Westfälische Hochschule

Fachbereich Informatik und Kommunikation

Studiengang **Praktische Informatik**

BACHELORARBEIT

Thema **Übersicht und Bewertung von Zahlungssystemen**

vorgelegt von **Tim Ziegler**

betreut durch:

Datum und Unterschrift des ersten Prüfers	Datum und Unterschrift des zweiten Prüfers

Hiermit versichere ich, die Arbeit selbstständig angefertigt und keine anderen als die angegebenen und bei Zitaten kenntlich gemachten Quellen und Hilfsmittel benutzt zu haben.

_____

Datum und Unterschrift des Verfassers

Diese Bachelorarbeit ist ein Prüfungsdokument. Eine Verwendung zu einem anderen Zweck ist nur mit dem Einverständnis von Verfassern und Prüfern erlaubt.

INHALTSVERZEICHNIS

Abbildungsverzeichnis

Abbildung 19: Kriterien zur Auswahl eines Bezahlverfahrens bei Online-Einkäufen.
Diagramm, eigene Darstellung in Anlehnung an: Wittmann, Georg; Stahl, Ernst; Wittmann, Michael; Pur, Sabine; Weinfurtner, Stefan (2013): *Erfolgsfaktor Payment. Der Einfluss der Zahlungsverfahren auf Ihren Umsatz*. Ibi Research an der Universität Regensburg GmbH, Regensburg, S. 36 (verfügbar unter: http://homepages-nw.uni-regensburg.de/~ecl60018/download/Studie_Erfolgsfaktor_Payment_2013.pdf, abgerufen am 13. August 2014).

Abbildung 20: Anzahl halbjährlich sichergestellter falscher Euro-Banknoten im Verlauf von 2004 bis 2014.
Diagramm, eigene Darstellung in Anlehnung an: EZB. (Juli 2014): *Anzahl der halbjährlich sichergestellten falschen Euro-Banknoten von 2004 bis zum 1. Halbjahr 2014 (in 1.000)*. In Statista - Das Statistik-Portal. http://de.statista.com/statistik/daten/studie/29171/umfrage/faelschungen-von-euro-banknoten-halbjaehrlich-seit-2004/ (abgerufen am: 21. August 2014)

Abbildung 21: Prozessschritte des Handels beim Umgang mit Bargeld.
Diagramm, aus Kleine, J, Krautbauer, M, Weiler, T (2013): *Cost of Cash. Status Quo und Entwicklungsperspektiven in Deutschland* Research Center for Financial Services der Steinbeis-Hochschule Berlin, München. S. 7.

Abbildung 22: Gesamtbewertung des Zahlungssystems Bargeld.
Diagramm, eigene Darstellung

Abbildung 23: Manipulationen von Geräten zum Zwecke der Erlangung von Kartendaten.
Diagramm, eigene Darstellung mit Daten aus:

1. Bundeskriminalamt (2011): *Zahlungskartenkrimininalität. Bundeslagebild 2011*, Wiesbaden (verfügbar unter: http://www.bka.de/nn_227456/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaetBundeslagebild2011,templateId=raw,property=publicationFile.pdf/zahlungskartenkriminalitaetBundeslagebild2011.pdf, abgerufen am 26. August 2014)

2. Bundeskriminalamt (2012): *Zahlungskartenkrimininalität. Bundeslagebild 2012*, Wiesbaden (verfügbar unter: http://www.bka.de/nn_227456/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaetBundeslagebild2012,templateId=raw,property=publicationFile.pdf/zahlungskartenkriminalitaetBundeslagebild2012.pdf, abgerufen am 26. August 2014)

3. Bundeskriminalamt (2013): *Zahlungskartenkrimininalität. Bundeslagebild 2013*, Wiesbaden (verfügbar unter: http://www.bka.de/nn_227456/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Zahlungskartenkriminalitaet/zahlungskartenkriminalitaetBundeslagebild2013,templateId=raw,property=publicationFile.pdf/zahlungskartenkriminalitaetBundeslagebild2013.pdf, abgerufen am 26. August 2014)

Abbildung 47: Erfüllung der Kriterien für Zahlungsinstrumente durch die einzelnen Instrumente aus Nutzersicht.

Diagramm, eigene Darstellung mit Daten von: IPSOS. *Zahlungsverhalten in Deutschland. Erfüllung der Kriterien für Zahlungsinstrumente durch die einzelnen Instrumente aus Nutzersicht*, 2010. http://de.statista.com/statistik/daten/studie/13137/umfrage/erfuellung-einzelner-kriterien-durch-zahlungsinstrumente/ (abgerufen am: 13. Juni 2014).

Abbildung 48: Umfrage zur künftigen Nutzung von mobilen Zahlungssystemen.

Diagramm, eigene Darstellung in Anlehnung an: Recke, Renko (2014): *Im Supermarkt mit dem Handy bezahlen?* http://mingle-trend.respondi.com/de/07_11_2014/im-supermarkt-bezahlen/ (abgerufen am 17. November 2014).

Abkürzungsverzeichnis

abzügl.
abzüglich

BaFin
Bundesanstalt für Finanzdienstleistungsaufsicht

BLE
Bluetooth Low Energy

BMF
Bundesminsterium der Finanzen

BTC
Bitcoin

bzw.
beziehungsweise

ECDSA
Elliptic Curve Digital Signature Algorithm

E-Geld
Elektronisches Geld im Sinne der Richtline 2000/46/EG

EMV
Europay International, MasterCard, Visa

EStG
Einkommensteuergesetz

etc.
et cetera

ggf.
Gegebenfalls

i.d.R.
in der Regel

KWG
Gesetz über das Kreditwesen

NFC
Near Field Communication

PDA
Personal Digital Assistant

PIN
Persönliche Identifikationsnummer

POS
Point-of-Sales

PPC
Peercoin

QR-Code
Quick Response Code

SET
Secure Electronic Transaction

SIM
Subscriber Identity Module, deutsch: Teilnehmer Identitätsmodul

u. a.
unter anderem

UNL
Unique Node List

UStG
Umsatzsteuergesetz

u. U.
unter Umständen

vgl.
vergleiche

XRP
Eigene Währungseinheit innerhalb eines Ripple-Netzwerks

ZAG
Gesetz über die Beaufsichtigung von Zahlungsdiensten

z.B.
zum Beispiel

Tabellenverzeichnis

Einleitung

Diese Bachelorthesis entstand im Rahmen des Studiums der Informatik, Studienrichtung Praktische Informatik, an der Westfälischen Hochschule im Fachbereich für Kommunikation und Informatik. Die Wahl des Themas erfolgte angesichts der Entwicklung von neuartigen Währungskonzepten wie Bitcoin, die in den letzten Jahren entwickelt wurden. Von ihren Erfindern sind diese Internetwährungen als Ersatz und Ergänzung der bisher vorhandenen Zahlungs- und Währungssysteme gedacht welche durch Finanzkrisen und damit verlorenes Vertrauen in bestehende Instanzen keine Lösung mehr darstellen.

Ziel der Arbeit

Die vorliegende Arbeit beschäftigt sich mit Zahlungssystemen, stellt die stattfindenden Abläufe grob dar und vergleicht verschiedene Systeme miteinander. Ein Zahlungssystem ist dabei laut duden.de ein „System, Verfahren, mit dem gezahlt, etwas bezahlt wird“ (1). Etwas konkreter wird die Wikipedia: „Als Zahlungsverfahren werden alle Formen und Prozesse der Übertragung von Eigentumsrechten an Zahlungsmitteln bezeichnet. Alternativ wird auch von Bezahlverfahren, Zahlungssystemen oder Zahlungsinstrumenten gesprochen“ (2). Beiden Ausführungen gemein ist, dass Zahlungssysteme, als Systeme beschrieben werden, mit denen bezahlt werden kann.

Heutzutage fallen eine Vielzahl von Systemen und Verfahren unter Zahlungssysteme. Dies sind zum einen die wohl bekannten Verfahren, wie die Barzahlung, die Zahlung mit Kartensystemen wie girocard und Kreditkarte, aber auch Entwicklungen, wie Mobile Payment Dienste, und als neueste Entwicklung, von einer Community entwickelte, Internetwährungen. Die Arbeit vermittelt dabei einen Überblick über aktuelle Zahlungssysteme und fasst die bestehenden Systeme in Kategorien zusammen.

Im Allgemeinen werden die Stakeholder von Zahlungssystemen und deren Interessen ermittelt, um daraus Kriterien zu ermitteln, anhand derer die unterschiedlichen Systeme bewertet und verglichen werden. Die Bewertungen ermöglichen es, zu beurteilen, welche Zahlungssysteme welche Interessen am besten umsetzen.

Durch die Aufführungen der Bewertungen sowie den zugehörigen Begründungen, wird zudem jeder Leser in die Lage versetzt, ein für sich geeignetes Zahlungssystem auszuwählen und ihm einen Eindruck davon vermitteln, welche Akteure an welchen Systemen beteiligt sind. Entstehen künftig neue Zahlungssysteme können diese somit ebenfalls in das bestehende Umfeld einsortiert werden und deren Vor- und Nachteile einfacher erkannt werden.

Methodik

Zunächst wurde recherchiert welche Systeme derzeit am Markt vertreten sind und ein grober Überblick über die Abläufe, Stärken und Schwächen gesammelt. Gerade bei mobilen Zahlungssystemen und Internetwährungen gibt es eine riesige Vielfalt. Hier lassen sich Namen wie SQWallet, cashcloud, paij, GO4Q, Yapital, PayPal Beacon, kesh, NXT, Litecoin, Primecoin, SmartTrust Portigo, qooqo und zahlreiche andere finden. Ausgewählt wurden letztlich Systeme, die verschiedene Ansätze, hinsichtlich ihrer Finanzierung, verwendeten Technologie und Ansätze bieten. Voraussetzung ist jedoch, dass das System auch in Deutschland verfügbar und nutzbar ist.

Im Kapitel 1 werden die ausgewählten Systeme zunächst in Kategorien eingeteilt und dann kurz vorgestellt, um darzustellen, wie diese funktionieren und welche Abläufe dahinter stecken.

Zur Ermittlung der Interessen verschiedener Gruppen an Zahlungssystemen (Kapitel 2.1 – 2.3) wurden, soweit verfügbar, verschiedene Studien und Umfragen zu Hilfe genommen, aus denen die Interessen abgeleitet wurden, um darauf aufbauend Vergleichskriterien (Kapitel 2.4 Bewertungskriterien) zu entwickeln, an denen alle Systeme gemessen werden.

Für die Bewertung der Systeme, werden pro Kriterium Punkte vergeben. Eine Erläuterung der Punktevergabe sowie die pro Kriterium vergebene Maximalpunktzahl findet sich ebenfalls in Kapitel 2.4. Die eigentliche Bewertung und Punktevergabe erfolgt in Kapitel 3, dass derselben Aufteilung wie Kapitel 1 folgt.

1 Vorstellung der einzelnen Zahlungssysteme

Das folgende Kapitel dient der Vorstellung der einzelnen Zahlungssysteme, jedoch findet noch keine Wertung statt. Hierbei wird für jedes System dargestellt wie eine Zahlung abläuft. Falls es das Verfahren erforderlich macht, wird zwischen der Bezahlung am Point-of-Sales[1] (POS) und der Bezahlung im Internet unterschieden.

Die derzeit existierenden Zahlungssysteme lassen sich grob in vier Kategorien einteilen, die sich in den folgenden Kapiteln widerspiegeln.

In Kapitel 1.1 werden die bereits etablierten, klassischen Zahlungssysteme, wie Bargeld, girocard, GeldKarte und Kreditkarte vorgestellt. Diese existieren schon längere Zeit, während die Zahlungssysteme anderer Kategorien in der Regel jüngeren Datums sind. Außerdem sind sie im Handel weit verbreitet und werden von vielen Stellen akzeptiert.

Kapitel 1.2 beschreibt die Weiterentwicklung der Systeme des ersten Kapitels. Es handelt sich hierbei um kontaktlose Bezahlverfahren, wie MasterCard PayPass, girogo und Visa payWave, die nach und nach in die vorhandenen Karten integriert werden und zu einer Beschleunigung des Bezahlens führen sollen.

Das Kapitel 1.3 umfasst mobile Zahlungssysteme, die einen derzeit stark wachsenden Markt darstellen. Hierunter fallen alle Systeme, die für die Bezahlung das Smartphone in der einen oder anderen Form nutzen. Grundsätzlich ist hier eine weitere Unterteilung auf Basis der verwendeten Technologie möglich. So gibt es Systeme, die die NFC[2]-Technologie nutzen (Abschnitt 1.3.1), welche nicht durch alle Smartphones unterstützt wird, während andere auf QR-Codes (Abschnitt 1.3.2) oder Bluetooth Low Energy[3] (BLE, Abschnitt 1.3.3) setzen.

Kapitel 1.4 umfasst nicht nur reine Bezahlverfahren, sondern Internetwährungssysteme, die auch ein Zahlungssystem integrieren. Für diese werden zusätzlich systembedingte Eigenheiten, wie beispielsweise die Regulierung und die Besteuerung erläutert.

---

[1] Der Point-of-Sales, zu deutsch Verkaufsort, ist der Ort, an dem der Kunde auf dem auf den Händler trifft, also i. d. R. ein Ladengeschäft. Im engeren Sinne umfasst der POS den Kassenarbeitsplatz innerhalb des Geschäfts.

[2] Near Field Communication: Funktechnologie zum Austausch weniger Daten über kurze Distanzen.

[3] Erweiterung der Bluetooth-Funktechnologie um ein stromsparenderes Verfahren, was gerade bei mobilen Geräten, wie Smartphones, zu keiner merklichen Laufzeitreduzierung bei eingeschaltetem Bluetooth führen soll. Die Datenübertragungsrate ist dafür im Ausgleich auch geringer, so dass BLE nur für kleine Datenmengen eingesetzt werden kann.

1.1 Klassische Zahlungssysteme

Zunächst werden im Folgenden die Systeme vorgestellt, die bereits auf dem Markt der Zahlungssysteme etabliert sind, und den meisten Lesern vermutlich auch bekannt sind.

1.1.1 Bargeld

Die Zahlung mit Bargeld bedeutet eine direkte Übergabe von Banknoten und Münzen. Jede Münze und jede Banknote hat einen Nennwert, der aufgedruckt bzw. eingeprägt ist. In Deutschland sind seit 2002 ausschließlich auf Euro lautende Münzen und Banknoten unbeschränkte gesetzliche Zahlungsmittel. Diese Einstufung bedeutet, dass in Deutschland jeder Gläubiger zur Annahme von Bargeld verpflichtet ist. Die Annahme aller anderen Zahlungsmittel geschieht auf freiwilliger Basis des Gläubigers (3, 4).

Bei der Barzahlung erfolgt die Zahlung ausschließlich direkt zwischen Kunde und Händler, ohne die Einbeziehung von Dritten. Theoretisch kann auch die Bargeld ausgebende Stelle in diesem Prozess einbezogen werden. Da jedoch keine Verbindung zwischen dieser und dem Händler – mit Ausnahme des Kunden – besteht, sind dies zwei voneinander unabhängige Vorgänge, die nicht durch eine der beiden Stellen zusammengeführt werden können.

Der Händler übergibt hierbei dem Kunden die Ware und erhält im Gegenzug den Warenwert in Münzen und Banknoten durch den Kunden. Es ist keine weitere Partei in den Bezahlprozess involviert.

1.1.2 girocard

Die girocard tritt seit 2007 sukzessive die Nachfolge der ec-Karte an und ist immer an ein Girokonto gebunden. Die Deutsche Kreditwirtschaft[4] fasst unter dem Begriff der girocard zwei Verfahren zusammen: Zum einen das Verfahren zur bargeldlosen Bezahlung mit Karte und PIN (electronic cash) und zum anderen das Verfahren zur Beschaffung von Bargeld an Geldautomaten (5). Ziel der Deutschen Kreditwirtschaft ist es, mit dem noch recht jungen System einen einheitlichen bargeldlosen Zahlungsverkehr zu ermöglichen (6).

Einer Statistik der Deutschen Bundesbank zufolge, besitzen 94% der Deutschen eine gircoard (7, S. 27). In 2014 sind dies dem Bundesverband deutscher Banken zufolge bereits 103,1 Mio. Karten ausgegeben worden (8, S. 11).

[4] Die Deutsche Kreditwirtschaft (DK) ist ein Zusammenschluss des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken, des Bundesverbandes deutscher Banken, des Bundesverbandes Öffentlicher Banken Deutschlands, des Deutschen Sparkassen- und Giroverbandes und des Verbandes deutscher Pfandbriefbanken. Sie ging 2011 aus dem Zentralen Kreditausschuss hervor.

Im Folgenden wird zunächst das Verfahren electronic cash näher betrachtet, dass die Bezahlung am POS ermöglicht. Zu Beginn wird die girocard des Kunden eingelesen und der Kunde authentisiert sich durch Eingabe der korrekten PIN (Schritt 1). Das Zahlungsterminal[5] des Händlers übermittelt PIN und Zahlbetrag an den Chip der girocard, um die Zahlung zu autorisieren zu lassen. Ist auf dem Chip ein noch ausreichender Verfügungsrahmen, den das Kreditinstitut auf dem Chip hinterlegt, gespeichert wird die Zahlung direkt freigegeben (Schritt 3) und der Verfügungsrahmen auf dem Chip um den Zahlbetrag verringert. Die Zahlung ist damit abgeschlossen, sodass die Schritte 4 – 10 entfallen.

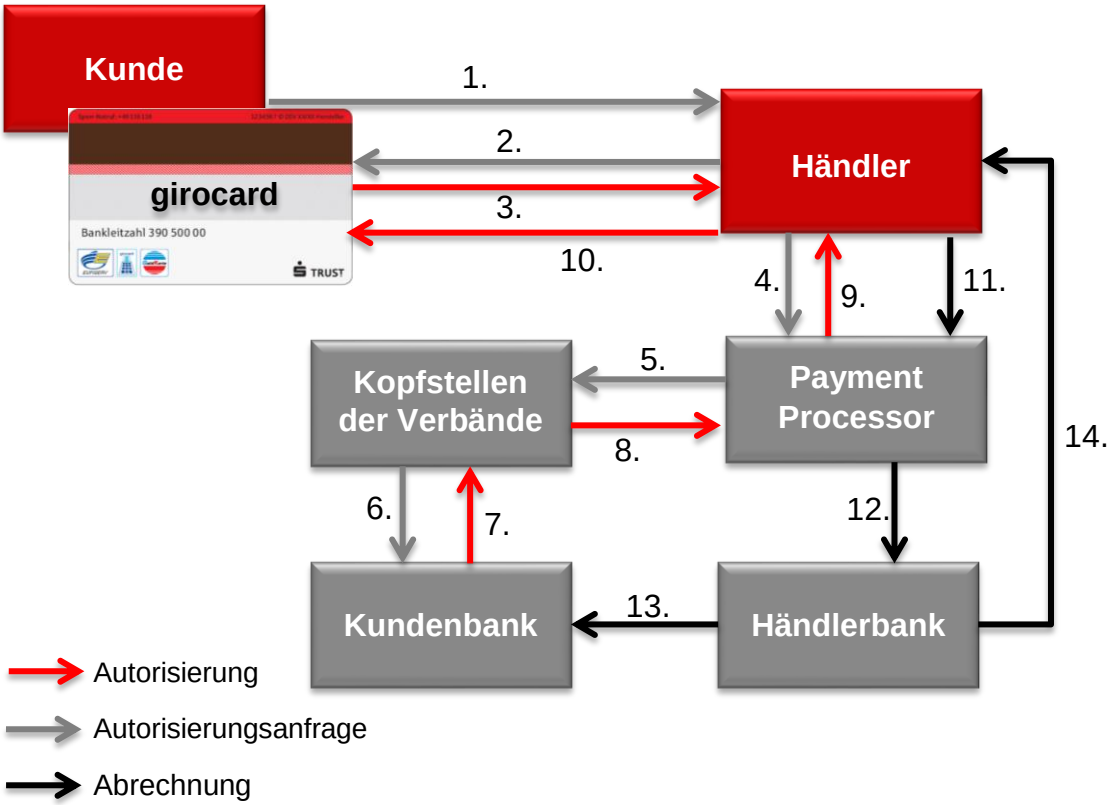

Abbildung 1: Ablauf einer Zahlung mit electronic cash.

Kann der Chip die Zahlung nicht selber autorisieren, so stellt das Zahlungsterminal des Händlers eine Verbindung zur Kundenbank über den *Payment Processor*[6] und die Kopfstellen der Verbände her. Es folgt eine Autorisierungsanfrage (Schritte 4 - 6) an diese. Die Kundenbank prüft, ob die Karte gesperrt ist und der Zahlbetrag innerhalb des Verfügungsrahmens des Kunden liegt. Ist die Prüfung positiv verlaufen, also die Karte nicht gesperrt und der Betrag innerhalb des möglichen Verfügungsrahmens, wird die Zahlung freigegeben (Schritte 7 – 9). Außerdem wird an den Chip

[5] Gerät zum Einlesen von Karten zur bargeldlosen Zahlung. Das Zahlungsterminal kommuniziert dabei auf der einen Seite mit dem Benutzer, also dem Kunden, sowie dem Rechenzentrum der Bank des Kunden.

[6] Der Payment Processor wird durch den Händler mit der Abwicklung von Transaktionen beauftragt. Er erhält die Daten des Kunden und nutzt diese zur Prüfung mit Hilfe eigener Systeme, die den Missbrauch von Zahlungsdaten erkennen sollen, kommuniziert mit der Bank des Kunden und kümmert sich um die Verrechnung der Zahlung.

der girocard eine Information gesendet, bis zu welcher Gesamtsumme er Zahlungen bis zum Ablauf einer bestimmten Periode auch ohne Prüfung bei der Bank autorisieren darf (Schritt 10).

Am Tagesende erfolgt Kassenabschluss am Zahlungsterminal durch den Händler (Schritt 11). Der Netzbetreiber leitet die Transaktion an die Händlerbank weiter (Schritt 12), die dann die Lastschrift vom Kundenkonto vornimmt (Schritt 13) und dem Händler die entsprechende Summe gutschreibt (Schritt 14).

Zum Zahlen im Internet kann die girocard bisher nicht eingesetzt werden. Hier kann über das Lastschriftverfahren oder per Vorauskasse mit Überweisung über das eigene Girokonto gezahlt werden.

1.1.3 Kreditkarte

Erstmals tauchte die Kreditkarte in dem Science-Fiction Roman „Looking Backward or Life in the Year 2000“ von Edward Bellamy aus dem Jahre 1887 auf. Er beschrieb sie als Karte von der der der Wert eines Einkaufs abgezogen wird. Bevor jedoch die erste universelle Kreditkarte von Diners Club ausgegeben wurde vergingen noch etwa 63 Jahre (9). In 2013 besaßen schätzungsweise 36,64 Millionen Deutsche eine Kreditkarte (10).

An der Abwicklung einer Kreditkartentransaktion sind mehrere Parteien beteiligt. Im Einzelnen sind dies:

a. die kartenausgebende Stelle, auch *Issuer* genannt, die eine Lizenz zur Vergabe der Karten hält,
b. der Karteninhaber oder Konsument, der eine Ware erwirbt und diese Leistung mit seiner Kreditkarte bezahlt,
c. der Händler, der eine Zahlung des Konsumenten empfängt, und
d. der *Acquirer*, der alle Forderungen des Händlers an den entsprechenden *Issuer* weiterleitet.

Issuer und *Acquirer* sind dabei über ein internationales Kreditkartennetzwerk miteinander verbunden. In einigen Fällen werden *Issuer*, *Acquirer* und/oder Händler durch ein Unternehmen vertreten.

In den Schritten 1 – 7 werden jeweils die Transaktionsdaten zwischen den einzelnen Parteien ausgetauscht. Der *Acquirer* fordert in Schritt 3 - 4 eine Autorisierung der Transaktion durch den *Issuer* an. Dieser prüft u.a. die Bonität des Kunden und akzeptiert die Transaktion oder lehnt sie ab (Schritte 5 - 6). Ist die Transaktion akzeptiert, erhält auch der Kunde die Transaktionsdaten im Rahmen seiner Abrechnung (Schritt 7), um diese zu begleichen (Schritt 8). Der *Issuer*, das Kreditkartennetzwerk und der *Acquirer* erhalten jeweils die Zahlung und leiten diese nach Abzug Ihrer Gebühren an die nächste Stelle weiter (Schritte 9 – 11).

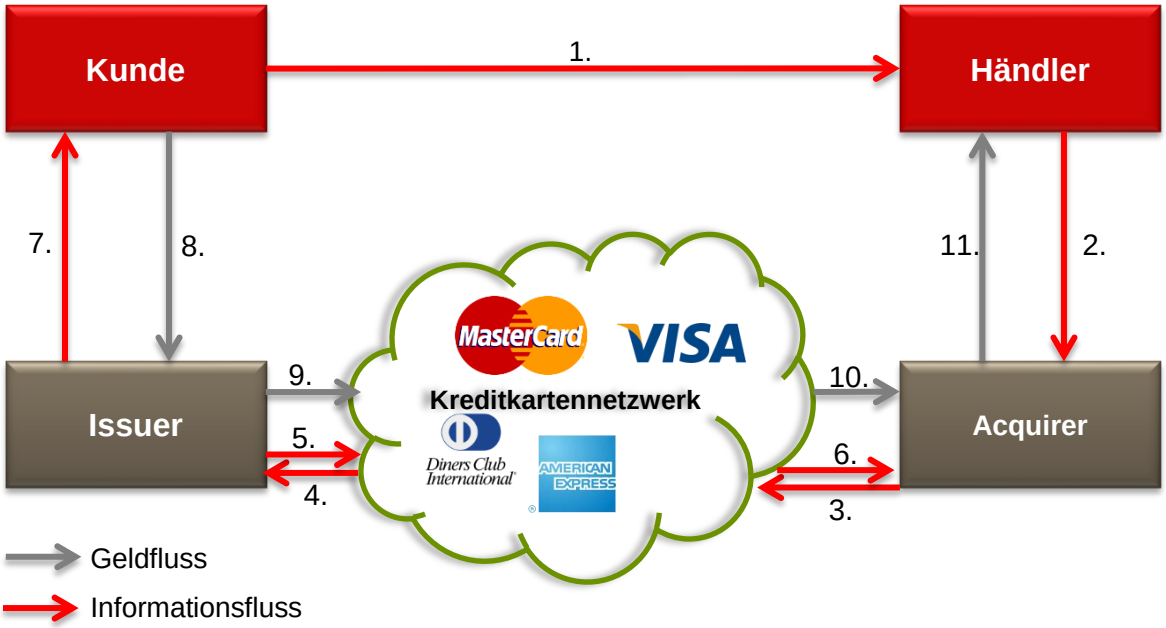

Abbildung 2: Ablauf einer Kreditkartentransaktion.

Für die Nutzung im Internet planten Visa, MasterCard, IBM, Microsoft, Netscape, Verisign, RSA und andere ab 1996 den Secure Electronic Transaction Standard, kurz SET. Dieser spezifiziert ein Protokoll zur Kommunikation zwischen Kunden, Händlern und Banken, um Zahlungen zu tätigen. Hierbei ist sowohl für den Kunden als auch für den Händler eine gesonderte Registrierung nötig, bei der jeder Teilnehmer entsprechende digitale Zertifikate bekommt (11), mit denen er übertragene Daten verschlüsseln und signieren kann (12). Die Zahlung läuft dabei so ab, dass der Händler nur die Bestelldaten und die Bank nur die Bezahldaten lesen kann (11). Aufgrund der komplexen Registrierung für den Kunden und den damit verbundenen hohen Kosten setzte sich SET nie durch.

Heute laufen aus diesem Grund Bezahlvorgänge mit Kreditkarten über das Internet durch Eingabe von Kartennummer, Ablaufdatum der Karte und Prüfziffer. Diese Daten sind direkt auf die Karte gedruckt bzw. geprägt und werden an den Händler übermittelt. Dieser leitet sie wiederum zusammen mit dem Rechnungsbetrag an seinen *Acquirer* weiter. Jeder Händler – egal ob stationär oder im Internet – kennt diese Daten, sofern bei ihm die entsprechende Kreditkarte bereits zuvor eingesetzt wurde. Deshalb setzen die Betreiber der Kreditkartennetzwerke bei der Nutzung im Internet auf eine zusätzliche Authentifizierung des Kunden. Dieses Verfahren trägt bei Visa den Namen verified by Visa, bei MasterCard SecureCode und bei anderen Anbietern J/Secure oder SafeKey. Allen Verfahren gemeinsam ist, dass der Kunde vor Durchführung der Transaktion auf Seiten des Kreditkartenherausgebers geleitet wird und sich dort mit einem selbst gewählten Passwort authentifizieren muss. Erst nach erfolgreicher Authentifizierung erfolgt die Zahlung (13). Dieses Kennwort wird dabei niemals an den Händler übermittelt sondern ausschließlich an die Bank des Kunden übermittelt. Dieses Verfahren wurde 2011 laut einer Studie von ibi research von 48% der befragten Händler eingesetzt (14, S. 79).

1.1.4 GeldKarte

Die GeldKarte wurde in Deutschland schon 1996 mit dem Ziel eingeführt auch die Zahlung von Kleinbeträgen zu ermöglichen (11). Sie ist Bestandteil vieler Debitkarten[7], beispielsweise bei den Sparkassen, kann aber auch separat als White Card[8] erworben werden. Erkennbar sind Sie immer anhand des GeldKarten-Logos, welches auf der Karte aufgedruckt ist. Die Deutsche Kreditwirtschaft, die die GeldKarte verantwortet, sieht sie als „elektronische Geldbörse“, die vorrangig dem Kleingeldersatz dienen soll. Bis 2011 wurden rund 89 Millionen GeldKarten ausgegeben (15, S. 74), auf die im selben Jahr aber nur 41,3 Millionen Transaktionen (16) entfielen.

Über beide Wege, Debitkarte und White Card, erhält der Kunde eine Prepaid-Karte, die mit Beträgen bis 200,- € aufgeladen werden kann. Die Aufladung erfolgt dabei entweder an einem Geldautomaten, einem gesonderten Ladeautomaten oder über Barzahlung. Alternativ kann die Karte auch von zu Hause aufgeladen werden. Voraussetzung hierfür ist mindestens ein einfaches Kartenlesegerät der Klasse 3[9].

Das GeldKarten-System ist ein rein deutsches System, so dass Zahlungen mit der GeldKarte ausschließlich in Deutschland möglich sind. Auch wenn in anderen Ländern ähnliche Systeme, wie beispielsweise Quick in Österreich oder Chipknip[10] in den Niederlanden, existieren, so sind diese doch nicht kompatibel zueinander (17).

Das Bezahlen mit der GeldKarte ist für den Kunden recht einfach gehalten: Er legt die Karte vor, die von einem Terminal eingelesen wird (Schritt 1). Dieses übermittelt den Zahlbetrag an die Karte des Kunden (Schritt 3) und des Händlers (Schritt 2), auf der der verfügbare Betrag entsprechend verringert bzw. erhöht wird. Außerdem speichert die Karte des Kunden die letzten 15 Transaktionen (18) mit Umsatz, Datum und Händlerterminalnummer (19, S. 9). Der Kunde muss sich nicht authentifizieren und der Händler benötigt keine Online-Abfrage der Daten, so dass eine Bezahlung schnell und einfach durchzuführen ist.

Mit dem Kassenschluss übermittelt der Händler alle bis dahin nur auf seiner Karte gespeicherten Transaktionen an seine Evidenzzentrale (Schritt 4). Die übermittelten Transaktionsdaten enthalten mindestens die Karten-ID, die Uhrzeit und die Höhe der Transaktion sowie die Identität des genutzten Kartenterminals. Die Evidenzzentralen sind für die Abwicklung sowie die Prüfung der

---

[7] Debitkarten sind Bank- und Sparkassenkarten, die mit einem Girokonto verbunden sind, das sofort nach der Bezahlung belastet wird.

[8] Eine White-Card kann separat erworben werden. Sie ist nicht an ein spezielles Konto, weshalb sie auch kontoungebunden genannt wird.

[9] Kartenlesegeräte werden nach ihren Funktionen in die Sicherheitsklassen 1 – 3 eingeteilt. Die sichersten Geräte der Klasse 3 bieten dem Nutzer eine Tastatur und ein Display, Geräte der Klasse 2 besitzen nur eine Tastatur und die günstigen Geräte der Klasse 1 besitzen weder Tastatur noch Display.

[10] Chipknip wird zum Ende des Jahres 2014 eingestellt.

Transaktionen von GeldKarten zuständig und verrechnen diese mit den einzelnen Teilnehmern am System.

Die Händlerevidenzzentrale gibt zum einen die Summe der Gutschriften an die Bank des Händlers weiter (Schritt 5), die diese dem Konto des Händlers gutschreibt, und zum anderen gibt sie die Transaktionen an die Kundenevidenzzentrale weiter (Schritt 6). Diese führt für jede Karte ein Schattensaldo, auf dem hinterlegt ist, welches Guthaben eine Karte derzeit aufweist. Außerdem nimmt die Kundenevidenzzentrale eine Lastschrift auf dem Börsenverrechnungskonto[11] des kartenausgebenden Instituts vor (Schritt 7). Hierfür wird diesem die Summe aller Bezahlungen mitgeteilt.

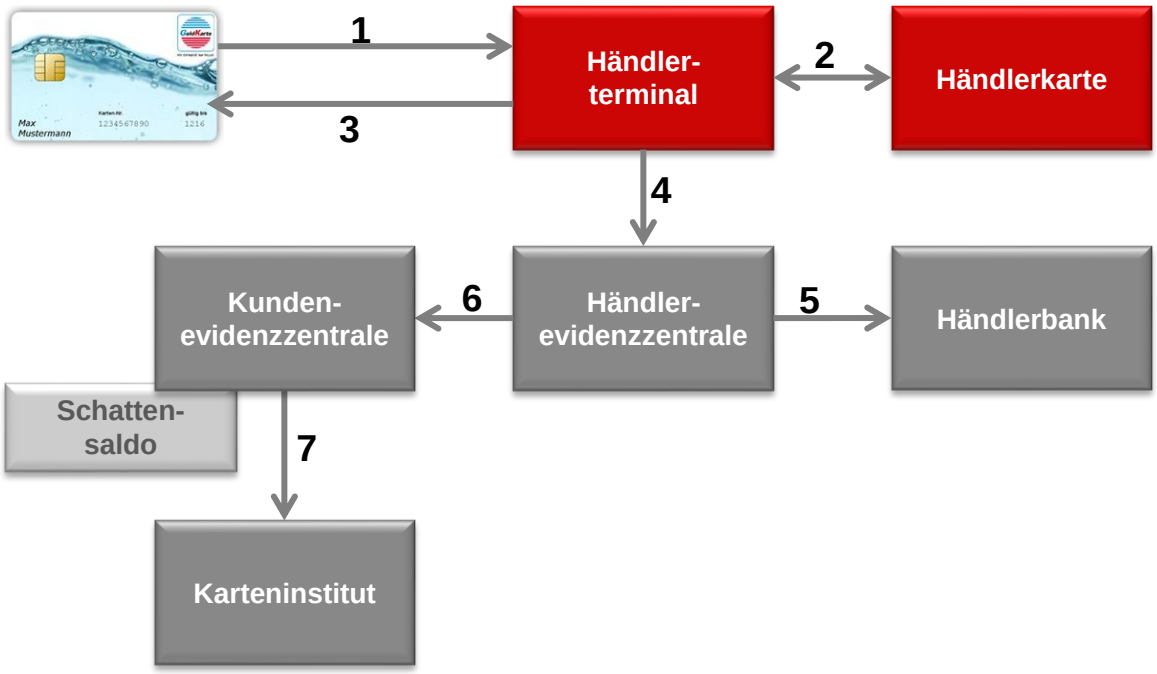

Abbildung 3: Ablauf einer Transaktion mit der GeldKarte.

Als das Einkaufen im Internet zu Beginn des 21. Jahrhunderts ein immer größerer Markt wurde, kam die Idee auf, das Bezahlen mit der GeldKarte auch im Internet zu ermöglichen. Der Bezahlvorgang selbst orientierte sich dabei stark an der Bezahlung am Point-of-Sales: Der Kunde benötigt ein Kartenlesegerät mit der passenden GeldKarten-Software, wobei die Klasse des Geräts keine Rolle spielt. Der Händler benötigt einzig ein digitales Zertifikat mit dem er sich gegenüber dem Kunden identifiziert (11).

Die Bezahlung erfolgt indem der Kunde innerhalb des Shops die GeldKarte als Bezahlart wählt. Daraufhin erstellt das Shopsystem eine virtuelle Rechnung, die über den Computer des Kunden an das Lesegerät gesendet wird. Nachdem die GeldKarte in das Lesegerät eingelegt wurde, zeigt es den Rechnungsbetrag an und wartet auf eine Bestätigung des Kunden. Ist die Bestätigung

[11] Auf dem Börsenverrechnungskonto werden alle Gut- und Lastschriften eines Instituts für alle von der Bank ausgegebenen GeldKarten vorgenommen. Von diesem Konto werden auch die Umsätze der Händler abgebucht (20).

erfolgt, wird sie verschlüsselt an den Händler übertragen, der die entsprechenden Umsätze an seine Bank und die Evidenzzentrale weiterreicht (11, 21). Dieses Verfahren fand allerdings keinen großen Anklang, so dass es mittlerweile wieder eingestellt wurde. Eine Nutzung der GeldKarte im Internet ist damit nicht mehr möglich.

1.2 Kontaktlose Zahlungssysteme

In den letzten Jahren haben nahezu alle Anbieter klassischer Bezahlverfahren neue Systeme vorgestellt, die den Bezahlvorgang an der Kasse beschleunigen sollen. Gemeinsam ist allen neuen Systemen, dass diese über Funktechnologien, wie beispielsweise NFC, kontaktlos funktionieren. Für eine Verbreitung dieser neuen Systeme wird gesorgt, indem die neuen Funktionen in neu ausgegebene Karten integriert werden. So enthalten beispielsweise neue girocards der Sparkasse neben der GeldKarte auch einen NFC-Chip für das System girogo.

1.2.1 MasterCard PayPass / Visa payWave

MasterCard PayPass ist eine NFC-basierte Erweiterung für Kreditkarten von MasterCard. Das System wurde im Dezember 2002 erstmals präsentiert und ist seit 2004 bereits verfügbar. Visa zog erst einige Jahre später nach und stellte 2007 der Öffentlichkeit das System Visa payWave vor (22, 23). Beide Systeme basieren im Wesentlichen auf Transaktionen wie sie bereits von den Kreditkarten bekannt sind. Der einzige Unterschied besteht in dem Austausch der Daten zwischen Karte und Lesegerät, welcher nun über Funktechnologie realisiert wird.

1.2.2 girogo

Die Weiterentwicklung der GeldKarte zu einem Bezahlinstrument ohne Kontakt ist girogo. Hierzu wurden alle Eigenschaften der GeldKarte übernommen: Es handelt sich weiterhin um ein Prepaid-System, welches Zahlungen bis maximal 20,- € ermöglicht. Zahlungen über 20,- € können nur kontaktbehaftet über die GeldKarte abgewickelt werden (24). Die Funktionsweise von girogo entspricht weitestgehend der der GeldKarte. Einzig die Übertragung der Daten zwischen Händlerterminal und Karte erfolgt nun kontaktlos über NFC.

1.3 Mobile Zahlungssysteme

Der Markt für mobile Bezahlverfahren wächst ständig, wobei auch mit verschiedenen Technologien experimentiert wird. So prognostiziert beispielsweise Gartner ein Wachstum des Umsatzes über Mobile Payment Systeme von 48,9 Milliarden Dollar in 2010 auf 721 Milliarden Dollar in 2017 (25). Ein solch stark wachsender Markt weckt natürlich Begehrlichkeiten bei den Anbietern von Zahlungssystemen, die einen Anteil daran haben möchten. Dadurch entstehen immer mehr Systeme, die untereinander nicht kompatibel sind und nicht an allen Stellen akzeptiert werden. Im Folgenden werden deshalb nur die in Deutschland größten Systeme und aussichtsreichsten Systeme betrachtet.

1.3.1 NFC-basierte Systeme

NFC ist eine Funktechnologie über kurze Distanzen von wenigen Zentimetern, die allerdings nur geringe Geschwindigkeiten von maximal 424 kbit/s bietet (26), dafür aber wenig Strom benötigt. Nachdem NFC-Chips in den vergangenen Jahren hauptsächlich in den hochpreisigen Smartphones verbaut wurden, gibt es mittlerweile auch günstigere Modelle, die diese Technologie unterstützen.

Eine Ausnahme stellt Apple mit seinen iPhones dar, die bis zur Einführung des iPhone 6 gar kein NFC unterstützen und seit dem iPhone 6 NFC. Dieses ist jedoch derzeit nicht für alle Entwickler freigegeben, sondern kann nur für den eigenen Bezahldienst Apple Pay genutzt werden. Anbieter, die Zahlungssysteme auf NFC-Basis anbieten, stellen aus diesem Grund oftmals auch Alternativen, wie NFC-Sticker oder NFC-Kreditkarten zur Verfügung, um auch iOS[12]-Nutzer und Nutzer von nicht NFC-fähigen Smartphones oder klassischen Mobiltelefonen zu erreichen, die andernfalls von ihren Systemen ausgeschlossen wären. Würden sie dies nicht tun, würden sie ihre Kundenbasis beschränken und den Erfolg ihres Systems möglicherweise verhindern. Diese Alternativen finden in den folgenden Betrachtungen jedoch keine Berücksichtigung.

Um sofort möglichst viele Akzeptanzstellen anbieten zu können, kooperieren viele Anbieter mit den Kreditkartennetzwerken Visa und MasterCard, die für ihre Systeme PayPass und payWave bereits viele Akzeptanzstellen gewinnen konnten. Durch die Kooperation stehen diese den neuen Anbietern auch sofort zum Start zur Verfügung.

Für NFC-basierte mobile Paymentsysteme prognostiziert ABI Research ein Wachstum des Marktvolumens von rund 4 Mrd. US-Dollar in 2012 auf 191 Mrd. US-Dollar in 2017 (27).

[12] iOS ist Betriebssystem von Smartphones der Firma Apple.

1.3.1.1 mpass

mpass ist Ende 2008 aus einer Kooperation von Vodafone und Telefónica O2 entstanden (28). Ende 2010 stieg auch die Deutsche Telekom in das Projekt ein. Mittlerweile scheint mpass jedoch mehr und mehr ein reines Telefónica O2-Projekt zu werden. Auch wenn weder Vodafone noch Telekom die Kooperation offiziell aufgekündigt haben, ist in Werbevideos für mpass die Rede von dem „modernen Zahlungssystem von O2“ (29). Auch übernimmt Telefónica, die Muttergesellschaft von O2, verschiedene Aufgaben rund um das Projekt mapss: So ist die Domain mpass.de über Telefónica Germany GmbH und Co. OHG registriert worden und Marketingmaßnahmen werden durch die Telefónica Media Services durchgeführt. Einzig Vodafone tritt noch als Pressekontakt in Erscheinung – allerdings auch neben einem Vertreter von Telefónica Deutschland.

Ursprünglich bot mpass ausschließlich das Bezahlen kleinerer Beträge im Internet über das Mobiltelefon an. Mittlerweile hat sich mpass jedoch zu einem universellen Zahlungssystem gewandelt, dessen Vorteil der kurze Registrierungsprozess für die Vertragskunden der drei Netzbetreiber ist. Für diese liegen die notwendigen Daten, wie Adresse und Bankverbindung für das Lastschriftverfahren, bereits vor und können ohne Neueingabe bei mpass direkt genutzt werden. Kunden, die eines der Prepaid-Angebote nutzen, und Kunden von E-Plus müssen einen aufwendigeren Registrierungsprozess durchlaufen, bei dem alle relevanten Daten abgefragt werden.

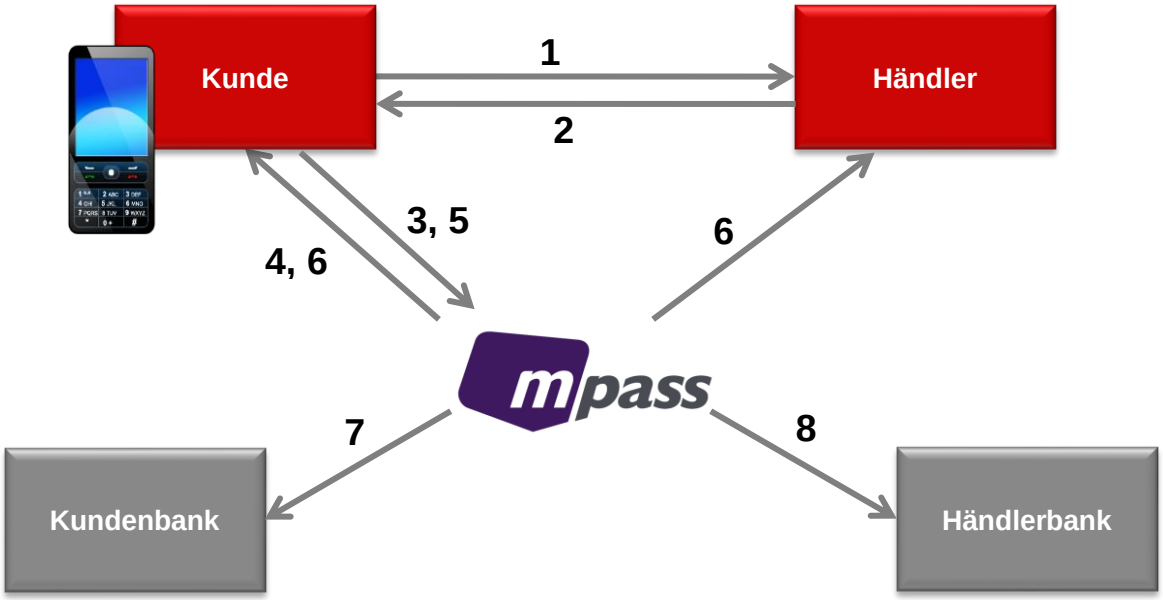

Abbildung 4: Ablauf einer Zahlung mit mpass unter Verwendung des SMS-Tan-Verfahrens.

Die Bezahlung erfolgt bei Zahlungen über das Internet durch die Übermittlung des Wunsches mit mpass zu bezahlen an den Händler (Schritt 1). Dieser leitet den Kunden dann auf eine mpass Seite weiter (Schritt 2), auf der zunächst die registrierte Mobilfunknummer und das Kennwort für das Kundenkonto eingegeben werden müssen (Schritt 3). mpass generiert eine zu dieser Transaktion gehörende TAN, die per SMS an den Kunden übermittelt wird (Schritt 4). Diese gibt der Kunde auf der nächsten Seite wieder ein und sendet diese an mpass zurück (Schritt 5). Stimmt

die TAN meldet mpass die erfolgreiche Transaktion an den Händler und leitet den Kunden zurück auf die Seiten des Händlers (Schritt 6). Im Nachgang initiiert mpass die Lastschrift vom Konto des Kunden (Schritt 7) und die Gutschrift auf das Händlerkonto (Schritt 8), um den Bezahlvorgang abzuschließen.

In 2012 startete mpass auch als Bezahlverfahren am Point-of-Sales. Hierzu begann eine Kooperation mit Wirecard Card Solutions und MasterCard. mpass ist im Unterschied zu MyWallet und SmartPass bisher eine reine Sticker-Lösung. Der NFC-Sticker enthält die Kreditkartendaten, wie sie auch für MasterCard PayPass verwendet werden, so dass es sich hierbei im Prinzip um ein PayPass-Derivat handelt. Einziger Unterschied ist die angebotene mpass-App, in der alle Transaktionen, Shops, die PayPass unterstützen, sowie zusätzliche Aktionen, wie Rabattprogramme, aufgelistet werden.

Die zu der dahinterliegenden Kreditkarte gehörigen Daten wie Kreditkartennummer, Ablaufdatum und Sicherheitscode sind sowohl im mpass-Kundenkonto als auch in der App einsehbar, so dass diese auch für das online Bezahlen verwendet werden können. mpass bezeichnet dies als virtuelle Kreditkarte, die in allen Onlineshops eingesetzt werden kann die mpass nicht über SMS-Tan unterstützen.

Als Nutzer mir einem O2-Mobilfunkvertrag und einem unterstützten Smartphone von Samsung kann mpass auch wie O2 Wallet vollständig ohne Aufkleber über das Smartphone verwendet werden.

Somit stellt mpass insgesamt drei verschiedene Bezahlverfahren für unterschiedliche Anwendungszwecke zur Verfügung.

1.3.1.2 Telekom MyWallet / Vodafone SmartPass / O2 Wallet / E-Plus Mobile Wallet

Alle vier genannten Systeme arbeiten auf vergleichbare Art und Weise. So kooperieren die Mobilfunkbetreiber mit einem Kreditkartennetzwerkbetreiber – meist MasterCard oder Visa – und einem Inhaber einer E-Geld-Lizenz[13]. Letztere ist notwendig, da es sich bei keinem der Anbieter um ein Kreditinstitut im klassischen Sinne handelt und diese nach der Europäischen Richtlinie 2000/46/EG mit elektronischem Geld umgehen.

MyWallet, als Dienst der Deutschen Telekom, kooperiert mit click&buy, einer Telekom-Tochter, die eine Lizenz zur Ausgabe und Verwaltung von E-Geld in Großbritannien hält, und MasterCard. Nachdem der Dienst 2012 zunächst in Polen startete, ist er seit Anfang Mai 2014 auch in Deutschland verfügbar (31).

[13] Elektronisches Geld (E-Geld) ist im Sinne der EU-Richtlinie ein elektronischer Ersatz für Münzen und Banknoten. Es wird elektronisch gespeichert und kann für die Durchführung elektronischer Zahlungen verwendet werden (30).
Eine E-Geld-Lizenz ermöglicht dem Inhaber mit E-Geld umzugehen und Dienste, die darauf basieren, anzubieten.

Bereits Ende 2013 startete Vodafone seinen Service SmartPass in Kooperation mit der Wirecard AG, die über ihre Tochter Wirecard Bank AG eine deutsche Vollbanklizenz[14] hält (33), und Visa zunächst in Spanien. Seit Anfang 2014 wird der Dienst nun auch in Deutschland angeboten (34).

E-Plus kooperiert, genau wie Vodafone, mit der Wirecard AG, verwendet aber statt des payWave-Systems von Visa das PayPass-System von Maestro (35). Maestro ist ein Dienst von MasterCard, über den Debitkarten angeboten werden (36). Da Maestro zu MasterCard gehört kann mit der E-Plus Mobile Wallet an allen PayPass-fähigen Akzeptanzstellen gezahlt werden.

Der spanische Telekommunikationsanbieter Telefónica bietet über seine Marke O2 die O2 Wallet an. Auch hierbei handelt es sich um eine Maestro Card, die durch mpass und somit durch die Wirecard Bank AG ausgegeben wird.

Neben den, durch den Dienst ausgegebene Karten, planen alle Anbieter auch die Einbindung anderer Karten. So kündigt O2 beispielsweise in seinen FAQ zur O2 Wallet an, künftig auch Visa- und American Express-Karten zu unterstützen (37). Außerdem sehen alle Pläne der Netzbetreiber auch die Integration von Kundenkarten, Fahrscheinen, sowie Eintrittskarten für Veranstaltungen und Gutscheinsystemen vor.

Grundlage für alle Dienste bilden somit das PayPass-System von MasterCard bzw. payWave von Visa über das die Bezahlvorgänge abgewickelt werden. Gemein ist ebenfalls allen Systemen, dass die Netzbetreiber lediglich eine App für Smartphones bereitstellen, über die die Zahlungen verwaltet werden können. Voraussetzung für die Nutzung ist jedoch eines der durch den Netzbetreiber freigegebenen Smartphone-Modelle mit einer durch den Netzbetreiber bereitgestellten Firmware (38–41). Im Falle der Deutschen Telekom werden derzeit 18 Smartphone-Modelle unterstützt, während mit dem System von O2 gerade einmal zwei Modelle kompatibel sind. Somit ist der Dienst nur für Kunden nutzbar, die Kunden des jeweiligen Netzbetreibers sind und ihr Smartphone direkt über den Netzbetreiber erworben haben. Die Telekom selbst gibt an, das MyWallet dadurch für mehr als zwei Millionen ihrer Kunden nutzbar ist (31).

Alle Kunden, die kein kompatibles Endgerät besitzen, haben die Möglichkeit einen NFC-Sticker anzufordern, auf dem die Kreditkartendaten hinterlegt sind, um diesen zum Bezahlen zu verwenden. Ein Bezahlvorgang über den Sticker entspricht der Zahlung mit MasterCard PayPass bzw. Visa payWave und wird im Folgenden nicht weiter betrachtet. Wird der Sticker auf einem Smartphone angebracht, dass auch NFC unterstützt, so kann dies zu Problemen bei der Zahlung führen, da die Zahlungsterminals den Vorgang abbrechen, sobald mehr als ein NFC-Sender in den Empfangsbereich des Terminals kommt (42, 43).

[14] Gemäß §§ 32 Abs. 1 Kreditwesengesetz (KWG) ist für das Betreiben von Bankgeschäften und das Erbringen von Finanzdienstleistungen eine Erlaubnis der Bundesanstalt für Finanzdienstleistungsaufsicht erforderlich. Diese sogenannten Banklizenzen werden in Vollbanklizenzen für CRR-Kreditinstitute (vgl. §1 Abs. 3d KWG) und Teilbanklizenzen für beispielsweise den Umgang mit E-Geld unterschieden (32).

Für die Nutzung wird eine spezielle SIM-Karte des Netzbetreibers, NFC-SIM genannt, benötigt. Diese enthält ein Secure Element[15] auf dem die Daten einer virtuellen Kreditkarte gespeichert sind. Die rund 1,3 MB Speicherplatz (45) dieses Elementes dient der verschlüsselten Speicherung der Kreditkarten- und Transaktionsdaten, aber auch für andere Karten. Diese Daten können, laut E-Plus, nur über einen gesicherten Kanal durch den Netzbetreiber beschrieben werden (46).

Der Bezahlvorgang selbst läuft wie bei PayPass bzw. payWave ab, wobei das Handy die Kreditkarte simuliert. Zunächst startet der Kunde die App seines Anbieters mit seiner PIN und beginnt dann den Bezahlvorgang auf seinem Gerät, indem er die entsprechende Schaltfläche wählt. Nun wird der NFC-Chip aktiviert und reagiert erst jetzt auf Anfragen des Lesegeräts. Beträge bis 25,- € können ohne jegliche Authentifizierung bezahlt werden. Bei größeren Summen ist eine Autorisierung der Zahlung mittels PIN notwendig.

1.3.2 QR-Code basierte Systeme

Eine andere Variante des mobilen Bezahlens arbeitet mit QR-Codes. QR-Codes sind von der ISO/IEC[16] standardisierte 2D-Codes, die beliebige Informationen enthalten und beispielsweise durch Smartphones oder andere, mit einer Kamera ausgestattete Geräte, ausgelesen werden können (47). Hierdurch sind die Voraussetzungen für die Nutzung relativ gering, da die meisten Smartphones eine Kamera enthalten, die hierfür verwendet werden kann.

1.3.2.1 Yapital

Yapital wurde 2011 als hundertprozentige Tochter der Otto Group gegründet. Diese positioniert Yapital als „europäisches, bargeldloses Cross-Channel-Payment“-System (48). Hierzu erwarb Yapital an seinem Firmensitz in Luxemburg eine Banklizenz, um als E-Geld-Institut anerkannt zu werden. 2013 startete Yapital am Markt und kann seitdem als alternative Bezahlmethode in allen Rewe-Filialen der REWE Markt GmbH, sowie bei einigen Unternehmen der Otto Gruppe, zu denen u.a. SportScheck und BAUR gehören, eingesetzt werden.

Außerdem besteht eine Kooperation mit MasterCard, auf Grundlage dessen jeder Nutzer eine Kreditkarte von MasterCard bekommt. Damit kann überall dort bezahlt werden, wo Yapital nicht

[15] Da das Smartphone grundsätzlich als unsicheres System betrachtet wird, ist es zur Speicherung sicherheitsrelevanter Daten, wie eben der Kreditkartendaten, erforderlich ein zusätzliches Hardwaremodul zu verwenden, auf dem diese Daten kryptographisch gesichert abgelegt werden. Dieses Hardwaremodul kann Teil der SIM-Karte oder einer Speicherkarte sein, aber auch direkt in das Smartphone integriert sein, wie bspw. bei Apples iPhone (44).

[16] Die ISO (International Organization for Standardization) und die IEC (International Electrotechnical Commission) arbeiten gemeinsam an weltweiten Standards.

direkt als Bezahlmethode akzeptiert wird. Diese wird in der folgenden Bewertung allerdings nicht berücksichtigt.

Anfang Juni 2014 wurde Yapital mit dem eco Internet Award 2014 ausgezeichnet, da es „eine innovative App, die einfach und pragmatisch gesicherte Transaktionen ermöglicht“ (49), bietet. Die Jury meint, dass „damit eine echte Alternativ zum Bezahlen mit EC- oder Kreditkarte zur Verfügung“ (49) steht.

Um Yapital nutzen zu können, muss sich der Kunde zunächst registrieren. Nach erfolgter Registrierung kann die App für Android, iOS und Windows Phone heruntergeladen und mit dem Yapital-Konto gekoppelt werden. Vor dem ersten Bezahlen muss Yapital nun noch eine Zahlungsquelle hinzugefügt werden. Dies kann aktuell entweder ein Bankkonto oder eine Kreditkarte sein. Yapital kann sowohl als Pre- als auch als Postpaid[17]-Verfahren verwendet werden. In beiden Fällen findet eine Lastschrift statt (Schritt 1).

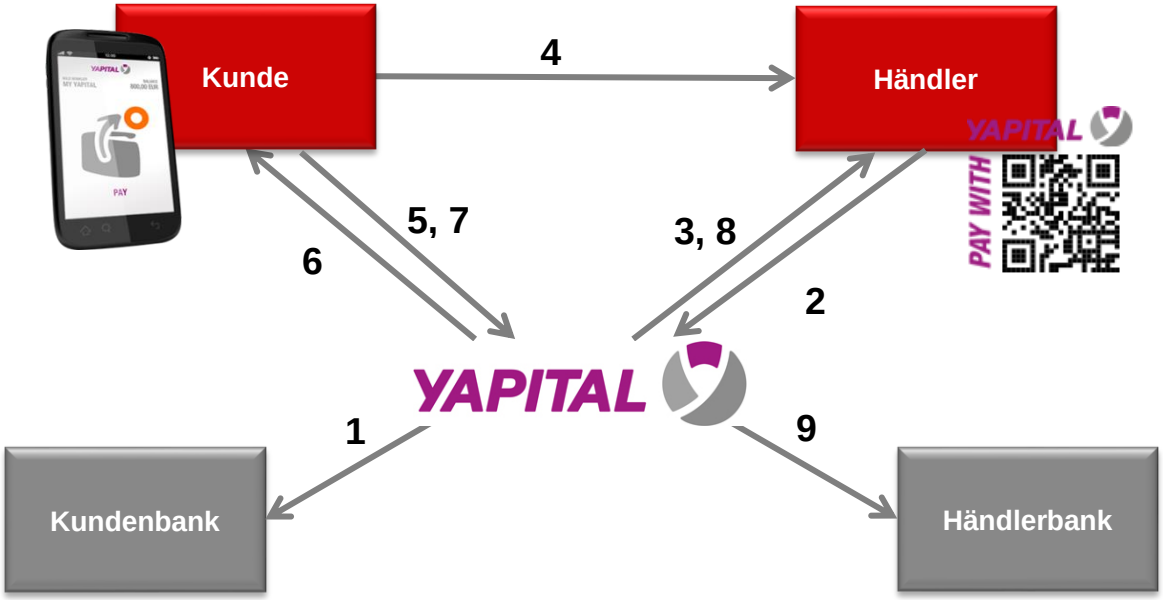

Abbildung 5: Ablauf einer Transaktion mit Yapital.

Der Bezahlvorgang läuft wie folgt ab: Zunächst meldet der Händler eine Transaktion bei Yapital an (Schritt 2). Yapital generiert hierzu eine Transaktionsnummer, die es an den Händler zurückmeldet (Schritt 3). Dieser generiert einen passenden QR-Code, den er entweder direkt am POS, im Laufe des Bezahlprozesses auf seiner Webseite oder auf der Rechnung anzeigt. Der Kunde scannt diesen anschließend mit der Yapital-App (Schritt 4). Die App liest die Transaktionsnummer aus, sendet sie an Yapital (Schritt 5) und ruft die zu dieser Transaktion gehörenden Daten über die Internetverbindung des Smartphones ab (Schritt 6). Laut den Yapital Datenschutzbe-

[17] Im Falle der Postpaid-Zahlung wird ein mit Yapital bezahlter Betrag erst danach vom verknüpften Bankkonto abgebucht, so dass das Yapital-Konto wieder ausgeglichen ist. Im Unterschied zur Prepaid-Zahlung muss das Konto im Vorhinein also nicht aufgeladen werden.

stimmungen sind diese Daten „insbesondere Summen, Referenzen, Daten, Informationen zur Identität des Bezahlers oder des Begünstigten, zugehörige Waren und Dienstleistungen, usw.“ (50). Der Kunde bestätigt die Zahlung nun auf seinem Gerät (Schritt 7). Diese Bestätigung wird auch an den Händler übermittelt, um den Bezahlvorgang abzuschließen (Schritt 8). Im Anschluss erfolgen entsprechende Gut- bzw. Lastschriften (Schritt 9) durch Yapital.

1.3.2.2 PAYMEY

PAYMEY ist ein mobiles Bezahlverfahren der PAYMEY GmbH aus Welzheim bei Stuttgart. Gegründet wurde das Unternehmen in 2013 nachdem der Gründer während seines Urlaubs sein Portemonnaie vergessen hatte und nur mit seinem Smartphone unterwegs war. Zusammen mit Informatikern und anderen Fachleuten entwickelte er ein System, welches das Bezahlen über ein Smartphone ermöglichen sollte (51).

Nachdem die Planungen abgeschlossen waren, wurde ein Patent für die Generierung von mobilen TANs eingereicht und parallel dazu eine Crowdfunding-Kampagne gestartet, über die eine erste Finanzierung sichergestellt werden sollte. Das Ziel von 100.000,- € wurde bereits nach 31 Stunden erreicht und auf 300.000,- € erhöht. Anfang Januar 2014 erschien dann zunächst eine iOS-App. Eine App für Android soll im zweiten Quartal 2014 erscheinen, eine Windows Phone App ist bisher nur geplant, aber noch nicht angekündigt.

PAYMEY sieht sich, genau wie Yapital, als Zahlungssystem über alle Kanäle und Marketinginstrument. So beabsichtigt das Unternehmen u.a. die Einbindung von Beacons, bei der mittels Bluetooth Low Energy Informationen über Produkte an das Endgerät des Kunden gesendet werden können.

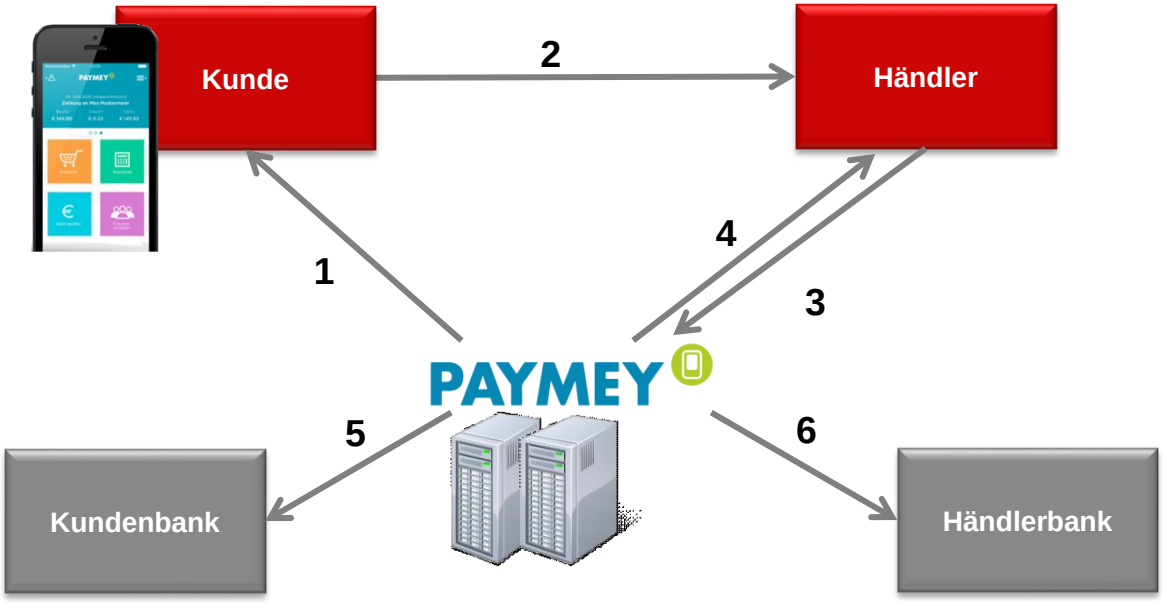

Abbildung 6: Ablauf einer Zahlung mit PAYMEY (52).

Wie andere Anbieter mobiler Zahlungssysteme benötigt auch PAYMEY eine Banklizenz für den Umgang mit E-Geld. Diese Lizenz hat das Unternehmen durch eine Kooperation mit der deutschen net-m Privatbank 1891 AG. Die Verarbeitung der PAYMEY überlassenen Daten findet in Irland statt (53).

Teil des durch Tobias Pfütze, Gründer und Geschäftsführer von PAYMEY, eingereichten Patents ist die Abwicklung von Bezahlvorgängen am POS, bei denen der Kunde keine Internetverbindung benötigt. Hierzu tauschen der PAYMEY-Server und die App auf dem Kundengerät vor dem Bezahlvorgang Transaktionscodes aus, die zu einem späteren Zeitpunkt zum Bezahlen verwendet werden können (52). Die Zahlung am POS erfolgt dann, indem der Händler als Bezahlart die PAYMEY-Bezahlung auswählt und den zu zahlenden Betrag eingibt. Parallel dazu startet der Kunde die App auf seinem Smartphone, wählt die Bezahlen-Option aus und authentifiziert sich mit seinem PIN-Code. Die App generiert daraufhin einen Barcode, der durch den Zahlungsempfänger eingelesen wird. Der Barcode besteht aus einem zufällig ausgewähltem Teil der Benutzerkennung und dem Transaktionscode. Der Händler übermittelt diese Daten an PAYMEY, die die Zahlung autorisieren. PAYMEY führt anschließend eine Lastschrift auf dem Konto des Kunden und eine Überweisung auf das Konto des Händlers aus.

Zusätzlich kann PAYMEY auch als Marketinginstrument verwendet werden. So ist es beispielsweise möglich, einen PAYMEY QR-Code auf eine Anzeige für ein Produkt zu drucken. Scannt der Kunde diesen, kann er den beworbenen Artikel direkt bestellen. Im Hintergrund übermittelt PAYMEY die Bestellung an den Anbieter zusammen mit der bei PAYMEY hinterlegten Adresse des Kunden.

1.3.3 Bluetooth Low Energy basierte Systeme

Eine andere Technologie, die in vielen Smartphones integriert ist und vielen Nutzern bekannt sein dürfte, ist Bluetooth. Die Technologie wird bereits für viele Zwecke genutzt, insbesondere zum Austausch von Daten, wie Kontakten zwischen mobilen Geräten, Verbindungen von Headset und Smartphone sowie ähnlichen Anwendungen. Ein Problem war bisher der relativ hohe Stromverbrauch, der dazu führte, dass viele Nutzer Bluetooth vollständig deaktiviert haben. Mit dem neuen Bluetooth 4.0 Standard[18] wurde jedoch Bluetooth Low Energy (BLE) spezifiziert, welches genau dieses Problem lösen soll und mittlerweile auch in immer mehr Geräten verfügbar ist.

[18] Der Standard Bluetooth 4.0 wurde 2009 offiziell verabschiedet und fügte dem bisherigen Protokollstapel, Bluetooth Classic genannt, einen weiteren für Low Energy hinzu. Entsprechende Chips waren ab 2010 verfügbar, allerdings unterstützte Googles Betriebssystem Android Bluetooth 4.0 erst ab Version 4.3, die Mitte 2013 erschien. Apples iPhone unterstützt Bluetooth 4.0 seit dem iPhone 4S.

1.3.3.1 PayPal Beacon

PayPal schlägt mit seinem Bezahlverfahren einen etwas anderen Weg ein als alle anderen Anbieter. Zwar wird ein Smartphone mit passender App benötigt, dieses kann jedoch während des Einkaufens und Bezahlens komplett in der Tasche verbleiben und muss nicht durch den Kunden bedient werden.

Bisher ist Beacon noch nicht in Deutschland verfügbar, allerdings hat PayPal in Amerika bereits in einer Kooperation mit Anbietern für Kassensysteme zusammengearbeitet. Die Bezahlung erfolgt letzten Endes mit dem PayPal-Konto, welches 148,40 Millionen Menschen weltweit bereits nutzen (54).

