Bitcoin und E-Commerce

Dennis Assenmacher
Westfälische Wilhelms-Universität Münster
Institut für Witschaftsinformatik
Leonardo-Campus 3
48149, Münster
d_asse01@uni-muenster.de

ABSTRACT

Sowohl reale als auch virtuelle Währungen müssen, um sich langfristig in der Gesellschaft etablieren zu können, alle notwendigen Geldfunktionen erfüllen. Die Tauschmittelfunktion, als bestimmendes Geldkriterium, ist dabei besonders zu beachten. Bitcoin, das neue, dezentrale Peer-to-peer Zahlungssystem, steht heute vor der Herausforderung, eine händlerseitige Akzeptanz dieser digitalen Währung zu schaffen und die Zahl der anfallenden Transaktionen zu maximieren. In dieser Seminararbeit werden die wesentlichen Vor- bzw. Nachteile der Nutzung von Bitcoin als Zahlungsmittel, im Bereich des E-Commerce, betrachtet. Dabei liegt der Fokus der Ausarbeitung auf der Aufstellung von Anforderungen an elektronische Zahlungssysteme und der Abschätzung, inwieweit Bitcoin diese erfüllen kann. Sowohl die Möglichkeit der unternehmenseigenen Verwaltung von Bitcoins als auch das Auslagern an externe Dienstleister wird diskutiert und einem Vergleich unterzogen. Final wird, auf Basis der theoretischen Erkenntnisse, eine Handlungsempfehlung für Unternehmen entwickelt, die in Zukunft Bitcoin als Zahlungsmittel in ihren Online- Shops akzeptieren wollen.

1. EINLEITUNG

Geld ist in der heutigen Gesellschaft nicht mehr wegzudenken. Der einstige Naturalientausch, der bereits vor tausenden von Jahren von Menschen praktiziert wurde, ist heute größtenteils durch Währungen substituiert worden[15]. Auch wenn sich in der Geschichte der Menschheit immer wieder Probleme mit verschiedenen Währungen und Geldformen beobachten lassen, scheint das Vertrauen in Geld immer weiter zu bestehen. Nach der Definition von Geoffrey Crowther muss Geld drei wichtige Funktionen erfüllen: Wertaufbewahrungs, Rechen- und Tauschmittelfunktion[17]. Geld muss also erbrachte Leistung in gewisser Weise konservieren, um diese später gegen geeignete Äquivalente, seien es Sach- oder Dienstleistungen, einzutauschen. Den Fokus legt Crowther ganz klar auf die Tauschmittelfunktion. Der konkrete Vorgang des Tausches, also die gegenseitige Übertragung von Gütern, wird Transaktion genannt. Geld oder eine Währung kann langfristig also nur dann überleben, wenn es allgemein akzeptiert wird und viele Transaktionen stattfinden.

Handel und Transaktionen im Internet werden heutzutage fast ausschließlich über Banken und andere Institutionen wie Paypal abgewickelt[20]. Ihnen wird Vertrauen entgegengebracht und sie schützen, bis zu einem gewissen Grad, vor Betrug. Für diesen Service, Risikoaufschläge und Betriebskosten verlangen sie verschiedene Gebühren. Es gibt neben Gebühren für die Kontoführung auch Gebühren pro Transaktion. Daraus ergibt sich teilweise ein großes Problem für Händler: Die untere Preisschranke für Transaktionen steigt. Gerade im E-Commerce Bereich rentieren sich Transaktionen, die in den Micropayment Bereich fallen, nur teilweise oder gar nicht. [15]

Bitcoin geht einen neuen Weg und könnte sich für Unternehmen im E-Commerce Bereich als geeignetes elektronisches Zahlungssystem durchsetzen. Eine konkrete Aussage bezüglich der Eignung von Bitcoin als Zahlungsmittel kann jedoch erst auf Basis einer detaillierten Anforderungsanalyse von elektronischen Zahlungssystemen geschehen. Ein fundamentales Verständnis des gesamten Bitcoin Protokolls ist notwendig, um den Nutzen des Systems, unter Berücksichtigung der verschieden Anforderungen, zu quantifizieren. Im Folgenden werden systematisch relevante Anforderungen an Zahlungssysteme dargestellt und kategorisiert. Anschließend wird das Bitcoin Protokoll und dessen technische Implementierung erläutert, um darauf aufbauend eine Nutzenanalyse hinsichtlich der aufgestellten Anforderungen durchzuführen.

Online Händler müssen sich nicht zwangsläufig in das Bitcoin System einarbeiten und ein tiefes technisches Verständnis der Architektur entwickeln, um die Währung als Zahlungsmittel zu akzeptieren. Unternehmen wie Bitpay, BIPS uvm. haben sich darauf spezialisiert, Komplettlösungen für Händler zu entwickeln. Gegen eine fixe oder variable Gebühr ermöglichen diese Dienstleister, Bitcoin im Rahmen von Online Geschäftstätigkeiten zu akzeptieren. Sie stellen sowohl die nötige Infrastruktur, als auch das nötige Fachwissen zur Verfügung, um es den Händlern zu ermöglichen Transaktionen mit Bitcoin zu tätigen. Diese Angebote werden hinsichtlich verschiedener Kriterien untersucht und anschließend wird eine Handlungsempfehlung für E-Commerce Unternehmen entwickelt die zwei Ansprüche erfüllen soll: Erstens soll ein Rahmen vorgegeben werden, in dem es sich für Online Shops lohnt, Bitcoin als Währung zu akzeptieren. Darauf aufbauend soll zweitens ein Leitfaden entwickelt werden, der für verschie-

dene E-Commerce Einsatzszenarien konkrete Realisierungen vorschlägt.

2. GRUNDLAGEN DES E-COMMERCE

Durch die wachsende technische Infrastruktur haben immer mehr Menschen dauerhaft Zugang zum Internet[31]. Dieses neue Medium ermöglicht zwischen den einzelnen Nutzern, aber auch zwischen Unternehmen und Kunden, neue Wege, Transaktionen abzuschließen. Laut einer BITKOM Studie aus dem Jahr 2012 kaufen 9 von 10 Kunden Waren im Internet ein, 40% davon regelmäßig[10]. Die Entwicklung eines einheitliches Verständnisses bezüglich der Begrifflichkeiten und Fachtermini im Bereich des E-Commerce ist für eine Untersuchung und Analyse möglicher Zahlungssysteme daher eine wichtige und notwendige Maßnahme.

2.1 Definition und Klassifikation

Bevor die Eignung von Bitcoin im Bereich des E-Commerce untersucht werden kann, ist eine formale Definition und Klassifizierung dieses Begriffes notwendig. Allgemein lässt sich in der wissenschaftlichen Literatur keine einheitliche Definition vorfinden[22]. Merz definiert E-Commerce beispielsweise als „*die Unterstützung von Handelsaktivitäten über Kommunikationsnetze*“[26][S.18]. Aus dieser, eher abstrakten Beschreibung lassen sich unterschiedliche Anwendungsbereiche ableiten: Digitales Geld, Shopping-Malls, Smart Cards etc. Eine weitere Definition findet sich bei Laudon und Taver: „*The use of the Internet and the Web to transact Business. More formally, we focus on digitally enabled commercial transactions between and among organizations and individuals*“[33][S.10]. Eine Übersicht aller relevanten Definitionen lässt sich bei Lars Jäger finden.[22] Allgemein lässt sich feststellen, dass alle Definitionen den Fokus auf die elektronisch unterstützte Tausch bzw Handelsfunktion zwischen zwei oder mehreren Transaktionspartnern legen. Dabei wird je nach Detaillierungsgrad zwischen den einzelnen Phasen einer Transaktion unterschieden.

Die Bereiche des E-Commerce können durch einen eindimensionalen Klassifikationsrahmen beschreiben werden. Dieser richtet sich nach den, an der Transaktion beteiligten, Akteuren. Zwei Rollen sind hier allgemein zu beobachten: der Käufer, Kunde oder Konsument und der Verkäufer oder Händler. Beide Rollen können von verschiedenen juristischen Personen eingenommen werden. Dabei kann es sich sowohl um reale Personen, als auch um Institutionen, wie Unternehmen oder Staaten handeln. Merz stellt einige dieser Zweierbeziehungen heraus: *Business-to-Business-*, *Business-to-Consumer-* und *Consumer-to-Consumer-Commerce*[26]. Im Rahmen dieser Seminararbeit liegt der Fokus auf dem *Business-to-Consumer-Commerce*, also dem Bereich des Massengeschäftes mit dem Endkunden und den *Consumer-to-Consumer* Bereich. Diese Spezialisierung ist notwendig, da sich die Anforderungen an Zahlungssysteme in diesen Bereichen voneinander unterscheiden.[22][S.36]

2.2 Kaufprozess

Der E-Commerce Kaufprozess unterscheidet sich auf den ersten Blick nur geringfügig von dem des traditionellen Handels. Dabei besteht eine Transaktion generell aus drei Phasen: Informationsphase, Vereinbarungsphase und Abwicklungsphase[26][S.26f], [18][S.10ff]. Während der Informationsphase beobachtet der potentielle Käufer den Markt. Er sammelt alle nötigen Informationen über das gewünschte Produkt und vergleicht Preise zwischen den Anbietern. In der Vereinbarungsphase trifft der Kunde die Entscheidung, welche der vorhandenen Alternativen er erwerben möchte, also auch bei welchem Händler er die Transaktion durchführen will. Dies geschieht aufgrund von vorigen Verhandlungen.

Abschließend wird in der Abwicklungsphase das eigentliche Tauschgeschäft durchgeführt. Dazu gehören sowohl die Übermittlung der Zahlung als auch die Distribution des jeweiligen erworbenen Gegenstandes.

