Kryptocoin Diebstähle

Jan Luca Pawlik
Betreuer: Marcel von Maltitz
WS2017/2018
Seminar Innovative Internet-Technologien und Mobilkommunikation
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: luca.pawlik@tum.de

KURZFASSUNG

Mit dem steigenden Wert und der steigenden Beliebtheit von Kryptowährungen steigen auch die Anreize für Hacker, Betrüger und andere Kriminelle, sich mit diesen zu beschäftigen. Um einen Überblick über die Gefahrenpotentiale der verschiedenen Diebstahlszenarien zu erhalten, ist eine Analyse von bisherigen Fällen bezüglich verschiedener Charakteristika interessant.
Dazu werden insgesamt 55 Diebstähle untersucht, die zwischen 2011 und 2017 stattfanden und zur Erstellung einer Taxonomie verwendet.

Schlüsselworte

Bitcoin, Ethereum, MtGox, ICO, Diebstahl, Betrug, Hack, Blockchain

1. EINLEITUNG

Die Vergangenheit hat gezeigt, es gibt eine Vielzahl von Angriffen auf die mittlerweile sehr heterogene Kryptocoinservice-Szene. Gerade wegen des aktuellen Hype um Bitcoins, Ether und andere Kryptowährungen und den teilweise überforderten Anbietern von Crpytocoinservices [21] bietet sich eine Untersuchung bereits erfolgter Diebstähle von Coins an.
Zweck dieses Papers ist es, einen Überblick über die verschiedenen Angriffe zu geben und eine Taxonomie dieser zu erstellen.
Dazu wird in Abschnitt 2 zunächst auf die grundlegenden Daten eingegangen und zusätzliche Fakten genannt.
In Abschnitt 3 wird aus untersuchten Vorfällen eine Taxonomie der Diebstähle erstellt.
Anschließend wird in Abschnitt 4 mit Hilfe dieser Taxonomie untersucht, wie sich die Angriffe entwickeln, das heißt, ob es aktuell oder in der Vergangenheit Trends gab oder immer wieder die gleichen Fehler gemacht wurden.
Aufgrund dieser Erkenntnisse werden dann in Abschnitt 5 grundlegende Verteidigungsstrategien vorgestellt.
In Abschnitt 6 wird die Auswirkung von Diebstählen auf die Verwendung auf Kryptowährungen diskutiert. In Abschnitt 7 wird ein Überblick über andere, verwandte Arbeiten gegeben.
Abschließend werden die Erkenntnisse des Papers in Abschnitt 8 noch einmal zusammengefasst dargestellt, die wichtigsten Erkenntnisse hervorgehoben und eine Einschätzung zur Zukunft im Bezug auf Kryptocoin Diebstähle gegeben.

2. DATEN

Die erfolgreichste Kryptowährung Bitcoin (BTC) existiert seit 2009 [4]. Erstmals gehandelt wird sie 2010. Der Preis für ein Bitcoin liegt in jenem Jahr bei maximal 0,30 USD [1]. Die ersten großen Bitcoindiebstähle finden 2011 statt.
Das Paper beschäftigt sich mit Fällen zwischen 2011 und 2017. Es werden für die Arbeit insgesamt 55 Diebstähle von verschiedenen Kryptotoken untersucht. Dabei werden nur Diebstähle an Services und nicht an Einzelpersonen betrachtet.
Der Gesamtwert der in den untersuchten Vorfällen gestohlenen Coins beträgt 1,4 Milliarden US-Dollar [1]. Den größten Anteil hat dabei der Hack der Coinhandelsplattform Coincheck. Bei diesem Hack wurden insgesamt 523 Millionen NEM mit einem damaligen Gegenwert von 523 Millionen US-Dollar gestohlen [20]. Zuvor war der Hack von MtGox, einer weiteren Coinbörse, mit Abstand der für die Angreifer ertragreichste. Im Fall MtGox wurden insgesamt wurden 650.000 Bitcoins mit damaligem Wert [2] von ca. 359 Millionen US-Dollar gestohlen [8].

2011	2012	2013	2014	2015	2016	2017	2018
7	8	12	4	4	5	13	2

Tabelle 1: Anzahl untersuchter Diebstähle pro Jahr

Der Großteil der untersuchten Vorfälle stammt aus den Jahren 2013 sowie 2017. Eine Übersicht über die Anzahl der Fälle pro Jahr ist in Tabelle 1 zu finden. Betrachtet wird hierbei jeweils das Datum der ersten vom Besitzer der Coins nicht autorisierten Überweisung. Dies ist insofern wichtig, da mehrere der Diebstähle jahresübergreifend stattfanden. Für Fälle vor 2014 wird [35] als Grundlage genutzt, da Aufgrund der mangelnden Interesse der Medien zu dieser Zeit wenige Quellen existieren. Die entnommenen Fälle und Quellen wurden zusätzlich geprüft.
Test

3. TAXONOMIE

Im folgenden Abschnitt werden die verschiedene Charakteristika anhand von Beispielen vorgestellt und definiert.

3.1 Art der Diebstähle

[1] Die gestohlenen Token werden jeweils mit dem zum Diebstahlzeitpunkt gültigen Kurs bewertet. Dazu werden aus den historischen Daten von `https://www.finanzen.net/devisen/bitcoin-dollar-kurs/historisch` der Abschlusskurs des jeweiligen Tages verwendet.
[2] Schlusskurs vom 24.2.2014: 552,85, erste offizielle Angabe des Verlustes

doi: 10.2313/NET-2018-03-1_06

Bei den verschiedenen Diebstählen kann zunächst zwischen unterschiedlichen Kategorien unterschieden werden, die wiederum eigene Unterarten aufweisen können. Die in den Vorfällen vorgekommenen Arten von Diebstählen werden im Folgenden vorgestellt, definiert und mit einem Beispiel erklärt.

3.1.1 Hacks

40 der 55 untersuchten Diebstähle wurden mithilfe von Hacking ausgeführt. Hacking bezeichnet hierbei das unerlaubte Eindringen in ein System bzw. das illegitime Nutzen eines Systems. Neben dem Fakt, dass Hacks die größte Gruppe der Diebstähle bilden, sind sie auch mit ca. 1,36 Milliarden US-Dollar für den größten Teil des gestohlenen Wertes verantwortlich. In 11 der Fälle wurde neben der Angabe, dass es einen Hack gab, keine weiteren Informationen veröffentlicht. Aufgrund der fehlenden Informationen wird oft auch ein Betrugsversuch vermutet, bei dem die Betreiber einen Hack nur vortäuschen, um so in den Besitz der von den Nutzern eingezahlten Kryptocoins zu kommen [3]. Dies trifft in 4 Fällen zu. Über diese Fälle sind nicht genug Informationen vorhanden um ein Urteil zu fällen.

