Risiken bei Kryptowährungen

Immer wieder wird über Kryptowährungen berichtet. Dabei richtet sich die Aufmerksamkeit insbesondere auf die massiven Kursschwankungen. Darüber hinaus fällt auf, dass Kryptowährungen häufig von massiven Hackerangriffen betroffen waren. In diesem Artikel beleuchtet Curentis die Hintergründe. Bei Hackerangriffen auf Kryptowährungen geraten Krypto-Handelsplattformen ins Visier. Dabei ist bereits ein Schaden von mehr als eine Milliarde EURO entstanden. [1]

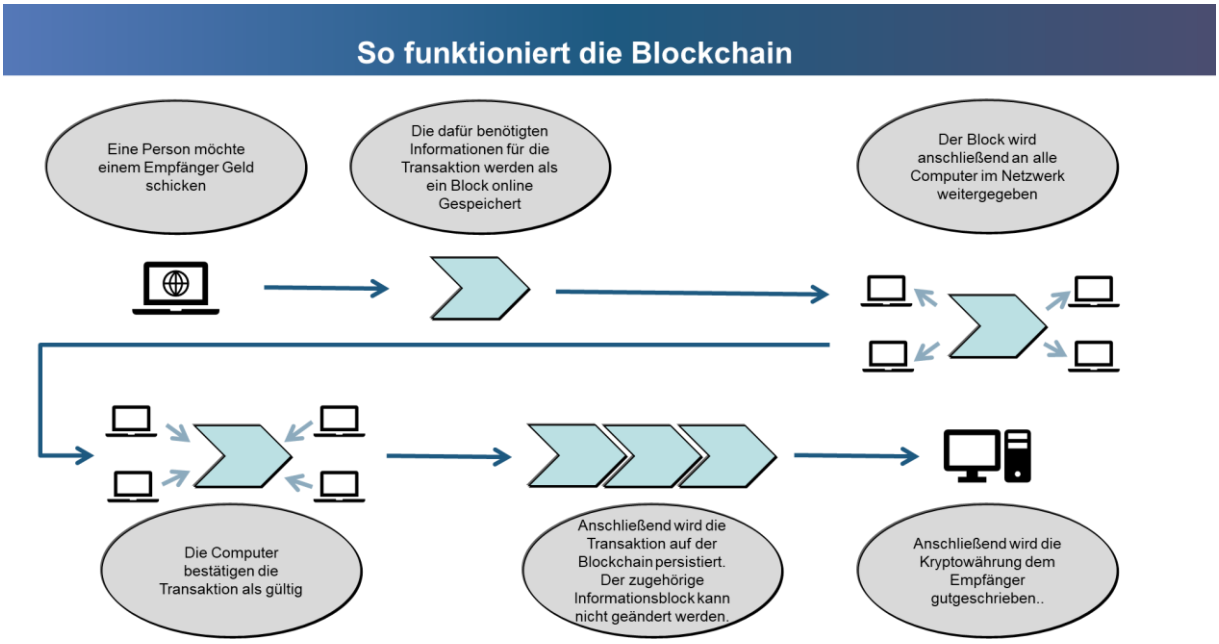
[1] (Siehe:https://www.wallstreet-online.de/nachricht/10922583-cyber-crimes-jahresbeginn-bitcoin-kryptos-wert-milliarde-dollar-gestohlen)

Grundsätzlich bauen Kryptowährungen auf einer sehr sicheren Technologie auf. Eine Transaktion auf dem Netzwerk kann nicht manipuliert werden, ohne vor Anfang der Transaktion Zugriff auf das Konto oder die Transaktionsdaten zu bekommen. Nicht die Verwundbarkeit der Transaktionen und der Konten der Kryptowährungen sind das Problem, sondern die Verwaltung der Konten durch Drittanbieter auf Krypto-Handelsplattformen. Diese sind nicht annähernd so reguliert und sicher wie die Datenbanken der Zentralbanken, welche die Kontostände der Geldeinlagen sicher, integer und vertraulich speichern. Trotzdem verwalten diese Krypto-Handelsplattformen erhebliche Summen, so dass sie eine attraktive Angriffsfläche für kriminelle Cyber-Aktivitäten darstellen.

Um die Sicherheit der intrinsischen Technologie von Kryptowährungen zu erklären und die Verwundbarkeit der Krypto-Handelsplattformen verständlich zu machen, beschreiben wir nachfolgend die technologischen Grundlagen – insbesondere der Blockchain-Technologie, auf der die Kryptowährungen basieren.

Wie funktioniert Blockchain?

Die Blockchain Technologie gleicht einer riesigen Datenbank. Diese Datenbank wird jedoch nicht an zentraler Stelle verwaltet, wie es bei Privateinlagen auf Bankkonten der Fall ist. Stattdessen wird die Datenbank von allen Teilnehmern aus dem Kryptowährungsnetzwerk gespeichert und verwaltet. Sogenannte Miner führen Transaktionen durch und validieren diese. Nur wenn genug Miner zugestimmt haben, kann eine Transaktion auf dem Netzwerk erfolgen. Als Gegenleistung erhalten Miner eine kleine Transaktionsgebühr, die vom Sender der Cyber-Coins bezahlt wird.



