Angriffe auf Bitcoin

Robin Meis

RWTH Aachen
robin.meis@rwth-aachen.de

Abstract. Bitcoin wurde als sichere und dezentrale Währung konzipiert. Verschiedene Angriffsmöglichkeiten erlauben jedoch die Übernahme einzelner Teile des Netzwerks. Diese Arbeit erklärt Routing Angriffe, Bribery und Selfish Mining. Zudem werden Updatemöglichkeiten beschrieben.

Keywords: Bribery · Selfish Mining · Routing.

Motivation

Seit dem ersten Release der Kryptowährung Bitcoin im Jahre 2009 haben Bitcoins stark an Wert und Bedeutung gewonnen. Die zentralen Aspekte einer jeden Währung stellen die Verfügbarkeit sowie Fälschungs- und Transaktionssicherheit dar. Dies gilt insbesondere für Transaktionen digitaler, dezentralisierter Währungen, deren Ziel es ist eine unabhängige und durch den Nutzer selbst betriebene, sichere Infrastruktur zu schaffen. Durch den Entfall zentraler Banken wird es notwendig eine alternative Kontoführung zu implementieren. Die dabei verwendete Blockchain verspricht die Gewährleistung sicherer Transaktionen [21] [1].

Durch die steigende Beliebtheit gewinnen Angriffe auf Kryptowährungen an Attraktivität. Ziel eines Angreifers ist, es in Besitz von mindestens 50% der gesamten Rechenleistung im Netzwerk zu gelangen. In der Folge erhält er durch Double Spending Angriffe, also die Ausführung von Transaktionen mit dem selben Ursprung an zwei unterschiedliche Empfänger, hohe Erträge [21].

Dem Angriff durch Einzelne im Rahmen finanzieller Interessen steht die Destabilisierung von Kryptowährungen entgegen. Dabei ist es das Ziel, das Vertrauen der Nutzer zu verringern. Seit Anfang 2018 versucht die chinesische Regierung den Bitcoin stärker zu regulieren. Neben dem Verbot virtueller Handelsplattformen, soll auch das Mining dort stärker reguliert werden [12] [11].

In Europa zeigt sich seit 2014, dass Banken in Folge von Strafzinsen zusätzlich Bargeld einlagern, um zusätzlichen Ausgaben zu entgehen. Nach Diskussionen über die Ausweitung von Strafzinsen auf private Anleger, werden zunehmend alternative Anlagemöglichkeit genutzt. Private Anleger, die ihr Kapital in Bitcoin oder anderen Kryptowährungen anlegen, entziehen sich staatlicher Kontrolle und somit auch möglichen Strafzinsen [9] [13].

Diese beiden Beispiele zeigen, dass staatliche Angreifer Interesse an möglichst geringem Vertrauen in Kryptowährungen haben, um langfristig die Kontrolle

über finanzielle Mittel und Transaktionen zu behalten. Hierzu eignen sich erfolgreiche Angriffe, sodass Sparer von der Investition in Bitcoin abgehalten werden.

Diese Arbeit soll einen Einblick in Angriffsmöglichkeiten geben, sowie Lösungsansätze aufzeigen. Zudem werden die Möglichkeiten der Durchführung von Aktualisierungen beschrieben, die zur Anpassung der Software im Fall neuer Angriffsszenarien zur Behebung genutzt werden können.

1 DNS Angriffe

Das Domain Name System dient der Bestimmung von IP-Adressen zu einer einzelnen Domain. Durch Manipulationen lassen sich Anfragen umleiten oder verhindern. Nachfolgend werden die Auswirkungen auf das Bitcoin Netzwerk analysiert.

1.1 DNS

Im Folgenden werden die Funktionsweise von DNS und mögliche Manipulationen beschrieben.

