Bitcoin Sicherheit

Marc Herschel

Hochschule Hannover, Ricklinger Stadtweg 120 30459 Hannover, Germany
marc.herschel @stud.hs-hannover.de

Abstract. Wir untersuchen die Sicherheit der Kryptowährung Bitcoin und beschäftigen uns dabei sowohl mit dem Sicherheitsprinzip dieser neuartigen Währung als auch mit verbundenen Sicherheitsrisiken für Endnutzer. In diesem Paper geht es sowohl um Angriffe auf das Zahlungsnetzwerk selbst wie zum Beispiel DoS Attacken, Sybil Angriffe, die 51% Attacke in ihren verschiedenen Formen und spieltheoretische Angriffe als auch um Risiken für den Endnutzer bei der Benutzung von Bitcoin im Alltag und Probleme mit seiner Privatsphäre und den Risiken, die ein dezentrales System mit sich bringt. Ein dezentrales System ist in seiner Natur für alle Teilnehmer durchschaubar, und es ist durchaus anzunehmen, das Regierungen, Geheimdienste und kriminelle auch hier versuchen, Einfluss zu gewinnen. Ziel dieser Arbeit ist es herauszufinden, wie sich Bitcoin neben traditionellen etablierten zentralen Zahlungssystemen sicherheitstechnisch verhält und ob mit der Dezentralisierung mögliche neue Angriffe und Probleme auftauchen, mit denen eine Untergrabung des Netzwerkes oder die Enthüllung der pseudonymen Zahlungsteilnehmer möglich ist.

Keywords: Bitcoin · IT Sicherheit · Blockchain · Kryptowährungen

1 Einleitung

Bei der Kryptowährung Bitcoin[1] handelt es sich um ein dezentralisiertes digitales Zahlungsmittel, dass eine Alternative gegenüber zentralisierten Institutionen wie zum Beispiel Banken und Bargeldtransferanbietern wie Westernunion anbietet.[1, s.1] Bitcoins Sicherheitsmodell unterscheidet sich drastisch zu dem der alteingesessen Finanzinstitutionen und bietet somit neue Chancen und Risiken. Die persönlichen Daten der Transaktionspartner sind nicht notwendig, um bei diesem System mitzumachen und das Zahlungsnetzwerk wird dezentral von den Nutzern selber betrieben[2, s. 269-270].

Da der Kurs der Währung mittlerweile einen deutlich höheren Wert aufweist als zur Adaptionszeit (Gewichteter Tageskurs Juni 2014 um die 450€, April 2019 um die 4500€ mit einem Extremum um den Dezember 2017 mit 12200€)[3] und die Währung somit die Aufmerksamkeit von Kriminellen auf sich zieht, die besonders auf neue, meist technisch nicht versierten Investoren abzielen[4], ist

es wichtig, sich mit den sicherheitstechnischen Aspekten dieser Währung zu befassen. Geklärt wird das dezentralen Zahlungssystem und die möglichen Risiken, denen Nutzer bei der Benutzung von Bitcoin gegenüberstehen. Sicherheit und Privatsphäre gehören unweigerlich zusammen und spielen gerade in Zeiten des zunehmenden Identitätsdiebstahls[5] bei zentralen Zahlungssystemen und aufzeichnen (Tracking) von Nutzerverhalten eine Rolle. Zuletzt wird sich noch mit der Frage der Angriffe auf das Zahlungsnetzwerk beschäftigt, wie wahrscheinlich diese sind und welche Folgen sie haben können.

2 Dezentralisiertes Zahlungssystem

Bitcoins zentrales Sicherheitsprinzip ist die Dezentralisierung des Zahlungsnetzwerkes. Traditionelle zentralisierte Zahlungsmodelle wie zum Beispiel Banken oder PayPal arbeiten mit Zugangskontrollen und Überprüfung der Nutzeridentitäten, um böswillige Akteure fernzuhalten. In einem dezentralisierten System wie zum Beispiel Bitcoin ist der Nutzer erst mal nicht gezwungen, seine Identität preiszugeben, es gibt daher auch keine zentralen Datenbanken mit "Kundeninformationen" im klassischen Sinne. Identitätsdiebstahl ist somit erst mal nicht möglich, da durch die Dezentralisierung die gesamte Blockchain öffentlich zugänglich ist und in dieser zwar die Transaktionen stehen, die öffentlich einsehbaren Transaktionen bei Bitcoin allerdings kein Zugriff auf die Coins eines Nutzers erlauben.

Verglichen mit zum Beispiel der Kreditkartenzahlung fällt hiermit gleich ein riesiger Angriffsvektor weg. Kreditkartenzahlungen sind akribisch auf Verschlüsselung und Vertraulichkeit der Nutzerdaten angewiesen. Ein einziger Fehler in der Ende-zu-Ende Verschlüsselung oder Speicherung der Daten für Abonnements führt zu einem Diebstahl der Kundenidentität. Eine Kreditkartentransaktion führt immer die Nummer, das Ablaufdatum, den CVC und persönliche Informationen des Kunden mit. Mithilfe dieser Daten ist es jedem möglich, Einkäufe zu tätigen. Eine Bitcoin Transaktion enthält ein Locking- und Unlocking-Skript, mit dem die Gültigkeit der in der Transaktion verwendeten UTXOs überprüft wird. Ein Angreifer kann mit diesen Daten allerdings nichts anfangen, außer die Gültigkeit besagter Transaktion zu überprüfen. Bei dem dezentralisierten Modell von Bitcoin fällt also außerdem die Notwendigkeit von Ende-zu-Ende Verschlüsselungen bei der Übertragung und Speicherung der Transaktionsdaten weg, welches wieder einen Angriffsvektor verhindert.[2, s. 269-270]