Auch bei traditionellen Handelsbeziehungen werden diese drei Phasen durchlaufen. Der Unterschied ist offensichtlich: Bei E-Commerce Kaufprozessen finden alle drei Phasen im Internet statt und werden durch Produktkataloge, virtuelle Verkaufsräume und Suchdienste unterstützt[24][S.40], während im traditionellen Kaufprozess der persönliche Kontakt, gerade in Phase 2 und 3, gegeben ist. Die daraus entstehenden Informationsasymmetrien haben weitreichende Folgen für die Anforderungen an elektronische Zahlungssysteme. Der Nachfrager hat keine Informationen über die Seriosität des Anbieters und die Qualität der Leistung bzw. des Produktes, da er in diesem virtuellen Markt außerhalb des Kontaktkreises des Kunden liegt[24][S.80]. Auch der Händler ist von diesen Asymmetrien betroffen. So muss er sich um die Seriosität des Kaufauftrages und den Zahlungswillen des Kunden Gedanken machen. Aufgrund des unpersönlichen Kontaktes und den damit verbundenen Unsicherheiten sind beide Parteien, sowohl Händler als auch Käufer, also darauf angewiesen, dem Medium und dem Zahlungssystem Vertrauen entgegenzubringen und sicherzustellen, dass die jeweiligen Funktionalitäten ihre Interessen unterstützen.

3. ANFORDERUNGEN AN ELEKTRONISCHE ZAHLUNGSSYSTEME

Unter elektronischen Zahlungssystemen oder E-Payment-Systemen definiert man „*Verfahren, die es ermöglichen, für den Bezug von Gütern und Dienstleistungen eine Gegenleistung über elektronische Netzwerke zu erbringen und deren Ziel allein die Herstellung der Zahlungsfähigkeit von Wirtschaftssubjekten ist*“[22]. Unbedingt abzugrenzen ist ein elektronisches Zahlverfahren von einem Zahlungsmittel. Das Verfahren beschreibt den Vorgang der Zahlung, also in welcher Weise das Zahlungsmittel übertragen wird. Das Mittel wiederum ist lediglich ein Objekt mit einem gewissen Wert, das zur Begleichung der Verbindlichkeit übergeben wird[22][S.41]. Traditionelles Geld ist hier nur als ein mögliches Zahlungsmittel zu nennen. Gerade im elektronischen Bereich haben sich verschiedene Zahlungsmittel herausgebildet.

Wie in der Analyse des Kaufprozesses bereits angedeutet wurde, sind die kunden- bzw. händlerseitigen Anforderungen an Zahlungssysteme, gerade im Bereich des E-Commerce, dem fehlenden persönlichen Kontakt der beiden Parteien geschuldet. Der Händler hat keinerlei Informationen über den Kunden und weiß nicht, ob dieser überhaupt zahlungsfähig ist oder nicht. Der Kunde wiederum weiß nicht, ob der Händler vertrauenswürdig ist und die Ware auch wirklich besitzt. Die Sicherheit des Zahlungssystems ist also für beide Parteien relevant. Dies deckt sich auch mit Ergebnissen der Online Umfrage der Universität Karlsruhe aus dem Jahr

2008[25]. In dieser Studie wurden die wichtigsten Kriterien hinsichtlich der Wahl von Zahlungssystemen auf Seiten der Verbraucher ermittelt. Nahezu alle Verbraucher gaben an, dass die Sicherheit des Systems ein wichtiges Kriterium bzgl. der Entscheidung der Nutzung eines Systems sei. Auch Heng bezeichnet die empfundene Sicherheit als *„Absolutes KO-Kriterium des E-Business*“[19]. Weitere relevante Kriterien sind: Einfache Handhabung, Verbreitung des Verfahrens, Bekanntheit und internationale Einsetzbarkeit. Auch auf Seiten der Händler kann der Wunsch nach einem sicheren System verifiziert werden. So ergab eine Kurzumfrage der Universität Regensburg, dass Kosten und Sicherheitsaspekte die wichtigsten Faktoren für die Auswahl der Zahungsverfahren sind[30][S.14]. Weiter wurde festgestellt, dass die Verbreitung, der Schutz vor Zahlungsausfällen und die Kosten die Hauptanforderungen für die Einführung neuer Zahlungssysteme darstellen.

Der Versuch, die Anforderungen an elektronische Zahlungssysteme strukturiert darzustellen, wurde in der wissenschaftlichen Literatur bereits mehrfach unterschiedlich angegangen[32, 22]. Ein einheitliches Klassifikationsschema lässt sich jedoch nicht aus den jeweiligen Quellen extrahieren. Konsens herrscht lediglich hinsichtlich der Gruppierung in allgemeine Anforderungen und spezielle Anforderungen. Unter allgemeinen Anforderungen versteht Henkel eine „*Reihe von Anforderungen an Zahlungsverfahren, die so selbstverständlich erscheinen, dass man sie beinahe übersehen könnte*“[32][S.106]. Darunter fallen, neben den bereits erwähnten Sicherheitsanforderungen, die Reputation und Verlässlichkeit, Internationalität und Fälschungssicherheit, Konvertierbarkeit, Umlauffähigkeit. [22][S.219]

Obwohl sowohl der Kunde als auch der Händler die technische Sicherheit als eine der wichtigsten Anforderungen an elektronische Zahlungssysteme angeben, geben die Umfragen keinen Aufschluss darüber, was genau unter einem sicheren System verstanden wird[25], [30]. Hierfür ist eine Analyse bestehender Literatur notwendig. Aufgrund der großen Anzahl an unterschiedlichen Sicherheitsanforderungen, die sich dort finden lassen, lohnt es sich, diese weiter zu klassifizieren. Henkel bedient sich dabei dem aus der Informatik bekannten Akronym ACID. ACID steht für Atomicity, Consistency, Independence und Durability[32][S.106]. Dies sind die Eigenschaften, die für Datenbankmanagement- sowie verteilte Systeme, also auch elektronische Zahlungssysteme, nötig sind. Im Folgenden werden kurz alle Eigenschaften erläutert, da der im Kontext dieser Ausarbeitung verwendete Klassifikationsrahmen diese Anforderungen auch berücksichtigt.

Atomicity (Atomarität) beschreibt die Anforderung, dass eine Transaktion entweder vollständig ausgeführt wird oder gar nicht. Dabei wird eine Transaktion als atomarer Ausführungsschritt betrachtet, die nicht von anderen Prozessen unterbrochen werden kann.

Consistency (Konsistenz) beschreibt einen Zustand, in dem zu jedem Zeitpunkt alle Parteien die gleichen Informationen bezüglich einer Transaktion besitzen. Jede Transaktion muss ein konsistentes System wiederum in einen konsistenten Zustand überführen.

Independence (Unabhängigkeit) der Transaktionen wird gefordert, um zu verhindern, dass Transaktionen sich gegenseitig beeinflussen.

Der Begriff Durability (Dauerhaftigkeit) sagt aus, dass alle Daten, also alle geführten Transaktionen die jemals getätigt wurden, dauerhaft im System bleiben. Dies gilt insbesondere für Systemausfälle aufgrund von Hardwarefehlern.

Eine weitere Sicherheitsanforderungen stellt die Fälschungssicherheit dar. Gerade bei Systemen im Bereich des Electroinc Cash ist dies eine unabdingbare Eigenschaft, die eingehalten werden muss. Dies bedeutet insbesondere, dass digitales Geld nicht beliebig vervielfältigt werden kann und doublespending[1] auf einer technischen Basis verhindert wird.[32]

Integrität stellt sicher, dass Transaktionen während der Übertragung nicht verändert werden können. Dies betrifft sowohl die absichtliche, als auch die unabsichtliche Änderung von Daten.

Nichtabstreitbarkeit stellt die Anforderung dar, dass Zahlungssysteme so konstruiert werden, dass alle Transaktionen zu einem beliebigen Zeitpunkt nachzuvollziehen sind[22][S.221]. Damit wird sichergestellt, dass die Beteiligten der Transaktion diese nicht leugnen können[22][S.221].

Diese allgemeinen Sicherheitsanforderungen sind essentielle Bestandteile eines Zahlungssystems und müssen unbedingt erfüllt werden[19][S.422]. Daneben existieren weitere Anforderungen, die im Rahmen dieser Arbeit in Händler bzw. Verbraucheranforderungen kategorisiert werden.[19] [32][S.107ff]

Auf Seiten der Händler sind hohe Verbreitung bei Kunden, niedrige Gesamtkosten und Zahlungsgarantie als die wichtigsten Anforderungen festzustellen[19, 35, 20],[32][S.113]. Letztere steht im Interessenskonflikt mit der Anforderung des Kunden nach der Möglichkeit des Widerrufes der Zahlung. Da Rückbuchungen generell mit zusätzlichen Gebühren auf Seiten der Händler verbunden sind, stellt die jeweilige Rückbuchungsquote einen wesentlichen Faktor für den Erfolg des Unternehmens dar[19][S.421]. Unter dem Aspekt der niedrigen Gesamtkosten fallen sowohl monetäre Größen wie Transaktions- bzw. Einrichtungskosten als auch nicht monetäre Größen wie schneller Zahlungseingang und Aufwand der Integration in bestehende Shopsysteme[35][S.302].

Bei Kunden ist zu beobachten, dass neben allgemeinen Sicherheitsanforderungen der Wunsch nach einer einfachen Handhabung des Systems dominiert[25][S.32]. Darunter fällt der Einstiegsaufwand, wie die Beschaffung von digitalen Zertifikaten und Hard- bzw. Software, aber auch der Aufwand, der mit dem Erlernen des Verfahrens verbunden ist[32][S.108f]. Auch die Verbreitung des Verfahrens auf Seiten der Händler ist von Relevanz [25][S.32].

Neben den voneinander unabhängigen Anforderungen der Händler und Verbraucher existieren Anforderungen, die im Widerspruch zueinander stehen. Dies sind auf Seiten der Kunden die Forderung nach Anonymität und der Möglichkeit des Widerrufes einer Transaktion[35][S.23], [19][S.422]. Der Händler besitzt hingegen Interesse daran, möglichst viele

[1] Mehrfaches Bezahlen mit der gleichen Währungseinheit siehe Kapitel 4.2

Händler	Allgemein	Kunden
• Hohe Verbreitung • Niedrige Gesamtkosten – Transaktionskosten – Einrichtungskosten – Schnelle Zahlungen – Aufwand der Integration • Zahlungsgarantie • Viele Informationen	• Technische Sicherheit – Atomarität – Konsistenz – Unabhängigkeit – Dauerhaftigkeit – Fälschungssicherheit – Integrität – Nichtabstreitbarkeit – Authentifizierung • Internationalität • Umlauffähigkeit • Hohe Verbreitung	• Hohe Verbreitung • Einfache Handhabung • Anonymität • Widerrufbarkeit

Tabelle 1: Anforderungen an Zahlungssysteme im E-Commerce in Anlehnung an Henkel, Heng und Jäger

Informationen über den Kunden zu erhalten, um sich so vor Zahlungsausfall abzusichern. Tabelle 1 gibt eine Übersicht über die, in diesem Kapitel erarbeiteten Anforderungen.