Funktionsweise Sofern eine Anwendung auf eine bestimmte Domain zugreifen möchte, wird zunächst eine Anfrage an einen DNS Server geschickt. Dieser beantwortet die Anfrage mit einer oder mehreren zu dieser Domain hinterlegten IP Adressen. Sofern ein DNS Server eine Anfrage aufgrund fehlender Informationen nicht beantworten kann, leitet er die Anfrage an andere DNS Server weiter. Nachdem die angeforderte Domain aufgelöst wurde, nutzt die Anwendung diese IP-Adresse, um auf das Zielsystem zuzugreifen [19].

Angriffe Auf einem DNS Server können Einträge für Domains angelegt werden, die den Einträgen des Domainbesitzers widersprechen. Bei einer Anfrage der betroffenen Domain, greift der DNS Server dann ausschließlich auf diesen veränderten Eintrag zu.

Durch die Veränderung von Einträgen lässt sich der Zugriff auf einen Dienst unterdrücken, indem eine ungültige IP-Adresse zurückgegeben wird. Alternativ kann eine Anfrage auch auf eine andere IP-Adresse umgeleitet werden, sodass der Dienst weiterhin erreichbar, aber durch Dritte kontrollierbar wird. Derartige Verfahren werden unter anderem bei staatlicher Zensur in China oder während des Katalonien Referendums eingesetzt [20] [10].

1.2 Bedeutung für Bitcoin

Nachfolgend wird ein daraus möglicher Angriff beschrieben und in Bezug auf seine Umsetzbarkeit bewertet.

Initialer Verbindungsaufbau Beim ersten Start des Bitcoin Clients, sind dem Client andere Nodes vollständig unbekannt, sodass zu diesem Zeitpunkt kein Zugriff auf die Blockchain besteht. Daher ist es zunächst erforderlich, dass ein Node andere Nodes findet.

Als erste Methode kommt dabei die Auflösung von DNS Einträgen zum Einsatz. Die A Records eines DNS Eintrags zeigen dazu auf die Zieladresse [19]. Aus sieben verschiedenen und unabhängigen *Seed Domains* [7] werden A Records aufgelöst, die auf vorhandene Nodes zeigen. Der neue Node baut im Anschluss eine Verbindung zu diesen Nodes auf und erhält auf Anfrage die IP-Adressen weiterer Nodes. Somit entsteht eine wachsende Liste, sodass weitere DNS Anfragen entfallen [6].

Ungültige DNS Einträge Durch die Manipulation der A Records auf ungültige IP-Adressen kann ein Angreifer die Verbindung zum Netzwerk zunächst verhindern. In diesem Fall wird auf im Node einkompilierte IP-Adressen zurückgegriffen, über die eine erste Verbindung zum Netzwerk aufgebaut wird [5].

Manipulierte DNS Einträge Setzt ein Angreifer einen A Records auf ein durch ihn kontrolliertes System, kann er einem neuen Node eine Liste ebenfalls durch Ihn kontrollierter Nodes bereitstellen. Somit werden die Clients in ein paralleles Netzwerk, dass eine andere Blockchain enthalten kann, verbunden. Hierbei muss er jedoch einkompilierte Checkpoints erfüllen [2].

Bewertung der Umsetzbarkeit Da viele Provider für ihre Kunden eigene DNS Server betreiben, können diese leicht manipulierte Einträge anlegen. Diese Provider können von staatlicher Seite zudem gezwungen werden derartige Manipulationen vorzunehmen. Für einen einzelnen Angreifer ist dieser Angriff nur schwer durchführbar.

2 Routing Angriffe

Bei den beschriebenen Angriffsszenarien versucht ein Angreifer einen Angriff auf Netzwerkebene durchzuführen und somit die Kommunikation zwischen Nodes zu manipulieren.

2.1 Grundlagen

Nachfolgend werden die für den Angriff erforderlichen technischen Grundlagen der Netzwerkinfrastruktur erklärt.

CIDR Mithilfe des **C**lassless **I**nter-**D**omain **R**outing werden IP Adressbereiche beschrieben. Die Notation besteht aus Präfix und Netzmaske, wobei aus dem Präfix der Beginn des Adressbereichs und aus der Netzmaske die Größe abgeleitet wird [18].