Vertrauen stellt in zentralisierten Systemen ebenfalls ein Problem da. Diese Systeme sind meist schichtartig aufgebaut, mit der "Root of Trust" in der inneren, robustesten Schicht untergebracht und je weniger vertrauenswürdig nach außen hin. In Bitcoin sind solche Schichten nicht vorgesehen, der Ledger bietet hier mit dem Genesisblock die "Root of Trust" an, welche bis zum neusten Block mit dem größten akkumulierten Proof of Work ausgebaut wird und mit einem Konsensmechanismus gegen spätere Änderung geschützt wird. [2, s. 270]

Mithilfe des Konsensmechanismus Proof of Work wird letztendlich verhindert, dass ein Angreifer einfach mal bereits finalisierte Blöcke, die Transaktionen enthalten, umschreiben kann, umso zum Beispiel Transaktionen zu widerrufen. Es gibt allerdings trotzdem einige Attacken, die darauf abzielen, welche später in diesem Paper behandelt werden. In einem zentralisierten System ist es dem Betreiber jederzeit möglich, Transaktionen zu ändern.

Anstatt einer einzigen mächtigen Entität wird das Zahlungsnetzwerk von mehreren Nutzern betrieben. Jedem Nutzer steht es frei, einen Knoten entweder fürs Validieren oder sogar Minen zu betreiben. Solange es eine gleichmäßige Verteilung zwischen Knoten und Nutzern gibt, ist das System dezentral und somit nicht durch eine Entität kontrolliert. Auch hier gibt es wieder Attacken, die später behandelt werden. Das dezentralisierte Modell von Bitcoin hat allerdings auch Schwachpunkte. Der Nutzer muss die Kontrolle über seine privaten Schlüssel behalten, nur mit diesem kann er seine Coins verwalten. Verlust dieser durch Diebstahl oder Hacking ermöglicht es einem Angreifer, Kontrolle über die Coins des Nutzers zu erlangen[2, s. 270]. Ein weiteres Problem stellt die Integration von Bitcoin als Zahlungsmittel in Diensten da. Wird das Modell der Dezentralisierung verletzt, indem der Nutzer zum Beispiel gezwungen wird, die Kontrolle über seine Schlüssel oder Coins abzugeben oder ein Versuch unternommen, die Transaktionen außerhalb des Bitcoins Netzwerkes zu verrichten, kann dies zu katastrophalen Ergebnissen führen. Es sollte außerdem nur einer komplett validierten Blockchain (mit dem größtem Proof of Work) vertraut werden. Ein Dienst, der irgendetwas anderem vertraut, macht sich implizit angreifbar, ein gutes Beispiel bieten hier die zahlreichen Hacks von Kryptobörsen. [2, s. 271]

Von der Dezentralisierung lässt sich nur profitieren, wenn das Sicherheitsmodell angenommen wird und kein Versuch entsteht, dieses mit der Zentralisierung zu mischen.

3 Sicherheitsrisiken für Nutzer

3.1 Verwahrung

Bei Bitcoin ist die sichere Verwahrung des eigenen Wallets am wichtigsten, um zu garantieren, dass Fremde keinen Zugriff auf die eigenen Vermögenswerte haben[2, s. 269]. Digitale Sicherheit ist verglichen mit der Entwicklung der Zivilisation ein neues Thema. Heutige Betriebssystem sind komplex und nicht sicher genug, um große Summen von Bitcoin zu lagern. Von einem durchschnittlichen Endanwender kann nicht großes Wissen im Bereich der IT-Sicherheit erwartet werden, nur um Bitcoin sicher zu verwenden.[2, s. 272]

Es ist jedoch positiv zu bewerten, dass gerade wegen Bitcoin neue Verfahren zur sicheren Verwahrung von digitalen Wertanlagen entwickelt wurden und durchschnittliche Nutzer mehr auf dieses Thema aufmerksam werden.[2, s. 271, 272]

Verlust des Wallets durch andere Faktoren als Diebstahl wie zum Beispiel Bitrot, mangelnde Backups und Verlust der Passphrasen[7] sind ebenfalls ernst zu nehmende Probleme. Für diese Fälle gibt es sogenannte Paper Wallets, mit denen Nutzer ihre Seedphrasen von zum Beispiel einem hierarchisch deterministischen Wallet kalt, sprich, als Gegenstand der realen Welt ohne Anbindung zum Internet lagern können. Diese Wallets müssen auch sicher verwahrt werden, jedoch ist es mit BIP-38 möglich, die Seedphrase zu verschlüsseln und so physischen Diebstahl zu erschweren.[2, s. 88, 273] Hardware Wallets bieten ebenfalls eine sichere Alternative zu auf dem System gespeicherten Wallets mit Internetanbindung (hot wallets), bei einer Kompromittierung des Systems muss der Nutzer mögliche schädliche Transaktionen über sein Gerät bestätigen und kann so selbst bei einem infizierten System einem Diebstahl entgehen.[2, s. 98] Ein besonderes Problem stellen Wallets da, die online bei einem Drittanbieter gespeichert werden (hot wallets), bei diesem kann der Nutzer die Sicherheit nicht selber beeinflussen und muss möglicherweise damit rechnen, dass besagter Anbieter seine privaten Schlüssel kennt und damit auch Zugriff auf seine Coins hat. Die ehemalige südkoreanische Tauschbörse Youbit[6] zeigt hier insbesondere die Risiken, die mit dem Vertrauen gegenüber einer zentralisierten Drittpartei entstehen. Ein Hacker entwendet einen circa 35 Millionen US-Dollar äquivalenten Wert an Bitcoin. Es gibt zahlreiche weitere Beispiele für gehackte Tauschbörsen, in denen der Versuch ein zentrales System um das dezentralisierte Bitcoin Zahlungsnetzwerk zu bauen, scheiterte. Gerade hier bieten Hardware Wallets eine bequeme Lösung für Endanwender an und ermöglichen auch technisch nicht versierten Nutzern eine sichere und unkomplizierte Lagerung.[2, s. 273] Lagerung aller Coins in einem Wallet ist ebenfalls ein Problem. Eine Diversifizierung seiner Werte und somit eine Aufteilung auf verschiedene Speichermethoden garantiert keinen Totalverlust, sollte eine Methode versagen.[2, s. 274] Multisignatur Adressen[2, s. 274] sind gerade für große Bitcoin basierte Unternehmen wie zum Beispiel die zentralisierten Tauschbörsen von Interesse. Zahlungen sind hier nur möglich, wenn mehrere private Schlüssel zum Signieren der Transaktion verwendet werden. Im Falle der Tauschbörse MT. Gox hätte, so der wahrscheinliche Insider Diebstahl[9] von ungefähr 650.000 BTC[8] verhindert werden. Brute-Force-Angriffe auf Private Schlüssel sind kein Problem, solange diese kryptografisch sicher erstellt wurden. Die verwendete Hashfunktion SHA-256 gilt als sicher und deckt mit 2^{256} möglichen Werten einen zu großen Bereich ab, um sinnvoll eine Brut-Force-Attacke zu verwenden. Auch Kollisionen sind zu unwahrscheinlich, um als Risiko zu gelten.