Im nachfolgenden Kapitel wird die technische Implementierung des Bitcoin Protokolls vorgestellt, um darauf aufbauend eine Analyse der Eignung als elektronisches Zahlungssystem anhand der vorgestellten Anforderungen durchführen zu können.

4. DAS BITCOIN PROTOKOLL: TECHNISCHE GRUNDLAGEN

Im Jahr 2008 erarbeitete Satoshi Nakamoto, dessen wahre Identität bis heute nicht bekannt ist, in seinem Beitrag "Bitcoin: A Peer-to-Peer Electronic Cash System", ein dezentrales Peer-to-Peer Zahlungssystem, das versucht, die Dominanz von zentralen Institutionen, wie Staat oder Banken, im Bereich des Internethandels anzufechten.[28] Ohne Kreditkarte, Lastschriftverfahren oder Online-Services wie Paypal war es zu diesem Zeitpunkt nur schwer möglich, Güter oder Dienstleistungen online zu erwerben. Banken boten als zentrale, überwachende Institutionen als einzige die Möglichkeit, das sogenannte double-spending Problem zu verhindern.

Unter double-spending versteht man im Kontext des digitalen Geldes die Möglichkeit, dass eine Geldeinheit theoretisch beliebig oft kopiert und vervielfacht werden kann und eine Person A dadurch mehr Geld ausgegeben kann als sie eigentlich besitzt. Die Banken und andere Services wie Paypal repräsentieren hier eine zentrale Instanz, über die alle elektronischen Transaktionen abgewickelt werden. Sie stellen sicher, dass jede Währungseinheit, die sich im Besitz einer Person befindet, auch genau einmal ausgegeben wird[15]. Oberstes Ziel war es also, ein System zu entwerfen, welches unabhängig von zentralen Instanzen Transaktionen ausführen kann, und gleichzeitig double-spending verhindert. Im Folgenden werden die zentralen technischen Aspekte von Bitcoin, die eine Realisation dieser beiden Bedingungen ermöglichen, vorgestellt.

4.1 Konten und digitale Signaturen

Eine Währungseinheit in Bitcoin wird *coin* genannt. Ein *coin* kann wiederum in nach dem Erfinder benannte Satoshi's unterteilt werden. Ein STC entspricht dabei 0.00000001 BTC. Wollen zwei Parteien über elektronische Medien miteinander handeln, also eine Transaktion durchführen, muss sichergestellt werden, dass der Empfänger eindeutig identifizierbar ist. Dies entspricht der Anforderung der Authentifizierung. Im Bankensystemen besitzt jeder Kunde ein Konto mit einer eindeutigen Kontonummer. Wird nun eine Transaktion durchgeführt, kann diese Nummer als Zieladresse angegeben werden. Weiter muss sichergestellt werden, dass nicht jede Partei beliebig viele Transaktionen durchführen kann, sondern nur in der Lage ist, von dem eigenen Konto Geld zu verschicken.

Dieses Problem löst Bitcoin mit einem asymmetrischen Kryptosystem. Der öffentliche Schlüssel k_{pub} repräsentiert das Konto und ermöglicht das Empfangen von Beträgen, während der private Schlüssel k_{priv}, durch die Fähigkeit Nachrichten digital zu signieren, das Senden ermöglicht. Eine Bitcoin Adresse, also ein öffentlicher Schlüssel, besteht im Allgemeinen aus einer Folge von 27-32 zufällig erzeugten, alphanumerischen Symbolen. Die Erzeugung eines Schlüssels kann von dem jeweiligen Bitcoin Client offline durchgeführt werden und erfordert zu vernachlässigenden Rechenaufwand. Dies ist der Grund, dass eine Person nicht nur ein (k_{pub}, k_{priv}) Schlüsselpaar besitzt, sondern viele verschiedene. Diese werden alle zusammen in einer digitalen Geldbörse, der E-Wallet, gespeichert und verwaltet. So ist es theoretisch möglich, jede Transaktion mit einer eigenen, nur diesem Zweck dienenden Kontonummer zu tätigen. Auch Online Händler können von dieser Möglichkeit profitieren. So ist es beispielsweise möglich, dass jede Bestellung an eine eigene Adresse geknüpft ist. Der Händler kann also diese Adresse überwachen und weiß sofort, wann der Kunde bezahlt hat.

4.2 Transaktionen und Blockchain

Bitcoin ist ein Peer-to-Peer Zahlungssystem. Es ist daher offensichtlich, dass Transaktionen direkt zwischen Sender und

Empfänger stattfinden und keine Instanz dazwischen steht. Nachfolgend wird ein Überblick über die Funktionsweise von Transaktionen und der Aufbau der Blockchain gegeben.

Nakamoto definiert ein *coin* als eine Kette von digitalen Signaturen[28]. Jede Transaktion repräsentiert ein Glied dieser Kette. Will nun eine Person A einer Person B ein Bitcoin schicken, fügt sie an das Ende der Kette ein neues Glied hinzu, indem folgende Schritte geschehen:

- Die neue Transaktion, inklusive eines Hashes der vorigen Transaktion und dem öffentlichen Schlüssel des Empfängers B wird mit dem privaten Schlüssel von A signiert.
- Die neue Transaktion kann vom Empfänger B der Transaktion verifiziert werden.

Abbildung 1 enthält eine vereinfachte Visualisierung einer Transaktionskette eines *coins* nach Nakamoto.

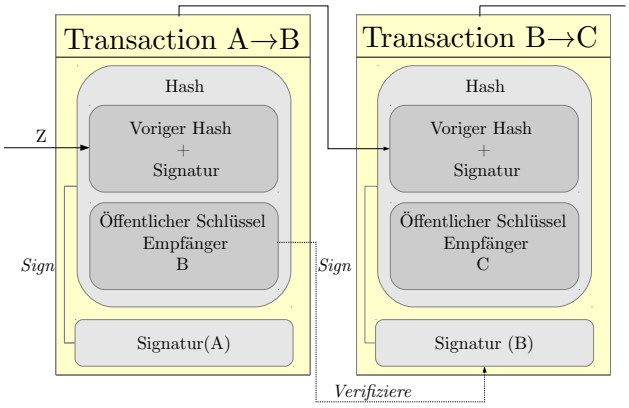

Abbildung 1: Transaktion

Problematisch ist nun noch der Umstand, dass A simultan zwei verschiedene Transaktionen erstellen kann, die sich nur darin unterscheiden, dass die Schlüssel der Empfänger unterschiedlich sind. A schickt also den *coin* sowohl an B als auch an C. Man spricht hier vom double-spending Problem. Zentrale Instanzen können dieses Problem verhindern, indem jede Transaktion einzeln überprüft wird und so zu jedem Zeitpunkt ein konsistenter Zustand erreicht wird.[28]

Bitcoin löst dieses Problem, indem jede einzelne Transaktion öffentlich gemacht wird, was dazu führt, dass alle Teilnehmer sich gegenseitig überwachen können. Weiter muss es einen Zustand an gültigen Transaktionen geben, auf den sich alle Teilnehmer einigen. Dies wird mit der sogenannten Blockchain und dem damit verbundenen Proof-of-Work erreicht.

Die Blockchain definiert einen gültigen Status des Protokolls. Alle Clients müssen, um erfolgreich am System teilzunehmen, diesen Status akzeptieren. Ein Block besteht allgemein aus einem *header* und einem *body*. Im *body* befindet sich eine Sammlung von Transaktionen. Die durchschnittliche Anzahl von Transaktionen in einem Block A_t, auf Basis der Daten der kompletten Blockchain, beträgt 76.79096. Der *header* ist die zweite, den Block bestimmende Komponente. Hier wird, neben einer 32 Bit Nonce, ein SHA-256 Hash des unmittelbaren Vorgängers gespeichert. Findet nun eine Transaktion statt, wird diese initial über das Netzwerk verteilt. Alle Teilnehmer, die die Transaktion empfangen, speichern diese lokal in ihren eigenen Blöcken. Es ist zu beachten, dass diese Blöcke nur lokal gelten und noch nicht als gültiger Zustand akzeptiert werden. Damit ein Block an das Ende der Blockchain hinzugefügt werden kann, und alle darin enthaltenen Transaktionen gültig werden, versuchen die Teilnehmer, ihre Blöcke so zu hashen, dass folgende Bedingung erfüllt wird:

- $b_{SHA} \leq t$, wobei b_{SHA} der SHA-256 Hash des Blockes b und t das sogenannte target repräsentieren.

b_{SHA} muss also eine bestimmte Restriktion erfüllen. Durch die Möglichkeit, t beliebig zu wählen, kann das System die Schwierigkeit variieren und so die Erfolgswahrscheinlichkeit der Suche verringern oder erhöhen.Das Bitcoin Protokoll ist so konzipiert, dass das target so gewählt wird, dass es im Schnitt 10 Minuten dauert bis ein neuer, gültiger Hash gefunden wird. Die Nonce, die sich im header befindet dient dem Zweck neue Hashes des Blocks zu finden. Wird der Wert der Nonce verändert, verändert sich auch der Output der Hashfunktion.