Zur Verwendung der Technologie benötigt der Händler einen Beacon-Dongle von PayPal, einen Bluetooth USB-Stick, der zusätzlich ein WLAN zur Verfügung stellt. Der Dongle arbeitet dabei unabhängig von einem PC und benötigt lediglich Strom, so dass er auch über einen Adapter direkt in der Steckdose betrieben werden kann.

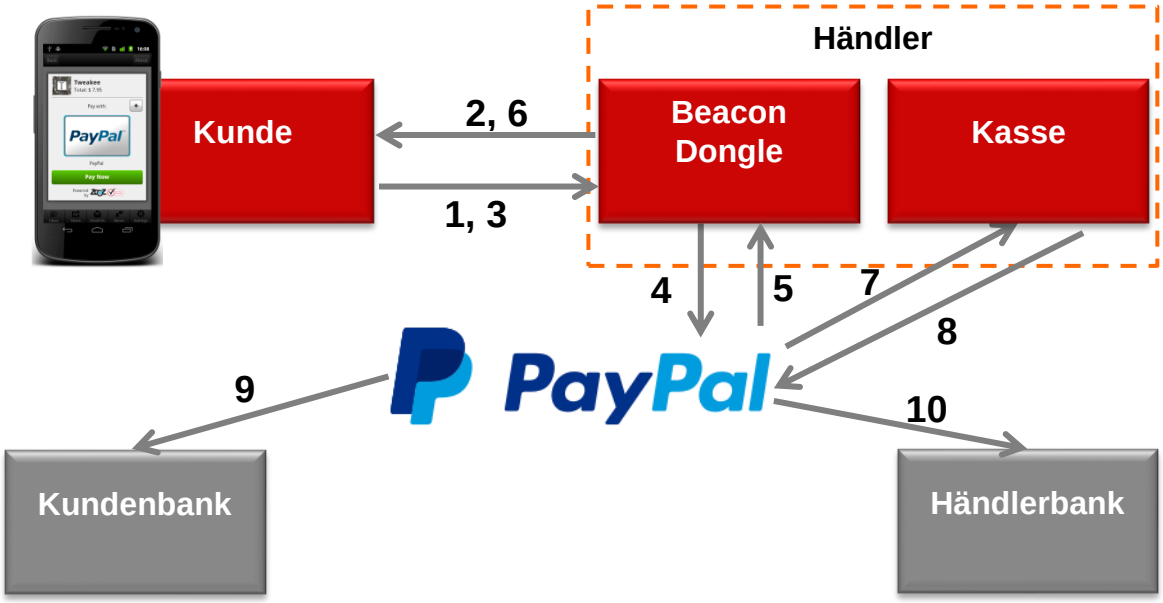

Abbildung 7: Ablauf einer Transaktion mit PayPal Beacon.

Die Funktionsweise von PayPal Beacon wird durch PayPal-Mitarbeiter John Lunn im Developer Blog des Unternehmens wie folgt erläutert (55): Das Smartphone des Kunden fragt regelmäßig in seiner Umgebung nach Bluetooth Signalen. Kommt es in die Nähe eines Beacon-Dongles, so empfängt das Smartphone dessen Signal und die PayPal App wird aktiviert, verbindet sich mit dem Dongle und fordert einen Token, eine eindeutige Zeichenfolge, an. Der Dongle sendet der App neben einem der in seinem Cache[19] gespeicherten Token, eine Nonce[20], einige Metadaten[21]

[19] Der Beacon besitzt einen Speicher, in dem er einige, mit den PayPal-Servern ausgetauschte Token vorhält.

[20] Eine Nonce ist eine frei wählbare, beliebige Zeichenfolge.

[21] Die Metadaten geben der App an, in welchem Geschäft der Check-In erfolgen soll.

und ein zu der Nachricht gehörende kryptographische Signatur. Die App überprüft, dass die Signatur zu dem in der App hinterlegten Public Key passt. Sofern der Kunde dies erlaubt hat, checkt die App ihn anhand der Metadaten automatisch im Laden ein. Andernfalls ist ein manueller Check-In nötig, bei dem der Kunde in der App hinterlegen kann, dass er in diesem Geschäft künftig automatisch eingecheckt werden möchte. Zu diesem manuellen Check-In fordert die App den Nutzer ggf. auf. Die Einstellung bezüglich des automatischen Login bezieht sich immer nur auf ein Geschäft, so dass der Kunde pro Geschäft das gewünschte Verhalten auswählen kann. Der manuelle Check-In ist bereits heute für Kunden möglich und lässt sich, nach einem erfolgreichen Test in Berlin, nun Deutschlandweit bei teilnehmenden Händlern nutzen (56).

Ist der Check-In über einen der beiden Wege erfolgt, sendet die App Daten an den Dongle zurück, der in diesem Fall den Check-In auf den PayPal-Servern übernimmt. War dieser erfolgreich, meldet der Beacon dies an die App zurück und die Verbindung zwischen App und Dongle wird abgebaut. Findet kein Check-In statt wird die Verbindung direkt wieder abgebaut und es wurden keine Daten, die den Kunden identifizieren könnten, an den Beacon übertragen.

Das Kassensystem fragt bei PayPal an, welche Kunden aktuell im eigenen Geschäft eingecheckt sind. Zu jedem Kunden erhält die Kasse ein Foto und die ID. Der Kunde teilt dem Händler beim Bezahlen einfach mit, dass er mit PayPal bezahlen möchte. Der Händler wählt das Foto des Kunden aus. Im Hintergrund fordert das Kassensystem bei PayPal den entsprechenden Betrag vom Kundenkonto an. PayPal erstellt eine Transaktion hierfür und der Bezahlvorgang ist abgeschlossen, ohne dass der Kunde aktiv werden musste. Letzterer erhält lediglich eine Benachrichtigung innerhalb der App bezüglich des Einkaufs und auf Wunsch auch eine E-Mail, jeweils mit allen Informationen zu seinem Einkauf.

1.4 Internetwährungen

Im Folgenden werden die Systeme vorgestellt, deren Entwicklung primär als Zahlungssystem für das Internet begann und die für Zahlungen eigene Einheiten verwenden.

Historie

Bereits 1982 begann der sich viel mit Kryptographie befassende Erfinder David Chaum sich Gedanken über ein neues Zahlungssystem zu machen, dass dem Wachstum des neu aufkommenden Online-Bankings gerecht werden sollte. Hierzu entwickelte er die Idee der „Blind Signature“ deren Einsatzzweck er bei anonymen, elektronischen Wahlen sah. Chaum erkannte aber auch, dass ähnliche Anforderungen für das Bezahlen gelten, denn auch hier ist es der Wunsch des Nutzers, dem Zahlungsempfänger gegenüber seine Bezahldaten nicht preisgeben zu müssen. Gleichzeitig hat der Staat das Bedürfnis Zahlungen überwachen zu können, um beispielsweise Geldwäsche zu unterbinden (57).

Erste Versuche ein solches Zahlungssystem im Internet umzusetzen unternahm Chaum mit seinem Unternehmen DigiCash, welches eCash entwickelte. Das System wurde nach der Idee von DigiCash mit dem Bankkonto des Kunden verbunden.

Wollte ein Kunde Geld an andere übertragen, so erzeugte er mittels der eCash-Software eine verschlüsselte Datei, die den Wert der Überweisung darstellte. Da dieser im Nachhinein nicht mehr änderbar war und durch eine Seriennummer identifiziert werden konnte, bezeichnete DigiCash die Dateien als Cybercoins. Die erzeugte Datei wurde an die Bank übertragen, die wiederum prüfte, ob ein ausreichendes Guthaben auf dem Kundenkonto vorhanden war. War dem so, signierte die Bank die Datei und verringerte das Guthaben auf dem Kundenkonto entsprechend. Für die Signierung verwendete die Bank einen Schlüssel, der eindeutig dem gewählten Betrag zuzuordnen war. Die so veränderte Datei wurde an die eCash-Software auf dem Kundenrechner zurückgesendet. Diese entfernte die Signatur, die sie selbst vor der Übertragung an die Bank hinzugefügt hatte, um die Anonymität des Nutzers sicherzustellen. Im nächsten Schritt musste die Datei ausgetauscht werden, damit der Betrag an einen anderen Nutzer transferiert wurde, was ebenfalls über die eCash-Software möglich war, prinzipiell aber auch über andere Wege möglich gewesen wäre (58).

Missbrauch sollte verhindert werden, indem jeder Teilnehmer dazu verpflichtet wurde, ein eCash-Konto bei einer Bank zu führen, die die Nutzung gegebenenfalls reglementieren konnte. Als Partnerbanken, die eCash-Konten unterstützten, konnte unter anderem die Deutsche Bank gewonnen werden. Mit der Insolvenz von DigiCash und dem damit einhergehenden

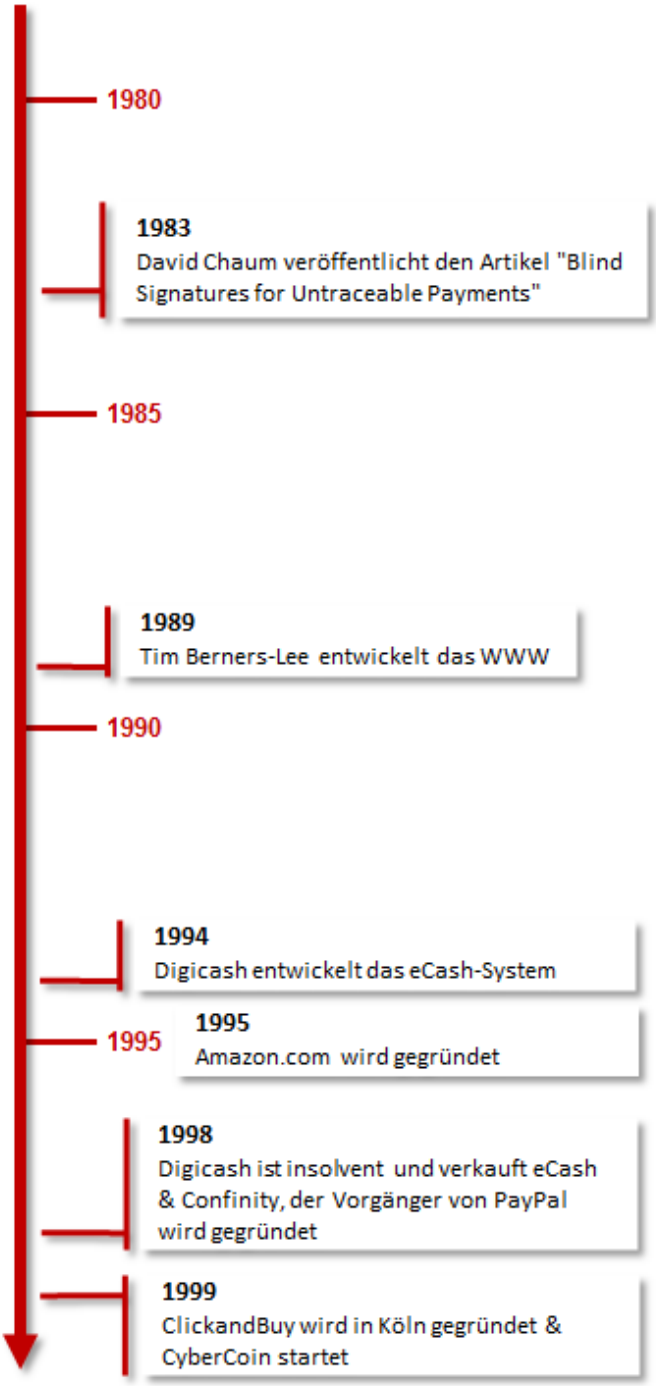

Abbildung 8: Entwicklung von Internetzahlungssystemen (1980 - 1999).

Verkauf von eCash, sowie dem ausbleibenden Erfolg des Systems, wurde das System 2001 in Deutschland eingestellt. Ein Beispiel für den ausbleibenden Erfolg ist, dass die Deutsche Bank nie mehr als 50 Händler, die eCash akzeptierten, gewinnen konnte (59).

Das vergleichbare System CyberCoin des Unternehmens CyberCash, welches in Deutschland die Dresdener Bank als Partner gewinnen konnte, hatte ähnliche Probleme wie eCash: Nur wenige Händler unterstützten das System und das Interesse der Kunden war zugleich gering, was sicherlich auch daran lag, dass nicht jeder von einer zusätzlichen Software nur zum Bezahlen begeistert war. Auch CyberCash stellte das System 2001 ein (60, 61).

Während diese beiden ersten Systeme langsam untergingen, entstanden parallel dazu weitere Systeme mit anderen Ansätzen. So gründeten Ende 1998 Max Levchin und Peter Thiel das Unternehmen Confinity mit dem Ziel eine digitale Geldbörse für den Palm Pilot[22] und andere Personal Digital Assistants (PDA)[23] zu entwickeln. Im Oktober 1999 schließlich stellte Confinity einen Service vor, bei dem Geld über E-Mail übertragen werden konnte (62).

Unterdessen erkannte eBay, als Anbieter einer Plattform für Auktionen, den Nutzen eines eigenen Zahlungssystems für sein Geschäftsmodell. Es kaufte das Unternehmen Billpoint, welches sich auf Geldübertragungen zwischen zwei Personen spezialisiert hatte (63). eBay nannte Billpoint fortan „eBay Payments“, integrierte das System in seine Auktionsplattform und entfernte die Möglichkeit der Nutzung außerhalb der eBay-Plattform. Allerdings fand das System nicht so viel Anklang bei den eBay-Nutzern wie das ähnliche System von Confinity (64).

Anfang 2000 wurde Confinity von der Online-Bank X.com übernommen, die ebenfalls einen Dienst zur Übertragung von Geld via E-Mail betrieb (65). In 2001 wurde aus dem Namen des Produkts von X.com der neue Firmenname: PayPal. Nachdem Anhänger PayPals auf einer Konferenz für eine Integration PayPals in eBays Plattform warben, übernahm eBay PayPal 2002 (62).

Gemein ist allen drei Systemen – X.com, Confinity und Billpoint – das sie andere Ansätze verfolgten als eCash. Es war keine Client-Software notwendig, dafür war die Privatsphäre aber auch nicht derartig geschützt, wie es bei eCash der Fall war. Trotzdem setzte sich PayPal durch, was vor allem auf die einfache Verwendung und die Unterstützung durch eBay zurückzuführen sein dürfte.

In Europa, genauer gesagt in Köln, entstand zur selben Zeit das Zahlungssystem ClickandBuy des Unternehmens Firstgate, welches nach einem ähnlichen Prinzip wie PayPal noch heute funktioniert (66). 2004 begann auch der Kanadier Ryan Fugger mit der Entwicklung eines neuen, offenen Bezahlnetzwerkes, welches auf gegenseitigem Vertrauen und Kreditgewährung der Nut-

[22] Pilot ist der Name des ersten PDA der Firma Palm, der im Jahr 1996 veröffentlicht wurde.

[23] Tragbarer Computer, der hauptsächlich für Kontakt-, Aufgaben- und Terminverwaltung genutzt wird. Heutzutage sind PDAs durch Smartphones fast vollständig verdrängt worden.

zer untereinander basiert. Diese Ripple-Netzwerk genannte Entwicklung ist angelehnt an die Idee eines lokalen Tauschsystems, die Michael Linton schon in den 1980er Jahren zu entwickeln begann. Im Unterschied zum lokal begrenzten System von Linton wollte Fugger ein globales System schaffen, was einige Änderungen erforderte. Diese Entwicklung eines Zahlungsnetzwerkes blieb jedoch weitgehend unbemerkt (67).

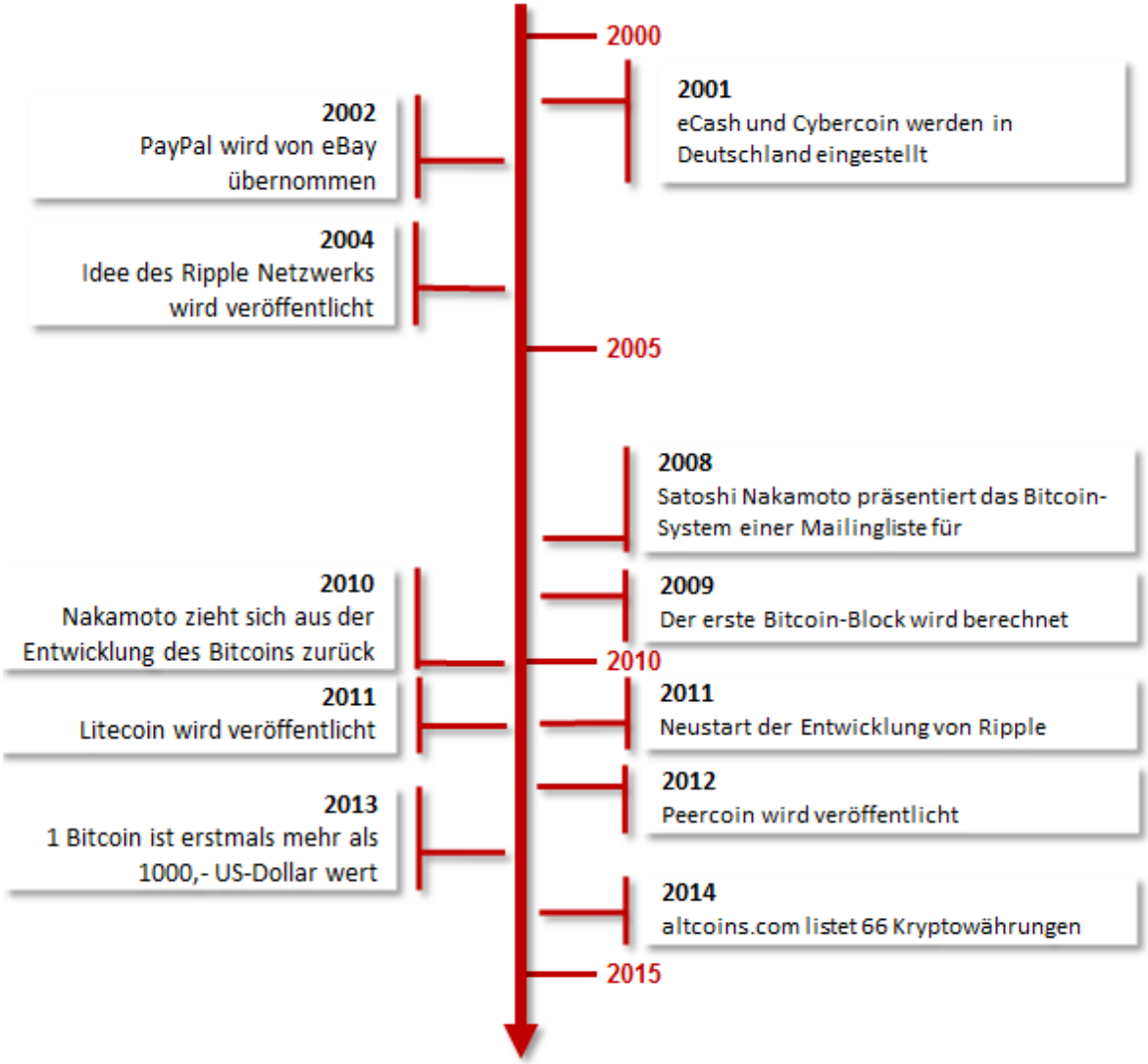

Abbildung 9: Entwicklung von Internetzahlungssystemen (2000 - 2014).

2009 ließ Satoshi Nakamoto die Idee eines anonymen Systems, wie es David Chaum vorschwebte, mit seinem Paper „Bitcoin: A Peer-to-Peer Electronic Cash System“ wiederauferstehen. Allerdings sollte Bitcoin einige Änderungen im Vergleich zum damaligen eCash-System bringen. So war auch bei eCash das Vertrauen in den Staat und die Banken notwendig, die die dahinterstehende Währung verantworten und Zahlungen signierten. Bitcoin hingegen macht dieses durch ein reines P2P-System überflüssig. In Folge der Entwicklung des Bitcoin-System entstanden seit 2011 immer mehr alternative Währungssysteme, die sich – mehr oder weniger – an der Idee des Bitcoin orientieren.

2011 war aber auch das Jahr, in dem Jed McCaleb, der Entwickler des eDonkey-Netzwerks und Gründer der Bitcoin Handelsplattform Mt. Gox, auf die Idee des Ripple-Netzwerkes aufmerksam wurde und einen Neubeginn wagte, nachdem er Mt. Gox an Mark Karpelès, eines der Gründungsmitglieder der Bitcoin Foundation, verkauft hatte. Hierfür gründete er im folgenden Jahr, zusammen mit Chris Larsen, der zuvor u.a. die Mikrokreditvergabeplattform Prosper Marketplace gründete, das Unternehmen OpenCoin. 2013 wurde OpenCoin in Ripple Labs umbenannt und der Source Code der bisherigen Entwicklung unter Open-Source-Lizenz veröffentlicht.

Heute werden allein auf der Website altcoins.com 66 Alternativen zu Bitcoin gelistet. Auch schreitet die Entwicklung stetig voran: Es wird für das Mining verschiedener Coins optimierte Hardware veröffentlicht, neue Systeme entstehen und andere bewähren sich auf Dauer nicht oder sind den Anforderungen der Nutzer nicht gewachsen. Immer mehr Anbieter von Gütern und Dienstleistungen wie Dell oder Expedia setzen auf Bitcoin als Zahlungsmittel und auch PayPal kündigte eine Integration von Bitcoin in sein System an, so dass sich die Sichtbarkeit von Internetwährungen im Alltag stetig erhöht (68, 69).

Entstehende Problem

Mit der Entstehung von Internetwährungen, wie Bitcoin, Peercoin und Co., kommen auf den Staat zunächst einige ungelöste Probleme und Fragestellungen zu. Denn diese Systeme werden von den Befürwortern häufig als Währung bezeichnet, sind diesen zwar auch nicht unähnlich, aber gesetzlichen Währungen deswegen keinesfalls gleichgestellt. So stellt sich für den Staat die Frage, ob dies tatsächlich eine Währung im rechtlichen Sinne ist, die dann auch alle Vorteile einer Währung genießen darf. Diese aufsichtsrechtliche Einordnung hat einige Konsequenzen, denn hierüber bestimmt sich letztlich, ob einzelne Geschäftsmodelle einer Erlaubnis der Aufsichtsbehörde bedürfen und auch ob und welche Steuern auf einzelne Geschäfte entfallen. Diese Fragen werden in den nächsten Abschnitten behandelt, allerdings kann nur der aktuelle Stand wiedergeben werden.

Aufsichtsrechtliche Beurteilung

Für die Aufsicht über Finanzdienstleister ist in Deutschland die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), die als Behörde direkt der Aufsicht des Bundesministeriums der Finanzen unterstellt ist, zuständig (70). Sie „beaufsichtigt Banken, Finanzdienstleister, Versicherungen und den Wertpapierhandel [mit dem Ziel] die Funktionsfähigkeit, Stabilität und Integrität des deutschen Finanzmarktes zu sichern“ (71). Ihre rechtliche Grundlage bildet das Gesetz über das Kreditwesen (KWG), in dem auch die Aufgaben der BaFin definiert werden (vgl. §6 KWG).

In §32 KWG wird festgelegt, dass bestimmte Geschäfte in Deutschland eine Erlaubnis der BaFin benötigen. Zu den Erlaubnispflichtigen Tatbeständen zählen das gewerbsmäßige Betreiben von

Bankgeschäften sowie das Erbringen von Finanzdienstleistungen nach §1 Abs. 1a Satz 2 Nr. 1 – 5 oder Nr. 11 (§32 Abs. 1 KWG). Finanzdienstleistungen im Sinne der genannten Nummern umfassen auch die Vermittlung von An- und Verkäufen von Finanzinstrumenten, den Betrieb von börsenähnlichen Systemen (Multilaterale Handelssysteme), die Personen zusammenbringen, um den An- und Verkauf von Finanzinstrumenten innerhalb des Systems zu vollziehen, sowie das kontinuierliche Anbieten des (Ver)Kaufs von Finanzinstrumenten an einem organisierten Markt oder in einem multilateralen Handelssystem zu selbst gestellten Preisen. Unter dem Begriff Finanzinstrumente subsummiert der Gesetzgeber unter anderem Aktien, Vermögensanlagen, Schuldtitel, Geldmarktinstrumente, Devisen, Rechnungseinheiten und Derivate (72). Eine vollständige Definition des Begriffs findet sich in §1 Nr. 11 KWG.

Prinzipiell wäre eine Einordnung als E-Geld im Sinne der EU-Richtlinie 2000/46/EG denkbar – und aufgrund des Namens naheliegend. Die Umsetzung dieser Richtlinie führte in Deutschland zu einer Anpassung des Gesetzes über die Beaufsichtigung von Zahlungsdiensten (ZAG), in dem auch der Begriff des E-Gelds definiert ist. Nach §1a Abs. 3 ZAG ist E-Geld „jeder elektronisch, darunter auch magnetisch, gespeicherte monetäre Wert in Form einer Forderung gegenüber dem Emittenten, der gegen Zahlung eines Geldbetrages ausgestellt wird, um damit Zahlungsvorgänge im Sinne des § 675f Absatz 3 Satz 1 des Bürgerlichen Gesetzbuchs durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird.“ (73)

Diese Definition trifft auf Bitcoins nicht vollständig zu. Zwar handelt es sich um elektronisch gespeicherte Werte, allerdings gibt es keinen Emittenten, der für die Ausgabe von Bitcoins verantwortlich ist. Dieser wäre aber nach der Definition notwendig. In der EU-Richtlinie heißt es deshalb auch, das E-Geld „einen monetären Wert in Form einer Forderung gegen die ausgebende Stelle [darstellt], der

i.) auf einem Datenträger gespeichert ist,
ii.) gegen Entgegennahme eines Geldbetrags ausgegeben wird, dessen Wert nicht geringer ist als der ausgegebene monetäre Wert,
iii.) von anderen Unternehmen als der ausgebenden Stelle als Zahlungsmittel akzeptiert wird.“ (30)

Aus diesem Grunde handelt es sich nach Einschätzung der Bundesanstalt für Finanzdienstleistungsaufsicht bei Bitcoins auch nicht um E-Geld, und analog dazu vermutlich auch nicht bei allen anderen Internetwährungen, sondern um Rechnungseinheiten (74, 56). Dies führt letztlich dazu, dass gewisse gewerbliche Tätigkeiten im Umgang mit Bitcoins eine Erlaubnis der BaFin voraussetzen.

Werden Bitcoins ausschließlich als Tauschgut verwendet, um Waren oder Dienstleistungen zu bezahlen, so wird hierfür keinerlei Erlaubnis benötigt. Auch das Mining allein ist kein grundsätzlich erlaubnispflichtiger Tatbestand. Als erlaubnispflichtige Tätigkeiten im Zusammenhang mit

Bitcoins hat die BaFin Finanzkommissionsgeschäfte, den Betrieb eines multilateralen Handelssystems, die Vermittlung und den Eigenhandel identifiziert.

Finanzkommissionsgeschäfte sind nach §1 Abs. 1 Nr. 4 KWG Geschäfte, bei denen Finanzinstrumente im eigenen Namen, aber auf fremde Rechnung angeschafft oder veräußert werden (72). Die BaFin hat in dem Fachartikel „Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer“ von Jens Münzer einige Kriterien festgelegt, die die Einordnung erleichtern sollen. So muss eine Erlaubnis für ein Finanzkommissionsgeschäft eingeholt werden, „wenn:

- die einzelnen Teilnehmer den Plattformen gegenüber bis zur Ausführung der Order weisungsbefugt sind, indem sie die Zahl und den Preis der Geschäfte vorgeben,
- den jeweiligen Teilnehmern ihre Handelspartner nicht bekannt sind und die BTC-Plattform nicht als Vertreter der Teilnehmer, sondern im eigenen Namen auftritt,
- die wirtschaftlichen Vor- und Nachteile der Geschäfte die Teilnehmer treffen, die Geld auf Plattform-Konten überweisen oder BTC auf deren Adressen übertragen, und
- die BTC-Plattform verpflichtet ist, den Teilnehmern über die Ausführung der Geschäfte Rechenschaft abzulegen und angeschaffte BTC zu übertragen.“ (74)

Unter dem Betrieb eines multilateralen Handelssystems versteht der Gesetzgeber nach §1 Abs. 1a Nr. 1b KWG ein System mit festgelegten Regeln, dass einer Vielzahl von Personen ermöglicht Finanzinstrumente anzukaufen bzw. zu verkaufen, indem es ihre Interessen so zusammenbringt, dass dies zu einem Kauf von eben jenen Finanzinstrumenten führt (72). Die BaFin beschreibt dies im Zusammenhang mit Bitcoins als Systeme, in denen Angebote zum Kauf und Verkauf von Bitcoins zu, durch den Kunden definierten Konditionen gemacht werden können. Das System findet dann zusammenpassende Offerten und Nachfragen und führt die Transaktion aus, ohne die Zustimmung für die konkrete Transaktion einzuholen (74).

Als Vermittlung beschreibt die BaFin den Betrieb von Verzeichnissen, die gegen Entgelt zugänglich sind und Personen listen, die Bitcoins kaufen oder verkaufen (74). Hierbei handelt es sich um eine Anlage- oder Abschlussvermittlung. Das KWG versteht unter der Anlagevermittlung „die Vermittlung von Geschäften über die Anschaffung und die Veräußerung von Finanzinstrumenten“ (§1 Abs. 1a Nr. 1 KWG) und unter Abschlussvermittlung „die Anschaffung und die Veräußerung von Finanzinstrumenten im fremden Namen für fremde Rechnung“ (§1 Abs. 1a Nr. 2 KWG). Unter Eigenhandel versteht die BaFin den Betrieb von Plattformen ähnlich den Wechselstuben, in denen gesetzliche Währungen in Bitcoin getauscht werden können (74). Konkret auf bekannte Geschäftsmodelle im Umfeld von Bitcoins bezogen bedeutet dies, dass das Betreiben eines Mining-Pools erlaubnispflichtig ist, da mit dieser Tätigkeit ein besonderer Beitrag zur Schaffung und Erhaltung des Marktes für Bitcoins geleistet wird. Dies kann zusätzlich auch ein Eigenhandel sein, wenn der Pool-Betreiber seine Mitglieder mit gesetzlichen Währungen bezahlt. Einzelne Mitglieder eines Pools, die Mining betreiben, benötigen keine gesonderte Lizenz für ihre Tätigkeit. Gleiches gilt für das alleinige Mining.

Handelsplattformen werden immer eine Lizenz benötigen, da sie, je nach Geschäftsmodell, ein Finanzkommissiongeschäft, eine Anlagenvermittlung oder einen Eigenhandel betreiben. So unterhält beispielsweise die Bitcoin Deutschland AG mit ihrer Plattform bitcoin.de eine Anlagenvermittlung im Sinne des KWG. Die hierfür notwendige Lizenz hält die FIDOR Bank AG, die die Haftungsübernahme für die Bitcoin Deutschland AG bei der BaFin angezeigt hat. Die Bitcoin Deutschland AG tritt damit nur als „vertraglich gebundener Vermittler“ der FIDOR Bank AG auf (75).

Neue Anbieter eines Dienstes, die in irgendeiner Art und Weise mit Bitcoins umgehen möchten, sollten sich aufgrund der geringen Erfahrungswerte und der nicht immer eindeutig bestimmbaren Richtlinien frühzeitig an die BaFin wenden, um die individuelle Situation klären zu können.

Steuerliche Aspekte

Um zu verstehen, weshalb welche Steuern auf Bitcoins oder den Erwerb und Handel mit Internetwährungen zu zahlen sind, werden die in Frage kommenden Steuern im Folgenden zunächst kurz erläutert. Im Anschluss erfolgt eine Einordnung welche Steuern in welchen Fällen fällig werden können. Da es bisher noch keinerlei abschließende Bewertung durch das Bundesministerium für Finanzen gibt, sind alle Aussagen nur solange gültig bis eine verbindliche Regelung geschaffen wird. Diese ist jedoch bisher noch nicht angekündigt.

Umsatzsteuer

Die Umsatzsteuer, auch als Mehrwertsteuer bezeichnet (76), ist eine Verkehrssteuer (77), also eine Steuer, die auf die Teilnahme am Rechts- und Wirtschaftsverkehr erhoben wird (78). Sie wird vom Endverbraucher getragen, wobei die Steuer nicht direkt, sondern indirekt durch den Verkäufer eines Wirtschaftsguts oder einer Dienstleistung erhoben wird, der die Steuer auf seinen Verkaufspreis aufschlägt und an das Finanzamt abführt.

Dabei schlägt jedes im Verlauf der Entstehung des Verkaufsprozesses involvierte Unternehmen die Umsatzsteuer auf Ihren Produktpreis auf. Das einkaufende Unternehmen kann diese Steuern als Vorsteuer geltend machen, so dass letztendlich der Endkunde allein diese Steuern trägt. Abbildung 10 erläutert das Prinzip des Vorsteuerabzugs und die Berechnung der Vorsteuer.

Der Steuersatz liegt in Deutschland bei 19% des Waren- und Dienstleistungswertes. Allerdings gibt es auf einige Warengruppen und Dienstleistungsangebote Ausnahmen für die ein verminderter Steuersatz von 7% gilt. Diese Ausnahmen, wie beispielsweise Leistungen aus einer Tätigkeit als Zahntechniker, sind in §12 UStG festgelegt. Grundsätzlich fällig wird die Umsatzsteuer nach §1 Umsatzsteuergesetz (UStG) auf alle Leistungen, die ein Unternehmen gegen Entgelt erbringt, wie z.B. Lieferungen, Einfuhr oder Erwerb von Gegenständen innerhalb der Europäischen Union

(79). Eine Lieferung wird dabei in §3 Abs. 1 UStG definiert als das Verschaffen der Verfügungsmacht, also der Befähigung eines Dritten (dem Lieferungsempfänger) über einen Gegenstand zu verfügen.

Nach bisheriger Definition ist die Umsatzsteuer bei jedem Kauf fällig. Allerdings kennt das Umsatzsteuergesetz einige nicht steuerpflichtige Ausnahmen, die in §§4 – 9 UStG beschrieben sind. Hierzu zählt u.a. die Lieferung von Gold an Zentralbanken (§4 Nr. 4 UStG), die Gewährung und Vermittlung von Krediten (§4 Nr. 8a UStG), sowie die Umsätze und die Vermittlung der Umsätze von gesetzlichen Zahlungsmitteln (§4 Nr. 8b UStG)

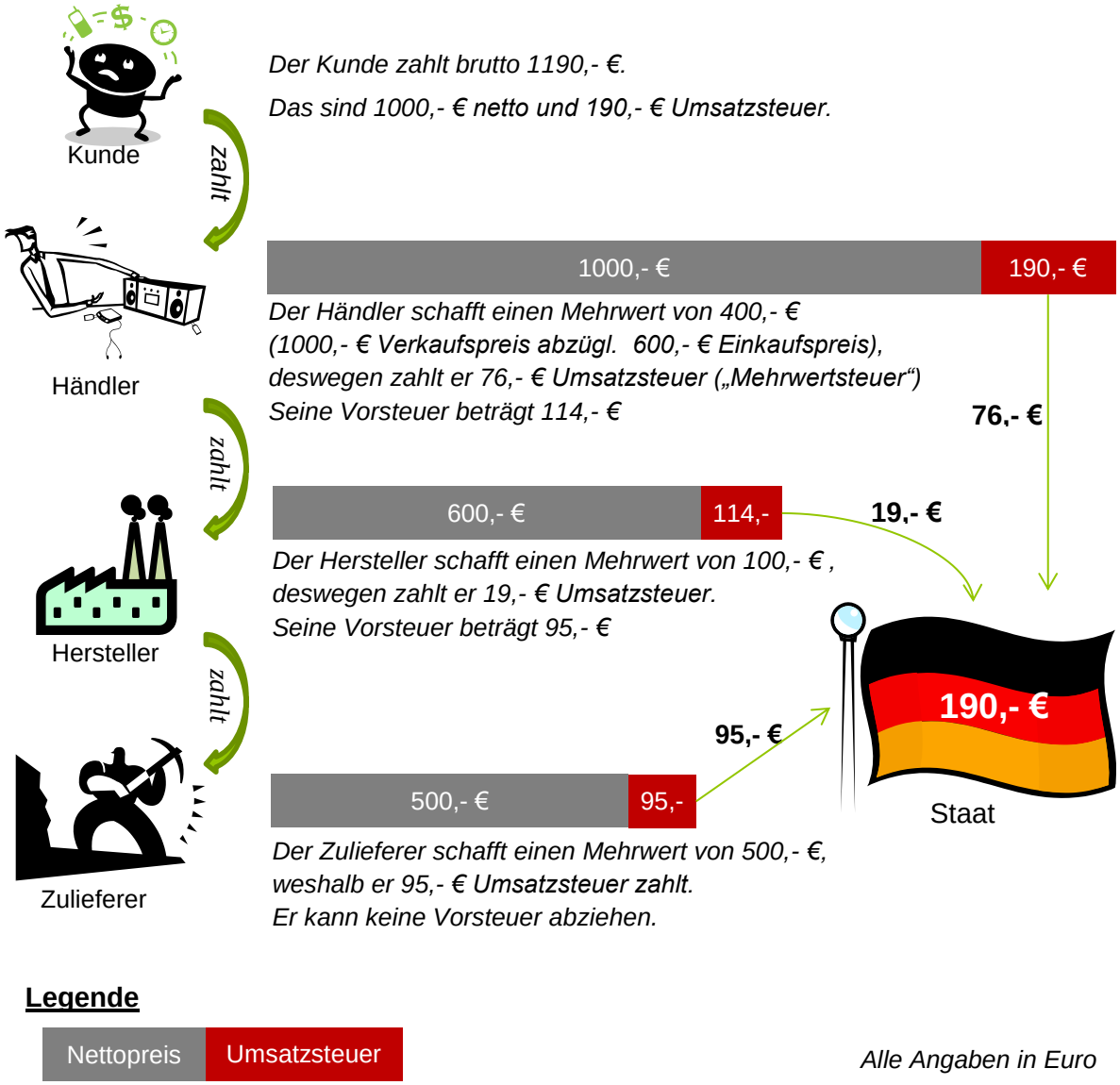

Abbildung 10: Beispiel der Zusammensetzung von Umsatzsteuer und Vorsteuerabzügen über eine einfache Wertschöpfungskette.

Einkommensteuer

Die Einkommensteuer ist im Einkommensteuergesetz (EStG) definiert als eine Steuer, die nach §1 EStG von allen natürlichen Personen, die in Deutschland wohnen oder dort ihren gewöhnlichen Aufenthaltsort haben, zu zahlen ist (80). Die Steuer wird dabei mit der jährlich fälligen Einkommensteuererklärung eingezogen.

Besteuert werden nach §2 EStG Einkünfte aus Land- und Forstwirtschaft, Gewerbebetrieben, selbständiger und nichtselbständiger Arbeit, Kapitalvermögen, Vermietung und Verpachtung, sowie sonstige Einkünfte im Sinne des § 22 EStG, der u.a. auch private Veräußerungsgeschäfte umfasst. Unter privaten Veräußerungsgeschäften nach Definition aus §23 EStG versteht der Gesetzgeber zum einen Veräußerungsgeschäfte über Grundstücke und Rechte (§23 Abs. 1 Nr. 1) und zum anderen Veräußerungsgeschäfte über andere Wirtschaftsgüter, sofern diese innerhalb eines Jahres veräußert werden (§23 Abs.1 Nr. 2). Ausgenommen hiervon sind Wirtschaftsgüter des täglichen Gebrauchs (§23 Abs. 1 Nr. 2 Satz 2 EStG), wobei nicht näher erläutert wird, was hierunter zu verstehen ist.

Steuerliche Beurteilung

Bitcoins werden sowohl von der Bundesanstalt für Finanzdienstleistungsaufsicht als auch vom Bundesministerium der Finanzen (BMF) als Recheneinheit gewertet (81, 74). Somit handelt es sich bei Bitcoins, wie zuvor schon erläutert, um ein Wirtschaftsgut.

Nach geltender Rechtsprechung handelt es sich bei einem Wirtschaftsgut um Sachen, Tiere und nicht körperliche Gegenstände, „sofern sie am Bilanzstichtag bereits als realisierbarer Vermögenswert angesehen werden können, als auch bloße vermögenwerte Vorteile einschließlich tatsächlicher Zustände und konkreter Möglichkeiten, soweit diese derart sind, dass sich der Kaufmann ihre Erlangung etwas kosten lässt, sie nach der Verkehrsauffassung einer selbstständigen Bewertung zugänglich sind und i.d.R. einen Nutzen für mehrere Wirtschaftsjahre erbringen“ (82).

Die Abgeordneten des Deutschen Bundestages Frank Schäffler und Tim Ostermann, beide Mitglieder des Finanzausschusses, stellten bezüglich der Steuerbarkeit von Bitcoin entsprechende Anfragen an die Bundesregierung. Aus den Antworten der Bundesregierung lassen sich folgende Aussagen entnehmen:

1. Die Einnahme von Bitcoins ist, sofern sie zu einer der im Einkommensteuergesetz genannten Einkommensarten gehört, Einkommensteuerpflichtig (83). Dies können private Veräußerungsgeschäfte, also der Verkauf von Bitcoins gegen anerkannte Währungen oder der Tausch gegen andere Waren, sein (84), aber auch Einkünfte aus sonstigen Leistungen. Werden innerhalb eines Jahres weniger als 600,- € durch private Veräußerungsgeschäfte, also dem Verkauf von Bitcoins, erzielt, so bleibt der Betrag steuerfrei. Liegt er oberhalb dieser Freigrenze ist der komplette Betrag, inklusive der 600,- €, zu versteuern.

Verluste, die bei privaten Veräußerungsgeschäften von Bitcoins entstehen, können mit anderen privaten Veräußerungsgeschäften verrechnet werden (85).
Nach Ansicht einiger Rechtsanwälte wird zur Bestimmung der Haltefrist das FiFo-Prinzip (First-In-First-Out) pro Wallet angewendet, da jedes Wallet mit einem eigenen Portfolio vergleichbar ist (86). Das Finanzministerium hat sich hierzu bisher nicht konkreter geäußert.
Für Betriebe gilt diese Freigrenze nicht. Hier stellt der Gewinn, der bei dem Verkauf von Bitcoins anfällt, einen steuerpflichtigen Betriebsgewinn dar (86).

2. Bitcoins sind nicht nach §4 Nr. 8b UStG steuerfrei. Diese umsatzsteuerbefreiende Ausnahme umfasst Umsätze und die Vermittlung von Umsätzen von gesetzlichen Zahlungsmitteln. Da Bitcoins aber nicht als gesetzliches Zahlungsmittel anerkannt sind, sondern lediglich als Rechnungseinheit eingeordnet werden, ist eine Umsatzsteuerbefreiung aufgrund der genannten Regelung nicht möglich (81).

3. Umsatzsteuerbefreit sind jedoch Umsätze, die im Sinne von §4 Nr. 8c UStG: „[…] im Geschäft mit Forderungen, Schecks und anderen Handelspapieren sowie die Vermittlung dieser Umsätze, ausgenommen die Einziehung von Forderungen," (87) anfallen. Geschäfte mit Bitcoins können laut dem Bundesministerium der Finanzen unter diese Ausnahme fallen (88). Welche Geschäfte genau hier runter fallen erläutert das BMF jedoch nicht, so dass eine eindeutige Klärung noch aussteht. Bis dahin können alle Geschäfte, bei denen mit Bitcoins gehandelt wird, steuerfrei behandelt werden und bei Streitigkeiten mit dem Finanzamt eine Einzelfallklärung vor Gericht erreicht werden (86).

4. Das Mining ist nur dann steuerfrei, wenn es privat und nicht gewerblich betrieben wird. Gewerblich ist eine Tätigkeit nach §15 Abs. 2 Satz 1 EStG wenn eine „nachhaltige Betätigung, die mit der Absicht, Gewinn zu erzielen, unternommen wird […], wenn die Betätigung weder als Ausübung von Land- und Forstwirtschaft noch als Ausübung eines freien Berufs noch als eine andere selbständige Arbeit anzusehen ist." (80, §15 Abs. 2 Satz 1) Dies dürfte auf Miner zutreffen, die extra zum Zwecke des Minings in spezielle Hardware investieren. Nutzer, die die Mining-Software laufen lassen wenn der Rechner nicht genutzt wird, dürften von dieser Definition nicht erfasst werden und handeln somit steuerfrei. Die Kosten für Hardware und Strom dürften als Kosten bei der Veräußerung angesetzt werden, um den Gewinn zur Berechnung der Einkommenssteuer zu bestimmen (86).

Sämtliche genannte Regelungen beziehen sich nur auf Deutschland. In anderen europäischen Ländern sieht die Situation, beispielsweise hinsichtlich der Umsatzsteuer, zum Teil noch anders aus. So hat die britische Steuerbehörde Anfang März verlauten lassen, das Bitcoin ihrer Einschätzung nach Privatgeld sei, auf das keine Umsatzsteuer fällig wird (89). In Schweden ist derweil der Streit des Betreibers der Webseite bitcoin.se mit der dortigen Steuerbehörde vor dem Europäischen Gerichtshof gelandet, da die schwedische Steuerbehörde die Gerichtsentschei-

dung, dass der Handel mit Bitcoins umsatzsteuerfrei sei, angefochten hat (90). Eine Klärung, ob der Handel mit Bitcoins nach der europäischen Mehrwertsteuer-Richtlinie 2006/112/EG von der Umsatzsteuer befreit ist, steht derzeit noch aus. Tabelle 1 fasst die Situationen, in denen bei der Verwendung von Bitcoins, Steuern anfallen noch einmal abschließend zusammen.

	Privat	**Gewerblich**
Mining	Einkommenssteuerpflichtig („Einkommen aus sonstigen Leistungen“) bei mehr als 256,- € Einnahmen*	gewerbliche => steuerpflichtige Gewinn durch Betriebsvermögensvergleich oder Einnahmenüberschussrechnung zu ermitteln.*
	** Ausgaben wie Strom und Hardware sind steuerlich absetzbar*	
Ankauf	Umsatzsteuer (da wie Wirtschaftsgut behandelt)	
Verkauf	Einkommenssteuer, wenn Bitcoins nach weniger als einem Jahr verkauft werden (vermutlich FIFO-Prinzip getrennt nach Wallets) Zu Versteuern sind Wertsteigerungen/Verluste, die durch den Besitz der Bitcoins erreicht wurden.	
	Freigrenze: 600,- €/Jahr	Keine Freigrenze
Bezahlen	Steuerfrei	
Zahlung empfangen	Steuerfrei	
Vermittlung	Steuerfrei	Noch ungeklärt

Tabelle 1: Übersicht von auf Bitcoin fällige Steuern.

1.4.1 Bitcoin

Ende Oktober 2008 veröffentlichte Satoshi Nakamoto, von dem, der oder denen keine weiteren Informationen bekannt sind, seine Idee einer Währung ohne zentrale Instanz erstmals in einer Mailinglist für Kryptographie (91). Mit dieser neuen Währung verfolgt Nakamoto die Ziele, Händler vor Betrug zu schützen, indem keine Rückbuchungen möglich sind, ein globales System zu schaffen, in dem Bezahlungen ohne zentrale Instanz vorgenommen werden können, und Transaktionen kostengünstiger zu gestalten, um auch Mikrotransaktionen lohnenswert zu machen (92). Um letzteres zu ermöglichen lassen sich Bitcoins auch teilen. Die kleinste Einheit wird – zu Ehren des Erfinders – Satoshi genannt und entspricht 0,00000001 (einem 100 Millionstel) Bitcoin.

Bereits wenige Monate später, Anfang Januar 2009, entstanden die ersten fünfzig Bitcoins mit der Berechnung des Genesis-Blocks. Kurz darauf veröffentlichte Nakamoto für alle Interessierten auch eine erste Version des Bitcoin-Clients zum Download.

Voraussetzungen

Um am Bitcoin-System teilnehmen zu können, benötigt jeder Nutzer ein Schlüsselpaar aus Public und Private Key, durch das der Besitz von Bitcoins nachgewiesen wird. Außerdem wird eine Bitcoin-Adresse benötigt, um Zahlungen empfangen und versenden zu können. Diese ist 27 – 34 Zeichen lang und beginnt mit einer 1 oder 3 (93). Sie wird generiert, indem die Koordinate aus dem öffentlichen Schlüssel des ECDSA[24]-Schlüsselpaares genutzt wird. Zunächst werden der Wert 1, x- und y-Wert der Koordinate konkateniert. Von dem Ergebnis wird der Hashwert[25] mittels des SHA256 berechnet, zu dessen Ergebnis der Hashwert mittels des RIPEMD160 berechnet wird. Das Ergebnis ist ein 20 Byte langer Wert, dem die „Network ID“, also i.d.R. der Wert 0 für das „Main Network“, vorangestellt wird. Diese 21 Byte sind auch bereits der erste Teil der fast fertigen Bitcoin-Adresse. Die letzten vier Byte werden berechnet, indem ein doppelt ausgeführter SHA256 hiervon berechnet wird. Die vorderen vier Byte des Ergebnisses sind dann die noch fehlenden vier Byte der fast fertigen Bitcoin-Adresse (94). Da einige Zeichen, wie beispielsweise die Zahl 0, die dem Buchstaben O sehr ähnlich sieht, nicht in Bitcoin-Adressen vorkommen sollen, wird das bisherige Ergebnis noch in einen BASE58-String konvertiert. Eine beispielhafte Adresse könnte dann `18bzwDuPR27iLYyGbg72zenMKFREgZWcbw` lauten.

Ein Guthaben von Bitcoins ist immer an eine Bitcoin-Adresse gebunden. Der Besitz dieser Adresse und der damit verknüpften Bitcoins wird durch den Besitz des privaten Schlüssels nachgewiesen. Alle Schlüssel werden durch den Teilnehmer generiert, so dass keinerlei Registrierung oder Offenlegung der Identität notwendig ist.

Zur Nutzung wird ein Bitcoin-Client benötigt, der die notwendigen Funktionen bietet, um Schlüsselpaare und Adressen zu generieren, sowie Nachrichten in das Bitcoin-Netzwerk zu senden und zu empfangen. Dieser lädt zunächst die vollständige, mit Stand von Anfang November 2014 über 23 Gigabyte große Blockchain herunter, in der sämtliche Transaktionen gespeichert sind (95).

Alternativ kann auch ein Wallet bei einem Anbieter wie Coinbase im Internet erstellt werden. Hierbei übernimmt der Anbieter die Erzeugung der Schlüssel und Adressen sowie die Verwaltung der Blockchain, was für den Nutzer einen Komfortgewinn, aber auch einen Kontrollverlust bedeutet.

---

[24] Der Elliptic Curve Digital Signature Algorithm ist eine Variante des Digital Signature Algorithm, einem Standard der US-Regierung für digitale Signaturen.

[25] Ein Hashwert stellt eine Prüfsumme für beliebige Daten dar. Er hat eine feste Länge und wird mittels einer mathematischen Einwegfunktion berechnet. Diese ermöglicht es, den Hashwert recht einfach zu bestimmen, aber erlaubt nicht aus dem Hashwert die Daten zu rekonstruieren.

Transaktionen

Ist einer Bitcoin-Adresse eine Anzahl von Bitcoins zugeordnet, so kann diese als Zahlungsadresse verwendet werden und Bitcoins an andere Adressen übermitteln.

Jede Transaktion hat folgenden Aufbau:

Größe (Byte)	4	1 – 9	variabel	1 – 9	variabel	4
Feld	Version	Anz. In	In List	Anz. Out	Out List	Lock Time

Tabelle 2: Aufbau von Transaktionen in der Bitcoin-Blockchain.

Das Feld *Version* ist derzeit immer 1 und wurde eingeführt, um eine spätere Versionierung zu ermöglichen. Im folgenden Feld *Anz. In* wird angegeben, wie viele Inputs zu der Transaktion gehören. Jeder Input ist Output einer vorherigen Transaktion, so dass ein verzweigtes Netz aus Transaktionen entsteht. Die Anzahl an Inputs muss eine ganze Zahl größer als 0 sein, so dass es prinzipiell möglich ist, dass zu einer Transaktion Bitcoins aus verschiedenen Vorgängertransaktionen gehören können. Das äquivalente Feld *Anz. Out* ist notwendig, da jeder Output nur genau einmal Input einer Transaktion sein kann. Sollen also Summen transferiert werden, die kleiner als der Input sind, so wird der restliche Teil, quasi als Wechselgeld, wieder an eine eigene Adresse übertragen. Abbildung 11 verdeutlicht dies.

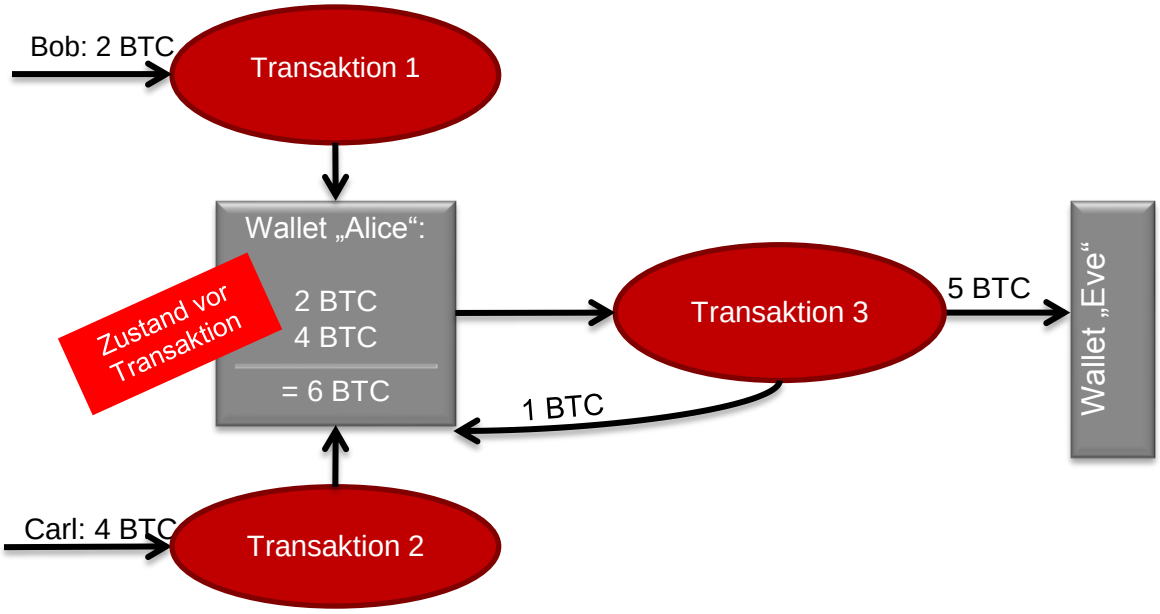

Abbildung 11: Wertstellungen einer Transaktion.

Die *In List* gibt an, welche Outputs vorheriger Transaktionen als Input verwendet werden sollen. Für jeden verwendeten Input enthält sie folgende Informationen:

- Den Hash der Transaktion, aus der ein Output als Input verwendet soll.
- Ein Index, der angibt, welcher Output der Transaktion genutzt werden soll.
- Eine Skript-Signatur zur Verifikation, dass der Input verwendet werden kann.

Die *Out List* enthält für jeden Output folgende Informationen:

- Die Summe der Satoshis (1 Satoshi = 0,00000001 Bitcoin), die zu dem Output gehören.
- Ein Skript zur Festlegung des Empfängers der Zahlung.

Für einen Input wird kein Wert angegeben, da immer der vollständige, referenzierte Output verwendet werden muss, so dass der Wert einfach über den referenzierten Output ermittelt werden kann. Grundsätzlich gilt: Die Summe der Bitcoins aller Inputs muss größer oder gleich der Summe der Bitcoins aller Outputs sein: $\sum_{i=1}^{Anz.In} Wert(Input_i) \geq \sum_{j=1}^{Anz.Out} Wert(Output_i)$. Ist die Summe eingehender Bitcoins echt größer als die Summe ausgehender Bitcoins wird der Rest als Transaktionsgebühr abgeführt.

Das Feld *Lock Time* enthält einen Zeitstempel, anhand dessen festgemacht werden kann, wann die Transaktion stattfand. Verwenden zwei Transaktionen denselben Output einer anderen Transaktion als Input, so wird das Netzwerk nur die frühere der beiden Transaktionen ausführen und die zweite, spätere verwerfen. Alle Transaktionen, die innerhalb einer bestimmten Zeit eingehen, werden zu einem Block zusammengefasst. Dieser Block muss durch das Bitcoin-Netzwerk bestätigt werden. Ein Block besteht aus

- einer magischen Zahl, die immer 0xD9B4BEF9 ist,
- der Blockgröße in Byte,
- einem Blockheader,
- der Anzahl der Transaktionen, die dieser Block umfasst
- und einer Liste der Transaktionen.

Im Blockheader sind folgende Informationen hinterlegt:

- eine Versionsnummer,
- der Hashwert des vorherigen Blocks,
- der Hash aller Transaktionen,
- ein Zeitstempel,
- der Schwierigkeitsgrad
- und einem frei wählbaren Wert.

Der Schwierigkeitsgrad ist eine Zahl, die festlegt, wie groß der Hashwert des Blockheaders maximal sein darf. Da die Rechenleistung im Bitcoin-Netzwerk schwanken kann, aber ungefähr alle 10 Minuten ein neuer Block entstehen soll, wird der Schwierigkeitsgrad regelmäßig angepasst. Um das entsprechende Ziel zu erreichen wird dieser Wert entsprechend angepasst.

Proof-of-work

Der zuvor beschriebene Schwierigkeitsgrad gibt die Problemstellung, die Challenge, des in das Bitcoin-Protokoll integrierten Proof-of-work-Algorithmus HashCash vor. Ziel ist es einen Hashwert für Header eines Blocks zu finden, der kleiner ist als der gegebene Schwierigkeitsgrad. Der Hashwert wird dabei durch die doppelte Verwendung des SHA256-Algorithmus berechnet (96).

Ein Hashwert mit der geforderten Eigenschaft kann nur durch Ausprobieren herausgefunden werden, da Hash Algorithmen die Eigenschaft haben, das kleine Änderungen der Eingabedaten zu großen Änderungen am Hashwert, dem Ergebnis, führen. Diese Änderungen des Hashwerts kann nicht vorausgesagt werden, so dass unter Variation der Nonce innerhalb des Headers ausprobiert werden muss, welcher Hashwert zu diesem Header gehört. Es müssen also Zeit und Rechenkraft investiert werden, um das gestellte Problem zu lösen.

Der Miner, der die Challenge eine passende Nonce zu finden zuerst löst, hat einen den Anforderungen genügenden Block berechnet, den er der Blockchain hinzufügt. Alle anderen Miner beenden dann die Berechnung dieses Blocks und beginnen mit der Berechnung des folgenden Blocks. Proof-of-work ist also das Mittel, das für Sicherheit im Bitcoin-Netzwerk sorgt.

Entstehung von Bitcoins

In klassischen Währungssystemen ist ein zentraler Emittent, in der Regel eine Zentralbank, mit der Ausgabe des Geldes betraut. Sie sorgt dafür, dass ausreichend Geld vorhanden ist, aber nicht zu viel, da dies zu einer Inflation führen würde. Letztendlich sorgt sie damit für die Stabilität der Währung (4).

Bei Bitcoins gibt es keine zentrale Instanz, die diese Aufgabe übernehmen könnte. Das Netzwerk muss dies also selber regeln. Neue Bitcoins entstehen bei der Erzeugung eines Blocks. Derjenige, der den Block berechnet hat, fügt eine Transaktion vom Typ coinbase ein, die Bitcoins ohne Angabe einer In-List an eine durch den Blockersteller anzugebende Out-List hinzufügt (97). Die Anzahl der Bitcoins, die so verdient werden kann, halbiert sich in etwa alle vier Jahre. Zu Beginn waren es noch 50 Bitcoins, heute noch 25 Bitcoins.

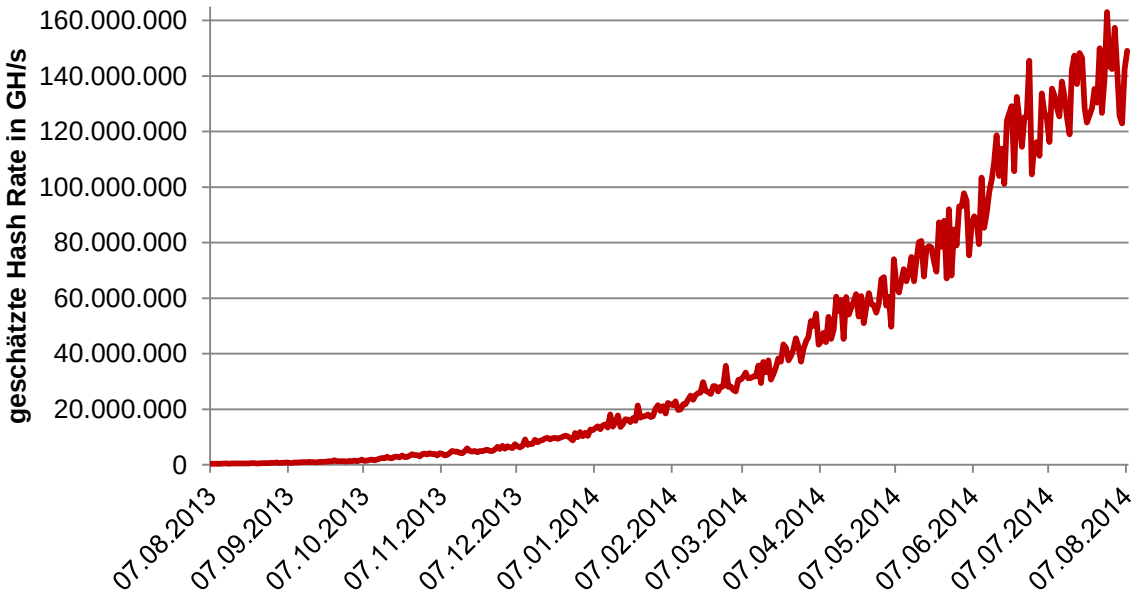

Abbildung 12: Anstieg der Rechenleistung zur Berechnung neuer Blöcke innerhalb des Bitcoin Netzwerks.

Erwerb von Bitcoins

Aufgrund der immer weiter steigenden Rechenleistung (98), die die Miner in das Bitcoin-Netzwerk investieren, ist die Wahrscheinlichkeit mit heimischen Ressourcen über das Mining Bitcoins zu verdienen recht gering geworden. Die stetig steigende Rechenleistung ist u.a. auf speziell auf die Anforderungen des Minings angepasste Hardware und die Bildung großer Mining-Pools zurückzuführen. Um also Bitcoins zu erhalten müssen diese gekauft oder getauscht werden. Hierzu gibt es zwei Varianten: Entweder werden Bitcoins an einem Marktplatz, wie beispielsweise bitcoin.de, ersteigert oder an einer Börse, wie Paymium, gekauft.

In der Regel ist in beiden Fällen eine Verbindung zu einem klassischen Zahlungssystem notwendig, um den Kauf der Bitcoins abwickeln zu können.

1.4.2 Ripple XRP

Einen etwas anderen Ansatz als Bitcoin verfolgt RippleLabs Inc, früher OpenCoin, mit seinem Zahlungsnetzwerk Ripple und der darin verwendeten Währung, die XRP oder Ripples genannt wird. Hier steht nicht die Währung im Mittelpunkt, sondern das Netzwerk zum Tätigen von Zahlungen. In diesem Design wird die eigene Währung nur innerhalb des Netzwerkes verwendet, um Geld von einem Teilnehmer zum anderen zu transferieren. Die von RippleLabs entwickelte Software ist als Open Source Software freigegeben.

XRP basieren, wie Bitcoin auch, auf mathematischen Berechnungen. Allerdings sind im Unterschied zu Bitcoin mit Gründung des Netzwerkes bereits alle XRP durch RippleLabs erzeugt worden – in Summe 100 Milliarden XRP. 20 Mrd. davon gehören den Gründern und Geldgebern von Ripple, zu denen u. a. auch Google Venture gehört. Die restlichen 80 Mrd. XRP bekam RippleLabs und verteilt diese nun an die Nutzer. Zum 30. April 2014 waren bereits rund 7,8 Milliarden XRP verteilt (99). XRPs können sowohl gekauft werden, RippleLabs vergibt sie aber auch als Belohnung für soziales Engagement.

Vertrauen

Das Ripple-Netzwerk basiert auf Krediten, die Nutzer einander geben, und dem Vertrauen, bekannten Personen bestimmte Summen problemlos ausleihen zu können. So haben im unteren Beispiel (Abbildung 13) beispielsweise Alice und David ein Vertrauensverhältnis, wobei Alice David bis zu einer Summe von 4,- € traut, David Alice aber nur bis zu 3,- €. Genauso bestehen Vertrauensverhältnisse zwischen Alice und Bob sowie zwischen Bob und Carol. Leiht Bob sich von Alice nun 2,- € schuldet er ihr diese. Aus welchen Gründen auch immer leiht sich David 4,- € bei Carol. Da zwischen beiden kein direktes Vertrauensverhältnis besteht, verschieben sich die Schuldverhältnisse wie folgt (vgl. Abbildung 14): Bob schuldet Carol 4,- €, Alice schuldet Bob nun zwei Euro und David schuldet Alice 4,- €.

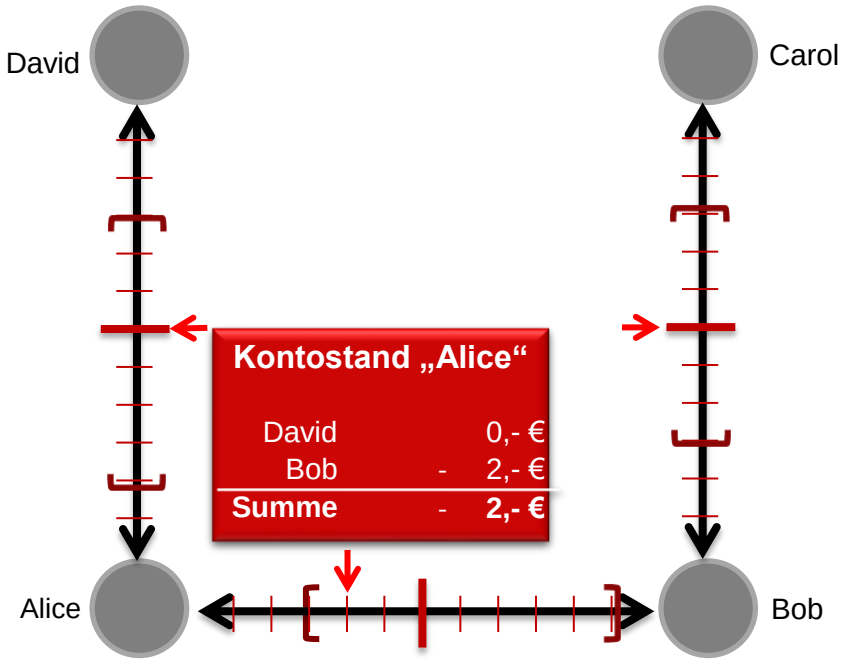

Abbildung 13: Darstellung eines beispielhaften Vertrauensverhältnisses.

Somit ändern sich zwar die Schuldverhältnisse, aber die Kontostände von Alice und Bob bleiben unverändert. Alice schuldet Bob nun 2,- €, bekommt aber 4,- € von David. In Summe bekommt sie also weiterhin die 2,- €, die sie Bob geliehen hat. Und da Sie sowieso Bob und David vertraut macht es für sie keinen Unterschied, von wem sie ihr Geld letztlich bekommt.

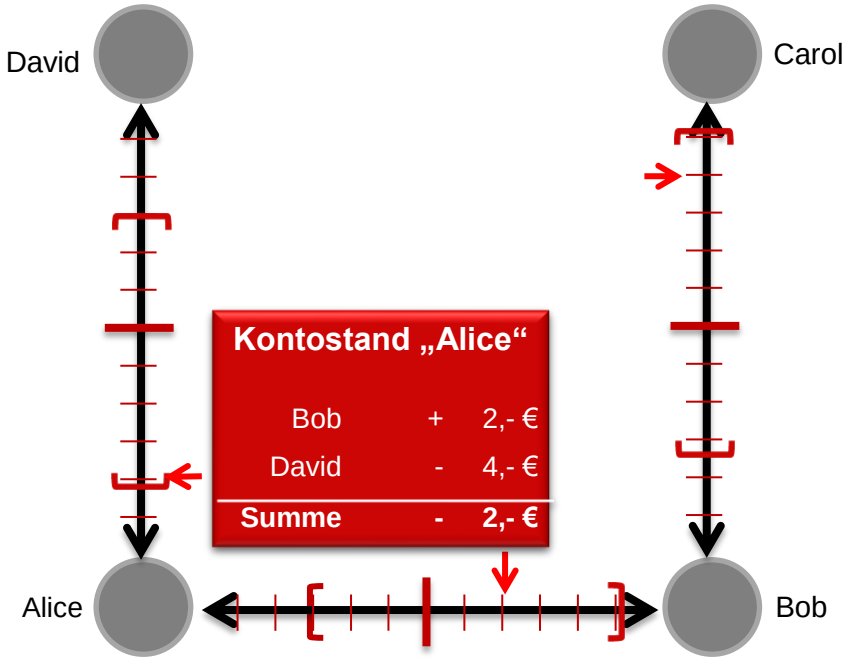

Abbildung 14: Schuldverhältnisse nachdem David sich 4,- € von Carol geliehen hat.