3.2 Anonymität

Bei Bitcoin handelt es sich um eine pseudonyme Währung, diese erfordert zwar keine persönlichen Informationen bei der Transaktion, ist allerdings nicht anonym, da alle Transaktionen öffentlich abrufbar sind. Adressen können hier als die Pseudonyme beschrieben werden, die der echten Identität mit genug Informationen zugeordnet werden können. Es ist einem Nutzer geraten, für jede Transaktion

eine neue Adresse zu benutzen[10, s. 11], um Verfolgung (Tracking) zu erschweren.

Die meisten modernen Wallets unterstützen so ein Verfahren heutzutage bereits und auch Unternehmen generieren häufig pro Transaktion eine neue Adresse, um so die Privatsphäre ihrer Kunden zu schützen. Eine Verschwendung von Adressen stellt kein Problem dar, da RIPEMD-160[12], welches zu Adressgeneration verwendet wird, einen Adressraum von 2^{160} Adressen zur Verfügung stellt. Ein Problem stellt jedoch die Verfügbarkeit von Nutzerbezogenen Informationen außerhalb des Bitcoin Zahlungsnetzwerks da.[10, s. 15,16]Es ist Analysten durchaus möglich, durch Informationen von Drittparteien wie zum Beispiel Tauschseiten und Geschäften eine Adresse und somit auch einen öffentlichen Schlüssel mit bestimmten Transaktionen zu verknüpfen. Mögliche Informationen sind zum Beispiel eine Lieferadresse, IP-Adresse oder sogar eine Bankverbindung[13]. Die deutsche Tauschbörse bitcoin.de benötigt ab einer bestimmten Menge Fiatgeld sogar eine Verifizierung der Identität. Tracking dieser Art ist nicht verhinderbar, der einzige Weg, anonym Coins zu beschaffen, ist in Bitcoin durch die Coinbase-Transaktion beim erfolgreichen Schürfen eines Blockes. Vollkommene Anonymität ist also im Bitcoin Netzwerk nicht möglich, um dieses Problem anzugehen und die Herkunft von Coins zu verschleiern, wurden verschiedene Verfahren entwickelt. Eines ist das Verfahren des zentralisierten vertrauten Mixers[10, s. 9], dieser nimmt von mehreren Teilnehmern zu anonymisierende Münzen an und vermischt diese über mehrere Runden, um sie später wieder an die Teilnehmer auszuzahlen. Dieses Verfahren stellt allerdings ein Risiko für die Nutzer dar, da sie die Kontrolle über ihrer Coins mittels einer Transaktion an den Mixer abgeben und so anfällig für Betrug sind und der Mixer somit gegen die Dezentralisierung verstößt.

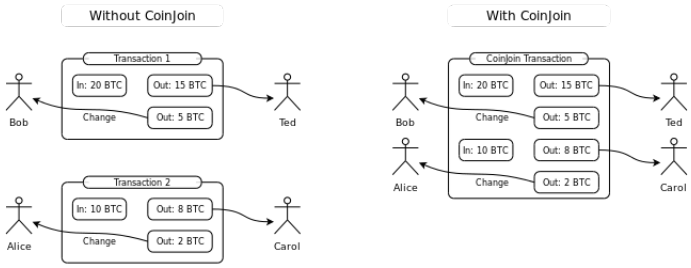

Fig. 1: CoinJoin-Verfahren, Quelle: github.com/nopara73/ZeroLink

Ein sichereres Verfahren, bei dem die Nutzer nicht die Kontrolle über ihre Coins abgeben müssen, stellt CoinJoin da, welches zum Beispiel über das ZeroLink-Verfahren[11] implementiert wird. Das Ziel von CoinJoin ist die Vereinigung der einzelnen Transaktionen mehrerer Teilnehmer zu einer großen, von allen

signierten Transaktion, um somit die Zuordnung zwischen Input und Output zu verschleiern.

Um eine erfolgreiche Zuordnung zu erschweren, muss CoinJoin über mehrere Runden mit einem festgelegten Rundenwert durchgeführt werden. In Fig. 1. ist es möglich durch Zusammenzählen der Beträge die Verschleierung zu entschleiern. In Fig. 2. zeigt sich auf der linken Seite ein einfach deanonymisierbaren CoinJoin, auf der rechten Seite ein CoinJoin mit dem Rundenwert 1. Dieser ist schon nach einmaliger Durchführung nicht eindeutig zuordenbar.