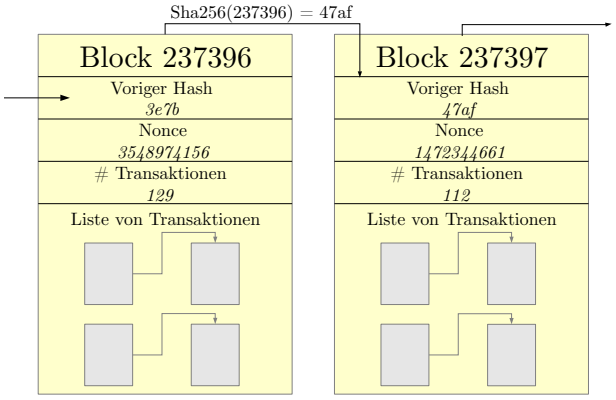

Abbildung 2: Blockchain

Die Notwendigkeit der Berechnung von gültigen Blöcken ergibt sich aus dem Umstand, dass überprüft werden muss, ob demjenigen, der den neuen Block veröffentlicht hat, Kosten entstanden sind. Könnte jeder Teilnehmer des Systems beliebig neue Blöcke veröffentlichen und würde die Akzeptanz nur auf Basis des Mehrheitsprinzips beruhen, wäre ein Sybil Angriff nicht auszuschließen . Der *proof-of-work* ist somit notwendig, um die Kompromittierung des Systems zu verhindern. Abbildung 2 zeigt zwei aufeinanderfolgende Blöcke der Blockchain mit den Blocknummern 237396 und 237397 inklusive aller relevanten Informationen.

Im Bezug auf Online Shops und deren Bitcoin Transaktionen hat dies weitgreifende Folgen: Es kann erst dann sichergestellt werden, dass eine Transaktion allgemeine Gültigkeit besitzt,

wenn die Transaktion in der Blockchain veröffentlicht wurde. Im Schnitt muss der Verkäufer also 10 Minuten warten, ehe er seine Leistung erbringen kann. In Kapitel 3.3 wird diese Erkenntnis speziell für fast-payment noch einmal aufgegriffen und auf die Geschwindigkeitsanforderung untersucht.

Für die Berechnung von gültigen Hashes ist Rechenleistung notwendig. Direkt damit verbunden sind Kosten, die beispielsweise durch den Stromverbrauch der Computer anfallen. Hier entsteht ein offensichtliches Dilemma: Um die volle Funktionalität des Systems zu garantieren, also double-spending auszuschließen, müssen die Teilnehmer kontinuierlich nach gültigen Blöcken suchen, was wiederum Kosten verursacht. Keine gültigen Blöcke zu suchen und somit die Gefahr des Systemausfalles zu fördern, erscheint unter diesen Bedingungen eine rationale Handlungsempfehlung. Bitcoin löst dieses Dilemma mit einem Anreizsystem: Jeder gefundene Block berechtigt zur Generierung einer bestimmten Anzahl von Bitcoins durch eine initiale Transaktion. Es ist die einzige Möglichkeit, *coins* zu erzeugen und in den Umlauf zu bringen. Das Problem der initialen Verteilung der Währung wird damit nebenbei gelöst. Die Belohnung für das Finden eines Blockes betrug anfänglich 50 BTC und wird nach jeweils 210.000 Blöcken halbiert[4]. Die maximale Anzahl der sich jemals im Umlauf befindlichen Bitcoins kann folgendermaßen berechnet werden:

$$\sum_{k=0}^{\infty}(210.000 * 50 * \frac{1}{2}^{k}) \overset{geom}{=} \frac{10.500.000}{1-\frac{1}{2}} = 21.000.000$$

Insgesamt werden in Zukunft also höchstens 21 Millionen Bitcoins im Umlauf sein. Berücksichtigt man, dass die kleinste Stückelung von *coins*, also ein Satoshi genau 0.00000001 BTC betragen, lässt sich die Anzahl an Blöcken bestimmen, die benötigt werden, um alle Bitcoins auszuschütten. Es ist zu beachten, dass dreiviertel der maximalen Bitcoins bereits nach ca. 420.000 Blöcken also nach ungefähr 8 Jahren ausgeschüttet werden.

Hinsichtlich der Anforderungen an elektronische Zahlungssysteme kann also zusammengefasst werden: Das Verhindern von double-spending Angriffen durch Einführung eines Mehrheitsprinzips und die gegenseitige Überwachung garantieren Fälschungssicherheit.[2] Dies geschieht jedoch auf Kosten der Konsistenz, da ein konsistenter Zustand nur mit einer gewisser Wahrscheinlichkeit garantiert werden kann. Langfristig kann jedoch davon ausgegangen werden, dass das System einen gültigen Zustand erreicht. Weiter ist zu beachten, dass Transaktionen sich nicht gegenseitig beeinflussen können, was die Anforderung nach Unabhängigkeit gewährleistet. Auch Dauerhaftigkeit und Nichtabstreitbarkeit sind solange gewährleistet, wie Nutzer an dem Peer-to-peer System teilnehmen. Die Nichtabstreitbarkeit resultiert daraus, dass die Blockchain zentraler Aspekt des Bitcoin Protokolles ist und für jeden einsehbar und abrufbar ist. Alle jemals getätigten Transaktionen können also nachvollzogen werden. Das asymmetrische Kryptosystem und die verwendeten digitalen Signaturen garantieren eine eindeutige Authentifizierung und die Integrität des Systems. Nur mit dem privaten Schlüssel hat man das Recht, Transaktionen mit dem dazugehörigen öffentlichen Schlüssel zu tätigen

[2]unter der Voraussetzung das lange genug gewartet wird

4.3 Wallet

Nachdem nun die allgemeine Funktionsweise von Bitcoin erläutert wurde, konzentriert sich dieser Abschnitt auf die in der Einleitung bereits erwähnte Wallet. Eine Wallet kann naiv als eine Bitcoin Geldbörse betrachtet werden. Es ist ein Ort, an dem die privaten und die dazugehörigen öffentlichen Schlüssel gespeichert werden. Zugriff auf die Wallet impliziert volle Kontrolle über alle Bitcoins. Die Sicherheit der Wallet ist folglich eines der primären Themen, mit denen sich Bitcoin User auseinandersetzen müssen. Gerade im Bereich des E-Commerce sollten Händler sicherstellen, dass ihre Schlüssel gesichert sind, denn mit den privaten Schlüsseln kann leicht auf alle Einnahmen zugegriffen werden. Es gibt verschiedene Möglichkeiten, die eigenen Schlüssel oder die ganze Wallet zu speichern, auf die im Folgenden näher eingegangen wird.

4.3.1 Desktop Clients

Desktop Clients speichern lokal eine Datei, die alle auf dem Computer gespeicherten Schlüsselpaare (k_{pub}, k_{priv}) enthält. Da es zur Zeit keine formal einheitliche Spezifikation des Bitcoin Protokolls gibt, unterscheiden sich die Inhalte der Wallet-Datei von Client zu Client. Der ursprüngliche Client speichert in der wallet.dat einen Pool von Schlüsselpaaren, die damit verbundenen Transaktionen, einen defaultkey als Standardadresse und weitere zusätzliche Informationen. Wallets, die kontinuierlich mit dem Internet verbunden sind, werden Hot Wallets genannt.[6] Das Pendant zu der Hot Wallet ist die Cold Wallet. Diese zeichnet sich dadurch aus, dass es keine direkte oder indirekte Verbindung zum Internet gibt, der Computer also nicht über das Netzwerk kontaktiert werden kann.

4.3.2 Online Wallets

Die Verwendung einer Online Wallet ist der leichteste Weg, Bitcoins zu verwalten, da von jedem internetfähigen Computer auf sie zugegriffen werden kann[13]. Externe Anbieter sichern die Schlüssel direkt oder indirekt auf ihren Servern und besitzen somit faktisch die Kontrolle über die Konten der Nutzer. Sowohl das Vertrauen in den Betreiber des Dienstes, dass er die Daten nicht für eigene Zwecke nutzt, als auch Vertrauen in die jeweilige Sicherheitsarchitektur muss vorhanden sein. Bekannte Fälle von Hacking Angriffen auf verschiedene Dienstleister wie Instawallet oder MyBitcoin belegen, dass auch große Anbieter sich momentan noch nicht hundertprozentig vor Diebstahl sichern können.[27]

4.3.3 Paper Wallets

Paper Wallets sind eine Möglichkeit eine Cold Wallet zu realisieren. Alle privaten und die dazugehörigen öffentlichen Schlüssel werden auf ein Papier gedruckt und können physisch, beispielsweise durch das Einschließen in einen Tresor, gesichert werden. Die Vorteile sind offensichtlich: Es gibt keine Möglichkeit für Hacker an den privaten Schlüssel zu gelangen, ohne dabei den Tresor zu knacken. Außerdem wird eine Sicherung der Langlebigkeit durch die Unabhängigkeit von technischen Defekten garantiert. Idealerweise trägt der Besitzer des privaten Schlüssels immer den dazugehörigen öffentlichen Schlüssel mit sich und kann so seine Adresse jedem zur Verfügung stellen, der ihm Geld zukommen lassen will.

Die privaten Schlüssel verlieren nie ihre Gültigkeit und können, solange das Bitcoin Netzwerk existiert, immer eingelöst werden. Ein wesentlicher Nachteil ist, dass von den Adressen, die sich auf dem Papier befinden keine Transaktionen signiert werden können, solange sich das Papier im Tresor befindet. Will der Besitzer der Bitcoin Addresse Transaktionen durchführen und seine *coins* ausgeben, muss er sich den privaten Schlüssel aus dem Tresor holen. Somit ist für eine regelmäßige Durchführung von Transaktionen diese Wallet ungeeignet.

5. NUTZENANALYSE

Die allgemeinen technischen Anforderungen elektronischer Zahlungssysteme wurden bereits in Kapitel 4 auf ihre Gültigkeit untersucht. Das folgende Kapitel widmet sich der Analyse der speziellen Anforderungen, sowohl auf Seiten der Händler als auch auf Seiten der Kunden.