Rollen innerhalb des Ripple-Netzwerks

Das Ripple-Netzwerk besteht aus Teilnehmern, die verschiedene Rollen einnehmen: Gateways, Zahlungsempfänger und –sender, sowie Market Makers. Gateways dienen der Ein- und Auszahlung anderer Währungen, wie Bitcoin, Euro, US-Dollar oder Amazon Coins, in oder aus dem Ripple-Netzwerk heraus. Hierbei entscheidet der Gatewaybetreiber, welche Währungen er akzeptiert (100). Um Einzahlungen ermöglichen zu können muss der Nutzer das gewählte Gateway in seinem Konto hinzufügen und hinterlegen, bis zu welcher Summe er ihm in welchen Währungen vertraut (101). So entstehen die zuvor beschriebenen Vertrauensbeziehungen.

Neben Gateways existieren Zahlungsempfänger und Zahlungssender, die das Netzwerk nutzen, um hierüber zu bezahlen. Sie vertrauen in der Regel einem Gateway, über das sie ihre Zahlungen abwickeln möchten (102). Somit entstehen bisher einzelne „Inseln“ und Nutzer können nur an andere Nutzer, die dasselbe Gateway verwenden, Zahlungen tätigen. Um zu verhindern, dass Kriminelle mehrere Ripple Wallets nutzen, die dazu dienen Angriffe auf das Netzwerk durchzuführen, ist für jedes Wallet eine Reserve von 50 XRP vorgesehen. Dies entspricht mit Datum vom 4. Juli 2014 ungefähr 0,12 Euro.

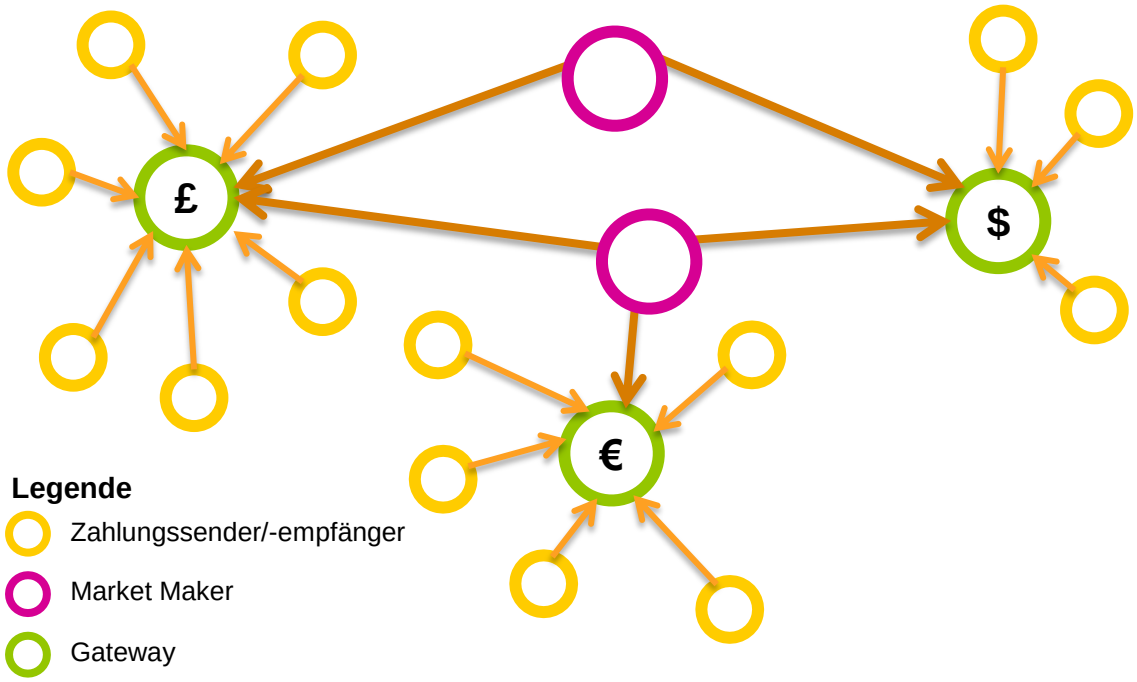

Abbildung 15: Beispielhaftes Netz von Beziehungen innerhalb des Ripple-Netzwerks.

Die Verbindungen zwischen den einzelnen Gateways sind die Market Makers. Diese vertrauen zwei oder mehr Gateways und tauschen die Währungen der Gateways zu einem selbst festgelegten Wechselkurs. Das Ripple-Netzwerk setzt sich dabei zum Ziel, immer den günstigsten Weg vom Zahlungssender hin zum Empfänger zu finden. Prinzipiell ist dem Netzwerk also egal, welche Währungen darüber abgewickelt werden, da es Währungsneutral ist (103). So setzt beispielsweise die deutsche Fidor Bank AG ein Ripple-Netzwerk ein, um Zahlungen zwischen den Dependancen verschiedener Länder schneller abwickeln zu können (104).

Das Ledger und Transaktionen

Vergleichbar zu der Blockchain im Bitcoin-Netzwerk existiert bei Ripple das Ledger. Es ist die wohl wichtigste Komponente innerhalb des Ripple-Netzwerk, denn es enthält alle Transaktionen, die durchgeführt wurden, und den aktuellen Kontostand aller Nutzer. Das Ledger liegt in der aktuellen Fassung, dem Last Closed Ledger, auf allen aktiven Nodes des Ripple-Netzwerks und muss über alle Nodes hinweg synchron gehalten werden. Hierzu setzt das Ripple Netzwerk auf eine Konsensfindung, die im Folgenden näher betrachtet wird, da sie sich von der Konsensfindung über Proof-of-work, wie es bei Bitcoin eingesetzt wird, unterscheidet.

Das Ledger besteht aus einem Header, der folgende Informationen enthält (105):

- Eine über alle Ledger fortlaufende Nummer, die Sequenz Nummer.
- Die Summe der XRP, die noch nicht zerstört wurden. Denn XRP werden, wenn sie für Transaktionsgebühren verwendet wurden, zerstört und können dann nicht wieder genutzt werden.
- Der Hashwert des vorherigen Ledgers.
- Ein Hashwert über alle Transaktionen, die durchgeführt wurden.
- Ein Hashwert über alle Kontostände die in diesem Ledger gespeichert sind.
- Die Zeit, zu der das Ledger geschlossen wurde.
- Die Zeit, zu der das vorherige Ledger geschlossen wurde.
- Verschiedene Flags[26], die bestimmte Eigenschaften des Ledgers festlegen.

Um ein neues Last Closed Ledger zu bilden, muss innerhalb des Ripple-Netzwerks eine Konsensfindung ablaufen, welche Transaktionen akzeptiert und ausgeführt werden und welche nicht. Die Konsensfindung läuft in verschiedenen Schritten ab (106):

1. Zunächst wird zwischen den einzelnen Nodes ständig ausgetauscht, welche Transaktionen diese gerade empfangen haben.

2. Mit Beginn eines Timers rutschen alle bis dahin empfangenen Transaktionen in die Liste der Transaktionen, für die ein Konsens gefunden werden soll. Diese wird auch „Closing Bundle“ genannt.

3. Zusätzlich empfängt und sendet jeder Node Proposals. Diese enthalten die Transaktionen, die der sendende Server kennt und ausführen möchte. Bei Eingang wird geprüft, ob das sendende System Teil der eigenen Unique Node List (UNL) ist. Diese Liste enthält alle Nodes, denen vertraut wird und von denen Proposals akzeptiert werden. Ist das sendende System nicht in der UNL, werden die empfangenen Proposals verworfen.

4. Ist die Prüfung der Proposals erfolgreich verlaufen, werden diese ausgewertet. Jede Transaktion, die in dem Proposal und dem Closing Bundle enthalten ist erhält dabei eine Stimme.

[26] Kennzeichnungen, die festlegen, ob eine Eigenschaft zutrifft oder nicht.

5. Nach Ablauf eines Timers wird geprüft, welche Transaktionen bereits mehr als 50% Zustimmung in den empfangenen Proposals erfahren haben. Diese werden in das eigene Proposal verpackt und an alle Systeme aus der UNL gesendet.

6. Die Schritte 3 – 5 wiederholen sich nun, wobei der Schwellwert von 50% mit jeder Wiederholung erhöht wird. Der Prozess endet, wenn sich 80% der Server von der UNL auf eine Liste von Transaktionen geeinigt haben, die durchzuführen sind. Diese werden in das neue Last Closed Ledger aufgenommen. Alle Transaktionen, die keine Zustimmung erfahren, verbleiben im Closing Bundle.

Ein Ledger ist ungefähr zwischen zwei und zwanzig Sekunden alt ehe das nächste Last Closed Ledger entsteht. Somit sind Transaktionen auch spätestens nach zwanzig Sekunden ausgeführt und können nicht wieder rückgängig gemacht werden.

1.4.3 Peercoin (PPC)

Peercoin wurde von zwei Entwicklern nach dem Vorbild von Bitcoins geschaffen. Sie erkannten, dass Bitcoins noch Potential für Verbesserungen haben. So erfordert die Verwendung des Proof-of-work-Verfahrens viel Rechenleistung und damit auch entsprechend Strom. Außerdem sind King und Nadal, die Entwickler des Peercoin, der Ansicht, dass ein 51%-Angriff, bei dem ein Miner dauerhaft mehr als 50% der gesamten Rechenleistung zur Berechnung neuer Blöcke zur Verfügung stellt, immer wahrscheinlicher wird, da durch die ständig steigende Hashrate im Bitcoin-Netzwerk kleinere Miner aussteigen. Die ursprüngliche Dezentralität geht dadurch ebenfalls immer weiter zurück. So gelang es dem Miningpool ghash.io Mitte 2014 kurzfristig tatsächlich über 51% der Rechenleistung zu stellen (107). Beide Schwachpunkte sollen mit Peercoin gelöst werden. Den grundsätzlichen Gedanken einer dezentral verwalteten Blockchain, in der alle Transaktionen zusammengefasst sind, wird trotzdem beibehalten (108).

Proof-of-stake & minting

Das Mining, wie es schon bei Bitcoins stattfindet, läuft zunächst auch bei Peercoin über dasselbe Proof-of-work Verfahren wie bei Bitcoin, verliert aber mit der Zeit an Bedeutung für das Peercoin-Netzwerk. Es dient der anfänglichen, raschen Erstellung neuer Coins, die mit der Zeit an Bedeutung verliert, sobald ausreichend Coins im Umlauf sind. Zusätzlich kennt Peercoin aber auch das Minting („prägen“), welches an Bedeutung gewinnt je mehr Coins existieren. Hierbei wird ein Proof-of-Stake-Verfahren verwendet, welches zwar nicht durch King und Nadal entwickelt, bei Peercoin aber erstmals für eine Internetwährung verwendet wurde.

Proof-of-stake bedeutet so viel wie „Nachweis durch Besitz“. Im Gegensatz zu Proof-of-work muss also keine entsprechende Leistung, die auch mit hohen Unkosten verbunden ist, erbracht werden, sondern es genügt der Besitz entsprechender Coins. Peercoin verwendet hierfür das

Coin-Alter, welches sich aus der Multiplikation der Coin-Werte und der Dauer, die diese Coins bereits im eigenen Besitz sind, ergibt. Zur Berechnung des Coin-Alters ist jeder Transaktion ein Feld für die Zeit der Transaktion hinzugefügt worden, um berechnen zu können, wie lange die Coins bereits gehalten werden. Wenn Alice beispielsweise 10 Peercoins 50 Tage lang hält haben diese Coins ein Alter von 500. Das maximal gewertete Alter eines Coins beträgt 90 Tage. Coins die länger gehalten werden altern nicht mehr weiter. Überträgt Alice die Coins nun an Bob wird das Coin-Alter „konsumiert“, also auf 0 zurückgesetzt (108).

Bei Bitcoin wird immer die längere Blockchain verwendet, falls mehrere parallel existieren. Peercoin verwendet neben der Länge noch das Kriterium des konsumierten Coin-Alters einer Blockchain, um zu bestimmen, welche Blockchain gültig ist. Deswegen sorgt auch das Minting für Sicherheit innerhalb des Peercoin-Netzwerkes.

Aufgrund der Tatsache, dass sowohl Proof-of-work als auch Proof-of-stake bei Peercoin Verwendung finden, gibt es zwei verschiedene Block-Typen. Zum einen die von Bitcoin bekannten Proof-of-work-Blöcke, zum anderen die neuen Proof-of-stake-Blöcke. Letztere tragen den Namen coinstake. Mit jeder coinstake-Transaktion wird das Coin-Alter konsumiert und dafür das Recht, einen neuen Block erstellen zu dürfen, an den Nutzer ausgegeben.

Der Ablauf des Mintings ist wie folgt: Sobald Coins ein Alter von 30 Tagen erreicht haben können Sie am Minting teilnehmen, sofern der Nutzer dies wünscht. Es wird eine coinstake-Transaktion erzeugt, die aus einem Kernel[27] und optional mehreren Inputs besteht. Am wichtigsten ist der Kernel, denn für diesen wird das Coin-Alter bestimmt und überprüft, ob es zu dem im Netzwerk gegebenen Hash-Target passt. Die Entwickler vergleichen das Prinzip mit einer Lotterie: Der Benutzer setzt eine entsprechende Anzahl Lose, das Coin-Alter, und es wird nun ermittelt, welche Losnummer gewinnt. Im Unterschied zu anderen Lotterien sind Lose, die nicht gewonnen haben jedoch nicht aus dem Spiel, sondern bleiben für die nächsten Runden erhalten (109).

Präziser ausgedrückt wird für jeden Peercoin aus dem Kernel pro Sekunde ein Hashwert generiert. Ist diese kleiner als das gegebene Hash-Target, so hat der Nutzer die Lotterie gewonnen und erstellt einen neuen Block, der Transaktionen in die Blockchain aufnimmt und dem Nutzer 101% der in Kernel und Stake-Input gesetzten Coins gutschreibt. Somit wurden 1% neue Coins erzeugt. Die neuen Coins des Nutzer unterliegen jedoch der Einschränkung, dass diese nicht sofort verwendet werden können, sondern erst nachdem sie in mindestens 520 Blöcken verifiziert wurden. Dies entspricht, unter der Annahme, dass alle zehn Minuten ein neuer Block entsteht, in etwa drei bis vier Tagen (109, 108).

Die Vermehrung der Coins um 1% dient zum einen dazu, langsam neue Coins in das System einzuführen, zum anderen stellen sie eine Art Bezahlung des Nutzers dar, der durch die Verwendung seiner Coins für das Minting für die Sicherheit des Systems sorgt. Im Gegensatz dazu sorgt

[27] Der Kernel ist der erste Input eines neuen Blocks.

das Mining für eine schnelle Erzeugung von Coins und ist daher gerade in der Anfangsphase des Systems wichtig und verliert mit der Zeit an Bedeutung für das System. Alternativ wäre eine initiale Erzeugung einer großen Menge Peercoins, ähnlich wie bei Ripple, möglich gewesen (110).

Sicherheitsmechanismen

Neben den genannten Proof-of-stake und Proof-of-work Verfahren zur Bildung und Sicherung der Blockchain verwendet Peercoin noch Checkpoints. Diese dienen dazu, den aktuellen Stand der Blockchain einzufrieren, so dass vergangene Transaktionen nicht mehr verändert werden können. Die Verteilung der Checkpoints erfolgt zunächst zentral, wird aber künftig an Bedeutung verlieren (110).

In seinem „Weekly Update“ erklärte Entwickler Sunny King im Juni 2013, dass das Checkpoint System eingeführt wurde, um 51%-Angriffen, bei denen einzelne Miner mehr als 51% der Rechenleistung stellen, begegnen zu können, die mehrere neu entstehende Systeme ereilt haben (111).

Weiterhin verlangt Peercoin pro Transaktion eine minimale Transaktionsgebühr von 0,01 Peercoins, die allerdings nicht pro Transaktion fällig werden, sondern pro Kilobyte Transaktionsdaten, so dass diese unter Umständen auch höher liegen können. Diese wird bei Peecoin jedoch verlangt und nicht nur durch die Implementierung des Clients vorgegeben, wie es bei Bitcoin der Fall ist (110).

2 Vorstellung der Bewertungskriterien und Bewertungsskala

Alle untersuchten Zahlungssysteme werden an zuvor festgelegten Kriterien gemessen. Diese sollen sich an den Bedürfnissen von Kunden, Händlern und Staaten orientieren, weshalb sie zunächst analysiert werden müssen. Im Anschluss werden entsprechende Kriterien für eine Bewertung ermittelt und zusammen mit der Bewertungsskala vorgestellt.

2.1 Bedürfnisse der Kunden

Kunden haben verschiedene Anforderungen an das Bezahlen. Im Rahmen einer Studie der deutschen Bundesbank aus dem Jahr 2010 wurde deutschen Bundesbürgern eine Liste möglicher Kriterien vorgelegt, die diese nach ihrer Wichtigkeit bewerten sollten. Die Ergebnisse sind in Abbildung 16 dargestellt.

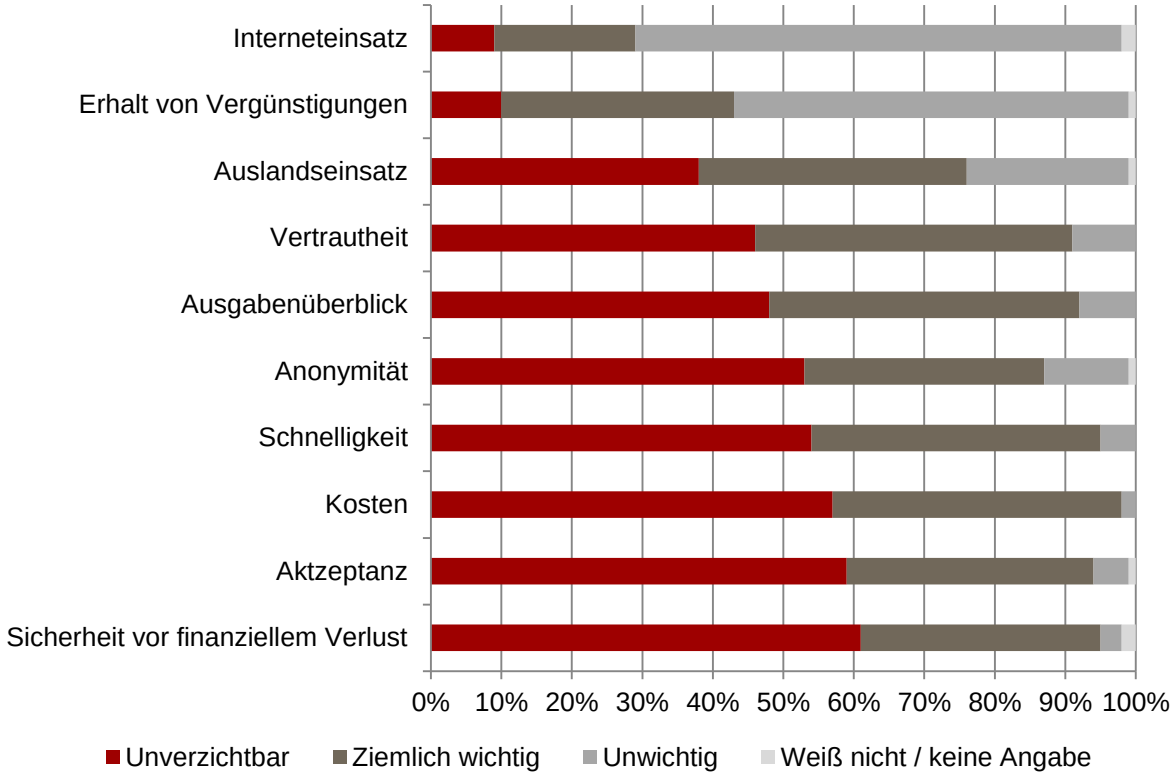

Abbildung 16: Bedeutung einzelner Kriterien bei Zahlungsinstrumenten aus Nutzersicht..

Besonders wichtig ist den Deutschen demzufolge Sicherheit: Zum einen die Sicherheit vor finanziellen Verlusten, die 95% der Befragten für ziemlich wichtig oder unverzichtbar halten, und zum anderen die Anonymität der eigenen Person beim Einsatz des Zahlungsmittels, die 87% als ziemlich wichtig oder unverzichtbar einschätzen. Unter der Sicherheit vor finanziellem Verlust wird dabei das Verlust- und Betrugsrisiko zusammengefasst. Beide Kriterien, also Sicherheit vor finanziellem Verlust und Anonymität, sind dabei Frauen tendenziell wichtiger als Männern. Während bei der Anonymität keine Abhängigkeit von Einkommen erkennbar ist, gilt dies für die Sicherheit vor finanziellem Verlust nicht. Mit steigendem Einkommen steigt auch das Bedürfnis

nach der Sicherheit, keinen finanziellen Verlust zu erleiden. Im Hinblick auf die Herkunft der Befragten ist ebenfalls für beide Kriterien erkennbar, dass diese den Deutschen aus den neuen Bundesländern wichtiger sind, als den Befragten aus den alten Bundesländern (7).

Das zweitwichtigste Kriterium nach der Sicherheit vor finanziellem Verlust ist für 94% (davon 59% unverzichtbar und 35% ziemlich wichtig) der Befragten eine breite Akzeptanz des Zahlungsmittels, so dass Kunden nicht auf mehrere Zahlungssysteme angewiesen sind. Dies ist unabhängig von Geschlecht und Einkommen, allerdings steigt mit dem Alter auch der Wunsch nach breiter Akzeptanz von Zahlungsmitteln (7, S. 12–14).

Am unwichtigsten ist den Befragten der Einsatz eines Zahlungsmittels im Internet (56%) sowie der Erhalt von Vergünstigungen (69%). Vermutlich liegt dies daran, dass der Erhalt von Vergünstigungen häufig nicht mit dem für viele Befragten wichtigen Wunsch nach Anonymität vereinbar ist. Für den Einsatz im Internet lässt sich das gering ausgeprägte Interesse mit Diensten wie PayPal erklären, die auf das Bezahlen im Internet spezialisiert sind und von vielen Personen genutzt werden.

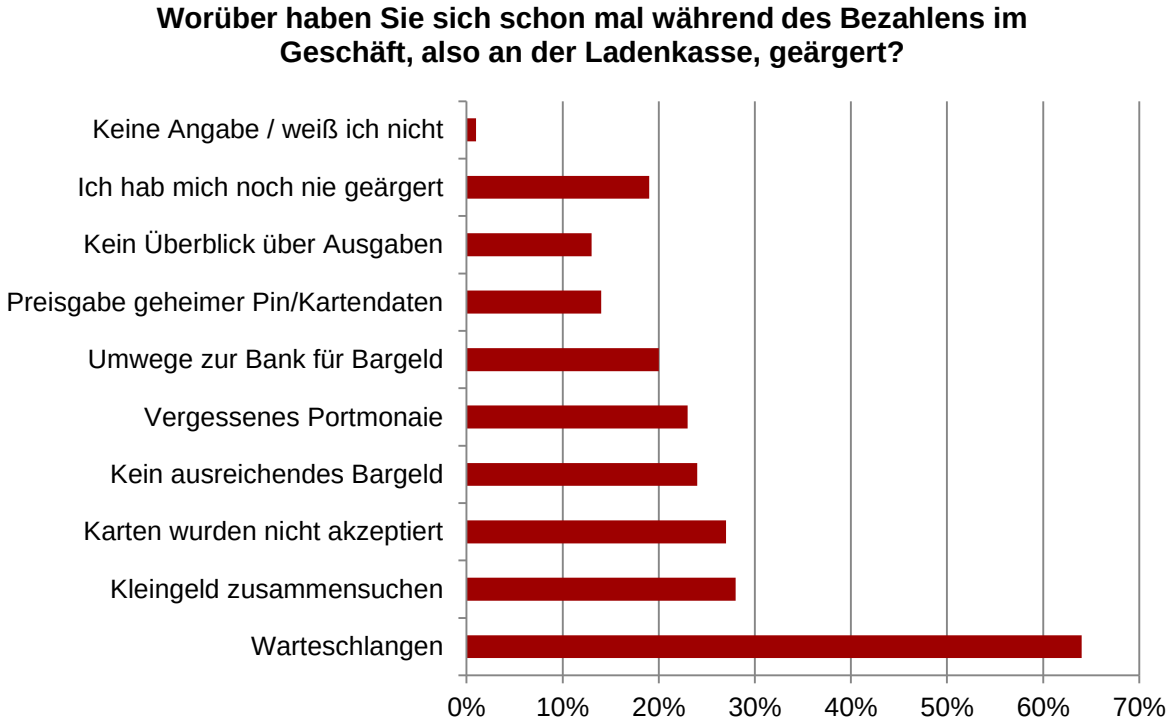

Abbildung 17: Ärgernisse für Kunden beim Bezahlen an der Kasse.

Die von der Bundesbank ermittelten Kriterien und deren Bewertung spiegeln sich auch in anderen Umfragen wieder. So hat Yapital in Zusammenarbeit mit TNS Infratest eine Studie mit dem Titel „Wunsch und Wirklichkeit“ veröffentlicht, die die Anforderungen der Kunden an Zahlungssysteme ermitteln soll. Ferner werden im Rahmen der Studie ärgerliche Erfahrungen von Kunden mit den bekannten Systemen.

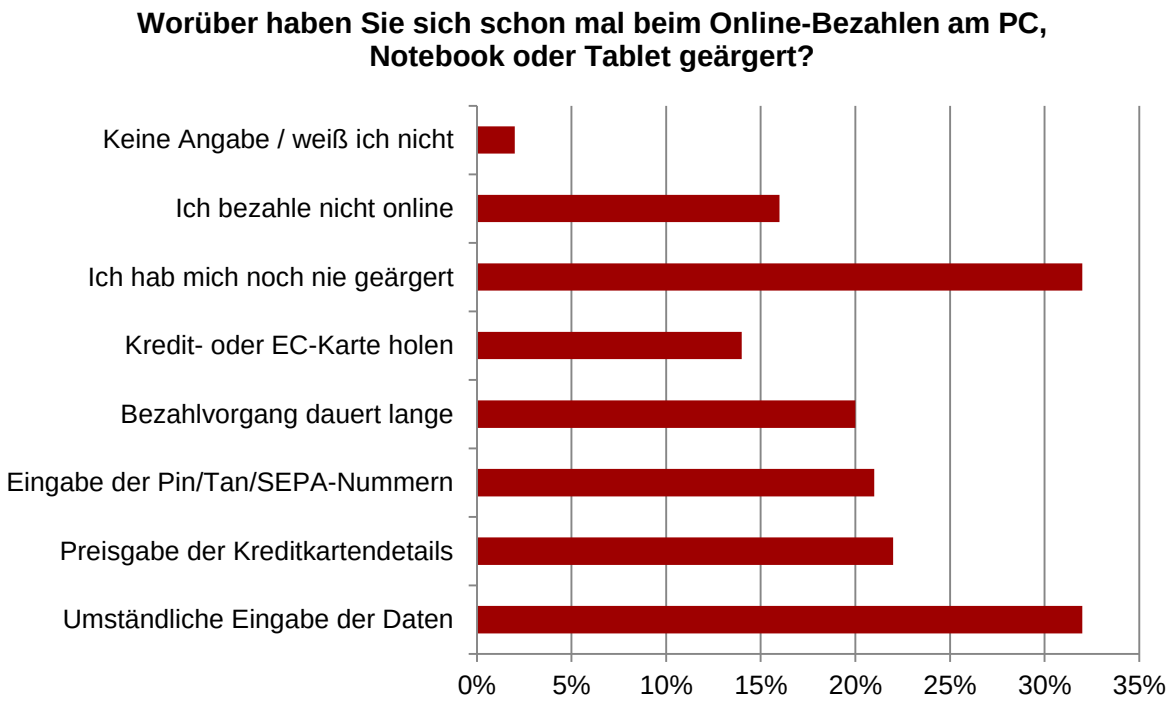

Abbildung 18: Ärgernisse für Kunden beim Online Bezahlen.

Die häufigsten Nennungen für Bezahlvorgänge im Einzelhandel (vgl. Abbildung 17) waren mit 64% der Ärger über lange Warteschlangen und mit 28% die Suche nach Kleingeld (112, S. 10). Dieses Fazit passt zu dem Ergebnis der Bundesbank, wonach für 95% der Befragten die Schnelligkeit des Bezahlvorgangs unverzichtbar oder ziemlich wichtig ist – unabhängig von Geschlecht und Einkommen. Hinsichtlich des Alters sind jedoch Unterschiede erkennbar, denn älteren Befragten war dieses Kriterium grundsätzlich wichtiger als den jüngeren Teilnehmern der Studie. Auch ist ein Unterschied zwischen den neuen und alten Bundesländern zu erkennen: So gaben Befragte aus den neuen Bundesländern signifikant häufiger an, dass Schnelligkeit für sie unverzichtbar sei als dies Befragte aus den alten Bundesländern taten (113, S. 10–12). Auch bei dem Bezahlen mit dem Computer (vgl. Abbildung 18) ist Schnelligkeit ein wichtiges Kriterium. So gaben 20% der Teilnehmer der von Yapital in Auftrag gegebenen Studie an, dass das Bezahlen mit dem Computer für sie schon einmal zu lange dauerte (112, S. 10).

Bei der konkreten Auswahl eines Bezahlverfahrens spielen auch die Bekanntheit und Reputation des Händlers, sowie die Höhe des Kaufpreises eine entscheidende Rolle, wie die Studie „Erfolgsfaktor Payment“ von ibi research, einem Beratungs- und Forschungsinstitut der Universität Regensburg, herausfand (114). Diese Kriterien können im Folgenden allerdings keine Berücksichtigung mehr finden, da sie nicht an ein Zahlungssystem, sondern an spezifische Attribute eines Einkaufs, gebunden sind. Ein Großteil der weiteren Nennungen bezieht sich auf die bereits genannten Kriterien, wie beispielsweise die Wahrung der Anonymität. Auffällig ist jedoch dass, obwohl Kunden beispielsweise die Anonymität grundsätzlich sehr wichtig ist, diese bei der konkreten Entscheidung für ein Bezahlinstrument nur einen geringen Einfluss auf die Entscheidung hat.

Abbildung 19: Kriterien zur Auswahl eines Bezahlverfahrens bei Online-Einkäufen.

2.2 Bedürfnisse der Händler

Neben den Bedürfnissen der Kunden entscheiden auch die Interessen der Händler über den Erfolg eines Zahlungssystems, denn sie entscheiden darüber, ob ein entsprechendes System verwendet werden kann oder nicht.

Prof. Dr. Riggert von der FH Flensburg hebt in seiner Vorlesung „Sicherheit und Bezahlen im Internet“ fünf Kriterien hervor, die Händler bei der Auswahl von Zahlungssystemen anlegen. Obwohl er sich ausdrücklich auf Bezahlverfahren im Internet beschränkt, gelten alle Kriterien ebenfalls für den stationären Handel. Zunächst nennt er den Kostenaspekt, unter dem er sowohl die Kosten für die Integration als auch die laufenden Kosten, wie Fix- und Transaktionskosten, zusammenfasst (115, S. 51).

Robert Herzig, Head of POS Clearing / Financial Services der METRO Group, nennt diesen Aspekt ebenfalls, allerdings erwartet er eine internationale Standardisierung der Zahlungssysteme, die zu geringeren Integrationskosten durch einheitliche Kassensysteme führen würde (116, S. 9). Ferner zählen die laufenden Kosten zu seinen wichtigen Kriterien. Diese sollten transparent und

preiswert für den Händler sein (116, S. 13). Zusammen umfassen sie grob die von Prof. Dr. Riggert genannten Punkte und die internationale Vereinheitlichung.

Als weitere Kriterien zählen beide die Sicherheit vor Zahlungsausfällen, sowie im Sinne der Angreifbarkeit durch Hacker auf, die versuchen können, Transaktionen zu manipulieren oder Systeme in ihrer Funktionsfähigkeit zu beeinträchtigen. Zusätzlich erwähnt Herzig das Vertrauen der Kunden in das Zahlungssystem. Denn wenn die Kunden dem System nicht vertrauen, werden sie es auch nicht nutzen (116, S. 12, 115, S. 51).

Auch die Frage nach der Haftung bei Zahlungsausfällen ist für den Händler ein entscheidendes Kriterium bei der Auswahl seiner Bezahloptionen. So bieten einige Systeme Zahlungsgarantien für den Händler, die aber in der Regel zu höheren Kosten führen, da der Anbieter eventuelle Zahlungsausfälle in seine Kostenkalkulation mit aufnimmt.

Dem Kundeninteresse konträr gegenüber steht der Wunsch der Händler möglichst viele Daten für Marketingzwecke zu erfassen (115, S. 51). Hierzu muss der Kunde eindeutig identifizierbar sein, um die gekauften Waren mit ihm in Verbindung bringen zu können. Außerdem ist es wünschenswert für den Händler eine Möglichkeit zur Kontaktaufnahme mit dem Kunden zu erhalten. Herzig erwähnt hierzu den Aspekt der Kundenbindung, zu dem auch integrierte Bonuspunktesysteme oder Rabattkarten gehören (116, S. 11).

Weiterhin ist für den Händler, ebenso wie für den Kunden, Schnelligkeit ein wichtiges Kriterium, um lange Warteschlangen an der Kasse zu vermeiden. Somit kann die Anzahl der pro Kassenkraft bedienten Kunden gegebenenfalls soweit gesteigert werden, dass die Zahl der Kassenkräfte reduziert werden kann und somit weitere Einsparungen für den Händler entstehen. Den Aspekt der Schnelligkeit hebt ebenso die Deutsche Bundesbank in ihrer Studie zum Zahlungsverhalten hervor, obwohl sich die Studie fast ausschließlich auf das Kundeninteresse bezieht (113).

Weiterhin ist für den Händler die Akzeptanz eines Systems ein entscheidendes Merkmal. Denn je weiter ein Zahlungssystem verbreitet ist, desto mehr Kunden werden das System nutzen, so dass die Fixkosten schneller gedeckt sind.

Neben den genannten Kriterien dürfte die durchschnittliche Umsatzhöhe des Bezahlinstruments durch die Händler berücksichtigt werden, da diese ein natürliches Interesse an Umsatzsteigerungen haben (113, 116, S. 11).

Der Händler muss also für einen ausgewogenen Mix an Zahlungssystemen sorgen, um keinen Kunden zu verlieren. So stellte beispielsweise die 38. WWW-Benutzer-Analyse W3B von Fittkau Maaß Consulting an Kunden die Frage, was für sie Gründe für den Abbruch eines Online-Einkaufs waren. Die häufigste Nennung war hierbei mit 29,2% das Fehlen einer gewünschten Zahlungsart (117). Ähnliches, wenn auch nicht in diesem Ausmaß, dürfte für den stationären Handel gelten.

Die Studie „Erfolgsfaktor Payment“ von ibi research hat für den Fall, dass ein Online-Händler ausschließlich die bei Kunden unbeliebte Bezahlung per Vorkasse anbietet, herausgefunden, dass 88% der Kunden den Webshop wieder verlassen. Selbst wenn dies der einzige Shop ist, der das gewünschte Produkt anbietet, würden 57% der Befragten auf einen Kauf verzichten (114, S. 39–40).

Letzten Endes wird ein Händler aber ein durch den Kunden stark nachgefragtes Zahlungssystem immer einbinden, sofern seine Interessen nicht zu stark verletzt werden.

2.3 Bedürfnisse von Staaten

Die Interessen einzelner Staaten und der Staatengemeinschaften stehen denen der Kunden und Händler zum Teil konträr gegenüber. Während Kunden beispielsweise anonyme Systeme bevorzugen haben Staaten das Bedürfnis, Geldflüsse möglichst genau nachvollziehen zu können, um Straftaten besser verfolgen zu können. So ist beispielsweise Bargeld genau deshalb bei den Strafverfolgungsbehörden ein Problem, da es sich vergleichsweise anonym nutzen lässt. Der Stockholmer Polizeipräsident bezeichnete Bargeld deshalb als „das Blut in den Adern der Kriminalität“ (118).

So beschloss der Rat der Europäischen Union bereits 2009, dass neue Zahlungssysteme, die außerhalb der Reichweite von Banken und Payment Service Providern liegen, einer Kontrolle unterliegen sollten, um Fälle von Kinderpornografie aufklären zu können. Ferner wird darauf hingewiesen, dass über eine Kooperation mit den Vereinigten Staaten von Amerika Konten von Händlern kinderpornografischen Materials eingefroren werden konnten (119). Dies war nur durch eine Kontrolle des Geldflusses möglich. Selbst das Bundesverfassungsgericht erlaubte 2009 die maschinelle Überprüfung von Kreditkartenzahlungen zu diesem Zwecke und stärkt somit die staatlichen Interessen (120). 2007 konnte das bayrische Landeskriminalamt durch die Kontrolle von Geldflüssen einige Fälle von Handel mit kinderpornografischen Materials aufklären. Ebenso gelang den Ermittlern aus Halle an der Saale ein ähnlicher Erfolg gegen Pädophile, die zum Pauschalpreis entsprechendes Bildmaterial erwarben. So konnten mit einer entsprechenden Abfrage bei Visa und MasterCard 322 Tatverdächtige ermittelt werden, die die entsprechende Summe an das fragliche Konto gezahlt haben (121).

Um diese Strafverfolgung auch in anderen Fällen, wie Drogenhandel oder Steuerhinterziehung, effektiver gestalten zu können, ist ein für den Staat möglichst transparentes Zahlungssystem von Vorteil. Hierzu ist es von staatlicher Seite vorteilhaft Anbieter von Zahlungssystemen im eigenen Land zu haben, um eine einfachere Herausgabe von Daten erzwingen zu können. Ist dies nicht der Fall, sind Staaten auf Kooperationen des Anbieters oder des jeweiligen Herkunftslandes eines Systems angewiesen. Dass dies zum Teil problematisch, ist zeigt das sogenannte SWIFT-Abkommen. Hinter SWIFT verbirgt sich die Society for Worldwide Interbank Financial Telecommunication, ein belgisches Unternehmen, dass ein Netzwerk zum Nachrichtenaustausch zwi-

schen Banken betreibt über das nach eigener Aussage täglich über zwei Millionen Nachrichten zwischen den 10.689 angeschlossenen Finanzinstituten aus 212 Ländern verschickt werden (122, 123). Das SWIFT-Abkommen ermöglicht, nach dem Umzug der Serverinfrastruktur von Amerika nach Europa, den amerikanischen Behörden weiterhin den Zugriff auf das Netzwerk, um Transaktionen zur Terrorismusbekämpfung nachverfolgen zu können (124). Dies zeigt einmal mehr, wie wichtig es Staaten ist, Geldflüsse nachvollziehen zu können.

2.4 Bewertungskriterien

Im folgenden Kapitel werden die Bewertungskriterien zunächst einzeln vorgestellt und erläutert, wie die Punkte für die jeweiligen Kriterien vergeben werden. In diesem Zusammenhang wird immer wieder ein Bezug zu den in den vorherigen Kapiteln ermittelten Bedürfnissen der einzelnen Akteure Kunde, Händler und Staat hergestellt.

Die Kriterien, nach denen die Bewertung der einzelnen Systeme vollzogen wird, lassen sich grob in die Kategorien Sicherheit und Anwendung unterteilen. Unter die Kategorie Sicherheit fallen die Aspekte der Anonymität, der Systemsicherheit, der finanziellen Sicherheit und der Verantwortlichkeit über das Zahlungssystem. Diese Kriterien werden in den Abschnitten 2.4.1 bis 2.4.4 näher erläutert. Die Abschnitte 2.4.5 bis 2.4.9 umfassen die Bewertungskriterien aus der Kategorie Anwendung. Hierunter fallen die Aspekte der Verbreitung eines Systems, sowohl online wie offline, als auch die Kosten für Kunden und Händler, sowie die Komplexität bei der Registrierung und Nutzung für Kunden, Händler und weitere Akteure.

2.4.1 Anonymität

Der Wunsch nach einem anonymen Zahlungssystem ist bei vielen Kunden verbreitet, wie die Analyse im Abschnitt *2.1 Bedürfnisse der Kunden* ergab. Kunden wünschen sich möglichst wenig Daten bei einzelnen Bezahlvorgängen zu hinterlassen, da das Bewusstsein, dass alle gesammelten Daten auch missbraucht werden können, mittlerweile recht hoch ist.

Händler können durch das Verknüpfen von Warenkörben und Bezahldaten Kundenprofile erstellen, sowie deren Einkaufsgewohnheiten analysieren. Betreiber eines Zahlungssystems können grobe Bewegungsprofile erstellen und, falls sie zusätzlich Daten des Händlers über den Warenkorb erhalten, noch besser das Einkaufsverhalten der Kunden analysieren, da die Einkäufe bei unterschiedlichen Händlern für die Analyse kombiniert werden können. Ferner würde dies dem Wunsch der Händler und des Staates entsprechen, die eine solche Transparenz zu Marketingzwecken bzw. zur Strafverfolgung erstreben.

Hierbei wird für jedes System analysiert, welche Akteure beteiligt sind und – soweit möglich – recherchiert, welche Daten welchem Akteur zur Verfügung stehen. Je mehr Daten bekannt sind,

desto geringer fällt die Punktzahl für dieses Kriterium aus. Im besten Fall, in dem keinerlei Daten gespeichert werden, können zehn Punkte erzielt werden. Außerdem führt eine Zentralisierung der Datensammlung zu Punktabzügen, da es dem Staat und Angreifern hierdurch besonders leicht gemacht wird diese Daten abzufragen. Eine gewisse Verteilung stellt zumindest eine leichte Erschwerung dar.

2.4.2 Systemsicherheit

Die Frage nach der Systemsicherheit ist sowohl für Kunden als auch für Händler gleichermaßen wichtig. Hier wird untersucht, welche Angriffsmöglichkeiten ein System theoretisch bietet. Weiterhin wird recherchiert, ob bereits erfolgreiche Angriffe auf das System stattgefunden haben und ob diese Angriffe Schäden für Kunden oder Händler verursacht haben. Zusätzlich wird in die Bewertung miteinbezogen, wie der Betreiber des Systems auf erfolgreiche Angriffe reagierte.

Sollten weder praktische Angriffe bekannt noch theoretische Angriffe möglich sein, so werden zehn Punkte vergeben. In allen anderen Fällen erfolgt eine Abwertung, die im Einzelnen erläutert wird.

2.4.3 Finanzielle Sicherheit

Ungeachtet der Systemsicherheit ist die Frage nach der finanziellen Sicherheit zu stellen. In diesem Zusammenhang wird untersucht, wie Kunden und Händler vor finanziellen Verlusten durch fehlerhafte Transaktionen oder Missbrauch des Systems geschützt werden.

Für den Händler ist beispielsweise eine Zahlungsgarantie oder ein System, welches Rückbuchungen nicht ermöglicht, wünschenswert. Den Kunden dürfte besonders interessieren, wie mit fehlerhaften Transaktionen umgegangen wird. Für ihn ist ein System der Rückabwicklung einer Transaktion natürlich von Vorteil.

Aufgrund dieser, zum Teil konträren Anforderungen erfolgt die Vergabe der zehn Punkte für dieses Kriterium ausschließlich aus Sicht des Händlers. Die Bewertung aus Sicht des Kunden kann aus den jeweiligen Erläuterungen abgeleitet werden.

Genauso wie für die vorherigen Kriterien wird ebenfalls für dieses Kriterium eine Recherche durchgeführt, in der untersucht wird, ob Kunden und / oder Händler bereits finanzielle Verluste hinnehmen mussten.

2.4.4 Verantwortlichkeit

Das Kriterium der Verantwortlichkeit dient der Analyse der Struktur des Zahlungssystems. Von diesem Kriterium hängt besonders ab, wer sich für ein System verantwortlich zeigt, welche Ziele und Interessen diese Stelle verfolgt, sowie welche Eingriffsmöglichkeiten in das System zur Verfügung stehen. Diese Einflussmöglichkeiten können vom Ausschluss einzelner Teilnehmer oder Bewohner bestimmter Länder bis hin zur Zurückhaltung einzelner Transaktionen reichen. Für staatliche Stellen ist dies natürlich ebenfalls interessant, da durch solcherlei Eingriffsmöglichkeiten staatliche Sanktionen durchgesetzt werden können. An dieser Stelle sei noch erwähnt, dass das Anonymitätskriterium zwar in direkter Abhängigkeit zum Kriterium Verantwortlichkeit steht, jedoch in diesem Abschnitt nicht erneut behandelt wird.

Für dieses Kriterium werden fünf Punkte vergeben, wobei die Höchstpunktzahl für Systeme vergeben wird, die keinerlei Eingriffsmöglichkeiten in Transaktionen bieten. Eine Abwertung findet statt falls die verantwortliche Stelle ihre theoretischen Eingriffsmöglichkeiten bereits einmal aktiv zum Nachteil von Kunden oder Händlern genutzt hat.

2.4.5 Verbreitung

Das Kriterium der Verbreitung wird insofern bewertet, wie nutzbar ein Zahlungssystem ist. Dies umfasst zum einen ganz generell die Möglichkeiten für den Einsatz im Internet und am Point-of-Sales, aber auch die Internationale Verwendbarkeit wird bei der Bewertung berücksichtigt. Neben den bereits existierenden Akzeptanzstellen findet auch die Strategie des Anbieters Akzeptanzstellen zu gewinnen, Berücksichtigung bei der Bewertung.

Ebenfalls Berücksichtigung findet die Möglichkeit Mikrotransaktionen durchführen zu können. Einschränkungen des Systems auf bestimmte Länder, Zugangsbeschränkungen für Nutzer oder Einschränkungen bei der Nutzung führen zu Abwertungen. Insgesamt werden in dieser Kategorie fünf Punkte vergeben. Diese Punktzahl können offene, weltweit zugängliche Systeme erhalten.

2.4.6 Kosten

Der Kostenaspekt ist besonders für Händler nicht zu vernachlässigen. Während viele Systeme für Kunden kostenlos oder gegen geringe Entgelte nutzbar sind, um eine gewisse Verbreitung im Markt zu erreichen, zahlen Händler zum Teil hohe Gebühren, um eine Bezahlmöglichkeit anbieten zu können. Hierzu gehören, neben den variablen Kosten und Fixkosten, einmalige Kosten für eventuelle Hard- und Software, sowie die Schulung von Mitarbeitern.

Insgesamt werden für dieses Kriterium 15 Punkte vergeben – fünf Punkte beziehen sich auf die Kosten für den Kunden, die anderen zehn auf die Kosten für den Händler.

2.4.7 Komplexität für Kunden

Ein weiterer wichtiger Aspekt eines Zahlungssystems ist die Komplexität für den Nutzer des Systems. Hierzu zählt ein möglichst einfacher und schneller Registrierungsprozess mit möglichst geringen Anforderungen an die vom Nutzer benötigte Hardware.

Aber auch die Komplexität des Bezahlvorgangs, sowohl online als offline, hat Einfluss auf die Bewertung dieses Kriteriums. Ein Bewertungsmaßstab hierfür ist die Anzahl der benötigten Schritte zum Bezahlen, sowie die ggf. an den Nutzer gestellten technischen Anforderungen.

Positiv bewertet wird außerdem die Möglichkeit, möglichst in Echtzeit einen Einblick in getätigten Transaktionen zu erhalten, um einen aktuellen Stand über alle Ausgaben zu bekommen. In Summe werden für dieses Kriterium zehn Punkte vergeben.

2.4.8 Komplexität für Händler

Neben der Komplexität der Kunden ist die Komplexität des Systems aus Sicht der Händler ein weiteres Kriterium. Hierbei spielt vor allem die Schnelligkeit eine wichtige Rolle, da Händler durch schnellere Systeme die Warteschlangen an ihren Kassen reduzieren können, was wiederum zu erhöhter Kundenzufriedenheit führt.

Ferner wird bewertet, wie einfach die Integration des Systems in bestehende Kassen und E-Commerce-Systeme möglich ist. In diesem Zusammenhang spielen die technischen Anforderungen eine wichtige Rolle. Auch für dieses Kriterium werden maximal zehn Punkte vergeben.

2.4.9 Alleinstellungsmerkmale

Dieses Kriterium bietet die Möglichkeit zusätzliche Optionen einzelner Zahlungssysteme, wie beispielsweise die Möglichkeit P2P-Zahlungen durchführen zu können oder Rabatt-, Schlüssel- oder Ticketsysteme zu integrieren, zu berücksichtigen. Hier können maximal fünf Punkte erreicht werden, die individuell vergeben werden.

3 Bewertung

Dieses Kapitel umfasst die Bewertung aller in Kapitel 1 vorgestellten Systeme, nach den aus in Kapitel 2 bestimmten Kriterien. Die Reihenfolge der Zahlungssysteme ist dabei dieselbe wie bei der Vorstellung der Zahlungssysteme.

3.1 Klassische Zahlungssysteme

Zunächst werden die klassischen Zahlungssysteme bewertet, die bereits vielen Personen bekannt sein dürften.

3.1.1 Bargeld

Das erste System, welches bewertet wird, ist Zahlung mit Bargeld. Eine Beschreibung dieses Systems ist in Kapitel *1.1.1 Bargeld* erfolgt und sollte vor der Lektüre dieses Abschnitts gelesen werden.

Anonymität

Die Barzahlung ist eine äußerst anonyme Form des Bezahlens, da sie ausschließlich zwischen den beiden, an einem Kauf beteiligten Personen stattfindet und keine weitere Instanz involviert ist. Außerdem fallen keinerlei Daten an, die die andere Partei nutzen könnte. Der Händler erfährt keinerlei persönliche Daten des Käufers, so dass Barzahlen vollkommen anonym ist. Insgesamt wird für dieses Kriterium die volle Punktzahl von 10 Punkten vergeben.

Systemsicherheit

Die Sicherheit des Bargelds wird durch verschiedene Sicherheitsmerkmale auf Banknoten und Münzen sichergestellt. Hierzu haben die Finanzminister der zum Euro-Währungsraum gehörenden Länder mit der Europäischen Zentralbank Merkmale festgelegt, die laut Aussage der Deutschen Bundesbank dazu führen, dass es „unmöglich (ist), eine Fälschung herzustellen, die alle Sicherheitsmerkmale überzeugend nachbildet“ (4, S. 36). Zudem wird versucht, die Schwierigkeit der Nachbildung aller Sicherheitsmerkmale zu erhöhen, indem mittlerweile eine zweite Serie der Eurobanknoten herausgebracht wird, die andere Sicherheitsmerkmale mitbringt als die erste Serie, die aber weiterhin gültig bleibt. Bisher wurden die neue fünf Euro und zehn Euro Banknoten herausgebracht. In den kommenden Jahren werden jedes Jahr neue Banknoten in aufsteigender Wertigkeit erwartet (4, S. 33–35).

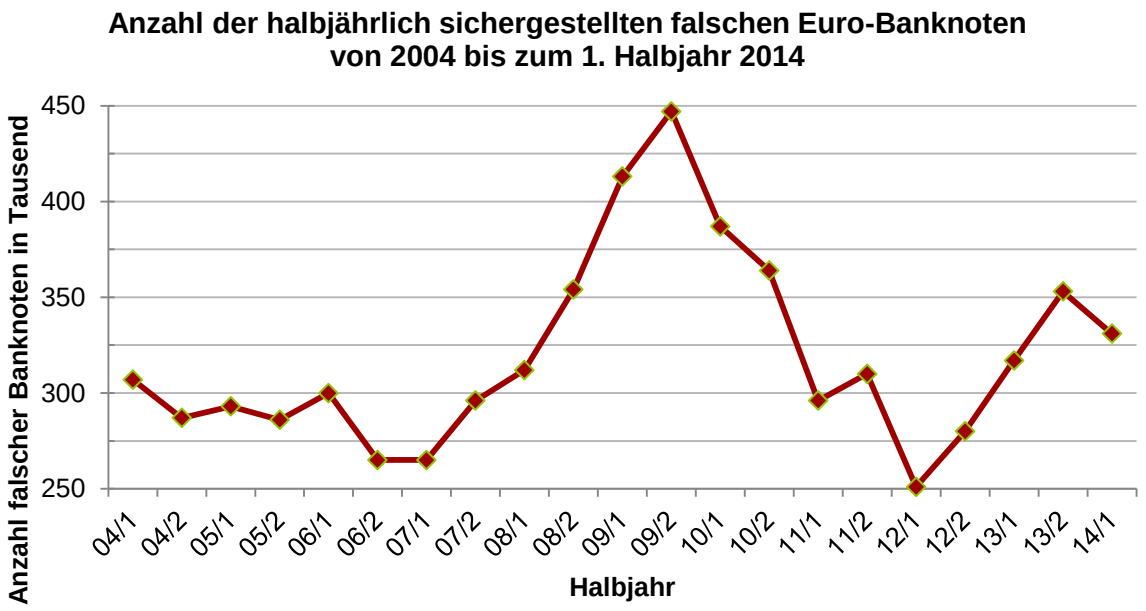

Abbildung 20: Anzahl halbjährlich sichergestellter falscher Euro-Banknoten im Verlauf von 2004 bis 2014.

Zu den Sicherheitsmerkmalen gehören unter anderem Hologramme, Wasserzeichen, ein fühlbares Druckbild und eine Smaragdzahl. Dies sind alles Merkmale, die relativ einfach überprüft werden können. Hilfestellungen zum Erkennen von Fälschungen stellt beispielsweise die Deutsche Bundesbank für alle Bürger zur Verfügung.

Im ersten Halbjahr 2014 wurden 20.156 gefälschte Euromünzen allein im deutschen Zahlungsverkehr registriert (125), während weltweit im gleichen Zeitraum 331.000 gefälschte Eurobanknoten sichergestellt wurden (126). Diese Tatsache zeigt, dass es durchaus kontinuierlich Fälschungsversuche gibt. Allerdings sind sie im Vergleich zu 16,379 Mrd. Banknoten, die im Juni 2014 in Umlauf waren, nur ein relativ geringes Risiko (127).

Nimmt ein Gläubiger Falschgeld an, so entsteht ihm der Schaden, da es für Falschgeld in Deutschland keinen Ersatz gibt und eine Weiterverbreitung strafbar ist. Daher muss von der maximalen in dieser Kategorie erreichbaren Punktzahl ein Punkt abgezogen werden, so dass die Wertung neun Punkte beträgt.

Finanzielle Sicherheit

Aus Sicht der finanziellen Sicherheit steht die Barzahlung ebenfalls sehr gut dar. Denn da die Bezahlung in der Regel immer ein Tausch von Ware gegen Bargeld beinhaltet, hat der Gläubiger sofort den entsprechenden Wert in der Hand, so dass der Händler die Sicherheit hat, dass die Zahlung erfolgreich erfolgt ist. Eine Rückbuchung ist somit nur durch das Mitwirken des Gläubigers möglich, weshalb dieser nach dem Bezahlen die volle Kontrolle über das Geld besitzt.

Die einzige Unsicherheit besteht in der Annahme von Falschgeld, was zu Verlusten für den Händler führt. Allerdings sind die Sicherheitsmerkmale relativ simpel zu kontrollieren. In Summe werden für dieses Kriterium neun von zehn Punkten vergeben. Ein Punkt Abzug im Vergleich zur Höchstpunktzahl basiert auf der möglichen Gefahr, Falschgeld anzunehmen.

Verantwortlichkeit

Die reine Bezahlfunktion des Bargelds ist, da sie ausschließlich zwischen Schuldner und Gläubiger abläuft, nicht kontrolliert und liegt deshalb ausschließlich im Verantwortungsbereich dieser beiden Parteien. Keine dritte Partei hat die Möglichkeit in den Bezahlvorgang einzugreifen und diesen zu beeinflussen. Somit kann für Bargeld die volle Punktzahl in Höhe von fünf Punkten vergeben werden.

Verbreitung

Bargeld ist in Deutschland das einzig unbeschränkte gesetzliche Zahlungsmittel, was bedeutet, dass jeder Gläubiger es zur Begleichung von Schulden annehmen muss. Mit Bargeld können also, wenigstens in Deutschland, alle Schulden, egal welcher Höhe, beglichen werden (3).

Durch die physische Übergabe ist ein Einsatz der Barzahlung allerdings nur am POS möglich, ein Einsatz im Internet ist nicht vorgesehen. Die Cash Payment Solutions GmbH bietet mit dem Service barzahlen.de jedoch die Möglichkeit auch online mit Bargeld zu bezahlen, indem am Ende der Bestellung ein Zahlschein ausgedruckt wird, der in einem teilnehmenden Geschäft beglichen werden kann (128). Allerdings handelt es sich hierbei um ein eigenes Zahlungssystem, das auf der Zahlung mit Bargeld basiert. Es erfährt in dieser Bewertung somit keine Berücksichtigung.

International betrachtet kann Bargeld theoretisch in allen Ländern verwendet werden, wobei die jeweilige Landeswährung benötigt wird, was einen Wechsel in vielen Fällen nötig macht. Auch ist Bargeld in einigen Ländern nicht gern gesehen. So hatten bis Mitte 2012 330 von 1200 schwedischen Bankfilialen die Annahme und Ausgabe von Bargeld vollständig eingestellt (129). Auch ein Blick nach Nordamerika zeigt, dass Bargeld dort nur eine Nische besetzt. Gerade einmal 6% der Amerikaner gaben bei einer Befragung an, dass ihre bevorzugte Bezahlmethode die Barzahlung sei (130). Laut einer ähnlichen Umfrage in Deutschland sehen jedoch 62% der Deutschen Bargeld als ihre bevorzugte Bezahlart an (131). Ein Einsatz ist somit in vielen Fällen, aber eben nicht in allen, möglich. In Summe werden für dieses Kriterium, aufgrund des unbeschränkten Einsatzes in Deutschland, drei Punkte vergeben. Abzüge im Vergleich zur Höchstpunktzahl entstehen durch Beschränkungen beim Einsatz im Internet und im Ausland.

Kosten

Aus Sicht des Kunden ist Bargeld eine preisgünstige Möglichkeit des Bezahlens, da das bei den Banken liegendes Buchgeld[28] in der Regel kostenfrei ausgezahlt werden kann, wenn das eigene Finanzinstitut oder ein angeschlossenes Partnerinstitut verfügbar sind. Die Möglichkeit des Bargeldabhebens bei anderen Instituten ist zum Teil eine kostenpflichtige Leistung der Banken, die mit teilweise fixen Gebühren zwischen 1,95- € und 7,50- € aber auch prozentual von der abgehobenen Summe, berechnet werden (132). Weitere Kosten für den Kunden fallen nur und einmalig indirekt, beispielsweise für die sichere Aufbewahrung des Geldes oder den Zinsverzicht, an. Dies ist jedoch optional und nicht direkt Teil des Bezahlvorgangs, weshalb es nur zu einem geringen Abzug von einem Punkt aus Sicht des Kunden führt.

Aus Sicht des Handels entstehen jedoch verschiedene Kosten: Lagerung und Transport des Bargelds müssen sicher organisiert und in der Regel auch versichert werden. Dies schlägt laut einer Studie der Steinbeis-Hochschule Berlin mit jährlichen Kosten in Höhe von 6,7 Mrd. allein für den Einzelhandel in Deutschland nieder (133). Die Edeka-Gruppe bezifferte die gesamten Kosten, die durch den Umgang mit Bargeld entstehen, auf 0,14 Prozent ihres Jahresumsatzes (134), der sich 2013 allein für den selbstständigen Einzelhandel, der zur EDEKA-Gruppe gehört, auf mehr 22,6 Mrd. Euro belief (135).

Neben den Kosten für den Einzelhandel entstehen aber auch Kosten für Banken, die Geldautomaten betreiben und Schaltermitarbeiter bezahlen müssen. Die einzigen Teilnehmer, denen durch Bargeld keine Kosten sondern Gewinne entstehen, sind die Deutsche Bundesbank und der Staat, die in Summe einen Gewinn von 1,7 Mrd. Euro durch die Ausgabe von Euro-Banknoten erzielten (136, S. 4–6). Die Kosten der Banken finden allerdings keine weitere Berücksichtigung in dieser Bewertung. Diese sind jedoch in den Kosten des Händlers und der Kunden enthalten, da die Banken ihre Kosten auf die anderen Parteien umlegen.

Die oben genannten Zahlen umfassen im Falle des Beispiels von Edeka sämtliche Kosten, mit Ausnahme von Zinsverlusten, die durch das Vorhalten von Bargeld entstehen. In Summe fallen also durch die Verwendung von Bargeld als Zahlungsmittel für den Händler nicht zu vernachlässigende Kosten an, weshalb für diesen Aspekt aus Händlersicht nur fünf von zehn Punkten vergeben werden. In Summe werden für den Kostenaspekt also neun von 15 möglichen Punkten verteilt, vier für die Kosten des Kunden und fünf für die Kosten aus Händlersicht.

[28] Buchgeld ist das Guthaben eines Kunden auf einem Bankkonto, über das zu jeder Zeit ohne Einschränkung verfügt werden kann. Es wird oftmals direkt von einem Bankkonto auf ein anderes übertragen, weshalb es auch Giralgeld („giro“ ist italienisch für „Rundreise“) genannt wird.

Komplexität für den Kunden

Für den Kunden ist der Vorgang des Bezahlens relativ simpel gehalten: Es ist keine Registrierung und keine Einrichtung einer Software oder dergleichen nötig. Der Bezahlvorgang selber ist für sich genommen ebenfalls einfach. Es muss lediglich eine passende Anzahl an Münzen und Scheinen abgezählt werden. Dies kann jedoch einige Zeit in Anspruch nehmen, gerade wenn der Kunde möglichst passend bezahlen möchte. Zahlt er nicht passend, ist er zwar schneller fertig mit dem Abzählen seines Geldes, allerdings muss die Kassiererin dann mehr Wechselgeld abzählen.

Eine Übersicht über Einnahmen und Ausgaben haben Kunden durch die Barzahlung nicht. Sie kennen lediglich ihren aktuellen Verfügungsrahmen durch manuelles Zählen ihres Bargeldbestands.

Durch die nicht notwendige Registrierung und Einrichtung auf der einen Seite und dem fehlenden Überblick über getätigte Transaktionen, sowie der aufwendige Vorgang des manuellen Geldabzählens auf der anderen Seite, werden für die Komplexität aus Sicht des Kunden sieben von zehn möglichen Punkten vergeben.

Komplexität für den Händler

Aus Sicht des Händlers birgt das System der Barzahlung hingegen durchaus eine hohe Komplexität. Die technischen Anforderungen sind zwar gering und auch eine Integration in die Kassensysteme ist einfach realisierbar, aber vorher und nachher verbergen sich große Aufwände für den Händler. Diese reichen von der Beschaffung von Wechselgeld, über den Transport und die Lagerung von Wechselgeld und Einnahmen, sowie das manuelle Zählen des Kassenbestands, bis hin zur Umwandlung in Buchgeld. Abbildung 21 stellt die durch den Händler notwendigen Prozessschritte dar.

Der Händler muss sich zum einen auf eine Barzahlung vorbereiten. Hierzu muss er entsprechendes Wechselgeld bereithalten, welches ebenso wie die Einnahmen, gelagert werden muss. Auch muss der Abtransport vorbereitet werden. Hierzu ist es notwendig ein Transportunternehmen zu beauftrag, aber auch das Zählen des Geldes gehört dazu. Die Überprüfung der Sicherheitsmerkmale einzelner Geldscheine erfordert genaue Kenntnisse derselben, was wiederrum Einweisungen für die mit Bargeld betrauten Personen erfordert. Auch die Prüfung selbst nimmt benötigt einige Zeit, was den Bezahlvorgang neben dem Abzählen des Wechselgeldes weiter verzögert. Der Aufwand für den Händler ist also beträchtlich, weshalb für dieses Kriterium drei von zehn möglichen Punkten vergeben werden.

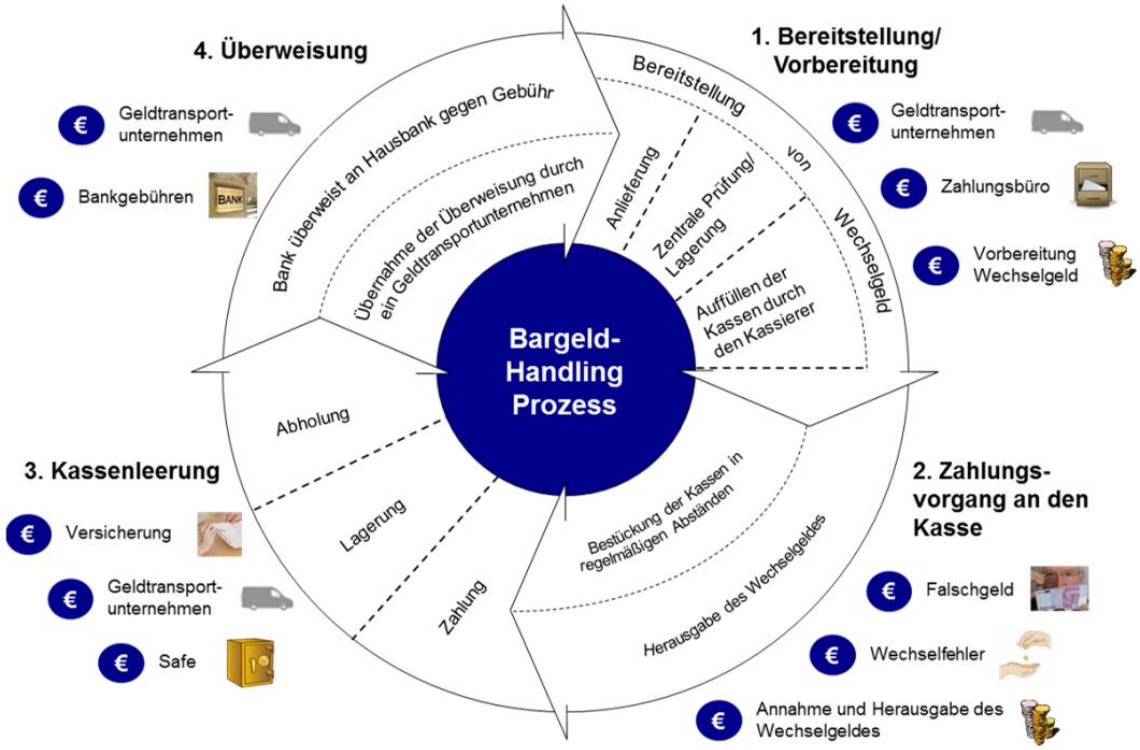

Abbildung 21: Prozessschritte des Handels beim Umgang mit Bargeld.

Alleinstellungsmerkmal

Neben den erwähnten Kriterien bietet Bargeld die Möglichkeit des Peer-to-Peer-Geldaustausches, da jeder ohne jegliche Voraussetzung die Rolle des Gläubigers und Schuldners einnehmen kann. Einschränkende Voraussetzung hierfür ist jedoch, dass sich Schuldner und Gläubiger zumindest einmal persönlich treffen, um das Geld übergeben zu können. Somit kann ein Punkt für dieses Alleinstellungsmerkmal vergeben werden.

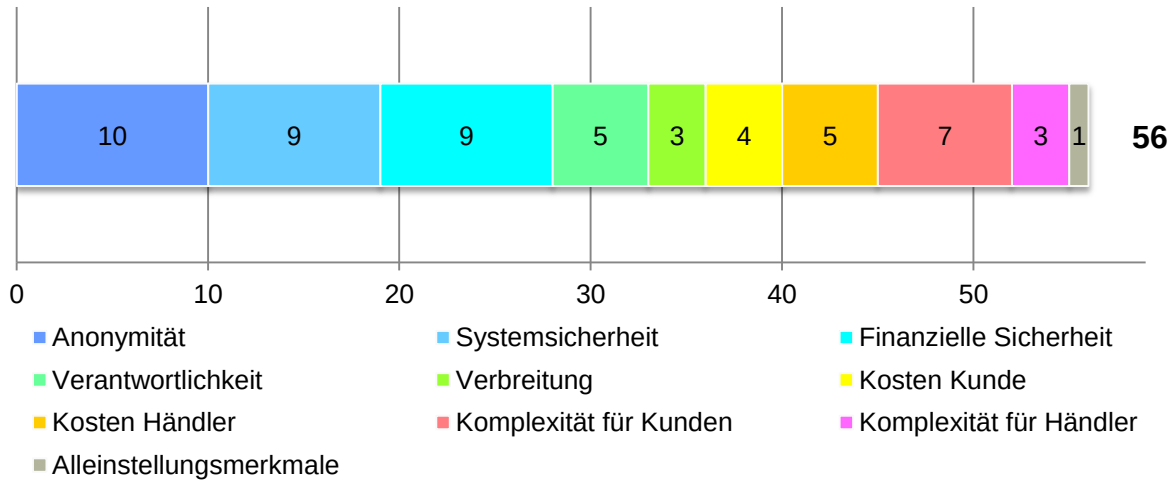

Abbildung 22: Gesamtbewertung des Zahlungssystems Bargeld.

