypto*, wo wir zuerst definieren wieviel BTC wir liquidieren und auf unser Bankkonto auszahlen möchten. Danach klicken wir auf *Continue*.



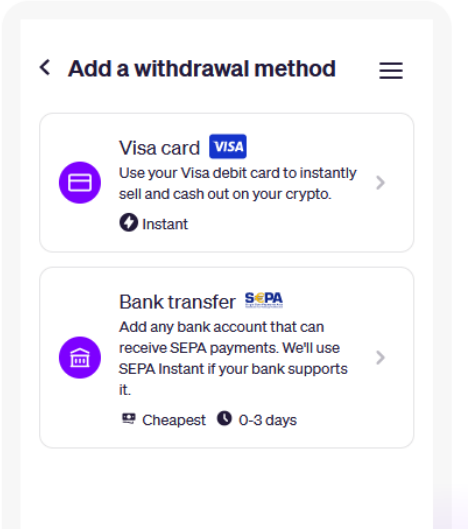
Im nächsten Schritt geben wir unsere Email Adresse ein, mit der wir uns bei der MoonPay Website beim Erstkauf registrierten und klicken auf *Continue*. Haben wir uns noch nicht auf MoonPay registriert, müssen wir uns zuerst mit einer Email Adresse registrieren.



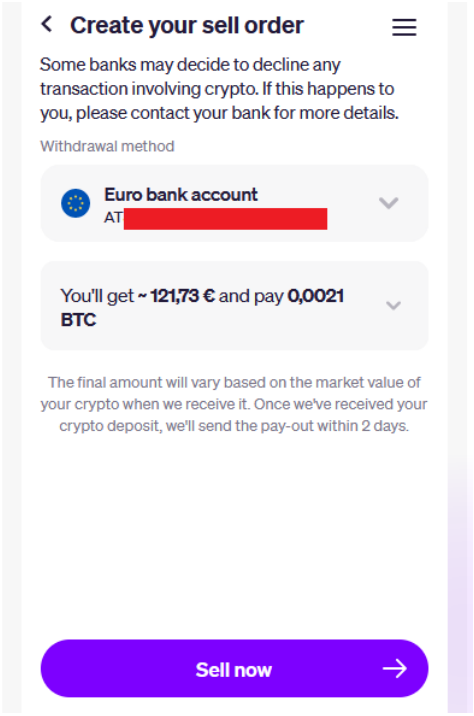
Nach der Eingabe der Email Adresse sendet uns MoonPay einen Bestätigungscode auf unsere Email Adresse. Den Bestätigungscode geben wir auf der MoonPay Seite ein und klicken auf *Continue*.



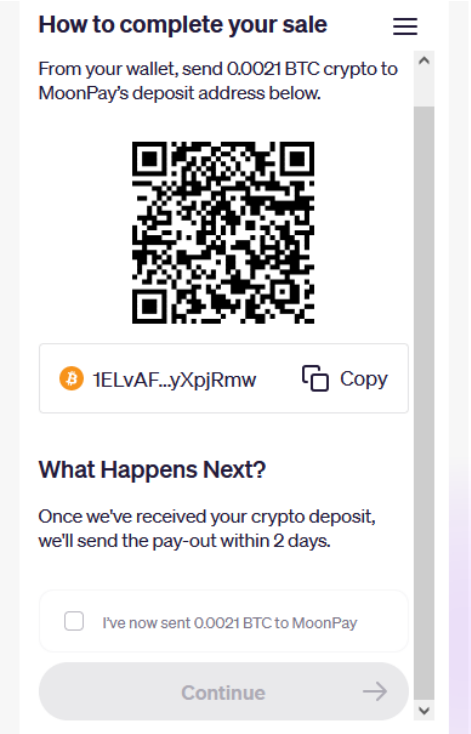
Im nächsten Schritt fügen wir ein Bankkonto hinzu, auf das die Überweisung durchgeführt werden soll.