5.1 Verbreitung

Um die aktuelle Verbreitung darzustellen, bietet sich, neben der Analyse der Nutzerzahlen, eine Betrachtung der entgegengebrachten Aufmerksamkeit und der damit verbundenen Bekanntheit an. Nutzer von Bitcoin haben die Möglichkeit, beliebig viele Adressen zu generieren, was die Analyse der Nutzeranzahl anhand der Anzahl von Konten ausschließt. Die Häufigkeit der getätigten Transaktionen kann zwar auch keine finale Aussage über die Anzahl der Teilnehmer machen, erscheint aber für eine Tendenzaussage ein geeigneter Indikator zu sein. Die Anzahl der durchschnittlich getätigten Transaktionen auf Basis der Blockchain können in Abbildung 3 betrachtet werden. Es ist ein steigender Trend zu beobachten, was eine erhöhte Nutzeranzahl vermuten lässt. Auch eine Betrachtung der entgegengebrachten Aufmerksamkeit auf Basis der Daten von Google Trends unterstützt diese Vermutung[34].

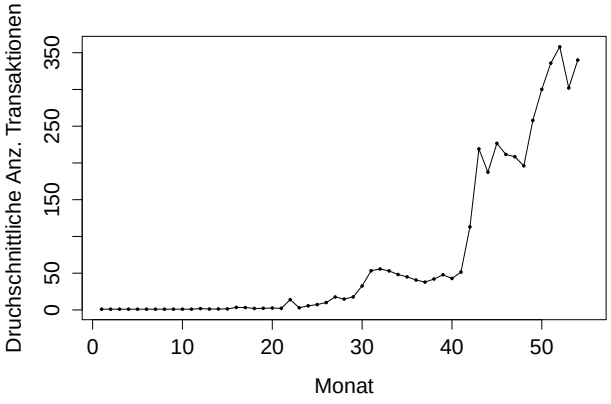

Abbildung 3: Anzahl der Transaktionen pro Monat

Tatsächlich lässt sich beobachten, dass immer mehr Online-Shops Bitcoin als Zahlungsmittel akzeptieren. In einem speziellen Wiki werden alle Anbieter, die Bitcoin akzeptieren, nach den jeweiligen Gütern kategorisiert und aufgelistet. Materielle Güter sowie Online Produkte bilden die beiden größten Kategorien, aber auch Dienstleistungen im Bereich von technischem Support oder Webadministration sind vorzufinden. Besonders im Bereich der Online Produkte scheint es eine größere Akzeptanz als im Bereich der materiellen Güter zu geben. Weiterhin ist auffällig, dass verhältnismäßig viele Anbieter im Bereich des Glücksspiels gelistet sind.[9] Tägliche Updates, die neue Anbieter hinzufügen, unterstützen die Vermutung, dass eine Steigung der Akzeptanz dieser Währung zu beobachten ist.

Wie bereits erwähnt, kann die entgegengebrachte Aufmerksamkeit von Presse und anderen Medien ein Indikator für eine erhöhte Verbreitung sein.[1] Dies ist jedoch kritisch zu betrachten: Die gesteigerte Aufmerksamkeit und die damit verbundene erhöhte Anzahl an Berichterstattungen über ein bestimmtes Thema können auch negative Folgen haben. Eine Berichterstattung, die nur die schlechten Seiten an der Währung beschreibt, würde folglich die Akzeptanz nicht steigern, sondern vielmehr negativ beeinflussen.

Eine allgemeine Akzeptanz der Währung lässt sich abschließend jedoch nicht feststellen. Von den führenden 20 deutschen E-Commerce Unternehmen bietet keines die Möglichkeit an, mit Bitcoins zu bezahlen. [21] Obwohl ein steigendes Interesse bezüglich Bitcoin zu beobachten ist[34], gibt es noch keine Anzeichen für eine Etablierung als gängiges Zahlungssystem.

5.2 Transaktionskosten

Paypal, Kreditkarte, Lastschriftverfahren und dies sind laut einer Studie der Universität Regensburg, die vom Kunden am häufigsten genutzten Zahlungsverfahren im Bereich des E-Commerce[30][S.13]. Händler stehen vor dem Problem, möglichst viele Methoden der Zahlung zur Verfügung zu stellen, um so eine möglichst große Menge an potentiellen Käufern zu erreichen. Dem Kunden wird dadurch die Möglichkeit eingeräumt, sich sein persönlich präferiertes Zahlungsverfahren auszuwählen. Generell entstehen bei bereits etablierten Zahlungssystemen für den Kunden keine Kosten. Lediglich der Händler muss Gebühren in Kauf nehmen[16][S.25]. Diese sind bei Paypal für jede Transaktion 1.9% des Kaufpreises sowie eine zusätzliche Gebühr von 0.30€. Für Mikropayments, also Beträge $\leq$ 3€sind es 10% plus 0.10€[29].

Um die anfallenden Transaktionskosten des Bitcoin Protokolles zu bestimmen muss auf die technische Realisierung der Transaktion eingegangen werden. Wie bereits erwähnt, repräsentiert ein *coin* eine Kette von Transaktionen. Der Versand einer einzelnen Einheit wäre jedoch in der Praxis nicht praktikabel, zumal ein BTC momentan etwa 74,75€ [3] entspricht. Eine Aufteilung und Kombination der Bitcoins wird folglich als notwendige Bedingung für reale Handelsmöglichkeiten gesehen[28].

Transaktionen besitzen in ihrer konkreten Implementierung nicht nur den Input einer einzelnen Vorgängertransaktion, sondern eine Liste von Inputs und eine Liste von Outputs. Diese Inputs enthalten als jeweilige Referenzen die Outputs der Vorgängertransaktion. Wird nun eine neue Transaktion erstellt, wird die Summe der verfügbaren Inputs gebildet. Dies ist der Betrag, der aktuell maximal als Output angegeben werden kann. Natürlich ist es möglich, den Betrag

[3]Stand: 28.Juni 2013

wieder in beliebig viele Outputs aufzuteilen. Interessant im Zusammenhang mit Transaktionskosten ist der Betrag, der übrig bleibt: Schickt der Ersteller der Transaktion die übrig gebliebene Summe von Inputs nicht wieder an eine seiner eigenen Adressen, geht der Betrag automatisch an den Miner, der den gültigen Hash für den Block gefunden hat, in dem die Transaktion veröffentlicht wird. Generell muss der Erzeuger einer Transaktion also keine Transaktionsgebühren bezahlen, es sei denn, er richtet seine Transaktion so ein, dass es eine Differenz zwischen Input und Output gibt, die dann an den Miner geht. In der Praxis verlangen die Ersteller der Blöcke jedoch eine minimale Transaktionsgebühr um Transaktionen überhaupt in ihre Blöcke aufzunehmen. Bitcoin-Qt, der Client, der den ursprünglichen Referenzcode von Satoshi Nakamoto verwendet, lässt keine Transaktionen zu, die eine Gebühr von 0.0005 BTC unterschreiten. Dies entspricht aktuell in etwa 0,05€. Natürlich kann ein eigener Client entwickelt oder Alternativen verwendet werden. Es gibt auch Miner, die in ihre Blöcke Transaktionen einbetten, die keine Gebühr bezahlen. Jedoch sollte man beachten, dass es umso länger dauert, bis solche Transaktionen bestätigt und in die Blockchain aufgenommen werden können.

Falls Transaktionsgebühren bezahlt werden, geschieht dies durch den Nutzer, da er derjenige ist, der die Bitcoins verschicken und eine Transaktion einrichten muss. Der Händler muss diese Tatsache bei der Preisbildung berücksichtigen und ggf. Anpassungen vornehmen damit der Kunde, der es nicht gewohnt ist, Gebühren für die Zahlung zu zahlen, nicht auf andere Systeme zurückgreift. Es ist final zu beachten, dass die Analyse der Transaktionskosten auf der Prämisse aufbaut, dass der Händler seine Wallet selber verwaltet, also lokal auf seinem eigenen Computer speichert. Es ist nicht unüblich, dass Anbieter bestimmter Händler Services für jede getätigte Transaktion eine variable Bearbeitungsgebühr berechnen. [4]

5.3 Geschwindigkeit

Viele Unternehmen im Bereich des E-Commerce bieten neben materiellen Gegenständen auch immaterielle Waren an. Diese liegen meist in digitaler Form vor und können direkt über das Internet verschickt bzw. empfangen werden. Besonders der Kunde kann davon profitieren, indem er einerseits keine zusätzlichen Gebühren für Verpackung und Versand bezahlen muss und andererseits die Ware zeitnah erhält. Der Händler wiederum kann die Ware erst verschicken, wenn das Geld auf seinem Konto eingegangen ist. Es entsteht also ein offensichtlicher Konflikt. Der Kunde bezahlt und will den erworbenen Inhalt möglichst schnell erhalten. Der Händler muss, um sich vor Betrug zu schützen, solange warten, bis er das Geld wirklich erhalten hat. Lastschriftverfahren oder ähnliche Zahlungsmöglichkeiten sind also auszuschließen. Bei Kreditkartenzahlungen garantiert die Bank, dass der Betrag auch wirklich überwiesen wird und kommt im Betrugsfall für entstandene Schäden auf. Das Bitcoin Protokoll definiert sich dadurch, dass eine zentrale Überwachungsinstanz gerade vermieden werden soll. Es muss also eine Betrachtung der durchschnittlichen Wartezeit, bis eine Transaktion als gültig eingestuft wird, stattfinden.

Eine Transaktion eines Kunden k kann genau dann als allgemein gültig angesehen werden, wenn sie in mindestens einem Block aufgenommen, und 5 nachfolgende Blöcke gefunden worden sind[5]. Erst dann kann der Händler h mit einer sehr hohen Wahrscheinlichkeit davon ausgehen, dass double-spending nicht stattgefunden hat. Diese Erkenntnis basiert auf der Annahme, dass ein Angreifer nicht mehr als 10% der verfügbaren Hashrate besitzt. Ein Angreifer bräuchte mindestens 50% der gesamten Rechnerkapazität des Bitcoin Systems, um gleichzeitig eine längere Kette von Blöcken zu generieren, die dann vom System als allgemein gültiger Zustand akzeptiert werden würde. Dies ist praktisch nicht umsetzbar[23]. Bitcoin wurde so entworfen, dass es im Schnitt 10 Minuten dauern soll, bis der nächste Block gefunden wird. Eine Analyse der Zeitintervalle zwischen zwei Blöcken auf Basis der Blockchaindaten bestätigt dies. Das arithmetische Mittel aller Zeitintervalle betrug 9.808625 Minuten mit einer Varianz von 424.0713. Abbildung 4[5] zeigt die durchschnittlichen Zeitintervalle zwischen zwei Blöcken, für jeden Monat, seit der Veröffentlichung des Genesis-Blockes. Die einzige Möglichkeit des Händlers, seine Leistung vor den rund 60 Minuten Wartezeit zu erbringen, ist die Akzeptanz des Risikos. Ergebnisse einer wissenschaftlichen Untersuchung von Sicherheitsrisiken bei *fast payments* haben ergeben, dass die Wahrscheinlichkeit eines erfolgreichen double-spending Angriffes bei einem entsprechend kurzem Zeitintervall bei nahezu 100% liegt[23].