Autonome Systeme (*AS*) stellen die einzelnen Netze des Internets dar. Dabei werden die Daten innerhalb dieser Netze transportiert. Für Pakete, deren Ziel außerhalb eines autonomen Systems liegt, werden die Daten über Router zwischen den autonomen Systemen ausgetauscht. Jedes AS verfügt über eine eindeutige Nummer [18].

BGP Das **B**order **G**ateway **P**rotocol wird verwendet, um die Verbindung zwischen verschiedenen autonomen Systemen herzustellen. Dabei tauschen die Systeme untereinander Informationen über die jeweiligen Netze (*Announcements*) aus. Auf diese Weise entstehen Routen zwischen den Systemen [18]. Mittels BGP Hijacking lassen sich Pfade auf ein unberechtigtes Zielsystem anlegen, sodass die illegale Übernahme von IP-Adressen möglich ist [15].

2.2 Angriffe auf BGP Routing

Aktive Angriffe Da BGP die Autorisierung eines Announcements nicht verifizieren kann, ist es jedem autonomen System möglich eigene, ungültige Routen bekanntzugeben. Dadurch lässt sich der Datenverkehr für einen Präfix an ein unberechtigtes autonomes System umleiten. Der Betreiber dieses Systems hat die Möglichkeit, die Daten entweder zu verwerfen oder die Kommunikation zu verändern [15] [14].

Passive Angriffe kommen ohne die Manipulation von Routen aus. Dabei kann allerdings nur der Datenverkehr angegriffen werden, der über das autonome System zu einem weiteren Zielsystem weitergeleitet wird [14].

Hybride Angriffe kombinieren passive und aktive Techniken. Neben dem Angriff auf Daten, die über das System weitergeleitet werden, kündigt der Angreifer zusätzliche Präfixe an, sodass die Datenmenge gesteigert wird [14].

2.3 Angriffe auf Bitcoin

Aus den beschriebenen Angriffsmöglichkeiten ergibt sich die Möglichkeit der Teilung des Bitcoin Netzwerks sowie die Verzögerung der Datenströme. Zur Durchführung benötigt der Angreifer die Kontrolle über ein einzelnes autonomes System.

Verbindungen zwischen Nodes Zwischen den Nodes des Bitcoin Netzwerks wird eine unverschlüsselte TCP Verbindung aufgebaut. Zur Verringerung der Zentralisierung sind Verbindungen zu mindestens 8 verschiedenen Nodes erforderlich, die in unterschiedlichen /16 IP Netzen liegen [14].

Teilung des Bitcoin Netzwerks Durch die Blockade von Datenströmen lässt sich das Bitcoin Netzwerk in zwei unterschiedliche Partitionen teilen, sodass ein Austausch von Transaktionen blockiert wird. Es entstehen zwei unterschiedliche Blockchains, solange die Teilung besteht. Ein Angreifer kann nun, ohne über Mining Leistung zu verfügen, Double Spending Angriffe durchführen, indem er in beiden Partitionen Transaktionen von der selben Ausgangsadresse an zwei verschiedene Zieladressen durchführt [14].

Nach Ende des Angriffs werden die Partitionen nur langsam wieder zu einer Partition zusammengefügt. Blöcke, die auf der Seite mit der geringeren Mining Kapazität erzeugt wurden, werden ungültig [17].

Verzögerung der Datenströme Sobald der Datenverkehr zwischen zwei Nodes länger als 20 Minuten blockiert wird, erkennen die Nodes eine gestörte Verbindung und versuchen Verbindungen zu anderen Nodes aufzubauen. Wird der Verkehr jedoch lediglich verzögert, kann ein Node den Angriff nicht mehr erkennen [14].