Sicherheit des angegriffenen Services: Ein erstes Merkmal bei Hacking-Angriffen ist die Qualität der Sicherheitsmaßnahmen. Ein Beispiel für einen Fall, in dem keine Sicherheitsmaßnahmen genutzt wurden, ist der Hack von Sheepmarket. Sheepmarket war eine Darknet Drogenhandelsplattform. Laura Shin, Autorin beim Wirtschaftsmagazin Forbes, schreibt dazu in einem Artikel [24]: „There was no hacking. This was just a poorly created website that was just exploited by very young kids who immediately accepted responsibility for their actions “.

Professionalität der Angreifer: Ähnlich zur Sicherheit des Angegriffenen Services ist auch die Professionalität der Angreifer ein interessantes Merkmal von Diebstählen durch Hacking. Dabei wird ein Angreifer als professionell bezeichnet, wenn er gezielt und möglicherweise über längere Zeit einen Angriff auf einen Service durchführt und sich auch von technischen Hürden nicht aufhalten lässt, während ein nicht professioneller Angreifer einen zufällig im System gefundenen Fehler ausnutzt und/oder über kein großes technisches Wissen verfügt.
Ein Beispiel für einen besonders professionell durchgeführten Angriff ist der Fall Bitstamp [32], bei dem über längere Zeit mithilfe von Social Engineering, Spear Phishing und in ein Word Dokument eingebetteter Schadsoftware Zugriff auf die Server erlangt werden konnte.

3.1.2 Betrug

Von den 55 Fällen handelt es sich bei 13 um Diebstähle durch Betrug. Im Folgenden werden verschiedene Arten von Betrug im Zusammenhang mit Kryptowährungen erläutert.

Ponzi-Schema: Bei einem Ponzi-Schema wird mit hohen Renditen zum investieren angeregt. Die hohen Renditen werden dabei über neue Investoren gedeckt. Wenn der Zustrom der Investoren abbricht, werden zunächst meist technische Probleme vorgetäuscht, bis irgendwann die Seite, auf der investiert werden kann, verschwindet [2]. Ein Beispiel von vielen hierfür ist die Website Richmond Berks, die 1,4% Rendite pro Tag anbot, bevor sie verschwand [9]. Auch wenn in den hier untersuchten Fällen die Zahl dieser Betrugsfälle gering ist, ist diese insgesamt nicht zu unterschätzen. Eine Liste von Betrug im Zusammenhang mit Bitcoin lässt sich unter `http://www.badbitcoin.org/thebadlist/` finden. Oft werden Ponzi-Schemas von Betrügern als sogenannte High Yield Incestmens Plans (HYIP) angeboten [17]. Sie versprechen sehr hohe Renditen (mehrere Prozent pro Tag), wobei sie durch den Fachbegriff Vertrauen erzeugen wollen. HYIPs gibt es nicht nur im Bereich der Kryptowährungen. Sie sind allgemein ein beliebtes Betrugswerkzeug.

Exit Scam: Ein Exitscam bezeichnet einen Betrug, bei dem die Betreiber eines Services diesen abschaltet und dabei die Guthaben der Nutzer nicht auszahlt. Dies ist häufig bei illegalen Drogenmarktplätzen im Darknet der Fall. Der Service muss allerdings nicht immer illegal sein. Ein Beispiel hierfür ist die chinesische Bitcoinbörse GBL, die mit den bei ihr hinterlegten Bitcoins im Wert von 4,1 Millionen US-Dollar verschwand [23].

Fake Coin: Bei einem Fake-Coin-Betrug werden Schein-Kryptowährungen an Anleger verkauft. Ein Beispiel dafür ist die angebliche Währung E-Coin, mit der Betrüger sich insgesamt über 4 Millionen Schweizer Franken[4] aneignen konnten [30].

Phishing/Fake Apps: Beispielhaft für den Punkt Phishing/Fake Apps steht der aktuelle Fall Iotaseed (2018) [22]. Iotaseed war eine Applikation die es Nutzern der Cryptowährung IOTA ermöglichte sogenannte Seeds zu generieren. Diese Seeds lassen sich dabei mit einem Privatekey, der z.B. bei Bitcoin verwendet wird, vergleichen. Ne Der Service speicherte diese Seeds allerdings um später die mit den Seeds verwalteten IOTA Token zu stehlen.

3.2 Täter

Weiter soll bei den verschiedenen Diebstählen nach der Art des Täters unterschieden werden. Diese verschiedenen Täterprofile werden im folgenden definiert und erläutert.

3.2.1 Hacker

Ein Großteil der Täter lässt sich als Hacker beschreiben. Dabei bezeichnet der Begriff Hacker, analog zum Begriff Hack in Unterunterabschnitt 3.1.1, Angreifer die unerlaubt in ein System eindringen oder es auf illegitime Weise nutzten. Durch die große Anzahl ist eine weitere Differenzierung interessant, aber aufgrund von wenig Informationen nicht immer unproblematisch.

Professionelle (nichtstaatliche) Hacker (Black Hats): Als professionelle Hacker werden Hacker eingeordnet, die wie im Fall Bitstamp gezielt und mit technisch versierten Mitteln Angriffe ausführen. Zum Fall Bitstamp ist dabei ein interner Bericht geleakt worden, der interessante Einblicke in einen solchen Angriff gibt [32].

Staatliche Hacker: Es gibt noch keinen Fall in dem bewiesen wurde, dass staatliche Hacker für einen Diebstahl

[3] Solange es allerdings keine Beweise dafür gibt werden die Vorfälle als Hack bewertet.

[4] ca. 4 Millionen US-Dollar

doi: 10.2313/NET-2018-03-1_06

verantwortlich waren. Im Fall Bitthumb, der größten Südkoreanischen Coinbörse, wird jedoch von den Behörden ein Angriff von Nordkorea bzw. nordkoreanischen Hackern vermutet [12]. Als staatliche Hacker sind Hacker, die ihre Fähigkeiten für einen Staat einsetzen. Sie müssen dabei jedoch nicht offiziell für den Staat arbeiten, sondern können auch nur geduldet sein.