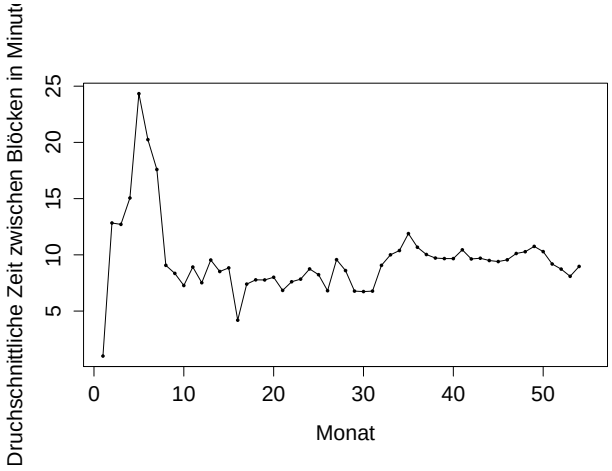

Abbildung 4: Durchnittliches Zeitintervall zwischen Blöcken

Für *fast payments* ist Bitcoin also nicht geeignet. Der Händler muss sich entscheiden, ob er dem Kunden eine Wartezeit von 10 Minuten zumuten kann oder ob es sich bei seinen Waren um Inhalte handelt, die umgehend freigeschaltet werden müssen. Es gibt jedoch einen signifikanten Vorteil gegenüber herkömmlichen Zahlungsmethoden wie Lastschriftverfahren. Sind einmal die Bitcoins an eine Adresse verschickt worden und stehen dann als Input zukünftiger Transaktionen zur Verfügung, hat der vorige Besitzer keine Möglichkeit mehr, die Transaktion rückgängig zu machen. Eine Form der Rückbuchung ist somit ausgeschlossen, was der Anforderung der Händler bzgl. einer Zahlungsgarantie entspricht. Daraus folgt auch, dass die komplementäre Anforderung der Kunden nach

[4] siehe dazu Kapitel 6.2

[5] Programmiert mit Java und den Daten der Blockchain

der Widerrufbarkeit von Transaktionen durch das Bitcoin Protokoll nicht realisiert wird.

5.4 Anonymität und Kontrollierbarkeit

Generell spielen die Anonymität und Kontrolle für Händler eine eher untergeordnete Rolle. Die Kunden auf der anderen Seite können von einer anonymen Währung profitieren, da sie nicht bei jedem Kauf dem Unternehmen eine Vielzahl an Daten übermitteln müssen. Obwohl die Anforderungen des Händlers in diesem Bezugspunkt nicht erfüllt werden, kann er diesen Umstand zu seinem Vorteil nutzen. Er kann mit einer Währung, die Anonymität verspricht werben und somit mehr Kunden gewinnen. Eine Analyse der Anonymität von Bitcoin kann somit auch für Händler von Relevanz sein.

Jeder Nutzer des Bitcoin Systems kann beliebig viele Paare von öffentlichen und privaten Schlüsseln erzeugen. Theoretisch kann er sogar jede seiner Transaktionen mit einem neuen Schlüssel tätigen. Dies ist zwar ein Aspekt, der es erschwert, Zahlungen zurückzuverfolgen und mit Identitäten zu verknüpfen, aber kein Beweis für die Anonymität des Systems. Um zu untersuchen, ob Bitcoin ein anonymes System ist, muss eine Definition des Begriffes der Anonymität vorgenommen werden. Nach §3 des Bundesdatenschutzgesetzes bezeichnet man unter Anonymisieren das *"Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"*. Dies trifft bei Bitcoin nicht zu. Jede Transaktion kann, bis einschließlich des Genesis-Blockes zurückverfolgt werden. Es ist so theoretisch möglich, dass jemand Datenbanken mit Schlüsseln und den dazugehörigen Identitäten nachhält. Das Hauptproblem liegt dabei an den beiden Schnittstellen Einzahlung und Auszahlung. In einer Versuchsreihe der International Association for Cryptologic Research wurden knapp 40% der Nutzerdaten zurückverfolgt[3]. Im Fall von Bitcoin kann man also nur von Pseudonymität sprechen.

5.5 Evaluierung

Die Analyse der Bitcoin Protokolles hat ergeben, dass die allgemeine Sicherheitsanforderungen alle erfüllt werden. Zahlungen, können unter Beachtung bestimmter Kriterien [6] als sicher angesehen werden. Auch die speziellen Anforderungen werden weitestgehend erfüllt. Bei den zueinander komplementären Anforderungen der Händler und Verbraucher geht Bitcoin einen scheinbaren Kompromiss ein: Auf der einen Seite sind die Transaktionen, wenn sie einmal in der Blockchain aufgenommen werden, unwiderrufbar, auf der anderen Seite bietet das Protokoll den Vorteil der Pseudonymität. Es existieren also für beide Parteien Anreize das System zu verwenden.

6. MÖGLICHKEITEN DER NUTZUNG

Generell existieren zwei Möglichkeiten für E-Commerce Unternehmen, Bitcoin als Zahlungsmittel einzuführen. Entweder werden die Zahlungen jeweils vom Händler selber verwaltet oder diese Aufgabe wird an einen externen Dienstleister ausgelagert. Im Folgenden werden beide Möglichkeiten seperat betrachtet und auf ihre Vor- bzw. Nachteile eingegangen.

[6]Angemessene Wartezeit etc.

6.1 Eigene Verwaltung

Von der technischen Seite betrachtet ist für die Verwaltung der Bitcoins lediglich ein Computer mit einer bestehenden Internetverbindung notwendig. Wie in Kapitel 2.3 beschrieben, gibt es eine Vielzahl verschiedener Clients, die sich teilweise in ihrer Implementierung unterscheiden. Dabei muss der Händler keine Hot-Wallet vorhalten, sondern geht im optimalen Fall wie folgt vor: Erst wird an einem Computer, der nicht mit dem Internet verbunden ist, ein Pool von Schlüsselpaaren erzeugt. Wird nun eine Transaktion abgeschlossen, wird ein öffentlicher Schlüssel mit genau dieser Transaktion assoziiert[8]. Der Händler muss also diesen Schlüssel in der Blockchain überwachen und kann so genau bestimmen, zu welchem Zeitpunkt die Zahlung eingegangen ist. Die privaten Schlüssel können nach Belieben offline sicher verwahrt werden, sei es duch eine Paper Wallet oder Cold Storage Realisierungen. Somit ist die Unsicherheit einer Hot-Wallet und das damit verbundene Risiko des Diebstahls nicht mehr existent. Trotz der offensichtlichen Vorteile, die sich aus der eigenen Verwaltung ergeben, sollte der Aufwand der Zahlungsüberwachung nicht vernachlässigt werden. Der E-Commerce Dienstleister muss sich um folgende Aspekte kümmern wenn er Bitcoin Zahlungen akzeptieren will:[8, 11, 37, 7]

- Für jede Transaktion muss eine neue Bitcoin Addresse erstellt und in einer Datenbank gespeichert werden. Nur so kann verifiziert werden, welcher Kunde gerade seine Verbindlichkeiten getilgt hat.
- Die generierte Addresse mit dem Zahlungsbetrag muss an den Kunden übermittelt werden.
- Der Kurs muss kontinuierlich geupdatet werden, um Verlust durch Kursschwankungen zu vermeiden.
- Alle Adressen, die eine Zahlung erwarten, müssen überwacht werden, um möglichst zeitnah die verkaufte Ware zu versenden. Dabei muss jedoch darauf geachtet werden, dass ausreichend Blöcke veröffentlicht wurden um double-spending Angriffe zu verhindern.
- Beträge die aufgrund des fluktuierenden Kurses von Bitcoin zu viel oder zu wenig gezahlt wurden müssen ggf. erstattet bzw. eingezogen werden.
- Erworbene Bitcoins müssen in die jeweilige Währung eingewechselt und Kursrisiken berücksichtigt werden[7]
- Bei Umtausch müssen Bitcoins zurück an den Absender geschickt werden. Hier kann es vorkommen, dass die Adresse des Empfängers sich von der ursprünglichen Zahlungsadresse unterscheidet.

Es ist offensichtlich, dass die Erfüllung der o. g. Anforderungen mit erheblichem programmiertechnischen Aufwand verbunden ist. Das Fachwissen, das für die Implementierung eines voll funktionsfähigen und insbesondere zuverlässigen Systems notwendig ist, kann nicht von jedem E-Commerce

[7]Dies ist nicht immer der Fall sondern betrifft die Händler die Bitcoins nicht langfristig angelegen wollen.

Unternehmen aufgebracht werden. Obwohl bereits Programme existieren, die dem Programmierer erheblichen Arbeitsaufwand abnehmen[8], ist ein fundiertes Verständnis von Datenbanksystemen und Web-Programmiersprachen notwendig. Weiterhin ist der Schutz vor Betrug noch immer nicht hundertprozentig gegeben. Gelingt es einem potentiellen Angreifer, auf die Datenbank des E-Commerce Unternehmens zuzugreifen, kann er zwar keine privaten Schlüssel ausfindig machen, aber einen öffentlichen Schlüssel in den Pool von Schlüsselpaaren einschleusen. Dies hat zur Folge, dass der Kunde den zu zahlenden Betrag de facto an den Angreifer überweist[8]. Aufgrund der Tatsache, dass Transaktionen nicht rückgängig gemacht werden könnens sind die Bitcoins dieser Transaktion für immer verloren.