Miner erhalten Informationen über neue Blöcke nur verzögert, sodass sie an einem Folgeblock arbeiten, der bereits gefunden wurde. Finden und veröffentlichen die betroffenen Miner diesen Block, stellt er einen Fork dar und wird nicht mehr in die Blockchain aufgenommen [17].

Zentralisierung Das Bitcoin Netzwerk ist durch seine P2P Infrastruktur dezentralisiert aufgebaut. Aus Routing Sicht ist das Netzwerk jedoch stark zentralisiert. 30% des Netzwerks gehören zu 13 autonomen Systemen, wobei 50% der Clients zu lediglich 50 autonomen Systemen gehören. Der Verkehr dieser 50 Systeme lässt sich mit der Ankündigung von 900 Präfixen erreichen [14].

3 Bribery

Damit der Angreifer Double Spending Angriffe durchführen kann, benötigt er 50% der Rechenleistung im Netzwerk. Dazu kann er durch finanzielle Ausgaben Zugriff auf Miner erhalten.

3.1 Angriffe

Nachfolgend werden Möglichkeiten beschrieben, die dem Angreifer den Kauf von Rechenleistung ermöglichen.

Mieten von Miningkapazität Verschiedene Anbieter vermieten den Zugriff auf Miner als Dienstleistung. Gegen Bezahlung erhält der Mieter dann die während der Mietzeit erzeugten Bitcoins. Ein Angreifer kann Miner anmieten, hat jedoch in Abhängigkeit von den angebotenen Zahlungsmöglichkeiten Probleme seine Anonymität zu gewährleisten. Zudem muss der Angreifer von Anfang an die vollständige Miete bezahlen, ohne dabei sicher sein zu können, die bestellte

Leistung wirklich zu erhalten [16]. Aufgrund der eingeschränkten Anonymität und dem fehlenden Vertrauen zum Anbieter ist dieser Angriff für einen Angreifer unattraktiv.

Negative Gebühren in Pools Pools dienen zum Zusammenschluss von Minern. Dabei werden die Erträge von gefundenen Blöcken unter den Minern aufgeteilt, sodass die Schwankung der Erträge für einen einzelnen Miner minimiert wird [4]. Der Poolbetreiber hat die Möglichkeit Gebühren festzulegen, um den Betrieb der notwendigen Infrastruktur zu finanzieren. Er erhält dann in Abhängigkeit der Gebühren einen Anteil an den erzeugten Bitcoins.

Technisch ist es möglich, Gebühren zu deaktivieren oder negative Gebühren festzulegen. Im Fall von negativen Gebühren geben die Miner keine Gebühr an den Poolbetreiber ab, sondern erhalten eine zusätzliche Belohnung durch den Poolbetreiber.

Ein Pool mit negativen Gebühren hat eine Anziehungswirkung auf Miner, da diese an einem möglichst hohen Gewinn interessiert sind. Mit steigendem Wachstum durch steigende Bekanntheit kann der Pool mit der Zeit auf die benötigte Größe anwachsen. Das Vertrauen zwischen Minern und Poolbetreiber wird Stückweise mit dem Finden neuer Blöcke durch die Miner und der anschließenden Zahlung der Belohnung durch den Betreiber des Pools aufgebaut.

Der Angriff lässt sich durch die Besitzer der Miner leicht erkennen, da negative Gebühren für einen seriösen Poolbetreiber insbesondere bei vielen Minern untragbar sind [16].

3.2 Probleme

Der Angreifer benötigt bis zum Erfolg ein hohes Grundkapital, um die benötigte Kapazität mieten zu können oder die Belohnung auszuzahlen. Zudem wächst ein Pool möglicherweise nur langsam, sodass ein Angreifer die Belohnung über einen langen Zeitraum hinweg zahlen muss. Sobald er seine Zahlungen an Miner einstellt, werden diese in attraktivere Pools wechseln. Ist das Kapital des Angreifers erschöpft und die erforderliche Poolgröße nicht erreicht, verliert der Angreifer seine gesamten Investitionen. Dies führt zu einem hohen finanziellen Risiko für den Angreifer.