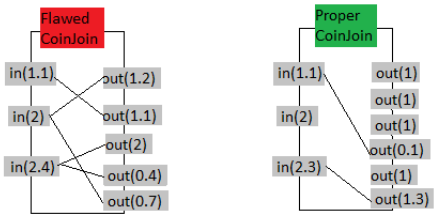

Fig. 2: Schlechter und guter CoinJoin, Quelle: github.com/nopara73/ZeroLink

Eine beliebte Implementierung von CoinJoin nutzt zwar einen zentralen Server zur Koordination zwischen den Teilnehmern, verwendet allerdings ein Blinding Verfahren[11, Sektion II.] um die Zuordnung IP und Teilnehmer Input zu verschleiern. Dadurch, dass sämtliche Teilnehmer ihren Teil der Transaktion nur signieren, wenn der Koordinationsserver diese nicht verändert entsteht ein Verfahren ohne Vertrauen gegenüber dem Server oder anderen Teilnehmern. Der Nutzer muss niemals seinen privaten Schlüssel verraten oder die Kontrolle über seine Coins aufgeben. Erst wenn alle Teilnehmer ihren Teil der Transaktion signiert haben, sendet der Koordinationsserver die Transaktion an die Knoten im Zahlungsnetzwerk. Hierbei sind Denial of Service Angriffe durch zum Beispiel Nicht-Signieren seiner Transaktion oder Ausgabe der UTXOs nach Signieren seiner Transaktion möglich.

4 Sicherheit durch Proof of Work

Es gibt neben Proof of Work noch andere Konsensmechanismen, einer davon ist Proof of Stake. Bei Proof of Stake wird kein mathematisches Problem wie bei Proof of Work gelöst, stattdessen wird der Block von einem zufälligen Teilnehmer validiert. Diese zufällige Ziehung hängt allerdings auch stark vom Anteil (Stake) an der Währung dieses Teilnehmers ab, Teilnehmer mit einem höheren Anteil haben eine höhere Wahrscheinlichkeit, einen Block zu validieren und finalisieren und damit auch belohnt zu werden. Proof of Work hat mit den verbrauchten Ressourcen für das Mining einen Gegenwert in der Realität, während es bei Proof

of Stake ausreicht, an einen großen Teil der sich in Umlauf befindenden Münzen zu gelangen. Dies könnte zum Beispiel durch Hacks von großen zentralisierten Diensten wie Tauschbörsen oder Aufstockung an Coins während der Adaptionszeit einer Währung möglich sein. Bei einer Proof of Work basierten Währung müsste ein Angreifer jedoch an eine Mehrheit der Rechenleistung gelangen, um die Möglichkeit zu erlangen, die Blockchain umzuschreiben, welches bei Bitcoin momentan schwierig ist.

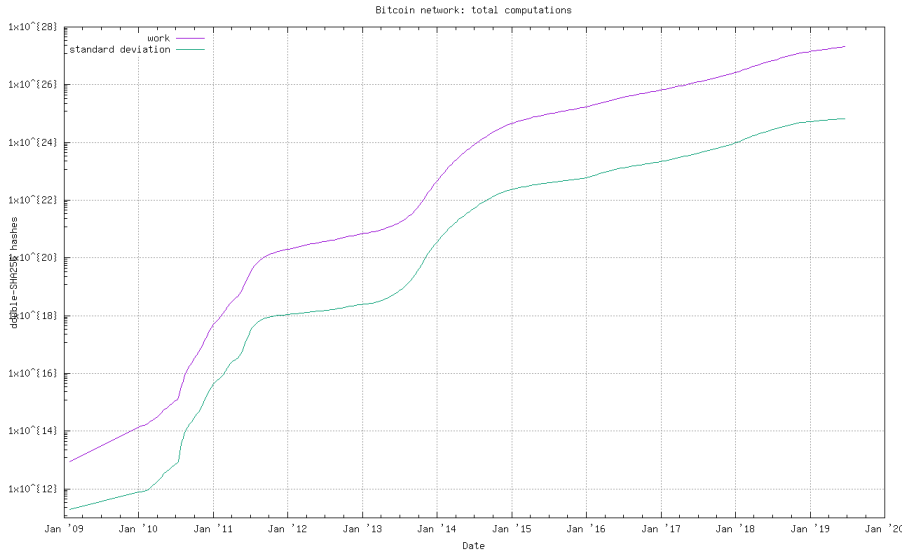

Fig. 3: Anzahl an Hash-Operationen im Bitcoin Netzwerk, Quelle: bitcoin.sipa.be

Bei Proof of Work ist die gültige Blockchain immer die mit dem meisten akkumulierten Proof of Work. Um derzeit eine neue Blockchain beginnend vom Genisisblock zu bauen, sind wie in Fig. 3 abgebildet nahezu 10^{28} Hash Operationen notwendig. Ein Angreifer mit 100% der gesamten derzeitigen Rechenleistung des Netzwerkes würde dafür momentan knapp 430 Tage[14] brauchen. Damit kann Bitcoins Blockchain als thermodynamisch sicher betrachtet werden, da es unwahrscheinlich ist, dass eine Entität in absehbarer Zeit soviel Rechenleistung kontrollieren kann.

