Bitcoin & Co.

Wohin damit: Wallet (Teil 3)

In den Teilen 1 und 2 ging es um die Theorie der Blockchain-Technik am Beispiel des Bitcoin. Jetzt kommt die Praxis.

Symbolischer ep-Bitcoin
Quelle: A. Purwin

„Be your own bank" – sei deine eigene Bank. Damit ist klar, wer für alles verantwortlich ist: Sie selbst! Und das im strengsten Sinne. Eigentlich sollte jeder die grundsätzlichen Regeln über private IT-Sicherheit kennen. Beim Thema „digitales Geld" bestimmen diese Regeln mit über Erfolg oder Verderben. Daher folgen dazu ein paar Tipps, vorrangig für PC-Nutzer.

- Verwenden Sie ein aktuelles Betriebssystem, das mittels Updates auf dem neuesten Stand gehalten wird.
- Nutzen Sie professionelle Virenscanner.
- Verwenden Sie Login-Anmeldungen für Windows und ggf. auch für das BIOS.
- Bewahren Sie solche Anmeldedaten grundsätzlich sicher auf (z. B. Bankschließfach). Zettel unter der Tastatur sind wie Bargeld unter der Tastatur.
- Sensible Daten gehören nicht ungeschützt auf eine Festplatte oder einen USB-Stick. Windows hat von Haus aus eine kostenlose Verschlüsselungstechnik im Gepäck: „bitlocker". Hochsensible Daten sollten überhaupt nicht auf solchen Datenträgern lagern.
- Vermeiden Sie Einfallstore im DSL-Router. Setzen Sie z. B. nicht bedenkenlos Web-Cams vom Discounter ein.
- Achten Sie generell in Ihrem (sicher konfigurierten) Browser in der Eingabezeile auf sicheres Surfen: Ein Schlüsselsymbol, gefolgt von https:// in grüner Schrift weist auf eine sichere Web-Seite hin. Das muss zu einer festen Angewohnheit werden.
- Verwenden Sie sichere Passwörter. Dabei kommt es nicht so sehr darauf an, dass kryptische Sonderzeichen enthalten sind. Entscheidend ist die Länge des Passworts (Anzahl der Zeichen). Geraten wird zu mindestens zwölf Zeichen. Passwortmanager bringen da eine große Erleichterung, wie beispielsweise 1Password.
- Verwenden Sie die 2FA (Zwei-Faktor-Autorisierung), wenn möglich.

Autor
Dipl.-Ing. (FH) Hannes Leidenroth, LeiTech GbR, Sandkrug, unterstützt von Co-Autor Dipl.-Ing. (FH) Thomas Imhoff.

Digitale Geldbörse

Der Begriff „wallet" steht stellvertretend für Portemonnaie/Geldbörse. Man könnte also denken, Kryptowährungen werden in den eigenen Wallets gespeichert. Das fühlt sich in der Praxis auch so an, doch genaugenommen stimmt es nicht. Welcher Wert hinter welcher Adresse liegt, ist nur auf der Blockchain gespeichert, und diese Datenbank ist ja weltweit vorhanden. Eine Wallet ist so gesehen eigentlich nur der Schlüsselbund, um Zugang zum eigenen Guthaben zu erreichen. Dort (in der Wallet) liegt der private Schlüssel des jeweiligen Eigentümers.
Stellen Sie sich vor, Sie hätten z. B. über den Online-Händler bitcoin.de Bitcoins im Wert von 10 000,– € gekauft. Auf Ihrem dortigen Account können Sie danach das Bitcoin-Guthaben einsehen bzw. kontrollieren. Spätestens jetzt wird jeder darüber nachdenken, ob das Geld dort sicher aufgehoben ist oder nicht. Die Antwort lautet: es ist nicht sicher (genug) aufgehoben. Diese Online-Händler bzw. Kryptobörsen (z. B. Kraken, Coinbase, Bitstamp) sind keine Banken. Daher ist Misstrauen stets die richtige Einstellung.
Es kommt leider regelmäßig vor, dass solche Handelsplätze gehackt werden, wie beispielsweise Anfang 2018, als die japanische Börse Coincheck gehackt wurde und umgerechnet rund 430 Mio. € der Währung NEM („new economic money", im asiatischen Raum beliebt) verschwanden. Dieser Coin hat sich eigentlich zum Ziel gesetzt, für eine gerechtere Verteilung von Reichtum zu stehen, was wohl jemand falsch verstanden haben muss. Hier bemerkt man bereits die Auswirkungen, wenn es an bestimmter Regulierung fehlt: manche Börsen schlampen bei der Sicherheit.
Aber zurück zum Handelsplatz bitcoin.de: Hier hat der Betreiber scheinbar selbst hohe Sicherheitsvorkehrungen getroffen, was lobenswert ist. So heißt es dort, dass 98 % aller Kryptoguthaben in sog. „cold wallets" aufgehoben werden. D. h., diese Wallets haben keinen Kontakt zum Internet und lassen sich folglich nicht per Hack abräumen (im Gegensatz zu „hot wallets"). Trotzdem gilt auch hier: kein blindes Vertrauen! Eigenes Geld sollte man in eigenen Wallets aufheben. Das heißt dann in der Praxis: Das Guthaben von bitcoin.de an die eigene Wallet transferieren (dabei immer auf evtl. anfallende Gebühren achten).
Es gibt unterschiedliche Wallet-Ausführungen bzw. Möglichkeiten:

- Desktop-Wallet
- Web-Wallet
- Paper-Wallet
- Hardware-Wallet
- Mobile-Wallet

Desktop-Wallet: stellvertretend nenne ich hier z. B. die kostenlose Exodus-Wallet. Diese ist sehr einfach zu bedienen. Außerdem verwendet sie im Hintergrund eine Anbindung an die „Wechselstube" ShapeShift, auf die später noch eingegangen wird. Aber bei Desktop-Wallets muss der eigene PC sicher vor Angriffen sein. Daher würde ich diese Wallets anfangs nur für eher kleinere Beträge verwenden. Auch die Firma Ledger hat neuerdings eine Desktop-Wallet im Programm.

Web-Wallet: diese Wallets sind (meines Erachtens) nicht zu empfehlen, denn dann könnte man das Guthaben gleich beim Online-Händler lassen.

Paper-Wallet: man kann sich alle Adressen, Daten, Guthaben usw. auf Papier notieren bzw. ausdrucken und es sicher aufbewahren. Dann ist es zumindest vor Hacker-Angriffen geschützt. Eine Möglichkeit dazu bietet die sichere Seite „bitaddress.org" (man darf sich nicht verschreiben, da es ähnlich lautende Seiten gibt, die an Ihr Vermögen gelangen wollen). Diese HTML-Seite kann man sich abspeichern und danach mit dem PC offline weiterarbeiten. Durch Mausbewegungen erzeugt man sich a) eine zufällige Bitcoin-Adresse (öffentlicher Schlüssel), an die jemand Geld transferieren kann, und b) den zugehörigen privaten Schlüssel („private key"). Eine auf diesem Wege erzeugte Bitcoin-Adresse ließe sich später auch wieder in andere Anwendungen importieren. Bis dahin

muss man aber dieses Stück Papier extrem sicher aufbewahren. Es gibt Schätzungen, dass 20 bis 30 % aller bislang geschürften 17 Mio. Bitcoins für immer verloren sind, weil diese privaten Schlüssel bzw. PINs oder Zugangsdaten nicht mehr verfügbar sind.

Hardware-Wallet: Diese gehören zu meinen Favoriten. Sie haben Ähnlichkeit mit USB-Sticks und wenn man sie abzieht, sind sie nicht angreifbar („cold wallet"). Zwei Hersteller sind sehr bekannt: Trezor (Bild 8) und Marktführer Ledger. Allerdings sind Hardware-Wallets mit rund 80 € nicht gerade billig. Die Handhabung der Trezor-Wallet ist für Neueinsteiger jedoch einfacher als beim Ledger. Im Januar 2019 hat der Chaos-Computer-Club (CCC) im Rahmen seines 35. CCC-Kongresses scheinbar bewiesen, dass auch diese Wallets zu knacken sind, aber das muss man relativieren. Wenn drei Experten drei Monate lang dafür brauchen, sagt das schon mal aus, wie schwierig so etwas ist. Und wenn Wallet-Nutzer die zusätzliche „Passphrase" innerhalb der Wallet benutzt hätten, wäre auch dieser Angriff erfolglos geblieben (Trezor-Wallet). Auf die genauere Handhabung wird gleich eingegangen.