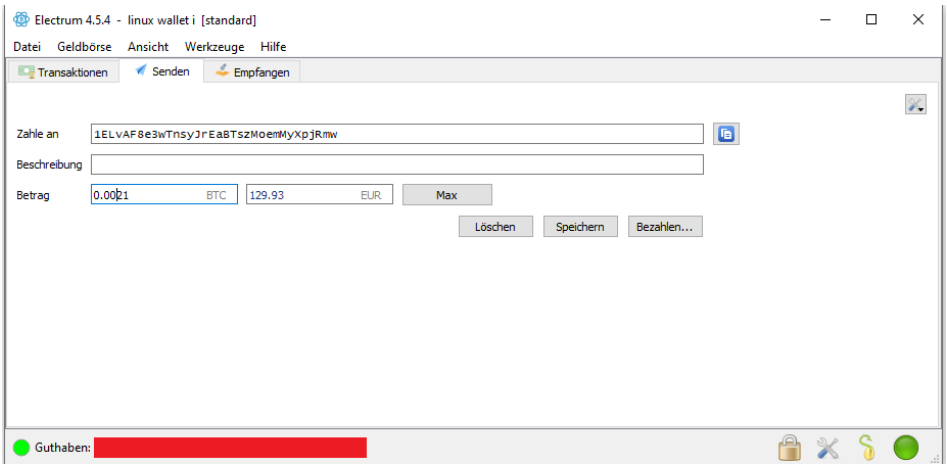
Nachdem wir die IBAN der Kontonummer eingegeben haben, können wir nochmals die Transaktion überprüfen. Sind die Kontoinformationen korrekt, klicken wir auf *Sell now*.



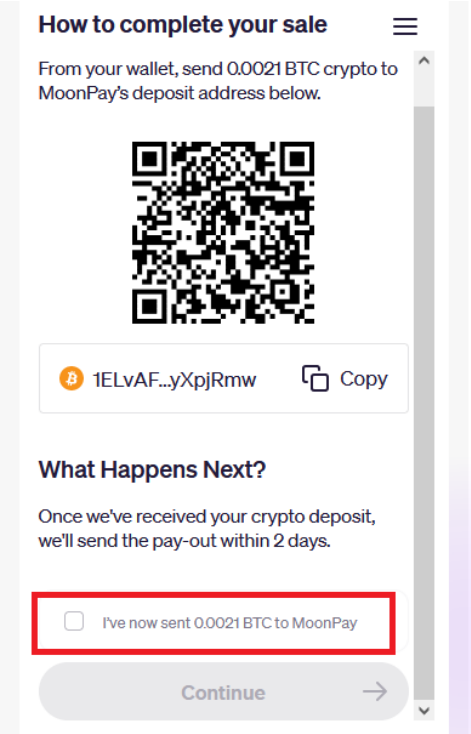
Abschließend erhalten wir die Bitcoin Adresse von MoonPay und den BTC Betrag, den wir von unserer Wallet aus versenden müssen. Wir kopieren die Adresse und wechseln zur Wallet.



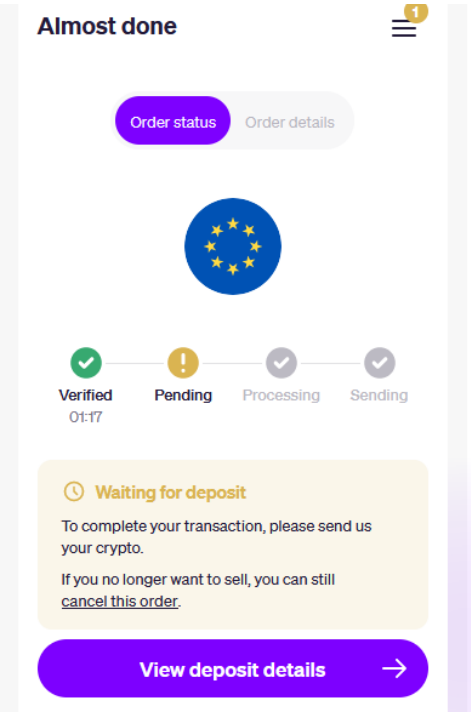
In der Wallet wechseln wir auf den Reiter *Senden* und tragen die Transaktionsdaten ein. Danach klicken wir auf *Bezahlen*, definieren das Gebührenziel, klicken auf *OK* und bestätigen die Transaktion mit dem Wallet Passwort und dem Google Authenticator Code.