5 Angriffe auf das Zahlungsnetzwerk

5.1 51% Angriff

Eine 51%-Attacke auf das Bitcoin Netzwerk ist ein Angriff auf den Konsensmechanismus der Blockchain. Dieser besagt, dass sich im Falle eines Forks immer die Teilkette mit dem meisten kumulierten Proof of Work durchsetzen wird,

während andere parallel laufende Teilketten verworfen werden.[2, s. 217] Die Attacke basiert daher darauf, dass der Angreifer mehr als 50% der gesamten Netzwerkrechenleistung in Form der sogenannten "Hashrate" zur Verfügung hat. Unter dieser Voraussetzung hat der Angreifer nun die Möglichkeit, in der Theorie immer die längste Proof of Work Kette zu erzeugen. Bereits bei einem Netzwerk Anteil von 51% findet man von 100 neuen Blöcken, 51 davon selbst, während der Rest des Netzwerkes nur 49 gefunden hat. Damit kann man das Bitcoin Netzwerk teilweise beeinflussen. Beispielsweise könnte man dadurch 100% aller Block Belohnungen, also die derzeitigen 12.5 BTC, für das erfolgreiche Finden eines neuen Blockes für sich selbst beanspruchen.[15, s. 42] Dies würde dadurch erfolgen, dass man vor jedem Block, der nicht vom Angreifer selbst gefunden wurde, einen Fork auslöst, um diesen zu umgehen. Da man mit der Mehrheit der Netzwerkrechenleistung wie eben erläutert immer die längste Proof of Work Kette erzeugen kann, erlaubt es einem so alle Blöcke erfolgreich zu umgehen. Gleichzeitig könnte man auch Transaktionen dadurch regulieren, wodurch man bestimmen könnte, wer Transaktionen durchführen darf und wie hoch die Transaktionsgebühren für diese wären.

Eine weitere Möglichkeit ergibt sich durch das "Double Spending" Problem. Der Angriff basiert auf dem Prinzip, einen Bitcoin Betrag mehr als einmal erfolgreich auszugeben, obwohl dies normalerweise nicht möglich sein sollte[2, s. 12]. Eingehende Transaktionen sind anfangs für Händler mit "0/unconfirmed" geflaggt[2, s. 14]. Dieser Händler wartet daraufhin auf $\boldsymbol{n}$ neue Blöcke, die dem Block mit der zu bestätigenden Transaktion folgen, um diese final zu bestätigen. Hierbei liegt $\boldsymbol{n}$ derzeit bei 6 Blöcken.[16] Um dies zu umgehen, kann ein Angreifer versuchen, mithilfe eines 51% Angriffes die Geschichte der Blockchain zu verändern, um dennoch einen erfolgreichen "double spend" durchzuführen. Der Angreifer initiiert dafür eine neue Transaktion und wartet, bis diese von einem Miner in einen Block geschrieben wird. Währenddessen löst er eine Fork vor dem genannten Block aus, gibt diese neue Teilkette jedoch noch nicht dem Netzwerk bekannt. In den ersten Block dieses neuen Forks platziert er nun erneut die gleiche Transaktion für einen anderen Zweck. Nun wartet er, bis die öffentliche Kette seine Transaktion bestätigt, während der Angreifer selbst an seiner eigenen, parallelen Kette weiterarbeitet. Ist die ursprüngliche Transaktion jetzt bestätigt, so wartet der Angreifer, bis seine parallele Kette über die größere Proof of Work Summe verfügt. Dies für ihn möglich, da er die Mehrheit der Netzwerkrechenleistung besitzt. Wenn dieser Fall eintritt, veröffentlicht der Angreifer seine private Kette, sodass die eigentliche Kette mit der bereits bestätigten Transaktion verworfen wird. In der neuen Kette ist nun aber auch die neue Transaktion, weswegen diese auch ausgeführt und bestätigt wird. Es wurde erfolgreich ein Bitcoin Betrag zweimal ausgegeben.[17]

Doch wie wahrscheinlich ist ein 51% Angriff auf das Bitcoin-Netzwerk? Betrachtet man die derzeitige Verteilung der Rechenleistung zwischen den einzelnen Mining Pools, sieht man, dass der größte Mining Pool momentan einen Anteil von ungefähr 20% hat, während die drei nächstgrößeren jeweils um die 10%

liegen.[18] Die Wahrscheinlichkeit auf einen erfolgreichen 51% Angriff von einem einzigen Pool ist mit einer Erfolgswahrscheinlichkeit von 1% oder weniger daher sehr gering.[19] Jedoch ergibt sich trotzdem die Möglichkeit auf Kollusion. Die vier größten Mining Pools könnten geheim zusammenarbeiten und hätten damit die Mehrheit der Netzwerkrechenleistung. Eine weitere Variante wäre als Angreifer die benötigte Hardware selbst zu kaufen, jedoch ist dies aufgrund der Anzahl der Netzwerkteilnehmer sehr teuer. Eine Stunde lang die Hardware zu mieten würde bereits 700,000$US kosten[20] - die gleiche zu kaufen um die 9 Milliarden US-Dollar.[21]

5.2 Blacklisting

"Blacklisting" beschreibt generell das Konzept, jemanden von etwas auszuschließen. Bezogen auf das Bitcoin Netzwerk bedeutet es, jemanden davon abzuhalten, exemplarisch Transaktionen ausführen zu können und ihn somit aus dem Netzwerk auszuschließen.

Punitive Forking Dieser Angriffstyp basiert erneut auf dem Ansatz, die Mehrheit der am Netzwerk teilnehmenden Rechenleistung zu besitzen. Jedoch muss dies in diesem Falle nicht durch einen Angreifer geschehen, sondern könnte auch beispielsweise durch eine geografische Region erfolgen, die eine entsprechende Rechenleistung ausweist und politisch reguliert wird. Fällt diese Regierung nun den Entscheid, eine bestimmte Person nicht mehr am Bitcoin Netzwerk in Form von Transaktionen teilnehmen zu lassen, so haben sie dazu die Möglichkeit, in dem sie das Netzwerk beeinflussen. Ihre Strategie ist dabei, in die von ihnen selbst gefundenen Blöcke keine Transaktionen dieser Person aufzunehmen und anderen Blöcken die Transaktion dieser Person enthalten, auszuweichen. Auf der Grundlage der vorher angesprochenen 51% Angriffsprinzipien haben sie die Möglichkeit dazu. Veröffentlicht die Regierung nun ihre Strategie, so wird der Rest des Netzwerkes auch dieser Strategie folgen, da sie sonst nicht mehr die Möglichkeit hätten, Blockerträge zu erhalten. Die Person wurde nun also effektiv aus dem Netzwerk in Form von Transaktionen ausgeschlossen.[15, s. 31-35]