8 Hardware-Wallet der Firma Trezor

Quelle: Trezor

Mobile-Wallet: Wenn sich „Unterwegs-Einkäufe mit Bezahlung per Krypto" mehr durchsetzen (was wohl noch dauern wird), braucht man dafür eine einfache Handy-App. Via QR-Code lassen sich Transaktionen damit sehr einfach ausführen. Hier sollen beispielhaft die Apps von „Coinbase" oder die Bread-Wallet (BRD) genannt werden.Wem eine Hardware-Wallet zu kompliziert ist, der sollte bei der seit Januar 2019 erhältlichen Bison-App gut aufgehoben sein (Sowa Labs, Deutsche Börse Stuttgart). Diese ist so einfach gestaltet, dass das Handling massentauglich sein sollte. Private Schlüssel, lange Adressen und Firmware-Updates werden einem hier nicht zugemutet. Aber man vertraut seine Einlagen dann dieser Plattform an. Dafür ist es so einfach wie Online-Banking. Dort sind anfangs folgende Coins handelbar: Bitcoin BTC, Ethereum ETH, Litecoin LTC und Ripple XRP.

My Trezor

Die Handhabung bzw. Ersteinrichtung dieser „Kryptogeldbörsen" (oder besser „Schlüsselbunde") ist zunächst etwas gewöhnungsbedürftig. Die spätere Verwendung gestaltet sich dann aber relativ einfach. Früher konnte man nur wenige Währungen in solchen Wallets aufbewahren, heute sind es aber beim Trezor sehr viele verschiedene Kryptos

(teils direkt, teils über Verlinkung). Auf die verschiedenen Währungen/Coins wird noch eingegangen.

Die Einrichtung ist menügeführt, wobei dazu die (sichere) Internetseite trezor.io benötigt wird. Diese Seite wird auch für die spätere Verwendung der Wallet regelmäßig benötigt. Sprich: wer glaubt, er hätte eine einfache „USB-Geldbörse“, der täuscht sich. Ohne „online“ zu sein, geht hier nichts mehr. Bargeldanhänger müssen da also schon das erste Mal tief durchatmen. Allerdings wird die Trezor-Wallet auch von anderen Seiten unterstützt, so dass man nicht zwingend auf trezor.io angewiesen ist, falls es dort mal heißen sollte „server down“.

Der wichtigste Punkt bei der Einrichtung solch einer Wallet ist der sogenannte „seed“ (auch „recovery phrase“ genannt). Dabei handelt es sich um ein langes Super-Passwort, das zur Erstellung einer möglichen Ersatzwallet benötigt wird, sollte die normale Wallet defekt sein oder gestohlen worden sein.

Die Erstellung dieses Super-Passwortes (das ist der echte „private Schlüssel“) ist im gewissen Sinne automatisiert, aber man muss sich 24 einfache, englische Wörter notieren. Diese 24 Wörter sind der Tresorschlüssel und daher muss man ihn absolut sicher (evtl. mehrfach an verschiedenen Orten) aufbewahren. Werden hier Fehler gemacht, besteht die Möglichkeit, das komplette Kryptovermögen zu verlieren.