3.1.2 girocard

Das im Folgenden bewertete System ist die girocard, die die Nachfolge der ec-Karte angetreten ist. Leser, die keine Kenntnis dieses Systems haben, wird empfohlen, zunächst Kapitel *1.1.2 girocard* zu lesen.

Anonymität

Spätestens mit dem Kassenabschluss werden die Daten der einzelnen Transaktionen, zu denen mindestens die Karten- und Kontodaten des Kunden, eine Händleridentifikationsnummer, die genaue Zeit und der Ort des Bezahlvorgangs, sowie die angefallene Summe gehören müssen (137), an den Payment Processor übermittelt. Dieser reicht die Daten entsprechend an die Bank des Kunden und des Händlers weiter, die die Pseudonymität der Kontodaten aufheben können. Somit ist es für Behörden und nachrichtendienstliche Organisationen, die diese Daten abfragen dürfen, kein Problem diese zu erhalten. Eine Anonymität ist also grundsätzlich nicht gegeben. Auch die Pseudonymität ist fragwürdig, da Kontonummer und Bankleitzahl keine besonders geschützten Informationen sind. So ist es beispielsweise bei Unternehmen üblich, diese Daten auf dem Briefpapier mit anzugeben.

Für den Händler ist der Kunde aber schon anhand dieser Daten eindeutig zu identifizieren, was eine prinzipielle aggregierte Auswertung aller Einkäufe des Kunden im eigenen Unternehmen ermöglichen würde. Der Payment Processor kann sogar die Daten mehrerer Unternehmen zusammenführen und so detailliertere Kunden- und sogar einfache Bewegungsprofile erstellen. Einer der größeren Payment Processoren, die easycash GmbH aus Rattingen, geriet Anfang 2011 in die Schlagzeilen, als das Unternehmen darüber nachdachte, die gesammelten Daten zu nutzen und Bonitätsprofile der Kunden zu erstellen (138). Die dafür notwendigen Daten liegen dem Unternehmen durch seine Tätigkeit bereits vor. Allerdings kennt der Payment Processor nur grundsätzliche Transaktionen und keine kompletten Warenkörbe, so dass nicht bekannt ist, welche Artikel gekauft wurden. Diese Informationen liegen nur dem Händler vor. In Summe kann also festgestellt werden, dass die Bezahlung über die girocard nicht anonym ist. Es können für dieses System zwei Punkte vergeben werden, da zumindest dem Payment Processor nicht alle Daten bekannt sind und dem Händler gegenüber wenigstens eine, wenn auch gering zu bewertende, Pseudonymität besteht.

Systemsicherheit

Die Sicherheit des Zahlungssystems basiert auf der Sicherheit des eingesetzten EMV[29]-Chips und der Kenntnis des PIN-Codes bzw. der korrekten Unterschrift. EMV ist eine Spezifikation für Hardware und Protokolle, die in den Bezahlterminals zum Einsatz kommt. Außerdem werden in ihr die Schnittstelle und die verwendeten Protokolle zur Kommunikation zwischen Terminal und Karte spezifiziert. Hierzu existieren in der aktuellen Fassung 4.3 vier Bücher. Die Bücher tragen die folgenden Titel und können über die Website der EMVCo, der Organisation, die die Pflege und Weiterentwicklung des EMV-Systems verantwortet, bezogen werden.

Book 1: „Application Independent ICC to Terminal Interface Requirements“

Book 2: „Security and Key Management“

Book 3: „Application Specification“

Book 4: „Cardholder, Attendant, and Acquirer Interface Requirements“

Im Rahmen dieser Bücher werden die genauen Funktionen der Karte nicht beschrieben, sondern lediglich die Schnittstelle zwischen Karte und Terminal.

2010 präsentierten Forscher der University of Cambridge im Rahmen des „IEEE Symposium on Security and Privacy“ einen erfolgreichen Angriff auf ein EMV-basiertes System. Hierbei bauten die Forscher eine Karte, die in das Terminal eingeführt wird und die Schnittstelle zu einer echten Debitkarte oder Kreditkarte bildet. Der Angriff basiert darauf, dass die gefälschte Karte dem Terminal mitteilt, dass die Autorisierung über PIN erfolgreich gewesen sei und gleichzeitig die echte Karte die Nachricht erhält, dass die Zahlung über Unterschrift autorisiert wurde (139, 140).

In Deutschland ist ein solcher Angriff laut der Deutschen Kreditwirtschaft nicht möglich, da die Karte dem Terminal vorgibt, wie die Autorisierung zu erfolgen hat. Im Szenario der Forscher würde die Karte eine Autorisierung per PIN anfordern und die Rückmeldung erhalten, dass die Autorisierung per Unterschrift erfolgte. Diesen Widerspruch sollte die Karte bei korrekter Implementierung erkennen und deshalb die Freigabe der Zahlung verweigern (141, 139). Es ist aber grundsätzlich nicht auszuschließen, dass durch eine ungünstige Kombination von Protokollen für die girocard aus dem EMV-Katalog ähnliche Angriffe möglich sind, da das EMV-Verfahren laut einem der Forscher komplex und unübersichtlich ist (139).

Ein weiterer Schwachpunkt des Systems ist der Vergleich mit der Unterschrift zur Autorisierung einer Zahlung. Dieser wird am POS häufig nicht mit der notwendigen Sorgfalt durchgeführt, gerade dann wenn die Warteschlange bereits sehr lang ist. Auch können Kriminelle, die im Besitz der Karte sind, die Unterschrift üben bis diese der Referenzunterschrift gleicht. Allerdings können

[29] EMV ist die Kurzform von Europay International, MasterCard und Visa, den drei Gesellschaften, die diesen Standard für Zahlungskarten und zugehörige Lesegeräte entwickelten. Er enthält Spezifikationen zum Aufbau von Karten und den verwendeten Kommunikationsschnittstellen, um weltweite Verwendung zu ermöglichen.

Kriminelle sich nicht darauf verlassen, dass der Bezahlvorgang durch eine Unterschrift autorisiert werden muss. In den meisten Fällen, laut einer Erhebung der Deutschen Bundesbank in rund 75%, erfolgt die Autorisierung der Zahlung über die, zu der Karte gehörende PIN (7, S. 16). Dies dürfte damit zu begründen sein, dass die Haftung im Falle eines Zahlungsausfalls des Kunden bei Einsatz der PIN auf die Bank des Kunden übergeht, während im Falle einer Unterschrift der Händler selbst haftet.

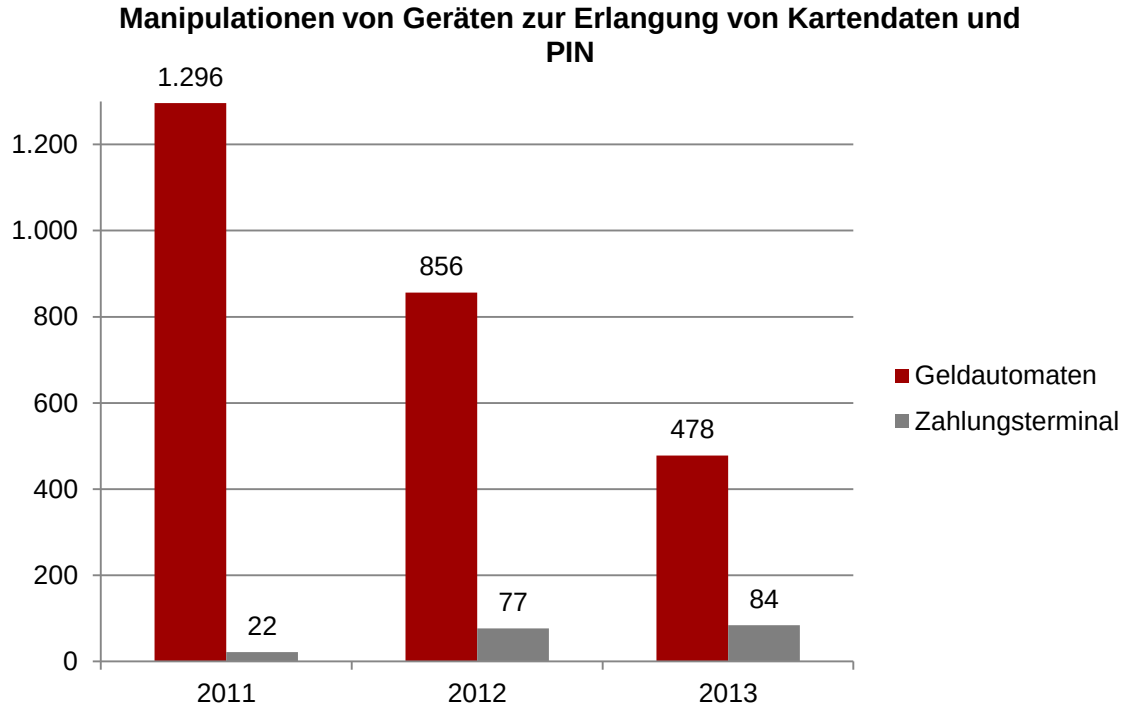

Abbildung 23: Manipulationen von Geräten zum Zwecke der Erlangung von Kartendaten.

Ein weiteres mögliches Angriffsszenario ist die Manipulation von Geldautomaten und Zahlungsterminals am POS mit dem Ziel Kartendaten und PINs abzugreifen. In Deutschland ist die Zahl der Manipulationen von Geldautomaten seit Jahren rückläufig, da die Sicherheitsmaßnahmen der Banken gegen das sogenannte Skimming erfolgreich wirken. Dafür nimmt die Manipulation der Zahlungsterminals zwar langsam, aber stetig zu. Allerdings wurden 2013 nur in 24 Fällen Kartendaten erbeutet, die im Anschluss genutzt wurden. In den restlichen Fällen wurden die Manipulationen rechtzeitig erkannt, so dass letztlich kein Schaden entstand (142). In Summe lässt sich somit festhalten, dass das System Angriffspunkte bietet, die beispielsweise aus der hohen Komplexität der EMV-Spezifikation resultieren. Diese sind allerdings derzeit nicht öffentlich bekannt. Aktuelle Angriffspunkte sind die Geldautomaten und Zahlungsterminals am POS. Die Anzahl der bekannten Fälle ist allerdings stark rückläufig bzw. sehr gering. Für die Sicherheit des Systems werden aus diesen Gründen sieben von zehn Punkten vergeben.

Finanzielle Sicherheit

Aus Sicht der Händler bietet das System der girocard einige Vorteile. So gibt die kartenausgebende Bank eine Zahlungsgarantie auf alle Transaktionen, die mittels PIN autorisiert wurden. Das bedeutet der Händler hat in dem Fall, dass er dieses Verfahren anbietet, die Sicherheit, das Geld auch zu erhalten. Dies gilt selbst dann, wenn die Karte missbräuchlich verwendet wurde. Hierbei haftet die Bank, die ggf. dem Kunden Fahrlässigkeit im Umgang mit seiner PIN vorwirft.

Im Falle der Autorisierung mittels Unterschrift gibt der Kunde lediglich eine Einzugsermächtigung. Der Händler erhält in diesem Fall keine Garantie der Bank auf Einlösung, da die Lastschrift aufgrund eines Widerspruchs des Kunden zurückgerufen werden kann oder wegen mangelnder Deckung des Kontos gar nicht erst ausgeführt wird. Für diesen Fall erlaubt der Kunde mit seiner Unterschrift für gewöhnlich auch, dass die Bank die Kontaktdaten herausgeben darf, um dem Händler zu ermöglichen seine Forderung geltend zu machen. War die Karte zum Zeitpunkt der Zahlung jedoch bereits gesperrt und hat der Händler dies nicht mit der Sperrdatei der Bank verglichen, hat er keinerlei Ansprüche – weder gegen die Bank noch gegen den Kunden (143).

Bei der Zahlungsautorisierung über PIN ist es für den Kunden zudem nicht möglich eine Rückabwicklung der Transaktion zu veranlassen, während es bei der Autorisierung per Unterschrift acht Wochen lang möglich ist. Denn hier handelt es sich aus Sicht der Bank um eine gewöhnliche Lastschrift. Somit ist die Wertung dieser Kategorie davon abhängig für welche Variante der Händler sich entscheidet. Rund 75% aller girocard Transaktionen, die durchgeführt wurden, nutzen die Autorisierung über PIN (7, S. 16). Wegen der unsicheren Variante mit der Autorisierung über Unterschrift kann für diese Kategorie nicht die volle Punktzahl vergeben werden. Aus diesem Grund wird ein Punkt abgezogen, so dass neun von zehn möglichen Punkten vergeben werden können.

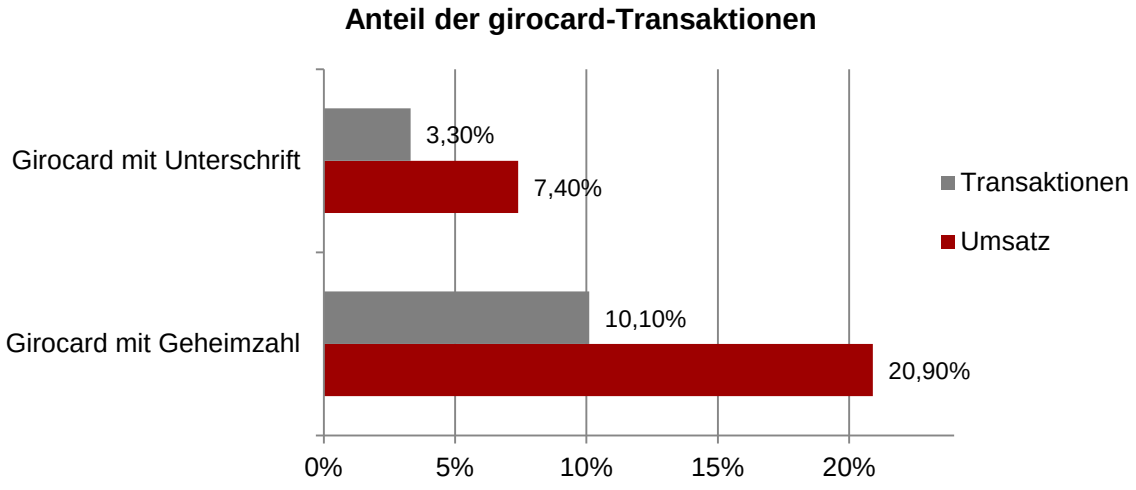

Abbildung 24: Prozentualer Anteil von girocard-Transaktionen an allen Transkationen in Deutschland.

Verantwortlichkeit

Das System der girocard liegt in der Verantwortung der Deutschen Kreditwirtschaft, dem Zusammenschluss des Bundesverbandes der Deutschen Volksbanken und Raiffeisenbanken, des Bundesverbandes deutscher Banken, des Bundesverbandes Öffentlicher Banken Deutschlands, des Deutschen Sparkassen und Giroverbandes und des Verbandes deutscher Pfandbriefbanken, der die Interessen der genannten Vereinigungen vertritt. Sie ist damit verantwortlich für die Auswahl geeigneter Verfahren für die Karten des girocard-Systems aus dem EMV-Katalog. Diese Auswahl bestimmt maßgeblich die Sicherheit des Systems. Allerdings ist die Deutsche Kreditwirtschaft nicht in die einzelnen Transaktionen involviert und hat somit keine Einflussmöglichkeiten auf selbige.

In den Bezahlprozess involviert sind dafür aber die Banken des Händlers und des Kunden, sowie der Payment Processor, den der Händler mit der Abwicklung der girocard-Zahlungen beauftragt hat. All diese Parteien können einzelne Transaktionen blockieren, verzögern oder verändern. Ein solcher Fall ist allerdings noch nicht bekannt geworden. In der Regel ist im Falle eines Problems das Konto des Zahlenden gesperrt oder der maximale Verfügungsrahmen ausgeschöpft. Theoretisch ist jedoch auch die Sperrung aus politischen oder anders motivierten Gründen möglich, so dass eine entsprechende Abwertung für dieses Kriterium stattfinden muss. Daher können in dieser Kategorie drei von fünf möglichen Punkten vergeben werden.

Verbreitung

Die girocard ist ein deutsches System und wird in der Regel zu jedem Girokonto von der jeweiligen Bank ausgegeben, so dass rund 94% aller Deutschen im Besitz einer solchen Karte sind (7, S. 28). Aufgrund ihrer Eigenschaften, die die Nutzung eines EMV-Chips vorsehen, ist sie nicht für den Interneteinsatz konzipiert. Hierfür werden andere Methoden wie beispielsweise Lastschrift oder Vorkasse, verwendet, um mit dem Guthaben auf dem eigenen Konto zu bezahlen. Für den Einsatz der girocard wäre der Einsatz von zusätzlicher Hardware notwendig, so dass bei der Entwicklung des Systems direkt auf diese Möglichkeit verzichtet wurde. Aus diesem Grund lässt sich die girocard, wie beschrieben nur am POS einsetzen, wo sie 2013 an 743.624 Zahlungsterminals akzeptiert wurde (125, S. 6).

Auch im internationalen Zahlungsverkehr wird die girocard akzeptiert. Hierzu gehen die ausgebenden Banken Kooperationen mit den Anbietern Visa und MasterCard ein, die mit Maestro und V-Pay eigene Debitkartensysteme betreiben. Das entsprechende Logo ist auf der girocard aufgedruckt. V-Pay wird dabei von der Postbank, Targobank, BW Bank, LBB, einigen Sparkassen sowie einigen Volks- und Raiffeisenbanken verwendet, während die meisten anderen Banken auf Maestro setzen. Die beiden Systeme unterscheiden sich allerdings erheblich hinsichtlich ihrer internationalen Verwendungsmöglichkeiten. Während Maestro weltweit von über 15 Millionen Stellen akzeptiert wird, ist V-Pay nur innerhalb Europas und in einigen ausgewählten Ländern

(Schweiz, Türkei, Andorra, Bosnien-Herzegowina, Gibraltar, Island, Israel, Kroatien, Liechtenstein, Monaco, Montenegro, Norwegen, San Marino, Serbien und Vatikanstadt) an über 7 Millionen Akzeptanzstellen nutzbar (144). Durch die auf den stationären Handel beschränkten Einsatzmöglichkeiten und die, zumindest bei den V-Pay Karten, stark eingeschränkte internationale Verwendungsmöglichkeiten werden in dieser Kategorie zwei von fünf möglichen Punkten vergeben.

Kosten

Dem Kunden entstehen durch die Nutzung der girocard zum Bezahlen im Inland keine Kosten. Bei Zahlungen im Ausland werden ggf. Kosten entsprechend des Preisverzeichnisses der eigenen Bank fällig. Im Fall der Sparkasse Gelsenkirchen sind Zahlungen kostenfrei, die im Europäischen Wirtschaftsraum abgewickelt werden, der Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Liechtenstein, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich von Großbritannien und Nordirland sowie Zypern umfasst. Andernfalls entstehen Kosten in Höhe von 1%, mindestens jedoch 1,- €, die auf maximal 4,- € pro Zahlung begrenzt sind (145, S. 24). Außerdem ist die Ausstellung der girocard oftmals kostenfrei bei einem Girokonto enthalten. In einigen Fällen werden hierfür jedoch Gebühren berechnet. Für den Kunden entstehen somit nur in wenigen Fällen Kosten und selbst Zinsverluste entstehen nicht, da das Geld bis zur Bezahlung auf dem eigenen Konto liegt und dort gemäß der Vertragsvereinbarungen mit der Bank verzinst werden kann. Einzig der Einsatz im Ausland ist vergleichsweise teuer, weshalb aus Kundensicht vier von fünf möglichen Punkten für das Kostenkriterium vergeben werden können.

Aus Sicht des Händlers entstehen allerdings verschiedene Kosten. Zum einen verlangt die Deutsche Kreditwirtschaft pro Transaktion, die mittels PIN autorisiert wurde, ein Entgelt in Höhe von 0,3% des Umsatzes, wenn dieser über 22,56- € liegt. Liegt der Umsatz unter dieser Grenze werden pauschal 0,08- € berechnet (146, S. 4). Die einheitlichen Gebührenstruktur wird aber ab spätestens Ende Oktober 2014 wegen Bedenken des Bundeskartellamts zu Gunsten frei verhandelbarer Gebühren zwischen Händler und Bank aufgegeben werden (147). Es ist also damit zu rechnen, dass große Handelsketten Rabatte auf die bisherigen Gebühren bekommen. Im Fall von Rewe existiert bereits seit Mitte 2012 eine Ausnahme dieser Regelung, die eine Senkung der Gebühren auf 0,2% beinhaltet, dafür aber die Autorisierung mittels PIN für alle Zahlungen verlangt (148). Für die Autorisierung mittels Unterschrift werden keine Entgelte durch die Deutsche Kreditwirtschaft berechnet, denn hierbei handelt es sich nur um gewöhnliche Lastschriften.

Weitere Entgelte sind an den Payment Processor zu entrichten. So verlangt bspw. die easycash GmbH 0,14- € pro Transaktion, wenn die Transaktion mittels PIN autorisiert werden soll, und 0,04- € für die Variante mit Unterschrift. Zusätzlich kommen Kosten für Zahlungsterminals und die

notwendige Internetverbindung hinzu. Die easycash GmbH bietet hierfür zum Beispiel Geräte zu einem monatlichen Preis ab rund 20,- € an (149). In Summe fallen bei einer Zahlung also mindestens 0,22- € an. Hinzu kommen die beschriebenen fixen Kosten für Payment Processor, so dass das Bezahlen mittels girocard für den Händler moderate Kosten verursacht.

Der Einzelhändler Edeka hat beispielhaft für das Geschäftsjahr 2011 die Kosten für girocard-Zahlungen in Abhängigkeit vom Umsatz berechnet und festgestellt, dass diese 0,47% betrugen (134). Bei einem Umsatz von rund 20 Mrd. Euro im selben Jahr (135) bedeutet das Kosten in Höhe von 94 Millionen Euro für den EDEKA-Verbund. Aus den genannten Gründen wird dieses Kriterium aus Händlersicht mit acht von zehn möglichen Punkten bewertet. Zusammen mit den aus Kundensicht vergebenen Punkten ergibt sich eine Gesamtpunktzahl von zwölf Punkten.

Komplexität für den Kunden

Die Komplexität für den Kunden ist bei der girocard relativ gering. Für die Registrierung müssen keine separaten Dokumente beigebracht werden, da diese im Zusammenhang mit der Eröffnung des zugehörigen Girokontos schon vorgelegt wurden. Allerdings dauert es einige Zeit bis die girocard ausgestellt ist, der Nutzer die Karte in Händen hält und er den PIN mitgeteilt bekommt.

Der Bezahlvorgang selbst ist für den Kunden ebenfalls relativ simpel, da lediglich die Karte in das Zahlungsterminal eingeführt werden muss und die Zahlung anschließend mit PIN oder Unterschrift autorisiert wird. Durch die Ähnlichkeiten zu anderen Bezahlvorgängen und dem Geldabheben am Geldautomaten ist der Kunde mit dem Bezahlvorgang relativ schnell vertraut.

Nachteilig für den Kunden ist jedoch, dass er keinen sofortigen Überblick über seine Ausgaben hat. Denn es kann einige Zeit dauern bis die Zahlung als Abbuchung auf dem Kontoauszug sichtbar wird. Aufgrund dieser Tatsache und der langen Zeit, die vergeht, bis der Kunde seine girocard in Händen hält, werden für dieses Kriterium sieben von zehn möglichen Punkten vergeben.

Komplexität für den Händler

Für den Händler ergibt sich ein anderes Bild, da er neben einem Konto bei einer Bank einen Payment Processor benötigt, der ihn mit dem girocard-System verbindet und ein entsprechendes Zahlungsterminal zur Verfügung stellt. Dieses muss entsprechend an bestehende Kassensysteme angebunden werden. Eine Integration in E-Commerce-Systeme ist nicht möglich, da der Einsatz der girocard im Internet nicht möglich ist.

Die Geschwindigkeit des Bezahlvorgangs ist eher langsam und durch einige Wartezeiten geprägt. So kann beispielsweise die Freigabe der Transaktion durch die Kundenbank einige Sekunden dauern, ebenso wie das Unterschreiben durch den Kunden und den Vergleich der Unter-

schriften durch den Händler. Für dieses Kriterium werden wegen der langwidrigen Registrierung und der Dauer des Bezahlvorgangs sechs von zehn möglichen Punkten vergeben.

Alleinstellungsmerkmale

Neben den erwähnten Kriterien bietet die girocard kein Alleinstellungsmerkmal, so dass hierfür auch kein Punkt in der Bewertung vergeben werden kann.

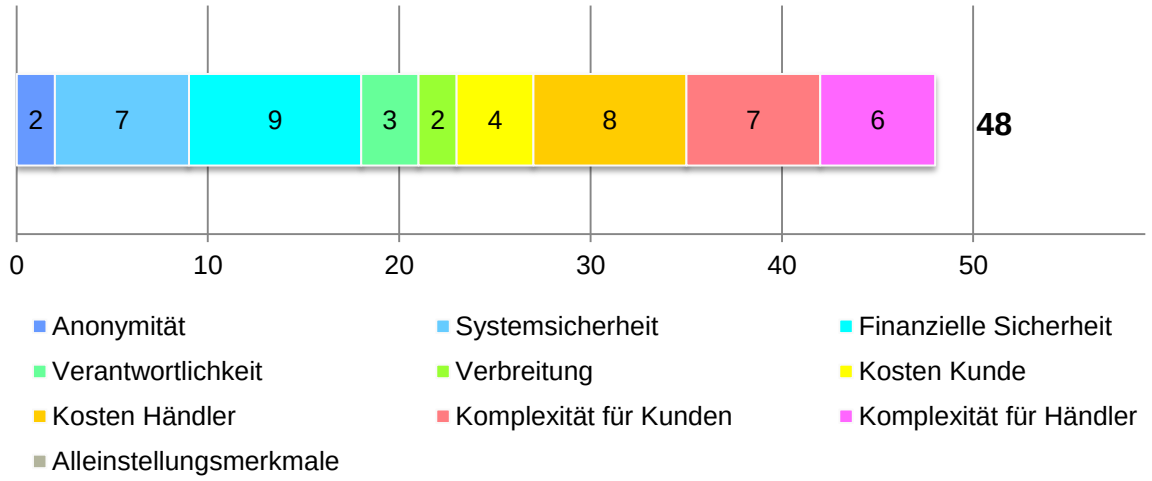

Abbildung 25: Gesamtbewertung des Zahlungssystems girocard.

3.1.3 Kreditkarte

Im Folgenden wird das Kreditkartensystem bewertet. Eine Beschreibung desselben ist in Kapitel *1.1.3 Kreditkarte* vorhanden, welches vor der Lektüre dieses Kapitels empfohlen wird.

Anonymität

In den Bezahlprozess mittels Kreditkarte sind, wie bereits bei der Vorstellung des Systems erwähnt, verschiedene Stellen involviert. An zentralster Position stehen dabei die Betreiber des Kreditkartennetzwerks, also z.B. Visa oder MasterCard, die jede Transaktion, die mit einer ihrer Karten abgewickelt wird, verarbeiten.

Da die größten Kreditkartenanbieter amerikanische Unternehmen sind und das Kreditkartennetzwerk in Ihrer Hand liegt, kann davon ausgegangen werden, dass alle Transaktionen amerikanischen Behörden zugänglich sind. Innerhalb der NSA sammelt beispielsweise die Abteilung „Follow the money“ diese Transaktionsdaten in der Datenbank Tracfin (150). Aber auch andere Behörden der USA sind an diesen Daten interessiert und verschaffen sich Zugriff auf diese (151). Selbst wenn die Daten außerhalb der USA liegen versucht die amerikanische Justiz Zugriff auf diese Daten zu erlangen, wenn dies ihren Zielen dient. Derzeit versucht Microsoft einen Zugriff

der US-Justiz auf in der EU gespeicherten Daten zu verhindern, scheiterte aber vor Gericht (152). Dieses Urteil könnte für amerikanische Unternehmen einen Präzedenzfall darstellen, so dass auch die Kreditkartenunternehmen u.U. gezwungen sein könnten Daten aus Europa amerikanischen Behörden offenzulegen.

Deutsche Behörden haben ebenfalls die Möglichkeit Zugriff auf diese Daten zu erhalten (120), offiziell beispielsweise um Straftaten aufklären zu können. So gelang es im Herbst 2006 Oberstaatsanwalt Peter Vogt aus Halle (Saale) durch Überprüfung aller Visa- und MasterCard-Konten 322 Personen zu ermitteln, die kinderpornographisches Material erworben hatten (121). Zu welchen Zwecken Behörden diese Daten ansonsten noch abfragen ist nicht bekannt.

Aber die Anbieter der Kreditkartennetzwerke können die gesammelten Daten auch an andere weitergeben. So heißt es beispielsweise in den Datenschutzbestimmungen von MasterCard:

> „*MasterCard kann auch persönliche Verbraucherdaten offenlegen, ohne Personen die Möglichkeit des Opt-outs zu geben, (…) wenn MasterCard glaubt, dass die Offenlegung erforderlich oder angemessen ist, um physischen Schaden oder finanzielle Verluste abzuwenden, oder im Zusammenhang mit einer Untersuchung vermuteter oder tatsächlicher betrügerischer oder illegaler Aktivitäten*“ (153)

Durch diesen Passus seiner Datenschutzbestimmungen liegt es allein im Ermessen von MasterCard dies zu entscheiden, was für den Nutzer äußerst intransparent ist, zumal er keine Möglichkeit hat, der Nutzung seiner Daten zu widersprechen oder davon erfährt.

Die Anbieter versuchen aus Ihren zentralen Datensammlungen mittlerweile noch weiteren Nutzen zu ziehen, indem die Daten aggregiert und ausgewertet werden, um beispielsweise zielgenaue Werbung zu ermöglichen. Das Programm „MasterCard Audiences“ bietet genau diesen Service für Unternehmen an (154) und ermöglicht die Auswertung nach verschiedenen Kategorien, wie Gastronomie oder Finanzdienstleistungen (155). Aufgrund der genannten Punkte werden in dieser Kategorie 0 Punkte für das Kriterium der Anonymität vergeben, da durch die zentrale Datenhaltung, die intransparenten Datenschutzbestimmungen und die Nutzung der Daten das System keinerlei Anonymität für den Nutzer bietet.

Systemsicherheit

Das Bezahlen der Kreditkarte erfolgt an vielen Stellen im Handel durch die Autorisierung mittels Unterschrift. Hierfür gilt dieselbe Kritik, die bereits bei der girocard zum Tragen kam. Durch unzureichende Vergleiche der Unterschrift mit der Referenzunterschrift können Zahlungen durch Fremde leicht durchgeführt werden. Das zeigt unter anderem das Beispiel eines Kellners aus Zürich, der mit Kopien der Originalkarten und seiner eigenen Unterschrift in verschiedenen Geschäften erfolgreich einkaufen konnte (156).

Für den Einsatz im Internet wurden früher – und zum Teil auch noch heute – lediglich die auf der Karte abgebildeten Daten abgefragt. Dies umfasst die Kartennummer, den Namen des Karteninhabers, das Ablaufdatum der Karte sowie den drei- bzw. vierstelligen Card Verification Value (CVV). All diese Daten können leicht kopiert werden wenn die Karte verfügbar ist. Oftmals geraten aber auch die Kreditkartendaten durch Hacks in Onlineshops in die Hände von Kriminellen. So vermuteten Mitarbeiter von UPS, dass über sieben Monate hinweg die Kartendaten der Kunden aus einigen US-Filialen des Versanddienstleisters kopiert worden waren (157). Im Weihnachtsgeschäft 2013 wurden zuvor bereits die Daten von weiteren 100 Millionen Kunden, die bei der US-Handelskette Target eingekauft hatten, entwendet (158). Darunter befanden sich u.a. auch Kreditkartendaten. Gemein ist den genannten Fällen, dass der CVV i.d.R. nicht in den Datensätzen enthalten ist. Allerdings wurde 2012 berichtet, dass dieser Code bei vielen Karten durch eine einfache Brute-Force-Attacke ermittelt werden konnte, ohne dass die Karte gesperrt wurde (159). In einigen Fällen ist dies aber gar nicht erst notwendig, da einige Anbieter, wie beispielsweise die TravelTainment GmbH aus Würselen, zusätzlich den CVV speichern, obwohl es nicht notwendig ist. Während eines Angriffs auf die Systeme der TravelTainment GmbH wurden diese Daten im vergangenen Jahr entwendet (160) und konnten sofort durch die Kriminellen genutzt werden.

Ein grundsätzlicher Schwachpunkt dieses Verfahrens ist also, dass Kreditkartendaten auf vielen verschiedenen Systemen gespeichert werden, die nicht alle optimal gesichert sind und auch nicht der Kontrolle der Kreditkartengesellschaften unterliegen. Um einen Missbrauch der Daten selbst bei Verlust an Kriminelle zu verhindern, haben die Kreditkartenanbieter in den letzten Jahren weitere Sicherheitsmaßnahmen, wie „verified by Visa“ oder „MasterCard SecureCode“, eingeführt. Diese bringen eine zusätzliche Sicherheit, da die Transaktion darüber hinaus durch die Bank, von der der Kunde seine Kreditkarte erhalten hat, freigegeben wird. Für diese Freigabe authentifiziert sich der Kunde mittels eines Passworts gegenüber seiner Bank.

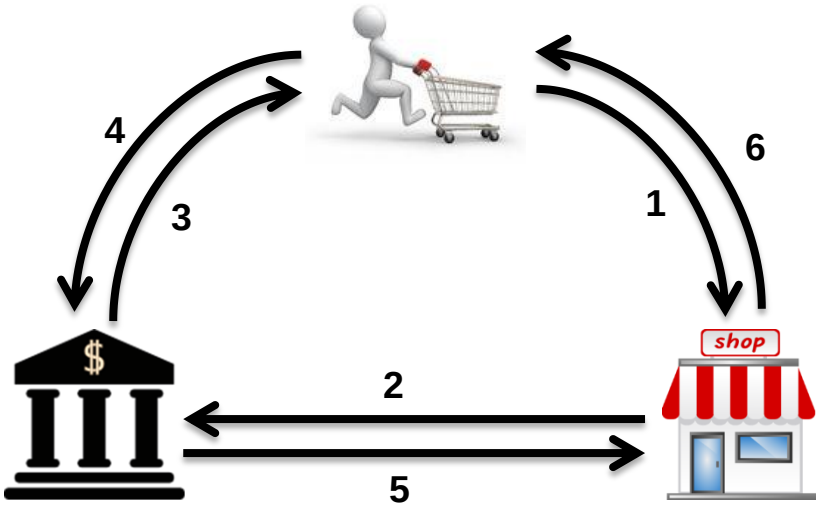

Abbildung 26: Ablauf der Zahlung bei Einsatz von MasterCard SecureCode.

Der Ablauf ist dabei wie folgt: Zunächst gibt der Kunde, wie gewohnt, seine Kreditkartendaten an den Onlineshop weiter (Schritt 1). Dieser fordert von der Bank des Kunden eine Autorisierung der Zahlung an (Schritt 2). Daraufhin stellt die Bank eine Verbindung zum Kunden her und verlangt die Eingabe des SecureCode (Schritt 3). Der Kunde gibt seinen SecureCode an die Bank (Schritt 4), die die Zahlung autorisiert (5), so dass der Einkauf beendet werden kann (Schritt 6).

Um den Missbrauch gestohlener Kreditkarten(daten) zu verhindern, unternehmen die Kreditkartenanbieter große Anstrengungen, da sie in vielen Fällen für entstandene Schäden haften. So betreiben Kartenanbieter eigene Abteilungen zur Verfolgung und Ermittlung von kriminellen Transaktionen, damit Schäden möglichst verhindert werden können. Hierzu werden auf jede Transaktion geheime Regeln angewendet, die die jeweilige Transaktion eigens klassifizieren. Eine einfache Regel ist beispielsweise die zeitliche und geographische Prüfung. Dadurch wird verhindert, dass mit ein und derselben Karte nicht erst eine Transaktion in Gelsenkirchen und zwei Stunden später eine in New York erfolgt (161). Auch das grundsätzliche Blockieren von Transaktionen aus bestimmten Regionen, das sogenannte Geoblocking, ist mittlerweile üblich. Beispielsweise ist die Nutzung außerhalb der EU mit Kreditkarten der Sparkassen nur nach vorheriger Freischaltung möglich (162), was die Sicherheit erhöht, aber den Komfort des Nutzers stark einschränkt – gerade wenn dieser die Regelung vergessen hat oder vorab nicht ausreichend informiert wurde.

Schlussendlich lässt sich festhalten, dass das bisherige System bei weitem nicht sicher ist. Vielmehr bieten die Anbieter dem Nutzer Sicherheit, indem sie Schäden in vielen Fällen übernehmen und hierdurch das Risiko für Kunden und Händler verringern. Trotzdem können für die Systemsicherheit nur wenige Punkte vergeben werden. Einige Punkte gibt es jedoch für die Übernahme von Schäden und die Bemühungen, Missbrauch zu verhindern. In Summe wird dieses Kriterium mit zwei Punkten bewertet.

Finanzielle Sicherheit

Die finanzielle Sicherheit für Händler ist begrenzt. Denn in der Regel besteht keine Zahlungsgarantie durch die Kreditkartengesellschaft, so dass Händler bei Zahlungsausfällen ein Schaden entsteht (163). Einzige Ausnahme bildet die Zahlung im Internet, die durch MasterCard SecureCode, verified by Visa oder ähnliche autorisiert wurde. Hierbei wird das Risiko aus Sicht der Banken auf den Kreditkartennutzer übertragen, da nach Aussage der Banken ein Missbrauch nur möglich wird, wenn der Kunde fahrlässig mit seinem für SecureCode oder verified by Visa gewählten Code umgegangen ist. Dies führte zum Start des Systems dazu, dass Verbraucherschutzzentralen und die Stiftung Warentest vor einer Nutzung warnten (164, 165). Mittlerweile haben jedoch Visa, MasterCard, Banken- und Sparkassen-Verbände gegenüber der Stiftung Warentest versichert, dass Kunden, die diese Verfahren nutzen, nicht schlechter gestellt würden, als andere Kunden (166).

Ferner existieren zahlreiche Möglichkeiten des Kunden, um Transaktionen rückabzuwickeln. Die Berliner Sparkasse listet auf ihrer Homepage Fälle auf, in denen eine Rückbuchung möglich ist. Zum einen sind dies Abbuchungen mit höchstwahrscheinlich kriminellem Hintergrund, wie Abbuchungen von unbekannten Händlern, kostenpflichtige Internetseiten, die Gebühren in ihren AGB versteckt haben, und Händler, die Kreditkartenangaben zur Altersprüfung anfordern und dann unberechtigt Gebühren einziehen. Zum anderen legitime Gründe, wie Abbrüche oder Fehler im Zahlungssystem, die trotzdem zu Buchungen führten. Aber auch schwer überprüfbare Argumente, wie Nicht-Erhalt der Ware oder Warenrücksendung, können Gründe für eine Rückbuchung sein (167).

Am Point-of-Sales gibt es, wie auch bei der girocard, zwei Varianten der Zahlungsautorisierung, wobei durch die Vorgaben des kartenausgebenden Instituts und die durch den Händler unterstützten Möglichkeiten entschieden wird, ob eine Unterschrift oder PIN verlangt wird. So kann es unter Umständen auch vorkommen, das Karte und Zahlungsterminal des Händlers keinerlei Möglichkeit haben miteinander zu arbeiten, da das Terminal beispielsweise nur Zahlungen mit PIN unterstützt, die Karte aber nur die Autorisierung mittels Unterschrift (168, 169). In Deutschland kommt derzeit noch in vielen Fällen die Variante mit Unterschrift zum Einsatz, die eben eine geringere Sicherheit bietet, da eine Referenzunterschrift auf der Kartenrückseite verfügbar ist. Somit können unberechtigte Zahlungen fälschlicherweise leicht zugelassen werden und somit Schäden für Händler und/oder Kunden verursachen.

Die Schäden werden zwar oftmals durch die Kreditkartengesellschaften getragen werden. Jedoch finanzieren diese die Zahlungen wiederum durch Gebühren, die letztlich die Kunden und Händler tragen. Somit besteht in Grenzen eine finanzielle Sicherheit für Händler, da nur in wenigen Fällen eine Zahlungsgarantie besteht und Kunden einige Möglichkeiten haben, Rückbuchungen zu veranlassen. Des Weiteren ist der Anteil von Zahlungen mit gestohlenen Kreditkarten mit 0,099% (170, S. 8) vergleichsweise hoch. Alles in allem gibt es durchaus Fälle, in denen Schäden entstanden sind, so dass für dieses Kriterium zwei Punkte für neuartige Ideen, wie SecureCode, vergeben werden können, die die kriminelle Verwendung zumindest erschweren.

Verantwortlichkeit

Das Kreditkartensystem besteht aus mehreren zentralen Netzwerken, die jeweils durch einen Anbieter kontrolliert werden. Derzeit existieren vier große Anbieter, nämlich MasterCard, Visa, American Express und Diners Club, die allesamt aus Amerika stammen. In jüngster Zeit hat sich gezeigt, dass dies durchaus von Nachteil sein kann, da Kreditkartennetzwerke durch die Politik als Druckmittel gegen unliebsame Teilnehmer verwendet werden. Im Zuge westlicher Sanktionen gegen Russland kündigten Visa und MasterCard an, keine Zahlungen mehr an russische Banken durchzuführen (171). Ferner sammelte die Plattform Wikileaks Spendengelder über Kreditkartenzahlungen, PayPal und Moneybookers. Nachdem immer mehr Dokumente auf Wikileaks veröf-

fentlicht wurden, stoppten Visa und MasterCard Zahlungen an die hinter Wikileaks stehende Stiftung (172).

Durch die Strukturen des Netzwerkes haben aber auch andere Beteiligte, wie *Acquirer* und *Issuer* die Möglichkeit Teilnehmer von dem Kreditkartennetzwerk auszuschließen. 2013 stellte beispielsweise der schwedische Dienstleister Payson Zahlungen an den Betreiber des VPN-Anbieters iPredator mit der Begründung ein, die Kreditkartengesellschaften verlangten dies. Auf Nachfrage gaben jedoch sowohl MasterCard als auch Visa an, keine solche Weisung herausgegeben zu haben (173). Es lässt sich somit feststellen, dass alle Kreditkartenorganisationen letztlich auch für die Ziele der US-Regierung genutzt werden. Aufgrund dieser Tatsache und der bereits erfolgten Eingriffe in die Netzwerke, werden für dieses Kriterium keine Punkte vergeben.

Verbreitung

Kreditkarten können, wie bereits erwähnt, sowohl einfach im Internet, durch Eingabe der Kartennummer und weiterer Daten, als auch am Point-of-Sales verwendet werden. MasterCard verfügt weltweit über 36 Millionen Akzeptanzstellen (174), während Visa sogar auf 37 Millionen Akzeptanzstellen verweist (175). In beiden Fällen kann demnach von einer weiten Verbreitung gesprochen werden.

Durch die hohe Verbreitung auf Kundenseite – allein in Deutschland waren 2013 36,64 Mio. Karten im Umlauf (10) – ist eine Akzeptanz für Händler auch lohnenswert, da viele potentielle Kunden erreicht werden können. Allerdings gibt es bei der Ausgabe der Kreditkarte durchaus Voraussetzungen, die der Karteninhaber erfüllen muss. In der Regel findet vor Ausgabe eine Bonitätsprüfung statt, die darüber entscheidet, ob der Anfordernde eine Kreditkarte bekommt oder nicht. Einige Personen sind also direkt von dem System ausgeschlossen. Aufgrund der letztgenannten Einschränkung können für dieses Kriterium lediglich vier der fünf möglichen Punkte vergeben werden.

Kosten

Die Kosten unterscheiden sich für den Kunden, je nachdem mit welchem kartenausgebenden Institut er einen Vertrag abschließt und welche Kreditkarte er auswählt. In der einfachsten Ausführung kostet eine Visa oder MasterCard bei der Sparkasse Gelsenkirchen beispielsweise 20,- € pro Jahr, wobei diese Gebühr zum Teil oder vollständig erlassen wird, wenn der Kunde zusätzlich bestimmte Konten bei der Sparkasse führt. Hinzu kommen eventuelle Kontoauszüge, die per Post versandt werden und für die die Sparkasse die Portogebühren von aktuell 60 Cent berechnet. Außerdem entstehen Gebühren bei der Bargeldauszahlung in Höhe von 2% des Umsatzes, mindestens jedoch 5,- €, sowie Kosten beim Auslandseinsatz der Karte in fremden Währungen

von 1%. Bei entsprechenden Umsätzen wird im Folgejahr unter Umständen eine Beitragsrückerstattung in maximaler Höhe der Jahresgebühr gezahlt (145).

Für den Nutzer entstehen somit nicht unerhebliche Gebühren, die zum Teil auch anfallen, wenn die Karte gar nicht genutzt wird. Dafür sind mit einigen Kreditkarten aber auch Zusatzleistungen verbunden, wie Rabatte an Tankstellen, Zugang zu einer Lounge am Flughafen oder Versicherungen, wie Reiserücktrittsversicherungen, Auslandskrankenversicherungen oder Einkaufsversicherungen, so dass sich die Kosten dadurch unter Umständen amortisieren können.

Ferner ist die Kostenstruktur für die Händler recht heterogen, denn die tatsächlich zu zahlenden Gebühren sind im Kreditkartenakzeptanzvertrag mit dem *Acquirer* festgeschrieben. Diese setzen sich jedoch aus verschiedenen Gebühren, wie Einrichtungsgebühren, Transaktionsgebühren und Disagio, zusammen, die je nach Branche, Höhe der zu erwartenden Umsätze und individueller Vereinbarungen divergieren. In dem Preis- und Leistungsverzeichnis der Concardis GmbH (176), einem deutschen *Acquirer*, findet sich beispielsweise die folgende Gebührenstruktur, die hier nur auszugsweise dargestellt wird. Zunächst wird eine einmalige Anschlussgebühr in Höhe von 75,- € fällig. Ein geeignetes Zahlungsterminal findet sich im ConCardis-Shop ab 499,- € einmalig oder 16,95 € pro Monat bei einer Laufzeit von 60 Monaten. Zur Anbindung an den *Acquirer* wird zusätzlich ein Internetanschluss benötigt, der separat erworben werden muss. Monatlich entstehen hier Kosten von 1,- €. Zusätzlich werden pro Zahlungsterminal und Jahr weitere 2,- € fixe Kosten erhoben. Die Disagio beträgt, abhängig von verschiedenen Faktoren, wie Branche des Händlers, Attraktivität für den *Acquirer* und Höhe der Umsätze, zwischen 2% und 5% Prozent pro Transaktion (177) – mindestens jedoch 0,25 € (176). Aufschläge reichen von 0,0075% als „MasterCard Acceptance Development Fee“ (176) bis hin zu 0,35% für die Verarbeitung von händisch in das Bezahlterminal eingegebenen Kartendaten. Weiterhin werden Gebühren fällig, wenn Kunden Zahlungen stornieren und zurückbuchen lassen („Chargeback-Gebühren“) (177). Die Kosten trägt der Händler. Diese betragen bei ConCardis 40,- € pro Rückbuchung (176).

In Summe lässt sich also festhalten, dass die Gebührenstrukturen sowohl für Kunden als auch für Händler sehr breit gefächert sind. Aus Sicht der Kunden gibt es günstige Angebote, deren Kosten sich durch Ausgleichszahlungen wieder aufheben können, so dass aus ihrem Blickwinkel nur zwei Punkte in die Bewertung einfließen können. Genauso viele Punkte werden aus der Sichtweise der Händler vergeben, da die Gebührenstrukturen mit all ihren Zuschlägen recht vielfältig und somit schwer überschaubar sind. Auch sind die Kosten für die Akzeptanz von Kreditkarten vergleichsweise hoch.

Komplexität für den Kunden

Der Einstieg ist für den Kunden im Vergleich zu anderen Systemen etwas komplizierter, da er sich zunächst für eine der auf dem Markt verfügbaren Karten und den passenden *Issuer* entscheiden muss. Hierzu hat er die Wahl aus einer großen Vielfalt von Anbietern, die i. d. R. ver-

schiedene Angebote vorzuweisen haben. Hat der Kunde sich für eine Variante entschieden, ist die Registrierung mitunter langwidrig. Denn in der Regel muss zunächst mindestens ein Einkommens- und Identitätsnachweis erbracht werden, um die Bonitätsinformationen der Auskunfteien ergänzen zu können. Da das Einholen und Bewerten der Informationen etwas Zeit benötigt und im Anschluss auch noch die Karte erstellt und versendet werden muss, vergeht einige Zeit, bis der Kunde Karte und PIN in Händen hält und verwenden kann. FinanzScout24.de gibt an, das dieser komplette Vorgang bis zu sechs Wochen dauern kann (178).

Der Bezahlvorgang mit der Kreditkarte ist sowohl am POS, als auch im Internet verhältnismäßig simpel. Am POS wird die Karte genauso verwendet wie auch die girocard. Bezahlterminal und Kreditkarte entscheiden dann, ob die PIN oder die Unterschrift zur Autorisierung der Zahlung verwendet wird. In beiden Fällen dauert die Zahlung etwas, da in jedem Fall ein Online-Abgleich mit der Sperrdatei stattfindet. Im Online-Einsatz gibt der Kunde seine Kartendaten, also die Kartennummer, den Namen des Inhabers, das Ablaufdatum und den Sicherheitscode, ein und bestätigt die Zahlung. Unterstützt der Händler MasterCard SecureCode oder vergleichbare Lösungen, so wird der Kunde nach Eingabe der genannten Daten auf eine Seite seines *Issuers* weitergeleitet. Dort gibt er seinen persönlich gewählten, zusätzlichen Sicherheitscode ein, bestätigt diesen, um die Zahlung abzuschließen. Insgesamt ist der Bezahlvorgang also relativ einfach, da die Offline-Nutzung mit der girocard vergleichbar, dementsprechend in den meisten Fällen bekannt ist, und die Online-Nutzung kein besonderes Wissen oder Equipment voraussetzt.

Eine Ausgabenübersicht bekommt der Kunde mit seinem Kontoauszug. Je nach *Issuer* wird dieser per Post oder E-Mail am Ende der Abrechnungsperiode versendet. Einige Anbieter ermöglichen zusätzlich über Apps oder die jeweilige Webseite eine Transaktionsübersicht einzusehen. Allerdings kann es einige Zeit dauern bis neue Transaktionen dort angezeigt werden. Zugleich versenden manche Anbieter nach jeder Transaktion eine SMS zur Information an den Kunden, die die Transaktionsdaten enthält. Eine Live-Übersicht aller Transaktionen kann von keinem Anbieter gewährleistet werden, weil Zahlungen durch Händler unter Umständen zeitverzögert übermittelt werden. Zusammenfassend werden in dieser Kategorie sechs von zehn Punkten vergeben. Denn obwohl die Registrierung einmalig lang dauert und einige Informationen beigefügt werden müssen, ist der einfache Bezahlvorgang, der den meisten Kunden vertraut sein dürfte, ein klarer Vorteil und auch, wenn es keine Live-Übersicht gibt, bieten die meisten *Issuer* die Möglichkeit, die bereits eingereichten Transaktionen einzusehen.

Komplexität für den Händler

Für den Einsatz der Kreditkarte als Zahlungsmittel benötigt der Händler einen Kreditkartenakzeptanzvertrag mit einem *Acquirer*, der ihn mit dem Kreditkartennetzwerk verbindet. Dieser setzt eine relativ aufwendige Registrierung und die Aushandlung der genauen Konditionen voraus. Dafür ist die Anbindung an vorhandene Kassensysteme in der Regel relativ einfach, da diese bereits ent-

sprechend vorbereitet sind. Es wird lediglich ein Zahlungsterminal benötigt, welches zusätzlich für andere Zahlungssysteme, wie girocard oder GeldKarte, genutzt werden kann. Eine Integration in bestehende E-Commerce-Systeme ist meist ebenfalls vergleichbar einfach, weil zahlreiche Plug-ins für diese Systeme existieren, die die Verbindung zum *Acquirer* herstellen. Die Sparkassen-Finanzgruppe bietet über ihren Händlerservice beispielsweise Plug-ins für die gängigen Shop-Systeme Magento, Oxid, Gambio, xtCommerce, Shopware und osCommerce an (179).

Der reine Bezahlvorgang benötigt einige Zeit aufgrund der Tatsache, dass sowohl eine Online-Autorisierung der Zahlung erfolgen als auch ein Abgleich mit der Kreditkartensperrdatei stattfinden muss. Alles in allem ist die Komplexität für den Händler sehr vergleichbar mit der Komplexität, die das girocard-System erfordert. Zum einen sind die technischen Anforderungen dieselben zum anderen ist ebenso der Bezahlvorgang vergleichbar mit dem einer girocard. Daher werden auch für das Kreditkartensystem sechs von zehn Punkten für dieses Kriterium vergeben.

Alleinstellungsmerkmal

Neben den erwähnten Kriterien bietet die Kreditkarte kein Alleinstellungsmerkmal, so dass hierfür auch keine Punkte in die Bewertung einfließen können.

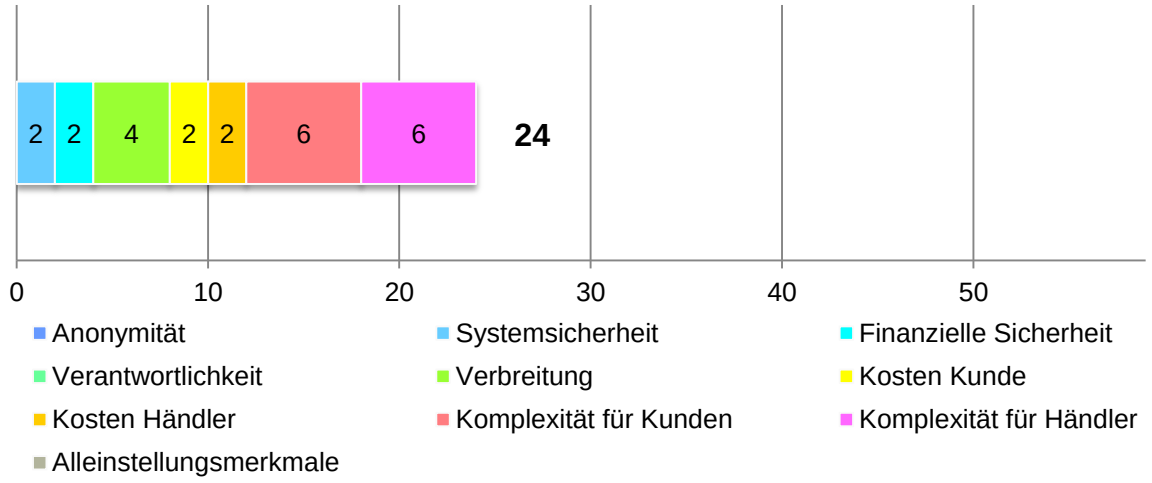

Abbildung 27: Gesamtbewertung des Zahlungssystems Kreditkarte.

3.1.4 GeldKarte

Das letzte klassische Zahlungssystem, welches im Rahmen dieser Arbeit bewertet wird, ist die GeldKarte. Eine Beschreibung des GeldKarten-Systems liegt in Kapitel *1.1.4 GeldKarte* vor.

Anonymität

Schließt der Händler am Ende des Tages seine Kasse ab, so übermittelt er alle bis dahin nur lokal gespeicherten Transaktionen an seine Evidenzzentrale weiter. Die übermittelten Daten enthalten mindestens die Karten-ID, die Uhrzeit und die Höhe der Transaktion, sowie die Identität des genutzten Kartenterminals. Die Händlerevidenzzentrale, an die der Händler die Daten übermittelt, leitet sowohl die Gutschriften an die Bank des Händlers weiter, übermittelt aber auch die Transaktion an die Kundenevidenzzentrale. Diese verbucht die Transaktion auf dem Schattenkonto der GeldKarte.

Laut Aussage der Deutschen Kreditwirtschaft ist die GeldKarte „im Verhältnis Karteninhaber – Akzeptanzstelle vollkommen anonym“ (180). Dies darf aber angezweifelt werden, denn die Akzeptanzstelle, also der Händler, liest die eindeutige Nummer der GeldKarte aus, so dass bestenfalls noch von einer Pseudonymisierung gesprochen werden kann. Allerdings kann der Verkäufer von der Karte zusätzlich den Namen des Karteninhabers ablesen und – theoretisch – der ausgelesenen Nummer somit auch einen Namen zuordnen, was die Anonymität des Käufers vollständig aufhebt.

Aus den Transaktionsdaten können die Evidenzzentralen mindestens feststellen, welche GeldKarte wann und wo genutzt wurde. Eine Zuordnung des Kunden ist nur durch Kooperation mit der kartenausgebenden Stelle möglich. Diese kann, da sie nur Gesamtsummen aller Transaktionen erfährt, keine Daten aus den Transaktionen gewinnen.

Außerdem sind auf jeder GeldKarte die letzten fünfzehn Transaktionen mit der Händlerkartennummer bzw. einer ID des Ladeterminals gespeichert. Diese können durch den Einsatz einfacher Lesegeräte durch jeden, der die GeldKarte in Händen hält, ausgelesen werden (181). Von Anonymität kann im Falle der GeldKarte also keine Rede sein, was selbst die Deutsche Kreditwirtschaft als Anbieterin des Systems durch ihre sehr einschränkende Aussage deutlich macht. Weil das System aber zumindest pseudonym gegenüber Händler, Payment Processor und Evidenzzentralen ist, können hierfür drei von zehn Punkten vergeben werden.

Systemsicherheit

Grundsätzlich ist die GeldKarte eine Smartcard[30], deren genauer Aufbau ebenso geheim ist wie der Quellcode des verwendeten Betriebssystems. Auf der Karte läuft eine spezielle Software, das eigentliche GeldKarten-System. Bei der Verwendung einer Karte zum Bezahlen oder Aufladen authentifizieren sich Terminal und Karte bei ihrem Gegenüber, um zu verhindern, dass fremde Terminals oder Karten mit betrügerischer Absicht verwendet werden. Nach demselben Verfahren authentifizieren sich bei der Abrechnung am Tagesende die Terminals bei den Händlerevidenzzentralen (181, 182).

Ein erfolgreicher Angriff ist bisher nicht bekannt, allerdings gibt es theoretische Ansätze, die jedoch in der Praxis zu kompliziert wären. Ein erster Angriffspunkt ist der Masterkey des GeldKarten-Systems. Von diesem Schlüssel sind letztlich alle anderen für Authentifizierung und Verschlüsselung benötigten Schlüssel abgeleitet. Der Masterkey selbst wird in zwei Teilen sicher in Tresoren der Deutschen Kreditwirtschaft verwahrt, während ein davon abgeleitete Reduced Masterkey auf jeder Händlerkarte hinterlegt ist. Da Händlerkarten auch als virtuelle Karte in Softwareform existieren können, könnte diese Software untersucht werden, um den Key zu extrahieren. Sollte dies gelingen könnten eigene GeldKarten erstellt werden (181). Das System kann also als recht sicher bezeichnet werden, so dass acht von zehn Punkten vergeben werden. Durch die doppelte Buchführung – einmal auf der GeldKarte und auf dem Schattenkonto – können Manipulationen auch vergleichsweise schnell aufgedeckt werden.

Finanzielle Sicherheit

Eben weil die GeldKarte nach Design ein Prepaid-System ist, ist die Höhe der Verluste von vornherein auf die Summe, die auf der Karte gespeichert ist, begrenzt. In der Standardeinstellung sind es maximal 200,- €, wobei dieser Betrag geringer, aber niemals höher, eingestellt werden kann. Ein Nachteil ist, dass den geladenen Betrag jeder ausgeben kann, da bei Summen unter 20,- € keine PIN benötigt wird und keinerlei Überprüfung stattfindet. Daher ist die GeldKarte in diesem Bereich mit Bargeld zu vergleichen.

Das Laden der Karte ist nur mit PIN möglich, weil während des Ladevorgangs das an die Karte gebundene Girokonto belastet wird. Bei kontoungebundenen Karten erfolgt die Aufladung gegen Bargeld, so dass weitere Ladevorgänge bei verloren oder gestohlenen Karten keinen Schaden für den Kunden bedeuten.

Eine Sperrung der Karte, falls diese abhandengekommen sein sollte, ist machbar, greift allerdings nicht im Zuge des Bezahlvorgangs, denn dieser erfolgt vollständig offline. Lediglich weitere Aufladungen, für die Kontakt mit der Kundenevidenzzentrale aufgenommen wird, lassen sich auf

[30] Eine Smartcard ist ein Sicherheitsmodul in der Größe einer EC-Karte. Als kleiner Computer stellt sie neben den bekannten Bestandteilen wie CPU, RAM und ROM eine I/O-Schnittstelle zur Verfügung, über die die gesamte Kommunikation stattfindet.

diese Weise verhindern. Eine Auszahlung von eventuell auf der Karte vorhandenem Guthaben kann erst erfolgen, wenn die Gültigkeit der Karte abgelaufen ist. In diesem Fall wird das Restguthaben anhand des Schattenkontos ermittelt.

Ebenfalls vergleichbar mit Bargeld sind die Tatsachen, dass zum einen für auf die Karte geladene Guthaben keinerlei Zinsen gezahlt werden und zum anderen, dass für Händler eine Zahlungsgarantie besteht. Der Kunde kann nur die aufgeladenen Beträge ausgeben – also nur Geld, welches er auch tatsächlich besitzt. Aufgrund der geringen, möglichen finanziellen Verluste werden für dieses Kriterium zehn von zehn möglichen Punkten vergeben.

Verantwortlichkeit

Das System GeldKarte wird durch die Deutsche Kreditwirtschaft, die aus dem Zentralen Kreditausschuss hervorgegangen ist, verantwortet. Diese ist für die Kartenspezifikation und die Definition der Schnittstellen verantwortlich, hat allerdings keinerlei Einfluss auf die Teilnehmer des Systems oder die durchzuführenden Transaktionen. Die Ausgabe der GeldKarte erfolgt durch die Banken oder als White-Card durch die Sparkasse Frankfurt. Diese können einzelne Kunden von dem System ausschließen, indem sie ihnen keine Karte ausstellen. Auf Transaktionen haben sie keinen Einfluss, da diese vollständig offline und ohne Autorisierung durch das ausgebende Institut erfolgt. Allerdings könnte die Aufladung der GeldKarte verhindert werden, da diese online stattfinden muss, um das Schattenkonto entsprechend zu aktualisieren. Ein solcher Eingriff ist allerdings nicht bekannt, so dass in Summe für die wenigen Eingriffsmöglichkeiten fünf Punkte vergeben werden.

Verbreitung

Die GeldKarte ist ein rein deutsches System, so dass ein Einsatz im Ausland nicht möglich ist. In Deutschland existieren allerdings 420.000 Akzeptanzstellen, wie verschiedene Automaten, Packstationen oder Imbisse in Sportstadien (183). An den Fahrkartenautomaten der Bogestra AG, dem Nahverkehrsdienstleister in Gelsenkirchen und Bochum, ist die GeldKarte neben Bargeld sogar die einzige Bezahloption.

Eine Nutzung im Internet stand bei Design der GeldKarte nicht im Fokus der Entwickler, wurde jedoch später ergänzt. Allerdings benötigt der Kunde hierfür ein Kartenlesegerät der Klasse 3, so dass die Verbreitung im Internet nur sehr eingeschränkt ist, da dem Handel die nutzende Kundschaft fehlt. Aus diesem Grund fand die GeldKarte als Zahlungssystem im Internet nie große Verbreitung. Hat der Kunde jedoch ein passendes Lesegerät existiert auch die Möglichkeit die GeldKarte von zu Hause zu laden.

Aufgrund der geringen Nutzung durch Kunden haben die Volksbanken im Sommer 2014 angekündigt, künftig auf die GeldKartenfunktion bei den von ihnen ausgegebenen Karten zu verzich-

ten, weil die Kosten gegenüber dem Nutzen überwogen und das System daher nicht wirtschaftlich betrieben werden konnte (184, 185). Durch diese Maßnahme wird die Verbreitung weiter eingeschränkt, da Kunden der Volksbanken, die die GeldKarte nutzen möchten, nun nur der Weg über eine White-Card bleibt, die separat angefordert werden muss. Aufgrund des sehr begrenzten Einsatzes im Internet und der fehlenden Möglichkeit einer Nutzung im Ausland, wird für dieses Kriterium nur ein Punkt vergeben.

Kosten

Für den Kunden ist die GeldKarte ein recht günstiges Zahlungsmittel. Die Karte erhält er in der Regel zusammen mit seiner girocard, so dass hierfür nur Zusatzkosten anfallen, wenn der Kunde eine kontenungebundene Karte wünscht. Diese kostet einmalig 13,90 € und kann online über den GeldKarten-Shop erworben werden (186).

Weitere Kosten für den Kunden entstehen nur in wenigen Fällen, u.a. wenn der Kunde die GeldKarte an einem nicht zu seinem Finanzinstitut gehörenden Automaten auflädt. Die Sparkasse Gelsenkirchen beispielsweise berechnet hierfür zwar keine Gebühren (145), der Betreiber kann dies jedoch tun. In Summe werden aus Kundensicht für diesen Aspekt vier von fünf möglichen Punkten vergeben.

Aus Sicht des Händlers ist die GeldKarte zudem ein vergleichsweise günstiges Zahlungsmittel, da die Händlerentgelte ziemlich gering ausfallen. So wird bei Umsätzen bis 5,- € lediglich ein pauschales Entgelt von 0,01 € fällig. Bei Beträgen zwischen 5,01 € und 10,- € fallen 0,02 € Händlerentgelt an und bis 20,- € werden 0,03 € fällig. Bei allen Umsätzen ab 20,01 werden 0,3% des Umsatzes als Händlerentgelt berechnet. Laut Aussagen der Deutschen Kreditwirtschaft ist die GeldKarte damit „(…) das günstigste Zahlungsmittel mit Zahlungsgarantie im Micropayment“ (187). Diese günstigen Konditionen dürften vor allem auf die fehlende Online-Autorisierung der Zahlung zurückzuführen sein.

Allerdings werden neben den Händlerentgelten weitere Entgelte, für beispielsweise den Internetzugang zur Übermittlung an die Evidenzzentralen, fällig. Diese richten sich nach individuellen Vereinbarungen mit den jeweiligen Anbietern. Zusätzlich fallen Kosten für das Zahlungsterminal an, über das die Zahlungen abgewickelt werden. Dieses kann jedoch auch für andere Kartensysteme verwendet werden, so dass sich die Kosten hierfür auf die verschiedenen Bezahlarten aufteilen. Aufgrund der Tatsache, dass das System im Vergleich günstige Konditionen für Händler anbietet, können für dieses Kriterium aus Sicht der Händler neun von zehn Punkten vergeben werden. In Summe werden somit 13 Punkte für den Kosten-Aspekt gewährt.

Komplexität für Kunden

Die Anmeldung für die Nutzung der GeldKarte ist in den meisten Fällen sehr einfach, weil sie mit dem Vertragsabschluss eines Girokontos mit girocard zusammenfällt. Für die GeldKarte müssen dabei keine zusätzlichen Informationen vorgelegt werden, was freilich nicht für kontounabhängige GeldKarten gilt. Bei Beantragung einer solchen erfolgt im GeldKarten-Shop eine Bestellung, die nicht mehr Daten erfordert als ein normaler Online-Einkauf.

Die Dauer, bis die GeldKarte ausgestellt wird, ist stark unterschiedlich. Die Ausstellung einer kontengebundenen Karte dauert in der Regel länger, da diese auf der girocard enthalten ist. In diesem Fall sind Ausgabezeiten von mehreren Wochen die Regel. Kontenungebundene Karten hingegen haben im GeldKarten-Shop eine Lieferzeit von zwei bis fünf Werktagen.

Kompliziert an der Kartennutzung ist jedoch, dass, während kontogebundene Karten an jedem Geldautomaten geladen werden können, dieses einfache Prinzip nicht immer bei kontenungebunden Karten zutrifft. Letztgenannte können nämlich nur an speziellen Automaten geladen werden, die entweder zwei Karten gleichzeitig lesen können oder Bargeld akzeptieren (188). Ferner funktionieren die Aufladung und das Bezahlen auch in den Shops, die die GeldKarte als Zahlungsoption anbieten, sowie online über die Webseite der Deutschen Kreditwirtschaft. Letzteres ist allerdings aufgrund der bereits erwähnten, technischen Voraussetzungen vergleichsweise kompliziert.

Die Zahlung am POS hingegen ist verhältnismäßig einfach, denn sie ist mit Kreditkarten und der girocard vergleichbar, so dass die Nutzung den meisten Kunden geläufig sein dürfte. Einziger Unterschied ist, dass bei Umsätzen unter 20,- € keine PIN oder Unterschrift erwartet wird. Insgesamt werden für dieses Kriterium sechs von zehn Punkten vergeben, weil nicht jede Karte überall ladbar ist, was einige Nutzer verwirren kann. Zudem kann der Interneteinsatz durch die technischen Anforderungen nicht ohne weiteres durchgeführt werden.