Miner können den Pool nicht automatisch wechseln. Somit können sie auf der einen Seite nicht automatisch an einem Angriff teilnehmen, jedoch können sie einen Angriff auch nicht erkennen und die Arbeit im Pool automatisch verweigern. Es bleibt somit in der Verantwortung des Besitzers seine Miner in ehrlichen Pools einzusetzen.

Sofern der Angriff erfolgreich ist, ist mit hohen finanziellen Verlusten zu rechnen, die auch die Miner treffen würden. Daher ist es fraglich, ob sich eine signifikante Menge der Miner an einer für sie potentiell schädlichen Aktion beteiligen würde [16].

4 Selfish Mining

Ziel des Selfish Minings ist es, die Rechenleistung anderer Miner zu verschwenden, indem gefundene Blöcke geheimgehalten werden.

4.1 Grundlagen

Ein Miner berechnet den Nachfolgeblock für den letzten bekannten Block der Blockchain. Ein gefundener Block wird umgehend veröffentlicht, sodass er der Blockchain hinzugefügt wird und die Miner nun am Nachfolger für diesen Block arbeiten. Da jeder Block den Hash des vorherigen Blocks enthält, kann ein Block nur genau einen Vorgänger haben. Ein Block kann jedoch mehrere Nachfolger haben (Fork). Existiert ein Fork, wird der Fork in die Blockchain aufgenommen, der die längste Kette bildet und somit die höchste Rechenleistung erbracht hat.

4.2 Voraussetzungen

Ähnlich wie beim beschriebenen *Bribery* Angriff wird auch beim *Selfish Mining* ein Pool mit ausreichender Größe benötigt. Die Gesamtkapazität des Pools kann jedoch kleiner als 50% der Mining Kapazität des Bitcoin Netzwerks sein. Ziel des Angriffs ist es, einen höheren Ertrag als andere Miner zu erreichen. Dabei werden ehrliche Miner dazu gebracht sinnlose Rechenoperationen durchzuführen [17].

4.3 Durchführung

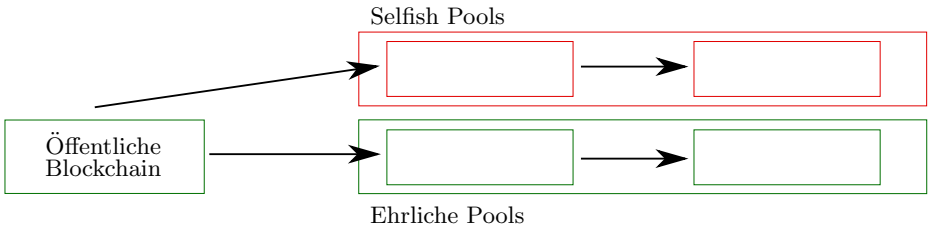

Fig. 1. Blockchain

Im ersten Schritt beginnen die ehrlichen Miner und die Selfish Miner am ersten Folgeblock für die aktuelle Blockchain zu arbeiten. An dieser Stelle ist die Voraussetzung, dass der Selfish Pool diesen Block vor einem ehrlichen Pool findet. Sobald der Selfish Pool den Block gefunden hat, hält er ihn geheim. Nun beginnt er auf Basis dieses Blocks am Nachfolger zu arbeiten.

Im nächsten Schritt ist es entscheidend, ob ein Selfish Pool zuerst den Nachfolger für seinen bereits gefundenen Block findet, oder ob ein ehrlicher Pool den ersten Block findet und veröffentlicht. Beide Fälle werden nachfolgend beschrieben.