White Hat Hacker: White Hat Hacker versuchen durch ihre Fähigkeiten Sicherheitslücken zu entdecken, bevor sie von kriminellen Hackern ausgenutzt werden können. Beispiel hierfür ist dabei der Hack des DAO Projektes[5]. Das DAO Projekt war der Versuch über Ethereum Smart Contracts eine dezentralisierte autonome Organisation zu erschaffen. Problematisch war allerdings, dass die Funktion, die es Investoren erlaubte, ihre Investition aus the DAO zu entziehen, einen Fehler hatte. Dem Angreifer war es durch diesen Fehler möglich, die Auszahlungsfunktion innerhalb der Funktion erneut aufzurufen und somit die Überprüfung der Legitimität der Auszahlung zu umgehen [28]. Allerdings konnten White Hat Hacker, nachdem die Sicherheitslücke bekannt wurde rechtzeitig die in das DAO Projekt eingezahlte Token sichern [26].

3.2.2 Betrüger

Analog zu Unterunterabschnitt 3.1.2 gibt es die Täterkategorie Betrüger. Große Unterscheidungen gibt es bei diesem Typ nicht. Möglicherweise kann man in Zukunft Wiederholungstäter identifizieren.

3.2.3 Mitarbeiter

Die Täterkategorie Mitarbeiter wird im Fall Shapeshift sinnvoll. In diesem verkaufte ein Mitarbeiter Informationen und Zugangsdaten an eine Person, die daraufhin mehrmals in das System von Shapeshift einbrach [31]. Genauere Informationen zu diesem Vorgang enthält eine auf Wunsch von Shapeshift veröffentlichte Analyse [6].

3.3 Opfer der Diebstähle

Die Kategorie Opfer der Diebstähle beschäftigt sich mit der Frage wer letztendlich den Schaden trägt.

3.3.1 Service(-betreiber):

Bei seriösen Services wird oft versucht, den Schaden der Nutzer zu übernehmen. Allerdings kann es dabei dazu kommen, dass dies über einen längeren Zeitraum geschieht, wenn die gehackten Services nicht genügend Reserven haben. Ein Modell für eine solche Lösung wäre die Ausgabe eines neuen Token, der nach und nach von der Börse wieder aufgekauft wird.

Coinbörsen: Coinbörsen sind in den untersuchten Fällen am häufigsten (insgesamt 21 mal) das Opfer von Diebstählen geworden. Coinbörsen sind Handelsplätze für Kryptowährungen, ähnlich wie eine Börse.

Miningpools: Im Zusammenhang mit Kryptowährungen ist auch das sogenannte minen (deutsch. Abbauen) zu nennen. Um eine Transaktion in einer Blockchain zu übernehmen muss meist eine aufwendige Berechnung ausgeführt werden [7], deren Ergebnis wiederum einfach zu überprüfen ist. Der Versuch, diese Aufgabe zu lösen, wird mining genannt. Derjenige, der die Lösung als erstes berechnet, erhält dafür eine Belohnung in der jeweiligen Währung der Blockchain. Detaillierter erklärt wird dies unter anderem in einem Artikel auf BTC Echo[13].
Miningpools sind Zusammenschlüsse mehrerer Personen bzw. Hardwaresysteme. Durch den Zusammenschluss wird eine größere Rechenleistung und damit eine höhere Wahrscheinlichkeit, eines dieser Probleme zu lösen, erreicht. Die Belohnung wird dabei gerecht anhand der eingebrachten Rechenleistung verteilt. Dazu werden allerdings die geminten Token in einem zentralen Wallet zwischengespeichert. Oft wird auch erst auf Wunsch ausgezahlt. Somit ist dieses Wallet ein lohnendes Ziel für Angreifer.
Von den untersuchten Fällen waren 4 Angriffe auf Miningpools.

Webwallets: Webwallets sind Serviceanbieter die Nutzern ermöglichen mit den verschiedenen Blockchains zu interagieren, ohne selbst eine Software dafür installieren zu müssen. Dabei ist darauf zu achten, wie der private Schlüssel des Wallets gesichert wird. Allgemein ist zu bedenken, dass ein solcher Anbieter ein deutlich lukrativeres Ziel für Hacker ist als ein einzelnes lokales Wallet.

Startups: Der innovative Charakter der Blockchain begünstigt die Gründung von Startups. Kryptocoinbezogene Startups versuchen sich dabei meist über ein sogennantes Initial Coin Offering, wie unter Unterunterabschnitt 3.4.3 beschrieben, zu finanzieren.

Darknet Markt: Der Begriff Darknet bezeichnet ein Netzwerk, das innerhalb des Internets existiert, aber zusätzliche Programme mit zusätzlichen Protokollen benötigt, um darauf zuzugreifen. Dabei wird durch diese versucht, die Identität der Kommunikationspartner geheimzuhalten. Aus diesem Grund wird das Darknet auch oft verwendet, um illegalen Aktivitäten wie dem Handel mit Drogen nachzugehen. Dies geschieht dafür auf eigens geschaffenen Plattformen. Diese Anonymität führt allerdings oft auch zu Betrugsfällen. Des weiteren ist das Sicherheitsniveau dieser Seiten oft nicht so hoch wie das von legalen Handelsplätzen außerhalb des Darknets. Ein Beispiel für einen unsicheren gehackten Darknethandelsplatz ist Sheepmarket [24].

Lokale Clients: Ein Blockchainclient, oft fälschlicherweise Wallet genannt, ist ein Programm, das dabei hilft, Kryptowährungen zu verwalten und mit der dazugehörigen Blockchain zu interagieren. Da diese dadurch auch mit dem Internet verbunden sind, können auch sie Ziel eines Angriffs sein. Als Beispiel dient hier der Ethereum-Client *Parity*. Dieser hatte einen Fehler in der Implementierung von sogenannten Multisignature Wallets. Ein Multisignature Wallet kann man sich als ein Konto vorstellen, das bei Überweisungen die Autorisierung durch die Mehrheit der Besitzer erfordert. Durch einen Bug in der Implementierung konnte die Besitzerliste eines solchen Wallets überschrieben und somit die darin enthaltenen Token gestohlen werden [34].

[5] DAO steht für dezentrale autonome Organisation

[6] `https://de.scribd.com/doc/309591980/ShapeShift-Postmortem`

[7] Oft wird mit einer Berechnung gleich ein ganzer Block validiert

doi: 10.2313/NET-2018-03-1_06

Shopping: Durch die extremen Schwankungen der Preise von Kryptowährungen sind Händler, die solche akzeptieren, selten. Sollte sich jedoch eine Kryptowährung als Zahlungsmittel etablieren, könnte diese Kategorie häufiger vertreten sein.
Unter den untersuchten Fällen befindet sich mit Purse.io allerdings nur ein Anbieter, der Einkäufe bei Amazon mit Bitcoin ermöglichen will.

3.3.2 Kunden/Nutzer:
Vor allem zu Beginn der Kryptowährungsära (2011-2013) trugen letztendlich die Nutzer den Schaden davon.