Feather Forking Da es sehr schwer ist, einen Rechenleistungsanteil von mehr als 50% zu haben, betrachtet man mithilfe von Feather-Forking einen Ansatz, der bereits mit einem geringeren Netzwerkanteil funktioniert. Es handelt sich dabei um einen spieltheoretischen Ansatz, also Einen, der darauf beruht, dass alle Teilnehmer des Netzwerkes eine rationale Entscheidung treffen, um ihren Profit zu maximieren[35]. Der Angreifer kündigt daher seine Strategie, die Transaktionen der jeweiligen Person zu umgehen, wie im vorherigen Ansatz an. q sei dabei sein Anteil an der Netzwerkrechenleistung mit $0 < q < 1$. Man setzt voraus, dass man den Versuch, einen Block mit den Transaktionen der jeweiligen Person zu umgehen, bereits nach einem neu darauf gefundenen Block abbricht. Daher ergibt sich eine Chance von q^2 deren Transaktion erfolgreich zu umgehen. Der

Angreifer sei dabei nun ein Mining-Pool mit einem Netzwerk Anteil von 20%, also $\boldsymbol{q = 20\%}$.

Daraus ergeben sich die folgenden beiden Ereignisse:

$$E(include) = (1 - q^2) * BlockBelohnung + Transaktionsgebuehr \quad (1)$$

$$E(don't include) = BlockBelohnung \quad (2)$$

Das Ereignis $\boldsymbol{E(include)}$ ergibt sich dadurch, dass durch die Strategie des Angreifers der Rest des Netzwerkes eine Chance von $\boldsymbol{q^2}$ hat, den Block zu verlieren. Stellt man diese beiden Ereignisse nun gleich, so ergibt sich als Ergebnis, dass die Person die $\boldsymbol{BlockBelohnung * q^2}$ an Transaktionsgebühren bezahlen müsste, damit es sich für den Rest des Netzwerkes lohnen würde dessen Transaktionen in ihre Blöcke mit auszunehmen. Sie müsste also nach derzeitigen Kursen $\boldsymbol{0.04 * 12.5\ BTC = 0.5\ BTC}$ pro Transaktion zahlen, was ungefähr 3410 $USD entspricht. Falls die Person nun nicht bereit ist diesen Betrag pro Transaktion zu bezahlen, wurde sie praktisch aus dem Netzwerk ausgeschlossen.[15, s. 36-39]

5.3 Sybil Angriff

Ein Sybil Angriff ist generell ein Angriff auf ein Peer-to-Peer Netzwerk mithilfe von falschen Identitäten. Dabei versucht der Angreifer so viele dieser falschen Identitäten wie möglich im Netzwerk unterzubringen, damit sich ein ehrlicher Benutzer, der Teil des Netzwerkes ist, bestenfalls nur mit Angreifer Netzknoten verbindet.[22, s. 1] Falls sich ein ehrlicher Netzknoten nun nur mit dem Angreifer Knoten verbindet, hat der Angreifer eine Vielzahl an Möglichkeiten. Beispielsweise könnte er nun jegliche Informationen, die über seine falschen Knoten normalerweise weitergeleitet werden, dem ehrlichen Nutzer vorenthalten, sodass dieser keine neuen Informationen vom Netzwerk erhält und quasi davon ausgeschlossen wurde. Des Weiteren hat der Angreifer die Möglichkeit, falsche Netzwerk Informationen weiterzuleiten, die er selbst kreiert hat und die für die jeweilige Person profitabel sind.[23]

Erschwert wird dieser Angriff jedoch durch die Kosten eine neue Identität zu erstellen. Bei online Foren wird dies durch eine E-Mail oder neuerdings auch durch eine Handynummer bei der Registration realisiert. Die Kosteneinschränkung um Bitcoin Netzwerk ist dabei der Proof of Work Algorithmus, welcher in diesem Kontext besagt, dass jeder Netzwerkteilnehmer über Rechenleistung verfügen muss.[24, s. 4] Anschließend ist anzuführen, dass bereits eine einzige Verbindung zu einem weiteren ehrlichen Netzwerkknoten reicht, um den Angriff zu entlarven, weswegen es nur sehr schwierig ist, in einem Netzwerk mit sehr vielen Teilnehmern einen Sybil Angriff über längere Zeit durchzuführen.

5.4 Routing Angriff

In der Einleitung wurde das Bitcoin Netzwerk als ein “dezentralisiertes Netzwerk” beschrieben, jedoch hat sich laut in einer Studie der ETH Zürich im Zeitraum zwischen dem 5. November 2015 und dem 15. November 2016 herausgestellt, dass sich eine sogenannte Netzwerkzentralisierung über die Jahre gebildet hat. Dabei hosten 13 Internetdienstanbieter (ISP) um die 30% des gesamten Bitcoin Netzwerkes. Des Weiteren hat sich herausgestellt, dass 60% aller Bitcoin Verbindungen über nur drei unterschiedliche ISPs erfolgen.[25] Diese Entwicklung ermöglicht es für einen Angreifer, einen großen Teil des Bitcoin Netzwerkes mithilfe eines infizierten oder bösartigen Internetdienstanbieters zu beeinflussen.

