Geld stinkt, Bitcoin auch – Eine Ökobilanz der Bitcoin Block Chain

Jörg Becker, Dominic Breuker, Tobias Heide, Justus Holler, Hans Peter Rauer, Rainer Böhme

Institut für Wirtschaftsinformatik - ERCIS
Westfälische Wilhelms-Universität Münster
Leonardo-Campus 3
48149 Münster
{becker, breuker, heide, holler, rauer, boehme}@wi.uni-muenster.de

Abstract: Ein modernes, globales Wirtschaftssystem ist ohne elektronisches Geld kaum vorstellbar. In der Regel stellt eine zentrale Kontrollinstanz die Integrität des Zahlungssystems sicher. Mit Bitcoin wurde eine elektronische Währung entwickelt, die die zentrale Instanz durch ein dezentrales, kryptographisches Protokoll ersetzt. In einer öffentlich sichtbaren Block Chain sind sämtliche Transaktionen dokumentiert. Die Teilnehmer eines Peer-to-Peer-Netzwerks wenden zur Erstellung dieser Block Chain eine große Menge Rechenleistung auf. Um die Block Chain zu manipulieren, müsste ein Angreifer dem ebenso viel Rechenleistung entgegensetzen. Die Sicherheit beruht auf der Annahme, dass niemand dazu in der Lage sein wird. Von einigen „Bitcoin-Evangelisten" wird dies als Chance gefeiert, Transaktionskosten einzusparen und, darauf aufbauend, Finanzinstitute und Regierungen zu entmachten. Dabei ist jedoch alles andere als klar, wie groß die Einsparungen tatsächlich sein könnten (bzw. ob überhaupt gespart werden kann). Da die zur Aufrechterhaltung einer sicheren Block Chain benötigte Rechenleistung mit großem Energiebedarf einhergehen könnte, stellt sich darüber hinaus die Frage nach den Konsequenzen für die Umwelt. Dieser Aufsatz demonstriert anhand einer vorsichtigen, quantitativen Abschätzung, dass die monetären wie ökologischen Kosten der Block Chain durchaus beachtlich seien könnten.

1 Motivation

Bereits seit vielen Jahren ist kryptographisches Geld Thema der Informatik. Ein prominenter Vertreter ist DigiCash [CFN88]. Es wurde mit dem Ziel entwickelt, bei elektronischen Zahlungen für Anonymität zu sorgen. Hintergrund solcher Entwicklungen ist die Tatsache, dass elektronisch abgewickelte Transaktionen Vertrauen in die involvierten Finanzinstitute voraussetzen. Sie haben die Macht, Transaktionen zu überwachen oder abzuweisen. So haben zum Beispiel viele Finanzinstitute, darunter Visa, MasterCard und PayPal, Ende 2010 sämtliche Zahlungen an die Enthüllungsplattform „Wikileaks" eingestellt; angeblich auf Druck der Vereinigten Staaten von Amerika [Bu11a]. Neben der

Macht, die Betreiber elektronischer Transaktionssystem haben, spielen auch die Kosten eine Rolle. Die Abwicklung von Transaktionen ist eine Dienstleistung, die selbstverständlich bezahlt werden muss. Insbesondere Kreditkarteninstitute stehen dabei oft im Verdacht, überhöhte Gebühren zu verlangen [BH08]. Auch aus diesem Grund besteht Interesse daran, Transaktionen dezentral abzuwickeln.

Die Umsetzung eines solchen Systems ist jedoch ein nicht-triviales Unterfangen. Es muss sichergestellt werden, dass niemand Geld aus dem Nichts erschafft, bestehendes Geld kopiert, fremdes Geld verwendet etc., also dass niemand die Integrität des Systems kompromittiert. Ohne zentrale Kontrolle fehlt die Instanz, auf die sich im Zweifel berufen werden kann.

Mit Bitcoin [Na08] wurde erstmals ein praktischer Versuch gestartet, die zentrale Institution in der Abwicklung von elektronischen Zahlungen vollständig zu entfernen und Kontrolle dezentral umzusetzen. Dabei kommt eine Technik zum Einsatz, die ursprünglich zum Verhindern von Denial-of-Service Angriffen entwickelt wurde [Ba02]. Sie basiert darauf, durch teilweises Invertieren einer Hashfunktion zu beweisen, dass eine gewisse Rechenarbeit, also einen „Proof-of-Work“, erbracht wurde. Die kollektiv von einem Peer-to-Peer-Netzwerk erbrachte Rechenarbeit wird bei Bitcoin dazu verwendet, eine Historie öffentlich bekannter Transaktionen zu erstellen, die sogenannte Block Chain. Sie dient dazu, alle Aktivitäten zu dokumentieren und Betrug zu verhindern. Einzelne Teilnehmer des Netzwerks vertrauen immer derjenigen Block Chain, für die die meiste Arbeit erbracht wurde. Auf diese Art einigen sie sich auf eine gemeinsame Historie. Angreifer, die eine alternative, manipulierte Block Chain erstellen wollten, müssten mehr Rechenleistung aufbringen als der ehrliche Teil des Netzwerks. Die Integrität von Bitcoin wird also durch konstantes Erbringen hoher Rechenleistung erreicht.