3.3.3 Investoren:
Durch die teils extremen Wertsteigerungen von verschiedenen Kryptowährungen sind Kryptowährungen mittlerweile auch für Investoren interessant. Diese können allerdings nicht nur durch die extremen Kursschwankungen Verluste machen, sondern auch durch Betrug oder den Hack eines von ihnen unterstützten Startups.

3.4 Angriffziel/Angriffsfläche
Im folgenden wird aufgearbeitet, über welche Angriffsflächen Services angegriffen werden.

3.4.1 Server/Software
Die Server eines Services bzw. Software, die im Zusammenhang mit Kryptocoins verwendet wird, sind eine klassische Angriffsfläche. Dabei deckt diese Kategorie sowohl die Software der Services als auch die der Blockchain und darauf basierender Technologien ab.

Smart Contract Ein Smart Contract ist Code, der in einer Blockchain ausgeführt wird wenn gewisse Bedingungen eintreten [6]. Dadurch lassen sich unter anderem Multisignaturwallets, Verträge oder sogar ganze Organisationen realisieren. Trotz allem sind Smart Contracts Code, so dass es möglich ist Fehler in diesem auszunutzen. Das bedeutet im Zusammenhang mit Blockchains und Kryptowährungen, dass diese Fehler direkt zu einem finanziellen Schaden führen können. Beispiele für Angriffe auf Smart Contracts sind das Multisignaturewallet des Ethereumclients *Parity* [34] oder das DAO Projekt, dass bereits in Unterunterabschnitt 3.2.1 angesprochen wurde.

Coinprotokoll Beim Zieltyp Coinprotokoll geht es um Angriffe auf die Protokolle der verschiedenen Blockchains, wie der theoretisch mögliche 51% Angriff [25], der allerdings ein allgemeines Problem von konsensbasierten P2P Netzwerken ist. Bisher kam es ein einziges Mal zu einem Problem mit dem Protokoll von Bitcoin. 2010 wurden durch einen "value overflow"knapp 185 Milliarden Bitcoins erzeugt. Die Anzahl der Bitcoins ist eigentlich auf 21 Millionen begrenzt. Durch einen „soft-fork“ konnte die Erzeugung der neuen Bitcoins annulliert werden [3].

3.4.2 Webpräsenz/Social Media
Der Punkt Webpräsenz überschneidet sich auf den ersten Blick mit dem vorhergegangenen Punkt Server/Software. Webpräsenz/Social Media bezieht sich allerdings nicht darauf, diese über Sicherheitslücken anzugreifen, sondern durch die Übernahme dieser, falsche Informationen an die Nutzer/Investoren weiterzugeben. Zu beobachten war diese Angriffsfläche meist im Zusammenhang mit Startups.

3.4.3 Initial Coin Offerings
Initial Coin Offerings (ICOs) sind eine Art des Crowdfundings von Kryptowährungsstartups. Dabei erhalten Investoren gegen herkömmliche oder kryptobasierte Währung Token des neuen Unternehmens. Dabei ist das Initial Coin Offering die erste Möglichkeit an diese Token zu kommen. ICOs sind ein relativ neues Modell. Dies sieht man auch daran, dass die vier Angriffe auf ICOs alle im Jahr 2017 stattfanden. Die Angriffe auf ICOs stehen oft im engen Zusammenhang mit Attacken auf die Webpräsenz oder die Social Media Kanäle des Startups, wie die Beispiele CoinDash [7] und Enigma.co [18] zeigen.

3.4.4 Mitarbeiter
Neben Angriffen auf Software sind Angriffe über die Mitarbeiter eines Unternehmens ein möglicher Weg für Angreifer. Ein Szenario dabei ist ein Angriff über Spear Phishing, wie unter Unterabschnitt 3.5 beschrieben, bei dem die Mitarbeiter dazu gebracht werden sollen, dem Angreifer unwissend Zugang zu den Systemen zu ermöglichen. Allerdings können die Mitarbeiter nicht nur das Angriffsziel sein, sondern auch die Täter wie der Fall Shapeshift zeigt [31].

3.4.5 Webhoster
Mit Linode wurde auch ein Webhoster im Zusammenhang mit Kryptowährungen angegriffen [15]. Auf Linode wurden die Wallets mehrerer Coinbörsen gehostet, die über diesen Weg gelehrt werden konnten. Allgemein ist der Hack des Webhosters nicht nur für Coinbörsen gefährlich sondern für jeden Service der keine eigenen Server verwendet.

3.5 Angriffsmethode
Neben der Angriffsfläche ist auch die genutzte Angriffsmethode interessant. Dabei hängen manche Angriffsflächen und Methoden, wie Software und Exploits, eng zusammen. Im Folgenden werden verschiedene, in den Fällen vorgekommenen Angriffsmethoden vorgestellt.

Exploits: Der Begriff Exploit bezeichnet Code, der gezielt Schwachstellen in anderem, fremden Code ausnutzt, um in diesem eigenen Code auszuführen oder ein ungewünschtes Verhalten herbeizuführen. Beispielhaft das Überweisen von Kryptowährung ohne das Wissen oder die Autorisierung des Besitzers. Ein Fall in dem ein, wenn auch relativ einfacher, Exploit genutzt ist ist der Hack von Sheepmarket [24].

Spearphishing: Bei Spearphishing handelt es sich um einen gezielten Angriff auf einige wenige Personen. Dabei werden auf die Interessen der Personen abgestimmte Nachrichten verfasst, die sie letztendlich zum ausführen von Code oder der Herausgabe von Informationen bringen soll. Ein solcher Angriff kann sich auch über eine längere Zeit ziehen. Beispielhaft dazu ist der Hack der Coinbörse Bitstamp zu nennen [32].

Defacing von Webseiten Das Defacing von Webseiten beschreibt einen Angriff bei dem zunächst Zugriff auf den Webserver des anzugreifenden Unternehmens erlangt wird. Im allge-

meinen werden dann Informationen auf der Seite geändert. Im Bezug auf Kryptowährungen werden dann vor allem Informationen wie Adressen für Spenden oder Investitionen geändert. Ein mögliches Fallbeispiel ist der Hack des Initial Coin Offerings CoinDash. Dort wurde die Adresse, an die Investoren Ethereum senden sollten, geändert. Die Angreifer bekamen damit Ether im damaligen Gesamtwert von 7,6 Millionen US-Dollar von den Investoren überwiesen [7].

Spam/Allgemeines Phishing: Im Gegensatz zu Spearphishing zielt allgemeines Phishing auf die breite Masse ab. Dazu können im Idealfall (aus Sicht der Angreifer) gehackte Social Media Accounts und E-Mail Adressen verwendet werden. Ein Beispiel hierfür ist der Angriff auf das ICO Enigma.co [18].