Ehrlicher Pool Findet ein ehrlicher Pool den Block, bevor der Selfish Pool den zweiten Block findet, veröffentlicht er ihn. Der Selfish Pool bemerkt die Veröffentlichung und gibt nun auch seinen bisher geheimgehaltenen Block bekannt. In Abhängigkeit von der Ausbreitungsgeschwindigkeit der Blöcke durch das Netzwerk, wird nun einer der beiden Blöcke in die Blockchain aufgenommen. Es gewinnt der Block, der den nächsten Nachfolger erhält. Der andere Block bleibt als Fork übrig, sodass die Miner für diesen Block keinen Ertrag erhalten.

Selfish Pool Falls der Selfish Pool zwei Blöcke findet, bevor ein ehrlicher Pool den ersten Block findet, wartet er mit der Veröffentlichung des zweiten Blocks ebenfalls. Sobald ein ehrlicher Pool den ersten Block findet und veröffentlicht, veröffentlicht der Selfish Pool beide Blöcke. Da die Kette des Selfish Pools länger ist, als die des ehrlichen Pools, wird die längere Kette in die Blockchain aufgenommen und der Block des ehrlichen Pools wird als Fork nicht belohnt. Die ehrlichen Miner verlieren an dieser Stelle ihren Ertrag [17].

Folgen für ehrliche Miner Die Rechenzeit ehrlicher Miner wird verschwendet, da sie die gefundenen Blöcke nicht erhalten. Somit verringern sich die Erträge und die Attraktivität einen Miner zu betreiben sinkt.

4.4 Folgen für das Bitcoin Netzwerk

Ähnlich wie bei *Bribery* ließe sich der Pool als offener Pool für alle Miner anbieten. Da ein *Selfish Pool* einen höheren Ertrag für den einzelnen Miner verspricht, hätte auch ein solcher Pool eine starke Anziehungskraft für Miner und könnte im Laufe der Zeit immer schneller wachsen [17]. Der Angriff ist für den Besitzer der Miner zwar erkennbar, jedoch ist die Erkennung mit Aufwand und benötigtem Hintergrundwissen verbunden. Daher ist es wahrscheinlich, dass die Nutzer sich aufgrund des höheren Ertrags für den Selfish Pool entscheiden, ohne sich über die Konsequenzen bewusst zu sein. In der Folge wäre ein Großteil der Miner langfristig mit sinnlosen Operationen beschäftigt, sodass der eigentlich kleinere Selfish Pool das Netzwerk übernehmen könnte.

4.5 Schutzmaßnahmen

Der Angriff kann erkannt werden, sobald zwei Blöcke sich gegenseitig ausschließen. An dieser Stelle können Miner, die derartige Blöcke hinzufügen wollen bestraft werden, indem der Ertrag für alle Betroffenen Miner verringert wird [22].

5 Updates

Durch die Entdeckung neuer Sicherheitslücken im Bitcoin Netzwerk, ist es unter Abwägung der Risiken nötig, Miner oder Clients zu aktualisieren, um Angriffe zu verhindern. Dazu ist es möglich neue Kriterien zu bestimmen, die ein Block erfüllen muss, um akzeptiert zu werden. In einer Blockchain bestehen die Updatemöglichkeiten aus Soft- und Hardforks.

5.1 Grundbegriffe

Bei Updates der an einer Blockchain beteiligten Software gibt es die Möglichkeit von Soft- und Hardforks. Diese werden nachfolgend in ihren Eigenschaften beschrieben.

Softfork Ein Softfork gewährleistet die Kompatibilität zwischen alten und neuen Softwareversionen, sodass die Abwärtskompatibilität gewährleistet ist. Bestehende Nodes akzeptieren die neuen Blöcke nach ihren Kriterien weiterhin. Neue Nodes verwerfen Blöcke jedoch unter Umständen, da sie über neue Kriterien verfügen [8].

Hardfork Ein Hardfork verändert die Kriterien für die Gültigkeit eines Blocks derart, dass nach alten Kriterien ungültige Blocks nun gültig sind. So können Blocks eines Forks der Blockchain gültig werden, die bisher aufgrund der Kriterien ungültig waren. Nodes mit veralteter Software können jedoch nicht auf diesen Fork zugreifen, da ihre Kriterien für gültige Blöcke dies nicht zulassen. [3].