Befürworter von Bitcoin preisen das System mit einer Vielzahl von Vorteilen an. Einerseits könne aufgrund dessen dezentraler Natur niemand Kontrolle über Transaktionen ausüben. Beispielsweise konnte Wikileaks als Reaktion auf die Spendenblockade Bitcoins akzeptieren und so weiterhin Zahlungen entgegennehmen [Gr11]. Andererseits lautet das wohl am meisten hervorgebrachte Argument, dass die anfallenden Transaktionskosten sehr gering seien, da niemand für zentrale Kontrolle bezahlt werden müsse. In seinem Vortrag auf der European Conference on Bitcoin and Future Technology argumentiert Rick Falgrine, dass Bitcoin drastische Einsparungen ermöglichen wird, indem Banken im Transaktionsprozess eliminiert werden [Fa11]. Unklar bleibt jedoch, wie groß dieses Einsparpotenzial ist und ob, provokant ausgedrückt, es überhaupt positiv ist. Mit genau dieser Frage befasst sich der vorliegende Aufsatz.

Eng damit verbunden ist die Frage, welche Auswirkungen eine durch Rechenleistung abgesicherte dezentrale Währung auf die Umwelt haben könnte. Deren Kosten werden zu einem großen Teil durch die zur Erbringung der Rechenleistung benötigte Energie getrieben. Während einige den Energiebedarf im Bitcoin Netzwerk für vernachlässigbar halten, schätzen andere, er könne für Transaktionskosten von bis zu 10% verantwortlich sein [Bu11b]. Deshalb werden in diesem Aufsatz ebenso die ökologischen Konsequenzen einer großflächig ausgerollten Währung wie Bitcoin untersucht.

Im weiteren Verlauf skizziert Kapitel 2 zunächst technische Details von Bitcoin. Dabei wird insbesondere beschrieben, wie Angriffe auf Bitcoin verlaufen könnten (oder bereits sind). Kapitel 3 dokumentiert die Methodik der vorliegenden Analyse. Es wird ein hypothetisches Szenario aufgestellt, in dem ein auf einer Block Chain basierendes Transaktionssystem mit einem zentralen Electronic Cash (EC) System verglichen wird. In Kapitel 4 wird dann eine erste, vorsichtige Abschätzung der Transaktionskosten unternommen. Dies geschieht sowohl im Hinblick auf monetäre als auch ökologische Kosten. Implikationen daraus werden in Kapitel 5 diskutiert. Kapitel 6 schließt den Aufsatz mit einer Zusammenfassung sowie einem Ausblick auf weitere Forschung ab.

2 Das Bitcoin-System

2.1 Funktionsweise

Geld bezieht seinen Wert aus dem Vertrauen darauf, Güter und Dienstleistungen im Tausch gegen eine bestimmte Menge dieses Geldes zu erhalten. Der Besitz von Geld bedeutet, ein Versprechen zu besitzen, für die zu dessen Erlangung an andere erbrachten Leistungen in der Zukunft entsprechend entschädigt zu werden [Ma09]. Aus diesem Grund ist Knappheit eine notwendige Eigenschaft von Geld, denn ließe sich Geld leichter herstellen als der mit ihm assoziierte Gegenwert, so würde niemand eine Leistung dafür erbringen. Darüber hinaus müssen bei einer Transaktion beide involvierten Parteien sicher sein können, dass das Geld zwischen ihnen tatsächlich korrekt transferiert wurde. Nur dann ist die Integrität des Gesamtsystems sichergestellt.

Bitcoin erreicht diese Eigenschaften durch eine Kombination kryptographischer Verfahren. Ein Bitcoin selbst wird im System als eine Sequenz öffentlich bekannter Transaktionen dargestellt. Jede Transaktion beinhaltet den Hashwert der vorherigen, was beide miteinander verbindet. Daneben ist ein öffentlicher Schlüssel Bestandteil einer Transaktion. Er bezeichnet den Empfänger des Coins. Der Empfänger der vorherigen Transaktion, also der aktuelle Besitzer des Coins, signiert die neue Transaktion mit seinem privaten Schlüssel. Jeder Teilnehmer des Netzwerks kann überprüfen, dass er wirklich der Besitzer ist. Verwendet jemand einen fremden Coin, so ist dies leicht zu erkennen und der Coin würde als Zahlungsmittel nicht akzeptiert werden.

