Cold-Storage VS Crypto-Exchange

Ich bin zwar schon seit knapp 3 Jahren im Cryptomarkt aktiv und die Problematik von Crypto-Exchanges ist mir seit GOX sehr wohl bewusst. Dennoch bin ich gutgläubiger Weise bisher bei Cryptsy geblieben, weil ich persönlich mit dieser Exchange die besten Erfahrungen gemacht habe. Die ganze Benutzeroberfläche und der Support haben mich bisher nie enttäuscht. Auch war ein Kriterium, dass ich den Chinesen bzw. Asiaten (BTER, etc.) oder den Osteuropäern (BTC-E, etc.) viel weniger traue, als den Amerikanern (CRYPTSY, POLONIEX, BITREX). Sicher, so Typen wie "Wolf of Wall Street" gibt es überall, aber eine hundertprozentige Sicherheit hat man leider nirgendwo.

Womit sich nun die Frage stellt, wohin am sichersten mit meinen Coins. Das große PRO für Crypto-Exchanges ist natürlich die große Auswahl von vielen unterschiedlichen Coins und die Möglichkeit, diese gegeneinander zu handeln. Doch was macht man nun, wenn man sich bei einigen Coins in Sicherheit wiegen möchte? Dann hat man nur die Möglichkeit, sich das zum jeweiligen Coin passende Online-Wallet auf dem PC zu installieren und die Wallet.dat auf einem Stick oder mehreren zu sichern. Bei gängigen Coins ist ein Paperwallet Auszug vielleicht auch eine Überlegung, habe damit aber persönlich noch keine Erfahrung gemacht.

Grundsätzlich kommt man leider an einer Crypto-Exchange nicht ganz vorbei. Das Problem ist, dass der Cryptomarkt derzeit noch unreguliert ist und es deshalb keine richtig seriösen Exchanges gibt. Egal wie, alle könnten sich von heute auf morgen aus dem Staub machen und keinen wird es interessieren, so wie damals bei GOX oder jetzt bei CRYPTSY. Dann bleibt als Alternative nur ein Online-Wallet mit Sicherung der Wallet.dat auf einem Cold Storage, wie USB-Stick oder externe Festplatte, die aber auch alle ihre gewissen Risiken bergen. Ein vergessenes oder verlegtes Passwort (bei 32 Zeichen kann das locker mal passieren) oder eine defekte Festplatte bzw. Stick und alle Coins wären verloren.

Hinzu kommt, dass für einige No-Name Coins kaum noch brauchbare Wallets zu bekommen sind. Nehmen wir als Beispiel mal den Fedora-Coin. Eine aktuelle Online-Wallet gibt es nicht, weil der Coin scheinbar nicht mehr unterstützt wird. Wenn man also dachte, man sichert sich seine Fedora-Coins auf USB-Stick und ist dann fein raus, der kann nun leider auch nichts mehr mit seinen Coins anfangen, weil sich die Blockchain nicht mehr mit der Online-Wallet synchronisieren lässt. Da wäre man mit der Crypto-Exchange besser gefahren, weil man dort seine Fedora-Coins noch umtauschen könnte. Wie man es scheinbar dreht und wendet, jede Coin-Sicherung hat eben auch ihre eigenen Risiken. Somit kann man auch davon ausgehen, dass es niemals mehr für alle Coins ein Online-Wallet geben wird, weil viele Coins nicht mehr unterstützt werden. Zudem ist es absolut unpraktikabel und aufwendig, von mehr als 10 verschiedenen Coins die Online-Wallets auf dem PC zu installieren. Unabhängig von der Datenmenge der Blockchains dauert es in der Regel immer sehr lange, bis man die Online-Wallets auf den aktuellen Stand gebracht hat, wenn man mal ein paar Wochen nicht Online war.

Der Vorfall bei Cryptsy zieht aber noch weit mehr Probleme nach sich, als der eventuelle Verlust der Cryptsy-Anleger. Die Sicherheitsfrage aller Crypto-Exchanges steht dadurch enorm auf dem Prüfstand. Durch Phishing oder Trojaner-Angriffe entstehen in der Cryptowelt enorme Sicherheitslücken und Risiken. Und wie aus dem Nichts kann daraus, von heute auf morgen, ein enormer Schaden entstehen.