Inside Job: Als Inside Job wird ein Angriff genannt, der von Innen durch einen Mitarbeiter oder mit Hilfe eines Mitarbeiters durchgeführt wird. Im Fall Shapeshift wurde angestoßen durch einen Mitarbeiter insgesamt drei mal das Hot Wallet gelehrt und letztendlich Coins im Wert von 230.000 US-Dollar entwendet [33].

3.6 Art der Coins

Unterschieden werden kann auch zwischen den verschiedenen Arten von Coins die gestohlen wurden.

Bitcoin (BTC): Bitcoin ist die erste Kryptowährung und existiert seit 2009. Zuerst gehandelt wurde Bitcoin im Jahre 2010 [10]. Aufgrund des großen Wertes ist Bitcoin im Vergleich zu anderen Kryptowährungen am häufigsten Ziel von Diebstählen. Das belegt auch, dass in 42 der untersuchten Fällen Bitcoins gestohlen wurden. In zwei davon wurden neben Bitcoin auch anderen Kryptowährungen gestohlen, dennoch machte Bitcoin den größten Anteil aus.

Ether (ETH): In 10 der untersuchten Fälle wurde Ether (ETH) gestohlen. Ether ist der Token, der im Ethereumnetzwerk genutzt wird. Vorteil von Ethereum ist, dass es im Gegensatz zu Bitcoin nicht nur als Währung genutzt werden kann. Vielmehr bietet Ethereum die Möglichkeit sogenannter Smart Contracts. Ein Smart Contract ist Code der im Ethereumnetzwerk ausgeführt wird [6]. Ether besitzt, nach Bitcoin, die zweitgrößte Marktkapitalisierung [14].

Sonstige: Neben Bitcoin und Ether gibt es noch weitere Coins, wie z.B. Dash, Litecoin, Monero oder Tether. Dabei ist zu beachten, dass manche Blockchains bzw. Coins voneinander abstammen. Dies kann dadurch geschehen, dass sich die Blockchain aufgrund von Differenzen in der jeweiligen Community aufspaltet[8]. Beispiele dafür wären Ethereum und Ethereum Classic sowie Bitcoin und Bitcoin Cash. Eine andere Möglichkeit ist, dass eine neue Blockchain aufbauend auf dem Code einer bereits existierenden Blockchain geschaffen wird.

3.7 Schadenshöhe und Auswirkung

Insgesamt wurden über 1,4 Milliarden US-Dollar in den untersuchten Fällen gestohlen. 1,36 Milliarden US-Dollar davon durch Hacking, 6 Millionen US-Dollar durch Betrug.

[8]Der Fachbegriff für ein solches aufspalten ist Fork

Verwendet man den heutigen Kurs[9] zu Berechnung des Wertes, wurden insgesamt mindestens 22 Milliarden US-Dollar in Bitcoins (1259185 BTC) gestohlen.
Der finanzielle Rahmen spannt sich dabei für Hacks von 15.534 US-Dollar, im Falle des Hacks des Glückspielanbieters betco.in, bis zu um die 534 Millionen US-Dollar im Fall Coincheck. Im Bezug auf Betrug wurden in den untersuchten Fällen, in denen Angaben zur Höhe gemacht wurden, zwischen 6461 US-Dollar und 4,3 Millionen US-Dollar gestohlen. Bei Betrugsfällen ist die Datenlage jedoch schwieriger, so dass oft gar keine Informationen über die Menge an gestohlenen Coins bzw. Geld verfügbar ist.
Den Großteil des gestohlenen Geldes macht das Geld aus Coinbörsen aus (1,1 Milliarden US-Dollar).
Der Hack der Coinbörse Cointrader macht dabei mit 33.600 US-Dollar den kleinsten Anteil aus.

Die fünf Diebstähle mit dem größten gestohlenen Wert sind:

1. Coincheck, 534 Millionen US-Dollar, Coinbörse, gehackt
2. MtGox, 359 Millionen US-Dollar, Coinbörse, gehackt
3. Bitthumb, 82 Millionen US-Dollar, Coinbörse, gehackt
4. Bitfinex, 71 Millionen US-Dollar, Coinbörse, gehackt
5. DAO, 62 Millionen US-Dollar, Smart-Contract im Ethereum Netzwerk, gehackt

4. (ZEITLICHE) KORRELATION DER CHARAKTERISTIKA

Kryptowährungen existieren seit 8 Jahren. Im folgenden wird deshalb untersucht, wie sich Angriffe seitdem verändert haben.

Die ersten Angriffe 2011 waren meist geringer Sicherheit geschuldet. Während es bei Angriffen auf MtGox (2011) und Sheepmarket (2013) nach Angaben noch (fast) keine Sicherheitsmaßnahmen gab [24], die umgangen werden mussten, werden heute für Angriffe deutlich besser Fähigkeiten benötigt. Die gestiegenen Kurse haben jedoch dazu geführt, dass Hacker mit entsprechenden Fähigkeiten mittlerweile Kryptowährungen als lohnendes Ziel ansehen.

Im Bezug auf den gestohlenen Gegenwert hat sich jedoch keine Entwicklung gegeben. Das heißt es gibt immer noch Fälle in denen sehr große Beträge im Millionenbereich gestohlen werden. Dies hängt aber wiederum mit den extrem gestiegenen Wechselkursen zusammen.

Coinbörsen sind das klassische Angriffsziel. In allen Jahren von 2011 bis 2017 gab es mindestens einen Hack einfacher Coinbörse. Im Allgemeinen lässt sich trotzdem ein Anstieg der Sicherheitsvorkehrungen nachvollziehen. So wird mittlerweile von nahezu allen Coinbörsen
2-Faktor-Authentifizierung unterstüzt und die Mittel in Hot und Cold Wallets aufgeteilt.

Mit dem Aufkommen von Initial Coin Offerings im Jahr 2017 hat es auch verstärkt Angriffe auf diese gegeben. Dabei

[9]Kurs am 20.12.2017 um 12:50 : 17321,97 US-Dollar pro Bitcoin

lässt sich feststellen, dass häufig die offiziellen, öffentlichen Kanäle der Startups von Angreifern übernommen werden. Die Überprüfung, ob eine Blockchainadresse wirklich einem Startup, Service oder Endanwender gehört, könnte in Zukunft ein interessantes Problem werden, da es für Statups und Services aus Sicherheitsgründen sehr wichtig ist, wohingegen einige Nutzer möglicherweise Kryptowährungen auch wegen der teilweise gegebenen Anonymität nutzten und diese bewahren wollen.