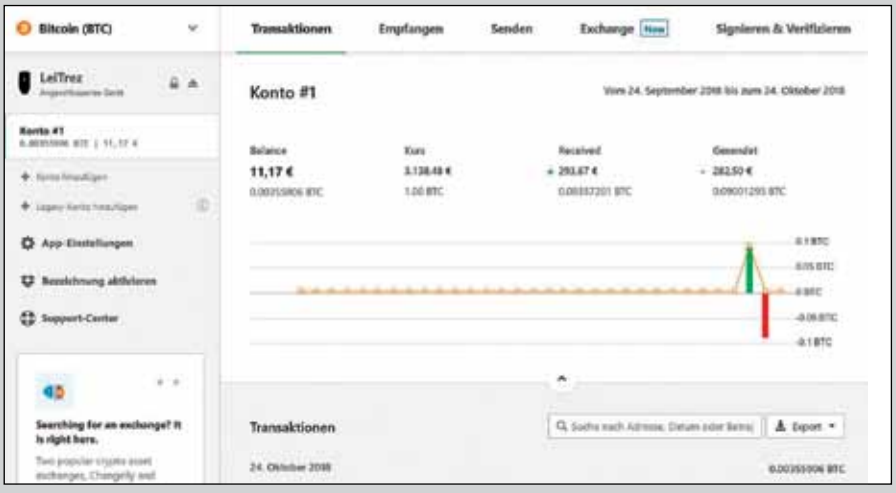
Hier dürfen Bargeldanhänger dann das zweite Mal durchatmen, denn dass die Software diesen heiligsten Privatschlüssel („seed“) vorschlägt und man diesen nur brav abschreiben muss, verlangt echtes Vertrauen, denn man würfelt hier ja nicht selbst. Aber das ist hierbei der normale Vorgang. Die Wahrscheinlichkeit, den Privatschlüssel zu knacken, ist kleiner, als neun Mal in Folge beim Lotto sechs Richtige mit Zusatzzahl zu erzielen. Aber man darf ihn eben nicht unter die Tastatur legen.

Ein Blick in die Wallet zeigt dann die privaten Daten und ist recht übersichtlich dargestellt, vergleichbar einem Kontoauszug (Bild 9). Trotzdem nochmals der Hinweis, dass speziell die Einrichtung dieser Hardware-Wallets nicht unbedingt als „massentauglich“ angesehen werden darf. Auch regelmäßige Updates der Firmware (oder möglicher Browser-Plug-Ins/bridge) sind durchzuführen, was auch nicht jedermanns Sache ist.

Diese Wallet dient also verschiedenen Zwecken: der Aufbewahrung des privaten Schlüssels, damit man jederzeit an seine Guthaben herankommt, und den Möglichkeiten, Geld an andere zu senden oder von anderen zu empfangen.

Im Folgenden wird gezeigt, wie z. B. eine Überweisung stattfinden kann (Transaktion „Senden“) und was dabei beachtenswert ist, weil es sich doch von einer „Sparkassen-IBAN-Überweisung“ stark unterscheidet. Unabhängig von der Wallet handelt es sich prinzipiell immer um den gleiche Vorgang. Derjenige, der von mir Geld haben will, muss mir vorab seine Empfangsadresse senden (das ist sein öffentlicher Schlüssel („public key“, vergleichbar zu seiner Konto-Nr.), in diesem Falle von einer Handy-Wallet erzeugt (Bild 10). An diese Adresse darf ich Bitcoin BTC senden. Vorsichtshalber sollte man immer vorher absprechen, dass man vom selben Coin redet, also in diesem Fall von Bitcoin „BTC“, sonst wäre das Geld verloren. Der Empfänger könnte immer genau diese Adresse an seine Freunde senden und immer auf dieser Adresse Geld empfangen. Aus Bequemlichkeit oder Unwissenheit wird das auch oft so gemacht. Ratsamer ist es aber, für jeden Transfer eine eigens dafür generierte Adresse zu verwenden.

Beim Transfer wird ein Betrag von einer Adresse an eine andere gesendet, mehr Informationen werden nicht übermittelt. Es gibt keinen Namen des Absenders (anonymer Transfer), keine Betreffzeile, keinen Verwendungszweck. Falls der Empfänger für diesen bevorstehenden Transfer eine eigene Adresse erzeugt hat, könnte er den zu erhaltenden Betrag später einer Person oder einem Vorgang zuordnen. Ich habe also jetzt z. B. per E-Mail seine Empfangsadresse für BTC erhalten. Nun verwende ich meine Wallet und die Funktion „Senden“, um an diese Empfangsadresse Geld zu senden. Dabei sollte man die langen Adressen immer nur über die Zwischenablage kopieren und sich im Kopf zur Sicherheit den Anfang und das Ende der Adresse kurz merken. Das dient nur der Kontrolle, dass man auch wirklich den gewollten aktuellen Inhalt der Zwischenablage bearbeitet. Man trägt die Adresse in die Sendemaske ein und den zu überweisenden Betrag (Bild 11). Normalerweise lässt sich die üblich gewünschte FIAT-Währung „Euro“ einstellen (unter „settings“), momentan war jedoch nur US$ möglich. Die Gebühr („fee“) wird separat ausgewiesen und könnte eigenverantwortlich noch verändert werden. Zahlen muss sie immer der Absender. Bei einer geringen Gebühr muss man mit einer Bestätigungszeit von ca. 40 min rechnen. Sechs Knoten des Bitcoin-Netzwerkes müssen die Transaktion als gültig bestätigen, dann kann sie in einen Block aufgenommen werden. Der Empfänger erhält jedoch schon meistens nach sehr kurzer Zeit (z. B. schon nach einer Bestätigung) eine Info über diesen Zahlungsvorgang, muss also nicht die volle Zeit war-