5.2 Voraussetzungen

Damit Aktualisierungen im Netzwerk wirksam werden, sind bestimmte Voraussetzungen erforderlich. Diese werden nachfolgend beschrieben.

Miner Damit ein Update im Bitcoin Netzwerk angewendet werden kann, muss es von mindestens 50% aller Miner akzeptiert werden. Ob ein Update erfolgreich ausgerollt werden kann, hängt somit von einer demokratischen Entscheidung der Betreiber der Miner ab [8].

Nodes akzeptieren bei einem Softfork neue Blöcke auch mit veralteten Software Versionen. Somit müssen Nodes nicht zwangsläufig aktualisiert werden, können jedoch durch Aktualisierungen zur Sicherheit beitragen [8].

5.3 Sicherheitsprobleme

Sofern die Miner im Bitcoin Netzwerk nur zu einem Teil aktualisiert werden, erkennt ein Teil der Miner weiterhin Blöcke als gültig an, die veralteten Kriterien folgen. Um die Sicherheit im Netzwerk zu gewährleisten ist es daher notwendig, dass alle Miner den neuen Kriterien möglichst schnell folgen.

Da Nodes ohne eine Aktualisierung weiterhin funktionieren, erkennen sie die Blöcke nicht aktualisierter Miner weiterhin als gültig an. Daher ist es erforderlich, dass alle Miner zeitnah aktualisiert werden [8].

6 Zusammenfassung

Bitcoin als dezentralisierte und sichere Währung, die sich staatlicher Kontrolle vollständig entzieht wird in den kommenden Jahren weiter an Interesse gewinnen. Der Bitcoin kann die an ihn gestellten Anforderungen derzeit jedoch nur teilweise erfüllen.

Mit *Bribery* und *Selfish Mining* bestehen Angriffsmöglichkeiten, die sich bereits von privaten Angreifern unter der Voraussetzung eines ausreichenden Kapitals ausnutzen lassen. Zudem hat sich Verwundbarkeit durch staatliche Einflüsse gezeigt.

Es wurde gezeigt, dass mittels *Softfork* eine geeignete Möglichkeit existiert, die verwendete Software unter Berücksichtigung der Abwärtskompatibilität abzusichern. Somit kann der Bitcoin auch in Zukunft die an ihn gestellten Anforderungen erfüllen.

7 Ausblick

Abschließend wird die Kombination der gezeigten Angriffe betrachtet und eine Folgenabschätzung für den Fall eines erfolgreichen Angriffs durchgeführt.

7.1 Kombination der Angriffe

Durch eine Kombination der aufgezeigten Angriffe, kann ein Angreifer die Effektivität erhöhen. Zunächst stellt er einen oder mehrere Pools bereit und steigert seine Attraktivität durch negative Gebühren. Sobald der Pool eine ausreichende Größe erreicht hat, kann der Angreifer seinen Angriff starten. Zunächst spaltet er einen Teil der Rechenleistung des Bitcoin Netzwerks durch BGP Hijacking ab. Zudem verschwendet er die Rechenzeit der verbleibenden Miner, indem er Selfish Mining betreibt. Diese Kombination ermöglicht es einem Angreifer die notwendige Rechenleistung für einen erfolgreichen Angriff gering halten und zugleich seine Ausgaben minimieren.

7.2 Attraktivität für Angreifer

Nach bekanntwerden eines erfolgreichen Angriffs wird der Bitcoin Kurs stark fallen. Ein Angreifer, der den Bitcoin aus finanziellen Gründen angreift, muss seine Bitcoins daher rechtzeitig in andere Währungen oder materielle Güter umwandeln.

Da ein erfolgreicher Angriff das Vertrauen in Kryptowährungen schwächen wird, ist ein Angriff aus staatlicher Sicht attraktiv und kann missbraucht werden, um die Nutzung staatlich regulierter Währungen zu stärken.