Danach wechseln wir wieder zurück zum Browser und bestätigen, dass die Transaktion von der Wallet gesendet wurde. Danach klicken wir auf *Continue*.



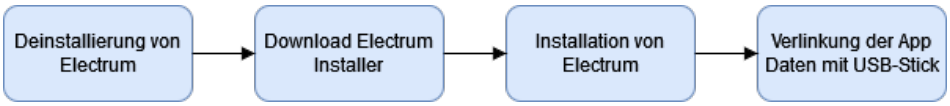
Nun warten wir, bis MoonPay die Transaktion erhalten und verarbeitet hat.



Ist die Transaktion abgeschlossen, sollte in den kommenden Tagen der Betrag auf dem Konto einlagen.

13.6 Electrum Wallet aktualisieren

Electrum hat aus Sicherheitsgründen keine Built-In Update Funktion implementiert. Das heißt, wenn man Electrum auf die neueste Version aktualisieren möchte, muss das Programm deinstalliert und neu installiert werden. Folgende Schritte wären dafür durchzuführen:



- In Schritt 1 deinstallieren wir die alte Version von Electrum und löschen den verlinkten *Electrum* Ordner im *Roaming* Ordner. Siehe Kapitel 9 Abschnitt 9.1.
- In Schritt 2 laden wir den Electrum Installer von der Electrum Website runter. Siehe Kapitel 7 Abschnitt 7.2.
- In Schritt 3 installieren wir die neue Version von Electrum. Siehe Kapitel 7 Abschnitt 7.3.
- In Schritt 4 verlinken wir abschließend das neuinstallierte Programm mit unseren App Daten auf dem USB-Stick. Siehe Kapitel 8 Abschnitt 8.3.

ACHTUNG! Sollte sich die Wallet nach der Verlinkung nicht öffnen lassen, kann es sein, dass das Entwicklerteam von Electrum die Ordnerstruktur der App Daten änderte und nun nicht mehr mit der Ordnerstruktur auf dem USB-Stick übereinstimmt. In diesem Fall müssen wir die Wallet mit der Seed Phrase wiederherstellen und das Programm erneut mit dem USB-Stick verlinken.

Folgende Schritte wären in einem solchen Fall durchzuführen:

- In Schritt 1 müssen wir Electrum nochmals deinstallieren und den verlinkten *Electrum* Ordner im *Roaming* Ordner löschen. Siehe Kapitel 9 Abschnitt 9.1.
- In Schritt 2 öffnen wir erneut den Installer der neuen Electrum Version, den wir zuvor gerade runtergeladen haben und installieren das Programm erneut. Siehe Abschnitt Kapitel 7 Abschnitt 7.3.
- In Schritt 3 führen wir die Wiederherstellung der Wallet mithilfe der Seed Phrase durch. Siehe Kapitel 9 Abschnitt 9.4.
- In Schritt 4 löschen wir den *Electrum* Ordner vom USB-Stick.
- In Schritt 5 verknüpfen wir erneut das neu installierte Electrum Programm mit dem USB-Stick. Siehe Kapitel 7 Abschnitt 7.6.

Nun sollte Electrum aktualisiert sein und die Wallet wieder wie gewohnt funktionieren.