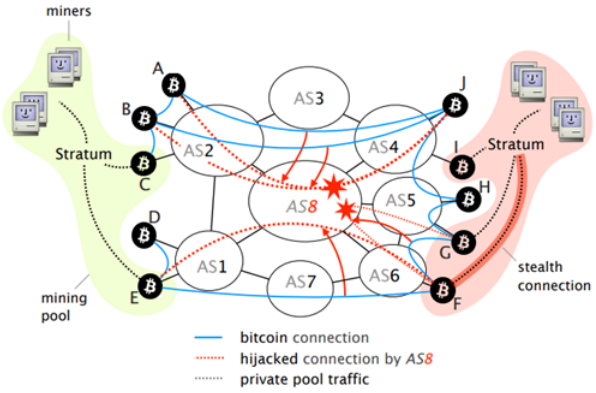

Fig. 4: Quelle: btc-hijack.ethz.ch

Ein mögliches Angriffsszenario wäre eine Teilung des Netzwerkes in zwei oder mehr disjunkte Partitionen. Daher könnte ein Angreifer beispielsweise versuchen, die Kommunikation zwischen zwei Mining Pools zu verhindern. Mining Pools kommunizieren innerhalb ihres eigenen Pools über ein weiteres Protokoll, wie zum Beispiel Stratum, weshalb die Kommunikation zwischen Teilnehmern des gleichen Pools nur schwer zu unterbinden ist. Jedoch kommunizieren die weiteren Pools nur über das Bitcoin Netzwerk miteinander. Ein Angreifer könnte nun mithilfe eines Internetdienstanbieters in Form eines autonomen Systems (AS), mit Hilfe eines BGP Hijacks den Netzwerkverkehr zwischen den beiden Pools unterbinden. BGP Hijacking ist generell ein Angriff auf Internet Routing Tabellen, die das Border Gateway Protocol verwenden, wodurch man unerlaubt IP Adressgruppen übernehmen kann.[26] Dies ermöglicht einem Angreifer, sämtlichen Netzwerkverkehr zu bestimmten IP Adressgruppen über seinen eigenen Netzwerkknoten zu leiten. Führt der Angreifer nun erfolgreich einen BGP-Hijack in unserem Szenario durch, so hat er die Möglichkeit, den Bitcoin Net-

zverkehr zwischen den beiden Mining Pools zu unterbinden. Aufgrund der fehlenden Kommunikation entstehen nun zwei unterschiedliche Blockchains, von denen am Ende des Routing Angriffs die kürzere verworfen wird, was ein Angreifer gezielt ausnutzen könnte.[25]

5.5 DoS-Angriff

Ein DoS-Angriff ist ein "Denial of Service"Angriff, also ein "Angriff auf die Verfügbarkeit eines Systems oder Dienstes"[27, s. 21]. Dies kann zur Verlangsamung oder sogar zur vollständigen Verhinderung des Zugriffs auf einen Dienst führen. Eines der häufigsten Vorkommen einer DoS-Attacke ist in Form eines DDoS, also einem verteilten DoS-Angriff, bei dem man beispielsweise über eine Vielzahl an http GET-Requests, auch bekannt als "http flooding", versucht, einen Server temporär unerreichbar für andere Nutzer zu machen[28], wie vergleichsweise bei einem der größten DDoS-Attacken bis dato auf den online Dienst "GitHub" im Jahre 2015.[29]

Flooding-Angriffe sind auf das Bitcoin Netzwerk als Transaktion-Flooding möglich, bei dem ein Angreifer versucht, so viele Transaktionen wie möglich zu initialisieren, sodass andere Transaktion so lange wie möglich brauchen, um bearbeitet zu werden. Ein historisches Beispiel solch eines Angriffes ist der Flooding-Angriff im Juli 2015, bei dem sich temporär mehr als 80,000 Transaktionen im Netzwerk befanden.[30] Heutzutage wird ein Angriff dieser Art jedoch erschwert aufgrund der hohen Transaktionsgebühren von ungefähr 2.50$US und der aktuellen Präventionsmaßnahmen, die sich im derzeitigen Satoshi beziehungsweise Bitcoin Client befinden. Die Gefahr auf einen anspruchsvolleren DoS-Angriff, wie etwa ein Transaktionsangriff, besteht jedoch immer. Dabei wird der Skriptteil einer Transaktion ausgenutzt, bei dem ein Nutzer anhand verschiedener Befehle Aktionen ausführen kann. In diesem spezifischen Fall wird eine besondere Transaktion angefertigt, die eine Größe von 955 Kilo Bytes aufweist und 200 Mal die Befehle OP_CHECKSIG und OP_TRUE ausführt. OP_CHECKSIG bewirkt dabei, dass die gesamte Transaktion mit Output, Input und Skript-Teil gehasht wird. Daher mussten die gesamten 955 Kilobytes der Transaktion 200 Mal neu gehasht werden, was zur damaligen Zeit bis zu drei Minuten gedauert hat. Dadurch war der Netzwerkknoten, der diese Transaktion verifizieren musste, für drei Minuten beschäftigt und unerreichbar.[32] Eine Attacke in dem Umfang ist jedoch heutzutage nicht mehr möglich, da seit Satoshi Client Version 0.8.0 Transaktionen, die größer als 100 Kilo Bytes groß sind, als nicht regulär betrachtet werden und daher auch nicht bearbeitet werden.[33]

Des Weiteren ist anzuführen, dass DoS-Attacken meist nicht an das Netzwerk selbst gerichtet sind, sondern an Drittanbieter wie zum Beispiel online Exchange und Wallet-Seiten, die Nutzern diverse Dienste anbieten. Dabei richten die Angriffe meist nur einen wirtschaftlichen Schaden für die Inhaber und Nutzer der Seite an.[34]