Dies wirft die Frage auf, wie der aktuelle Besitzer überhaupt bestimmt werden kann, wenn keine zentrale Institution die Transaktionen protokolliert. Kein Teilnehmer kann sicher sein, alle Transaktionen zu kennen, und die ihm bekannten erreichen ihn nicht notwendigerweise in korrekter Reihenfolge. Dieses Problem ist durch die sogenannte „Block Chain“ gelöst. Blöcke sind virtuelle Behälter für Transaktionen und, als Hashkette, wie diese ebenso geordnet. Durch die Blöcke wird eine eindeutige Reihenfolge der Transaktionen festgelegt. Zur Erstellung eines Blocks müssen der Block und dessen Transaktionen, kombiniert mit einer Zufallszahl, einen Hashwert von besonderer Struktur ergeben. Es wird davon ausgegangen, dass eine passende Zufallszahl nur durch rechenintensives Ausprobieren zu finden ist. Die Schwierigkeit des Problems wird so justiert, dass etwa alle zehn Minuten ein neuer Block „gefunden“ wird. Teilnehmer im

Netzwerk akzeptieren immer die längste ihnen bekannte Block Chain, da davon auszugehen ist, dass der Großteil des Netzwerks an ihrer Erstellung beteiligt war. Will eine Einzelperson die Block Chain manipulieren, so müsste sie schneller Blöcke finden als der Rest des Netzwerks, was für unmöglich gehalten wird. Auf diese Weise einigen sich alle Teilnehmer auf eine einzige Reihenfolge von Transaktionen.

Für weitere Details bezüglich der Funktionsweise von Bitcoin, wie dem Teilen von Coins oder dem sogenannten „minen" neuer Coins, sei auf [Na08] verwiesen.

2.2 Angriffsmöglichkeiten

Auf der einen Seite existieren eine Reihe von Angriffspunkten, die der technischen Implementierung von Bitcoin geschuldet sind. Wie in Unterabschnitt 2.1 beschrieben, ermöglicht der Besitz des privaten Schlüssels die Verwendung aller Coins, die an den zugehörigen öffentlichen Schlüssel transferiert wurden. Coins können also gestohlen werden, indem man sich Zugriff auf die privaten Schlüssel ihres Besitzers verschafft. So wurden in 2011 mehrere tausend Coins von einem großen Anbieter elektronischer Bitcoin-Brieftaschen („Wallets") gestohlen [Je11]. Über Diebstahl hinaus sind viele weitere potenzielle Schwachstellen vorhanden. Auf ein Peer-to-Peer-Netzwerk sind beispielsweise Denial-of-Service Angriffe leicht vorstellbar. Alle diese Angriffe hängen jedoch nicht direkt mit der Nutzung einer Block Chain zur Garantie von Integrität zusammen, sondern stellen Angriffe auf die technische Infrastruktur dar. Für einige Probleme sind bereits erste Lösungsvorschläge entwickelt worden [Ba12].

Auf der anderen Seite existiert ein Angriff, der speziell mit der Idee der Block Chain zusammenhängt. Schafft es ein Angreifer (oder eine Gruppe von Angreifern), mehr als die Hälfte der Rechenleistung des Netzwerks unter seine Kontrolle zu bringen, kann er die Block Chain nach seinen Wünschen zu manipulieren. Er kann dadurch direkt profitieren, indem er zunächst einen Coin transferiert und dafür eine Gegenleistung erhält. Parallel zur Block Chain des Netzwerks berechnet er heimlich eine eigene, in der er beispielsweise den Empfänger der Transaktion so manipuliert, dass eine zweite Adresse des Angreifers den Coin erhält. Sobald seine eigene Block Chain länger ist als die kollektiv erstellte, veröffentlicht er sie. Sie wird daraufhin von allen Teilnehmern des Netzwerks akzeptiert, und der Angreifer ist wieder im Besitz des Coins. Was den Angreifer motiviert, ist jedoch nicht notwendigerweise ökonomisches Kalkül. Ebenso denkbar sind beliebige, großflächige Manipulationen, um das Vertrauen in das System zu zerstören. Wäre Bitcoin wichtiger Bestandteil einer Volkswirtschaft, so könnte dies eine Form von Cyberterrorismus ermöglichen.

3 Analysemethodik

Die Fragen, die mittels der Analyse zu untersuchen sind, lauten:

- Rentiert sich dezentrales, auf einer Block Chain basierendes kryptographisches Geld als Ersatz für ein vergleichbares System unter zentraler Kontrolle?

- Mit welchen ökologischen Konsequenzen eines solchen Systems ist zu rechnen?

Offensichtlich sind Antworten auf diese Fragestellungen mit großer Unsicherheit behaftet. In diesem Aufsatz wird daher nur eine vorsichtige Schätzung präsentiert. Dies bedeutet konkret, dass für das dezentrale System besonders vorteilhaftes Szenario betrachtet wird. Ziel ist es, eine obere Schranke für die Kostenersparnis abzuschätzen.