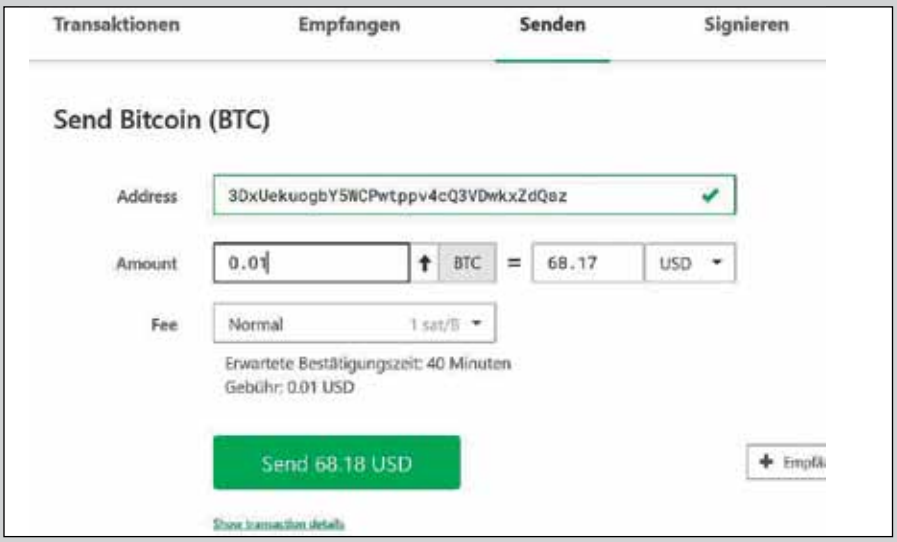


Quelle: H. Leidenroth

Quelle: H. Leidenroth

10 **Empfangsadresse einer Handy-App**

◀ 9 **Blick in die Wallet**



Quelle: H. Leidenroth

Quelle: H. Leidenroth

⓬ **Zahlvorgang in Arbeit/pending (Handy-App)**

◀ ⓫ **Sendemaske einer Wallet**

ten, um zu wissen, dass ihm das Geld gesendet wurde. Ausgeben kann er es aber erst wieder, wenn diese Transaktion endgültig in der Blockchain verewigt worden ist. Man erkennt aber, dass der Zahlungsvorgang in Arbeit ist (Bild ⓬).

Zum Schluss noch ein Beispiel als kleiner Hinweis: Ich möchte von einer Person eine Empfangsadresse haben, um ihm einen Krypto-Betrag zu senden. Zu meinem Erstaunen fragt mich die Gegenseite ebenfalls nach einer Empfangsadresse von mir, was auf den ersten Blick wenig Sinn ergibt. Dahinter verbirgt sich eine einfache Angelegenheit: Es kann vorkommen, dass mein Betrag aus irgendwelchen Gründen nicht genau passend ist, und ich daher Wechselgeld zurückerhalten muss. Und für diesen Rücktransfer benötigt mein Gegenüber dann natürlich eine Empfangsadresse von mir. Solche Situationen können bei automatischen Zahlungsvorgängen passieren, wenn man z. B. an Börsen eine Währung in eine andere tauscht. Insofern kann es doch sinnvoll sein, dass man einen „Wechselgeld-Rückkanal“ ermöglicht, was nur über eine ausgewiesene eigene Empfangsadresse passieren kann. Würde jemand das Wechselgeld an die ursprüngliche Sendeadresse zurückzahlen, wäre es für immer verloren. An diese Denkweise muss man sich gewöhnen, denn es ist eben nicht wie bei einer Konto-Nummer, die ja für beide Richtungen geschaffen ist. ■