6 Schlussfolgerung

Die Gefahr der eben genannten Angriffe steigt durch Kombination stark an. Zum Beispiel hätte ein Angreifer die Möglichkeit, einen Routingangriff durchzuführen, um temporär die Mehrheit der Netzwerkrechenleistung zu erreichen und damit Zugriff auf die dazugehörigen Angriffsmöglichkeiten zu erhalten, indem er Teilnehmer des Netzwerkes vom Netzwerk ausschließt. Dennoch lässt sich sagen, dass die eben genannten Angriffe aufgrund ihrer hohen Komplexität und Kosten nur sehr schwer durchzuführen sind, daher erfolgen die meisten Angriffe wie in Form eines DoS-Angriffes, eher auf Drittanbieter und Nutzer. Das Bitcoin Netzwerk selbst ist daher nach heutigen Standards ein relativ sicheres Netzwerk. Ein Endnutzer sollte trotzdem davon ausgehen, dass er sich nicht anonym innerhalb des Bitcoin Netzwerkes bewegen kann und mit besonderer Vorsicht über seine Vermögenswerte walten muss.

References

1. Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
2. Andreas M. Antonopoulos: Mastering Bitcoin, 2nd Edition, O'Reilly Media, Inc., 2017 ISBN: 9781491954379
3. Bitcoin Kurs: Ansicht 5y - https://www.bitcoin.de/de/chart, abgerufen am 10.05.2019
4. Jemima Kelly: Financial Times, Hackers target new cryptocurrency investors, 2018, https://www.ft.com/content/9cf6d460-6d8a-11e8-8863-a9bb262c5f53
5. dpa/shüs: Hacker stehlen Daten von 380.000 Kreditkarten, 06.09.2018, https://www.faz.net/aktuell/wirtschaft/unternehmen/british-airways-hacker-stehlen-380-000-daten-von-kreditkarten-15775490.html
6. Daniel Shane: Bitcoin exchange goes bust after hack, 20.12.2017, https://money.cnn.com/2017/12/20/technology/south-korea-bitcoin-exchange-closes/index.html
7. Benjamin Wallace: https://www.wired.com/2011/11/mf-bitcoin/ zu Stefan Thomas
8. MTGox Statement: www.mtgox.com/img/pdf/20140320-btc-announce.pdf
9. Axel Kannenberg: Untergang der Bitcoin-Börse Mt. Gox: Ermittlungen deuten auf Insider-Tat, 02.01.2015, https://www.heise.de/newsticker/meldung/Untergang-der-Bitcoin-Boerse-Mt-Gox-Ermittlungen-deuten-auf-Insider-Tat-2507602.html
10. Fergal Reid, Martin Harrigan: An Analysis of Anonymity in the Bitcoin System v2, 2012, https://arxiv.org/abs/1107.4524v2
11. nopara73, TDevD: ZeroLink: The Bitcoin Fungibility Framework, https://github.com/nopara73/ZeroLink
12. Hans Dobbertin, Antoon Bosselaers, Bart Preneel: RIPEMD-160: A strengthened version of RIPEMD
13. Bitcoin.de Statement - https://www.bitcoin.de/de/faq/was-brauche-ich-fuer-handel/94.html
14. http://bitcoin.sipa.be/index.html - Proof of Work Equivalent Days, abgerufen: 18.06.2019

15. Max Fang: How To Destroy Bitcoin, https://cyber.stanford.edu/sites/g/files/sbiybj9936/f/20180124_bpase_game_theoretical_attacks_on_bitcoin.pdf
16. mKraken - Cryptocurrency deposit processing times, https://support.kraken.com/hc/en-us/articles/203325283-Cryptocurrency-deposit-processing-times
17. Meni Rosenfeld: Analysis of hashrate-based double-spending, 13. Dezember 2012, https://bitcoil.co.il/Doublespend.pdf
18. Mining Pools, https://www.blockchain.com/en/pools
19. https://people.xiph.org/~greg/attack_success.html, Hashpower 0.6, 6 Confirmations
20. https://www.crypto51.app/
21. https://gobitcoin.io/tools/cost-51-attack/, Abgerufen: 21.06.2019
22. John R. Douceur: The Sybil Attack, 10. Oktober 2002
23. https://en.bitcoin.it/wiki/Weaknesses#Sybil_attack
24. Joongheon Kim, Aziz Mohaisen: The Sybil Attacks and Defenses: A Survey - https://www.researchgate.net/publication/259440924_The_Sybil_Attacks_and_Defenses_A_Survey
25. Maria Apostolaki, Aviv Zohar, Laurent Vanbever: Hijacking Bitcoin: Routing Attacks on Cryptocurrencies, https://btc-hijack.ethz.ch/
26. Matthias Wählisch, Olaf Maennel, Thomas C. Schmidt: Towards Detecting BGP Route Hijacking using the RPKI, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.266&rep=rep1&type=pdf
27. https://moodle.hs-hannover.de/pluginfile.php/351421/mod_resource/content/1/VL08-Betriebssystemsicherheit.pdf
28. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
29. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
30. https://en.bitcoin.it/wiki/July_2015_flood_attack,Archive-Link:https://web.archive.org/web/20190621204651/https://en.bitcoin.it/wiki/July_2015_flood_attack
31. Bitcoin Fees: https://bitcoinfees.info/
32. Bitcoin Talk, https://bitcointalk.org/index.php?topic=140078.0
33. https://bitcoin.org/en/release/v0.8.1#improvements
34. https://www.cloudflare.com/learning/ddos/cryptocurrency-ddos-attacks/
35. Wolfgang Leininger, Erwin Amann: Einführung in die Spieltheorie, https://www.ethz.ch/content/dam/ethz/special-interest/gess/chair-of-sociology-dam/documents/education/spieltheorie/literatur/Leininger%20Amann%20Einf%C3%BChrung%200708-ST1-Vorlesung-Skript.pdf