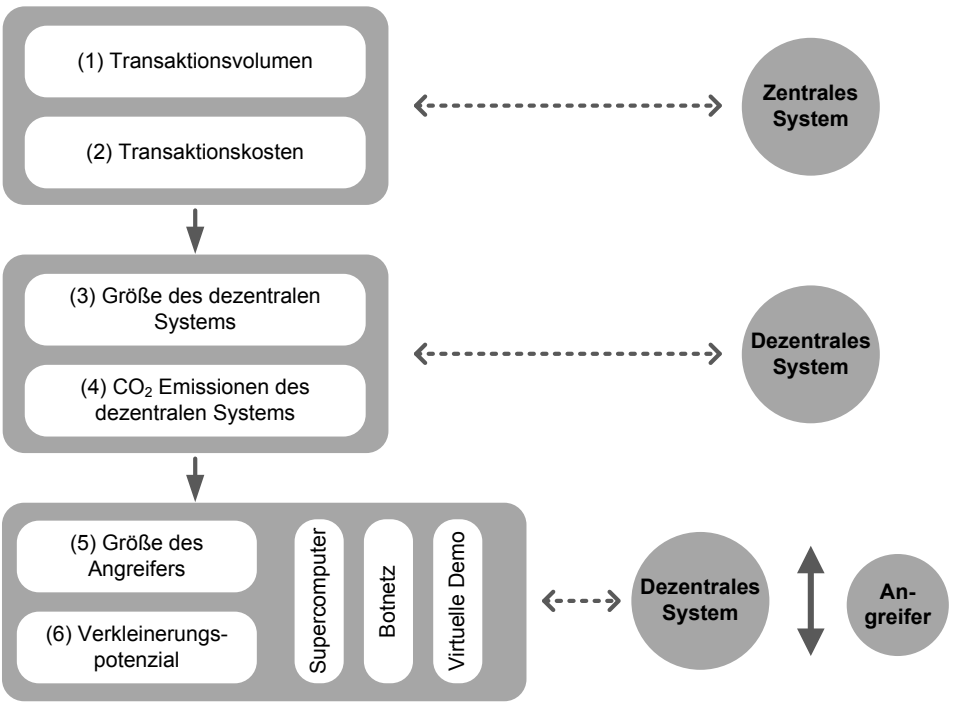

Abbildung 1: Vorgehensweise der Analyse

Die Analyse folgt dabei einer einfachen Logik. Sieht man von den Kosten für die Kommunikation innerhalb des Netzwerks ab, also das Verbreiten von Transaktionen und Blöcken, so bleiben die Kosten für das Erstellen der Block Chain übrig. Wie viel Rechenleistung darin investiert wird, hängt davon ab, was den Nutzern des Systems dessen Sicherheit wert ist, denn mit steigender Rechenleistung werden Angriffe unwahrscheinlicher. Die Rechenleistung ist dabei Treiber für die im Netzwerk anfallenden Kosten, da Hardware beschafft und betrieben werden muss. Ein wichtiger Bestandteil davon sind Kosten für Energie, deren Erzeugung wiederum negative Konsequenzen für die Umwelt hat. Die Kostenersparnis kann über einen Vergleich aller Kosten mit denen, die ein zentrales System gleichen Umfangs verursachen würde, abgeschätzt werden.

Mit diesen Überlegungen im Hinterkopf wird gemäß des in Abbildung 1 dargestellten Vorgehensweise der Vergleich umgesetzt. Zunächst ist für das zentrale System ein Transaktionsvolumen und abhängig davon dessen Kosten zu bestimmen (1 und 2). Diese Kosten dienen daraufhin als Referenz, anhand derer die maximale Größe eines äquiva-

lenten dezentralen Systems berechnet wird. Größe ist dabei in Form von Rechenleistung quantifiziert (3). Abhängig davon wird auch der CO_2-Ausstoß geschätzt und als Maß für die ökologischen Konsequenzen herangezogen (4). Letztlich werden drei verschiedene Angriffsszenarien konstruiert (5). Durch einen Vergleich der Rechenleistung von Angreifer und Gesamtnetzwerk wird ersichtlich, wie weit das Netzwerk im Vergleich zur Referenz verkleinert werden kann (6).

4 Kosten einer dezentralen Währung

Die im Folgenden dargestellten Ergebnisse umschreiben aus Platzgründen nur kurz die für die Abschätzung getroffenen Annahmen sowie die daraus resultierenden Ergebnisse. Für eine detailliertere Beschreibung sei auf [An12] verwiesen. Darüber hinaus ist die Berechnung in einem Excel-Sheet dokumentiert.[1] Die Autoren verstehen diesen Aufsatz als Einladung zu konstruktiven Kritik und zur schrittweisen Präzisierung der Annahmen.