Gesteigert haben sich vor allem die Anzahl der Betrugsfälle im Bezug auf Kryptowährungen. Dies lässt sich darauf zurückführen, dass zum einen der Preis von Kryptowährungen mittlerweile sehr hoch ist und zum anderen immer mehr Personen Kryptowährungen verwenden, die wenig Wissen über Technologie und Gefahren besitzen. Die meisten Betrugsfälle lassen sich bis auf den Umstand, dass sie den aktuellen Hype um Kryptowährungen ausnutzen, nicht von Betrugsmethoden in anderen Bereichen unterscheiden. Sie sind also im Gegensatz zur innovativen Technologie Blockchain konservativ.

In Zukunft ist vor allem abzuwarten, welche neuen Dienste welche neuen Angriffsflächen bieten. Dabei könnten neben klassischen Services wie zum Beispiel Shopping oder Glücksspielwebseiten auch innovativere Dienste mit völlig neuen Schwachstellen auftreten.

5. VERTEIDIGUNGSSTRATEGIEN

Im Folgeden sollen grundlegende Verteidigungsstrategien für die verschiedenen Opfertypen gegeben und auf weiterführendes Material verwiesen werden.

5.1 ... für Nutzer

Kryptowährungen sind ein Zahlungsmittel. Deshalb sollten sie auch wie herkömmliche Zahlungsmittel behandelt werden. Das bedeutet, dass Nutzer im übertragenen Sinne nicht ihr ganzes Geld bei sich haben sollten. Auf Kryptowährungen übertragen bedeutet das, dass es sinnvoll ist zwischen einem sogenannte Hot-Wallet und einem Cold-Wallet zu unterscheiden. Ein Hot-Wallet wird dabei im Alltag genutzt und sollte nicht mehr Coins enthalten als benötigt. Ein Cold-Wallet wiederum wird offline auf einer Festplatte oder einem nicht mit dem Internet verbundenen Rechner gespeichert. Es besteht auch die Möglichkeit eines sogenannten Paperwallets. Bei diesem werden Public- und Privatekey in einem maschinenlesbaren Format auf ein Stück Papier gedruckt. Auch wichtig ist es Backups des Wallets zu machen. Ohne den dazugehörigen Privatekey gibt es keine Möglichkeit über die eigenen Kryptotoken zu verfügen. Immer zu bedenken ist, dass Überweisungen in den verschiedenen Blockchainnetzwerken nicht rückgängig gemacht werden können.

5.2 ... für Servicebetreiber

Servicebetreiber sollten sich bewusst sein, dass sie oft einen bankenähnlichen Status einnehmen und somit Verantwortung für die Sicherheit der eingezahlten Coins haben. Wie für den einzelnen Nutzer ist auch Services die Nutzung von Hot- und Cold-Wallets zu empfehlen. Zusätzlich können auch Hardware-Sicherheitsmodule eingesetzt werden. Wie ein Einsatz eines solchen Moduls aussehen könnte wurde unter anderem unter [11] diskutiert. Es sollte darauf geachtet werden, dass Mitarbeiter starke Passwörter, die regelmäßig geändert werden, und 2-Faktor-Autorisierung verwenden. Negativbeispiel ist hierbei das ICO Startup Enigma, dessen CEO ein Passwort verwendete, dass, zusammen mit seiner E-Mail Adresse, bereits in der Vergangenheit durch den Hack von anderen Services geleakt wurde [18].

5.3 ... für Investoren

Kryptowährungen werden mittlerweile oft als Investition gesehen. Dabei ist zu bedenken, das die meisten Kryptowährungen extremen Wertschwankungen unterliegen. Von Investitionen die hohe Renditen ohne Risiko versprechen (HYIPs) sollte Abstand gehalten werden. Wchtig ist auch, sich ausreichend über die verschiedenen Währungen und Technologien zu informieren.

6. AUSWIRKUNGEN AUF DIE VERWENDUNG VON KRYPTOWÄHRUNGEN

Nach großen Hacks wurde immer wieder ein Ende der Kryptowährungen vorausgesagt [19]. Zwar gab es nach größeren Angriffen immer wieder Kurseinbrüche. Die Kurse der verschiedenen Kryptowährungen konnten sich bisher aber immer erholen.

Besonders hervorzuheben ist auch, dass es, bis auf die durch einen Value Overflow erzeugten zusätzlichen Bitcoins (siehe Unterunterabschnitt 3.4.1), keine Verluste\Diebstähle durch Fehler in den verschiedenen Blockchains gab. Weitaus kritischer für den Erfolg von Blockchain-basierten Währungen könnte andere Faktoren sein. Ein Punkt ist zum Beispiel Probleme wie der sehr hohe Stromverbrauch von Bitcoin[29].

7. VERWANDTE ARBEITEN

Neben dem allgemeinen Hype um Kryptowährungen wie Bitcoin sind diese und die dazugehörigen Technologien auch in der Informatik ein sehr aktuelles Thema. Das Paper Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk [27] untersuchte 40 verschiedene Coinbörsen. Dabei lag der Fokus auf der statistischen Auswertung. Unter anderem wurde untersucht, bei welchen Eigenschaften von Coinbörsen die Wahrscheinlichkeit der Schließung am höchsten ist. Ein anderes Paper [5] beschäftigt sich mit den Gefahren einer blockchainbasierten Währung, vor allem im Bezug auf kriminelle Machenschaften wie Geldwäsche und Darknet Drogenmarktplätze. Eine weitere Arbeit [16] beschäftigen sich mit der möglichen Bedrohung herkömmlicher Währungen und Finanzinstituten durch Bitcoin und inwiefern eine Regulierung notwendig ist.

8. ZUSAMMENFASSUNG

In diesem Paper wurden anhand verschiedener Diebstähle von Kryptowährungen Charakteristika solcher herausgearbeitet. Dazu wurden zunächst grundlegende Daten dargestellt. Anschließend wurden die verschiedenen Teile der Taxonomie definiert und mit Hilfe von Beispielen erläutert. Es wurde auf die Entwicklung der Charakteristika eingegangen, einige Verteidigungsstrategien angesprochen. Abschließend wurde Zusammengefasst, welche Auswirkungen die Diebstähle auf die verschiedenen Kryptowährungen hatten.

9. LITERATUR

[1] Bitcoin Price History. https://99bitcoins.com/price-chart-history/. Zuletzt aufgerufen am 14.12.2017.

[2] Ponzi Scheme. https://www.investor.gov/protect-your-investments/fraud/types-fraud/ponzi-scheme. Zuletzt aufgerufen am 24.01.2018.