Komplexität für Händler

Als Händler wird ein Vertrag mit einer Bank benötigt, die die Händlerkarte ausstellt, und ein Vertrag mit einem Dienstleister, der für Bereitstellung und Wartung des Bezahlterminals verantwortlich ist. Die eingesetzten Terminals sind dieselben, die auch für Zahlungen mit Kreditkarten und girocard verwendet werden, so dass letzterer unter Umständen gar nicht zusätzlich benötigt wird. Die Anbindung an die Kassensysteme ist deshalb ähnlich einfach wie bei beiden anderen Systemen. Die Einbindung in E-Commerce-Systeme ist hingegen deutlich komplexer, da das System im Internet deutlich seltener verwendet wird und somit Plug-ins für die Shop-Systeme deutlich seltener verfügbar sind.

Grundsätzlich sind Zahlungen mit der GeldKarte vergleichbar schnell, weil der Bezahlvorgang komplett offline erfolgt. Allerdings ist es für den Händler zusätzlicher Aufwand die Zahlungen am

Tagesende bei der Evidenzzentrale einzureichen. Da der Einsatz im Internet komplizierter ist als bei der Kreditkarte, die Zahlung dafür aber in aller Regel schneller abgewickelt werden kann, werden für die Komplexität aus Händlersicht fünf der zehn möglichen Punkte vergeben.

Alleinstellungsmerkmale

Die GeldKarte stellt, neben der reinen Bezahlfunktion, weitere Nutzungsmöglichkeiten zur Verfügung. So bieten kontogebundene Karten die Option ein Altersmerkmal zu speichern, um die Überprüfung der Volljährigkeit an Automaten und im Internet zu ermöglichen. Hierdurch soll beispielsweise an Zigarettenautomaten eine Abgabe an Tabakwaren an minderjährige Personen verhindert werden. Dieses Merkmal wird auf den Karten aller volljährigen Karteninhaber in Form eines fiktiven Datums hinterlegt, um den Karteninhaber nicht um Erlaubnis fragen zu müssen. 2006 war von den ausgegebenen GeldKarten jede zweite bereits mit einem Altersmerkmal ausgestattet und es wurde damit gerechnet, dass künftig noch mehr Karten entsprechend ausgerüstet werden (189).

Weiterhin besteht die theoretische Möglichkeit, die GeldKarte als Fahrkarte für den öffentlichen Personennahverkehr zu nutzen. Hierfür verfügt die GeldKarte über ein spezielles Verzeichnis in ihrem Speicher, in dem bis zu zehn Fahrscheine abgelegt werden können (190). Diese Extrafunktion stellt für die Verkehrsverbünde eine kostengünstige Ticketing-Lösung dar, die bislang jedoch von keinem dieser Unternehmen genutzt wird und stattdessen nur auf der Homepage der GeldKarte beworben wird. Insgesamt werden für diese Zusatzfunktionen zwei Punkte vergeben.

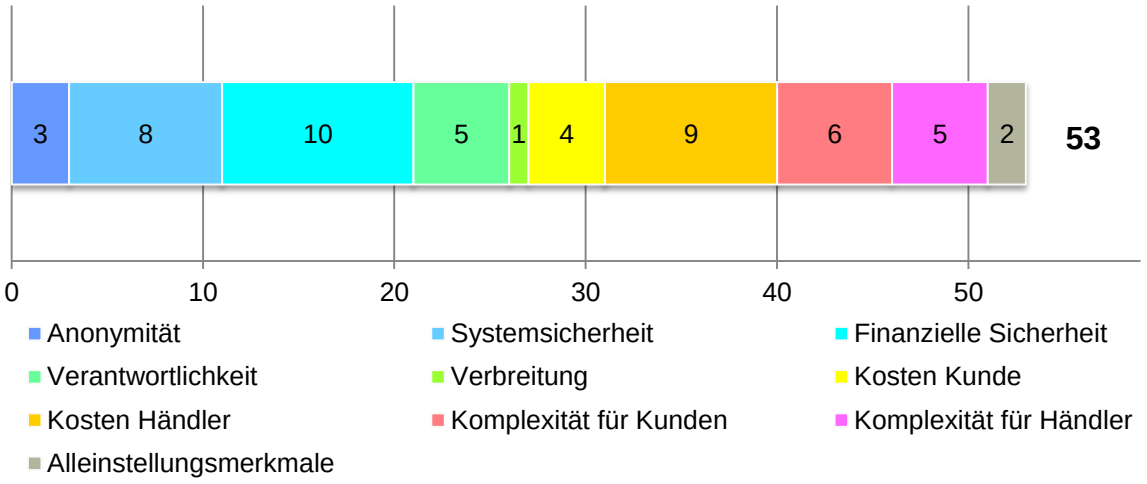

Abbildung 28: Gesamtbewertung des Zahlungssystems GeldKarte.

3.2 Kontaktlose Zahlungssysteme

Im Folgenden werden die kontaktlosen Zahlungssysteme bewertet, die als Weiterentwicklung klassischer Zahlungssysteme entwickelt wurden.

3.2.1 MasterCard PayPass / Visa payWave

Die in diesem Abschnitt dargestellten Systeme sind Weiterentwicklungen der klassischen Kreditkarten. Daher sind sie diesen Systemen in vielen Aspekten sehr ähnlich oder zu diesen gar identisch. Aufgrund dessen werden im Folgenden nur Bewertungen der Aspekte aufgeführt, die eine andere Bewertung als im Abschnitt *3.1.3 Kreditkarte* erfahren.

Anonymität

Weil Transaktionen genauso abgewickelt werden wie bisher bei Kreditkarten, gilt auch die Anonymitätsbewertung der Kreditkarten für diese beiden Systeme. Hinzugenommen werden muss jedoch noch die Tatsache, dass über die NFC-Schnittstelle die zu der Karte gehörigen Daten ausgetauscht werden. Über ein Smartphone mit NFC-Leser und einer selbstgeschriebenen App gelang es dem Entwickler Thomas Skora aus einer PayPass-Karte die Kartennummer, die Gültigkeitsdauer und die letzten Transaktionsdaten auszulesen (191). Mit entsprechender Hardware gelingt es zudem über größere Entfernungen, so dass das Auslesen auch unbemerkt geschehen kann. Der Karteninhaber ist hierdurch selbst Dritten gegenüber nur Pseudonym, da die Kartennummer ihn eindeutig identifiziert. Aus diesem Grund müssten eigentlich noch Punkte im VErgleich zu klassischen Kreditkarten abgezogen werden, da jedoch die Bewertung der Anonymität der Kreditkarten mit null Punkten abgeschlossen werden, ist dies nicht möglich. Die Bewertung dieses Aspekts ändert sich also nicht, es werden ebenso für das PayPass / payWave System null Punkte vergeben.

Verbreitung

Aktuell sind sowohl PayPass als auch payWave noch vergleichsweise neu auf dem Markt. MasterCard spricht derzeit von rund 400.000 Terminals weltweit, an denen mit den rund 100 Mio. ausgegebenen Karten kontaktlos bezahlt werden kann (192). In Deutschland sind allerdings schätzungsweise nur rund 5% der MasterCard-Akzeptanzstellen auch in der Lage PayPass-Karten zu akzeptieren (193). Visa gibt an, dass in Deutschland rund 45.000 Bezahlterminals mit payWave verwendet werden können (194), wobei bereits 1,2 Mio. Karten ausgegeben wurden (195). Indes hat MasterCard für Europa angekündigt, dass ab 2016 jedes neuaufgestellte Terminal auch PayPass-kompatibel sein soll, so dass 2020 an allen Akzeptanzstellen PayPass verfügbar sein wird (196): Weil in Deutschland der Umstieg schneller gelingen soll, schreiben die MasterCard-Richtlinien vor, dass bereits ab 2015 neu aufgestellte Terminals PayPass unterstützen

müssen. Durch den vorgezogenen Zwang soll PayPass schon 2018 flächendeckend in Deutschland verfügbar sein (193).

Soll die Karte für Zahlungen im Internet verwendet werden, erfolgt diese wie bei einer klassischen Kreditkarte. Denn die NFC-Technologie kann nicht direkt genutzt werden. Die Verwendung beim Online-Shopping ist also nur möglich, weil es sich nicht um reine PayPass-/payWave-Karten handelt, sondern um Kombinationen aus diesen mit einer klassischen Kreditkarte. Somit kann die Karte auch an allen Stellen verwendet werden, die diese Technologie nicht direkt unterstützen aber Kreditkarten akzeptieren. Insgesamt wird die Verbreitung aktuell mit zwei Punkten bewertet, da ein flächendeckender Einsatz derzeit noch nicht möglich ist. Positiv bewertet wird jedoch die Planung, den Ausbau in den nächsten Jahren voranzutreiben, und die Tatsache, dass an vielen Stellen weiterhin die klassische Kreditkarte, die die NFC-Technologie integriert, verwendet werden kann. Abwertend muss gesehen werden, dass ein Einsatz im Internet nur über den Umweg der klassischen Kreditkarte möglich ist.

Kosten

Für den Kunden entstehen durch die Nutzung von PayPass und payWave keinerlei Kosten, die nicht auch bei der Kreditkartenzahlung anfallen würden. Aus Sicht des Händlers fallen für alle Händler, die neu einsteigen ebenso nur die selben Kosten wie für die Kreditkartenakzeptanz an. Händler, die bereits klassische Kreditkarten akzeptieren, müssen zumindest einmalig weitere Kosten für den Austausch des bisherigen Bezahlterminals einplanen. Das preislich günstigste Terminal kostet im Vergleich zum günstigsten Terminal im Shop der Concardis GmbH 200,- € Aufpreis. Aufgrund der Tatsache, dass nahezu alle Kosten identisch mit denen der klassischen Kreditkarte sind, wird die Bewertung übernommen. Leidglich der höhere Preis des Terminals führt zu einer Abwertung von einem Punkt bei den Kosten des Händlers, so dass aus Sicht des Händlers nur noch ein Punkte vergeben werden kann. Die Wertung aus Sicht des Kunden bleibt unverändert bei zwei Punkten, so dass insgesamt drei Punkte für dieses Kriterium in die Bewertung einfließen.

Komplexität für Kunden

Für den Kunden ist die Registrierung nicht aufwendiger, aber auch nicht einfacher, als für eine klassische Kreditkarte, weil PayPass- bzw. payWave-Karten nur zusammen mit klassischen Kreditkarten ausgegeben werden. Für die Registrierung der kontaktlosen Systeme sind keine zusätzlichen Informationen erforderlich, die durch den Kunden vorgelegt werden müssten.

Allerdings ändert sich der Bezahlvorgang für den Kunden. Entgegen dem jahrelang erlernten Verhalten beim Bezahlen mit kontaktbehafteten Karten muss hier ein neuer Prozess erlernt werden, der einige Benutzer zunächst vor Fragen stellen wird. So ist beispielsweise die Stelle, an die

die kontaktlosen Karten gehalten werden müssen, nicht einheitlich. Bei manchen Geräten verbirgt sich der NFC-Leser hinter dem Display (197), bei anderen gibt es neben dem Terminal spezielle kontaktlose Lesegeräte, die eine markierte Auflagefläche für die Karte bieten (siehe Abbildung 29). Wieder andere Geräte verlangen die Karte neben das Gerät zu halten (198). Demzufolge ist das Vorgehen für den Kunden im Handel nicht einheitlich. Ist zudem das Personal an der Kasse nicht ausreichend über die neuen Bezahlmöglichkeiten informiert, kann dies schnell zu Problemen und Stress für den Kunden führen, sowie eine erfolgreiche Bezahlung verhindern.

Abbildung 29: Bezahlterminal mit kontaktlosem Lesegerät der Firma Paylife.

Hat der Kunde die kontaktlose Verbindung zwischen Karte und Terminal erfolgreich hergestellt, wird die Zahlung durchgeführt. Kleine Beträge unter 25,- € werden ohne PIN bezahlt. Bei größeren Beträgen wird dagegen – wie von der klassischen Kreditkarte bekannt, die PIN oder eine Unterschrift benötigt (199). Für dieses Kriterium werden aufgrund des neu zu erlernenden Bezahlvorgangs und der uneinheitlichen Gestaltung desselben, fünf von zehn Punkten vergeben. Eine Aufwertung erfolgt durch die Beschleunigung des Bezahlvorgangs gegenüber der klassischen Kreditkarte.

Komplexität für Händler

Aus Sicht des Händlers nimmt die Komplexität mit der Einführung von PayPass und payWave zunächst einmal zu, da i.d.R. neue Bezahlterminals mit kontaktlosen Lesegeräten benötigt werden. Diese können jedoch ähnlich simpel wie die bisherigen Terminals mit dem Kassensystem verbunden werden. Die Registrierung für das System verläuft genauso wie die Registrierung zur Akzeptanz von Kreditkarten. Es wird ebenfalls ein Kreditkartenakzeptanzvertrag benötigt, um

Zahlungen über diese Systeme abwickeln zu können. Das Kassenpersonal muss ferner über die neuen Bezahlmöglichkeiten informiert werden, damit sie ggf. unsichere Kunden unterstützen können. Außerdem sollte das Personal mit den möglichen Problemen und deren Lösungen vertraut gemacht werden, um Fähigkeiten zur raschen und selbstständigen Lösung zu entwickeln. Haben sich Kunden und Kassenpersonal einmal an den Bezahlvorgang gewöhnt, läuft dieser rascher ab als bei kontaktbehafteten Kartensystemen, so dass in Summe sieben von zehn Punkten für dieses Kriterium vergeben werden.

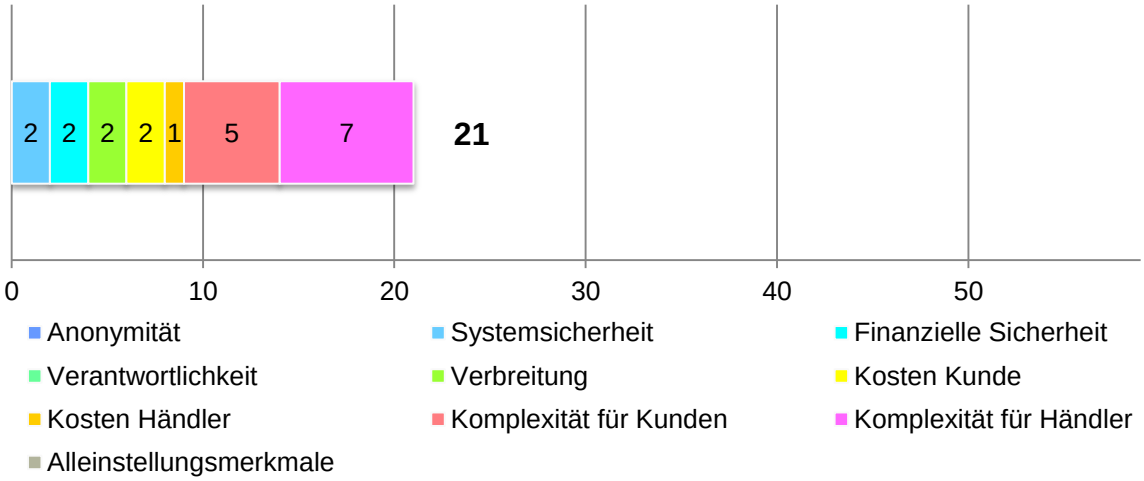

Abbildung 30: Gesamtbewertung der Zahlungssysteme MasterCard PayPass / Visa payWave.

3.2.2 girogo

Bei girogo handelt es sich um eine Erweiterung der GeldKarte, die eine kontaktlose Bezahlmöglichkeit bietet. Aus diesem Grund werden nur die Veränderungen gegenüber der GeldKarte neubewertet. Alle anderen Kriterien können in Kapitel *3.1.4* GeldKarte nachgelesen werden.

Anonymität

Da die Funktionsweise der der GeldKarte entspricht, gelten natürlich auch die Bewertungen der Anonymität entsprechend der GeldKarte. Durch die Wahl einer Funktechnologie kommen jedoch weitere Aspekte hinzu, die in die Bewertung miteingehen müssen. Prinzipiell können girogo-Karten mit jedem NFC-fähigen Lesegerät gelesen werden. Die Karte übermittelt eine eindeutige Kartennummer, die die Karte innerhalb des girogo-Systems identifiziert (200). Mit leicht zu bauender Hardware ist es jedoch möglich, die Karten auch über Entfernungen von mehreren Metern auszulesen (201). Somit könnten Ladenbesitzer, unter Verwendung entsprechender Auslesestationen, die ID ohne Wissen des Kunden auslesen und auf diese Weise seinen Weg durch den Laden verfolgen.

Neben der Bewertung für GeldKarten müssen girogo-Karten noch etwas kritischer betrachtet werden, da aufgrund der verwendeten Funktechnologie weitere Schwachpunkte im System entstanden sind. Wie zuvor beschrieben kann eben jeder mit entsprechender Hardware die Karte auslesen und ein Pseudonym für den Benutzer erhalten. Demnach ist girogo selbst Dritten gegenüber bestenfalls pseudonym, aber niemals anonym. Insgesamt werden aus den genannten Gründen null von zehn Punkten für dieses Kriterium vergeben.

Verbreitung

Genauso, wie die GeldKarte, ist auch girogo ein rein deutsches System, welches nicht im Ausland akzeptiert wird. Der Interneteinsatz ist mit girogo nun gar nicht mehr möglich. Stattdessen kann die Karte jedoch weiterhin als klassische GeldKarte genutzt werden, vorausgesetzt es findet sich einer der wenigen Onlineshops, die die GeldKarte akzeptieren. Am POS ist girogo allerdings nicht weit verbreitet. Gerade einmal 10.000 Stellen akzeptieren derzeit die 21 Mio. girogo-Karten (202). Aufgrund der wenigen Akzeptanzstellen und der fehlenden Möglichkeit, die Karte im Internet oder Ausland zu nutzen, werden in Summe null Punkte für dieses Kriterium vergeben.

Kosten

Aus Sicht des Kunden belaufen sich die anfallenden Kosten in etwa auf dieselbe Höhe wie bei der GeldKarte. Für den Händler gilt dies ebenso, allerdings mit dem Unterschied, dass er ein Zahlungsterminal benötigt, welches ein kontaktloses Lesegerät integriert hat. Genauso, wie für PayPass und payWave, kostet dieses ungefähr 200,- € mehr als ein Gerät ohne NFC-Leseeinheit. Eine NFC-Funktionalität ermöglicht dagegen technisch zusätzlich die Akzeptanz von kontaktlosen Kreditkarten. Aufgrund dessen wird in der Wertung aus Sicht der Händler ein Punkt im Vergleich zur GeldKarte abgezogen, so dass letztlich acht Punkte in die Bewertung einfließen. Da die Kosten aus Kundensicht unverändert bleiben, bleibt auch die Bewertung gleich. Es werden zusammen insgesamt zwölf Punkte für den Kostenaspekt vergeben.

Komplexität für Kunden

Die Registrierung für girogo ist aus Sicht des Kunden unverändert, wenn sie mit der Registrierung einer GeldKarte verglichen wird. Selbiges gilt äquivalent für das Aufladen der girogo-Karte, die immer denselben Kontostand aufweist wie die zugehörige GeldKarte. Daher kann ein Großteil der Bewertung von der GeldKarte übernommen werden. Negativ ist jedoch, dass ebenso, wie bei PayPass und payWave, nicht jedes Terminal die Leseeinheit für kontaktlose Karten an derselben Stelle integriert hat, was wiederum zu Verwirrungen des Kunden und möglichen Fehlbedienungen führen kann. Diese Tatsache hat eine Abwertung um einen Punkt im Vergleich zur GeldKarte zur Folge. Insgesamt werden für dieses Kriterium fünf von zehn Punkten vergeben.

Komplexität für Händler

Aus Sicht des Händlers ist das Anbieten der Zahlungsoption girogo nicht viel komplizierter als die Akzeptanz der GeldKarte, denn die technischen Voraussetzungen sind vergleichbar: In beiden Fällen wird ein Zahlungsterminal benötigt, welches in der Regel recht einfach an das Kassensystem angebunden werden kann. Allerdings wird in vielen Fällen für girogo ein neues Terminal benötigt, das eine entsprechende Leseeinheit für NFC-Chips integriert hat. Diese kann im Nachgang zudem für andere Systeme, die die NFC-Technologie nutzen, verwendet werden, sofern entsprechende Nutzungsverträge bestehen. Eine Einbindung in E-Commerce-Systeme hingegen ist nicht möglich, weil girogo nicht für dieses Anwendungsgebiet geschaffen wurde. Durch diese einmalige Umrüstung der Kassensysteme kann letztlich der Bezahlvorgang beschleunigt werden, da die Karte nur noch an das Terminal gehalten werden muss und eine gesonderte Autorisierung der Zahlung durch PIN oder Unterschrift erst bei Beträgen über 20,- € notwendig wird.

Neben der technischen Aufrüstung ist ferner eine Einweisung des Kassenpersonals notwendig. Dieses sollte mit dem Bezahlterminal so vertraut sein, dass es Kunden gegebenenfalls unterstützen kann. Hierzu ist es erforderlich zu wissen, an welche Stelle die kontaktlose Karte gehalten werden muss, um ausgelesen werden zu können. Außerdem sollte es Kenntnisse über häufiger auftretende Fehler sowie deren Lösungen haben. Die Bewertung für dieses Kriterium fällt aus den genannten Gründen ebenso mit fünf von zehn Punkten aus, wie für die GeldKarte. Zwar entsteht auf der einen Seite ein geringer Aufwand für die Einweisung der Mitarbeiter und den Austausch des Bezahlterminals, auf der anderen Seite aber wird der Bezahlvorgang beschleunigt.

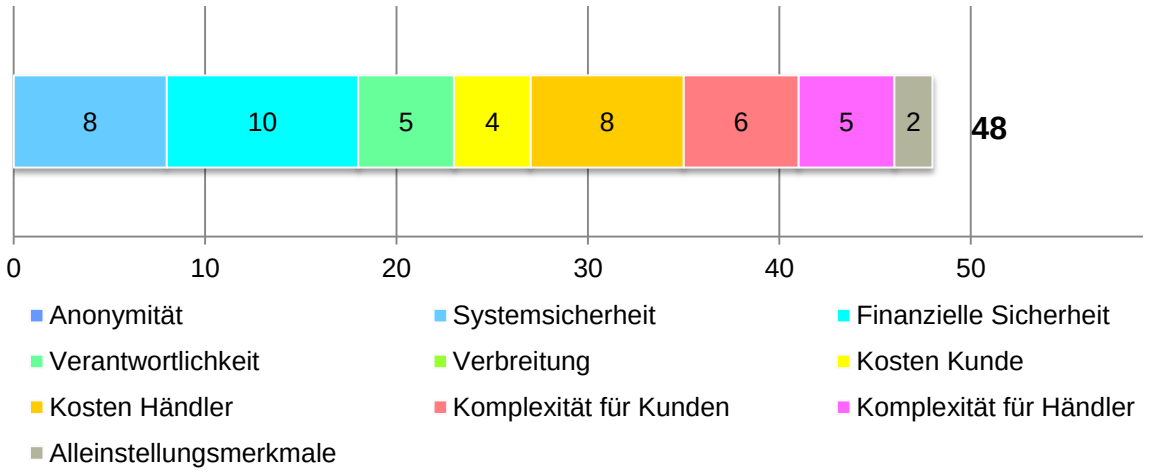

Abbildung 31: Gesamtbewertung des Zahlungssystems girogo.

3.3 Mobile Zahlungssysteme

Im Folgenden werden die mobilen Zahlungssysteme bewertet. Die hier bewerteten Systeme sind häufig noch relativ neu, weshalb diese vielen Lesern nicht bekannt sein dürften. Aus diesem Grund wird die Lektüre des Kapitels *1.3 Mobile Zahlungssysteme* vor diesem Kapitel empfohlen.

Die mobilen Systeme lassen sich dabei hinsichtlich der verwendeten Technologie kategorisieren. Diese Kategorisierung spiegelt sich in der folgenden Kapiteleinteilung wieder.

3.3.1 NFC-basierte Systeme

Die ersten Systeme, die im Folgenden bewertet werden, sind die Systeme, die, ähnlich wie die kontaktlosen Zahlungssysteme, auf der Nachfunktechnologie NFC basieren.

3.3.1.1 mpass

Zunächst erfolgt die Bewertung des Zahlungssystems mpass, welches eines der älteren Systeme, in der Kategorie der mobilen Zahlungssysteme ist. Eine Beschreibung liegt in Kapitel *1.3.1.1 mpass* vor und wird vor der Lektüre dieses Kapitels empfohlen.

Anonymität

In Bezug auf die Bewertung der Anonymität gilt für mpass bei der Bezahlung am Point of Sales dasselbe, was in gleicher Weise für MasterCard PayPass gilt. Bei beiden handelt es sich um dasselbe Verfahren, welches nicht in eine Plastikkarte sondern in einem Aufkleber verpackt ist. Demnach gilt im Grundsätzlichen zunächst die selbe Bewertung wie unter *3.2.1 MasterCard PayPass / Visa payWave* erläutert. Der Service wird durch die Wirecard Card Solutions Ltd. erbracht. Sie ist für die Ausgabe des NFC-Stickers und die Abwicklung der Zahlungen über diesen verantwortlich. Während der Anmeldung willigt der Kunde ein, dass Wirecard Händlern, die Wirecard als *Acquirer* gewählt haben, personenbezogene Daten, die sowohl Kontakt- als auch Zahlungsdaten umfassen, übermitteln darf (203).

Zu jeder Transaktion speichert Wirecard mindestens „die Höhe des Betrages, den Verwendungszweck und die E-Mailadresse oder Kontonummer der anderen Partei“ (203), wie es in der Datenschutzerklärung der Wirecard Card Solutions Ltd. nachzulesen ist. Zusätzlich wird diese Transaktion mit dem eigenen Kundenkonto verknüpft. Für die Bezahlung im Internet gelten etwas andere Regeln. In diesem Fall speichert Wirecard, neben den oben genannten Transaktionsdaten, auch noch die IP-Adresse eines jeden Kunden (203).

Die Netzbetreiber, Telekom, O2 und Vodafone, haben keinerlei Einblick in die Transaktionsdaten. Allerdings erfahren sie im Falle einer Online-Zahlung, dass diese stattfindet, da sie die SMS mit

der benötigten TAN übertragen. Sie erfahren jedoch nicht, in welcher Höhe und an wen die Zahlung erfolgt, weil diese Informationen nicht Teil der SMS sind.

Neben der reinen Bezahlfunktion bietet mpass für Händler die Möglichkeit die mpass-App für Marketingzwecke zu nutzen. Hierfür verantwortlich ist die Abteilung Media Services von Telefónica, die die Verknüpfung ortsbasierter Informationen oder der Bestandskundendaten von O2 anstrebt, um zielgruppenspezifisches Marketing zu ermöglichen (204). In Summe ist mpass damit ähnlich anonym wie PayPass und payWave – nämlich gar nicht. Es werden alle Transaktionen durch ein britisches Unternehmen gespeichert und verarbeitet. Zusätzlich werden personenbezogene Daten an Händler übermittelt, denen gegenüber der Kunde daher auch nicht anonym ist. Dieses Kriterium wird wegen der aufgeführten Gründe mit null Punkten bewertet.

Systemsicherheit

Die Sicherheit ist sehr ähnlich zu der des PayPass-Systems, da dieses ebenfalls in zwei von drei Fällen für das Bezahlen genutzt wird. Daher entfällt an dieser Stelle eine erneute Beschreibung. Es sei nur kurz erwähnt, dass es sich um ein auf Kreditkarten basierendes System handelt. Zusammen mit dem mpass-NFC-Sticker erhält der Kunde eine virtuelle Kreditkarte, also eine Kreditkarte, die nicht als Plastikkarte ausgegeben wird, sondern stattdessen nur die Kreditkartendaten im mpass-Kundenkonto online zur Verfügung stellt. Aus diesem Grund erfolgt an dieser Stelle keine Neubewertung für diese Bezahloptionen. Vielmehr findet hier nur die Online-Bezahlung mittels des SMS-TAN-Verfahrens Berücksichtigung, deren Bewertung mit der der Kreditkarte am Ende zusammengeführt wird.

Die Sicherheit des SMS-Tan-Verfahrens beruht darauf, dass der Kunde sein Kennwort für das System kennt und im Besitz des Handys mit der registrierten Telefonnummer ist. Ein Angreifer müsste also sowohl den Computer, um das Kennwort zu erfahren, als auch das Mobiltelefon des Kunden infizieren, um unberechtigt Transaktionen durchführen zu können. Das Kennwort kann, wie alle Kennworte, durch Social Engineering[31], Bruteforce[32] oder andere Methoden ermittelt werden. Die SMS mit der nötigen TAN ist dagegen schwieriger abzufangen – wird jedoch nicht zwangsläufig benötigt, da allein durch das Kennwort die Daten der virtuellen Kreditkarte inklusive Sicherheitscode aus dem Kundenkonto ausgelesen werden können (205). Zum einen gibt es die Möglichkeit, das Handy des Nutzers mit Schadsoftware zu infizieren, die die entsprechende SMS mit TAN heimlich weiterleitet. Da das selbe Verfahren ferner zur Autorisierung von Transaktionen im Online-Banking eingesetzt wird, nimmt die Verbreitung der Schadsoftware zu, wie Heise Online im Mai 2014 berichtete (206).

[31] Ein Angreifer nutzt Methoden der zwischenmenschlichen Beeinflussung, um dem Opfer Informationen, wie beispielsweise Passwörter oder Informationen zum Zurücksetzen des Passwortes zu entlocken.

[32] Ermitteln eines Passwortes durch ausprobieren aller möglichen Kombinationen, bis eine akzeptiert wird.

Einen alternativen Weg zeigten das Reportagemagazin Stern TV und die Zeitschrift Computerbild auf, die in einem Test versuchten, sich unberechtigterweise eine Ersatz-SIM-Karte für eine fremde Handynummer zuschicken zu lassen. Überraschenderweise gelang es in vier von fünf Fällen, denn die Provider prüften nicht genau nach, wer die Karte anforderte und versendeten diese an eine fremde Adresse, wenn der Anrufer angab, er sei umgezogen (207). Beide Varianten sind jedoch für den Angreifer aufwendig. Sie erfordern gute Kenntnisse über das Opfer und sind deswegen nur für gezielte Angriffe nutzbar. Das System bietet demnach durch die virtuelle Kreditkarte dieselben Angriffspunkte wie klassische Kreditkarten. Der Zugang zu den Daten inklusive des Sicherheitscode ist durch die Verfügbarkeit im mpass-Kundenkonto jedoch deutlich leichter. Dagegen existiert keine physische Karte, die gestohlen oder verloren werden kann, so dass ein Missbrauch am POS schwieriger wird. Insgesamt werden für die Sicherheit des Systems zwei von zehn Punkten vergeben.

Finanzielle Sicherheit

Da sich hinter allen Zahlungen mit mpass die Bezahlung über eine Kreditkarte verbirgt, gilt aus Sicht des Kunden die gleiche Bewertung. Aus Sicht des Händlers besteht über mpass jedoch eine Zahlungsgarantie, weil Wirecard im Falle der Online-Zahlung die Zahlung übernimmt, falls das Konto des Kunden nicht ausreichend gedeckt ist (204). Es konnte bisher kein Fall recherchiert werden, in dem ein Schaden für einen Nutzer des Systems entstanden wäre, was sich wiederum positiv auf die Bewertung dieses Kriteriums auswirkt. Die finanzielle Sicherheit wird, aufgrund der Zahlungsgarantie für den Händler und der Möglichkeit des Kunden, Rückbuchungen zu veranlassen, mit vier von zehn Punkten bewertet.

Verantwortlichkeit

Für die Abwicklung von Zahlungen ist die Wirecard Card Solutions Ltd. verantwortlich. Die Netzbetreiber Telekom, Vodafone und O2, die das System vermarkten, haben keinerlei Einfluss auf Zahlungen. Da alle Zahlungen auf jeden Fall über Wirecard abgewickelt werden, besteht für dieses Unternehmen die Möglichkeit, in den Zahlungsverkehr einzugreifen, sowie Transaktionen zu verhindern, zu verzögern oder Teilnehmer gegebenenfalls komplett von mpass auszuschließen. Ein solcher Eingriff ist bisher jedoch nicht bekannt geworden. Allerdings basiert das komplette Zahlungssystem auf Kreditkartenzahlungen, die über MasterCard ausgeführt werden. Dementsprechend hat MasterCard gleichermaßen die Möglichkeit, Zahlungen, genauso wie bei klassischen Kreditkarten, zu beeinflussen. Aus diesem Grund muss die Bewertung der Kreditkarte für dieses Kriterium äquivalent für mpass gelten, weshalb null von fünf Punkten vergeben werden.

Verbreitung

Zunächst einmal ist mpass ein deutsches Bezahlverfahren. Aufgrund der Tatsache, dass eine Kreditkarte verwendet wird, um Zahlungen abzuwickeln, kann mpass allerdings genauso im Ausland verwendet werden – und zwar an allen Akzeptanzstellen, die MasterCard PayPass unterstützen. Eine Ausnahme bilden dabei Reservierungen von Hotelzimmern oder Fahrzeugen, weil bei Abholung erwartet wird, dass eine physische Karte vorgelegt wird. Diese wird durch mpass jedoch nicht ausgegeben, so dass mpass hierfür nicht verwendet werden kann (205).

Durch die drei Bezahloptionen, NFC-Sticker, virtuelle Kreditkarte und Onlinezahlung mit SMS-TAN, ist das System sowohl für den stationären Handel als auch für den Einsatz im Internet geeignet. Im Internet werden dabei zum einen die native Zahlung über mpass mit Einsatz der SMS-TAN angeboten, was bisher allerdings nur wenige Shops unterstützen, und zum anderen der Einsatz der virtuellen Kreditkarte, die in allen Shops akzeptiert wird, die MasterCard-Kreditkarten anerkennen, was auf zahlreiche Shops zutrifft. Folglich ist der Einsatz von mpass in weiten Teilen des Internets und an immer mehr stationären Akzeptanzstellen möglich. Ferner wird bis 2020 mit dem Ausbau des PayPass-Systems die Zahlung an allen stationären PayPass-Akzeptanzstellen durchführbar sein.

Weiter findet, den Werbeaussagen auf der mpass-Homepage zufolge, keine Bonitätsprüfung vor Ausgabe der Kreditkarte statt (208). In den FAQ wird diese Aussage jedoch wiederum etwas eingeschränkt. Zwar erhält jeder mpass-Kunde die virtuelle Kreditkarte ohne Bonitätsprüfung, allerdings wird die Bonität geprüft, wenn der Kunde die Abrechnung mittels Lastschrift aktivieren will (205). Fällt die Bonitätsprüfung negativ aus, kann mpass nur als Prepaid-System, mit vorheriger Aufladung eines Guthabens, genutzt werden. Die Information, dass die Bonitätsprüfung negativ ausgefallen ist, scheint, einem Foreneintrag eines Vodafone-Kunden zufolge, dem mpass-Nutzer indes nicht mitgeteilt zu werden (209). Vielmehr verhindert mpass in diesem Fall Zahlungen solange, bis ein entsprechendes Guthaben auf das mpass-Konto aufgeladen wurde. In Summe werden für dieses Kriterium drei von fünf Punkten vergeben, da der Einsatz im stationären Handel bisher noch etwas eingeschränkt ist, genauso wie die native Unterstützung von mpass im Onlinehandel.

Kosten

Für den Kunden ist die Nutzung von mpass in weiten Teilen kostenfrei. Lediglich im Falle von Rücklastschriften, Aufladungen in Fremdwährungen, Mahnungen oder Anforderungen von Ersatzstickern entstehen Kosten für den Kunden (210). Allerdings können dem Kunden, bei Nutzung der Prepaid-Variante, Zinszahlungen entgehen, weil das Geld bis zur Ausgabe auf dem mpass-Konto liegt und dort nicht verzinst wird. Somit können aus Sicht des Kunden vier von fünf Punkten vergeben werden.

Aus Sicht des Händlers sieht die Kostensituation dagegen etwas differenzierter aus. Um mpass am POS akzeptieren zu können, ist die Akzeptanz von MasterCard PayPass notwendig, so dass zusätzlich die hierbei anfallenden Kosten entstehen. Im Interneteinsatz gilt gleiches für die Akzeptanz der virtuellen Kreditkarte.

Anders sieht es aus, wenn mpass nativ, also die Zahlung mittels SMS-TAN, unterstützt werden soll. In diesem Fall ist eine Registrierung als Händler bei mpass erforderlich, die allein schon 49,90 € kostet. Zusätzlich entstehen pro empfangener Zahlung pauschal 0,22 €, sowie 1,9% des Umsatzes an Gebühren. Ferner finden durch die Registrierung bei mpass Compliance Prüfungen des Händlers statt, die diesem mit jeweils 29,90 € in Rechnung gestellt werden (204).

Für die Nutzung am POS sind außerdem dieselben technischen Voraussetzungen an das Bezahlterminal zu erfüllen, wie für MasterCard PayPass, so dass hierfür auch konsequenterweise dieselben Kosten für den Händler anfallen. Aus Sicht des Händlers werden für die, im Vergleich zur Kreditkartenzahlung günstigen, in Summe aber dennoch hohen Gebühren zwei von zehn Punkten angesetzt, so dass für die Kosten insgesamt sechs Punkte vergeben werden.

Komplexität für Kunden

Für den Kunden ist die Anmeldung für mpass vergleichsweise einfach. Insbesondere trifft dies auf Vertragskunden von T-Mobile, Vodafone und O2 zu, da in ihrem Fall die Daten des Vertrags übernommen werden können. Alle anderen Nutzer benötigen für die Registrierung mindestens eine deutsche Mobilfunknummer und ein Bankkonto. Erstgenannte muss in jedem Fall zu Beginn eingegeben werden. Im Anschluss sendet mpass einen Verifizierungscode für die Registrierung als SMS an diese Nummer. Dieser Code muss eingegeben werden, um mit der Anmeldung fortfahren zu können. Im nächsten Schritt werden die Adressdaten inklusive der E-Mailadresse, das Geburtsdatum, eine Bankverbindung, sowie eine Sicherheitsfrage und ein Passwort für das Kundenkonto hinterlegt.

Wirecard wird nach erfolgter Registrierung ein Konto eröffnen, die virtuelle Kreditkarte erzeugen und den NFC-Sticker an den Kunden versenden, was schon allein aufgrund des Postweges einige Zeit dauern kann.

Möchte sich der Kunde für mpass Plus anmelden, um die für die Bezahlung geltenden Limits zu erhöhen und zusätzliche Funktionen zu nutzen, müssen ein Scan der Vorder- und Rückseite des Personalausweises, sowie eine Rechnung, ein Bankauszug oder eine Steuererklärung mit jeweils lesbarem Namen und Adresse per E-Mail an mpass gesendet werden (205). Die Prüfung nimmt zwar einige Zeit in Anspruch, doch der Kunde wird nach erfolgter Prüfung über die Freischaltung von mpass Plus informiert. Die Anmeldung ist also vergleichsweise einfach, denn diese kann vollständig online erledigt werden und für die einfache Version sind erst gar keine Dokumente notwendig.

Komplizierter ist für den Kunden hingegen die Tatsache, dass mpass aus drei verschiedenen Bezahlverfahren besteht, die für den Kunden jeweils unterschiedliche Handlungsweisen erforderlich machen. Ferner werden zwei der drei Bezahlverfahren nicht als mpass gekennzeichnet, so dass der Kunde wissen muss, wie er an welcher Stelle bezahlen und welche Bezahlverfahren der Händler akzeptieren muss, um eine erfolgreiche Bezahlung über mpass zu ermöglichen.

Die technischen Voraussetzungen sind dagegen für den Kunden relativ gering, weil er lediglich ein beliebiges Mobiltelefon benötigt. Für das Jahr 2010 ermittelte das Marktforschungsunternehmen eMarketer, dass rund 62,7 Mio. Deutsche ein Mobiltelefon besitzen und es mindestens einmal pro Monat nutzen (211). Über die App, welche derzeit nur für Android und iOS angeboten wird, und das Online-Kundenkonto kann der Kunde jederzeit einen Überblick über seine Zahlungen behalten. Aufgrund der vergleichsweise unkomplizierten Anmeldung, der geringen technischen Voraussetzungen, aber der notwendigen Kenntnis der Händlerseite, werden für dieses Kriterium sieben von zehn Punkten vergeben.

Komplexität für Händler

Die Komplexität des Systems aus Sicht des Händlers entspricht am POS der von PayPass, da für die Akzeptanz im stationären Handel die Akzeptanz von PayPass vorausgesetzt wird. Für die Akzeptanz im Internet bestehen seitens des Händlers zwei Möglichkeiten: Zum einen kann er Kreditkarten akzeptieren, was dem Kunden die Möglichkeit bietet mit seiner virtuellen Kreditkarte zu zahlen. Zum anderen kann er mpass mit der Nutzung des SMS-TAN-Verfahrens unterstützen. Für ersteres gilt dieselbe Bewertung, wie für klassische Kreditkarten, für letzteres ist eine eigene Bewertung notwendig.

Soll mpass im Onlinehandel explizit unterstützt werden, ist zum einen die Registrierung als Händler notwendig und zum anderen die Integration in das Shopsystem. Für einige Systeme stehen bereits Plug-ins zur Verfügung (212) bzw. einige Payment-Service-Provider bieten mpass ebenfalls als Option an (213), so dass eine Einbindung in Onlineshops relativ einfach umzusetzen ist. Unter Berücksichtigung aller Varianten wird die Komplexität aus Sicht des Händlers mit sieben von zehn Punkten bewertet.

Alleinstellungsmerkmale

Das mpass-System bietet, gegenüber anderen Zahlungssystemen, zwei zusätzliche Funktionen. Zum einen liefert die mpass-App für Android und iOS die Möglichkeit, für Händler spezielle Rabatte und Aktionen zu präsentieren, die anderen Kunden nicht zur Verfügung gestellt werden.

Zum anderen offeriert mpass kostenfreie P2P-Geldsendungen, also die Geldübertragung von einem Nutzer zu einem anderen. Die Abrechnung erfolgt dabei entweder auf Guthabenbasis oder per Lastschrift, je nachdem, was der Kunde wünscht und mpass ihm aufgrund seiner Bonität zu-

gesteht. Für die Geld-senden-Funktion ist es jedoch in jedem Fall notwendig, dass beide Teilnehmer mpass Plus nutzen, also die zusätzliche Identifizierung durchlaufen haben. Für beide Funktionen wird jeweils ein Bonuspunkt vergeben, weil beide einen zusätzlichen Nutzen für den Kunden bringen.

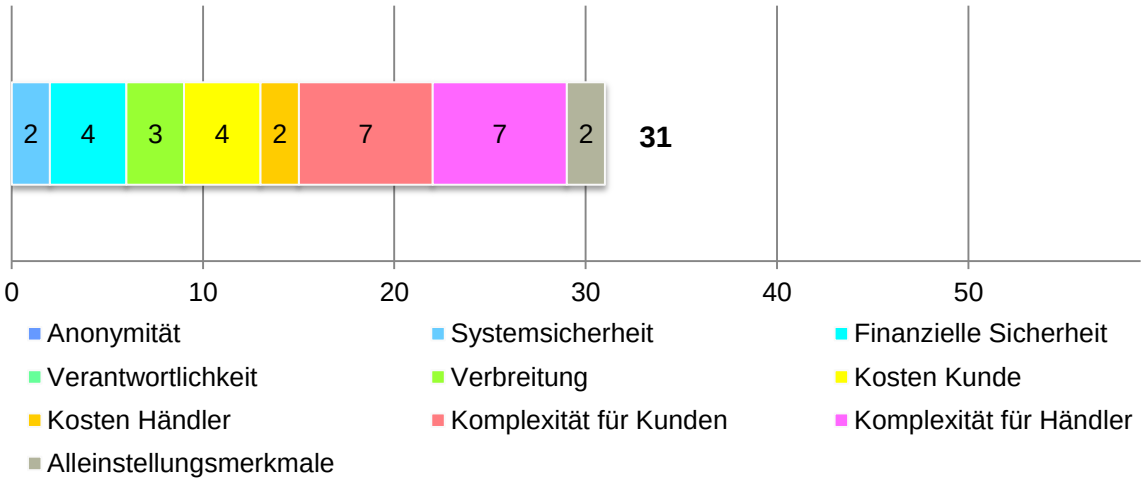

Abbildung 32: Gesamtbewertung des Zahlungssystems mpass.

3.3.1.2 Telekom MyWallet / Vodafone SmartPass / O2 Wallet / E-Plus Mobile Wallet

Da durch die Nutzung des PayPass- bzw. payWave-Systems bei allen Anbietern viele Gemeinsamkeiten mit diesen Systemen bestehen, erfolgt in diesem Kapitel nur eine Neubewertung der Kriterien, die nicht genauso zu bewerten sind, wie bei PayPass und payWave.

Anonymität

Der Bezahlvorgang selbst läuft wie bei PayPass bzw. payWave ab, wobei das Handy die Kreditkarte simuliert. Zunächst startet der Kunde die App seines Anbieters mit seiner persönlichen PIN und beginnt dann den Bezahlvorgang auf seinem Gerät, indem er die entsprechende Schaltfläche wählt. Jetzt erst wird der NFC-Chip aktiviert und reagiert auf Anfragen des Lesegeräts. Beträge bis 25,- € können ohne jegliche, weitere Authentifizierung bezahlt werden. Bei größeren Summen ist eine Autorisierung der Zahlung mittels Kreditkarten-PIN am Bezahlterminal notwendig. Im Unterschied zu PayPass oder payWave lässt sich das NFC-Element bei Nichtgebrauch also abschalten und ist bei gesperrtem Telefon sowieso inaktiv. Dies führt dazu, dass die Kreditkartendaten nicht unbedingt im Vorbeigehen ausgelesen werden können, wie es bei den NFC-Karten von girogo, Visa oder MasterCard möglich ist. Somit entspricht das Level der Anonymität dem der klassischen Kreditkartensysteme, was zur selben Bewertung von null Punkten führen muss.

Verbreitung

Die Verbreitung auf Seiten der Akzeptanzstellen entspricht der von PayPass bzw. payWave. Auf Kundenseite ist die Verbreitung allerdings deutlich geringer, weil durch die technischen Anforderungen des Systems nur wenige Kunden als Nutzer in Frage kommen. Die Telekom gibt beispielsweise an, dass MyWallet für über zwei Millionen ihrer Kunden nutzbar sei (31). Demgegenüber stehen insgesamt 39,6 Mio. Mobilfunkkunden der Telekom (214), von denen über 94% MyWallet nicht nutzen können. Alle anderen Anbieter veröffentlichen hierzu keine Zahlen, allerdings dürfte die Anzahl der Nutzer bei Vodafone bestenfalls auf demselben Niveau liegen, während die absoluten Zahlen von E-Plus und O2 deutlich niedriger liegen dürften. Die Anzahl der potentiellen Nutzer liegt damit deutlich unter acht Millionen.

Für die Bewertung spielt die Verbreitung auf Kundenseite allerdings keine große Rolle, da der Anreiz für Händler zur Implementation gegeben ist. Auf Seite der Händler sind nur die Voraussetzungen von PayPass bzw. payWave zu erfüllen und dadurch können alle Kunden erreicht werden, die Systeme verwenden, welche auf PayPass und payWave basieren. Dementsprechend wird die Bewertung von PayPass bzw. payWave bezüglich dieses Kriteriums mit zwei von fünf möglichen Punkten übernommen.

Kosten

Die Kosten für den Kunden unterscheiden sich bei allen Systemen. Während Vodafone, O2 und E-Plus ihre App kostenlos anbieten, ist diese bei der Telekom nur bis Ende 2015 kostenfrei. Danach wird eine Monatsgebühr in Höhe von 0,99 € berechnet (215).

Grundsätzlich sind bei MyWallet Einrichtungsgebühren allein dann fällig, wenn die Variante mit NFC-Sticker genutzt werden soll. Weitere Gebühren entstehen nur, falls Aufladungen oder Zahlungen in fremde Währungen erfolgen, die Aufladung über eine Kreditkarte getätigt, Geld am Automaten abgehoben wird oder Probleme bei der Zahlung zu einem Ausfall oder einer Mahnungen führen (216)

Vodafone verlangt zwar keine explizite Gebühr für die App, dafür aber eine Jahresgebühr in Höhe von 9,90 €, falls der Umsatz des Vorjahres weniger als 600,- € beträgt. Das erste Jahr ist jedoch in jedem Fall kostenfrei. Zusätzlich fallen Gebühren bei der Aufladung von Fremdwährungen, dem Geldabheben am Automaten und bei P2P-Zahlungen an (217).

O2 verfolgt die Strategie das Wallet künftig über mpass anzubieten, wodurch dieselben Gebühren, wie bei mpass anfallen würden.

Bei E-Plus ist die Nutzung der App grundsätzlich kostenfrei. Allerdings wird eine WalletCard[33] benötigt, die bei allen anderen Anbietern direkt mit ausgegeben wird. Für die Ausgabe der Wal-

[33] Virtuelle Kreditkarte, die in dem mobilen Wallet gespeichert wird.

letCard ist Wirecard Card Solutions Ltd. verantwortlich (218), die die entsprechenden Gebühren berechnet. In diesem Zusammenhang ist die Ausgabe der virtuellen Kreditkarte, die auf der SIM-Karte hinterlegt wird, kostenlos. Lediglich eine physische Karte wird dem Kunden in Rechnung gestellt. Ähnlich den anderen Anbietern, fallen zusätzliche Gebühren auch hier an, wenn die Aufladung in Fremdwährungen erfolgt, eine Rücklastschrift veranlasst oder als Methode zur Einzahlung die Sofortüberweisung gewählt wird. Ferner entstehen die typischen Gebühren, wenn Mahnungen erfolgen oder Geld bar abgehoben wird. Als einziges System werden bei E-Plus für die WalletCard monatlich Gebühren fällig, wenn diese zwölf Monate lang nicht benutzt wurde (219).

Zusammengefasst sind die Gebühren, die die Kunden zahlen, also recht ähnlich zu denen, die bei normalen Kreditkarten anfallen. Die Kosten, die der Händler zu tragen hat, entsprechen den Kosten, die er bei PayPass bzw. payWave trägt. Somit wird die entsprechende Wertung an dieser Stelle übernommen. Insgesamt werden zwei Punkte für die Kosten aus Sicht des Kunden und ein Punkt für die Kosten aus Sicht des Händlers, so dass in Summe drei Punkte für dieses Kriterium vergeben werden.

Komplexität für Kunden

Die Komplexität aus Sicht des Kunden ist vergleichsweise hoch, da schon die technischen Anforderungen nicht gering sind. In jedem Fall wird ein ausgewähltes, NFC-taugliches Smartphone benötigt, welches direkt über den Anbieter des Systems bezogen wurde, was wiederum nicht allen Nutzern klar ist. Auch der Begriff NFC-SIM irritiert einige Anwender, weil er suggeriert, die SIM-Karte würde einen NFC-Chip enthalten, so dass die Zahlung mit jedem Smartphone möglich wäre. So haben schon Kunden versucht, MyWallet mit einem iPhone zu nutzen, doch scheiterten sie an der Bezahlung, was letztlich zu Unzufriedenheit führte (220).

Außerdem ist die Registrierung für die Systeme nicht unbedingt einfach, da beispielsweise bei O2 mehrere Schritte durchlaufen werden müssen, die zwei Anmeldungen umfasst – zum einen bei O2 direkt, um eine NFC-SIM zu erhalten, und zum anderen bei mpass, um die Kreditkarte zu erhalten. Abbildung 33 stellt den Anmeldeprozess mit allen Schritten dar.

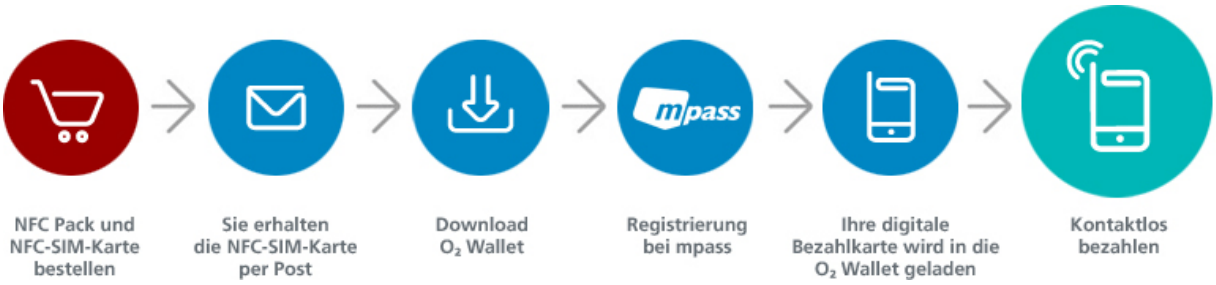

Abbildung 33: Schritte der Anmeldung für O2-Wallet.

Dafür ist die Bezahlung, nach dem recht komplexen Anmeldevorgang, vergleichsweise einfach, weil nur die App gestartet und das Smartphone an das Bezahlterminal gehalten werden muss. Wobei auch hier die schon bei PayPass und payWave geäußerte Kritik gilt, dass der Kunde sich an diesen ungewohnten Vorgang gewöhnen muss und jedes Bezahlterminal das NFC-Lesegerät an unterschiedlichen Stellen eingebaut hat. Aufgrund der genannten Argumente werden für dieses Kriterium drei von zehn Punkten vergeben, da der Bezahlvorgang nach einer Eingewöhnungsphase vergleichsweise schnell ist, die Anmeldung und Einrichtung aber lange dauert und kompliziert ist.

Alleinstellungsmerkmale

Neben den klassischen Bezahlfunktionen bieten Vodafone und E-Plus die Möglichkeit P2P-Zahlungen durchzuführen. Die Beschränkung ist, dass der Empfänger ebenfalls für das System registriert sein muss. Weitere Voraussetzungen, wie bei mpass, müssen sowohl bei Vodafone, als auch bei E-Plus erfüllt sein.

Ferner planen alle Anbieter, falls sie es derzeit nicht sogar schon selbst anbieten, weitere Karten, wie ADAC Mitgliedskarten, auf der NFC-SIM zu hinterlegen und über die App abrufbar zu machen. Auch die Integration von Rabattcoupons, Kundenkarten und Tickets in die Systeme ist vorgesehen. Bei MyWallet sind beispielsweise bereits Aktionen und Rabattcoupons von Edeka in die App integriert (221). O2 ermöglicht über eine Kooperation mit der Dortmunder Volksbank eine Einbindung der von der Volksbank ausgegebenen ClassicCard Mobile in die O2 Wallet (222). Weitere Banken sollen diesem Beispiel folgen. E-Plus hat bisher den ADAC als Kooperationspartner gewonnen, kündigt aber weitere Kooperationen an, um beispielsweise Kino- und ÖPNV-Tickets zu speichern (218). Für beide Zusatzfunktionen wird jeweils ein weiterer Punkt vergeben, so dass in Summe zwei Punkte für die Alleinstellungsmerkmale vergeben werden.

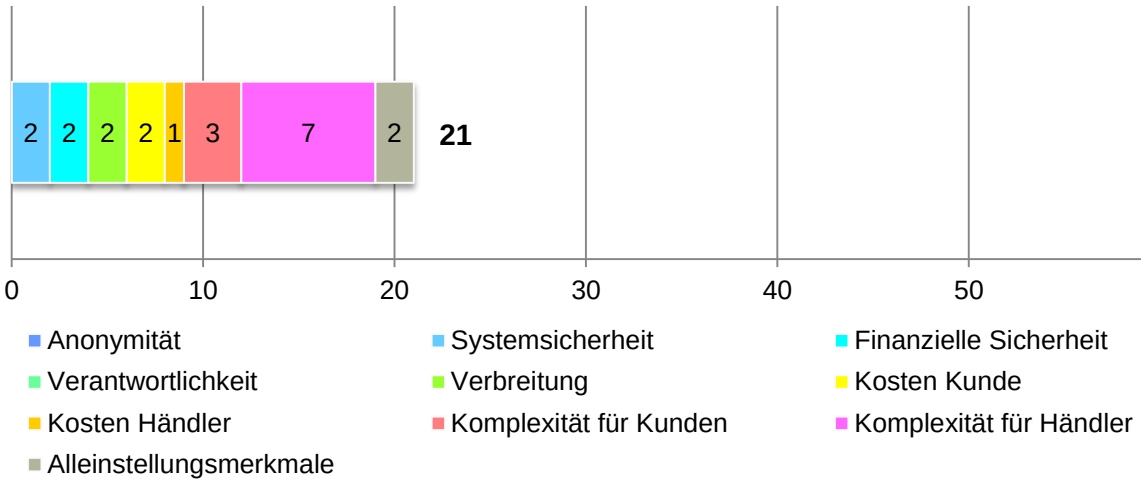

Abbildung 34: Gesamtbewertung der Zahlungssysteme Telekom Telekom MyWallet / Vodafone SmartPass / O2 Wallet / E-Plus Mobile Wallet.

3.3.2 QR-Code basierte Systeme

Dieses Kapitel umfasst die Systeme, die QR-Codes zur Abwicklung der Zahlung verwenden. Der Einsatz dieser Technologie wurde durch die Anbieter der Systeme gewählt, da QR-Codes vielen Nutzern bekannt sind und sie nur geringe Anforderungen an die Hardware des Nutzers stellen.

3.3.2.1 Yapital

Im Folgenden wird das System Yapitel bewertet. In Kapitel *1.3.2.1 Yapital* erfolgte die Beschreibung des Zahlungssystems, auf der die Bewertung basiert.

Anonymität

Bezahlungen über das System werden in jedem Fall über einen Yapital-Server abgewickelt, der zwischen Kunde und Händler vermittelt. Yapital erfährt somit in Echtzeit, wer welche Transaktionen mit wem tätigt. Da sowohl Händler als auch Kunden bei Yapital registriert sein müssen, kennt Yapital die Identitäten beider Teilnehmer, so dass keiner der beiden anonym ist. Weitere Instanzen sind in vielen Fällen nicht beteiligt, es sei denn, der Händler nutzt einen Payment Service Provider zur Abwicklung der Zahlung.

Die Datenschutzbestimmungen von Yapital sehen neben den üblichen Zusagen, Informationen für Behörden zu Strafverfolgungszwecken preiszugeben auch vor, dass Informationen denen zugänglich gemacht werden, mit denen der Kunde in einer „geschäftlichen Beziehung“ (50) steht. Außerdem erhalten die Händler, bei denen eingekauft und Yapital als Zahlungsmittel verwendet wurde, durch Yapital den Namen des Kunden. Zusätzlich stimmt der Kunde durch die Datenschutzbestimmungen zu, dass die erhobenen Daten für statistische Auswertungen verwendet werden dürfen (50, S. 5).

Die Server, auf denen Yapital Daten verarbeitet, stehen den Datenschutzbestimmungen zufolge, allesamt in Europa, genauer in Luxemburg. Sie unterliegen daher dem europäischen bzw. luxemburgischen Datenschutzrecht, so dass zumindest die, im Vergleich zu amerikanischen Systemen, strengeren Datenschutzregeln gelten und der Zugriff für amerikanische Behörden nicht möglich ist.

Aufgrund der Tatsache, dass es sich noch um ein recht junges und unbekanntes System handelt, sind bisher keinerlei Angriffe auf das System bekannt geworden, bei denen Daten entwendet wurden. Insgesamt wird dieses Kriterium aus den vorherstehenden Gründen mit drei von zehn Punkten bewertet, wobei sich positiv auswirkt, dass nur wenige Stellen involviert sind und es sich um ein rein europäisches System handelt.

Systemsicherheit

Die Sicherheit des Systems liegt in der Zentralisierung, denn für jede Aktion, die durchgeführt werden soll, ist der Kontakt mit den Yapital-Servern nötig. Dies führt dazu, dass die Manipulation von Zahlungen für einen Angreifer schwierig ist, da er zum einen die Verbindung zwischen dem Händler und Yapital manipulieren müsste, um die Transaktion zu verändern. Zum anderen wäre ebenfalls die Manipulation der Verbindung zwischen dem Kunden und Yapital notwendig, die in der Regel über eine andere Internetverbindung erfolgt. Denn dem Kunden müsste die vermeintlich richtige Transaktion dargestellt werden, weil dieser die Transaktionsdaten auf seinem Gerät angezeigt bekommt und diese bestätigen muss. Beide Verbindungen sind dabei über HTTPS mit einer Schlüssellänge von 2048 Bit gesichert, was den Angriff zusätzlich erschwert. Würde dem Angreifer all dies gelingen, erhält der Kunde aber in jedem Fall eine E-Mail, in der die Transaktionsdaten noch einmal dargestellt werden (223).

Weiterhin beruht die Sicherheit des Kundenkontos auf der Wahl des Passwortes. Gelangt es in die Hände eines Angreifers, kann dieser mit dem Kundenkonto Einkäufe tätigen oder Geld auf andere Yapital-Konten übertragen. Aus diesem Grund hat Yapital für die Wahl des Passwortes vergleichsweise strenge Regeln, wobei die Mindestlänge des Passwortes mit acht Zeichen noch unterhalb der Empfehlung des Instituts für Internetsicherheit von mindestens zehn Zeichen liegt (224, 225). Um diese Art von Missbrauch rasch erkennen zu können, versendet Yapital nach jeder erfolgten Zahlung eine E-Mail an den Kunden, in der die Transaktionsdaten und die kostenfreie Rufnummer des Supports genannt werden. Auf diese Weise soll der Kunde den Missbrauch schnell melden können, um weitere unberechtigte Zahlungen zu verhindern.

Zur Einbindung neuer Smartphones, die für die Zahlung verwendet werden können, ist die Registrierung desselben im Kundenkonto notwendig. Hierzu wird eine TAN per SMS an die hinterlegte Handynummer gesendet, die zur Vollendung des Vorgangs eingeben werden muss. Dadurch ist es Angreifern, selbst bei Kenntnis des Kennwortes, nicht möglich, weitere Geräte zu hinterlegen und diese für die Zahlung am POS zu nutzen. In Summe werden für die Sicherheit sieben von zehn Punkte vergeben, da die Sicherheit zwar relativ hoch ist und bisher auch kein Missbrauch bekannt wurde, diese allerdings weiter erhöht werden könnte, in dem die verwendete Verschlüsslung bei der Kommunikation längere Schlüssel verwendet, der Kunde mindestens zehnstellige Passwörter nutzen muss und eine Zwei-Faktor-Authentifizierung für den Login angeboten würde.

Finanzielle Sicherheit

Yapital bietet, weil alle Zahlungen immer direkt über die eigenen Systeme abgewickelt werden, Gut- und Lastschriften in Echtzeit, so dass Händler und Kunden immer einen aktuellen Überblick über ihre Transaktionen in ihrem Kundenkonto einsehen können. Infolge, dass Zahlungen sofort abgewickelt werden und nicht rückgängig gemacht werden können, besteht für den Händler eine

Zahlungsgarantie, sobald sie die Bestätigung von Yapital erhalten, dass die Zahlung durch den Kunden bestätigt wurde (226). Wie erwähnt sind Rückbuchungen zwar nicht möglich, allerdings unterstützt der Yapital-Support den Kunden schnell und unkompliziert, falls bei einer Zahlung etwas schiefläuft. Außerdem vermittelt er zwischen Kunden und Händlern, um eine Lösung herbeizuführen.

Durch die Zertifizierung als europäisches E-Geld-Institut untersteht Yapital der Aufsicht durch die luxemburgische Finanzaufsichtsbehörde (227). Sie kontrolliert und reglementiert Yapital, so dass davon ausgegangen werden darf, dass die notwendigen Sicherheitsstandards denen der etablierten Finanzindustrie und Banken in etwa entsprechen. Bisher ist nicht bekannt, ob Kunden oder Händlern finanzielle Schäden durch die Nutzung von Yapital entstanden sind, so dass dieses Kriterium aus allen Erwägungen heraus mit acht von zehn Punkten bewertet wird.

Verantwortlichkeit

Allein verantwortlich für den Betrieb ist die Yapital Financial AG aus Luxemburg, die ein hundertprozentiges Tochterunternehmen der deutschen Otto Group ist. Als solches wird das Ziel einer hohen Verbreitung und kostengünstigen Abwicklung von Zahlungen für Unternehmen der Otto Group verfolgt, so dass die Otto Group alle Elemente des Shoppings aus einer Hand anbieten kann - beginnend bei den eigenen Läden und endend mit dem eigenen Lieferunternehmen. Durch die zentralisierte Ausgestaltung des Yapital-Systems entstehen weitreichende Eingriffs- und Kontrollmöglichkeiten. Da sowohl Händler als auch Kunden ein entsprechendes Konto bei Yapital benötigen, um Zahlungen zu tätigen, können einzelne Teilnehmer sehr leicht von dem System ausgeschlossen werden. Jede Zahlung wird über die Yapital-Systeme abgewickelt, so dass theoretisch einzelne Zahlungen verhindert werden könnten. Beides scheint bisher nicht vorgekommen zu sein und würde dem Ziel, eine hohe Verbreitung zu erreichen, zuwiderlaufen, da potentielle Kunden verschreckt würden. Daher können für diesen Aspekt vier von fünf möglichen Punkten vergeben werden.

Verbreitung

Die Verbreitung von Yapital ist derzeit noch recht übersichtlich. Als junges, europäisches Unternehmen mit deutscher Mutter befinden sich die meisten der rund 4.260 Akzeptanzstellen (Stand Dezember 2014) im stationären Handel in Deutschland. Als Partner wurden, neben einigen bekannten Händlern wie REWE, Douglas oder Gravis, auch einige Unternehmen der Otto Group, wie Sportscheck und Görtz, sowie kleinere Läden gewonnen (228–231). Im Onlinehandel ist die Verbreitung von Yapital ebenfalls noch sehr überschaubar, wenngleich auch hier einige der oben genannten Unternehmen und weitere Onlineshops, wie Rakuten oder Otto.de, Yapital mittlerweile als Bezahloption anbieten (228).

Um Kunden trotz der geringen, eigenen Verbreitung die Möglichkeit zu bieten, mit Yapital zu bezahlen, stellt Yapital seinen Kunden eine kostenfreie MasterCard-Kreditkarte zur Verfügung, mit denen an allen MasterCard-Akzeptanzstellen bezahlt werden kann. Vorrausetzung hierfür ist jedoch ein entsprechendes Guthaben auf dem Yapital-Konto, da es sich um eine Prepaid-Kreditkarte handelt (225). Zudem ist Yapital Partnerschaften mit Herstellern von Kassensystemen und Bezahlterminals, sowie Payment Service Providern eingegangen, um die Verbreitung des eigenen Systems künftig weiter zu steigern. Diese sollen eine einfache Integration in Onlineshops und am POS ermöglichen (232–236).

Weiterhin strebt Yapital Partnerschaften mit Banken an, damit dem Kunden die direkte Integration in sein bekanntes Onlinebanking angeboten werden kann und die Registrierung erleichtert wird, denn alle Daten, die für die Registrierung verlangt werden, sind der Bank bereits bekannt. Für die Bank würde sich der Mehrwert ergeben, dem Kunden eine neue Dienstleistung anbieten zu können und damit erster Ansprechpartner für Finanzdienste zu bleiben (237). In Summe werden, aufgrund der derzeit noch geringen, eigenen Verbreitung, aber der Möglichkeit, trotzdem mit der MasterCard-Kreditkarte zu bezahlen, und der Aussicht auf zukünftige, größere Verbreitung durch die zahlreichen Partnerschaften, drei von fünf Punkten vergeben.

Kosten

Für den Kunden ist die Nutzung von Yapital in den meisten Fällen kostenlos: Das Einrichten des Kundenkontos, das Einsehen elektronsicher Kontoauszüge, sowie das Aufladen bzw. die Lastschriften von Bankkonten sind ebenso kostenfrei, wie das Bezahlen oder Geld senden und empfangen. Für die Aufladung des Kontos von Kreditkarten werden dem Kunden 2% des aufzuladenden Betrags abgezogen. Ähnlich sind Rückbelastungen und Auszahlungen von Guthaben kostenpflichtig (238). Zusätzliche Kosten für extra benötigte Hard- und Software fallen nicht an, so dass für Yapital, im Falle einer Nichtnutzung nach der Anmeldung, im Allgemeinen keine Kosten entstehen. Gebühren entstehen also nur in Sonderfällen, während die Nutzung und Registrierung in den meisten Fällen kostenfrei ist, so dass aus Sicht des Kunden vier von fünf Punkten vergeben werden.