14 Fazit

Ziel des vorliegenden Manuals war es, einen Anknüpfungspunkt für Bitcoin Neulinge und Interessierte zu schaffen, um sich im Bitcoin Space zurechtzufinden. Bitcoin bedeutet finanzielle Freiheit und Autonomie. Allerdings haben Freiheit und Autonomie ihren Preis. Der Preis dafür ist, dass man Selbstverantwortung übernimmt und Zeit investiert, um die Technologie zu verstehen und die eigene Wallet zu sichern. Dass man sich dabei in unbekanntes Terrain begibt und die eigene Komfortzone verlassen muss, ist Teil dieser Selbstverantwortung. Anders ausgedrückt: Die eigentliche Investition in Bitcoin ist nicht nur das Geld, das man sich anspart, sondern auch die Zeit und Energie, um sich weiterzuentwickeln und sich fortzubilden.

Damit unterscheidet sich Bitcoin nicht von anderen Technologien. Um die Steuerung und Handhabung eines Automobils zu erlernen, muss man sehr viel Zeit und Energie investieren. Dennoch verlassen wir unsere Komfortzone und lernen die Verkehrsregeln und die praktische Handhabung eines Automobils, da das Automobil äußerst nützlich ist und uns Freiheit und Autonomie in der Mobilität ermöglicht. Dies bedeutet nicht, dass jedes Detail der Technologie verstanden werden muss. Wenn wir mit dem Auto fahren, müssen wir nicht genau wissen, wie ein Motor oder die Elektronik funktioniert. Dennoch kann es hilfreich sein, ein grundsätzliches Verständnis davon zu haben.

Ähnlich ist es mit Bitcoin. Es ist nicht notwendig jedes technische Detail des Mining Prozesses oder des Proof-of-Work Algorithmus zu verstehen. Entscheidend ist, dass wir die Verkehrsregeln und die Handhabung kennen. Dennoch ist es hilfreich, die Technologie zu verstehen, um beispielsweise zu erkennen, warum die dezentrale Struktur des Netzwerks wichtig für die Resilienz und Sicherheit ist oder warum Energie und Rechenleistung notwendig sind, um das Netzwerk zu sichern.

Die Sicherung der Wallet liegt also in der persönlichen Verantwortung. Für die technische Sicherung der Wallet wurden die Konzepte Selbstaufbewahrung, Cold-Storage, 2FA und kryptographische Verschlüsselung kombiniert. Zusätzlich zur technischen Sicherung ist auch die sichere Aufbewahrung der Seed Phrase eine zentrale Herausforderung. Um den Wiederherstellungsschlüssel sicher aufzubewahren, empfiehlt sich eine Kombination aus Redundanz, Security Layer und Verschlüsselung. Bei größeren Sparsummen wird empfohlen auch ein Schließfach für die Aufbewahrung der Seed Phrase in Betracht zu ziehen. Zudem wird empfohlen, dass man sich um den digitalen Nachlass kümmert, um im Todesfall die Ersparnisse weiter vererben zu können.

Wird die Wallet als Cold-Storage Wallet mit einer 2-Factor Authentication konfiguriert, sollte das Risiko eines Hackerangriffs auf ein Minimum reduziert sein. Dennoch liegt es in der persönlichen Verantwortung, die Wallet instandzuhalten und zu sichern und den Umgang mit der Wallet zu lernen. Wichtig ist auch, dass man sich nicht durch Phishing Attacken austricksen lässt und Passwörter, Wiederherstellungsschüssel und 2FA-Codes an Unbekannte weitergibt. Zugangscodes wie der Wiederherstellungsschlüssel, Passwörter oder andere Informationen der Wallet sollten unter keinen Umständen an Unbekannte weitergegeben werden. Darüber hinaus ist man dazu angehalten, den eigenen Computer zu warten und zu upgraden.