Möchte ein E-Commerce Dienstleister also erreichen, dass jede Transaktion auch mit Bitcoins bezahlt werden kann und will er dabei nicht mit dem Aufwand und den Risiken der eigenen Verwaltung konfrontiert werden will, lohnt sich die Betrachtung sog. Händlerservices.

6.2 Externe Verwaltung – Payment Processors

Das Auslagern der Verwaltung von Bitcoins an externe Dienstleister kann, besonders für kleine E-Commerce Unternehmen, eine attraktive Alternative zu der eigenen Verwaltung darstellen. Erklärtes Ziel dieser Anbieter ist es, die Vielzahl der zu berücksichtigenden Aspekte der Implementierung[9] auf ein Minimum zu reduzieren. Dabei werben diese Services damit, dem Händler die Vorteile von Bitcoin Zahlungen auch ohne ein tiefgreifendes Verständnis der Materie zu ermöglichen. Im Folgenden wird ein Überblick über aktuelle Händler Services gegeben, indem ein Klassifizierungsrahmen für aktuelle Angebote entworfen wird.

Aktuell existieren bereits viele Anbieter die Service Leistungen für Händler rund um Bitcoin anbieten. Dabei handelt es sich um Angebote, die mit einprägsamen Slogans wie *„Bitcoin Made Easy“* [14], *„Start Accepting Bitcoin Now“*[12] und *„...accepting Bitcoins within minutes“* werben. Obwohl diese Slogans alle den gleichen Inhalt suggerieren, unterscheiden sich die einzelnen Services teils erheblich voneinander. Hier kann keine pauschale Aussage für alle Angebote getroffen werden und eine Analyse des jeweiligen konkreten Anbieters ist notwendig. Generell kann jedoch beobachtet werden, dass es erhebliche Differenzen der Angebote untereiander gibt. Das eigentliche Ziel, nämlich die Reduktion des Aufwandes, der mit der Einführung von Bitcoin verbunden ist, kann als Hauptkriterium herangezogen werden. Es gibt Anbieter wie Bitpay, die fast alle nötigen Anforderungen, die mit der eigenen Verwaltung von Bitcoin anfallen[10], übernehmen. Hierzu gehört das Anlegen eines Pools von Schlüsselpaaren, Kursupdates, die Überwachung der Zahlung und Benachrichtigung bei Zahlungseingang, der Umtausch in gängige Währungen und die Integration in Standardsoftware. Daneben gibt es auch Anbieter die sich auf ein Minimum an Funktionalität beschränken und den Händler nur bei einzelnen Anforderungen wie die Generierung von Bitcoin Addressen unterstützen[2]. Dies spiegelt sich auch im Spektrum der anfallenden Kosten wieder. Während einige Angebote komplett kostenlos sind, verlangen diverse Anbieter teilweise 1% Gebühr für jede empfangene Transaktion. Es ist zu beachten, dass es sich bei diesen Services lediglich um die Vereinfachung des Zahlvorganges handelt, also die Möglichkeit Bitcoin, anzunehmen. Ein Online Shop mit den dazugehörigen Funktionalitäten muss auf Seiten des Händlers bereits vorhanden und implementiert sein.

Im Rahmen dieser Arbeit wird ein Klassifikationsrahmen vorgeschlagen, der die jeweiligen Anbieter danach kategorisiert, ob die jeweiligen Services Komplettlösungen für E-Commerce Shops anbieten oder ob lediglich Funktionalitäten angeboten werden, die den Händler dabei unterstützen, Bitcoin zu akzeptieren. Unter einer Komplettlösung fallen jene Angebote, die folgenden Anforderungen entsprechen: Ein Schlüsselpool muss bereitgestellt werden, der Bezahlvorgang muss über die Seite des Anbieters abgeschlossen werden, der Kurs muss aktuell gehalten werden, der E-Commerce Dienstleister muss bei eingehenden Zahlungen benachrichtigt werden, die eingenommenen Bitcoins müssen regelmäßig in eine gewünschte Währung eingetauscht und auf ein Bankkonto überwiesen werden und der Service muss Plugins für bestehende E-Commerce Shoplösungen bereitstellen. Gerade im Bezug auf letztere Anforderung unterscheiden sich viele Angebote voneinander. Während einige Anbieter das breite Spektrum an etablierten E-Commerce Plattformen unterstützen, setzen andere Services auf die Nutzung ihrer jeweiligen API. Dies kann insbesondere für Shopbetreiber interessant sein, die eigene Online Shop Lösungen implementiert haben und den Service in ihr System integrieren wollen. Lösungen, die eine volle Funktionalität bieten sind Bitpay, MtGox und WalletBit. Anbieter wie Coinbase, BitMerch oder Acceptbit fallen in die zweite Kategorie.

Neben diesen beiden Oberkategorien existieren weitere Kriterien hinsichtlich der die jeweiligen Systeme untersucht werden können. Ein wichtiges Merkmal für den Händler ist der Kostenaspekt. Hier haben sich unterschiedliche Arten von Gebühren etabliert. Zum einen können Gebühren pro empfangener Transaktion erhoben werden. Dabei nutzt der Anbieter den Umstand aus, dass alle Transaktionen ohnehin über sein System laufen, er die privaten Schlüssel also kennt und so in der Lage ist, sich seinen Anteil direkt abzuziehen. Ein weiterer Kostenfaktor stellt die Gebühr für den Tausch von Bitcoins in echte Währung dar. Hier gelten zudem, je nach Anbieter, unterschiedliche Beschränkungen hinsichtlich des minimalen Tauschbetrags. Tabelle 1 gibt eine Übersicht über aktuelle Systeme und zeigt für die o. g. Kriterien die jeweiligen Ausprägungen an.

Die unterschiedlichen Preisstrukturen sind deutlich zu erkennen. Während BitPay darauf setzt, pro Transaktion knapp 1% der Einzahlung einzubehalten, setzen MtGox und Coinbase darauf alle Transaktionen kostenlos zu bearbeiten und nur für den Umtausch und der Überweisung in die jeweilige Währung Gebühren zu veranschlagen. MtGox muss hier jedoch eine besondere Rolle zugeschrieben werden, da die Seite sich eigentlich als Bitcoin Exchange etabliert hat, also als Handelsplattform für Bitcoin. Anbieter wie WalletBit und Coinbase nutzen MtGox, um ihre Funktionalität des Währungstausches zu realisieren. Dies bedeutet im Speziellen, dass die Kosten bei diesen Anbietern sich pro Exchange erhöhen und zusätzliche Gebühren an MtGox gehen.

[8] Siehe Pywallet
[9] siehe. Kapitel 5.1
[10] siehe Kapitel 5.1

	Komplettlösungen				Teillösungen		
Kriterien	BitPay	MtGox	WalletBit	Paysius	Coinbase	BitMerch	Aceptbit
Kosten pro Transaktion	0,99%	0	0,89%	0,49%	0	0,5%	0
Kosten pro Exchange	0	1% +	0,89% +	1,49%	1% +0,15$	×	×
E-Wallet	✓	✓	✓	✓	✓	×	×
Aktueller Kurs	✓	✓	✓	✓	✓	✓	✓
Notifications	✓	✓	✓	✓	✓	✓	×
Währungstausch	✓	✓	✓	✓	✓	×	×
API	✓	✓	✓	✓	✓	✓	×
Plugins	Ja, siehe	Ja, teilweise	Ja	Ja, teilweise	Nein	Nein	Nein

Tabelle 2: Händler Services im Vergleich

Es wurde festgestellt, dass alle Anbieter eine eigene API anbieten. Somit kann jeder Anbieter die Services für eigene Shoplösungen verwenden. Auch Funktionen wie automatische Benachrichtigungen bei Zahlungseingang und das Umrechnen in den aktuellen Bitcoin Kurs scheinen Standardfunktionalitäten zu sein. Die Unterstützung der Plugins für E-Commerce Shoplösungen sollte gesondert betrachtet werden, da hier erhebliche Unterschiede bezüglich des quantitativen Erfüllugsgrades zu beobachten sind. BitPay und WalletBit schneiden hier am besten ab. Beide bieten Plugins für 10 verschiedene E-Commerce Standardlösungen an [12, 36]. Paysius und MtGox bieten diesen Umfang nicht an und beschränken sich auf 5 bzw. 1 Plugin. Abschließend sollte noch erwähnt werden, dass BitPay dem Händler den Service anbietet, die Kundendaten während des Kaufprozesses zu sammeln. Somit können Händler, die noch keinen Shop in ihrer Website implementiert haben, trotzdem Bitcoins annehmen. Für Einproduktunternehmen könnte dies eine interessante Alternative darstellen.

7. HANDLUNGSEMPFEHLUNG

Nachdem nun sowohl die eigene als auch die externe Verwaltung von Bitcoin vorgestellt wurde, wird abschlieSSend eine Handlungsempfehlung entwickelt, die E-Commerce Unternehmen dabei unterstützen soll, eine Realisierungsentscheidung zu fällen. Dabei orientiert sich dieser Leitfaden nach den im Kapitel 5.1 formulierten Anforderungen und berücksichtigt dabei den Vergleich der verschieden Anbieter aus Kapitel 5.2.