[3] . Value overflow incident. https://en.bitcoin.it/wiki/Value_overflow_incident, 2014. Zuletzt aufgerufen am 20.12.2017.

[4] Genesis block. https://en.bitcoin.it/wiki/Genesis_block, 3.2.2009. Zuletzt aufgerufen am 15.12.2017.

[5] S. T. Ali, D. Clarke, and P. McCorry. *Bitcoin: Perils of an Unregulated Global P2P Currency*, pages 283–293. Springer International Publishing, Cham, 2015.

[6] Alyssa Hertig. How Do Ethereum Smart Contracts Work? https://www.coindesk.com/information/ethereum-smart-contracts-work/. Zuletzt aufgerufen am 19.12.2017.

[7] Axel Kannenberg. Coindash: Kryptogeld-Crowdfunding mit Adressänderung gekapert. https://www.heise.de/newsticker/meldung/Coindash-Kryptogeld-Crowdfunding-mit-Adressaenderung-gekapert-3778227.html, 2017. Zuletzt aufgerufen am 16.12.2017.

[8] Axel Kannenberg. Geld gewaschen und Mt. Gox bestohlen: Mutmaßlicher Chef der Bitcoin-Börse Btc-e verhaftet Update. https://www.heise.de/newsticker/meldung/Geld-gewaschen-und-Mt-Gox-bestohlen-Mutmasslicher-Chef-der-Bitcoin-Boerse-Btc-e-verhaftet-3784467.html?artikelseite=2, 2017. Zuletzt aufgerufen am 15.12.2017.

[9] Bassam Jamal. Richmond Berks Review: Real Estate Ponzi Scam Stops Paying. http://binaryscamwatchmonitor.com/richmond-berks-review-scam/, 2017. Zuetzt aufgerufen am 16.12.2017.

[10] Bernard Marr. A Short History Of Bitcoin And Crypto Currency Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#4d8a68623f27, 2017. Zuletzt aufgerufen am 20.12.2017.

[11] Bitexperts. Bitcoin HSM implementation guide for securing a server-side hosted wallet. http://bitexperts.com/Question/Detail/1142/bitcoin-hsm-implementation-guide-for-securing-a-server-side-hosted-wallet. Zuletzt aufgerufen am 20.12.2017.

[12] British Broadcasting Corporation (BBC). North Korea 'hacked crypto-currency exchange in South'. http://www.bbc.com/news/world-asia-42378638, 2017. Zuetzt aufgerufen am 18.12.2017.

[13] BTC-Echo. Wie funktioniert Bitcoin-Mining? https://www.btc-echo.de/tutorial/wie-kann-ich-bitcoins-minen/. Zuletzt aufgerufen am 24.01.2018.

[14] coinmarketcap.com. Cryptocurrency Market Capitalizations. https://coinmarketcap.com/. Zuletzt aufgerufen am 20.12.2017.

[15] Dan Goodin. Bitcoins worth $ 228,000 stolen from customers of hacked Webhost. https://arstechnica.com/information-technology/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost/, 2012. Zuletzt aufgerufen am 16.12.2017.

[16] P. D. Filippi. *Bitcoin: A Regulatory Nightmare to a Libertarian Dream*. 2014.

[17] Financial Industry Regulatory Authority. HYIPs—High Yield Investment Programs Are Hazardous to Your Investment Portfolio. https://www.finra.org/investors/alerts/hyips-high-yield-investment-programs-are-hazardous-your-investment-portfolio, 2010. Zuletzt aufgerufen am 24.01.2018.

[18] Francisco Memoria. Hacker Nets over $500,000 after Hacking Enigma before ICO Date. https://www.ccn.com/hacker-nets-over-500000-after-hacking-enigma-before-its-ico-date/, 2017. Zuletzt aufgerufen am 21.12.2017.

[19] Jack Tatar. Is This the End of Bitcoin (Again)? https://www.thebalance.com/is-this-the-end-of-bitcoin-again-391268, 2015. Zuletzt aufgerufen am 20.12.2017.

[20] Jon Buck. Coincheck: Stolen $534 Mln NEM Were Stored On Low Security Hot Wallet. https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018. Zuletzt aufgerufen am 10.02.2018.

[21] Jörn Brien. Kursexplosion bei Bitcoin, Ether und Ripple: Börsen Coinbase und Bitfinex brechen zusammen. http://t3n.de/news/bitcoin-boersen-brechen-zusammen-885612/, 13.12.2017. Zuletzt aufgerufen am 13.12.2017, 10.54 Uhr.

[22] JP Buntinx. Online IOTA Seed Generator Starts Stealing Funds From Users. https://themerkle.com/online-iota-seed-generator-starts-stealing-funds-from-users/, 2018. Zuletzt aufgerufen am 10.02.2018.

[23] Kadhim Shubber. $4.1 Million goes missing as Chinese bitcoin trading platform GBL vanishes. https://www.coindesk.com/4-1m-goes-missing-chinese-bitcoin-trading-platform-gbl-vanishes/, 2013. Zuetzt aufgerufen am 16.12.2017.

[24] Laura Shin. Mystery Solved: $6.6 Million Bitcoin Theft That Brought Down Dark Web Site Tied To 2 Florida Men. https://www.forbes.com/sites/laurashin/2016/05/30/mystery-solved-6-6-million-bitcoin-theft-that-brought-down-dark-web-site-tied-to-2-florida-men/#34abc6f323d5, 2016. Zuletzt aufgerufen am 16.12.2017.

[25] learncryptography.com. 51% Attack. https://learncryptography.com/cryptocurrency/51-attack. Zuletzt aufgerufen am 20.12.2017.

[26] Lefteris Karapetsas. White Hat Siphoning has Occurred. What Now? https://blog.slock.it/white-hat-siphoning-has-occurred-what-now-f7ba2f8d20ef, 2016. Zuletzt aufgerufen am 18.12.2017.

[27] T. Moore and N. Christin. *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*. Springer

Berlin Heidelberg, Berlin, Heidelberg, 2013.

[28] Phil Daian. Analysis of the DAO exploit. http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/, 2016. Zuletzt aufgerufen am 24.01.2018.

[29] Powercompare.co.uk. Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa. https://powercompare.co.uk/bitcoin/, 2017. Zuletzt aufgerufen am 24.01.2018.

[30] Reuters. Schweizer Behörden gehen gegen E-Coin-Betrüger vor. https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/erfundene-kryptowaehrung-schweizer-behoerden-gehen-gegen-e-coin-betrueger-vor/20346512.html, 2016. Zuletzt aufgerufen am 18.12.2017.