Erklärt das mal einem Otto-Normalo, für den vorgegaukelte Sicherheit das A und O ist. Auch wenn einen die Banken am laufenden Band durch die Hintertüre abziehen und das gesamte FIAT-Money-System vor dem Zerfall steht, so gaukelt die Bankenwelt den Anlegern zumindest eine gewisse Sicherheit und angebliches Vertrauen vor. Und darauf vertraut der Otto-Normalo.

Doch der Cryptocoinmarkt zeigt sich nach Cryptsy mal wieder als extrem verwundbar. Bei Bits und Bytes gibt es scheinbar so viele Scheunentore, dass man aufpassen muss, dass einem nicht die Butter vom Brot gezogen wird. Da ist das Vertrauen in eine Exchange nur die Spitze des Eisbergs. Beim sichern seiner Coins lauern für Otto-Normalo noch viel mehr gefahren, eben in Form von Phishing, Passwortverlust, Trojaner, etc.

Die Frage ist deshalb, kann sich die Welt der Cryptocoins überhaupt bis zum Otto-Normalo durchsetzen. Egal ob Crypto-Exchange oder Online-Wallet, kann man in diese Virtuelle Welt überhaupt noch Vertrauen haben? Die Frage ist doch nicht, warum Cryptsy? Nein, die Frage sollte wohl ehr lauten, WHO IS NEXT?! Demnach wird der Cryptomarkt so schnell auch nicht für die Allgemeinheit interessant werden, denke ich, weil dort eben der Abzocke Tür und Tor geöffnet sind. Kryptografie hin oder her, die hart verdiente Kohle kann in der Cryptowelt der Bits und Bytes schneller weg sein, als einem lieb ist.

Zudem sind die ganzen Prozeduren noch viel zu kompliziert für Otto-Normalo. Da ist die Variante einer Crypto-Exchange noch die simpelste Form, seine Coins anzulegen. Aber erklärt mal einem Otto-Normalo, was der Unterschied zwischen Online-Wallet, Desktop-Wallet oder Papper-Wallet ist und wie diese Funktionieren und wie sein Geld dabei gesichert wird. Alles nur Nullen und Einsen im Nirvana der Kryptografie mit Hilfe des weltweiten Internets. Und vor allem, dass man dabei für jeden Coin extra eine neue Wallet installieren muss. Viele Otto-Normalos machen ja bis heute noch nicht mal Online-Banking, was ja eigentlich seit mehr als 15 Jahren keine Besonderheit mehr darstellt. Wie sollen die da mit Online-Wallets und Co zurecht kommen ?!

Technik muss simpel und einfach sein und eine gewisse Sicherheit bieten. Da ist aber der Cryptomarkt leider noch weit davon entfernt, denke ich. Das Runterladen der einzelnen Blockchains für jeden einzelnen Coin dauert ja schon eine halbe Ewigkeit von bis zu 12 Stunden und mehr. Erklärt das mal jemandem, der damit noch nie was zu tun hatte. Die meisten wollen schnell ne App runterladen und los legen. Und solange dies nicht der Fall ist, wird sich ein Otto-Normalo niemals auf das Labyrinth der Cryptowelt einlassen. Von einer Durchdringung bis in den Massenmarkt sind wird demnach noch sehr, sehr weit entfernt. Bisher ist der Cryptomarkt ehr eine Spielwiese für Neugierige, Risikofreudige oder Nerds.

Weitere Infos hierzu findet Ihr unter
https://bitcointalk.org/index.php?topic=1327445.0

In diesem Sinne viele nette Grüße :-)

Frank at www.coinking.de alias Mr.Dux alias Wiseman

Hier noch kurz einige Basics aus dem obigen Thread unter bitcointalk.org:

Um Coins einer Kryptowährung (Bitcoin, NXT oder was auch immer) überweisen zu können, benötigst du einen sogenannten privaten Schlüssel, also eine Art Passwort. Mit deinem Schlüssel kannst du auf die Coins auf deiner Adresse - die dem Schlüssel zugeordnet ist - zugreifen, sie gehören also Dir.