Aus Sicht des Händlers fallen schon deutlich mehr Gebühren an, wobei hier zwischen Zahlungen am POS und Online-Zahlungen unterschieden wird. Für E-Commerce-Transaktionen mit einem Umfang von bis zu fünf Euro fallen Gebühren in Höhe von 0,09 € sowie 9% der Transaktionshöhe an. Bei einem Transaktionsvolumen von mehr als fünf Euro sinkt der prozentuale Anteil auf 1,8 %. Dafür steigt der fixe Anteil auf 0,30 € pro Transaktion. Bei Zahlungen am POS entstehen in jedem Fall nur Gebühren in Höhe von 2,6 % der Transaktion. Diese Gebühren werden direkt von der ausgezahlten Summe einbehalten. Zusätzlich fallen Gebühren bei Auszahlungen auf ein Bankkonto, sowie bei fehlgeschlagenen Lastschriften an. Werden außerdem zu dem kosten-

freien, elektronischen Kontoauszug papierbehaftete Belege benötigt, entsteht für diese eine Bearbeitungsgebühr von 15,- € (239).

Die Kosten sind damit aus Händlersicht nicht unerheblich, zumal bei Beauftragung eines Payment Service Providers noch weitere Gebühren – abhängig von den ausgehandelten Konditionen – anfallen. Auch die benötigte Hardware am POS muss in die Betrachtung mit aufgenommen werden. Die Kosten hierfür fallen jedoch nur einmalig an und die Bezahlterminals können genauso für andere Bezahlarten genutzt werden. Unter Umständen kann das bereits vorhandene Bezahlterminal, nach einem Update der Software, weiterhin genutzt werden.

Günstig ist hingegen, dass keine fixen Gebühren, wie Anmeldegebühren oder Monatsbeträge, existieren, die entstünden, wenn keine Transaktion über Yapital abgewickelt würde. Außerdem ist die Gebührenordnung einfach zu durchschauen, so dass die konkreten Kosten im Vorhinein gut eingeschätzt werden können. Somit werden aus Händlersicht vier von zehn Punkten vergeben. Zusammen mit den Punkten aus der Kundensicht werden für dieses Kriterium insgesamt acht Punkte vergeben.

Komplexität für Kunden

Die Komplexität für den Kunden ist zu Beginn relativ hoch, weil für die Anmeldung und Ersteinrichtung verhältnismäßig viele Schritte notwendig sind. Dafür benötigt der Kunde lediglich eine Mobilfunknummer, aber keine zusätzlichen Dokumente. Die Registrierung verläuft relativ unspektakulär. Auch die Überprüfung der Handynummer durch eine SMS-TAN dürfte den meisten Nutzern keine Schwierigkeit bereiten. Jedoch werden allerlei Daten, wie Anmelde- und Kontaktdaten, abgefragt.

Nach der Registrierung sind die Ersteinrichtung des Smartphones und die Verknüpfung mit dem eigenen Bankkonto bzw. der eigenen Kreditkarte erforderlich. Zunächst muss die App auf das eigene Smartphone geladen werden. Danach erfolgt die Anmeldung mit den Zugangsdaten des Kundenkontos oder der Scan eines QR-Codes, der im Kundenkonto angezeigt wird. Nach Abschluss dieses Vorgangs muss eine vierstellige PIN festgelegt werden, die nur für die Yapital-Nutzung auf diesem Gerät verwendet wird. Außerdem muss eine Zahlungsquelle im Yapital-Kundenkonto hinterlegt werden. Diese kann entweder ein Bankkonto oder eine Kreditkarte von Visa bzw. MasterCard sein, wobei der Kunde selbst festlegen kann, ob er die automatische Lastschrift wünscht oder sein Yapital-Konto lieber manuell laden möchte.

Der Bezahlvorgang an sich läuft über alle Kanäle gleich ab: Es muss ein QR-Code mit der Yapital-App gescannt werden. QR-Codes sind dabei, laut einer Umfrage des Markforschungsunternehmens SKOPOS, 99% aller Deutschen bekannt (240), so dass die Bezahlung für die meisten Menschen kein Problem darstellen sollte. Der Nutzer muss sich zwar einmal an diese andere Art

des Bezahlens gewöhnen und den Bezahlvorgang erlernen, kann dieses erlernte Verhalten dann aber bei jeder Zahlung über Yapital wieder anwenden.

Wie in Kapitel *1.3.2.1 Yapital* beschrieben, besteht der Bezahlvorgang dabei aus fünf Schritten, bei denen Daten zwischen dem Händler, Yapital und dem Kunden ausgetauscht werden. Der Nutzer benötigt für die Bezahlung also zwingend eine Internetverbindung mit seinem Smartphone, was an einigen POS durchaus schwierig werden kann. In diesem Fall ist eine Zahlung mittels Smartphone nicht möglich. Yapital hat für dieses Problem jedoch zusammen mit POSPartner, einem Hersteller von Kassensystemen, eine Lösung entwickelt, bei der das Smartphone des Nutzers über Bluetooth Low Energy direkt mit der Kasse kommuniziert, was Zahlungen auch offline ermöglichen soll (235). Aufgrund der geringen Hardware-Voraussetzungen, der Kunde benötigt lediglich ein Smartphone mit Kamera, und dem einfachen Bezahlvorgang, werden für dieses Kriterium sieben von zehn Punkten vergeben. Abzüge ergeben sich durch die relativ lange Ersteinrichtung.

Komplexität für Händler

Wie schon für Kunden, ist auch als Händler vor der Nutzung von Yapital eine Registrierung notwendig. Diese läuft allerdings nicht online ab. Stattdessen ist der Händlervertrag auszufüllen, in dem einige Informationen über das Unternehmen und die dahinterstehenden Personen abgefragt werden (241). Zusammen mit einigen Dokumenten, wie einem Handelsregisterauszug oder einer Kopie des Gewerbescheins, wird dieser an Yapital zur Prüfung und Eröffnung des Kontos gesendet. Die Registrierung dauert somit mindestens einige Tage.

Eine Integration in bestehende E-Commerce-Systeme dürfte sich in vielen Fällen relativ simpel gestalten, da zahlreiche Plug-ins für gängige Shop-Systeme bereits existieren und eingekauft werden können (242). Am POS ist die Einbindung in bestehende Systeme ebenfalls verhältnismäßig einfach, weil Yapital Partnerschaften mit verschiedenen Anbietern dieser Systeme, Payment Service Providern und *Acquirern* eingegangen ist (243). Es wird lediglich eines der unterstützten Bezahlterminals, technisch wird mindestens ein Display vorausgesetzt, benötigt. Komplizierter wird es lediglich, wenn die Mobilfunkabdeckung am POS nicht gegeben ist. Die Integration, der hierfür entwickelten BLE-Lösung, dürfte sich aktuell aufgrund mangelnder Erfahrung noch umständlich gestalten.

Der eigentliche Bezahlvorgang ist unterschiedlich schnell. Die Geschwindigkeit hängt dabei zum einen von der Mobilfunkverbindung des Kunden und zum anderen von der Vorbereitung des Kunden ab. Dieser müsste, um den Bezahlvorgang zu beschleunigen, sein Smartphone bereits vor dem Bezahlen entsperren und die Yapital-App starten. Bei guter Mobilfunkverbindung, dauert der Bezahlvorgang nur wenige Sekunden. Andernfalls kann sich dieser um einige Zeit verzögern. Sobald sich die Kunden an diesen Vorgang gewöhnt haben, dürften Zahlungen aber relativ schnell abgewickelt werden können.

Eine Einführung des Kassenpersonals ist mit der Einführung auf jeden Fall erforderlich, da ihnen bekannt sein muss, wie Zahlungen über Yapital initiiert und abgewickelt werden, weil diese von den bekannten Bezahlvorgängen abweichen. Ist dies nicht der Fall, muss ein weiterer Mitarbeiter, i. d. R. die Filialleitung, herbeigerufen werden, um die Zahlung zu initiieren. In Summe werden aus den genannten Gründen für dieses Kriterium sieben von zehn Punkten vergeben.

Alleinstellungsmerkmale

Neben den erläuterten Bezahlfunktionen bietet Yapital einige weitere Funktionen. Es besteht die kostenfreie Möglichkeit von Geldsendungen an andere Yapital-Nutzer. Hierfür wird lediglich die bei Yapital hinterlegte E-Mailadresse des Zahlungsempfängers benötigt. Ein weiteres Alleinstellungsmerkmal von Yapital gegenüber anderen Systemen ergibt sich aus einer Kooperation mit AXA Assistance Deutschland GmbH, durch die alle mit Yapital bezahlten Waren 30 Tage lang kostenfrei gegen Diebstahl oder versehentliche Beschädigung versichert sind. Ferner wird durch die integrierte Versicherung der Fall abgedeckt, dass der Händler nicht oder die falsche Ware liefert (244).

Zusätzlich lässt sich Yapital für den Händler mit der Funktion Scan2Order als Marketinginstrument nutzen. Hierzu bietet Yapital die Möglichkeit, QR-Codes zu einzelnen Produkten zu generieren. Diese können in der Werbung oder in Katalogen abgedruckt werden. Scannt der Kunde einen dieser Codes mit der Yapital-App, hat er die Möglichkeit, den beworbenen Artikel direkt zu bestellen. Yapital übermittelt in diesem Fall die Bestellung und die Lieferdaten an den Händler, ohne dass der Kunde die Daten händisch eingeben muss. Bei Artikeln, bei denen der Kunde beispielsweise eine Farbe oder eine Größe auswählen kann, hinterlegt der Händ-

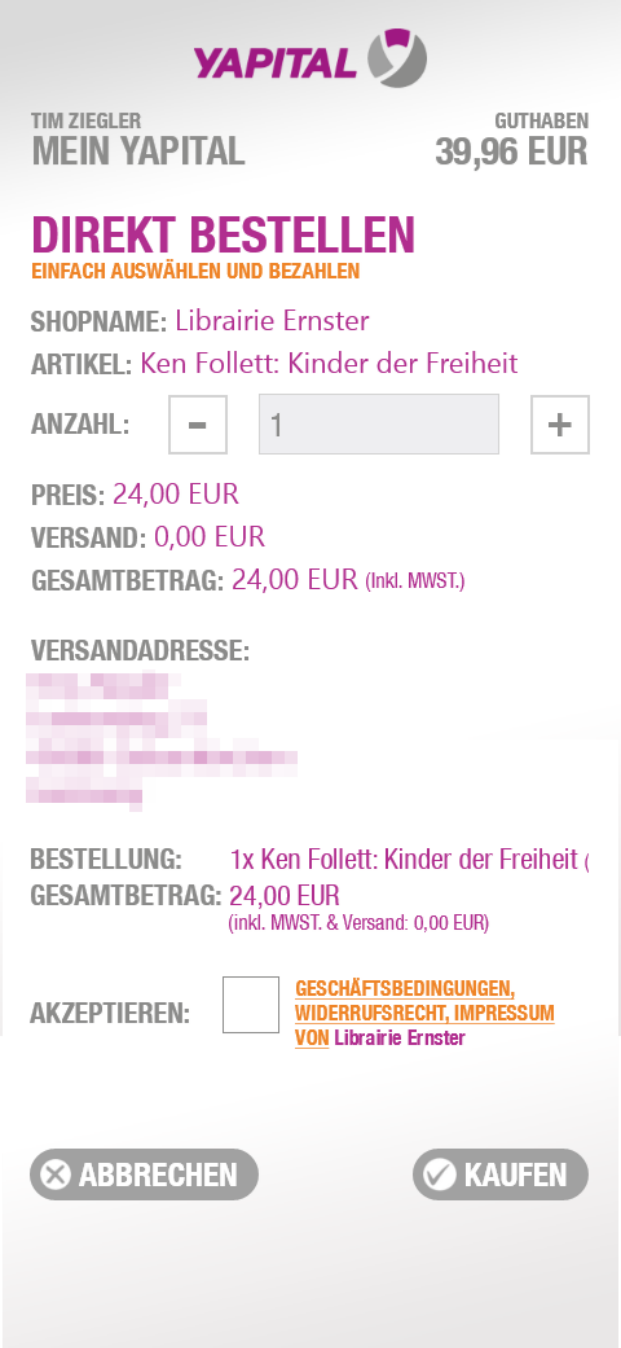

Abbildung 35: Screenshot der Yapital-App nach dem Scannen eines "Scan2Order"-QR-Codes.

ler alle Optionen bei Yapital, so dass der Kunde diese in der App festlegen muss (245). Angekündigt ist außerdem eine Integration von Couponing-Modellen (246). Für alle diese Funktionen wird jeweils ein Punkt zugesprochen, so dass für die Alleinstellungsmerkmale in Summe vier Punkte an Yapital vergeben werden.

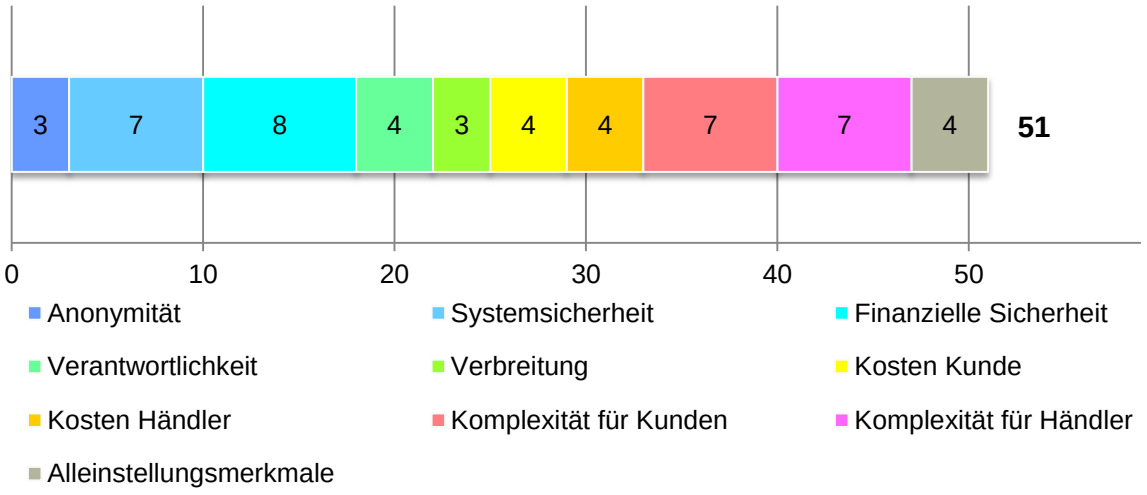

Abbildung 36: Gesamtbewertung des Zahlungssystems Yapital.

3.3.2.2 PAYMEY

Ein weiteres System, das auf QR-Codes für die Zahlungsabwicklung setzt, ist PAYMEY. Dieses wurde in Kapitel *1.3.2.2 PAYMEY* beschrieben.

Anonymität

Im Unterschied zu anderen mobilen Zahlungssystemen bezeichnet PAYMEY sich selbst als „erste Mobile Payment App, die ohne Austausch persönlicher, sensibler Daten auskommt und gleichzeitig Offline-Funktionalität bietet“ (247). Für die Zahlung am POS generiert die PAYMEY-App einen Barcode, der durch den Händler eingelesen wird. Dieser besteht aus einem zufällig aus der Benutzerkennung ausgewähltem Teil und dem Transaktionscode. Die Berechnung des Barcodes erfolgt über ein, durch PAYMEY patentiertes Verfahren, welches es dem Anbieter ermöglicht, die Transaktion einem jeweiligen Kunden zuzuordnen und entsprechend abzurechnen. Im Falle einer Offline-Zahlung wird, noch während der Kunde online ist, ein Satz Transaktionsnummer generiert, die der Kunde zu einem späteren Zeitpunkt verwenden kann (52). Der Händler erfährt also keinerlei Daten des Kunden, noch nicht einmal eine eindeutige Kundennummer, über die Kunden eindeutig identifiziert werden könnten.

Somit wäre der Kunde dem Händler gegenüber eigentlich anonym, wenn PAYMEY dem Händler in seiner Transaktionsübersicht nicht den Namen, die E-Mail-Adresse, das Datum der Anmeldung, die Anzahl der erhaltenen Zahlungen, die Information, ob der Kunde über ein verifiziertes

Bankkonto verfügt, sowie die Skype- und Telefonnummer, falls der Kunde diese bei PAYMEY hinterlegt hat, darstellen würde (53). Die ursprüngliche Anonymität ist damit also nicht mehr gegeben. PAYMEY gegenüber ist der Kunde von vornherein nicht anonym, da der Dienst Kunden- und Transaktionsdaten miteinander verbinden muss, um die Abrechnung durchführen zu können.

Im Falle der Nutzung des QR-Code-Shoppings, bei dem der Kunde über den Scan eines QR-Codes direkt eine Ware bestellen kann, übermittelt PAYMEY die Bestellung an den Anbieter zusammen mit der bei PAYMEY hinterlegten Adresse des Kunden. Dies ist notwendig, um den bestellten Artikel versenden zu können, trägt aber nicht dazu bei, das Versprechen einer anonymen Bezahl-App einzuhalten.

In Summe lässt sich also festhalten, dass aus dem Werbeversprechen, ohne den Austausch sensibler Daten auszukommen, letztendlich nicht viel übrig bleibt. Die einzigen nicht übermittelten Daten sind Kontodaten oder andere Daten, die zu klassischen Zahlungssystemen gehören. Zu Gute halten könnte man PAYMEY, dass es sich um ein rein deutsches Unternehmen handelt und somit den strengen deutschen Datenschutzrichtlinien unterliegt. Allerdings ist in den Nutzungsbedingungen nachzulesen, dass die Verarbeitung der Daten in Irland stattfindet, womit auch dieser Pluspunkt entfällt, da somit die irischen Datenschutzbestimmungen für die Speicherung und Verarbeitung der Daten gelten (53). Aus den genannten Erwägungen heraus werden für das Kriterium der Anonymität drei von zehn Punkten vergeben.

Systemsicherheit

PAYMEY verwendet für die Zahlungen Barcodes, in denen zum einen Teile der Benutzerkennung und zum anderen eine zuvor auf dem Server generierte Transaktions-ID enthalten sind. Kennt ein Angreifer die komplette Benutzerkennung und eine noch ungenutzte Transaktions-ID, kann er diese zur Generierung eines Barcodes nutzen. Zur Nutzung der App und der damit verbundenen Barcodes authentifiziert sich der Nutzer mit einer PIN, die lokal auf dem Gerät gespeichert ist, um die Offline-Zahlung zu ermöglichen.

Auch eine Bestätigung der konkreten Transaktion auf dem Endgerät entfällt bei Zahlungen am POS, so dass es theoretisch denkbar wäre, dass Zahlungen durch einen Angreifer abgefangen und geändert werden können. Hierfür muss lediglich die Kommunikation zwischen Kassensystem und PAYMEY-Server manipuliert werden

Anders sieht es beim Einkauf im Internet aus. Hier wird ein, mit dem PAYMEY-Konto des Nutzers verknüpftes Gerät benötigt, mit dem der, durch den Onlineshop generierte QR-Code eingelesen wird. Damit der Angreifer ein neues Gerät hinzufügen kann, genügt, genau wie bei Yapital, die Kenntnis des Benutzernamens und persönlichen Kennwortes, an welches dieselben Anforderungen, wie bei Yapital, gestellt werden. Sie liegen, wie zuvor bereits erwähnt, unterhalb der Empfehlungen des Instituts für Internetsicherheit bezüglich sicherer Passwörter.

Bisher sind jedoch noch keine Angriffe auf PAYMEY bekannt geworden, was allerdings daran liegen dürfte, dass es sich um ein sehr junges System handelt, dass bisher nicht häufig eingesetzt wird. Für die Sicherheit des Systems werden fünf Punkte vergeben, wobei eine Abwertung erfolgt, da PAYMEY zum Zeitpunkt der Recherche, Ende Oktober, auf seinen Webseiten ein Zertifikat verwendete, welches bereits vor mehreren Tagen abgelaufen war, so dass mit jedem Besuch der Seite eine Sicherheitswarnung des Browsers angezeigt wurde.

Finanzielle Sicherheit

PAYMEY bietet für Händler keinerlei Zahlungsgarantie. Darüber hinaus werden Transaktionen nicht, wie bei Yapital, in Echtzeit abgewickelt, sondern verzögert, um eine Risikoprüfung des Lastschriftverfahrens durchführen zu können. Zahlungen werden, bis zum Abschluss der Prüfung, einem Reservekonto des Zahlungsempfängers gutgeschrieben und in der Transaktionsübersicht als „offen“ angezeigt. Für offene Zahlungen übernimmt PAYMEY keinerlei Garantie, dass die Zahlung tatsächlich durchgeführt wird. Nachdem eine Transaktion abgeschlossen wurde, kann diese durch PAYMEY jedoch nicht mehr rückgängig gemacht werden (248).

Bislang sind keine Schäden entstanden oder zumindest nicht bekannt geworden. Allerdings ist dies zu einem großen Teil auf die Neuheit von PAYMEY und die damit verbundene, geringe Anzahl an durchgeführten Transaktionen zurückzuführen, so dass der aktuelle Status keine Rückschlüsse auf die tatsächliche finanzielle Sicherheit zulässt. Trotz der fehlenden Zahlungsgarantie werden für dieses Kriterium sechs von zehn Punkten vergeben, weil einmal ausgeführte Zahlungen nicht mehr rückgängig gemacht werden können.

Verantwortlichkeit

PAYMEY wird verantwortet durch die PAYMEY GmbH aus Welzheim. Kooperationen bestehen mit der attentra GmbH, die die Softwareentwicklung übernimmt und Geldgeber für die PAYMEY GmbH ist, sowie der net-m privatbank 1891 AG, die die Abwicklung der Lastschriften im Auftrag der PAYMEY GmbH übernimmt und die Banklizenz liefert.

Bei PAYMEY handelt es sich um ein zentralisiertes System, da jede Zahlung mit den eigenen Systemen ausgetauscht und abgewickelt wird. Auch jede Transaktion wird direkt mit PAYMEY ausgetauscht. Selbst die Zahlungen, die beim Kunden offline erfolgen, werden durch das Kassensystem unmittelbar an PAYMEY gesendet. Somit besteht für die PAYMEY GmbH die Möglichkeit, Zahlungen zu verändern oder zu blockieren. Für letzteres sind in den AGB des Anbieters sogar Fälle genannt, in denen Zahlungen blockiert werden. Eine vollständige Liste verbotener Aktivitäten ist unter Punkt 9 der AGB einsehbar. Hierzu gehören beispielsweise das „Einsetzen eines verdeckten Stellvertreters, um Ihre eigene Identität zu verschleiern“ (248, 9j) oder die „Nutzung von PAYMEY aus einem Land, das sich nicht innerhalb des EWR befindet.“ (248, 9t). Die

attentra GmbH als Entwickler der Software hat die Möglichkeit in die Software Hintertüren einzubauen, über die sie ebenfalls Zahlungen blockieren oder umleiten könnte.

Allerdings sind keine solche Eingriffe bekannt, was aber auch daran liegen dürfte, dass es sich, wie bereits erwähnt, um ein junges System handelt, dessen Verbreitung derzeit recht gering ist. Für dieses Kriterium werden, aus den zuvor genannten Erwägungen heraus, drei der fünf möglichen Punkte vergeben.

Verbreitung

Die Verbreitung von PAYMEY ist, wie bereits mehrfach erwähnt, derzeit noch sehr eingeschränkt. Bisher wird lediglich eine iOS-App zur Verfügung gestellt. Apps für andere Systeme sind zwar angekündigt, allerdings noch nicht verfügbar, obwohl der Terminplan der letzten Crowdfunding-Finanzierungsrunde eine Veröffentlichung der Android App im ersten oder zweiten Quartal 2014 vorsah (249).

Ferner sind bisher lediglich P2P-Überweisungen zwischen PAYMEY-Nutzern möglich. Partner, die Zahlungen mittels PAYMEY akzeptieren, sind bisher nicht bekannt. Trotzdem spricht Gründer Tobias Pfütze davon, dass man sich in „fortgeschrittenen Gesprächen mit Anbietern aus dem Verlagswesen und Elektronikkonzernen (befinde)“ (51), die das Produkt Print Pay einsetzen möchten, bei dem QR-Codes auf Plakate von Produkten gedruckt und damit direkt Bestellungen ausgelöst werden können. Zudem sollen „große Geschäftskunden mit einem Umsatz > 50 Mio. Euro“ (51) von PAYMEY überzeugt werden, sodass die eigene Verbreitung rasch gesteigert wird. Für den Einsatz im Internet ist PAYMEY zwar konzipiert, jedoch fehlen auch hier noch entsprechende Partner, die das System in ihren Shop einbinden.

Als rein deutsches System plant PAYMEY zunächst nur mit einer Expansion in Deutschland und Österreich (51), so dass für die nächsten Jahre nicht mit einer internationalen Verwendungsmöglichkeit zu rechnen ist. Aktuell ist die Registrierung sogar ausschließlich auf Kunden mit Wohnsitz in Deutschland beschränkt (248). Da zum jetzigen Zeitpunkt eine Verbreitung nicht umgesetzt ist, werden für dieses Kriterium null Punkte vergeben.

Kosten

Für Kunden ist die Zahlung kostenfrei und nur das Empfangen von Zahlungen kostenpflichtig. Hierfür werden, gemäß der Gebührentabelle aus dem Anhang der AGB, 1,2% des Transaktionswertes fällig, mindestens jedoch 0,35 €. Zusätzliche Kosten entstehen nur bei Problemen mit dem Lastschriftverfahren, die beispielsweise durch unzureichende Deckung des Bankkontos zustande kommen. Weitere Kosten fallen für Kunden, laut der Gebührentabelle, nicht an (248). Aufgrund der moderaten Transaktionsgebühren werden aus Sicht des Kunden drei von fünf Punkten vergeben.

Ebenso, wie für den Kunden, ist auch für den Händler das Bezahlen kostenfrei. Kostenpflichtig ist dagegen das Empfangen von Zahlungen, wobei die Gebühren individuell durch PAYMEY berechnet werden. Als grobe Richtlinie dient die Aussage, dass Unternehmen mit einem Monatsumsatz zwischen 25.001 € und 50.000 € bei PAYMEY 1% des Transaktionswertes plus einer festen Gebühr, zahlen. Je höher der monatliche Umsatz über PAYMEY steigt, desto geringer wird der prozentuale Anteil. Zusätzliche Gebühren fallen auch hier für fehlgeschlagene Abbuchungen und Rücklastschriften an. Bei Rückabwicklungen von Zahlungen über PAYMEY werden die für die Transaktion berechneten Gebühren einbehalten und dem ursprünglichen Zahlungssender der komplette Betrag gutgeschrieben. Außerdem werden Gebühren erhoben, wenn Dokumente, beispielsweise Informationen, weshalb ein Zahlungsauftrag abgelehnt wurde, bei PAYMEY angefordert werden. Kosten für zusätzliche Hardware am POS fallen nicht an, da lediglich ein Barcode-Scanner benötigt wird, der an den meisten Kassensystemen bereits vorhanden sein dürfte.

In Summe sind die Kosten aus Sicht des Händlers damit moderat und werden mit sechs von zehn möglichen Punkten bewertet, so dass für die Kosten aus Sicht des Kunden und des Händlers zusammen neun Punkte vergeben werden.

Komplexität für Kunden

Die Nutzung von PAYMEY beginnt mit der Registrierung, die sich vergleichsweise einfach gestaltet und vollständig online abläuft. Zu Beginn müssen die üblichen Daten, wie Kontakt- und Bankdaten, angeben werden. An die mitgeteilte Mobilfunknummer wird dabei ein Code versendet, der im Laufe der Registrierung auf der Webseite eingegeben werden muss, um die Nummer zu bestätigen. Im Anschluss muss die PAYMEY-App auf einem Smartphone eingerichtet werden. Dies funktioniert, indem die App zunächst installiert wird. Beim ersten Start ist die Eingabe des PAYMEY-Benutzernamens und Passwortes notwendig, sowie die Vergabe eines PIN-Codes. Nun muss die App mit dem PAYMEY-Konto synchronisiert werden, indem auf der Webseite der Synchronisationsprozess gestartet wird. Anfangs wird ein Name für das neue Gerät angegeben, unter dem es im Benutzerkonto geführt werden soll. Im Anschluss wird ein QR-Code angezeigt, der mit Hilfe der App gescannt werden muss. Ab sofort kann PAYMEY verwendet werden, wobei die Einschränkung existiert, dass, bis zur Verifizierung des Bankkontos, lediglich ein einmaliger Bezahlvorgang von maximal 40,- € in den ersten zehn Tagen nach der Registrierung möglich ist (250, 251). Zur Verifizierung des Bankkontos wird von PAYMEY ein Betrag von 0,01 € auf das angegebene Konto überwiesen, bei der im Verwendungszweck ein Zahlencode angegeben ist. Dieser ist, wie der SMS-Code, auf der Webseite einzugeben, um die zuvor beschriebene Beschränkung aufzuheben (250). Somit ist die Registrierung relativ einfach, benötigt aber, durch die Überweisung zur Verifikation des Bankkontos, einige Werktage, ehe PAYMEY richtig nutzbar ist.

Die technischen Voraussetzungen sind vergleichbar mit jenen von Yapital. Auch PAYMEY benötigt lediglich ein Smartphone, ist derzeit allerdings auf iOS-Geräte beschränkt. Eine App für Android war für das zweite Quartal 2014 angekündigt (249), ist bis Ende Oktober allerdings noch nicht veröffentlicht worden. Eine App für Windows Phone ist bisher nur in Planung.

Das Bezahlen mit PAYMEY unterscheidet sich je nachdem, wo bezahlt werden soll. Bei Zahlungen im Internet scannt der Kunde einen QR-Code. Währenddessen muss das Smartphone mit dem Internet verbunden sein, um die Zahlung an PAYMEY zu übermitteln. Am POS benötigt der Kunde keine Internetverbindung, allerdings generiert er hier einen Barcode, der durch die Kasse des Händlers eingelesen und verarbeitet wird (252, 253). Beides sind für den Kunden neu zu erlernende Verhaltensweisen zum Bezahlen. Nach der Eingewöhnung dürften Zahlungen aber vergleichsweise zügig ablaufen, weil nur wenige Schritte erforderlich sind und nur das Kassensystem mit PAYMEY-Servern kommunizieren muss.

Positiv ist zu erwähnen, dass dem Kunden, dadurch das alle Transaktionen immer über die Systeme von PAYMEY abgewickelt werden, jederzeit eine Übersicht aller Ausgaben zur Verfügung steht. Insgesamt werden für dieses Kriterium sechs von zehn Punkten vergeben, da die Registrierung einfach und der Bezahlvorgang schnell zu erlernen ist. Auch die Hardwareanforderungen sind prinzipiell nicht hoch, weil theoretisch nur ein Smartphone mit Kamera benötigt wird. Hingegen ist die Unterstützung von Smartphone-Betriebssystemen derzeit noch stark eingeschränkt, was zu einer Abwertung führte.

Komplexität für Händler

Die Registrierung des Händlers läuft vergleichbar zur Registrierung eines Kunden ab. Zunächst wird ein Online-Formular ausgefüllt und an PAYMEY gesendet. Im Nachgang werden die Vertragsdetails, u.a. bezüglich der genauen Kosten mit PAYMEY, verhandelt, so dass die Registrierung einige Tage bis hin zu Wochen dauern wird.

Die Hardware, die Händler für die Einbindung von PAYMEY am POS benötigen, ist in der Regel bereits bei allen Händlern vorhanden, da lediglich ein Barcode gescannt werden muss. Dem Personal ist dieser Vorgang durch das Einscannen der Waren sofort vertraut. Die Einführungskosten sind also gering, weil weder neue Hardware noch eine Schulung des Personals benötigt wird. Eine Kooperation mit TCPOS soll es künftig interessierten Händlern einfacher ermöglichen, PAYMEY am POS zu integrieren (249). Letztlich muss die Kassensoftware somit nur um eine Schnittstelle zu PAYMEY erweitert werden.

Im E-Commerce benötigt der Händler lediglich eine Schnittstelle für sein System, damit Zahlungen mit PAYMEY akzeptiert werden können. Leider existiert derzeit scheinbar für noch kein Shop-System ein entsprechendes Plug-in, so dass die Einbindung von PAYMEY kompliziert wird, da die Schnittstelle selbstständig implementiert werden muss. Der Aufwand hierfür ist relativ hoch

und wird einige Wochen in Anspruch nehmen. Zahlungen lassen sich anschließend allerdings sehr schnell abwickeln. Gerade im E-Commerce kann einige Zeit gespart werden, weil PAYMEY die Möglichkeit bietet, die Kundendaten zusammen mit der Zahlung an den Händler weiterzuleiten. Der Kunde muss hierfür nur den Warenkorb füllen, den generierten QR-Code scannen und die Bestellung auf dem Smartphone bestätigen, ohne irgendwelche Daten in dem Shop zu hinterlegen (253). In Summe ist die Komplexität der Einrichtung sehr unterschiedlich: Am POS ist eine Integration durch eine reine Software-Lösung machbar, die durch PAYMEYs Kooperationspartner TCPOS begleitet wird. Im Internet wird auch lediglich eine Schnittstelle für das verwendete System benötigt, die jedoch noch selbst entwickelt werden muss. Dafür lassen sich Zahlungen im Anschluss recht zügig abwickeln. Somit werden für dieses Kriterium fünf von zehn Punkten vergeben.

Alleinstellungsmerkmale

PAYMEY bietet, neben der Bezahlfunktion, die Möglichkeit von P2P-Zahlungen, bei der der Sender einen QR-Code generiert, den der Empfänger der Zahlung mit der App scannen muss. Hierdurch sind Zahlungen über große Distanzen nicht möglich, da sich Zahlungssender und -empfänger, wie beim Austausch von Bargeld, zum Austausch der Zahlung treffen müssen.

Weiterhin bietet PAYMEY, vergleichbar mit Yapital, eine Funktion bei der Waren durch Scannen eines QR-Codes bestellt werden können. PAYMEY verantwortet hier die Übermittlung der Bestellung sowie der Lieferadresse und kümmert sich um die automatische Abwicklung der Zahlung. Gleiches wird für den Online-Einsatz geboten: Statt einer Registrierung im Onlineshop, kann PAYMEY die Lieferdaten an den Shop übermitteln und dem Kunden somit einen einfachen Bestellvorgang ermöglichen. Vorteil für den Shop-Betreiber ist, dass durch den vereinfachten Bestellvorgang vermutlich weniger Bestellungen abgebrochen werden. Jede dieser Funktionen wird mit einem Punkt bewertet, so dass für die Alleinstellungsmerkmale noch einmal zwei Punkte vergeben werden.

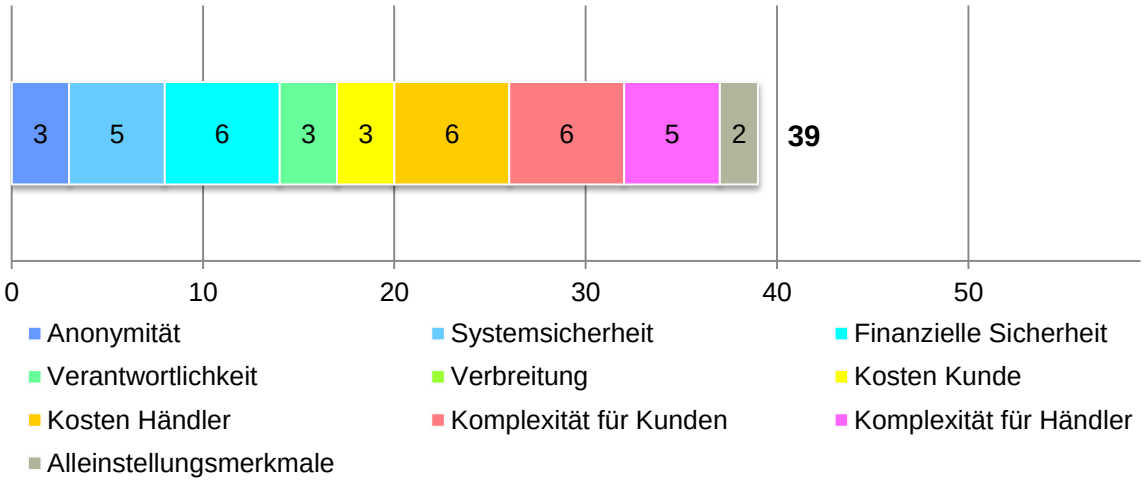

Abbildung 37: Gesamtbewertung des Zahlungssystems PAYMEY.

3.3.3 Bluetooth Low Energy basierte Systeme

Dieses Kapitel umfasst die Bewertung, der auf Bluetooth-Low-Energy-basierten Systeme. Diese ist eine Weiterentwicklung des Bluetooth-Standards, der besonders stromsparend sein soll.

3.3.3.1 PayPal Beacon

Das erste und einzige Zahlungssystem, welches in der Kategorie der Bluetooth-Low-Energy-basierten Systeme bewertet wird, ist PayPal Beacon. Dieses ist zwar noch nicht auf dem deutschen Markt verfügbar, wird aber derzeit in den Vereinigten Staaten von Amerika getestet und wird, im Erfolgsfall, auch den Weg auf den deutschen Markt finden. Auf diesem ist die Grundlage mit PayPal Check-In bereits gelegt, denn letztlich bietet PayPal Beacon nur eine Vereinfachung hiervon. Eine genau Beschreibung ist in Kapitel *1.3.3.1 PayPal Beacon* gegeben.

Anonymität

PayPal ist, als Unternehmen von eBay[34], das bevorzugte Zahlungssystem der gleichnamigen Auktionsplattform. Seit der Übernahme durch eBay ist PayPal jedoch immer mehr zu einem universellen System zum Bezahlen ausgebaut worden. Eine der neueren Ideen ist dabei PayPal Beacon, das PayPal zusammen mit PayPal Check-In nutzt, um auch an den POS vorzudringen, so dass PayPal in jeder Lebenssituation genutzt werden kann.

Bei Online-Einkäufen wird, neben den persönlichen Daten, der Warenkorb an PayPal übermittelt (255). Dies dient dazu, um dem Kunden während des Bezahlens anzeigen zu können, was Bestandteil der Rechnung ist. Wozu PayPal diese Daten noch nutzt, wird nicht verraten. Es darf jedoch davon ausgegangen werden, dass diese Informationen gespeichert und mit den restlichen Profilinformationen verknüpft werden.

Außerdem übermittelt PayPal, gemäß seiner Datenschutzbestimmungen, „Ihr[en] Name[n], Ihre E-Mail-Adresse, Ihre Skype-ID (sofern vorhanden), Ihre Telefonnummer (sofern vorhanden), das Datum der Anmeldung, die Anzahl der von verifizierten PayPal-Kunden erhaltenen Zahlungen und Informationen darüber, ob Sie über einen Zugriff auf ein verifiziertes Bankkonto verfügen, anderen PayPal-Kunden, an die Sie eine Zahlung gesendet haben, oder Absendern, die über PayPal-Services eine Zahlung an Sie senden möchten oder eine Zahlung von Ihnen anfordern[.] (…) Diese und andere Informationen können darüber hinaus auch an Dritte weitergegeben werden, wenn Sie diese Dritten zum Zugriff auf PayPal-Services nutzen.“ (256)

PayPal Beacon ist eine Erweiterung, um PayPal auch an den POS zu bringen. Die App ermöglicht dabei, den Check-In in einem Geschäft zu automatisieren, indem das Smartphone die Signa-

[34] Im September 2014 kündigte eBay Inc. an, dass PayPal ab 2015 als selbständiges, börsennotiertes Unternehmen agieren soll (254).

le des Beacons empfängt und als Auslöser nimmt. Der Kunde muss diesem bei seinem ersten Besuch immer manuell zustimmen, kann dann allerdings hinterlegen, dass der Check-In künftig automatisch stattfindet (55).

PayPal erfährt, im Falle einer Zustimmung, sofort den aktuellen Aufenthaltsort des Kunden, so dass die aktivierten, automatischen Check-Ins es PayPal ermöglichen, Bewegungsinformationen zu sammeln, weil bekannt ist bei welchem Händler der jeweilige Beacon steht. Diese Profile könnten selbst dann erstellt werden, wenn PayPal gar nicht zum Bezahlen genutzt wurde. Der Händler bekommt im Gegenzug Namen und Foto des Kunden angezeigt, so dass personalisierte Ansprachen ermöglicht werden und der Kunde dem Händler gegenüber nicht anonym ist.

Von Anonymität kann im Falle von PayPal also keine Rede sein, da PayPal sowohl von den Einkaufgewohnheiten des Kunden Kenntnis erlangt als auch persönliche Daten großzügig mit verschiedenen Parteien teilt. Aus diesen Gründen werden für dieses Kriterium null Punkte vergeben.

Systemsicherheit

Die Sicherheit des PayPal-Kontos basiert auf dem Kundenkennwort. Ist dieses einem Angreifer bekannt, kann er das Konto verwenden, um Transaktionen zu initiieren. Somit ist PayPal ein beliebtes Ziel für Phishing[35]-Angriffe. Zu diesem Schluss kommt auch eine Studie von Kaspersky. Laut dieser ist PayPal, mit 44,12% aller Attacken auf Zahlungssysteme, das attraktivste Ziel in dieser Kategorie (257). Aus diesem Grund bietet PayPal schon seit einigen Jahren eine Zwei-Faktor-Authentifizierung mit einem Token an, der als Hardware separat erworben (258) und bei jeder Anmeldung verwendet werden muss. Für Zahlungen über PayPal Beacon wird zum einen die Authentifizierung mittels des Passworts benötigt, um die App zu starten, und zum anderen erfolgt die Authentifizierung gegenüber dem Händler, durch einen Abgleich des Kunden mit einem in der App hinterlegten Foto, welches dem Händler auf seiner Kasse angezeigt wird. Das Foto kann jedoch mit Kenntnis des Kennwortes geändert werden, so dass die Geheimhaltung des Kennwortes die wichtigste Sicherheitsmaßnahme ist.

Anfang 2014 bewiesen Forscher von Duo Security, dass die App von PayPal noch keine Zwei-Faktor-Authentifizierung unterstützte. War die zusätzliche Authentifizierung dennoch eingeschaltet konnte die App nicht ohne den Sicherheitsschlüssel genutzt werden – so jedenfalls die Theorie. Besagte Forscher zeigten hingegen, dass eine Nutzung aufgrund einer fehlerhaften API[36] jedoch auch ohne Besitz des Sicherheitsschlüssels möglich war (259).

---

[35] Phishing ist der Versuch persönliche Daten oder Zugangsinformationen für Dienste über gefälschte Webseiten zu erlangen. Hierzu werden in der Regel E-Mails oder andere Nachrichten versendet, die das Opfer verleiten sollen, die gefälschte Webseite aufzurufen und dort die verlangten Daten einzugeben.

[36] Kurzform für Application Programming Interface; Eine API ist eine Schnittstelle einer Software, über die andere Anwendungen, wie beispielsweise Apps, mit dem Programm kommunizieren können.

Da PayPal ein häufig verwendetes System ist, kommt es immer wieder zu entsprechenden Problemen, bei denen Kundenkonten gehackt werden, wie unzählige Einträge in diversen Foren und Ratgeberseiten zeigen (260–263). In diesen Fällen wurden Schwachstellen des Systems, in der Regel die alleinige Authentifizierung über ein Passwort, ausgenutzt.

Die Sicherheit des Systems PayPal ist aus den genannten Gründen nicht allzu hoch, da die Authentifizierung mit Hilfe eines Passwortes vergleichsweise leicht gehackt werden kann. Daher werden insgesamt zwei Punkte für dieses Kriterium vergeben, denn PayPal reagiert in der Regel schnell und sperrt das Konto, sobald die internen Sicherheitssysteme Alarm schlagen. Ferner kann das Angebot einer Zwei-Faktor-Authentifizierung die Sicherheit erhöhen – allerdings wird es oft nicht genutzt, solang es keine Pflicht für den Nutzer darstellt.

Finanzielle Sicherheit

PayPal nutzt für die Zahlung ein hinterlegtes Bankkonto oder eine Kreditkarte, von der die Summen abgebucht werden. PayPal, als Intermediär, vermittelt das Geld zwischen beiden Parteien. Im Hintergrund laufen zeitgleich verschiedene Prüfungen ab, die missbräuchliche Zahlungen verhindern sollen. Fallen diese Prüfungen negativ aus, reagiert PayPal in der Regel sehr rigide und sperrt das komplette Konto. Dies kann für einige Nutzer von PayPal durchaus existenzbedrohend werden, wenn über größere Summen nicht verfügt werden kann. So klagte etwa ein Händler vor dem Landgericht Stuttgart, nachdem PayPal sein Konto eingefroren hatte. Die Klage endete mit einem Vergleich, bei dem PayPal sämtliche Kosten übernahm, um ein Urteil zu vermeiden (264).

Zudem sind die Gründe weshalb Konten gesperrt werden zum Teil fragwürdig. Beispielsweise wurde in der Sendung C’t TV berichtet, dass einem Händler sein Konto gesperrt wurde, da der Sohn des Kontoinhabers negativ bei PayPal aufgefallen war. Der Sohn hatte allerdings nie Zugriff auf das gesperrte Konto. Vielmehr wurde der Vater in Haftung für den Sohn genommen, der vollkommen unabhängig handelte (265).

Das ZDF berichtete in seinem Reportagemagazin ZDF.reporter davon, dass einem Händler ein PayPal-Konto mit einem Guthaben von mehr als 100.000 € eingefroren wurde. Dies hatte für den Händler zur Konsequenz, dass kein neues Material gekauft werden konnte, so dass neue Bestellungen nicht rechtzeitig oder gar nicht bearbeitet werden konnten. In der Folge musste der Händler zwölf seiner Mitarbeiter entlassen. Auch das Einreichen der von PayPal angeforderten Unterlagen, die weit über das Bankenübliche hinausgingen, führte nicht dazu, dass das Konto wieder freigegeben wurde (266).

Im Falle der Beschwerde eines Kunden, bucht PayPal zunächst den Betrag von dem Händlerkonto zurück. Dieser muss nun nachweisen, dass die Zahlung durchaus berechtigt war. Das ist jedoch nicht immer möglich und, falls doch, in jedem Fall sehr aufwendig.

Ein weiteres Problem ist, dass Zahlungen über gestohlene Kreditkarten getätigt werden können, selbst wenn diese bereits gesperrt sind. Denn PayPal erlaubt die Zahlung, ohne dass die Ergebnisse der Kreditkartendatenprüfung vorliegen (267). Auf diese Weise können Schäden entstehen, die durch PayPal beglichen werden müssen.

Die finanzielle Sicherheit von PayPal Beacon unterscheidet sich hiervon nicht, da die Transaktion zwar anders initiiert, aber letztlich äquivalent abgewickelt wird. Die zahlreichen Prüfungen, die PayPal durchführt, verfolgen zwar grundsätzlich das Ziel finanzielle Schäden zu verhindern. Durch die Maßnahmen, die PayPal ergreift, entstehen sie jedoch zum Teil erst. Aus diesem Grund wird dieses Kriterium mit nur einem Punkt bewertet.

Verantwortlichkeit

Das System PayPal Beacon wird allein durch PayPal Inc. und seine Tochterunternehmen verantwortet. Sämtliche Zahlungen werden immer online, direkt über PayPal abgewickelt und geprüft. Somit stehen PayPal alle Möglichkeiten offen, einzelne Zahlungen abzulehnen oder Teilnehmer komplett von seiner Plattform auszuschließen.

Die Sperrung kompletter Konten hat PayPal, wie zuvor bereits erwähnt, durchaus schon mehrfach wahrgenommen. Beispielsweise 2010, als die Whistleblower-Plattform Wikileaks, die Spenden u.a. über PayPal sammelte, von PayPal, aufgrund von Verletzungen der Nutzungsbedingungen, ebenso gesperrt wurde, wie die Wau-Holland-Stiftung, die ebenfalls Gelder für den Betrieb von Wikileaks sammelt (268, 269).

2011 begann PayPal in Deutschland damit, Händler von PayPal auszuschließen, die kubanische Produkte, wie Zigarren oder Rum, vertreiben, da die europäische Gesellschaft PayPal (Europe) S.à r.l. et Cie, S.C.A., als Tochter eines US-Unternehmens, dem US-Handelsembargo gegen Kuba unterliege. Händler, die sich weigerten, die betreffenden Produkte aus ihren Shops zu entfernen, wurde der Zugang zu PayPal gesperrt – zum Teil ohne jegliche Vorwarnung. Betroffen war beispielsweise die Drogeriemarktkette Rossmann, die in ihrem Onlineshop Zigarren aus Kuba anbietet. Sie entschied sich jedoch dafür, ihr Sortiment nicht zu ändern und stattdessen PayPal als Bezahlmethode nicht weiter zu unterstützen (270, 271).

Beide Blockaden durch PayPal wurden mittlerweile wieder aufgehoben. Dennoch ist jederzeit mit vergleichbaren Fällen zu rechnen. Schon in den Allgemeinen Geschäftsbedingungen von PayPal ist unter Abschnitt 10.2 zu lesen, dass PayPal „Ihr Recht, das Zahlungsinstrument oder das PayPal-Konto zu nutzen, ausschließen, aussetzen oder einschränken [kann]. Dies kann für das gesamte PayPal-Konto gelten oder für einzelne Zahlungsvorgänge. Beispielsweise können wir die Nutzung einer Ihrer Zahlungsquellen beschränken oder die Möglichkeit, Geld zu senden, Abhebungen vorzunehmen oder Finanzdaten zu entfernen. Grundsätzlich informieren wir Sie über solche Maßnahmen im Voraus. Wir können Ihr Recht, das Zahlungsinstrument bzw. Ihr PayPal-

Konto zu nutzen aber auch ohne vorherige Mitteilung ausschließen, aussetzen oder einschränken, wenn wir dies zum Beispiel aus Sicherheitsgründen für notwendig halten oder Sie diese Vereinbarung verletzt haben.“ (272)

Alle genannten Fälle beziehen sich auf die Online-Nutzung des PayPal-Kontos. Allerdings darf davon ausgegangen werden, dass auch Shops, die PayPal Beacon nutzen, ähnlich behandelt werden. Und letztendlich ist es ganz gleich, welche Variante von PayPal eingesetzt wird: Ist das dahinterliegende Konto gesperrt, funktioniert keine der verschiedenen Bezahlmethoden mehr. Aus den genannten Erwägungen heraus, dass PayPal eben auch politisch motivierte Sperrungen von Konten vornimmt, wird für dieses Kriterium kein Punkt vergeben Denn PayPal nutzt so seine Machtposition gegenüber Dritten aus und versucht eigene Ziele durchzusetzen.

Verbreitung

PayPal Beacon ist Teil des PayPal-Universums, welches verschiedene Angebote zur Zahlungsabwicklung umfasst. Zum einen ist dies die ursprüngliche Form im Internet zu bezahlen, aber auch das Angebot, einen Rechnungskauf anzubieten (BillSAFE), PayPal Check-In für die Zahlung am POS, das QR-Code-Shopping oder eben PayPal Beacon (273). Letzteres ist, als eine der neueren Entwicklungen von PayPal, bisher noch nicht verfügbar und lediglich ein Pilotprojekt, welches in Amerika getestet wird (274).

PayPal ist dabei immer ein Dienst, der international verfügbar ist und eingesetzt werden kann. Eine Umrechnung von Währungen findet dabei gegebenenfalls automatisch statt. Durch seine zahlreichen Produkte ist PayPal sowohl im Internet als auch am POS einsetzbar, wobei letzteres relativ neu ist und deshalb noch keine hohe Verbreitung erfährt.

Außerdem ist die Anzahl der Nutzer sehr hoch. So zählte PayPal im dritten Quartal 2014 156,9 Millionen aktive PayPal-Accounts (54). Diese hohe Verbreitung auf Seite der Kunden hat zur Folge, dass u. a. auch Unternehmen der Otto Group, die mit Yapital einen ähnlichen Dienst anbieten, PayPal integrieren. Daneben zählte das Bundesamt für Sicherheit in der Informationstechnik 2010 rund 20.000 Onlineshops in Deutschland, die PayPal als Bezahloption anbieten (275). Eine Studie des E-Commerce-Centers Köln ergab zudem, dass rund 70% der Befragten Deutschen PayPal zumindest kennen oder sogar schon einmal genutzt haben. Dieselbe Studie stellte fest, dass PayPal rund 29% der Onlinezahlungen in Deutschland abwickelt (276).

Somit ist die Verbreitung von PayPal in Summe als sehr hoch zu bewerten, weil es sowohl von Kunden als auch von Händlern vielfach genutzt und angeboten wird, wobei die Zahl der Angebote am POS noch am Anfang steht. Die Verbreitung von PayPal Beacon ist zurzeit nicht gegeben, da es sich bisher nur um einen Versuch handelt. Aus den genannten Gründen werden für dieses Kriterium vier von fünf Punkten vergeben.

Kosten

PayPal unterscheidet hinsichtlich der Gebühren, über nahezu alle Varianten der Bezahlung hinweg, zwischen privaten und geschäftlichen Zahlungen[37]. Weil PayPal Beacon sich jedoch explizit an Händler richtet, wird die folgende Bewertung anhand der Gebühren für geschäftliche Zahlungen vorgenommen.

Für PayPal fallen sowohl als Händler wie auch als Kunde keine Gebühren für Registrierung, fixe monatliche Kosten oder dergleichen an. Alle Gebühren sind im Anhang der Nutzungsbedingungen von PayPal aufgelistet.

Aus Sicht der Kunden ist die Zahlung kostenfrei. Eine Ausnahme bildet die Verwendung der Zwei-Faktor-Authentifizierung, für die ein Hardware-Token benötigt wird, der mit einmalig 23,- € für das Gerät und den Versand berechnet wird (258). Ist die Umrechnung von Währungen für einen Kauf notwendig, bei der der Händler die notwendigen Gebühren nicht übernimmt, werden dem Kunden, je nach Währung in die gewechselt werden muss, eine Gebühr von 3,0% bis 4,0% berechnet (272). In Summe werden aus Sicht des Kunden für die Kosten vier von fünf Punkten vergeben.

Aus Sicht des Händlers entstehen jedoch pro Transaktion gleich mehrere Gebühren. Standardmäßig verlangt PayPal 1,9% des Transaktionsumsatzes plus einer Festgebühr, die je nach Land, in dem der Händler sitzt, variiert. Allerdings können auf Antrag niedrigere, prozentuale Gebühren gewährt werden, wenn das Händlerkonto bestimmte Voraussetzungen, wie ein monatliches Verkaufsvolumen und dergleichen, erfüllt. Die fixen Kosten bleiben trotz allem erhalten. Im Fall der niedrigeren Prozente staffelt PayPal die Gebühren, so dass bei einem monatlichen Umsatz von 5.001,- € bis 25.000,- € nur noch 1,7% des Umsatzes einer Transaktion fällig werden. Zwischen 25.001,- € und 50.000,- € verlangt PayPal noch 1,5% und für alles darüber liegende 1,2%. Die Festgebühr beträgt für Händler, die mit Euro handeln, immer 0,35 €, während bei Nutzung von US-Dollar nur 0,30 USD fällig werden (272).

Weitere Gebühren müssen entrichtet werden, wenn der Käufer aus einem anderen Land kommt als der Händler. In solch einem Fall berechnet PayPal, je nach Herkunft des Käufers, für die „grenzüberschreitende Zahlung“ bis zu 3,3% zusätzlich pro Transaktion.

Ist eine Umrechnung der Währung erforderlich, werden weitere Gebühren fällig. Übernimmt der Verkäufer die Kosten liegen diese 2,5% über dem Ankaufwechselkurs (272). Zusätzlich erhebt PayPal Gebühren für Händler, falls sie Dokumente von PayPal anfordern, Zahlungen rückabwi-

[37] „Eine "geschäftliche Zahlung" ist eine Zahlung, die im Zusammenhang mit dem Kauf oder Verkauf von Waren oder Dienstleistungen geleistet wird. Dies umfasst auch Zahlungen, die Sie über die Funktion "Geld anfordern" in Ihrem PayPal-Konto erhalten. Eine "persönliche Zahlung" ist eine Zahlung, der kein Kauf oder Verkauf zugrunde liegt (d.h., die Zahlung wird nicht für Waren oder Dienstleistungen geleistet), sondern die beispielsweise an Freunde oder Familienmitglieder (…) gesendet wird oder die Sie von Freunden oder Familienmitgliedern erhalten.“ (272).

ckeln, Rücklastschriften erfolgen, Sammelzahlungen versendet werden oder Abbuchungen fehlschlagen (272). Ferner fallen für PayPal Beacon weitere Kosten für die Anschaffung eines oder mehrerer Beacon an. Die genaue Höhe der Kosten sind jedoch noch nicht bekannt (274).

PayPal basiert im Ganzen betrachtet auf verschiedenen Gebühren, die sich aus einer komplexen Gebührenordnung ergeben. Dadurch, dass allein der Händler die Kosten einer Transaktion trägt, sind diese vergleichsweise hoch, so dass nur ein Punkt vergeben werden kann. Zusammen mit den Punkten, die aus Kundensicht angerechnet werden können, ergibt sich eine Gesamtwertung von fünf Punkten für dieses Kriterium.

Komplexität für Kunden

Die Registrierung bei PayPal funktioniert vollständig und ausschließlich online, ohne Vorlage jedweder Dokumente, wodurch sie relativ einfach gestaltet ist. Während der Anmeldung müssen nur die gewöhnlichen Daten, wie Zugangs- und Kontaktdaten, inklusive der Bankverbindung oder der Kreditkartendaten eingegeben werden. Wird eine Bankverbindung übermittelt, veranlasst PayPal eine Gutschrift von 0,01 €, bei der als Verwendungszweck ein Code übermittelt wird, der dazu dient, den Zugriff auf das Konto nachzuweisen. Dieser Code muss nach Eingang der Überweisung innerhalb des PayPal-Kontos hinterlegt werden (277, 278).

Nach der Registrierung muss die PayPal-App auf einem Smartphone installiert und durch Eingabe der PayPal-Benutzerdaten mit dem Konto verknüpft werden. Innerhalb der App muss vor der ersten Verwendung von PayPal Beacon zudem ein Foto hinterlegt werden (279).

Im Anschluss an die Ersteinrichtung, die aufgrund der Verifizierung des Bankkontos bis zu einer Woche dauern kann (278), kann PayPal Beacon genutzt werden. Betritt der Kunde mit dem Smartphone ein Geschäft, welches PayPal Beacon bereits unterstützt, fragt die App, ob der Kunde in dem Geschäft „eingecheckt“ werden möchte. Er kann dies bestätigen und die Auswahl für den nächsten Besuch speichern, sodass die App bei weiteren Besuchen nicht mehr nachfragt, sondern den Kunden automatisch in dem betreffenden Geschäft anmeldet (55).

Zum Bezahlen gibt der PayPal-Kunde an der Kasse an, dass er PayPal nutzen möchte. Der Händler bekommt nach dem Check-In das Foto des Kunden auf der Kasse angezeigt und wählt dieses zur Bezahlung aus. Auf diese Weise ermöglicht PayPal dem Kunden die Zahlung, ohne selbst aktiv werden zu müssen. PayPal ist bisher der einzige Anbieter, der derart wenig Aktion des Kunden verlangt. Die Zahlung ist für den Kunden daher besonders einfach und schnell durchzuführen, weshalb die Komplexität für den Kunden mit neun von zehn Punkten bewertet.

Komplexität für Händler

Die Registrierung läuft für Händler zunächst sehr ähnlich zu dem Registrierungsvorgang des Kunden ab. Neben den Geschäftsdaten muss lediglich ein Passwort vergeben werden, mit dem sich der Händler künftig gegenüber PayPal authentifizieren muss. Ein Bankkonto wird, genau wie bei Privatkunden, während der Registrierung verknüpft und im Nachgang verifiziert (277).

Um PayPal Beacon anbieten zu können, wird ein entsprechender Bluetooth-Dongle von PayPal benötigt. Da dieser noch nicht verfügbar ist, ist im Moment weder bekannt, wie der Bestellprozess hierfür ablaufen wird und ob eine separate Registrierung notwendig ist, noch wie teuer dieser Dongle sein wird. Genauso ist die Integration in bestehende Kassensysteme derzeit noch nicht genau bekannt. Allerdings kooperiert PayPal mit verschiedenen Anbietern von Softwarelösungen für den POS und bietet ferner eine Option an, die Abwicklung vollständig über ein iPad zu erledigen (280, 274).

Wird ein Blick auf die Integration im E-Commerce geworfen, so existieren neben einem Developer Center (https://developer.paypal.com/), in dem die API erläutert und Beispiele zur Einbindung in eigene Systeme gegeben werden, auch zahlreiche Plug-ins für E-Commerce-Software, sowie Payment Service Provider, die PayPal in ihr Portfolio aufgenommen haben. Es darf also damit gerechnet werden, dass auch die Integration von PayPal Beacon vergleichsweise einfach und gut dokumentiert werden wird (281).

Die Bezahlung läuft am POS unschlagbar zügig ab, weil zwischen Händler und Kunde keinerlei Daten oder Geld getauscht werden muss. Der Kunde erscheint nach seinem Check-In auf dem Display des POS und muss durch den Händler nur noch ausgewählt werden. Im Internet ist die Zahlung über das Beacon-System nicht möglich, stattdessen kann das PayPal-Konto durch den klassischen Login mit Benutzername und Passwort verwendet werden. Durch den Express Checkout sind für den Kunden keine weiteren Schritte nötig, da PayPal die erforderlichen Daten an den Händler übermittelt.

Die Komplexität für den Händler ist damit überschaubar und auch der Bezahlvorgang ist sehr schnell – vorausgesetzt der Kunde hat den automatischen Check-In aktiviert oder sich rechtzeitig vor dem Bezahlen manuell eingecheckt. Andernfalls muss er sich am POS einchecken, so dass es einige Sekunden dauern kann, bis er auf dem Gerät des Händlers angezeigt wird. Komplexer wird der Umgang mit PayPal erst, wenn zusätzliche Daten zur Verifizierung des Kontos durch PayPal angefordert werden – beispielsweise nachdem das Konto eingefroren wurde. Ist dies geschehen, müssen zahlreiche Dokumente an PayPal übermittelt werden.

Fordert der Kunde den Käuferschutz von PayPal an, führt dies zunächst dazu, das PayPal die Bezahlung rückabwickelt. Der Händler hat in diesem Fall die Arbeit nachzuweisen, dass er korrekt gehandelt und geliefert hat, was zeitaufwendig und auch nicht immer möglich ist. In Summe werden aus diesem Grund acht von zehn Punkten für dieses Kriterium vergeben.

Alleinstellungsmerkmale

PayPal Beacon bietet dem Händler die Gelegenheit standortbasierten Marketings. Hierzu können Kunden, die sich in Nähe eines Beacons befinden, spezielle Angebote gemacht werden. Auch die Möglichkeit der persönlichen Ansprache, um die Kundenbindung zu erhöhen, besteht, weil PayPal nach dem Check-In Namen und Foto an den Händler übermittelt.

Funktionen, wie das QR-Code Shopping, bietet PayPal, ähnlich wie Yapital und PAYMEY, zusätzlich an. Somit werden weitere zwei Punkte für die Zusatzangebote von PayPal vergeben.

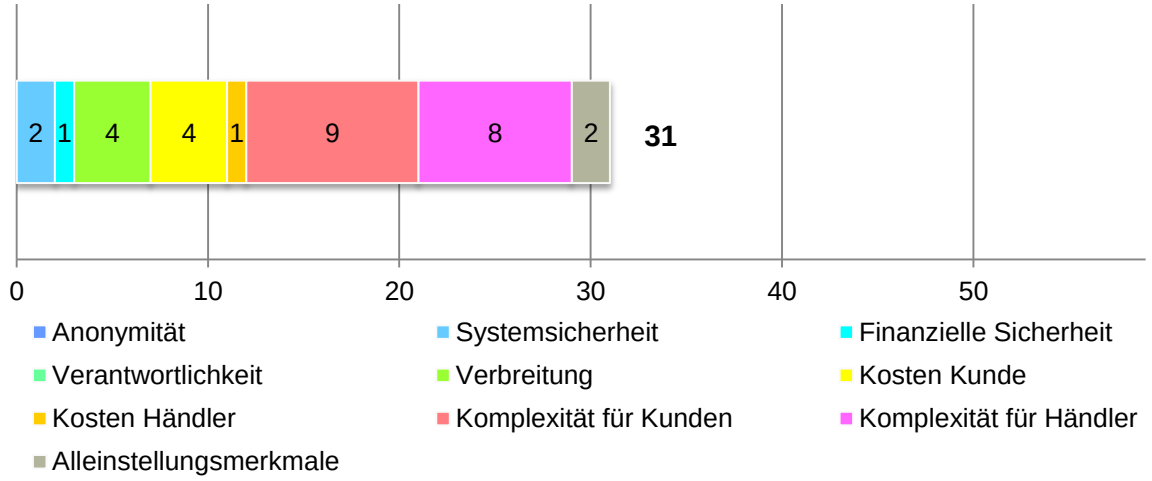

Abbildung 38: Gesamtbewertung des Zahlungssystems PayPal Beacon.

3.4 Internetwährungen

Den Abschluss der Bewertungen bildet die Kategorie der Internetwährungen. Diese sind in Kapitel *1.4 Internetwährungen* näher beschrieben.

3.4.1 Bitcoin (BTC)

Das erste Zahlungssystem aus der Kategorie Internetwährungen, welches im Folgenden bewertet wird, ist das System Bitcoin, dessen Idee die Grundlage für zahlreiche ähnliche Systeme bildet.

Anonymität

Aufgrund Ihres Designs mit eindeutigen Adressen und Schlüsselpaaren sind Bitcoins nur pseudonym. Die Pseudonymität kann prinzipiell nur durch den Benutzer selbst aufgehoben werden, da es nirgends eine Zuordnungstabelle von Adressen zu Benutzern gibt und somit nur der Eigentümer einer Adresse weiß, wem die Adresse gehört. Dies ändert sich jedoch, wenn die Wallet nicht auf einem eigenen Gerät gespeichert ist, sondern stattdessen Dienste, wie Coinbase, ge-

nutzt werden. Sie möchten dem Benutzer den Aufwand des Downloads der Blockchain und dem Aufbau notwendiger Schutzmaßnahmen abnehmen. Je nach Anbieter werden bei der Registrierung Daten abgefragt, mit denen der Benutzer identifiziert werden kann. Gleiches trifft ebenso auf den Kauf von Bitcoins bei Börsen oder an Marktplätzen zu. Bei Nutzung dieser Dienste ist in aller Regel eine Registrierung notwendig, bei der die Identität offengelegt werden muss (282). Hierbei ist die Identifizierung zum Teil sogar gewünscht und geht auf Regelungen zur Verhinderung von Geldwäsche zurück. So verlangt beispielsweise die Handelsplattform Paymium, vormals Bitcoin-Central.net, bei Eröffnung des Kontos einen Nachweis der Identität in Form eines eingescannten Personalausweises und den Nachweis über die korrekte Adresse. Für letzteres werden eingescannte Wasser-, Strom- oder Gasrechnungen, sowie Steuerbescheide, aus denen jeweils die Adresse des Kontoinhabers hervorgeht, akzeptiert (283).

Andere Plattformen, wie bitcoin.de, verlangen die Identifizierung nicht zwangsläufig. Stattdessen wird das Konto entsprechend den Geschäftsbedingungen limitiert, so dass das Transaktionsvolumen eines Kalenderjahres maximal 2.500,- € betragen darf und eine einzelne Transaktion nur bis zu einer Summe von 1.000,- € möglich ist. Eine Identifizierung des Kunden erfolgt in Deutschland z.B. über das Post-Ident-Verfahren und ist notwendige Voraussetzung für den unbegrenzten Handel (284, §10 Abs. 6 - §11). Zusätzlich sind jedoch weitere Kriterien zu erfüllen, die sich aus dem Trust-Level-Bewertungssystem ergeben (285).

Demnach sind Bitcoins vom Konzept her zwar pseudonym, durch Nutzung bestimmter Dienstleistungen nimmt die Pseudonymität aber zugunsten der Bequemlichkeit und Nutzbarkeit deutlich ab. Mit Hilfe von sogenannten Mixing Diensten kann die Pseudonymität allerdings wiederhergestellt werden. Hierzu nimmt der Dienst eine Summe Bitcoins entgegen und überweist dafür dieselbe Summe, abzüglich Gebühren, an verschiedene eigene Adressen zurück. Die übertragenen Bitcoins stammen aus anderen Transaktionen, so dass keine Verbindung zwischen Ein- und Ausgängen hergestellt werden kann (286).

Luxemburgische Forscher versuchten die Anonymität von Bitcoin aufzuheben, indem sie IP-Adressen zu Transaktionen ermittelten. Ihnen gelang dies auch unter Einsatz verschiedener Techniken mit einer Erfolgsquote zwischen elf und 60%, je nachdem welches Vorgehen gewählt wurde. Die Kosten belaufen sich dabei auf weniger als 1.500,- €, so dass dies für Staaten und staatliche Stellen keine große Hürde darstellt, Bitcoin-Transaktionen zu deanonymisieren (287). Unter Aufwendung noch größerer Summen und weiterer Forschung ließe sich die Quote sicherlich auch noch weiter verbessern, so dass eine Zuordnung von IPs zu Transaktionen möglich wird. Eine Auflösung von IP-Adressen zu Personen dürfte staatlichen Stellen durch Regelungen wie die Vorratsdatenspeicherung leicht fallen. Letztlich ist jeder durch sein Nutzungsverhalten zu einem großen Teil selbst dafür verantwortlich, dass die Pseudonymität erhalten bleibt, indem sich der einzelne Nutzer überlegt, welche Dienste er verwendet und wem gegenüber er seine Pseudonymität aufhebt, ohne sie wiederherzustellen. Aus diesen Gründen werden für das Kriterium der Anonymität acht von zehn Punkten vergeben.