4.1 Das zentralisierte Referenzsystem

Wie in Kapitel 3 erwähnt soll die mögliche Ersparnis durch das dezentrale System durch eine obere Schranke abgeschätzt werden. Bei konstanter Rechenleistung sinken die Kosten pro Transaktion offensichtlich mit deren Anzahl. Das größte vorstellbare Transaktionsvolumen würde erreicht, wenn alle Zahlungen weltweit über das System abgewickelt würden. Dabei sollen jedoch nur „gewöhnliche“ Zahlungen betrachtet werden, nicht aber extrem große, wie sie beispielsweise zwischen Banken stattfinden. Unsere Schätzung für das weltweite Transaktionsvolumen dieser Art beläuft sich auf 9,44E+13 US Dollar (USD), basierend auf Zahlen für das Jahr 2010 [Ba11].

Für die Kosten eines zentralisierten Referenzsystems können Marktpreise für gewöhnliche Transaktionen herangezogen werden. Kreditkartengesellschaften berechnen typischerweise 1-3% [WW05]. Andere Systeme hingegen, wie das Electronic Cash (EC) System in Deutschland, verlangen nur etwa 0,3% [Eu08], sind also deutlich günstiger. Da das EC-System keine zusätzlichen Leistungen wie kurzfristige Kredite gewährt und dem Leistungsspektrum einer dezentralen Währung wie Bitcoin damit ähnlicher ist, verwenden wir diesen Preis. Dies liefert Transaktionskosten von 2,83E+11 USD weltweit. Zum Vergleich: Das ist die Größenordnung des Bruttoinlandsprodukts von Finnland.

4.2 Das äquivalente dezentrale System

Zunächst wird nun bestimmt, welche Rechenleistung ein dezentrales System erbringen könnte, wenn es mit den in Unterabschnitt 4.1 bestimmten Kosten betrieben würde. Wir messen Rechenleistung dabei in Operationen pro Sekunde (Ops/s). Zunächst wird dazu anhand typischer Kostenstrukturen in Rechenzentren der Kostenanteil, der für Energie aufzuwenden ist. Dieser beläuft sich auf etwa 30% [Be07], was ein jährliches Budget

[1] http://dl.dropbox.com/u/1168860/DoesProofOfWorkPayOff.xlsx

von 8,49E+10 USD für Energie ergibt (die restlichen 70% der Kosten fallen für Akquisition von Hardware und Erhalt der Infrastruktur an). Kombiniert mit einem Strompreis von 0,10 USD/kWh, der niedrigste unter allen nennenswerten Stromproduzenten der Welt, lassen sich mit dem Budget 3,06E+18 Wattsekunden (Ws) erzeugen.

Auch die Größe des dezentralen Systems wird nun wieder von oben beschränkt. Dazu wird angenommen, dass die Rechenleistung in Abhängigkeit der aufgewendeten Energie erbracht wird, und dass dies besonders effizient geschieht. Somit überträgt sich diese Effizienz implizit auch auf alle anderen Arten von Kosten. Durchschnittlich erbringen die 500 umweltfreundlichsten Supercomputer der Welt etwa 1,82E+8 Ops/Ws [Gr12]. Wird diese Rate für das dezentrale System zugrunde gelegt, ergibt sich eine Rechenleistung von 1,76E+19 Ops/s.

Um den CO_2-Ausstoß zu bestimmen, den ein solches System zu verantworten hätte, wird nun ein einfaches gewichtetes Mittel berechnet. Der CO_2-Ausstoß verschiedener Energieträger [Lü07], gewichtet mit dem relativen Anteil dieser Energieträger an der weltweiten Gesamtproduktion [Ie11], ergeben einen Gesamtausstoß von ca. 6,10E+11 kg pro Jahr. Dies entspräche etwa 2,1% des weltweiten, von Menschen verursachten CO_2-Ausstoßes, und würde etwa mit dem globalen kommerziellen Luftverkehr gleichziehen.

4.3 Die Angriffsszenarien

In allen drei nun betrachteten Szenarien wird nun die Stärke des Angreifers in Form von Ops/s abgeschätzt. Sie sind als Worst-Case-Szenarien zu verstehen, und müssen als solche nicht notwendigerweise profitabel sein. Wie in Unterabschnitt 2.2 erwähnt, kann ein Angreifer auch destruktive Ziele verfolgen. Daher werden weder Nutzen noch Kosten eines Angriffs einbezogen. Allein die möglicherweise erreichbare Rechenkapazität ist von Interesse.

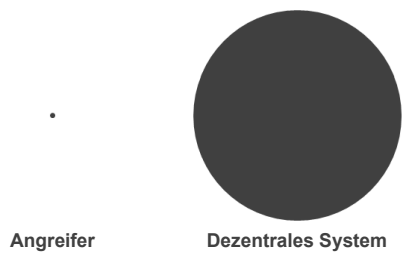

Abbildung 2: Verhältnis von Angreifer (Supercomputer) und dezentralem System

4.3.1 Supercomputer

Als einfachstes denkbares Angriffsszenario ist vorstellbar, dass ein großer Supercomputer gegen das dezentrale System antritt. Der aktuell leistungsfähigste ist der K Computer, welcher sich im japanischen Forschungsinstitut RIKEN befindet [To12]. Mit seinen 1,05E+16 Ops/s erreicht er lediglich 0,06% der Gesamtleistung des Referenzsystems.