[31] Shapeshift.io Blog. A Timeline: ShapeShift Hacking Incident. https://info.shapeshift.io/blog/2016/04/19/timeline-shapeshift-hacking-incident, 2016. Zuetzt aufgerufen am 16.12.2017.

[32] Stan Higgins. Details of $5 Million Bitstamp Hack Revealed. https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/, 2015. Zuetzt aufgerufen am 16.12.2017.

[33] Stan Higgins. ShapeShift lost $230k in String of Thefts, Report finds. https://www.coindesk.com/digital-currency-exchange-shapeshift-says-lost-230k-3-separate-hacks/, 2016. Zuletzt aufgerufen am 24.01.2018.

[34] steemit.com. Parity Wallet Hack Explained. https://steemit.com/cryptocurrency/@etheraveum/parity-wallet-hack-explained, 2017. Zuletzt aufgerufen am 20.12.2017.

[35] User dree12. List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses. https://bitcointalk.org/index.php?topic=576337, 2014. Zuletzt aufgerufen am 24.01.2018.

doi: 10.2313/NET-2018-03-1_06

A. LISTE VON UNTERSUCHTEN HACKS

Fall	Kategorie	Jahr	Anzahl Coins	Cointyp	Damaliger Wechselkurs	Höhe $ damals
MtGox	Coinbörse	2011-2014	650000	BTC	552,85 $/฿	359 Mio.
MyBitcoin	Coinbörse (Betrugsverdacht)	2011	78740	BTC	11,62 $/฿	10,73 Mio.
Bitomat	Coinbörse	2011	17000	BTC	13,62 $/฿	231.570
Bitcoin7	Coinbörse (Betrugsverdacht)	2011	5000	BTC	3,20 $/฿	15.980
Bitfloor	Coinbörse	2012	24086	BTC	11,34 $/฿	273.209
Linode	Webhoster	2012	46703	BTC	4,90 $/฿	228.845
Bitcoinia	Coinbörse	2012	38527	BTC	4,97 $/฿	191.638
Kronos	Startup	2012	4000	BTC	10,71 $/฿	42.859
BTC-E	Coinbörse	2012	4500	BTC	7,88 $/฿	35.452
Betcoin	Glücksspiel	2012	2900	BTC	5,36 $/฿	15.534
50BTC	Miningpool	2012	1174	BTC	11,45 $/฿	13.437
Silkroad	Darknetmarktplatz	2013	27618	BTC	752,50 $/฿	20,78 Mio.
Sheepmarket	Darknetmarktplatz	2013	5400	BTC	1047,90 $/฿	5,66 Mio.
PicoStocks	Börse	2013	5896	BTC	510,41 $/฿	3,01 Mio.
Inputs.so	Webwallet	2013	4000	BTC	195,84 $/฿	783.360
BIPS	Webwallet	2013	1295	BTC	510,39 $/฿	660.959
Bitcash	Coinbörse	2013	484	BTC	511,20 $/฿	247.422
Vicurex	Coinbörse	2013	1454	BTC	112,35 $/฿	163.351
Ozcoin	Miningpool	2013	922	BTC	114,53 $/฿	105.600
BTCGuild	Miningpool	2013	1254	BTC	57,56 $/฿	72.556
BitLC	Miningpool	2013	2000	BTC	25,74 $/฿	51480
Bitstamp	Coinbörse	2014	18866	BTC	279,00 $/฿	5,26 Mio.
SilkRoad2	Darknetmarktplatz (Betrugsverdacht)	2014	4400	BTC	616,05 $/฿	2,71 Mio.
BTER (1)	Coinbörse	2014	51,67 Mio.	NXT	0,03 $/NXT	1,65 Mio.
FlexCoin	Webwallet	2014	896	BTC	823,93 $/฿	738.240
Purse.io	Shopping	2015	10235	BTC	248,91 $/฿	2,55 Mio.
BTER (2)	Coinbörse	2015	7170	BTC	244,07 $/฿	1,75 Mio.
Coinapult	Webwallet	2015	150	BTC	286,67 $/฿	43.000
Cavirtex	Coinbörse	2015	-	BTC	- $/฿	-
Bitfinex	Coinbörse	2016	119756	BTC	593,70 $/฿	71,10 Mio.
The DAO	Smart Contract	2016	360000	ETH	17,32 $/ETH	62,35 Mio.
Gatecoin (ETH)	Coinbörse	2016	185000	ETH	10,63 $/ETH	1,97 Mio.
Gatecoin (BTC)	Coinbörse	2016	250	BTC	457,41 $/฿	114.352
Shapeshift	CoinWechselstube	2016	-	Misc.	-	230.000
Cointrader	Coinbörse	2016	-	BTC	- $/฿	-
Bitthumb	Coinbörse	2017	-	Misc.	-	82,7 Mio.
Tether	ICO	2017	30,95 Mio.	USDT	1,00 $/USDT	30,95 Mio.
Parity Wallet	Ethereum Client	2017	150000	ETH	200,00 $/ETH	3,00 Mio.
CoinDash	ICO	2017	43000	ETH	176,74 $/ETH	7,60 Mio.
Veritaseum	ICO (Betrugsverdacht)	2017	36000	VERI	205,49 $/VERI	7,40 Mio.
Enigma.co	ICO	2017	1500	ETH	300,00 $/ETH	450.000
Coincheck	Coinbörse	2018	523 Mio.	NEM	1,02 $/NEM	534 Mio.

doi: 10.2313/NET-2018-03-1_06

B. LISTE VON UNTERSUCHTEN BETRUGSFÄLLEN

Fall	Kategorie	Jahr	Anzahl Coins	Cointyp	Damaliger Wechselkurs	Höhe $ damals
Bitcoin Savings & Trust	HYIP	2011	146000	BTC	5,53 $/฿	807.380
Ubitex	Startup	2011	1139	BTC	13,62 $/฿	15.515
MyBitcoin	Coinbörse	2011	78740	BTC	13,62 $/฿	1,10 Mio.
Bitscalper	HYIP	2012	1350	BTC	4,73 $/฿	6461
GBL	Scam	2013	22000	BTC	195,95 $/฿	4,31 Mio.
MyEtherWallet	Webwallet	2017	-	ETH	-	-
Richmond Berks	HYIP	2017	-	BTC	-	-
Ethtrade	HYIP	2017	-	ETH	-	-
Neo BTC Bank	HYIP	2017	-	BTC	-	-
Nordebank	HYIP	2017	-	BTC	-	-
7thirty	HYIP	2017	-	BTC	-	-
Iotaseed	Phishing/Fake App	2018	-	IOTA	-	-

doi: 10.2313/NET-2018-03-1_06