References

1. Bitcoin Wechselkurs. https://www.finanzen.net/devisen/bitcoin-euro-kurs. [Online; abgerufen 09.07.2018].
2. Checkpoint Lockin. https://en.bitcoin.it/wiki/Checkpoint_Lockin. [Online; abgerufen 15.07.2018].
3. Hardfork. https://en.bitcoin.it/wiki/Hardfork. [Online; abgerufen 07.06.2018].
4. Pooled mining. https://en.bitcoin.it/wiki/Pooled_mining. [Online; abgerufen 11.07.2018].
5. Satoshi Client Node Connectivity. https://en.bitcoin.it/wiki/Satoshi_Client_Node_Connectivity. [Online; abgerufen 10.07.2018].
6. Satoshi Client Node Discovery. https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery. [Online; abgerufen 03.06.2018].
7. Seed domains. https://github.com/bitcoin/bitcoin/blob/master/src/chainparams.cpp#L132. [Online; abgerufen 03.06.2018].
8. Softfork. https://en.bitcoin.it/wiki/Softfork. [Online; abgerufen 07.06.2018].
9. Deutsche Banken horten Milliarden in Tresoren. http://www.spiegel.de/wirtschaft/unternehmen/banken-und-sparkassen-horten-milliarden-in-tresoren-wegen-strafzins-a-1185548.html, 2017. [Online; abgerufen 10.07.2018].
10. Referendum in Katalonien: Spanien blockiert zahlreiche Webseiten. https://netzpolitik.org/2017/referendum-in-katalonien-spanien-blockiert-zahlreiche-webseiten/, 2017. [Online; abgerufen 09.06.2018].
11. China nimmt angeblich Bitcoin-Miner ins Visier. https://www.heise.de/newsticker/meldung/China-nimmt-angeblich-Bitcoin-Miner-ins-Visier-3936191.html, 2018. [Online; abgerufen 10.07.2018].
12. China will Bitcoin-Regeln weiter verschärfen. https://www.handelsblatt.com/finanzen/maerkte/devisen-rohstoffe/handel-mit-kryptowaehrungen-china-will-bitcoin-regeln-weiter-verschaerfen/20848108.html?ticket=ST-507280-Oeel04XM2dDtK6UHCwfR-ap6, 2018. [Online; abgerufen 10.07.2018].
13. EU-Kommission will Bitcoin-Regulierung vorantreiben. http://www.spiegel.de/wirtschaft/unternehmen/krytowaehrungen-eu-kommission-will-bitcoin-regulierung-vorantreiben-a-1195484.html, 2018. [Online; abgerufen 05.07.2018].
14. Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. Hijacking bitcoin: Large-scale network attacks on cryptocurrencies. *CoRR, abs/1605.07524*, 2016.
15. Hitesh Ballani, Paul Francis, and Xinyang Zhang. A study of prefix hijacking and interception in the internet. In *ACM SIGCOMM Computer Communication Review*, volume 37, pages 265–276. ACM, 2007.
16. Joseph Bonneau. Why buy when you can rent? In Jeremy Clark, Sarah Meiklejohn, Peter Y.A. Ryan, Dan Wallach, Michael Brenner, and Kurt Rohloff, editors, *Financial Cryptography and Data Security*, pages 19–26, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
17. Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Nicolas Christin and Reihaneh Safavi-Naini, editors, *Financial Cryptography and Data Security*, pages 436–454, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

18. Christian Huitema. *Routing in the Internet*. Prentice-Hall, 2000.
19. Cricket Liu and Paul Albitz. *DNS and Bind*. O'Reilly Media, Inc., 2006.
20. Graham Lowe, Patrick Winters, and Michael L Marcus. The great dns wall of china. *MS, New York University*, 21, 2007.
21. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press, 2016.
22. Ren Zhang and Bart Preneel. Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In *Cryptographers' Track at the RSA Conference*, pages 277–292. Springer, 2017.