Dies bedeutet, dass das dezentrale System auf 0,12% der Referenzgröße geschrumpft werden müsste, damit der K Computer gleichzieht. Dieses Szenario bietet also einigen Raum für Einsparungen. Abbildung 2 illustriert das Kräfteverhältnis. Die Fläche der Kreise ist dabei proportional zur Rechenkapazität.

4.3.2 Botnetz

Das nächste Szenario unterstellt einen Angriff mit Hilfe eines großen Botnetzes. Zwei wesentliche Faktoren bestimmten die Stärke dieses Angriffs. Zum einen ist die Größe des Botnetzes von Interesse, zum anderen die durchschnittliche Rechenkapazität einzelner Bots. Die Größe eines Botnetzes zu messen ist nicht einfach und Gegenstand aktueller Forschung [Zh08]. Für unsere Worst-Case-Analyse betrachten wir es jedoch als gerechtfertigt, eine eventuell zu hohe Schätzung zu verwenden. Daher setzen wir eine Größe von 30 Millionen Bots an, was laut Wikipedia dem größten bekannten Botnetz entspricht [Wi12a]. Zur Bestimmung der Rechenleistung einzelner Bots wird eine Analogie gezogen. Die Berkeley Open Infrastructure for Network Computing (BOINC) ist eine Plattform für verteilte Berechnungen und veröffentlicht Statistiken zur erbrachten Leistung sowie Anzahl aktiver Nutzer [Bo12]. Mit dieser Plattform wird beispielsweise das bekannte SETI@home Projekt umgesetzt.

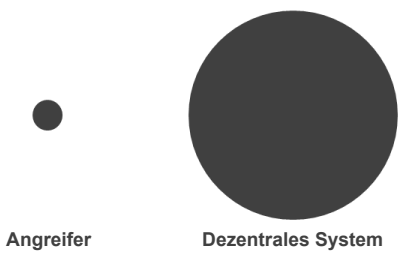

Abbildung 3: Verhältnis von Angreifer (Botnetz) und dezentralem System

Setzt man die durchschnittliche Rechenkapazität der Nutzer von BOINC für das Botnetz an, ergibt sich ein Wert von 3,70E+17 Ops/s. Dies ergäbe bereits 2,06% der gesamten Rechenleistung, würde das Botnetz für einen Angriff verwendet. Dieser Angreifer würde daher bereits bei einem dezentralen System mit einer Größe von 4% des Referenzsystems erfolgreich sein. In Abbildung 3 ist das Verhältnis von Angreifer und dezentralem Netzwerk dargestellt.

4.4.3 Virtueller Protest („Occupy Bitcoin“)

Zuletzt wird ein Angriff betrachtet, bei dem eine große Anzahl von Personen gemeinsam versucht, das System zu blockieren. Dadurch, dass die Block Chain durch eine dezentral agierende Masse geschützt wird, ist sie durch eine kollektiv angreifende Masse besonders verwundbar. Sie schafft damit eine Möglichkeit des virtuellen Protests. Finden sich genügend Teilnehmer, können sie gemeinsam die Block Chain blockieren, und so beispielsweise ihren Unmut über einen Krieg oder gierige Banker zum Ausdruck bringen.

Bewegungen wie Occupy Wall Street finden leicht Millionen von Anhängern aus aller Welt. Im Jahre 2003 protestierten gegen den Irakkrieg weltweit etwa 36 Millionen Menschen [Wi12b]. Für einen virtuellen Protest muss ein Teilnehmer, anders als heute üblich, nicht einmal seine Wohnung verlassen. Daher sind noch weitaus größere Teilnehmerzahlen vorstellbar. Für das Szenario nehmen wir an, dass 10% der Nutzer von Facebook für den Protest mobilisiert werden, was eine Anzahl von 84,5 Millionen Teilnehmern bedeutet.

Wird dieselbe durchschnittliche Rechenkapazität wie für das Botnetz angesetzt, erreichen die Angreifer zusammen 1,04E+18 Ops/s. Bezogen auf das dezentrale System sind das 5,59% der Gesamtleistung, was in Abbildung 4 dargestellt ist. Bereits bei einer Verkleinerung auf 12% der Referenzgröße ist dieser Protest erfolgreich.

Abbildung 4: Verhältnis von Angreifer (virtueller Protest) und dezentralem System

5 Implikationen

Mit der in diesem Aufsatz präsentierten Analyse wurde ein erster Schritt zur Beantwortung der Frage unternommen, ob sich eine durch eine Block Chain abgesicherte Währung tatsächlich rentiert. Dies ist nicht nur von wirtschaftlichem Interesse, da die für die Block Chain benötigte Rechenleistung mittelbar auch ökologische Kosten verursacht. Um Spekulationen auf ein Minimum zu reduzieren, wurde Annahmen auf Basis heutiger Technik getroffen. Darüber hinaus wurde kein Versuch unternommen, ein besonders realistisches Szenario zu entwerfen. Vielmehr war es Ziel, eine obere Schranke für Kosteneinsparung zu bestimmen.