Generell muss der Händler einen bestimmten Entscheidungsprozess durchlaufen um eine, für ihn angemessene Lösung zu finden. Initial muss entschieden werden ob der Zahlungsverkehr mit Bitcoins selber verwaltet werden soll oder aber externe Dienstleister herangezogen werden müssen. Hier kann sich der Händler im Rahmen einer Aufwandsanalyse, an den aus Kapitel 5.1 beschrieben Anforderungen orientieren. Eine pauschale Aussage kann hier nicht getroffen werden. Trifft der Händler die Entscheidung der eigenen Implementierung ist der Prozess abgeschlossen. Sollte er sich für externe Händler Services entscheiden muss die aktuelle Shop Lösung betrachtet werden. Dabei gibt es die Möglichkeit, dass ein eigenes Shop System für die Website entwickelt wurden ist oder das E-Commerce Standardsoftware verwendet wurde. Sollte letzteres der Fall sein lohnt sich eine Betrachtung der Komplettlösungen da die vorhandenen Plugins den Arbeitsaufwand erheblich verringern. Natürlich ist hier die Voraussetzung, dass es auch ein Plugin für die verwendete Softwarelösung gibt. Im Falle einer eingenen Implementierung des Shopsystems wird die Entscheidung nicht weiter eingeschränkt und hängt von anderen Faktoren ab. Eine weitere wichtige Entscheidung ist hinsichtlich dem Bedürfnis nach sofortigem Währungstausch zu treffen. Hält der Händler es nicht für nötig Bitcoin direkt, in die von ihm bevorzugte Währung umzutauschen, sollte eine Option gewählt werden, die möglichst keine Kosten pro Transaktion veranschlagt. Hier bietet sich Coinbase und MtGox an. Sollte hingegen ein Interesse an sofortigem Umtausch bestehen müssen die Preise pro Überweisung, der minimale Betrag pro Tausch und die Landesverfügbarkeit für jeden Anbieter überprüft werden. Geht der Händler nach diesem Prozess vor, sollte er einige Anbieter ausschließen können. Eine eindeutige Zuordnung kann jedoch nicht vermittelt werden und hängt auch von der Einschätzung des jeweiligen Unternehmens hinsichtlich eigener Kriterien wie der Repräsentation des Anbieters oder vorhandenen Sicherheitsaspekte ab.

8. FAZIT

Auf Seiten der Händler spricht viel für die Nutzung von Bitcoin als Zahlungssystem. Die Erfüllung händlerseitiger Anforderungen an elektronische Zahlungssysteme wurde überprüft und anhand des Bitcoin Protokolls verifiziert. Minimale Transaktionskosten, eine relativ schnelle Zahlungsbestätigungen und eine sichere, auf kryptografischen Methoden beruhende Systeminfrastruktur sind Argumente für eine händlerseitige Akzeptanz dieser Währung. Gerade im Bereich des Micropayment lassen sich signifikante Kostenvorteile gegenüber etablierten Systemen wie Paypal feststellen. Auch auf Kundenseite existieren Anreize, die für die Nutzung dieser Währung sprechen. Pseudonymität und die Unabhängigkeit vom Bankensystemen ermöglichen es dem Kunden, mit einer minimalen Weitergabe persönlicher Daten Produkte oder Dienstleistungen käuflich zu erwerben. Doch nicht für alle Szenarien scheint Bitcoin die Bestmögliche Alternative zu sein. Für fast payments ist Bitcoin nur teilweise geeignet da mindestens 6 Blöcke gefunden werden müssen, damit eine Zahlung als gültig angesehen werden kann. Ein weiterer negativer Aspekt kann der Umstand sein, dass Bitcoin als Zahlungssystem zum aktuellen Zeitpunkt noch große Verbreitung gefunden hat.

Weiter wurden die Möglichkeiten der Nutzung von Bitcoin als Zahlungsmittel diskutiert und ein Leitfaden entworfen, der Besitzer kleiner E-Commerce Unternehmen dabei unterstützen soll eine geeignete Wahl hinsichtlich der derzeitigen verfügbaren Alternativen zu treffen. Hierbei wurde jedoch kein Anspruch auf eine eindeutige Entscheidungsfindung konstituiert. Der Praktiker kann den Leitfaden dazu nutzen

bestimmte Services auszuschließen und sich anschließend auf die kritische Betrachtung der übrigen Alternativen konzentrieren.

Obwohl sich herausgestellt hat, dass Bitcoin die händlerseitigen Anforderungen an ein elektronsiches Bezahlsystem erfüllt, wurde ein Vergleich mit bereits etablierten Systemen wie PayPal, ClickandBuy etc. nicht vorgenommen. Ein strukturierter Vergleich könnte weitere Händler davon überzeugen, Bitcoin zu akzeptieren und so das System als gängiges Zahlungsmittel langfristig etablieren. Weiter wäre eine Untersuchung der rechtlichen Basis der Währung eine interessante Forschungsfrage für den Bereich des E-Commerce. Konkret könnte untersucht werden, zu welchem Zeitpunkt der Händler verpflichtet ist Mehrwertsteuern für die gekauften Artikel zu erheben.

8.1 Danksagung

Ich danke den anonymen Bewertern meiner Arbeit für die konstruktive Kritik und Dominic Breuker dafür, dass er mich auf den richtigen Pfad gebracht hat. Ein besonderer Dank geht an Raimo Radczewski für die Diskussionen rund um die Analyse der Blockchain.

9. REFERENCES

[1] Abel, Andreas and Rautenstrauch, Claus. Private Währungen im Internet-Fachkonzept und Einsatzpotenziale. *Wirtschaftsinformatik*, pages 325–344, 2003.

[2] Acceptbit. Acceptbit - Main Page, Juni 2013. http://acceptbit.com/.

[3] Elli Androulaki, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating User Privacy in Bitcoin. Technical report, IACR Cryptology ePrint Archive, 2012: 596, 2012.

[4] Bitcoin-Wiki. Blocks, May 2013. https://en.bitcoin.it/wiki/Blocks.

[5] Bitcoin-Wiki. Confirmation, Juni 2013. https://en.bitcoin.it/wiki/Confirmation.

[6] Bitcoin-Wiki. Hot wallet, May 2013. https://en.bitcoin.it/wiki/Hot_wallet.

[7] Bitcoin-Wiki. How to accept Bitcoin for small businesses, Juni 2013. https://en.bitcoin.it/wiki/How_to_accept_Bitcoin,_for_small_businesses.

[8] Bitcoin-Wiki. Merchant-Howto, Juni 2013. https://en.bitcoin.it/wiki/Merchant_Howto.

[9] Bitcoin-Wiki. Trade, May 2013. https://en.bitcoin.it/wiki/Trade.

[10] Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. BITKOM. Trends im E-Commerce. 1, 2013.

[11] Bitpay. bitpay-api, Juni 2013. https://bitpay.com/bitcoin-payment-gateway-api.

[12] Bitpay. Bitpay Main Page, May 2013. https://en.bitcoin.it/wiki/Trade.

[13] Vitalik Buterin. Bitcoin Wallet Reviews And Options. Website, 2012. Verfügbar auf http://bitcoinmagazine.com/bitcoin-wallet-options.

[14] Coinbase. Coinbase Main Page, May 2013. https://en.bitcoin.it/wiki/Trade.

[15] Sven Seuken David Parkes. Electronic currencies, 2011.

[16] Bastian Dombret. *Zahlungssysteme im Internet*. BoD–Books on Demand, 2008.

[17] Crowther Geoffrey. Outline of money, 1988.

[18] Tobias Hausen and Prof. Dr. Gerhard Schiefer. *Elektronischer Handel - Einbettung in Geschäftsbeziehungen und Supply Chains*. Deutscher Universitätsverlag, Wiesbaden, 2005. aufl. edition, 2005.

[19] Stefan Heng. E-Payment-Systeme: Treiber einer notwendigen Evolution der Zahlungssysteme. In *Handbuch E-Money, E-Payment & M-Payment*, pages 419–428. Springer, 2006.

[20] ibi Research. Das E-Payment-Barometer 2013. 1, 2013.

[21] Internetworld. Ranking: Die 100 größten Online-Shops in Deutschland 2011. Website, 2013. Verfügbar auf http://www.internetworld.de/Nachrichten/E-Commerce/Zahlen-Studien.

[22] Lars Jäger. *Die Bewertung ausgewählter Zahlungssysteme für den Electronic Commerce: eine theoretische und empirische Untersuchung*. PhD thesis, Books on Demand.

[23] Karame, Ghassan O and Androulaki, Elli and Capkun, Srdjan. Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. Technical report, IACR Cryptology ePrint Archive, 2012: 248, 2012.

[24] Jasmin C. Korb and Arnold Picot. *Kaufprozesse Im Electronic Commerce - Einflüsse Veränderter Kundenbedürfnisse Auf Die Gestaltung*. Dt. Univ.-Verlag, Wiesbaden, 2000. aufl. edition, 2000.

[25] M Krüger, K Leibold, and D Smasal. IZV9–Internet Zahlungssysteme aus der Sicht der Verbraucher. *Retrieved November*, 24:2009, 2008.

[26] Michael Merz. *Electronic Commerce. - Marktmodelle, Anwendungen und Technologien*. Dpunkt.Verlag GmbH, Heidelberg, 1999.

[27] Richard Meusers. Virtuelle Währung: Hack-Attacken bremsen Bitcoin-Rallye. Website, 2013. Verfügbar auf http://www.spiegel.de/netzwelt/web/.

[28] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1:2012, 2008.

[29] Paypal. Paypal – Gebühren für Händler, Juni 2013. https://www.paypal.com/de/webapps/mpp/gebuehren.

[30] Ernst Stahl, Stefan Weinfurtner, and GEORG WITTMANN. Die Qual der Wahl ? Wie Online–Händler ihre Zahlungsverfahren auswählen. *Regensburg, Universitätsverlag Regensburg*, 2009.

[31] Statista. Anteil der Internetnutzer in Deutschland von 2001 bis 2013. Website, 2013. Verfügbar auf http://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internetnutzung/-in-deutschland-seit-2001/.

[32] René Teichmann, Martin Nonnenmacher, and Joachim Henkel. *E-Commerce und E-Payment - Rahmenbedingungen, Infrastruktur, Perspektiven*. Gabler, Betriebswirt.-Vlg, Wiesbaden, 2001. aufl. edition, 2001.

[33] CG Traver and Kenneth Laudon. E-commerce: business, technology, society, 2003.

[34] Google Trends. Trenddaten zum Begriff Bitcoin, Juni 2013. http://www.google.de/trends/explore?q=

Bitcoin#q=Bitcoin&cmpt=q.

[35] Sebastian Van Baal and Jens-Werner Hinrichs. Internet-Zahlungssysteme aus Händlersicht: Bedeutung, Bewertung, Eigenschaften. In *Handbuch E-Money, E-Payment & M-Payment*, pages 293–305. Springer, 2006.

[36] Wallet-Bit. WalletBit - Plugins, Juni 2013. https://walletbit.com/shop.

[37] weusecoins. Bitcoin for Merchants, Juni 2013. https://www.weusecoins.com/en/merchant-tools.