Systemsicherheit

Das System Bitcoin bietet durch sein Design als dezentrales P2P-Netzwerk einige Angriffspunkte, die den Entwicklern bekannt sind, so dass Maßnahmen zur Vermeidung der Ausnutzung dieser Schwächen ergriffen werden können und zum Teil bereits ergriffen wurden. Eine Übersicht der Angriffspunkte bietet u.a. das Wiki des Bitcoin-Projekts, in dem die Schwächen in verschiedene Klassen eingeteilt wurden (288).

Ein bekanntes Beispiel für einen Angriff ist die sogenannte 51%-Attacke, bei der der Angreifer mindestens 51% der auf das Mining verwendeten Rechenkapazität stellt. Gelingt dies, kann anschließend die Durchführung von Transaktionen verhindert, Bitcoins doppelt ausgegeben oder hohe Transaktionsgebühren verlangt werden. Auch wenn ein solcher Angriff, aufgrund der erforderlichen Rechenkapazität, schwierig ist, ist er doch nicht komplett unmöglich. So vereinte der Mining-Pool Ghash.io in 2014 durchaus einmal ausreichend Rechenkapazität. Und durch die Ankündigung des deutschen Startups Bitcoin-Brothers neue performantere Mining-Hardware anzubieten, wird es in Zukunft einfacher, die für diesen Angriff notwendige Rechenleistung zur Verfügung zu stellen (289, 290).

In Summe kann das Design des Systems, trotz theoretischer Schwächen, als sicher bezeichnet werden. Allerdings ist die Sicherheit durch andere Schwachstellen weitaus mehr gefährdet. Ein Beispiel hierfür ist der ehemalige Handelsplatz Mt. Gox, der Anfang 2014 von der Bildfläche verschwand, nachdem über 850.000 Bitcoins der Börse verschwunden waren. Der Diebstahl der Coins wurde angeblich durch mangelhafte Software ermöglicht, in der eine seit 2011 bekannte und eigentlich gefixte Lücke noch vorhanden war (291).

Ferner ist der Diebstahl von Wallets, die beispielsweise auf privaten, oftmals unzureichend geschützten Rechnern gespeichert sind oder der Angriff entsprechender Online-Dienste deutlich einfacher (292–295). Insgesamt kann Sicherheit also hergestellt werden, allerdings ist dies sehr aufwendig und für den normalen Anwender nicht umsetzbar. Dadurch, dass das System offen ist, werden Schwachstellen prinzipiell durch jeden entdeckt und in der Gemeinschaft ausgebessert. Für dieses Kriterium werden deshalb sechs Punkte vergeben.

Finanzielle Sicherheit

Alle Transaktionen, aus denen sich die Guthaben aller Nutzer ergeben, sind in der Blockchain gespeichert. Einmal in die Blockchain aufgenommene Transaktionen gelten als durchgeführt und können nur durch den Zahlungsempfänger, der eine Rücküberweisung anstößt, rückgängig gemacht werden.

Schwierig ist jedoch der Fall, dass zwei Miner zeitgleich einen neuen Block finden und versuchen, diesen im Bitcoin-Netzwerk zu propagieren. In solch einer Situation würden die Knoten des Bitcoin-Netzwerkes jeweils nur einen der beiden Blöcke akzeptieren, ihn in ihre Blockchain auf-

nehmen und danach versuchen, hierzu den nächsten Block zu minen. Auf Dauer wird sich von beiden Varianten immer die längere Blockchain durchsetzen (296).

Eine rückwirkende Manipulation der Blockchain würde bedeuten, dass alle, dem manipulierten Block folgenden Blöcke neu berechnet werden müssten, weil sich diese jeweils auf ihren Vorgänger beziehen. Um jeden Teilnehmer des Bitcoin-Netzwerkes von dieser manipulierten Blockchain zu überzeugen, müsste diese länger sein als die originale Blockchain. In Folge dessen würden also viele Blöcke in kurzer Zeit berechnet werden müssen, was stochastisch sehr unwahrscheinlich ist, so dass rückwirkende Transaktionsmanipulationen quasi nicht möglich sind. Einmal durchgeführte Zahlungen können demnach nicht rückgängig gemacht werden, was einer Zahlungsgarantie für den Zahlungsempfänger entspricht.

Zu berücksichtigen ist jedoch, dass, wie erwähnt, zwei Blöcke gleichzeitig gefunden werden können. Aus diesem Grund sollte der Zahlungsempfänger nicht direkt, wenn er die Transaktion innerhalb des Bitcoin-Netzwerkes vorfindet, darauf vertrauen, dass sie bereits ausgeführt wurde. Es ist ratsam zumindest einige, folgende Blöcke abzuwarten. Die Hauptentwickler empfehlen bei großen Summen sogar bis zu sechs weitere Blöcke (297).

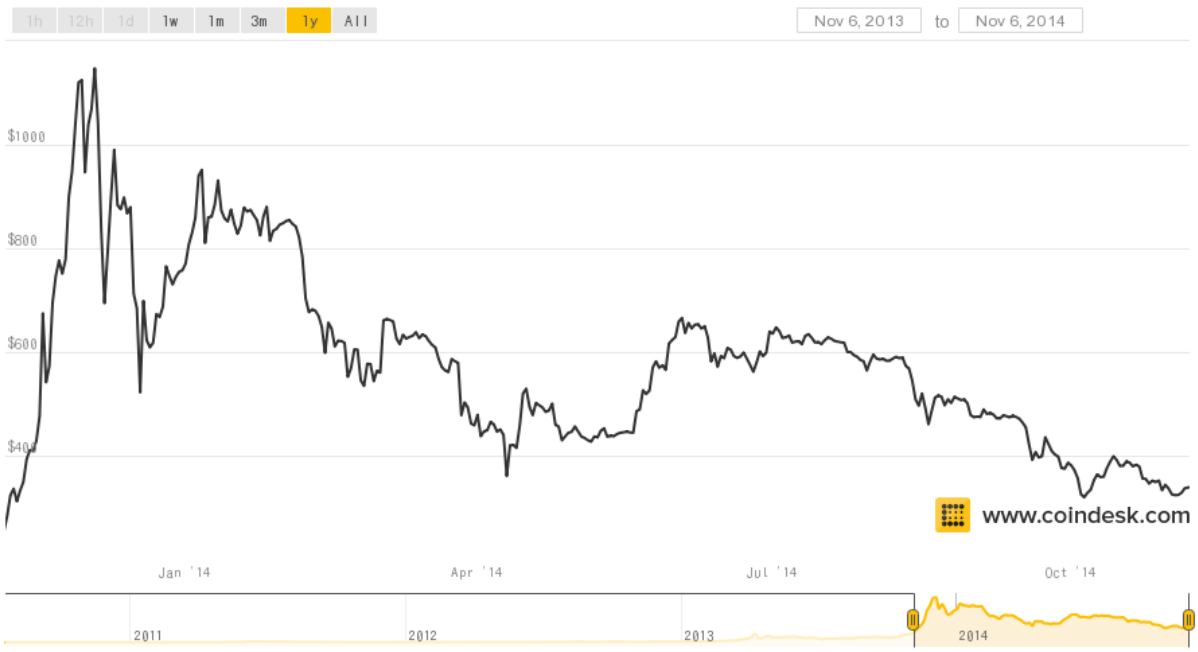

Abbildung 39: Entwicklung des Bitcoin-Preises von November 2013 bis November 2014.

Finanzielle Verluste können auftreten, wenn der Zugriff auf die in der Wallet hinterlegten Schlüssel verloren geht. Dies kann zum einen durch defekte Festplatten und damit einhergehenden Datenverlust geschehen oder zum anderen durch Angriffe mit kriminellen Hintergrund. Aber genauso führen menschliche Fehler immer wieder zum Verlust von Bitcoins. So entsorgte ein Brite 2013 eine Festplatte mit der einzigen Kopie seiner Wallet – und damit auch 7.500 Bitcoins (298). Die Wiederbeschaffung ist in einigen Fällen sicherlich möglich, jedoch sehr aufwendig und auch letztlich nicht immer erfolgreich. Es empfiehlt sich deshalb, Bitcoins, gerade bei größeren Sum-

men, nicht auf einem PC mit Internetanbindung oder in Onlinediensten zu sichern, sondern offline auf einem gut verwahrten Stück Papier, so dass Angriffe darauf deutlich erschwert werden.

Ein weiteres Problem, welches die finanzielle Sicherheit betrifft, sind die starken Kursschwankungen, denen Bitcoin immer noch unterliegt. Der Preis eines Bitcoins ergibt sich dabei immer aus Angebot und Nachfrage auf entsprechenden Handelsplätzen. Etabliert sich Bitcoin künftig weiter und wird öfters als Zahlungsinstrument anstatt als Spekulationsobjekt genutzt, wird sich der Kurs stabilisieren.

Abschließend lässt sich festhalten, dass die finanziellen Sicherheiten des Systems durchaus hoch sind, da Rückbuchungen nicht möglich sind und für Händler somit Zahlungsgarantien bestehen. Durch die Kursschwankungen und den falschen Umgang entstehen allerdings finanzielle Risiken, die niemand auf Kulanz ausgleicht, wie es bei klassischen oder mobilen Zahlungssystemen der Fall ist. Für dieses Kriterium werden demnach sieben von zehn Punkten vergeben.

Verantwortlichkeit

Für das System Bitcoin ist die dahinterstehende Community verantwortlich. Diese besteht zum einen aus den Entwicklern und den Minern, zum anderen aus allen Nutzern des Systems. Es gibt dabei keine zentrale Stelle, die alles allein verantwortet, oder Einflussmöglichkeiten hat, um einzelne Teilnehmer auszusperren oder Transaktionen zu verhindern. Alle diese Teilnehmer haben ein Interesse daran, das System stabil am Laufen zu halten, damit ihr eigenes Guthaben nicht beschädigt wird.

Eine Möglichkeit des Eingriffs, wäre. Dass einzelne Miner Transaktionen nicht in ihren neuen Block mitaufnehmen. Diese wird stattdessen von einem anderen Miner dem nächsten Block hinzugefügt, so dass es lediglich zu einer Verzögerung kommen wird. Bedingung ist jedoch, dass ausreichend viele Miner mitmachen und keiner von ihnen mehr als 50% der Rechenkapazität des Bitcoin-Netzwerkes stellt. Somit können für dieses Kriterium fünf Punkte vergeben werden, weil die Verantwortlichkeit in den Händen vieler liegt und diese sich gegenseitig kontrollieren.

Verbreitung

Bitcoin kann sowohl im Internet als auch am POS weltweit verwendet werden. Aufgrund der Tatsache, dass die Nutzung von Bitcoin keine Registrierung erfordert, ist das System seit seiner ersten Entwicklung weltweit uneingeschränkt verfügbar. Die Anzahl der Akzeptanzstellen ist dadurch, dass es sich um ein recht junges System handelt, noch relativ gering. Indes unterstützen seit dem Jahr 2014 mehrere große Anbieter, wie Dell oder Expedia, Bitcoin als Zahlungsmittel (68, 299, 300). Expedia teilte bereits einen Monat später in einem Interview mit Coindesk mit, dass die Erwartungen an die neue Bezahlmöglichkeit übertroffen wurden. Allerdings wurde nicht bekannt gegeben, was das genau bedeutet und in welchem Umfang Bitcoin genutzt wurde (301).

Ferner ist die Akzeptanz am POS über Mobile Payment-Lösungen gegeben. Hierbei ist es letztlich wichtig, dem Kunden zu ermöglichen, Betrag und Empfängeradresse nicht händisch eingeben zu müssen. Vielfach werden in diesem Zusammenhang QR-Codes genutzt, die der Händler auf einem Mobile Device generiert. Der Kunde scannt diesen mit seinem Gerät – eine entsprechende Bitcoin-App vorausgesetzt. Abschließend muss er die Transaktion nur noch bestätigen. Verschiedene Anbieter stellen bereits Lösungen zur Verfügung, etwa Coinbase, Coinkite, Bitpay oder zahlreiche andere.

Beispiele, dass das Bezahlen mit Bitcoin möglich ist, gibt es demnach viele, was einige Nutzer bereits dazu veranlasste, auszuprobieren, wie weit verbreitet Bitcoins bereits sind. Ein junges Ehepaar aus Utah begann 2013 zunächst mit dem Versuch auf einer Reise nach New York ausschließlich mit Bitcoins zu bezahlen. Nachdem dies, trotz einiger Schwierigkeiten, u.a. beim Tanken, funktionierte, beschlossen sie, den Versuch zu verlängern und reisten nur mit Bitcoins nach Europa und Asien – was ihnen ebenfalls gelang, auch wenn sie zwischendurch immer wieder Mittelsmänner benötigten, die ihre Bitcoins akzeptierten und dafür Waren aller Art anboten (302). Dies zeigt, dass Bitcoins noch nicht so weit verbreitet sind. Dadurch, dass ständig neue Akzeptanzstellen entstehen, nimmt die Verbreitung beständig zu. Aus diesem Grund werden für dieses Kriterium zwei Punkte vergeben.

Kosten

Das Bitcoin System an sich kennt keine Unterscheidung seiner Nutzer in Händler und Kunden, so dass für beide prinzipiell dieselben Kosten anfallen. Die Einrichtung ist dabei vollkommen kostenlos, die benötigte Software wird unter Open-Source-Lizenz ebenfalls kostenfrei verteilt. Auch sind viele Dienste rund um Bitcoin kostenlos nutzbar.

Der Verdienst für Miner ergibt sich bisher aus der Belohnung für das Mining. Derzeit werden 25 BTC pro Block neu erstellt und dem System in Form einer Gutschrift für den Miner zugeführt. Die Belohnung wird immer nach 210.000 Blöcken halbiert und irgendwann, voraussichtlich 2140, komplett entfallen. Aus diesem Grund gibt es Transaktionsgebühren, die an die Miner gezahlt werden, um eine Transaktion in einen Block aufnehmen zu lassen. Diese ist jedoch frei wählbar, wobei der offizielle Bitcoin-Client seit 2012 die Gebühren anhand der Speichergröße der Transaktion bemisst. Pro aufgerundeten 1.000 Byte, eine durchschnittliche Transaktion ist dem Bitcoin Wiki zufolge 500 Byte groß, berechnet er automatisch Transaktionsgebühren von 0,0001 Bitcoin (303). Die Regeln zur Berechnung der Transaktionsgebühr können gegebenenfalls durch die Community angepasst werden. In jedem Fall sind diese Kosten durch den Zahlungssender, in einer Handelsbeziehung den Kunden, zu zahlen.

Die unterschiedlichen Dienste sind frei in ihrer Entscheidung für ihre Leistungen Gebühren zu verlangen. Coinbase beispielsweise bietet seine Dienste, zu denen das Senden und Empfangen von Zahlungen gehört, kostenfrei an. Hingegen wird der Umtausch von Bitcoin in klassische

Währungen nur gegen Entgelt erbracht, wobei die ersten Coins bis zu einem Wert von 1.000.000 USD kostenlos getauscht werden (304, 305). Anders sieht das Verdienstmodell der Plattform BitPay aus. Diese bietet ihre Dienste ebenso vollständig kostenfrei an. Darüber hinaus besteht die Möglichkeit, einen besseren Support und die Integration in die Buchhaltungssoftware QuickBooks käuflich zu erwerben (306). In beiden Beispielen fallen diese Kosten nur für den Händler an und sind als günstig einzustufen.

Weitere Kosten für Hard- und Software fallen auf Kundenseite nicht an, da Software kostenfrei erhältlich und die benötigte Hardware, in Form eines PCs oder Smartphones, in aller Regel schon vorhanden ist. Händler benötigen ebenfalls Software, um Bitcoins akzeptieren zu können. Die meisten Kassensysteme ließen sich theoretisch durch ein einfaches Software-Update Bitcoin-tauglich aufrüsten, allerdings gibt es hierfür in der Praxis noch keine Lösung. Stattdessen werden neue Lösungen, die auf Smartphones oder Tablets basieren, angeboten. Die hierfür benötigten Geräte müssen einmalig gekauft werden und verursachen weitere Kosten durch Anschaffung und Wartung. Insgesamt dürfte dies günstiger sein als die restliche POS-Infrastruktur. Bitcoin sind also sowohl für Kunden als auch für Händler sehr preiswert, so dass für beide Sichtweisen jeweils die volle Punktzahl in die Bewertung einfließt. Dies sind fünf Punkte aus Sicht des Kunden und zehn aus Sicht des Händlers, so dass zusammen 15 Punkte angerechnet werden.

Komplexität für den Kunden

Die Komplexität aus Sicht der Kunden, die Bitcoin verwenden möchten, ist zu Beginn vergleichsweise hoch, da Bitcoin ein neues System ist und erlernte Verhaltensweisen des Bezahlens hierauf nicht 1:1 anwendbar sind. Zusätzlich muss sich der Nutzer an eine neue Währung gewöhnen, dessen Wert nicht festgeschrieben ist, sondern ständig variieren kann. Denn eine Ware, die an einem Tag für x Bitcoin ausgeboten wird, kann in diesem Fall günstig oder teuer sein. Hier fehlt es den Nutzern an einem Gefühl für den Wert, das aufgrund der aktuellen Kursschwankungen zudem nur schwer erreichbar sein wird.

Die Einrichtung von Bitcoin ist dagegen erst einmal relativ simpel. Je nach Anforderung wird entweder ein Konto bei einem Dienstleister erstellt oder eine Bitcoin-Software, die Wallets verwaltet, heruntergeladen. Der Download der Software und die Installation sind zügig erledigt. Abhängig von der Bandbreite der Internetverbindung nimmt das Herunterladen der kompletten Blockchain u. U. ein wenig mehr Zeit in Anspruch. Letztere hatte Anfang November 2014 eine Gesamtgröße von über 23 GB (95) und wächst ständig an. Nutzern eines Wallet-Dienstes im Internet bleibt dieser Download erspart, da der Dienst die Blockchain auf seinen Systemen vorhält.

Um mit Bitcoins bezahlen zu können, muss zu Beginn mindestens eine Bitcoin-Adresse erzeugt werden, an die im Anschluss eine beliebig hohe Einzahlung zu tätigen ist. Sie kann über einen der zahlreichen Marktplätze, wie bitcoin.de oder paymium.com, an denen Bitcoins gekauft werden können, oder privat über Freunde und Bekannte, die Bitcoins besitzen, erfolgen. Demnach ist

niemand auf einen der Dienste angewiesen. Die Bezahlung erfolgt immer in einer der Überweisung ähnlichen Form. Über den jeweils genutzten Dienst oder die genutzte Software veranlasst der Zahlungssender die Zahlung an die Adresse des Zahlungsempfängers. Hierfür muss i.d.R. lediglich der Betrag an Bitcoins und die Adresse des Empfängers eingetragen werden.

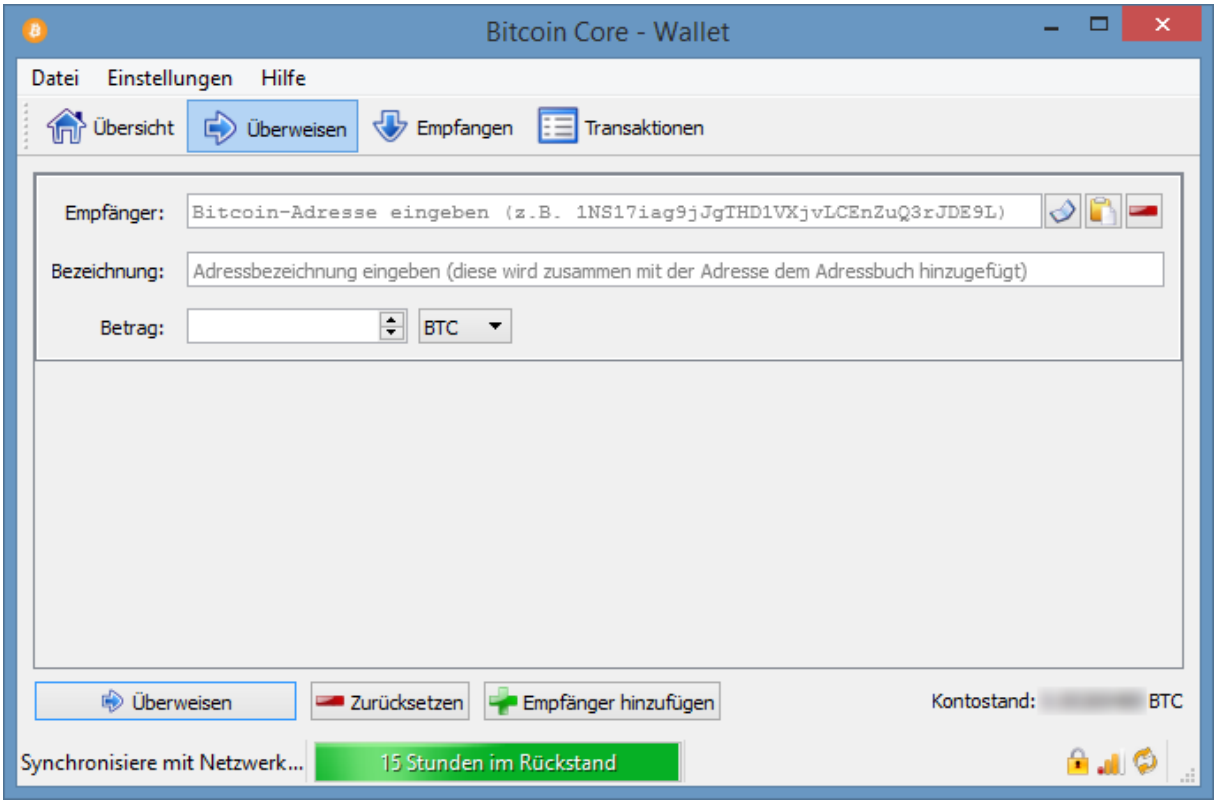

Abbildung 40: Oberfläche des Standard Bitcoin-Clients zum Tätigen einer Überweisung.

Ferner existieren zahlreiche weitere Varianten, wie die Zahlung durch Scan eines QR-Codes, über Debit- und Kreditkarten ähnliche Plastikkarten (307), die Zahlung über Apps, etc.. Grundsätzlich sind hier der Phantasie der Entwickler keine Grenzen gesetzt, was auch eine Integration in PayPal (69) oder andere, bereits existierende Systeme, wie Telekom MyWallet, einschließt. Diese Vielfalt an Bezahloptionen ist für den Nutzer jedoch eine Herausforderung, weil sie dazu führt, dass er mehrere, unterschiedliche Verhaltensweisen erlernen muss, um mit Bitcoin zahlen zu können. Dagegen würde die Integration in andere, bestehende Dienste dieses Problem verhindern, da die Nutzung dieser Dienste oftmals schon bekannt ist und die erlernten Verhaltensweisen dort, wie gewohnt, angewendet werden können.

Abschließend lässt sich festhalten, dass der Einstieg für Otto-Normal-Nutzer in die Welt der Bitcoins derzeit noch vergleichsweise kompliziert ist, weil es sich um ein neues System handelt, an welches sich die Nutzer erst gewöhnen müssen und das, aufgrund seiner Offenheit, viele Möglichkeiten bietet, aus denen jeder die für ihn passende auswählen kann. Hierfür ist letztlich zumindest ein grober Überblick über viele dieser Optionen notwendig. Aus diesen Gründen wird die Komplexität für den Kunden mit sechs von zehn Punkten bewertet, da, nachdem die Auswahl getroffen wurde, die Verwendung relativ einfach ist und schnell erlernt werden kann.

Komplexität für den Händler

Händler müssen vor der Akzeptanz von Bitcoin eine grundsätzliche Entscheidung treffen: Zum einen haben sie die Möglichkeit, Bitcoins zu akzeptieren und in ihrer Wallet zu behalten, was mit allen Vor- und Nachteilen verbunden ist, die dazu gehören. Zum anderen können sie, um Bitcoins zu akzeptieren, einen Dienst, wie Coinbase, nutzen, der Bitcoins sofort in eine Gutschrift in US-Dollar oder Euro auf einem gewöhnlichen Bankkonto zum jeweils gerade gültigen Wechselkurs umwandelt. Vorteil der letzten Variante ist, dass der Händler sich nicht großartig um gesetzliche Regelungen, bspw. zu der Versteuerung von Bitcoins, befassen muss, weil er selbst nie mit Bitcoins in Kontakt kommt. Außerdem wird der Produktpreis in Bitcoin jederzeit anhand des Wechselkurses neuberechnet, damit dem Händler immer dieselbe Menge Euro oder Dollar für ein Produkt zur Verfügung zu stehen.

Ist die Entscheidung gefallen, welche der beiden Varianten eingesetzt werden soll, ist die darauf folgende Integration in bestehende E-Commerce-Systeme in vielen Fällen relativ simpel, denn zahlreiche Plug-ins stehen bereits zur Verfügung. Diese kommen teilweise direkt von Diensten, wie bitpay (308), die ein entsprechendes Händlerkonto voraussetzen, oder von der Bitcoin Community. Ist kein Plug-in verfügbar, ist die Entwicklung definitiv zeit- und kostenintensiv.

Für die Einbindung am POS wird in aller Regel neue Hardware, meist Tablets oder Smartphones, benötigt, weil eine Integration in bestehende Kassensysteme (noch) nicht angeboten wird, obwohl diese technisch machbar wäre. Anbieter, wie coinbase, bitpay oder andere, vermarkten entsprechende Apps für den Händler, über die die Zahlungen abgewickelt werden können. Durch die Offenheit des Systems wäre jedoch auch hier denkbar, eigene Lösungen zu schaffen. Einige Anbieter, wie bspw. coinkite, setzen auf andere Lösungen, bei denen Zahlungen mit Bitcoin über ein Zahlungsterminal, vergleichbar zu denen für die Akzeptanz von Kredit- und Debitkarten, abgewickelt werden können (309). Händler stehen also, genau wie ihre Kunden, vor einer Fülle an Möglichkeiten und Anbietern, die sie, aufgrund unterschiedlicher Kostenstrukturen, sorgfältig miteinander vergleichen sollten, um das für sie beste Angebot auszuwählen.

Der Bezahlvorgang an sich ist, nach einer Eingewöhnungszeit der Kunden, einfach und schnell durchzuführen. Durch die Findung neuer Blöcke im Abstand von ungefähr zehn Minuten, ist die Zahlung auch vergleichsweise zügig. Werden zusätzlich einige Bestätigungen abgewartet, ist die Zahlung immer noch vergleichsweise schnell. Allerdings ist dies für digitale Güter, die am Ende des Bestellprozesses direkt heruntergeladen werden können, schwer durchzusetzen. Hier müssten Kunden mindestens so lang warten, bis die Zahlung in einen Block aufgenommen wurde und der Händler dies geprüft hat, da Letztgenannter ansonsten in Vorleistung tritt und keinerlei Garantie hat, dass die Zahlung auch tatsächlich stattfindet. Alles in allem werden für die Komplexität aus Sicht des Händlers ebenfalls sechs von zehn Punkten verteilt, weil Bitcoins zahlreiche Optionen für Händler bieten, aus denen die optimale erst gefunden werden will. Es dürfte sich aufgrund mangelnder Erfahrung jedoch als schwierig herausstellen, so dass viel Recherchearbeit notwendig ist.

Alleinstellungsmerkmale

Bitcoins bieten jedermann die Option, Zahlungssender und Zahlungsempfänger zu sein. Somit ist es möglich, Geld an jeden Teilnehmer des Netzwerkes zu zahlen, ganz gleich wo sich dieser befindet und das innerhalb von kürzester Zeit. Da hierbei nur minimale Gebühren anfallen, die immer gleich sind, lohnt sich Bitcoin auch für kleinere Transaktionsvolumen in andere Länder, für die normalerweise eine Währungswechsel erforderlich wäre. Für diese P2P-Zahlungsfunktion wird ein weiterer Punkt vergeben.

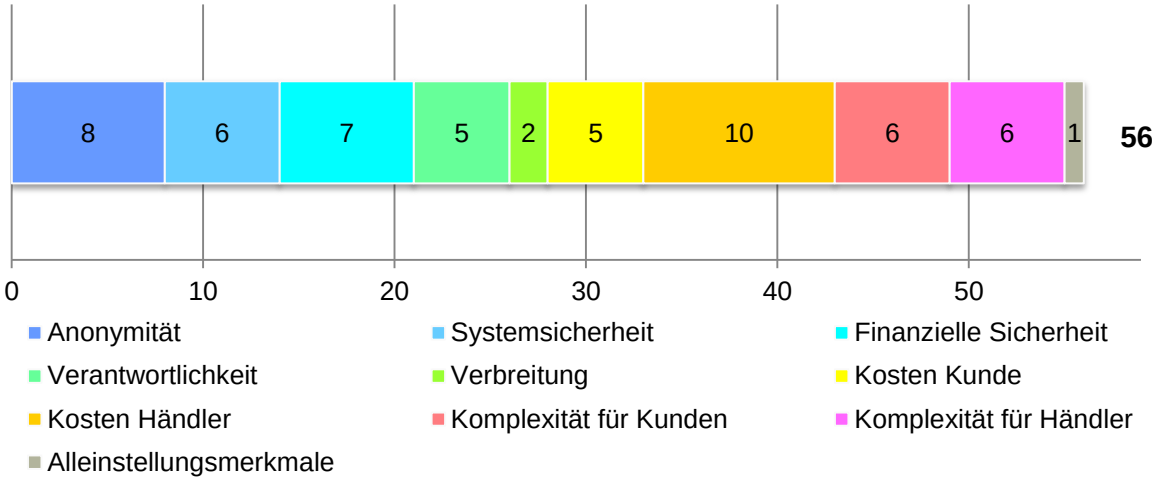

Abbildung 41: Gesamtbewertung des Zahlungssystems Bitcoin.

3.4.2 Ripple XRP

Das Zahlungssystem Ripple XRP, welches im Folgenden bewertet wird, verfolgt eine andere Idee als Bitcoin. Eine Beschreibung dieser Idee erfolgte in Kapitel *1.4.2* Ripple XRP, dessen Lektüre vor dem vorliegenden Kapitel empfohlen wird.

Anonymität

Für die Nutzung des Ripple-Netzwerkes sind als Kunde mehrere Registrierungen notwendig. Zum einen ist ein Wallet erforderlich, welches kostenlos und vollkommen anonym eröffnet werden kann. Hierzu wird der notwendige Client heruntergeladen. Es muss einzig und allein ein Passwort vergeben werden, um ein Wallet zu erstellen, welches in einer zuvor ausgewählten Textdatei gespeichert wird (310). Alternativ kann das Wallet online, unter Angabe von E-Mailadresse und Passwort, erstellt werden (311). Das Wallet bekommt eine Adresse, wie z.B. `rGaEzMD6dmqYDmommvyEZdAiMCD9LDbnT9`, die damit ein Pseudonym des Nutzers darstellt. Die Zuordnung der Adresse zu einer Person kann, wie schon bei Bitcoin, nur der Nutzer selbst machen. Allerdings muss sie gegenüber Personen, denen vertraut werden soll und die einem selber vertrauen möchten, aufgehoben werden. Denn wer will einer Person, die er nicht kennt, schon Geld anvertrauen?

Zusätzlich verlangen die meisten Betreiber eines Gateways ebenso eine Registrierung, die in der Regel umfangreicher ausfällt als für das Wallet. So verlangt beispielsweise SnapSwap.eu einen Identitäts- und Adressnachweis, durch den die Pseudonymität gegenüber SnapSwap jedenfalls aufgehoben wird (312). Laut Angaben der Betreiber ist dies notwendig, um die Richtlinien zur Verhinderung von Geldwäsche einzuhalten. Staaten könnten sich also an die Gatewaybetreiber wenden, deren Zahl (noch) überschaubar ist, um zu ermitteln, welche Ripple-Adresse wem gehört.

Gegenüber Händlern, denen man Zahlungen über das Ripple-Netzwerk zukommen lässt, ist jedoch die Pseudonymität gewährleistet, da sie nur die Ripple-Adresse sehen. Ein Rückschluss auf die Identität ist allein hierdurch nicht möglich. Somit ist die Nutzung von Ripple nur bei bestimmten Verhaltensweisen pseudonym. Wird die Zuordnung der Adresse zur eigenen Person öffentlich bekannt gemacht, kann die Pseudonymität nicht weiter bestehen bleiben. Aus diesem Grund wird dieses Kriterium mit vier von zehn Punkten bewertet.

Systemsicherheit

Die Sicherheit des ganzen Systems basiert auf der Idee der Konsensfindung, die bestimmt, welche Transaktionen in das Last Closed Ledger aufgenommen werden und welche nicht. Eine genauere Analyse dieses Algorithmus liefert das Whitepaper „The Ripple Protocol Consensus Algorithm“, in dem mathematisch erläutert wird, wie hoch das Risiko ist, dass Kartelle mit betrügerischer Absicht die Konsensfindung beeinflussen können, wenn die UNL bestimmte Größen erreicht (313). Hierin wird zudem darauf hingewiesen, dass die Zusammenstellung der UNL ausschlaggebend dafür ist, dass betrügerische Transaktionen verhindert werden können. Es sei ein Mix aus Servern in der UNL anzustreben, der Betreiber mit gegenläufigen Interessen beinhaltet. So ist es z.B. unwahrscheinlich, dass rechtsradikale Gruppierungen, die einen solchen Server betreiben mit einer jüdischen Gemeinde oder linken Gruppierungen zusammenarbeiten, um das Ripple-System zu stören. Wird ein solch ausgewogener Mix erreicht, ist die Manipulation der Konsensfindung für Angreifer äußerst schwierig. Allerdings ist die optimale Zusammenstellung der UNL nur schwer zu erreichen, weil prinzipiell jeder einen solchen Server betreiben kann und sich hierfür nirgends identifizieren muss.

Ein weiterer Schutz für das System ist, dass jedes Wallet eine Reserve von 25 XRP, umgerechnet rund 0,10 €, benötigt, damit er am Ripple-System teilnehmen kann. Hierdurch soll verhindert werden, dass Angreifer unnötig viele oder große Einträge in dem Ledger vornehmen können (314). Zur Vermeidung, dass Angreifer das Netzwerk durch viele kleine Transaktionen versuchen zu überlasten, wird für jede Transaktion eine Gebühr erhoben. Diese liegt standardmäßig bei 0,00001 XRP, umgerechnet also Bruchteile eines Eurocents. Gerät das Netzwerk jedoch aufgrund vieler Transaktionen unter Last, erhöht sich die Gebühr automatisch, so dass ein Angriff durch Überlastung des Netzwerkes den Angreifer teuer bezahlt wird (315).

Die Sicherheit der einzelnen Wallet hängt, wie auch bei PayPal oder ähnlichen Diensten, an der Sicherheit des durch den Nutzer selbst gewählten Passwortes, an das keine großen Anforderungen gestellt werden. Allerdings wird für Nutzer des Walletdienstes rippletrade.com eine optionale Zwei-Faktor-Authentifizierung angeboten, um das Konto zu schützen. Bei Verwendung des heruntergeladenen Ripple Clients wird das Wallet als Textdatei auf dem Rechner abgelegt. Dieses lässt sich zwar nur mit dem zugehörigen Passwort nutzen, dennoch sollten Nutzer auf eine sorgfältige Sicherung achten. Insgesamt ist die Systemsicherheit, abgesehen von der Möglichkeit, schwache Kennworte zu verwenden, die den einzigen Schutz der Wallet darstellen, gegeben. Für eine entsprechende Sicherung des Wallet-Dienstes bzw. der Offline-Wallet-Datei ist der Betreiber bzw. der Nutzer verantwortlich. Somit werden insgesamt acht von zehn Punkten für dieses Kriterium vergeben.

Finanzielle Sicherheit

Unter dem Aspekt der finanziellen Sicherheit sind sich Bitcoin und Ripple sehr ähnlich. Beide bieten sehr schnelle Zahlungen, wobei Ripple noch schneller ist, da keine Bestätigungen abgewartet werden müssen, sondern eine Transaktion auf jeden Fall durchgeführt wurde, sobald sie in einem Last Closed Ledger auftaucht, welches deutlich schneller gebildet wird als ein Bitcoin-Block. Ferner ermöglicht Ripple keine Rückbuchungen, z.B. bei einer falschen Transaktion oder ähnlichem, so dass quasi eine Zahlungsgarantie besteht. Allein der Zahlungsempfänger kann eine Transaktion rückgängig machen, indem er eine neue Transaktion veranlasst.

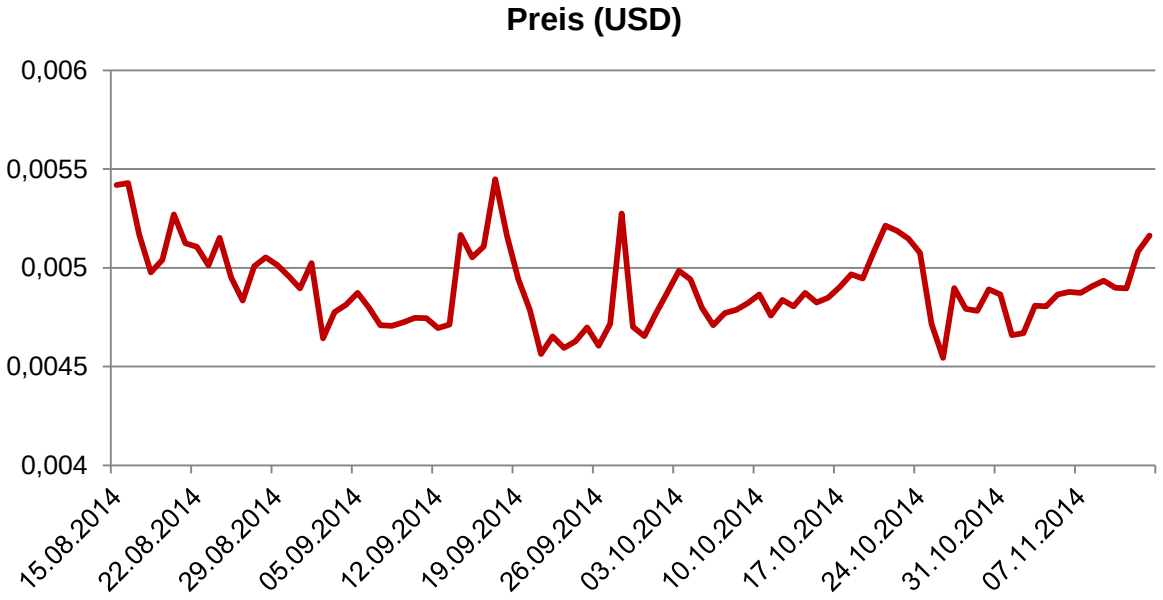

Abbildung 42: Kursverlauf für XRP.

Die Sicherheit des Wallets liegt in der Hand desjenigen, der die Wallet-Datei speichert. Das heißt, dass diese bei Verwendung des downloadbaren Clients in der Verantwortung des Benutzers und

bei Verwendung eines Online-Wallets im Verantwortungsbereich des Betreibers und des Benutzers liegt. Letztgenannter ist in jedem Fall für die Sicherheit des Passwortes zuständig ist.

Die finanzielle Sicherheit hängt außerdem stark davon ab, wem der Nutzer vertraut. Räumt er den falschen Personen einen Kreditrahmen ein, kann dies zu Problemen führen. Im Rahmen eines Beispiels nehmen wir an, dass Alice Bob und Bob Carol vertraut. Über das Ripple-System leiht sich Carol über Bob 50,- € von Alice. Hierdurch verlagert sich das Schuldverhältnis wie folgt: Alice leiht Bob 50,- € und Bob reicht die 50,- € an Carol weiter. Steigt Carol im Anschluss, ohne das Geld an Bob zurückzuzahlen, aus dem System aus, besteht das Schuldverhältnis zwischen den dreien unverändert fort. Verlangt Alice nun die Rückzahlung des Geldes durch Bob, kann Bob diese Forderung begleichen, ohne Aussicht, dass Carol die Forderung begleicht. Bob oder Alice entsteht in jedem Fall ein finanzieller Schaden, weil die Vertrauensverhältnisse nicht sinnvoll gewählt waren.

Wie Bitcoin unterliegen auch XRP Kurschwankungen (vgl. Abbildung 42). Diese sind aber nicht so groß und zudem werden XRP nicht als Zahlungsmittel benötigt, um über Ripple zu handeln. XRP werden lediglich für die Transaktionsgebühren gebraucht. Alle anderen Zahlungen können über gewöhnliche Fiat-Währungen[38] abgewickelt werden, so dass der Wechselkurs nur begrenzt relevant ist, zumal die Transaktionsgebühren angepasst werden, um auf Kursschwankungen zu reagieren. Aus den genannten Gründen werden für dieses Kriterium sechs von zehn möglichen Punkten vergeben, da die Vertrauensbeziehungen sinnvoll und mit Bedacht gewählt werden sollten, damit finanzielle Schäden vermieden werden.

Verantwortlichkeit

Die Software wird durch Ripple Labs und Freiwillige entwickelt, sowie unter Open-Source-Lizenz veröffentlicht. Betrieben werden können Ripple-Server und Gateways prinzipiell durch jeden. Somit handelt es sich bei Ripple, ähnlich wie bei Bitcoin, um ein dezentrales Netzwerk, in das keine Partei allein eingreifen kann, um Teilnehmer davon auszuschließen oder um Transaktionen zu verhindern.

Betreibern einzelner Dienste, wie beispielsweise Gateways, bleibt es allerdings freigestellt, einzelne Nutzer von ihren Dienstleistungen auszuschließen, was im Moment auf Grund der geringen Auswahl solcher Dienste einem Ausschluss von dem System gleich käme. Wächst das Netzwerk künftig weiter, verringern sich die Möglichkeiten, einzelne Nutzer auszuschließen. Es konnte jedoch kein zurückliegender Fall gefunden werden, in dem Nutzer von einer Plattform ausgeschlossen wurden.

[38] Währungen wie der Euro sind sogenannte Fiat-Währungen. Der Begriff leitet sich aus dem lateinischen („es werde“) ab und soll andeuten, dass der Wert einer Währung nicht durch hinterlegte Rohstoffe, wie z.B. Gold, gegeben ist, sondern durch Beschluss eines Staates entsteht, diese Währung als Zahlungsmittel zu verwenden (4).

Durch die geringe Anzahl an Gateways existieren quasi zentrale Punkte. Dies würde sich mit wachsender Verbreitung jedoch ändern, so dass die Verantwortung letztlich in den Händen der Ripple-Community liegt. Demnach unterliegen alle Akteure einer ständigen Kontrolle durch die anderen Teilnehmer, so dass ähnlich wie für Bitcoin, fünf Punkte vergeben werden.

Verbreitung

Die Verbreitung von Ripple ist derzeit noch äußerst gering. Die International Ripple Business Association listet auf ihrer Homepage nur wenige Ripple-Gateways. Market Makers und Marktplätze zum Kaufen und Verkaufen von XRP sind noch weniger gelistet (316–318).

Auch die Anzahl der Händler, die XRP akzeptieren, ist sehr gering. Eine Liste der International Ripple Business Association enthält gerade einmal drei Einträge von Händlern, die Zahlungen via Ripple akzeptieren (319). Ein Einsatz von Ripple als Zahlungssystem ist derzeit also nur sehr eingeschränkt möglich.

Um die Nutzbarkeit im Zahlungsverkehr zu erhöhen, ist der Gatewaybetreiber SnapSwap eine Kooperation mit Visa eingegangen, aus der die SmartyCash Visa Card hervorgegangen ist. Sie verbindet eine Ripple-Wallet mit einer Prepaid-Kreditkarte, die überall dort eingesetzt werden kann, wo Karten von Visa akzeptiert werden. Gegen ein Entgelt kann diese erworben werden und bringt dem Kunden pro Transaktion eine Rückvergütung von fünf Prozent, die er in seinem Ripple Wallet gutgeschrieben bekommt (320). SnapSwap zeigt so, dass sich Ripple und andere Zahlungssysteme ergänzen können. Es wird ein Weg aufgezeigt, über den sich Ripple künftig besser etablieren könnte. Aufgrund der derzeit begrenzten Einsatzmöglichkeiten, aber der Aussicht auf Verbesserung durch Ideen wie die SmartyCash Visa Card wird für dieses Kriterium ein Punkt vergeben.

Kosten

Die Kosten für die Nutzung des Ripple-Netzwerkes als Nutzer sind relativ gering. Um einen neuen Account zu validieren, ist eine Aufladung von 20 XRP erforderlich. Das entspricht gleichzeitig der Reserve an XRP, die jedes Ripple-Konto aufweisen muss. Erst nach der Gutschrift von 20 XRP ist der Account aktiviert und es können Gateways hinzugefügt, sowie das Netzwerk genutzt werden. Dieses Vorgehen ist sowohl für Händler als auch für Kunden notwendig (321).

Für die Nutzung benötigt der Kunde keine spezielle Hard- oder Software, so dass hierfür keine zusätzlichen Kosten anfallen. Es entstehen lediglich Gebühren für einzelne Transaktionen. Diese gestalten sich variabel: Zum einen gibt es einen fixen Anteil, der unregelmäßig angepasst wird, damit die Transaktionskosten bei einem Wertzuwachs von XRP nicht zu hoch ansteigen. Zum anderen gibt es eine variable Gebühr, die sich anhand der Auslastung des Ripple-Netzwerkes bestimmt (315).

Weitere Mehraufwendungen fallen ggf. beim Wechsel von Währungen an, die auf dem Weg zum Zahlungsempfänger notwendig sind. Sie werden durch die Market Makers festgelegt und müssen pro Transaktion individuell betrachtet werden. Im Vergleich zu anderen Systemen sind diese Gebühren jedoch eher gering.

Für Kunden, die Zusatzdienste wie die SmartyCash Visa Card nutzen, entstehen unter Umständen weitere Ausgaben, die der Dienstanbieter erhebt. Die Aufwendungen für die erwähnte Karte bewegen sich dabei im Rahmen normaler Kreditkarten, wobei der Nutzer durch die genannten Rückvergütungen, einen Teil dieser Kosten erstattet bekommt. Somit kann der Nutzer die entstandenen Auslagen bei ausreichender Nutzung erstattet bekommen (322). Aus Sicht des Kunden ist Ripple also ein sehr günstiges System, so dass fünf Punkte vergeben werden.

Aus Sicht des Händlers unterscheiden sich die Kosten nicht großartig. Für die Akzeptanz am POS wird im Ripple Wiki noch keine Lösung genannt, jedoch böte sich eine zu Bitcoin vergleichbare Lösung über QR-Codes und Smartphones / Tablets an. Für eine Einbindung in E-Commerce-Systeme bietet das Ripple Wiki bereits eine Anleitung an (323, 324). Notwendig ist die Installation des Ripple-Servers, der als Open-Source-Software kostenfrei angeboten wird, so dass an dieser Stelle keine zusätzlichen Kosten anfallen. Die Kosten sind ebenso, wie bei den Kunden, sehr gering. Aus Sicht des Händlers wird demnach die volle Punktzahl von zehn Punkten vergeben, so dass die Kosten insgesamt mit 15 Punkten bewertet werden.

Komplexität für Kunden

Das Ripple-System ist insgesamt sehr komplex und für Einsteiger schwer zu verstehen, zumal es bisher medial wenig Aufmerksamkeit erregt hat, weshalb auch nur wenige Erläuterungen zur Verfügung stehen. Außerdem werden Begrifflichkeiten in den Dokumentationen nicht eindeutig verwendet. Beispielsweise heißen XRP auch Ripples und damit fast genauso wie das Netzwerk.

Die Registrierung für ein Wallet ist dagegen allgemein sehr einfach, da lediglich eine E-Mailadresse und ein Passwort angegeben werden muss. Die Validierung der Mailadresse sollte, wie bei vielen anderen Diensten, für keinen Nutzer ein Hindernis darstellen. Schwieriger wird die Aktivierung des Wallets durch Aufladung von mindestens 20 XRP. Zwei Wege sind möglich: Zum einen kann ein Ripple-Nutzer dem Neueinsteiger die benötigten Ripples durch Überweisung schenken oder der Nutzer verwendet Bitcoins für die Aktivierung. Hierbei kann er die Bitcoin an eine eigens generierte Bitcoin-Adresse überweisen, um sie als XRP in der Wallet gutschreiben zu lassen. Rippleunion bietet außerdem die Möglichkeit, die notwendige Aufladung vorzunehmen, indem eine kanadische Amazon Geschenkkarte an Rippleunion übertragen wird (321).

Sind die Registrierung und Aktivierung des Wallets abgeschlossen, kann Ripple theoretisch genutzt werden. In der Praxis werden jedoch noch Vertrauensbeziehungen zu mindestens einem Gateway benötigt, um Ein- und Auszahlungen durchführen zu können. Die Registrierung bei ei-

nem Gatewaybetreiber, die von vielen Anbietern erwartet wird, ist dabei aber oftmals komplizierter. Das Gateway SnapSwap EU verlangt beispielsweise sowohl einen Identitäts- als auch einen Wohnsitznachweis (312), während andere Gateways weniger Daten benötigen (325). Das hängt jedoch vom Sitz des Gateway-Betreibers und den dort geltenden gesetzlichen Bestimmungen ab, so dass keine generelle Aussage über die Komplexität dieses Vorgangs getroffen werden kann.

Nach der Einrichtung der Gateways und Beziehungen mit den jeweiligen Vertrauenslimits, kann Ripple für Zahlungen genutzt werden. Diese funktionieren, ähnlich wie bei Bitcoin, durch die Eingabe der Empfangsadresse, der Auswahl der Zielwährung und des zu zahlenden Betrags. Durch entsprechende QR-Codes und Apps (326), mit denen diese gescannt werden, können Zahlungen ebenso getätigt werden, wie über Kartensysteme, z.B. die SmartyCash Visa Card (320). Aber an die meisten dieser Bezahlvorgänge wird sich der Kunde neu gewöhnen und diese erlernen müssen. In Summe werden, aufgrund des schwer durchschaubaren Systems, der langwidrigen Einrichtung und der zum Teil gewöhnungsbedürftigen Zahlungsabläufe, vier Punkte vergeben. Positiv wird gesehen, dass weder spezielle Hard- noch Software benötigt werden und sich auch bekannte Bezahlverfahren, wie Kreditkarten, in das System integrieren lassen.

Komplexität für Händler

Der Einstieg für Händler in das System ist ähnlich kompliziert, wie für Kunden, weil für sie das System ebenfalls schwer zu verstehen sein wird. Nachteilig ist auch, dass bisher keine Lösung für die Akzeptanz am POS existiert. Hierfür können künftig bspw. ähnliche Apps wie für Bitcoin, verwendet werden. Integrieren Hersteller von POS-Systemen auch Ripple, könnte der QR-Code, genau wie bei Yapital, auf dem Bezahlterminal oder einem anderen Bildschirm am POS angezeigt werden. Der Bezahlvorgang ließe sich dadurch vergleichsweise schnell abwickeln.

Für Zahlungen im Internet wird im Wiki von Ripple Labs beschrieben, dass ein rippled[39] Server eingerichtet werden muss. Außerdem wird ein Account bei einem Gateway benötigt, um Zahlungen auszahlen zu können. Für die Integration als Bezahloption in einem Onlineshop wird, aufgrund der geringen Verbreitung, in den meisten Fällen ein eigenes Plug-in geschrieben werden müssen (328). Die technischen Anforderungen sind damit höher als für Bitcoin, da ein vollständiger Ripple Server benötigt wird und eigene Plug-ins zur Integration in bestehende Systeme entwickelt werden müssen. Zahlungen lassen sich insgesamt aber schneller als bei Bitcoin durchführen, weil alle paar Sekunden ein Konsens über ein Ledger gefunden wird. Bei Bitcoin findet sich dagegen nur ungefähr alle zehn Minuten ein Block und gegebenenfalls müssen noch weitere Blöcke abgewartet werden. Die Komplexität ist deshalb für Händler ziemlich hoch, die Geschwindigkeit dafür allerdings auch, so dass für dieses Kriterium drei Punkte vergeben werden.

[39] rippled ist die Serversoftware des Ripple-Netzwerkes. Sie ist u.a. zuständig für die Validierung eines Ledgers und leitet Nachrichten innerhalb des Netzwerkes an andere Teilnehmer weiter (327).

Alleinstellungsmerkmal

Ähnlich, wie bei vielen anderen Systemen, bietet auch Ripple die Möglichkeit, Zahlungen direkt zwischen Nutzern durchzuführen. Diese können sowohl über kleine Summen als auch über große Entfernungen durchgeführt werden.

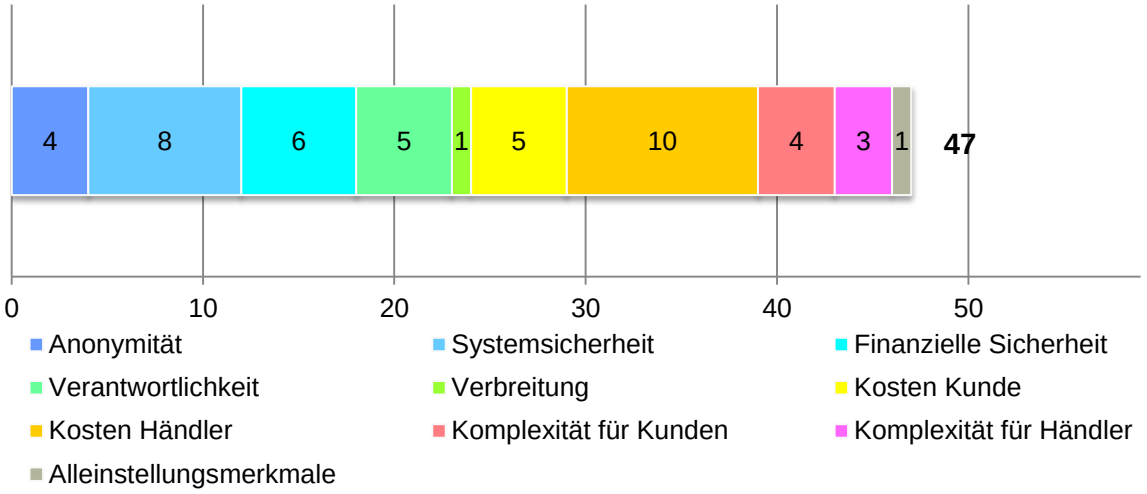

Abbildung 43: Gesamtbewertung des Zahlungssystems Ripple XRP.

3.4.3 Peercoin (PPC)

Peercoin ist in vielen Dingen sehr ähnlich aufgebaut wie Bticoin, weshalb die Bewertung einiger Kriterien gleich ausfällt. Diese werden im Folgenden deshalb nicht noch einmal betrachtet und können in Kapitel *3.4.1 Bitcoin (BTC)* nachgelesen werden.

Systemsicherheit

Die Sicherheit bei Peercoins gestaltet sich in großen Teilen sehr ähnlich zu Bitcoins. Das Mining, wie es von Bitcoin bekannt ist, existiert bei Peercoin ebenso. Jedoch sind in Peercoin weniger Miner involviert, so dass die Rechenleistung innerhalb des Peercoin-Netzwerkes deutlich geringer ist als die im Bitcoin-Netzwerk. Am 10. November 2014 lag der Schwierigkeitsgrad für das Mining bei Peercoin deshalb gerade einmal bei ungefähr 13, während die Schwierigkeit zur selben Zeit für Bitcoin bei 39.603.666.252,42 lag (329, 330)

Würden nun einige Bitcoin-Miner beginnen, Peercoin zu minen würden diese ziemlich sicher mehr als 50% der Rechenleistung des gesamten Netzwerkes stellen und dadurch das Netzwerk kontrollieren können. Damit das verhindern wird, existiert neben dem Mining noch das Minting. Um einen ähnlichen Angriff durchzuführen, müsste der Angreifer, wie zuvor erwähnt, mehr als 50% der im Netzwerk vorhandenen Rechenleistung stellen und gleichzeitig mehr als 50% aller vorhandenen Peercoins besitzen. Ein Angriff hätte sehr sicher einen starken Kursverlust zur Folge, der den Angreifer und seine Peercoin auch treffen würde. Somit ist ein derartiger Angriff un-

wahrscheinlicher und schwieriger als bei Bitcoin. Künftig ist es möglich, dass das Mining vollständig entfällt und nur noch Minting verwendet wird. Für den Beginn ist das Mining jedoch sinnvoll, um rasch eine größere Menge Coins erzeugen und in Umlauf bringen zu können.

Der Diebstahl einer Wallet ist bei Peercoin ebenso möglich wie bei Bitcoin, so dass sich bei der restlichen Bewertung keinerlei Unterschiede ergeben. Durch oben beschriebene zusätzliche Sicherheit werden acht Punkte vergeben.

Finanzielle Sicherheit

Auch die finanzielle Sicherheit ist sehr ähnlich zu Bitcoin. Alle getätigten Aussagen treffen äquivalent auf Peercoin zu. Allerdings ist der Verlauf des Wechselkurses ein anderer, weil Peercoins einen deutlich geringeren Wert haben als Bitcoins. Der Kurs ist ähnlich volatil, jedoch prozentual noch stärker schwankend. So verringerte sich der Kurs innerhalb des letzten halben Jahres auf weniger als die Hälfte.

Abbildung 44: Verlauf des durchschnittlichen Preises eines Peercoin in Euro.

Die Bewertung der finanziellen Sicherheit muss deshalb genauso ausfallen wie bei Bitcoin. Unter Beachtung dieses Aspekts werden auch für Peercoin sieben von zehn Punkten vergeben.

Verbreitung

Die Verbreitung von Peercoin ist derzeit noch stark beschränkt. Im Vergleich zu Bitcoin gibt es noch weniger Handelsplätze und Akzeptanzstellen. Eine Übersicht über verschiedene Dienste liefert das zu Peercoin gehörige Wiki unter https://github.com/ppcoin/ppcoin/wiki/List-of-services-

on-market. Im Unterschied zu Bitcoin ist allerdings derzeit keine Akzeptanz am POS bekannt, obwohl dies theoretisch ebenso möglich wäre wie bei Bitcoin.

Alternative Coins, wie Peercoin, genießen trotz oder gerade wegen ihrer Vielzahl eine medial deutlich geringere Aufmerksamkeit als Bitcoins, weshalb davon auszugehen ist, dass die Verbreitung auch in nächster Zeit nicht stark zunehmen wird. Vielmehr wird sich Peercoin gegen eine Vielzahl anderer Systeme durchsetzen müssen, wobei die Unterschiede nur technisch versierten Nutzern verständlich sind. Ein Ranking von CoinMarketCap zeigt, dass alle anderen Systeme hinter Bitcoin deutlich abgeschlagen sind (331). Insgesamt wird die Verbreitung deshalb mit null Punkten bewertet.

Kosten

Hinsichtlich der Kosten unterscheiden sich Bitcoin und Peercoin etwas. Während Bitcoin Transaktionskosten nur optional und nach Belieben des Zahlungssenders erwartet, sind die Gebühren bei Peercoin fix auf 0,01 Peercoin pro Transaktion (Gegenwert am 10.11.2014: ca. 0,0062 €) festgelegt. Auf diese Weise sollen unnötige Transaktionen, die einen Angriff auf die Funktionsfähigkeit des Systems darstellen können, vermieden werden. Die Kosten einer Transaktion sind also sehr niedrig. Steigt der Wechselkurs jedoch, bleiben die Transaktionskosten bei 0,01 Peercoin, die dann entsprechend mehr wert sind. Im Unterschied zu Bitcoin existieren auch noch keine Wallet-Dienste, die Gebühren erheben könnten. Wenn diese künftig starten sollten, werden die Gebühren aber vermutlich im selben Bereich liegen wie bei Bitcoin.

Aus Sicht der Händler fallen ebenfalls nur die Transaktionsgebühren an. Kosten, um die Akzeptanz am POS zu ermöglichen, entstehen zudem für die benötigte Hardware – ein Smartphone oder Tablet. Entsprechende Apps sind bisher nur für Android verfügbar. Eine Integration in bestehende Kassensysteme ist technisch möglich, wird aber bisher nicht angeboten. Die Kosten sind, trotz aller Unterschiede, vergleichbar mit denen für Bitcoin, so dass auch die Bewertung von insgesamt 15 Punkten übernommen werden kann.

Komplexität für Händler

Die Komplexität für Händler ist im Vergleich zu Bitcoin deutlich komplizierter, da keine Dienstleister äquivalente Dienstleistungen, wie bei Bitcoin, anbieten. Zahlungen müssen durch den Händler also direkt abgewickelt werden. Auf der offiziellen Peercoin-Homepage stellen die Entwickler eine Anleitung zur Verfügung, wie Peercoins im Internet akzeptiert werden können. Hierbei wird empfohlen eine hohe Anzahl von Peercoin-Adressen zu generieren und pro Transaktion eine Adresse zu verwenden, um die verschiedenen Zahlungen unterscheiden zu können (332).

Die benötigten Plug-ins zur Einbindung in E-Commerce-Systeme müssen jedoch selbst entwickelt werden und auch die Auszahlung in Euro, die bei Bitcoin durch Anbieter, wie Coinbase,

angeboten wird, ist selbst zu organisieren werden. Auf diese Weise empfängt der Händler selbst Peercoins, so dass er für die Einhaltung gesetzlichen Regelungen und steuerlichen Verpflichtungen nachkommen muss. Es steigt also der Aufwand für den Händler, da er vieles manuell erledigen und die notwendige Software selbst entwickeln muss. Daher wird dieses Kriterium mit einem Punkt bewertet.

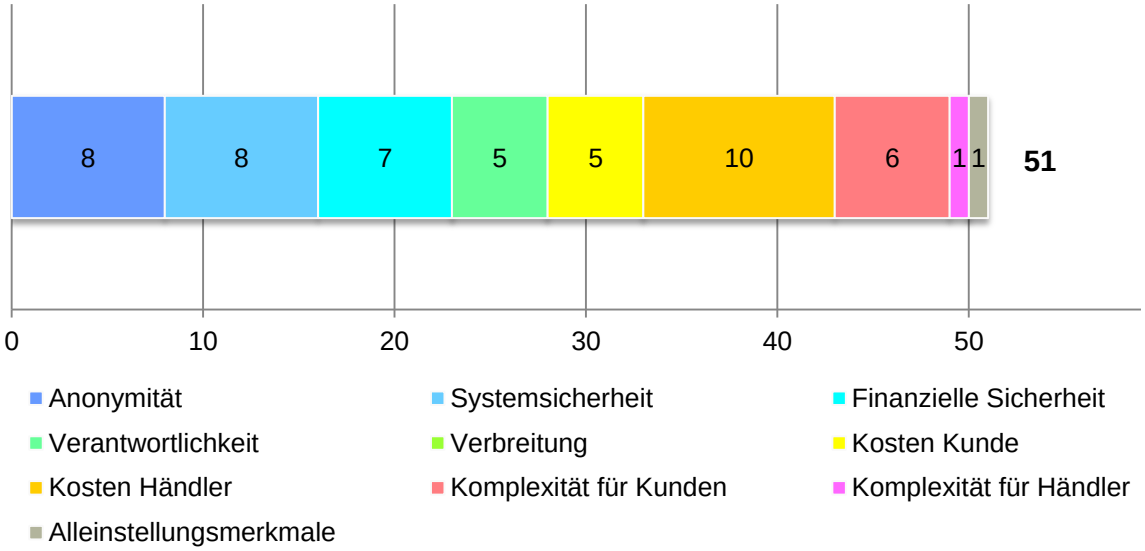

Abbildung 45: Gesamtbewertung des Zahlungssystems Peercoin.

3.5 Zusammenfassung aller Bewertungen

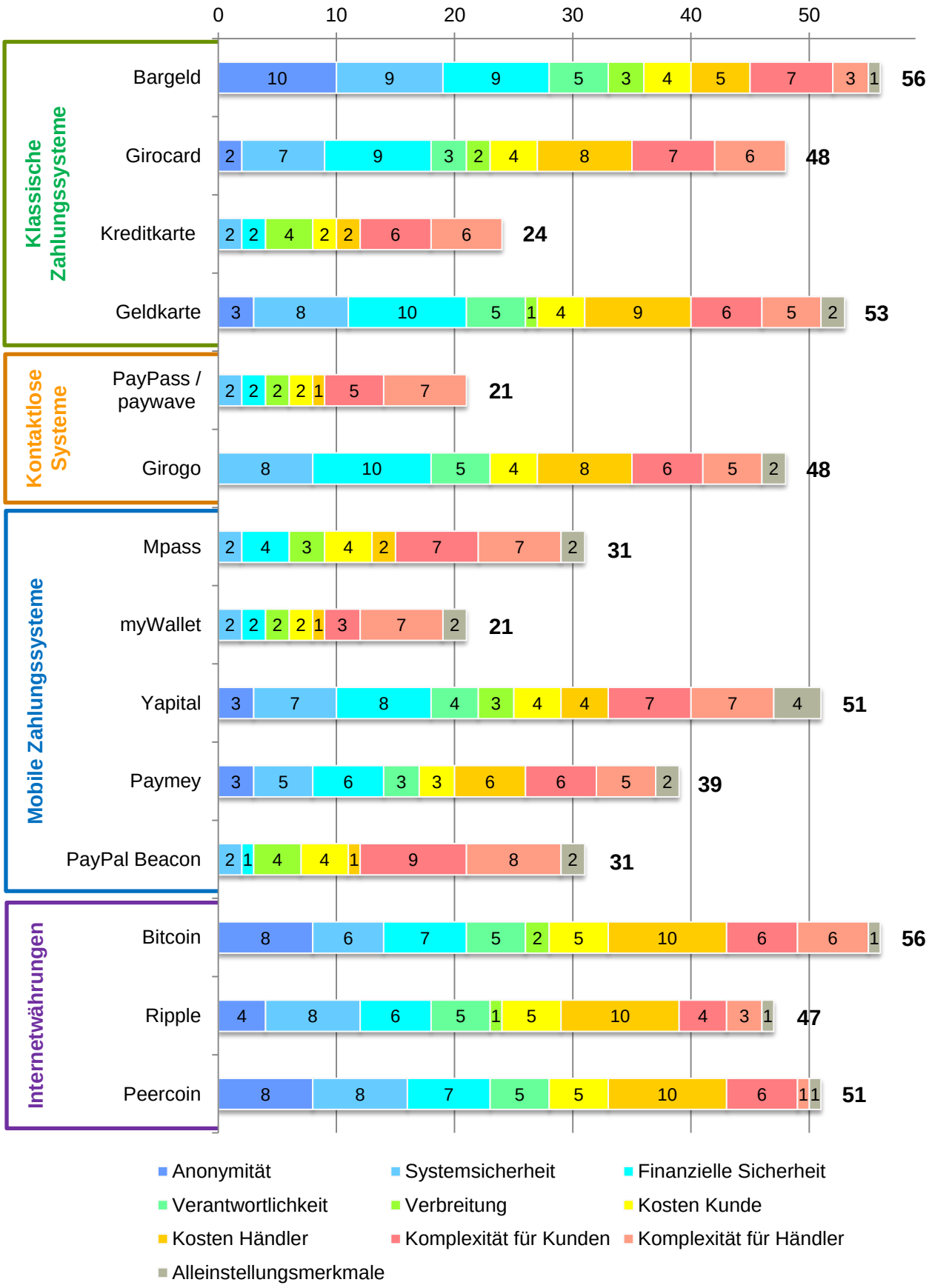

Abbildung 46: Zusammenfassung der Bewertungen aller Zahlungssysteme.

Die Übersicht aller Bewertungen zeigt, dass alle Zahlungssysteme Stärken und Schwächen haben. Keines der Systeme erreicht die Höchstpunktzahl von 80 Punkten. Selbst die am höchsten bewerteten Systeme erreichen nur 70% der maximal möglichen Gesamtpunktzahl. Es existiert also kein perfektes Zahlungssystem, welches alle Bedürfnisse vollkommen erfüllt. Dies war jedoch zu erwarten, da die Interessen zum Teil gegenläufig zueinander sind und somit niemals alle vollständig durch ein System abgedeckt werden können.

Auffällig ist jedoch, dass gerade die klassischen Systeme in den Kriterien ausgeprägte Schwächen haben, die den Kunden besonders wichtig sind (vgl. *2.1 Bedürfnisse der Kunden*). So ist keines der Systeme auch nur ansatzweise anonym und erfüllt den Wunsch der Kunden. Stattdessen wird hier deutlich, dass gerade die Händler und Staaten ihre Interessen, bei diesen Systemen deutlich durchgesetzt haben. So wird auch klar, weshalb gerade die Staaten, durch gesetzliche Regelungen, gegen neue Internetwährungen wie Bitcoin und Peercoin arbeiten, denn diese erfüllen den Wunsch der Nutzer sind vergleichsweise anonym. Einzig Bargeld fällt von den klassischen Zahlungssystemen durch dieses Raster und ist dieser Wertung folgend das anonymste aller Systeme. Die hohe Verwendung, 82% aller Zahlungen am POS werden laut einer Studie der Bundesbank mit Bargeld durchgeführt (7), lässt darauf schließen, dass dies auch vielen Deutschen bewusst ist und sie dieses Zahlungsmittel deshalb ganz bewusst wählen, denn ihnen ist ebenso bewusst, dass Bargeld in Sachen Anonymität die anderen klassischen Systeme bei weitem übertrumpft (333).