Selbst wenn die Wallet sicher eingerichtet ist und alle empfohlenen Sicherheitsvorkehrungen getroffen wurden, ist es wichtig, wachsam zu bleiben und sich kontinuierlich über neue Sicherheitsrisiken und -maßnahmen zu informieren. Die Cyberwelt und der Bitcoin-Space sind dynamisch und ständig im Wandel. Daher ist es unerlässlich, sich als Nutzer weiterzubilden und auf dem neuesten Stand zu bleiben, um die eigene finanzielle Autonomie langfristig zu schützen.

15 Weitereführende Literatur

Literatur

Ammous, Saifedean – The Bitcoin Standard.
https://academy.saifedean.com/product/tbs-hardcover/

Ammous, Saifedean – The Fiat Standard.
https://academy.saifedean.com/product/tfs-hardcover/

Bier, Jonathan - The Blocksize War: The Battle For Control Over Bitcoin's Protocol Rules.
https://www.goodreads.com/book/show/57429394-the-blocksize-war

Gervais, Arthur et al – On the Security and Performance of Proof-of-Work Blockchains.
https://tinyurl.com/49f93p3j

Graf, Konrad – Commodity, scarcity, and monetary value theory in light of Bitcoin.
https://tinyurl.com/4a26rrkk

Graf, Konrad – On the Origins of Bitcoin – Stages of Monetary Evolution.
https://cdn.nakamotoinstitute.org/docs/on-the-origins-of-bitcoin.pdf

Huerta de Soto, Jesus – Money, Bank Credit and Economic Cycles.
https://mises.org/library/book/money-bank-credit-and-economic-cycles

Hülsmann, Jörg Guido – The Ethics of Money Production.
https://mises.org/library/book/ethics-money-production

Mises, Ludwig von – The Theory of Money and Credit.
https://mises.org/library/book/theory-money-and-credit

Mises, Ludwig von – Human Action – A Treatise on Economics.
https://mises.org/library/book/human-action

Nakamoto, Satoshi – The Bitcoin Whitepaper – Bitcoin: A Peer-to-Peer Electronic Cash System.
https://bitcoin.org/bitcoin.pdf

Poon, Joseph & Dryja, Thaddeus – The Bitcoin Lightning Network: Scalable Off-Chain Instant. Payments.
https://lightning.network/lightning-network-paper.pdf

Rothbard, Murray – The Mystery of Banking.
https://mises.org/library/book/mystery-banking

Rothbard, Murray – What has Government Done to Our Money?
https://mises.org/library/book/what-has-government-done-our-money

Sun, Wei et al – Spatial Analysis of Global Bitcoin Mining.
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9226069/pdf/41598_2022_Article_14987.pdf

Podcasts

Ammous, Saifedean – The Bitcoin Standard Podcast.
https://www.youtube.com/@saifedean/videos

Bitcoin Mechanic - The Battle for Bitcoin.
https://www.youtube.com/watch?v=bCJR7v73r3Q

Breedlove, Robert – The What is Money Show.
https://www.youtube.com/@RobertBreedlove22/videos

Carter, Nic - Bitcoin Core Values at Lex Fridman.
https://www.youtube.com/watch?v=mDyBbGCiBUU

Lowery, Jason - Bitcoin as Non-Lethal Warfare.
https://www.youtube.com/watch?v=PInd7uRiGjs

McCormack, Peter – What Bitcoid Did Podcast.
https://www.youtube.com/@WhatBitcoinDid/videos

Saylor, Michael – Bitcoin Science.
https://www.youtube.com/watch?v=hCQKPBWwxeQ

Saylor, Michael – Bitcoin in the Boardroom.
https://www.youtube.com/watch?v=ciB4ZiehEIs

Saylor, Michael – Bitcoin is Digital Energy.
https://www.youtube.com/watch?v=x4-e5wq5AJ8

Saylor, Michael – 10 Rules for Life.
https://www.youtube.com/watch?v=-w-aYVXcOk4

Truth for the Commoner – TFTC Podcast.
https://www.youtube.com/@TFTC/videos