Der Kontostand jeder Person wird auf einem sogenannten Public Ledger dargestellt. Jeder Teilnehmer wird nur durch seinen „Public Key“ öffentlich identifiziert. Der Public Key erlaubt nur die Identifikation des Kontostandes oder kann als Zieladresse zum empfangen von Kryptowährungen dienen. Er erlaubt keinerlei Verfügungsmöglichkeit über die Cyber-Coins. Anders ist hingegen der „Private Key“. Durch den Private Key kann jemand Geld an eine beliebige Adresse verschicken. Er ermöglicht totale Kontrolle über den Kontostand. Verliert eine Person ihren Private Key, verliert sie damit ihr Konto. Erlangt ein Cyber-Krimineller Zugriff zum Private Key, kann dieser sofort alle Kryptowährungen des Opfers auf ein beliebiges Konto schicken.

Hackerangriff auf Mt. Gox

Der wohl bedeutsamste Hacker-Angriff auf Crypto-Währungen ist der Anfang 2014 vollendete Angriff auf die damals weltgrößte Bitcoin-Börse Mt.Gox. Circa 25.000 Kunden verloren hierbei insgesamt 650.000 Bitcoin. Zwischenzeitlich waren sogar 850.000 Bitcoin mit einer damaligen Marktkapitalisierung einer halben Milliarde USD verloren gegangen. Später wurden durch Zufall 200.000 der vermissten Bitcoins in einer elektronischen Geldbörse wiedergefunden.

Letztendlich musste die Plattform Mt. Gox Insolvenz anmelden und der damalige Chef Mark Karpeles wurde wegen Dokumentenfälschung zu einer Bewährungsstrafe

verurteilt. Schon vorher wurden der Cyberbörse Mt. Gox und ihrem Chef Mark Karpeles mangelnde Sicherheitsmaßnahmen und eine chaotische Geschäftsführung vorgeworfen.[2]

Mt. Gox hatte es versäumt ein valides IT-Sicherheit Management System einzuführen und zu verwalten.

Am 19.06.2011 gab es demnach einen Sicherheitsvorfall, bei dem ein Hacker Zugriffsdaten eines Mt. Gox Prüfers erlangt haben soll. Angeblich sei dies durch Diebstahl eines Mitarbeiters erfolgt, aber der genaue Vorgang, durch den die Zugriffsdaten erlangt wurden, bleibt bis heute unklar. Der Hacker konnte mit dem Zugang des Prüfers sehr viele Bitcoins an sich selbst schicken, und hat dies nach und nach weiter getan bis die Plattform 2014 den Sicherheitsvorfall bekannt gab und Insolvenz anmelden musste.

Weitere Hacking Angriffe

Nach dem Hackerangriff auf Mt. Gox gab es diverse andere Angriffe in denen auch größere Summen an Kryptowährungen der Kunden gestohlen wurden[3]:

- August 2016: Hier gab es beim Nachfolger von Mt. Gox, der Platform Bitfinex einen Hack, bei dem 73 Millionen USD verloren gingen.
- Dezember 2017: Cyber-Kriminelle ergaunern 63 Millionen USD in Crypto-Coins von NiceHash
- Januar 2018: Der größte Crypto-Hack aller Zeiten bei dem mehr als 500 Millionen USD Kryptowährungen von Coincheck gestohlen wurden
- Februar 2018: Hacker erbeuten 195 Millionen USD in Kryptowährungen von BitGrail
- Juni 2018: 40 Millionen USD wird von Cyber-Kriminellen aus der Plattform Coinrail entwendet
- Juni 2018: Durch einen Hack werden 30 Millionen USD in Kryptowährungen aus der Plattform Bithumb entwendet

[2] (Siehe: https://www.bloomberg.com/news/articles/2019-03-15/former-bitcoin-baron-mark-karpeles-gets-suspended-jail-term)

[3] (Siehe: https://hackernoon.com/a-huge-list-of-cryptocurrency-thefts-16d6bf246389 für eine detailliertere Liste)

Warum sind Krypto-Plattformen so anfällig für Hacker-Angriffe?

Kryptowährungen sind intrinsisch eine sehr sichere Technologie. Es ist nicht möglich eine Transaktion ohne weiteres zu manipulieren, da die Blockchain (die zuständige Datenbank, welche Transaktionen und Kontostände verwaltet) dezentral verwaltet wird. Um die Blockchain ganzheitlich zu ändern bedarf es der Zustimmung von c. 51% des Networks. Folglich müsste ein Hacker-Konglomerat die Kontrolle über 51% des Netzwerkes erlangen, um die Blockchain Transaktionen einer Kryptowährung zu kontrollieren. Dies ist bei normalen Kryptowährungen mit einer Marktkapitalisierung von vielen Millionen Euro bzw. sogar Milliarden wie es bei den bekannteren Cyber-Coins der Fall ist, faktisch unmöglich.