Die "Wallet" (Geldbörse) ist eine Datei, in der dieser Schlüssel gespeichert ist. (Eigentlich sind sogar mehrere gespeichert, aber das ist erst einmal egal). Bei Bitcoin und bitcoin-basierten Währungen heißt diese Datei "wallet.dat". Was oft falsch verstanden wird: In der Wallet sind keine Coins drin, sondern nur Schlüssel die zum Zugriff auf die Coins dienen. Die Coins selbst befinden sich in der verteilten Datenbank des Bitcoin-Netzwerks. Das dir bestimmte Coins gehören, bedeutet nichts anderes, als dass du den Schlüssel zum Zugriff auf sie besitzt.

Ein weiteres Missverständnis kann entstehen, da auch die Software, die zum Anlegen und Verwalten einer Wallet dient, manchmal auch "Wallet" genannt wird. Diese Software ist der sogenannte "Client". Also bei Bitcoin der "Bitcoin-Client", heute "Bitcoin Core" genannt. Diese Software hat in den allermeisten Fällen eine grafische Oberfläche, ist also auch für Laien gut bedienbar.

Bei NXT z.B. kann man den Client sogar über den Browser bedienen. Was aber etwas nervig sein kann: Wenn du viele Coins hast, brauchst du für jeden Coin einen Client, und diese nehmen nicht wenig Ressourcen (Speicherbelegung/ CPU/ Festplattenplatz) weg, wenn du sie parallel betreibst.

Eine Paperwallet ist nichts anderes als dass die Schlüssel auf Papier gedruckt werden. Dafür gibt es spezielle Software, die man aus Sicherheitsgründen auch offline bedienen kann.

Dann gibt es noch die Brainwallet. Hierbei handelt es sich um das Memorisieren des Schlüssels im Gedächtnis. Es gibt Software, die einen traditionellen aus Buchstaben und Zahlen bestehenden Schlüssel in einen leichter zu merkenden Satz umwandelt (der natürlich auch zur Sicherheit noch mal auf einem Zettel notiert werden kann). Bei NXT ist "Brainwallet" sogar die Standardvorgehensweise, bei Bitcoin ist es eher exotisch.

Sowohl bei Paperwallet als auch bei Brainwallet wird dir von der Software eine Deposit-Adresse generiert, wo du die Coins hintransferierst und sie sind dann mit dem gedruckten / memorisierten Schlüssel assoziiert. Um sie zu bewegen musst du die Software wieder aufrufen.

Die Onlinewallet dagegen ist in den allermeisten Fällen keine richtige Wallet, sondern eine Website, die Dir eine Art "Schuldschein" ausstellt, dass du bei ihr Coins geparkt hast. Also du hast keine Kontrolle drüber, wie schon gesagt wurde. Wie bei einem Exchange.

Es gibt dann noch die Hybridwallets wie coinb.in und blockchain.info, bei denen dir zwar ein Schlüssel ausgehändigt wird, aber die Website ebenfalls den Schlüssel speichert, was bedeutet, dass sie ebenfalls gehackt werden kann. Sie sind für kleine Beiträge OK, aber nicht für die BTC-Altersvorsorge.

Ob die Festplatte oder der USB-Stick abraucht, ist völlig irrelevant, denn die Blockchain kann man immer wieder runterladen, dazu brauchts nur irgendeinen PC mit Internet. Die "wallet.dat"-Datei ist, worin deine Schlüssel und damit dein Vermögen liegen. Die kannst du einfach sichern, wo immer du eine Datei unzugreifbar aufbewahren kannst und willst, und zwar solltest du sie immer sichern, wenn du eine neue Adresse in dein Adressbuch einträgst. Auch die Kopien der Wallet.dat Datei sind selbstverständlich identisch, daher kann jede Kopie dieses Backups später genutzt werden. Nach der Nutzung sollten natürlich wieder neue Backups angefertigt werden.

Wurden die Abzüge zu unterschiedlichen Zeiten gemacht, solltest Du immer die letzte Kopie nutzen. Die wallet.dat enthält (standardmäßig) 100 Schlüssel auf Vorrat. D.h. selbst mit einer älteren wallet.dat kann der aktuelle Stand wiederhergestellt werden, solange zwischen dem Zeitraum des Backup und dem Restore nicht allzu viele Transaktionen getätigt wurden.

Weitere Infos hierzu findet Ihr unter
https://bitcointalk.org/index.php?topic=1327445.0