Diese Analyse stellt die von [Fa11] oder [Na08] und anderen Bitcoin-Anhängern verbreiteten Hoffnungen auf massive Einsparungen in Frage. Im Vergleich zum heutigen EC-System wären selbst bei weltweiter Nutzung nur geringe Einsparungen möglich, ohne die Sicherheit des Systems aufs Spiel zu setzen. Eine solche Verbreitung erscheint jedoch sehr unwahrscheinlich. Auch die Kosten für die Einführung des Systems wurden ausgeklammert. Sicherlich würde dies geraume Zeit in Anspruch nehmen, in der das dezentrale System parallel zu seinen Alternativen verwendet würde. Entweder entstünden dadurch hohe Kosten, wenn es in voller Größe betrieben würde, oder eine verkleinerte Version wäre ständiger Bedrohung ausgesetzt. Wird letztlich noch die Unsicherheit bedacht, mit der unsere Schätzungen behaftet sind, wird klar, dass der behauptete Kostenvorteil nicht direkt offensichtlich ist und einer Begründung bedarf.

Aus hohen Kosten für die Block Chain ergäbe sich unter Umständen auch eine erhebliche Belastung für die Umwelt. Selbst mit der relativ „grünen“ Hardware, die in unserer Analyse zugrunde gelegt wurde, verursacht der Energiebedarf des Systems leicht einen CO_2-Ausstoß, der als Prozentsatz des aktuellen globalen Gesamtausstoßes angegeben werden kann. Darüber hinaus sind die Produktion der Hardware sowie die Infrastruktur des Netzwerks darin noch gar nicht enthalten. Dies zeigt, dass die ökologischen Konsequenzen einer Block Chain nicht notwendigerweise vernachlässigbar sind.

6 Zusammenfassung und weiterer Forschungsbedarf

In diesem Aufsatz wurde gezeigt, dass die Behauptung vieler Bitcoin-Anhänger, durch eine Block Chain abgesichertes elektronisches Geld reduziere die Kosten für Transaktionen, nicht über jeden Zweifel erhaben ist. Dies ist besonders im Hinblick auf den Stromverbrauch eines solchen Systems interessant. Soll es gegen jeden möglichen Angriff abgesichert werden, könnte der verursachte CO_2-Ausstoß schnell mit dem der globalen kommerziellen Luftfahrt gleichziehen. Es ist leicht vorstellbar, dass dies erheblichen Widerstand in der Bevölkerung hervorrufen würde.

Damit soll jedoch keinesfalls der Untergang von Bitcoin prophezeit werden. Die Schätzungen basieren, wie beschrieben, auf dem heutigen Stand der Technik. In der Zukunft könnte die Situation durch technische Innovation somit deutlich verändert werden. Die in der Analyse beschriebenen Kosten wären Rechtfertigung genug für spezialisierte Hardware, mit der Computer von Endnutzern nicht konkurrieren könnten. Dadurch könnten Angriffe weitaus unwahrscheinlicher werden, es stellt sich aber erneut die Frage nach der dezentralen Kontrolle derartig spezialisierter Hardware.

Darüber hinaus ist es auch vorstellbar, die von dem Netzwerk verbrauchte Energie zum Beheizen von Gebäuden zu verwenden. Das verringert zwar nicht den Energiebedarf, ermöglicht aber, an anderer Stelle Kosten einzusparen. Als dezentrales Netzwerk wäre dieses System dafür besonders geeignet. Neben der aufgewendeten Energie könnte auch die Rechenleistung selbst mehreren Zwecken dienen. Wäre es möglich, rechenintensive Probleme (z.B. Genomsequenzierung) mit der Block Chain zu verbinden, könnte deren Erstellung mit ohnehin anfallenden Berechnungen verbunden werden. Noch einen Schritt weiter gedacht, ist die Block Chain in ihrer Verwendung nicht unbedingt auf elektronisches Geld beschränkt. Beispielsweise können auch Commitment-Verfahren darauf aufbauen [Cl12]. Mit einer ausreichenden Anzahl Neuerungen in diese und andere Richtungen könnte in Zukunft auch eine noch weitaus mächtigere Block Chain gerechtfertigt sein. Wir hoffen, mit diesem Aufsatz solche Forschungen anzuregen.

Literaturverzeichnis

[An12] Anonymisiert: 2012. Abgerufen am 17.4.2012 von http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2041492

[Ba02] Back, A.: Hashcash – A Denial of Service Counter-Measure. 2002. Abgerufen am 9.4.2012 von http://www.hashcash.org/papers/hashcash.pdf

[Ba11] Bank for International Settlements: Statistics on payment, clearing and settlement systems in the CPSS countries – Figures for 2010, 2011.