Anders sieht es jedoch bei „Smart Contracts“ aus. Diese werden in Kryptowährungen der zweiten Generation (wie z.B. Ethereum) verwendet. Smart Contracts sind zusätzlicher exekutierbarer Code, welcher auf der Blockchain neben der Transaktionshistorie und den Kontoständen mitgespeichert wird. Dieser erlaubt zusätzlich zu Transaktionen, Verträge oder Vereinbarungen auf einer Blockchain festzuhalten und kann theoretisch die Einsatzmöglichkeiten einer Kryptowährung

CURENTİS AG | Ralf Penndorf | Vorstand | In der Au 19, D-61440 Oberursel | T: +49.6171.8875.301 | F +49.6171.8875.488 | M: +49.170 8529289 | ralf.penndorf@curentis.com | www.curentis.com |

erweitern. Besonders bei Kryptowährungen wie Ethereum sind die Smart Contracts sehr machtvoll. Die Programmiersprache, welche bei Ethereum benutzt wird, nennt sich Solidity, und wurde konstruiert um „Turing Complete“ zu sein. Dies bedeutet, dass alle Möglichkeiten, welche das tragende System bietet, auch durch den Programm Code implementiert werden können. Es wird also eine unbegrenzte Art an Komplexität angeboten, und Hacker lieben komplexen Code, da dieser auf unabsehbare Weise zu missbrauchen ist. Jedoch ist hier zu vermerken, dass im Normalfall solche Hacker-Angriffe auf Smart Contracts, die damit verbundenen Ether gefährden, und nicht das Ethereum Netzwerk als Ganzes unsicher machen.

Die dritte und wirklich gefährlichste Methode der Cyber-Kriminalität sind Angriffe auf die Krypto-Handelsplattformen. Bei der Größe und der Vielzahl an Schwachstellen (unter anderem auch menschliche) im System einer solchen Plattform, ist es nur eine Frage der Zeit bis eine Schwachstelle erkannt und ausgenutzt wird. Darüber hinaus stellen Crypto-Handelsplattformen einen Single-Point-of-Failure dar, bei dem ein erheblicher Gewinn bei einem erfolgreichen Hack auf den Betrüger wartet. Als zentralisierte Web-Applikation sind Crypto-Handelsplattformen anfällig für dieselben Sicherheitslücken wie alle anderen Websites auch und müssten durch hohe IT-Security Standards den Cyber-Bedrohungen entgegenwirken. Bei den hohen Investitionskosten und dem stark umkämpften Markt entwickeln leider viele dieser Plattformen nur unzureichende Informationssicherheit Management Systeme und werden irgendwann Opfer eines Angriffs. Dies ist auch vor allem darauf zurückzuführen, dass die Anbieter von Krypto-Handelsplattformen zum Teil von ihrem eigenen Erfolg überfordert waren. Durch das zum Teil explosive Wachstum des Handelsvolumens von Kryptowährungen fehlte einigen Handelsplattformen die Erfahrung und Zeit, um rechtzeitig Ihre Plattformen sicherer zu machen und ein fachgerechtes Informationssicherheit Management System aufzubauen.

Fazit: Handelsplattformen sind für Cyber-Kriminelle in der Cryptowelt das attraktivste Angriffsziel für maximalen Profitgewinn und werden noch einige Zeit anfällig bleiben

Um für mehr Sicherheit in der Cryptowelt zu sorgen, sind normierte IT-Sicherheitsstandards unabdingbar. Nur die größten Exchanges wie Binance haben in

ausreichende Sicherheitsmaßnahmen investiert, um Ihre Reputation als wichtige Handelsplattformen beizubehalten. Bei kleineren Crypto-Handelsplattformen, die ausschließlich auf das Traden von Altcoins ausgelegt sind, gibt es zum Teil noch nicht einmal eine KYC Policy oder ein Überprüfungsverfahren von Konten. Folglich wird ein gehacktes Konto für immer Verloren sein. Hacking-Opfer haben keine ihre Cyber-Coins zurückzubekommen, da es nicht möglich ist nachzuvollziehen, wem die Kryptowährungen anfangs gehört haben.

Nur regulatorische Gesetze können solch mangelhaften Sicherheitsstandards vorbeugen. Ob und inwiefern diese erlassen werden, wird stark mit dem zukünftigen Erfolg der Kryptowährungen in der Gesellschaft zusammenhängen.

CURENTIS AG | Ralf Penndorf | Vorstand | In der Au 19, D-61440 Oberursel | T: +49.6171.8875.301 | F +49.6171.8875.488 | M: +49.170 8529289 | ralf.penndorf@curentis.com | www.curentis.com |