[Ba12] Barber, S.; Boyen, X.; Shi, E.; Uzun, E.: Bitter to Better – How to Make Bitcoin a Better Currency. Proc. 16th Int. Conf. on Financial Cryptography and Data Security. Bonaire, Caribbean Netherlands, 2012.

[Be07] Belady, C. L.: In the data center, power and cooling costs more than the equipment it support. Electronics Cooling, 13(1), 2007; S. 24–27

[Bo12] Boincstats.com: BOINC Combined Project Statistics, 2012. Abgerufen am 16.2.2012 von http://boincstats.com/stats/project_graph.php?pr=bo

[BH08] Bradford, T.; Hayashi, F.: Developments in Interchange Fees in the United States and Abroad. Payments System Research Briefing, 2008.

[Bu11a] Burns, J. F.: Founder Says WikiLeaks, Starved of Cash, May Close. New York Times, 2011. Abgerufen am 9.4.2012 von http://www.nytimes.com/2011/10/25/world/europe/blocks-on-wikileaks-donations-may-force-its-end-julian-assange-warns.html

[Bu11b] Buterin, V.: The Wasted Electricity Objection to Bitcoin, Part II. Bitcoin Weekly, 2011. Abgerufen am 9.4.2012 von http://bitcoinweekly.com/articles/the-wasted-electricity-objection-to-bitcoin-part-ii

[CFN88] Chaum, D.; Fiat, A.; Naor, M.: Untraceable Electronic Cash. In (Goldwasser, S. Hrsg.): Advances in Cryptology – CRYPTO' 88, Santa Barbara, California, USA, 1988; S. 319–327

[CE12] Clark, J.; Essex, A.: CommitCoin: Carbon Dating Commitments with Bitcoin. Proc. 16th Int. Conf. on Financial Cryptography and Data Security. Bonaire, Caribbean Netherlands, 2012.

[Eu08] EURO Kartensysteme GmbH: Händlerbedingungen - Bedingungen für die Teilnahme am Electronic Cash-System der deutschen Kreditwirtschaft, 2008. Abgerufen am 16.2.2012 von http://www.electronic-cash.de/media/pdf/haendlerbedingungen.pdf

[Fa11] Falkvinge, R.: Banks: The Fourth Victim of Citizen's empowerment, 2011. Abgerufen am 9.4.2012 von http://www.youtube.com/watch?v=mjmuPqkVwWc

[Gr12] Green500.org: Green500, 2012. Abgerufen am 22.2.2012 von http://www.green500.org/

[Gr11] Greenberg, A.: WikiLeaks Asks For Anonymous Bitcoin Donations, Forbes, 2011. Abgerufen am 9.4.2012 von http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/

[Ie11] IEA: CO2 Emissions from Fuel Combustion 2011, 2011. Abgerufen am 16.2.2012 von http://www.iea.org/co2highlights/co2highlights.pdf

[Je11] Jeffries, A.: MyBitcoin.com Is Back: A Week After Vanishing With at Least $250 K. Worth of BTC, Site Claims It Was Hacked, BetaBeat.com, 2011. Abgerufen am 9.4.2012 von http://www.betabeat.com/2011/08/05/mybitcoin-disappeared-with-bitcoins/

[Lü07] Lübbert, D.: CO2-Bilanzen verschiedener Energieträger im Vergleich – Zur Klimafreundlichkeit von fossilen Energien, Kernenergie und erneuerbaren Energien, 2007. Abgerufen am 16.2.2012 von http://www.bundestag.de/dokumente/analysen/2007/CO2-Bilanzen_verschiedener_Energietraeger_im_Vergleich.pdf

[Ma09] Mankiw, N. G.: Principles of Economics. Book, 5. Aufl., South-Western Cengage Learning, Mason, OH, 2009.

[Na08] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Abgerufen am 16.2.2012 von https://www.crfdl.org/bitstream/handle/10838/959/bitcoin.pdf

[To12] TOP500.Org: Top500, 2012. Abgerufen am 20.2.2012 von http://top500.org/

[WW05] Weiner, S.; Wrigth, J.: Interchange fees in various countries: Developments and determinants. Review of Network Economics, 4(4), 2005; S. 290-323.

[Wi12a] Wikipedia: Botnet, 2012. Abgerufen am 9.4.2012 von http://en.wikipedia.org/wiki/Botnet

[Wi12b] Wikipedia: Protests against the Iraq War, 2012. Abgerufen am 9.4.2012 von http://en.wikipedia.org/wiki/Protests_against_the_Iraq_War

[Zh08] Zhu, Z.; Lu, G.; Chen, Y.; Fu, Z. J.; Roberts, P.; Han, K.: Botnet Research Survey. Computer Software and Applications, (COMPSAC'08), Turku, Finland, 2008; S. 967-972.