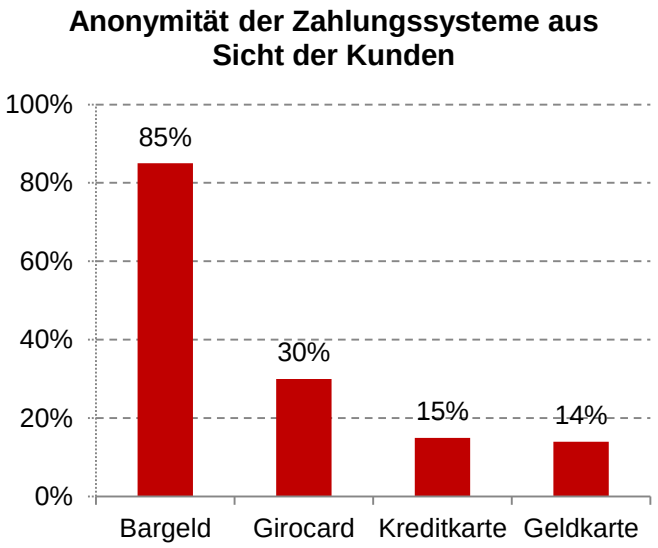

Abbildung 47: Erfüllung der Kriterien für Zahlungsinstrumente durch die einzelnen Instrumente aus Nutzersicht.

Letztlich wird es eine Frage des Drucks der Nutzer sein, ob die Beschränkungen und Hindernisse die Internetwährungen auferlegt werden, künftig aufgehoben werden. Gründe weshalb die anderen Systeme trotzdem Verwendung finden, dürften zum einen Bequemlichkeit und Unwissenheit und zum anderen Alternativlosigkeit sein. Gerade im Interneteinsatz sind derzeit keine anonymen Systeme verbreitet. Hier muss zwangsläufig auf eines der Systeme zurückgegriffen werden, die in dieser Wertung schlecht abschnitten. Internetwährungen, wie Bitcoin und Peercoin, die recht anonym und für den Interneteinsatz konzipiert sind, bieten derzeit nur wenige Händler an, wofür vermutlich in vielen Fällen die rechtlichen Unsicherheiten verantwortlich sein dürften. Im Einsatz am POS gilt natürlich ähnliches, hier kann allerdings auf eben die anonyme Zahlung mit Bargeld zurückgegriffen werden. Das dies nicht immer passiert, liegt in vielen Fällen wohl daran, dass

Kunden nicht immer erst einen Geldautomaten aufsuchen und dann das Bargeld bei sich tragen möchten. In diesen Fällen siegt die Bequemlichkeit der Nutzer und führt dazu, dass nicht anonyme Zahlungssysteme verwendet werden. Auch hält immerhin fast jeder dritte Deutsche die girocard für anonym. Solche Fehleinschätzungen dürften zum Teil jedenfalls auch mitverantwortlich für die Verwendung sein.

Weiterhin ist es Pflicht, dass ein vielfach eingesetztes System, möglichst einfach verwendet werden kann. Dies wird in der Bewertung vor allem durch die Kriterien der Komplexität für Händler und Kunden ausgedrückt. Zahlungssysteme, bei denen das Bezahlen schwierig ist oder komplexe Handlungen erfordert, haben es schwer sich durchzusetzen und Verwendung zu finden, da sie für den Kunden zu Frustration führen, die mit dem Händler assoziiert wird. Dies ist niemals im Sinne desselben, so dass er darauf achten wird, nur einfache Systeme anzubieten. Systeme hinter denen zentrale Instanzen stehen, werden deshalb große Anstrengungen daran setzen, dass das Bezahlen möglichst einfach ist. Bei Community-getriebenen Entwicklungen, wie eben den Internetwährungen, steht die Einfachheit nicht immer im Fokus und wird erst später hinzugefügt. Auch dies ist ein Grund, weshalb es gerade Ripple schwierig fallen wird sich im Endkundengeschäft durchzusetzen.

Ferner ist auffällig, dass gerade die Kreditkarte, als eines der beliebteren Systeme, mit am wenigstens Punkte erhalten hat. Die Verwendung der Kreditkarte dürfte auf ihre einfache Verwendbarkeit und Verbreitung, sowohl am POS als auch im Internet, zurückzuführen. Sie ist das einzige Zahlungsmittel, das nahezu überall akzeptiert wird und bietet dem Nutzer deshalb die Sicherheit, niemals in die Verlegenheit zu kommen, kein akzeptiertes Zahlungsmittel zur Hand zu haben. Gerade wenn der Blick auf die internationale Einsetzbarkeit gerichtet wird, bietet die Kreditkarte diese Sicherheit als eines der wenigen Systeme.

Indes sind auch die guten Bewertungen von Bitcoin, die punktgleich mit der Wertung für Bargeld die beste Wertung ist, und Peercoin in fast allen Kategorien auffällig. Das gute Abschneiden in vielen Kategorien bietet das Potenzial, dass sich gerade diese Systeme künftig etablieren und von Kunden sowie Händlern akzeptiert werden, wenn diese die Vorteile erkennen. Fraglich ist jedoch die Positionierung der Staaten hierzu, denn diese haben den Einfluss diese Zahlungssysteme langfristig zu behindern und ihren großflächigen Einsatz zu unterdrücken. Aus der Perspektive von Staaten betrachtet sind die bewerteten Internetwährungen allerdings besser zu überwachen als Bargeld, da alle Transaktionen in einer Blockchain oder einem Ledger öffentlich zugänglich sind. Die Zuordnung dieser Transaktionen zu Nutzern, ist ein Aufwand, den staatliche Stellen bewältigen müssten, der aber nicht unmöglich ist, wie ein Forscherteam am Beispiel von Bitcoin zeigte (287).

3.6 Fazit

Grundsätzlich lässt sich festhalten, dass, neben den vorgestellten Systemen in den Kategorien mobile Zahlungssysteme und Internetwährungen, noch zahlreiche andere Systeme existieren. Jedes dieser, sowie die vorgestellten Systeme bieten ihre eigenen Vor- und Nachteile. In Summe muss jeder, sowohl Kunde als auch Händler, überlegen, welches System ihm die meisten Vorteile bringt und mit welchen Nachteilen er zugleich am ehesten leben kann.

Ungeachtet dessen kann festgehalten werden, dass die kontaktlosen Systeme und einige der mobilen Zahlungssysteme aufgrund der verwendeten Technik ausschließlich am POS eingesetzt werden können. Jedoch existieren oftmals Lösungen, um zudem den Interneteinsatz zu ermöglichen. Dies sind zu einem großen Teil klassische Zahlungssysteme, für die zusätzlich Karten ausgegeben werden. Mobile Zahlungssysteme, wie PAYMEY und Yapital, die mit QR-Codes arbeiten, können auch für das Online-Shopping verwendet werden.

Durch die stetig steigende Verbreitung von Smartphones (334), steigt auch die Anzahl potentieller Nutzer mobiler Zahlungssysteme. Laut einer Erhebung von Google nehmen rund 64% der Smartphone-Nutzer ihr Gerät immer mit, wenn sie das Haus verlassen (335). Das Smartphone, welches für viele einen ständigen Begleiter darstellt, könnte also künftig das Portemonnaie ablösen. Die Vorteile für den Kunden liegen dabei auf der Hand, denn durch den Einsatz des Smartphones als Zahlungsmittel entfällt die Notwendigkeit, zusätzlich noch einen Geldbeutel mitzunehmen, den, wie die Gründungsgeschichte von PAYMEY zeigt, einige Menschen hin und wieder vergessen. Auch ist die Durchführung des Bezahlvorgangs in vielen Fällen schneller als bei Zahlungen mit Bargeld, weil das Abzählen von Kleingeld entfällt.

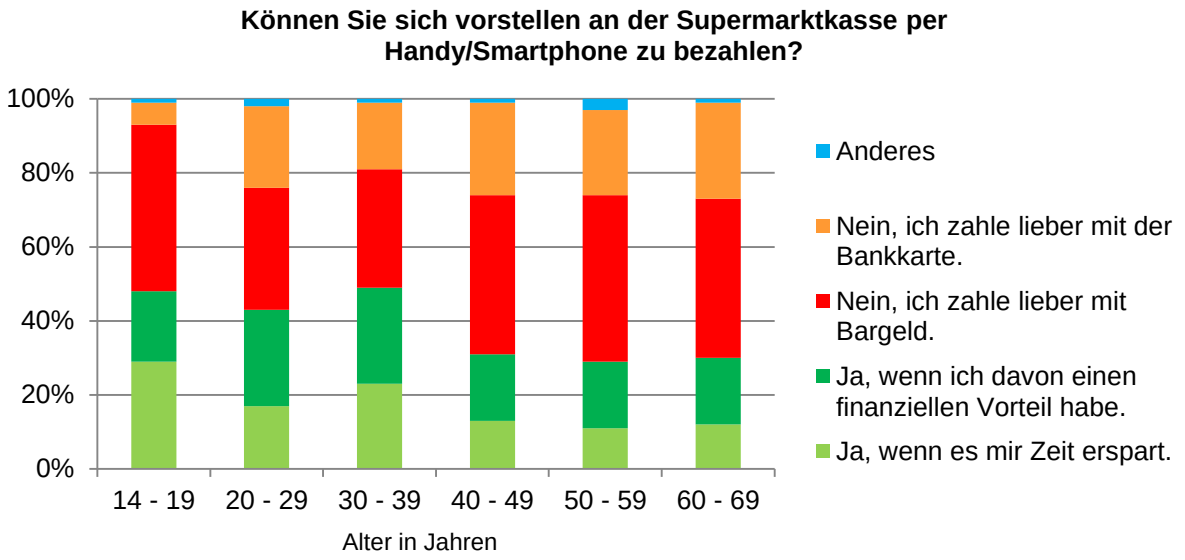

Abbildung 48: Umfrage zur künftigen Nutzung von mobilen Zahlungssystemen.

Eine repräsentative Umfrage der Respondi AG zeigt, dass sich mittlerweile auch viele Deutsche vorstellen können ein solches System zu nutzen, so dass für die Zukunft mit einem Durchbruch gerechnet werden kann.

Ein Nachteil mobiler Zahlungssysteme ist allerdings ihre Vielfalt. Künftig wird sich vermutlich eine Handvoll Lösungen etablieren, die den Bedürfnissen von Kunden und Händlern am besten entsprechen und den größten Zusatznutzen bieten. Vermutlich wird dies keine reine Prepaid-Lösung sein, da diese zusätzlichen Aufwand für den Kunden bedeuten. Bisherige Versuche Prepaid-Lösungen, wie die GeldKarte, zu etablieren, scheiterten an fehlender Begeisterung der Kunden. Denn obwohl es zahlreiche Akzeptanzstellen gibt, quasi jeder Bankkunde eine GeldKarte besitzt und entsprechendes Marketing betrieben wurde, findet die GeldKarte kaum Verwendung (7, S. 41).

Auch die Internetwährungen können durch die Entwicklung entsprechender Apps wie mobile Zahlungssysteme eingesetzt werden. Da zentrale Stellen entfallen, sowie auf ein eigenes Zahlungsnetzwerk gesetzt wird, ergeben sich niedrigere Gebühren und die Abgabe der Verantwortung in eine Community, die die Entwicklung des Systems steuert. Damit trotzdem ein Einsatz im größeren Rahmen ermöglicht wird, zum einen gesetzliche Regelungen für diese Systeme gefunden werden und zum anderen müssen die Systeme einfacher gestaltet werden, so dass sie massentauglich einsetzbar sind. Besonders Ripple scheitert im Moment an letzterem.

Ein großes Problem auf dem Weg zur Etablierung neuer Systeme ist allerdings immer, dass sowohl Kunden als auch Händler gerne auf weit verbreitete Lösungen setzen. Denn Kunden bevorzugen ein Verfahren, das ihnen die Zahlung an möglichst vielen Akzeptanzstellen ermöglicht, und Händler investieren nur in ein neues System, wenn sie ausreichend Kunden erreicht werden. Diese gegenläufigen Interessen machen es erforderlich, dass sich auf beiden Seiten begeisterte Nutzer finden lassen, die mit der Integration des Systems beginnen und auf diese Weise als Multiplikatoren auftreten, die andere von Nutzer von den Vorteilen ihres Systems überzeugen können.

Literaturverzeichnis

1. *BIBLIOGRAPHISCHES INSTITUT GMBH. Zahlungssystem, 2014. http://www.duden.de/node/710871/revisions/1192850/view (abgerufen am: 26. November 2014).*

2. *WIKIPEDIA. Zahlungsverfahren, 2014. 14. November 2014. http://de.wikipedia.org/w/index.php?oldid=135807798 (abgerufen am: 26. November 2014).*

3. *COMMERZBANK AG. Glossar: Gesetzliches Zahlungsmittel. https://www.commerzbank.de/portal/de/privatkunden/service-und-hilfe/glossar/G.html (abgerufen am: 11. August 2014).*

4. *DEUTSCHE BUNDESBANK. Geld und Geldpolitik. 2014. Auflage. Frankfurt am Main, 13. Mai. 2014.*

5. *DIE DEUTSCHE KREDITWIRTSCHAFT. "electronic cash" nun "girocard". http://www.die-deutsche-kreditwirtschaft.de/dk/zahlungsverkehr/kartengestuetzter-zahlungsverkehr/girocard.html (abgerufen am: 13. Mai 2014).*

6. *EINECKE, H. Girocard löst EC-Karte ab, 2010. http://www.sueddeutsche.de/geld/banken-girocard-loest-ec-karte-ab-1.211309 (abgerufen am: 13. Mai 2014).*

7. *DEUTSCHE BUNDESBANK. Zahlungsverhalten in Deutschland 2011. Eine empirische Studie über die Verwendung von Bargeld und unbaren Zahlungsinstrumenten, 2012. 17. Oktober 2012. https://www.bundesbank.de/Redaktion/DE/Downloads/Veroeffentlichungen/Bericht_Studie/zahlungsverhalten_in_deutschland_2011.pdf?__blob=publicationFile (abgerufen am: 5. Mai 2014).*

8. *BETHGE, I. Zahlen, Daten, Fakten der Kreditwirtschaft. Berlin, Oktober 2014.*

9. *Seit wann gibt es Kreditkarten? - Geschichte & Politik | PM Online. http://www.pm-magazin.de/r/gute-frage/seit-wann-gibt-es-kreditkarten (abgerufen am: 12. Mai 2014).*

10. *IFAK INSTITUT, IPSOS, MEDIA MARKT ANALYSEN. Verbrauchs- und Medienanalyse - VuMA 2014, 2013. http://de.statista.com/statistik/daten/studie/171485/umfrage/marken-der-persoenlichen-kreditkarten/ (abgerufen am: 12. Mai 2014).*

11. *KRETSCHMAR, S. Elektronische Zahlungssysteme. Grundlagen, Verbreitung, Akzeptanz, Bewertung. Saarbrücken: VDM-Verl. Müller, 2005. ISBN 3865501206.*

12. *MACGREGOR, R., C. EZVAN, L.F. LIGUORI und J. HAN. Secure Electronic Transactions. Credit Card Payment on the Web in Theory and Practice, 1997. http://www.redbooks.ibm.com/redbooks/pdfs/sg244978.pdf (abgerufen am: 5. Mai 2014).*

13. *VISA EUROPE. Infographiken zur sicheren Kartenzahlung, 2014. http://www.visa.de/sicher-mit-visa/sicher-online-mit-verified-by-visa/so-funktioniert-es/infographiken-zur-sicheren-kartenzahlung (abgerufen am: 29. Juli 2014).*

14. WEINFURTNER, S. Zahlungsabwicklung im E-Commerce. Fakten aus dem deutschen Online-Handel; aktuelle Ergebnisse zu Zahlungsverfahren, Risiko- und Forderungsmanagement sowie Internationalisierung aus dem Projekt E-Commerce-Leitfaden. Regensburg: Ibi Research, 2011. eCommerce-Leitfaden. ISBN 978-3-940416-33-9.

15. PAYSYS CONSULTANCY. Kartenmarkt-Statistik Deutschland 2002-2011, 2013. http://de.statista.com.statista.han.w-hs.de/statistik/daten/studie/207621/umfrage/anzahl-der-in-deutschland-ausgebenen-geldkarten-seit-2000/ (abgerufen am: 7. Mai 2014).

16. DIE DEUTSCHE KREDITWIRTSCHAFT. Statistik: Anzahl der Transaktionen mit Geldkarten in Deutschland in den Jahren 2001 bis 2011. http://de.statista.com.statista.han.w-hs.de/statistik/daten/studie/6791/umfrage/anzahl-von-bezahltransaktionen-mit-geldkarte-von-1996-bis-2008/ (abgerufen am: 7. Mai 2014).

17. WIKIPEDIA. Geldkarte, 11. Jul. 2014. 11. Juli 2014. http://de.wikipedia.org/w/index.php?oldid=130609476 (abgerufen am: 29. Juli 2014).

18. WEBER, P. Geldkarte - Einführung und Demo, 2005. 07. Juni 2005. http://ux-2n16.inf.fh-bonn-rhein-sieg.de/lehre/alt/05ss/sm1/pres-Geldkarte.pdf (abgerufen am: 21. Mai 2014).

19. STEPHAN, K. Geldkarte. Warum hat sie sich nicht durchgesetzt … oder ist sie noch dabei? Seminararbeit. Frankfurt am Main, 2002.

20. BEYKIRCH, H.-B. GeldKarten-Latein, 1998. 16. November 1998. http://www.heise.de/ix/artikel/GeldKarten-Latein-508139.html (abgerufen am: 20. November 2014).

21. GEIGER, J. Bezahlen im Internet - Die GeldKarte im Internet, 2003. 20. September 2003. http://www.chip.de/artikel/Die-GeldKarte-im-Internet-3_12872006.html (abgerufen am: 29. Juli 2014).

22. SMART CARD ALLIANCE. New Visa payWave Issuers and Merchants Sign Up for Faster, More Convenient Payments, 2007. 20. Juli 2007. http://web.archive.org/web/20140209220024/http://www.smartcardalliance.org/articles/2007/09/20/new-visa-paywave-issuers-and-merchants-sign-up-for-faster-more-convenient-payments (abgerufen am: 25. November 2014).

23. PEREZ, S. NFC in 2011: MasterCard Continues Exploring Mobile Payments, 2011. 15. April 2011. http://readwrite.com/2011/04/15/nfc-in-2011-mastercard-explores-mobile-payments (abgerufen am: 25. November 2014).

24. SPARKASSE SÜDHOLSTEIN. So funktioniert girogo. https://www.spk-suedholstein.de/firmenkunden/electronic_banking/girogo/details/index.php?n=%2Ffirmenkunden%2Felectronic_banking%2Fgirogo%2Fdetails%2F (abgerufen am: 16. Juli 2014).

25. GARTNER. Weltweiter Umsatz mit Mobile Payment in den Jahren 2010 bis 2012 und Prognose für 2013 und 2017 (in Milliarden US-Dollar), 2013. Juni 2013. http://de.statista.com/statistik/daten/studie/214247/umfrage/umsatz-durch-mobile-payment-weltweit/ (abgerufen am: 16. Juli 2014).

26. ELEKTRONIK-KOMPENDIUM.DE. NFC - Near Field Communication. http://www.elektronik-kompendium.de/sites/kom/1107181.htm (abgerufen am: 24. Juni 2014).

27. ABI RESEARCH. Mobile Payment - Umsatz weltweit 2012 | Prognose, 2012. http://de.statista.com/statistik/daten/studie/244800/umfrage/prognose-zum-mobile-payment-umsatz-weltweit/ (abgerufen am: 24. Juni 2014).

28. STRUNK, O. Mpass GmbH: Netzanbieter-Allianz soll NFC voranbringen, 2011. 16. August 2011. http://www.inside-handy.de/news/22498-telekom-vodafone-und-o2-mpass-gmbh-netzanbieter-allianz-soll-nfc-voranbringen (abgerufen am: 25. September 2014).

29. TELEFÓNICA GERMANY GMBH & CO. OHG. mpass - Einfach per Handy bezahlen, 2013. 26. September 2013. http://www.youtube.com/watch?v=YzdupzpeUSU (abgerufen am: 27. Juni 2014).

30. EUROPÄISCHES PARLAMENT UND EUROPÄISCHER RAT DER EUROPÄISCHEN UNION. Richtlinie über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten. Richtlinie 2000/46/EG, 27. Okt. 2000. 2000.

31. DEUTSCHE TELEKOM AG. Leder war gestern – MyWallet macht das Smartphone zur Brieftasche. Bonn, 6. Mai. 2014.

32. WIKIPEDIA. Banklizenz, 19. Okt. 2014. 19. Oktober 2014. http://de.wikipedia.org/w/index.php?oldid=134300566 (abgerufen am: 19. November 2014).

33. WIRECARD BANK AG. Informationen über die Wirecard Bank, 2014. http://www.wirecardbank.de/unternehmen/ueber-die-wirecard-bank/ (abgerufen am: 5. August 2014).

34. WIRECARD AG. Vodafone SmartPass startet mit Unterstützung von Wirecard. Aschheim, 22. Nov. 2013.

35. MIRZADEH, M. E-Plus Mobile Wallet – das Smartphone als Brieftasche. Düsseldorf, 22. Nov. 2013.

36. WIKIPEDIA. Maestro-Card, 5. Jul. 2014. 05. Juli 2014. http://de.wikipedia.org/w/index.php?oldid=130373465 (abgerufen am: 5. August 2014).

37. TELEFÓNICA GERMANY GMBH & CO. OHG. O2 Wallet FAQ, 2013. August 2013. http://static2.o2.de/blob/11086056/Binary/o2-wallet-faq.pdf?v=6 (abgerufen am: 5. August 2014).

38. E-PLUS SERVICE GMBH & CO. KG. BASE Wallet: Ihre digitale Brieftasche, 2014. http://www.base.de/Mobile-Services/BASE-Wallet-zahlen-per-App (abgerufen am: 5. August 2014).

39. TELEFÓNICA GERMANY GMBH & CO. OHG. Es ist Zeit für o2 Wallet, 2014. http://www.o2online.de/apps-services/mobile-payment/wallet/?o2_type=goto&o2_label=nfc (abgerufen am: 5. August 2014).

40. T-MOBILE DEUTSCHLAND GMBH. MyWallet - Mobiles Bezahlen mit dem Smartphone, 2014. https://www.t-mobile.de/apps-und-musik/mywallet/0,26294,28533-_,00.html (abgerufen am: 5. August 2014).

41. VODAFONE GMBH. Vodafone Wallet: bezahlen per Handy & Smartphone, 2014. http://www.vodafone.de/privat/service/vodafone-wallet.html (abgerufen am: 5. August 2014).

42. PAYLIFE BANK GMBH. FAQs zum neuen Quick mit Kontaktlos-Funktion, 2014. Mai 2014. http://www.paylife.at/web/export/system/Medien/Dokumente/Quick/Quick_FAQ_Handel.pdf (abgerufen am: 27. November 2014).

43. SPARKASSE DORTMUND. SparkassenCard mit girogo - Zahlen Sie schneller als Ihr Schatten. Fragen und Antworten. https://www.sparkasse-dortmund.de/privatkunden/konten_karten/girogo/fragen_und_antworten/index.php?n=%2Fprivatkunden%2Fkonten_karten%2Fgirogo%2Ffragen_und_antworten%2F (abgerufen am: 27. November 2014).

44. ZEFFERER, T. Secure Elements am Beispiel Google Wallet. Wien, 28. Apr. 2012.

45. LÜCKE, H. G&D liefert hochsichere SIM-Kartenplattform für MyWallet. Details zur NFC-SIM-Karte der Telekom, 2014. 07. Mai 2014. http://www.inside-handy.de/news/31234-details-zur-nfc-sim-karte-der-telekom-g-d-liefert-hochsichere-sim-kartenplattform-fuer-mywallet (abgerufen am: 16. Juli 2014).

46. RAMISCH, F. Interview: Michael Kaduk über das Mobile-Wallet-Konzept der E-Plus-Gruppe., 2013. 05. November 2013. http://mobilbranche.de/2013/11/interview-michael-kaduk/39920 (abgerufen am: 5. August 2014).

47. ITWISSEN.INFO. QR :: quick response :: QR-Code, 2012. 23. September 2012. http://www.itwissen.info/definition/lexikon/quick-response-QR-QR-Code.html (abgerufen am: 24. Juni 2014).

48. OTTO GROUP. Die Otto Group - Konzernfirmen - Yapital, 2014. http://www.ottogroup.com/de/die-otto-group/konzernfirmen/yapital.php (abgerufen am: 17. Juni 2014).

49. VERBAND DER DEUTSCHEN INTERNETWIRTSCHAFT E.V. Besten der Internetwirtschaft ausgezeichnet. Branchenverband verleiht eco Internet Award 2014, 2014. 05. Juni 2014. http://www.eco.de/2014/news/besten-der-internetwirtschaft-ausgezeichnet.html (abgerufen am: 17. Juni 2014).

50. YAPITAL FINANCIAL AG. Datenschutzrichtlinie, 2013. 21. Januar 2013. https://www.yapital.com/mediaObject/Legal-docs/Privacy-Policy/Yapital-Privacy-Policy_GER/original/Yapital+Privacy+Policy_GER.pdf (abgerufen am: 24. Juni 2014).

51. CASSALA, C. "Für den Nutzer dürfen keine Initialkosten entstehen", 2014. 30. September 2014. http://www.deutsche-startups.de/2014/09/30/fuer-den-nutzer-duerfen-keine-initialkosten-entstehen/ (abgerufen am: 29. Oktober 2014).

52. PFÜTZE, TOBIAS. Verfahren und System zur Durchführung einer Finanz-Transaktion. Erfinder: T. PFÜTZE. Anmeldung: 20. August 2012. Deutschland. DE102012214744A1.

53. PAYMEY. PAYMEY - Datenschutz, 2014. https://www.paymey.com/datenschutz.html (abgerufen am: 25. Juni 2014).

54. EBAY INC. PayPal - Anzahl der aktiven Accounts bis Q1 2014, 2014. April 2014. http://de.statista.com/statistik/daten/studie/300180/umfrage/aktive-accounts-bei-paypal-weltweit-quartalszahlen/ (abgerufen am: 27. Juni 2014).

55. *LUNN, J. How does PayPal Beacon work, 2013. 10. September 2013. https://devblog.paypal.com/how-does-paypal-beacon-work/ (abgerufen am: 27. Juni 2014).*

56. *Per Smartphone: Paypal ermöglicht Bezahlen in Restaurants landesweit - Golem.de. http://www.golem.de/news/bezahlen-per-smartphone-paypal-ermoeglicht-bezahlen-in-restaurants-landesweit-1407-107895.html (abgerufen am: 28. November 2014).*

57. *CHAUM, D. Blind signatures for untraceable payments [online]. Advances in Cryptology - Crypto '82, 1983, **1982**(3), 199-203. http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF*

58. *WIKIPEDIA. eCash, 29. Jun. 2014. 29. Juni 2014. http://de.wikipedia.org/w/index.php?oldid=128781927 (abgerufen am: 30. Juli 2014).*

59. *SEEGER, J. Deutsche Bank 24 stellt eCash ein, 2001. 08. April 2001. http://www.heise.de/newsticker/meldung/Deutsche-Bank-24-stellt-eCash-ein-43389.html (abgerufen am: 30. Juli 2014).*

60. *COMPUTERWOCHE. Online-Bezahlsystem steht offenbar vor dem Aus: Cybercash schließt seine elektronische Geldbörse, 2001. 05. Januar 2001. http://www.computerwoche.de/a/cybercash-schliesst-seine-elektronische-geldboerse,1062599 (abgerufen am: 30. Juli 2014).*

61. *BÜSCHER, W.A. Cybercoins vor dem Durchbruch, 1999. 05. August 1999. http://www.welt.de/print-welt/article579515/Cybercoins-vor-dem-Durchbruch.html (abgerufen am: 30. Juli 2014).*

62. *PAYPAL INC. History - PayPal. https://www.paypal-media.com/history (abgerufen am: 30. Juli 2014).*

63. *WIKIPEDIA. Billpoint - Wikipedia, the free encyclopedia, 23. Jul. 2014. 23. Juli 2014. http://en.wikipedia.org/w/index.php?oldid=614467196 (abgerufen am: 30. Juli 2014).*

64. *WIKIPEDIA. PayPal, 29. Jul. 2014. 29. Juli 2014. http://de.wikipedia.org/w/index.php?oldid=132448503 (abgerufen am: 30. Juli 2014).*

65. *ADVAMEG INC. Elon Musk Biography. http://www.notablebiographies.com/news/Li-Ou/Musk-Elon.html#b (abgerufen am: 30. Juli 2014).*

66. *WIKIPEDIA. ClickandBuy, 29. Jun. 2014. 29. Juni 2014. http://de.wikipedia.org/w/index.php?oldid=130986157 (abgerufen am: 30. Juli 2014).*

67. *WIKIPEDIA. Ripple (payment protocol), 27. Jul. 2014. 27. Juli 2014. http://en.wikipedia.org/w/index.php?oldid=618429405 (abgerufen am: 31. Juli 2014).*

68. *BLEICH, H. Dell akzeptiert Bitcoin als Zahlungsmittel, 2014. 19. Juli 2014. http://www.heise.de/newsticker/meldung/Dell-akzeptiert-Bitcoin-als-Zahlungsmittel-2263182.html (abgerufen am: 31. Juli 2014).*

69. KANNENBERG, A. eBay-Chef über Bitcoin & Co.: "Paypal wird digitale Währungen integrieren müssen", 2014. 06. Juni 2014. http://www.heise.de/newsticker/meldung/eBay-Chef-ueber-Bitcoin-Co-Paypal-wird-digitale-Waehrungen-integrieren-muessen-2217238.html (abgerufen am: 31. Juli 2014).

70. GRÜNDERKÜCHE.DE. BaFin - Was ist die BundesAnstalt für Finanzdienstleistungsaufsicht (BAFIN), 2014. http://www.gruenderkueche.de/lexikon/bafin-definition-bundesanstalt-fuer-finanzdienstleistungsaufsicht-bafin/ (abgerufen am: 5. August 2014).

71. BUNDESANSTALT FÜR FINANZDIENSTLEISTUNGSAUFSICHT. Die BaFin stellt sich vor. Frankfurt am Main, August 2013.

72. BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ. Gesetz über das Kreditwesen. KWG, 18. Jul. 2014.

73. BUNDESMINISTERIUM DER FINANZEN. Gesetz über die Beaufsichtigung von Zahlungsdiensten (Zahlungsdiensteaufsichtsgesetz). ZAG, 25. Jun. 2009.

74. MÜNZER, J. Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer, 2013. 19. Dezember 2013. http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html?nn=3803924#doc4689532bodyText2 (abgerufen am: 23. Juli 2014).

75. BITCOIN DEUTSCHLAND AG. Kundeninformation zur Ausführung der Anlagevermittlung und / oder der Abschlussvermittlung von Bitcoin-Geschäften durch die Bitcoin Deutschland AG als vertraglich gebundener Vermittler der FIDOR Bank AG, 2013. https://www.bitcoin.de/de/kundeninformation_anlagevermittlung (abgerufen am: 6. August 2014).

76. FINANZVERWALTUNG NRW. Was ist der Unterschied zwischen Umsatzsteuer und Mehrwertsteuer?, 2014. 24. Oktober 2012. http://www.fm.nrw.de/allgemein_fa/steuerzahler/fragen/20_faq_ust/01.php (abgerufen am: 31. Juli 2014).

77. BUNDESZENTRALAMT FÜR STEUERN. Umsatzsteuer - Allgemeines, 2009. 09.2009. http://www.steuerliches-info-center.de/DE/SteuerrechtFuerInvestoren/Unternehmen_Inland/Umsatzsteuer/Allgemeines/allgemeines_node.html (abgerufen am: 23. Juli 2014).

78. WIKIPEDIA. Verkehrsteuer, 25. Jun. 2014. 25. Juni 2014. http://de.wikipedia.org/w/index.php?oldid=131099510 (abgerufen am: 23. Juli 2014).

79. BUNDESZENTRALAMT FÜR STEUERN. Umsatzsteuer - Steuerpflichtige / steuerfreie Umsätze, 2009. http://www.steuerliches-info-center.de/DE/SteuerrechtFuerInvestoren/Unternehmen_Inland/Umsatzsteuer/SteuerpflichtigeSteuerfreieUmsaetze/steuerpflichtigeSteuerfreieUmsaetze_node.html;jsessionid=A2A2725264F2F757D9133CE78EB4F706 (abgerufen am: 23. Juli 2014).

80. BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ. Einkommensteuergesetz. EStG, 16. Okt. 1934.

81. KOSCHYK, H. Ihre Schriftliche Frage Nr. 409 für den Monat Juli 2013. Brief, 7. Aug. 2013. http://www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_08_07-Antwort-Koschyk-Bitcoins-Umsatzsteuer.pdf (abgerufen am: 24. Juli 2014).

82. DENNERLEIN, B., C. WEERTH, D. PIEKENBROCK, A. HENNING, W. SCHNEIDER und A. SZCUTKOWSKI. Gabler Wirtschaftslexikon, Stichwort: Wirtschaftsgut. http://wirtschaftslexikon.gabler.de/Archiv/3696/wirtschaftsgut-v11.html (abgerufen am: 24. Juli 2014).

83. KOSCHYK, H. Ihre schriftliche Frage Nr. 149 für den Monat Juni 2013. Brief, 20. Jun. 2013. http://www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_06_20-Antwort-Bitcoin-Koschyk.pdf

84. KOSCHYK, H. Ihre schriftliche Frage Nr. 408 für den Monat Juli 2013. Brief, 7. Aug. 2013. http://www.frank-schaeffler.de/wp-content/uploads/2013/08/2013_08_07-Antwort-Koschyk-Bitcoins-Besteuerung-Wirtschaftsgut.pdf

85. DATEV EG. Bitcoins im Steuerrecht [online]. TRIALOG, Das Unternehmermagazin Ihrer Berater und der DATEV, 2014, **2014**(1). http://www.hsp-steuerberater-wirges.de/2014/07/09/bitcoins-im-steuerrecht/

86. SCHWENKE, T. Bitcoins - Rechtsbelehrung Folge 13 (Jura-Podcast mit FAQ in Shownotes), 2014. 14. April 2014. http://rechtsanwalt-schwenke.de/bitcoins-rechtsbelehrung-folge-13-jura-podcast-faq-in-shownotes/ (abgerufen am: 6. August 2014).

87. BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ. Umsatzsteuergesetz. UStG, 26. Nov. 1979.

88. KOSCHYK, H. Ihre Schriftliche Frage Nr. 226 für den Monat September 2013. Brief, 27. Sep. 2013. http://www.frank-schaeffler.de/wp-content/uploads/2013/10/2013_09_27-Antwort-Koschyk-Bitcoin3.pdf (abgerufen am: 24. Juli 2014).

89. KANNENBERG, A. Bitcoinhandel in Deutschland wahrscheinlich umsatzsteuerpflichtig, 2014. 23. Mai 2014. http://www.heise.de/newsticker/meldung/Bitcoinhandel-in-Deutschland-wahrscheinlich-umsatzsteuerpflichtig-2196321.html (abgerufen am: 6. August 2014).

90. KANNENBERG, A. EuGH soll über Umsatzsteuerpflicht für Bitcoinhandel entscheiden, 2014. 30. Juli 2014. http://www.heise.de/newsticker/meldung/EuGH-soll-ueber-Umsatzsteuerpflicht-fuer-Bitcoinhandel-entscheiden-2278739.html (abgerufen am: 31. Juli 2014).

91. NAKAMOTO, S. Bitcoin P2P e-cash paper. E-Mail, 31. Okt. 2008.

92. NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. https://bitcoin.org/bitcoin.pdf (abgerufen am: 14. Mai 2014).

93. BITCOIN WIKI. Bitcoin Address, 2014. 08. April 2014. https://en.bitcoin.it/wiki/Address (abgerufen am: 21. Mai 2014).

94. BITCOIN WIKI. Technical background of version 1 Bitcoin addresses, 2014. 15. Januar 2014. https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses (abgerufen am: 21. Mai 2014).

95. BLOCKCHAIN.INFO. Bitcoin Blockchain Größe, 2014. 08. November 2014. https://blockchain.info/de/charts/blocks-size (abgerufen am: 8. November 2014).

96. BITCOIN WIKI. Hashcash, 2014. 02. August 2014. https://en.bitcoin.it/wiki/Hashcash (abgerufen am: 8. August 2014).

97. BITCOIN WIKI. Protocol specification, 2014. 02. August 2014. https://en.bitcoin.it/wiki/Protocol_specification (abgerufen am: 7. August 2014).

98. BLOCKCHAIN.INFO. Bitcoin Hash Rate, 1. Jul. 2014. 01. Juli 2014. https://blockchain.info/de/charts/hash-rate (abgerufen am: 1. Juli 2014).

99. RIPPLE LABS INC. XRP Distribution, 2014. 30. April 2014. https://www.ripplelabs.com/xrp-distribution/ (abgerufen am: 3. Juli 2014).

100. Ripple for Gateways - Ripple Wiki, 16. Mai. 2014. 16. Mai 2014. https://ripple.com/wiki/index.php?title=Ripple_for_Gateways&oldid=8069 (abgerufen am: 3. Juli 2014).

101. RIPPLER XRP. Ripple Client - An Introduction, 2013.

102. RIPPLE LABS INC. Ripple for Users - Ripple Wiki, 2014. 30. April 2014. https://ripple.com/wiki/index.php?title=Ripple_for_Users&oldid=7943 (abgerufen am: 3. Juli 2014).

103. RAPOPORT, P. Ripple: A Primer, 2013. 25. Oktober 2013. https://ripple.com/ripple_primer.pdf (abgerufen am: 20. Mai 2014).

104. AZZANO, M. Ripple Labs Announces Fidor Bank AG as First Bank to Use the Ripple Protocol. San Francisco, 5. Mai. 2014.

105. RIPPLE LABS INC. Ledger - Ripple Wiki, 2014. 13. Mai 2014. https://ripple.com/wiki/index.php?title=Ledger&oldid=8030 (abgerufen am: 3. Juli 2014).

106. RIPPLE LABS INC. Consensus Graphic - Ripple Wiki, 2013. 05. April 2013. https://ripple.com/wiki/index.php?title=Consensus_Graphic&oldid=3662 (abgerufen am: 3. Juli 2014).

107. KANNENBERG, A. Bitcoin: Erstmals gefährliche Konzentration der Mining-Leistung, 2014. 17. Juni 2014. http://www.heise.de/newsticker/meldung/Bitcoin-Erstmals-gefaehrliche-Konzentration-der-Mining-Leistung-2224113.html (abgerufen am: 7. August 2014).

108. KING, S. und S. NADAL. PPCoin: Peer-to-Peer Kryptowährung mit Proof-of-Stake, 2012. 19. August 2012. http://www.peercoin.net/assets/paper/peercoin-paper.pdf (abgerufen am: 7. August 2014).

109. PEERCOIN. What is Proof-of-Stake/Minting? http://www.peercoin.net/minting (abgerufen am: 8. August 2014).

110. DARK, S. Could Peercoin and "Proof-of-Stake" Turn Bitcoin Into The Myspace of Cryptocurrency?, 2014. 19. Januar 2014. http://cointrader.org/peercoin-proof-of-stake-and-bitcoin/ (abgerufen am: 8. August 2014).

111. KING, S. [PPC] [XPM] Peercoin/Primecoin Weekly Updates, 2013. 05. August 2014. https://bitcointalk.org/index.php?topic=114994.msg2501124#msg2501124 (abgerufen am: 11. August 2014).

112. YAPITAL FINANCIAL AG. Wunsch und Wirklichkeit. Das stört die Deutschen beim Bezahlen… … und das erwarten Sie von mobile Payment. Luxemburg, 30. Jun. 2014.

113. DEUTSCHE BUNDESBANK. Zahlungsverhalten in Deutschland. Eine empirische Studie über die Auswahl und Verwendung von Zahlungsinstrumenten in der Bundesrepublik Deutschland. Frankfurt am Main, 2009.

114. WITTMANN, G., E. STAHL, M. WITTMANN, S. PUR und S. WEINFURTNER. Erfolgsfaktor Payment. Der Einfluss der Zahlungsverfahren auf Ihren Umsatz. 2. Auflage. Regensburg, 2013.

115. RIGGERT, W. Technologie des Web-Business. Sicherheit und Bezahlen im Internet. Flensburg.

116. HERZIG, R. Anforderungen des Handels an moderne Bezahlsysteme. Berlin, 15. Jan. 2008. ZKA Infoveranstaltung.

117. FITTKAU MAAß CONSULTING. 38. WWW-Benutzer-Analyse W3B: Kaufentscheidung im Internet, 2014. 06.2014. http://de.statista.com/statistik/daten/studie/12862/umfrage/gruende-fuer-kaufabbruch-beim-online-shopping-2009/ (abgerufen am: 13. August 2014).

118. SIEDENBIEDEL, C. Mehr Kontrolle über Geldgeschäfte. Angriff auf das Bargeld, 2014. 17. Mai 2014. http://www.faz.net/aktuell/finanzen/meine-finanzen/geld-ausgeben/nachrichten/warum-banken-und-staaten-krieg-gegen-das-bargeld-fuehren-12944410.html?printPagedArticle=true#pageIndex_2 (abgerufen am: 18. August 2014).

119. RAT DER EUROPÄISCHEN UNION. Council Conclusions on the European Financial Coalition and national financial coalitions against child pornography on the Internet. 2969th JUSTICE and HOME AFFAIRS Council meeting. Luxemburg, 23. Okt. 2009.

120. HAMBURGER ABENDBLATT. Kinderporno: Zugriff auf Kreditkarten, 2009. 03. April 2009. http://www.abendblatt.de/politik/deutschland/article167895/Kinderporno-Zugriff-auf-Kreditkarten.html (abgerufen am: 24. Juni 2014).

121. MERTIN, A. "Junge Orchidee" [online]. SPIEGEL special, **2007**(3), 114. http://www.wiso-net.de/webcgi?START=A60&DOKV_DB=SSPE&DOKV_NO=Romberg-SPC-00132007000030011400&DOKV_HS=0&PP=1

122. SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION. Company information. http://www.swift.com/about_swift/company_information/company_information (abgerufen am: 18. August 2014).

123. SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION. SWIFT in figures. La Hulpe, Juni 2014.

124. TAGESSCHAU.DE. Fragen und Antworten zum SWIFT-Abkommen, 2013. 23. Oktober 2013. http://www.tagesschau.de/ausland/swiftfragen100~_origin-65d6cf96-430b-4aaa-9dbd-8ccc9f644265.html (abgerufen am: 18. August 2014).

125. DEUTSCHE BUNDESBANK. Im deutschen Zahlungsverkehr registrierte falsche Euro-Münzen in den Jahren von 2010 bis zum 1. Halbjahr 2014, 2014. Juli 2014. http://de.statista.com/statistik/daten/studie/1210/umfrage/anzahl-der-gefaelschten-euro-muenzen-in-deutschland/ (abgerufen am: 21. August 2014).

126. EUROPEAN CENTRAL BANK. Anzahl der halbjährlich sichergestellten falschen Euro-Banknoten von 2004 bis zum 1. Halbjahr 2014 (in 1.000), 2014. Juli 2014. http://de.statista.com/statistik/daten/studie/29171/umfrage/faelschungen-von-euro-banknoten-halbjaehrlich-seit-2004/ (abgerufen am: 21. August 2014).

127. EUROPEAN CENTRAL BANK. Euro-Banknoten im Bargeldumlauf im Juni 2014, 2014. Juli 2014. http://de.statista.com/statistik/daten/studie/186249/umfrage/euro-banknoten---bargeldumlauf/ (abgerufen am: 22. August 2014).

128. CASH PAYMENT SOLUTIONS GMBH. So einfach funktioniert Barzahlen, 2014. https://www.barzahlen.de/de/kunden/funktionsweise#sicher-online-einkaufen (abgerufen am: 20. August 2014).

129. ANWAR, A. und M. PREM. Schweden schafft das Bargeld ab, 2013. 26. Februar 2013. http://www.merkur-online.de/aktuelles/wirtschaft/schweden-schafft-bargeld-2769638.html (abgerufen am: 20. August 2014).

130. TSYS. 2013 Consumer Payment Choice Study. Payment preference when shopping at department stores, 2013. Oktober 2013. http://www.statista.com/statistics/294123/payment-preference-department-stores-us-2013/ (abgerufen am: 20. August 2014).

131. STATISTA. Infografik: Deutsche lieben das Bargeld, 2014. 24. Juni 2014. http://de.statista.com/infografik/2389/bevorzugte-bezahlmoeglichkeit-der-deutschen/ (abgerufen am: 20. August 2014).

132. STIFTUNG WARENTEST. Gebühren an Geldautomaten - Sparkassen und Volksbanken teuer, 2011. 31. Januar 2011. http://www.test.de/Gebuehren-an-Geldautomaten-Sparkassen-und-Volksbanken-teuer-4199327-0/ (abgerufen am: 22. August 2014).

133. LITTMANN, S. Bargeld ist teurer als Kartenzahlung, 2013. 21. Mai 2013. http://www.wiwo.de/finanzen/geldanlage/studie-zum-zahlungsverkehr-bargeld-ist-teurer-als-kartenzahlung/8232850.html (abgerufen am: 22. August 2014).

134. BENDER, H. Bargeldlogistik: Edeka beziffert Kosten des Bargeldhandlings, 2012. 02. Februar 2012. http://www.derhandel.de/news/technik/pages/Bargeldlogistik-Edeka-beziffert-Kosten-des-Bargeldhandlings-8223.html (abgerufen am: 22. August 2014).

135. EDEKA-VERBUND. Unternehmensbericht 2013. Hamburg, 29. Apr. 2014.

136. KLEINE, J., M. KRAUTBAUER und T. WEILER. Cost of Cash. Status Quo und Entwicklungsperspektiven in Deutschland. München, Mai 2013.

137. NACHRICHTENFERNSEHEN, n.-t. Kartenzahlung mit Unterschrift: Mehr gespeichert als erlaubt?d, 2010. 23. September 2010. http://www.n-tv.de/ratgeber/Mehr-gespeichert-als-erlaubt-article1557586.html (abgerufen am: 24. Juni 2014).

138. FOCUS ONLINE. Datenschutz: Easycash unter Beschuss, 2011. 14. September 2011. http://www.focus.de/finanzen/banken/datenschutz-easycash-unter-beschuss_aid_665450.html (abgerufen am: 25. August 2014).

139. BACHFELD, D. Chipkarten ausgehebelt, 2010. 27. Februar 2010. http://www.heise.de/ct/artikel/Phish-Chips-939329.html (abgerufen am: 25. August 2014).

140. MURDOCH, S.J., S. DRIMER, R. ANDERSON und M. BOND. Chip and PIN is Broken. In: 2010 IEEE Symposium on Security and Privacy, S. 433-446.

141. SCHMERGAL, M. Deutsche girocards und Kreditkarten von britischem Manipulationsversuch nicht betroffen. Berlin, 15. Feb. 2010.

142. BUNDESKRIMINALAMT. Zahlungskartenkriminalität. Bundeslagebild 2013. Wiesbaden, 2013.

143. SCHULTE, T. EC Karten Missbrauch – rechtliche Hintergründe, 2007. 17. Januar 2014. http://www.dr-schulte.de/rechtsgebiet/bank-und-kapitalmarktrecht/ec-karten-missbrauch-rechtliche-hintergruende (abgerufen am: 26. August 2014).

144. CHECK24 VERGLEICHSPORTAL GMBH. V PAY oder Maestro - welche Karte zum Girokonto?, 2014. http://www.check24.de/girokonto/vpay-maestro/ (abgerufen am: 27. August 2014).

145. SPARKASSE GELSENKIRCHEN. Preis- und Leistungsverzeichnis. Gelsenkirchen, 4. Jun. 2013.

146. EURO KARTENSYSTEME GMBH. Händlerbedingungen. Bedingungen für die Teilnahme am electronic cash-System der deutschen Kreditwirtschaft. Frankfurt am Main, 11. Mrz. 2008.

147. HANDELSBLATT GMBH. Einheitsgebühr für EC-Karten-Zahlung fällt weg, 2014. 08. April 2014. http://www.handelsblatt.com/unternehmen/handel-dienstleister/erleichterung-fuer-einzelhandel-einheitsgebuehr-fuer-ec-karten-zahlung-faellt-weg/9733750.html (abgerufen am: 27. August 2014).

148. BENDER, H. Kartenzahlung: Rewe drückt EC-Cash-Gebühren, 2012. 20. Juni 2012. http://www.derhandel.de/news/finanzen/pages/Kartenzahlung-Rewe-drueckt-EC-Cash-Gebuehren-8695.html (abgerufen am: 27. August 2014).

149. EASYCASH GMBH. Ingenico iCT220 - Jetzt bestellen!, 2014. https://www.easycash.de/de/easyshop/terminal/mieten/ingenico_ict220.html?no_cache=1 (abgerufen am: 27. August 2014).

150. THOMA, J. NSA sammelt weltweite Finanzdaten, 2013. 15. September 2013. http://www.golem.de/news/spionage-nsa-sammelt-weltweite-finanzdaten-1309-101602.html (abgerufen am: 12. Mai 2014).

151. DEUTSCHE WIRTSCHAFTS NACHRICHTEN. US-Behörden haben vollständigen Zugriff auf Kreditkarten-Daten, 2013. http://deutsche-wirtschafts-nachrichten.de/2013/07/01/us-behoerden-haben-vollstaendigen-zugriff-auf-kreditkarten-daten/ (abgerufen am: 12. Mai 2014).

152. *WILKENS, A. US-Zugriff auf EU-Rechenzentrum: Microsoft bekommt Aufschub, 2014. 01. August 2014. http://www.heise.de/newsticker/meldung/US-Zugriff-auf-EU-Rechenzentrum-Microsoft-bekommt-Aufschub-2281428.html (abgerufen am: 28. August 2014).*

153. *MASTERCARD WORLDWIDE. Safe-Harbor-Datenschutzrichtlinie, 2011. 26. April 2011. http://www.mastercard.com/de/privatkunden/datenschutz_safe_harbor.html (abgerufen am: 28. August 2014).*

154. *KANNENBERG, A. USA: Mastercard wertet Einkäufe für Werbung aus, 2012. 17. Oktober 2012. http://www.heise.de/newsticker/meldung/USA-Mastercard-wertet-Einkaeufe-fuer-Werbung-aus-1731775.html (abgerufen am: 5. September 2014).*

155. *MASTERCARD WORLDWIDE. Specify MasterCard Audiences for your Online Buys, 2014. http://www.mastercardadvisors.com/media_audiences.html (abgerufen am: 22. September 2014).*

156. *NEUE ZÜRCHER ZEITUNG AG. Aus dem Bezirksgericht Zürich: Wenn der Kellner die Kreditkarte kopiert, 2008. 14. Juli 2008. http://www.nzz.ch/aktuell/startseite/wenn-der-kellner-die-kreditkarte-kopiert-1.783297 (abgerufen am: 23. September 2014).*

157. *SCHRÖDER, T. Kreditkartendaten gestohlen: UPS bestätigt Hackerangriff, 2014. 22. August 2014. http://www.golem.de/news/kreditkartendaten-gestohlen-ups-bestaetigt-hackerangriff-1408-108751.html (abgerufen am: 23. September 2014).*

158. *HANDELSZEITUNG. 100 Millionen Kreditkartendaten geraubt - Schweizer betroffen, 2014. 14. Januar 2014. http://www.handelszeitung.ch/unternehmen/100-millionen-kreditkartendaten-geraubt-schweizer-betroffen-551849 (abgerufen am: 23. September 2014).*

159. *EGGELING, T. Kreditkarten: Prüfnummern sind leicht zu hacken, 2012. 10. August 2012. http://www.com-magazin.de/news/sicherheit/kreditkarten-pruefnummern-sind-leicht-zu-hacken-6068.html (abgerufen am: 23. September 2014).*

160. *SPIEGEL ONLINE. Expedia, Opodo, Tui: Dienstleister TravelTainment verliert Kreditkartendaten, 2013. 22. April 2013. http://www.spiegel.de/netzwelt/web/opodo-expedia-tui-kreditkartendaten-bei-traveltainment-entwendet-a-895751.html (abgerufen am: 23. September 2014).*

161. *HEEG, T. Kreditkartenbetrug: Lernen von den Trickbetrügern, 2011. 21. Januar 2011. http://www.faz.net/aktuell/wirtschaft/kreditkartenbetrug-lernen-von-den-trickbetruegern-1572477.html (abgerufen am: 22. September 2014).*

162. *SPARKASSE AACHEN. Geoblocking, 2014. 26. Juni 2014. https://www.sparkasse-aachen.de/pages/privatkunden/produkte/konto_karten/karten/sparkassencard/geoblocking/index.php?show=details (abgerufen am: 22. September 2014).*

163. *WGZ BANK. Kreditkarte. http://www.wgzbank.de/de/wgzbank/firmenkunden/zahlungsverkehr/ecommmerce/vr-pay/kreditkarte/ (abgerufen am: 6. Oktober 2014).*

164. BACHFELD, D. Verbraucherschutzzentrale warnt vor 3D-Sicherheitsverfahren bei Kreditkarten, 2011. 12. August 2011. http://www.heise.de/security/meldung/Verbraucherschutzzentrale-warnt-vor-3D-Sicherheitsverfahren-bei-Kreditkarten-1322375.html (abgerufen am: 23. September 2014).

165. STIFTUNG WARENTEST. Kreditkarten mit „SecureCode“ und „Verified by Visa“ - Haftungsrisiko bei Missbrauch, 2011. 06. Mai 2011. http://www.test.de/Kreditkarten-mit-SecureCode-und-Verified-by-Visa-Haftungsrisiko-bei-Missbrauch-4231197-0/ (abgerufen am: 6. Oktober 2014).

166. STIFTUNG WARENTEST. Kreditkarten mit „Mastercard SecureCode“ und „Verified by Visa“ - Mehr Sicherheit, 2011. 06. Mai 2011. http://www.test.de/Kreditkarten-mit-Mastercard-SecureCode-und-Verified-by-Visa-Mehr-Sicherheit-4233850-0/ (abgerufen am: 6. Oktober 2014).

167. BERLINER SPARKASSE. Reklamation Kreditkartenzahlung. https://www.berliner-sparkasse.de/privatkunden/banking/bezahlen_im_internet/reklamation_kreditkarten/index.php?n=%2Fprivatkunden%2Fbanking%2Fbezahlen_im_internet%2Freklamation_kreditkarten%2F (abgerufen am: 23. September 2014).

168. MASTERCARD EUROPE SPRL. Chip&PIN. http://www.mastercard.com/de/privatkunden/innovationen_chippin.html (abgerufen am: 6. Oktober 2014).

169. BARTSCH, C., S. KRIEG und M. HANFT. PIN Eingabe bei Kreditkarten. http://www.zahlungsverkehrsfragen.de/kartenzahlung/pin-eingabe-bei-kreditkarten (abgerufen am: 6. Oktober 2014).

170. EUROPEAN CENTRAL BANK. Report on card fraud. July 2012. Frankfurt am Main: European Central Bank, 2012. ISBN 978-92-899-0832-0.

171. DEUTSCHE WIRTSCHAFTS NACHRICHTEN. Russland plant wegen Sanktionen eigene Kreditkarte, 2014. 27. März 2014. http://deutsche-wirtschafts-nachrichten.de/2014/03/27/russland-plant-wegen-sanktionen-eigene-kreditkarte/ (abgerufen am: 27. Juni 2014).

172. PLUTA, W. Zahlungsstopp: Visa und Mastercard sperren Wikileaks (Update), 2010. 07. Dezember 2010. http://www.golem.de/1012/79942.html (abgerufen am: 27. Juni 2014).

173. ERNESTO. Mastercard and Visa Start Banning VPN Providers?, 2013. 08. Juli 2013. http://torrentfreak.com/mastercard-and-visa-start-banning-vpn-providers-130703/5988184/ (abgerufen am: 28. August 2014).

174. MASTERCARD EUROPE SPRL. Bargeldlos Zahlen. MasterCard ist ihr perfekter Reisebegleiter. Weltweit., 2014. http://www.mastercard.com/de/privatkunden/wissenswertes_bargeldlos_zahlen.html (abgerufen am: 6. Oktober 2014).

175. HYPOVEREINSBANK. VISA Kreditkarte. http://www.hypovereinsbank.de/portal?view=/de/privatkunden/karten/visa-card.jsp (abgerufen am: 6. Oktober 2014).

176. CONCARDIS GMBH. Preis- und Leistungsverzeichnis der ConCardis GmbH (Deutschland), 2013. 01. Dezember 2013. https://www.concardis.de/fileadmin/redaktion/downloads/Preislisten/ConCardis_Preisliste_DE_DE.pdf (abgerufen am: 7. Oktober 2014).

177. WILLKOMMER, J. Online Zahlungsanbieter - Der ultimative Marktüberblick, 2011. http://www.estrategy-magazin.de/ausgabe-04-2011/online-zahlungsanbieter-der-ultimative-marktueberblick.html

178. SCOUT24 SERVICES GMBH. Kreditkarte: Fragen & Antworten zu Kreditkarten, 2014. http://www.financescout24.de/geldanlage-banking/kreditkarte/fragen-und-antworten.aspx#kk16 (abgerufen am: 7. Oktober 2014).

179. SPARKASSEN-HÄNDLERSERVICE. Zahlschnittstelle für den E-Commerce und Mailorder, 2014. https://www.s-haendlerservice.de/e-commerce-versandhandel/zahlschnittstelle/ (abgerufen am: 8. Oktober 2014).

180. DIE DEUTSCHE KREDITWIRTSCHAFT. Das GeldKarte-System der Deutschen Kreditwirtschaft. Ein Systemüberblick, 2011. http://www.die-deutsche-kreditwirtschaft.de/uploads/media/Systembeschreibung_GeldKarte_DK_21-11-2011_01.pdf (abgerufen am: 8. Mai 2014).

181. SELHORST, M. Die Geldkarte. Eine "sichere" elektronische Geldbörse?! Seminararbeit. Bochum, 2002.

182. GREINER-MAI, J. Chipkarten, 1999. 04. November 2010. http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/BezahlenII/chipkarten.html (abgerufen am: 9. Oktober 2014).

183. EURO KARTENSYSTEME GMBH. Bezahlen, 2014. 19. Februar 2014. https://www.geldkarte.de/privatkunden/bezahlen/ (abgerufen am: 8. Oktober 2014).

184. VR-BANK IN MITTELBADEN EG. Rückzug aus dem GeldKarte-System, 2014. 20. Juli 2014. https://www.vr-miba.de/wir-fuer-sie/aktuelles-regionales/banksache/geldkarte.html (abgerufen am: 10. Oktober 2014).

185. VR-BANK EG IM ALTKREIS BERSENBRÜCK. FAQ GeldKarte – Kunde, 2014.

186. GELDKARTE SHOP. GeldKarte Online-Shop. Kontounabhängige GeldKarte, 2014. http://www.geldkarte-shop.de/index.php/category/Kontounabhaengige_GeldKarte (abgerufen am: 9. Oktober 2014).

187. EURO KARTENSYSTEME GMBH. Vorteile der Geldkarte, 2014. 11. März 2014. https://www.geldkarte.de/geschaeftskunden/vorteile/ (abgerufen am: 8. Oktober 2014).

188. EURO KARTENSYSTEME GMBH. So können Sie Ihre GeldKarte laden, 2014. 26. August 2014. https://www.geldkarte.de/privatkunden/aufladen/ (abgerufen am: 10. Oktober 2014).

189. Der Unbestechliche. Alterscheck per GeldKarte-Chip. ProChip, 2006, **2006**(1), 8-11.

190. ITZE, J.-E. Die GeldKarte bitte! [online]. Nahverkehrspraxis, 2002, **2002**(7/8-2002), 25-26. http://www.initag.de/share/news/Themen/GeldKarte_bitte.pdf

191. THOMA, J. Unsicheres NFC: Android-Applikation liest Paypass-Daten aus, 2012. 22. Juni 2012. http://www.golem.de/news/unsicheres-nfc-android-applikation-liest-paypass-daten-aus-1206-92709.html (abgerufen am: 26. Juni 2014).

192. MASTERCARD EUROPE SPRL. Schnell und einfach Zahlen mit einer Handbewegung, 2014. http://www.mastercard.com/at/privatkunden/innovationen_paypass.html (abgerufen am: 14. Oktober 2014).

193. HANDELSBLATT GMBH. Mastercard rüstet Terminals auf, 2014. 15. Juli 2014. http://www.handelsblatt.com/finanzen/vorsorge-versicherung/altersvorsorge-sparen/kontaktloses-bezahlen-mastercard-ruestet-terminals-auf/10201198.html (abgerufen am: 14. Oktober 2014).

194. VISA EUROPE SERVICES INC. Hier kontaktlos bezahlen mit Visa, 2014. August 2014. http://www.visa.de/kartenprodukte/kontaktloses-bezahlen-mit-visa/hier-kontaktlos-bezahlen-mit-visa (abgerufen am: 14. Oktober 2014).

195. VISA EUROPE SERVICES INC. Kontaktlos-Zahlungen, 2014. http://www.visa.de/zahlungsmoglichkeiten/kontaktlos-zahlungen (abgerufen am: 14. Oktober 2014).

196. VON REKOWSKI, E. Mastercard forciert NFC in ganz Europa, 2014. 12. September 2014. http://www.crn.de/telekommunikation/artikel-104086.html (abgerufen am: 14. Oktober 2014).

197. INGENICO GMBH. Kurzinfo iCT220 / iCT250. Berlin, 2010.

198. REA CARD GMBH. Die ersten Schritte mit Ihrem neuen stationären REA T5 retail mit Händlereinheit. Mühltal, 2013.

199. VERBAND DER SPARDA-BANKEN E.V. MasterCard PayPass. Kleinbeträge kontaktlos und schnell zahlen! http://www.sparda.de/paypass.php (abgerufen am: 15. Oktober 2014).

200. AK VORRATSDATENSPEICHERUNG. Girogo/Kritik - Freiheit statt Angst!, 2012. 06. August 2014. http://wiki.vorratsdatenspeicherung.de/index.php?title=Girogo/Kritik&oldid=119405 (abgerufen am: 18. Juni 2014).

201. BACHFELD, D. und h. SECURITY. Hacker liest unbemerkt RFID-Personaldokumente von US-Bürgern aus, 3. Feb. 2009. 03. Februar 2009. http://www.heise.de/security/meldung/Hacker-liest-unbemerkt-RFID-Personaldokumente-von-US-Buergern-aus-204911.html (abgerufen am: 18. Juni 2014).

202. SCHUBERT, S. und N. BAUM. 10.000 girogo-‐Akzeptanzstellen in Deutschland. Frankfurt am Main, 9. Sep. 2014.

203. WIRECARD CARD SOLUTIONS LTD. Datenschutzerklärung von wirecard, 2014. https://mpass.wirecard.com/mpass-signup/privacy.jsp (abgerufen am: 21. Oktober 2014).

204. DEUTSCHE TELEKOM AG, VODAFONE D2 GMBH und TELEFÓNICA GERMANY GMBH & CO. OHG. Ihre Vorteile als Händler, 2014. 05. Juni 2014. http://www.mpass.de/haendler/#Ihre-Vorteile (abgerufen am: 5. Juni 2014).

205. MPASS. Häufig gestellte Fragen | o2 - mpass, 2014. http://www.mpass.de/faq (abgerufen am: 21. Oktober 2014).

206. SCHERSCHEL, F. Online-Banking: Verstärkte Angriffe auf das mTAN-Verfahren, 2014. 19. Mai 2014. http://www.heise.de/security/meldung/Online-Banking-Verstaerkte-Angriffe-auf-das-mTAN-Verfahren-2193090.html (abgerufen am: 21. Oktober 2014).

207. STERN.DE GMBH. Sicherheitslücken bei mTAN-Verfahren: So leicht plündern Hacker fremde Bankkonten, 2013. 21. November 2013. http://www.stern.de/tv/sterntv/sicherheitsluecken-bei-mtan-verfahren-so-leicht-pluendern-hacker-fremde-bankkonten-2069062.html (abgerufen am: 21. Oktober 2014).

208. VODAFONE D2 GMBH, TELEFÓNICA GERMANY GMBH & CO. OHG und T-MOBILE DEUTSCHLAND GMBH. Modern bezahlen mit mpass, 2014. 27. Juni 2014. http://www.mpass.de (abgerufen am: 27. Juni 2014).

209. VODAFONE GMBH. "Fehlende Bonität" bei mpass, 2010. 04. Dezember 2010. https://forum.vodafone.de/t5/Alles-rund-um-CallYa-inaktives/quot-Fehlende-Bonit%C3%A4t-quot-bei-mpass/td-p/38290 (abgerufen am: 22. Oktober 2014).

210. WIRECARD CARD SOLUTIONS LTD. mpass Gebühren und Nutzungsbeschränkungen, 2014. 05. September 2014. https://mpass.wirecard.com/mpass-signup/pdf/mpass_Gebuehren_Hinweise_Nutzung.pdf (abgerufen am: 22. Oktober 2014).

211. EMARKETER. The New Digital Economy: How it will transform business, 2011. http://de.statista.com/statistik/daten/studie/199070/umfrage/anzahl-der-mobiltelefonnutzer-in-deutschland-seit-2009/ (abgerufen am: 22. Oktober 2014).

212. HEDEMANN, F. mpass - Kostenlose Magento-Schnittstelle für sicheres Online Payment, 2010. http://t3n.de/news/mpass-kostenlose-magento-schnittstelle-sicheres-online-285596/ (abgerufen am: 22. Oktober 2014).

213. T-MOBILE DEUTSCHLAND GMBH, VODAFONE D2 GMBH und TELEFÓNICA GERMANY GMBH & CO. OHG. mpass in Onlineshops für ihre Kunden, 2014. http://www.mpass.de/haendler/mpass_fuer_ecommerce#So-starten-Sie (abgerufen am: 22. Oktober 2014).

214. BUNDESNETZAGENTUR. Teilnehmerentwicklung im Mobilfunk, 2014. 13. November 2014. http://www.bundesnetzagentur.de/cln_1422/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Marktbeobachtung/Deutschland/Mobilfunkteilnehmer/Mobilfunknehmer.html?nn=268208 (abgerufen am: 21. November 2014).

215. TELEKOM DEUTSCHLAND GMBH. Gebühren - MyWallet, 2014. http://www.telekom.de/is-bin/INTERSHOP.enfinity/WFS/EKI-TELEKOM-Site/de_DE/-/EUR/ViewCategoryPage-Start?CatalogCategoryID=Q5IFejYN6zwAAAFF14YvC80R (abgerufen am: 23. Oktober 2014).

216. TELEKOM DEUTSCHLAND GMBH. MyWallet Cards - Preisübersicht, 2014. 16. September 2014. https://www.card.my-wallet.com/my-wallet/static/DE/web/ShowFees.html (abgerufen am: 23. Oktober 2014).

217. ALIGORAKI, J. Vodafone SmartPass Gebührentabelle, 2014 (abgerufen am: 23. Oktober 2014).

218. E-PLUS SERVICE GMBH & CO. KG. BASE Wallet: Ihre digitale Brieftasche, 2014. http://www.base.de/Mobile-Services/BASE-Wallet-zahlen-per-App (abgerufen am: 23. Oktober 2014).

219. WIRECARD CARD SOLUTIONS LTD. Walletcard Gebühren und Nutzungsbeschränkungen, 2014. 03. Juni 2014. https://walletcard.de/walletcard/resource/Walletcard_Gebuehren_Hinweise_Nutzung.pdf (abgerufen am: 23. Oktober 2014).

220. TELEKOM DEUTSCHLAND GMBH. NFC SIM im iPhone 4S und erfolgloser Einkaufsversuch, 2014. 27. Juni 2014. https://forum.telekom.de/foren/read/service/handys-mobile-datengeraete/iphone-ipad/nfc-sim-im-iphone-4s-und-erfolgloser-einkaufsversuch,870,11240615.html (abgerufen am: 23. Oktober 2014).

221. CHIP DIGITAL GMBH. MyWallet: Gutscheine bei Edeka und Hit anrechnen, 2014. 01. Juli 2014. http://business.chip.de/news/MyWallet-Gutscheine-bei-Edeka-und-Hit-anrechnen_70730212.html (abgerufen am: 23. Oktober 2014).

222. TELEFÓNICA GERMANY GMBH & CO. OHG. o2 Wallet, 2013. http://m.o2online.de/angebote/o2wallet/bank/ (abgerufen am: 23. Oktober 2014).

223. HEUTGER, C. Mobil bezahlen: Mobile Payment-Systeme unter der Lupe, 2014. 31. Juli 2014. http://www.psw-group.de/blog/mobil-bezahlen-mobile-payment-systeme-unter-der-lupe/1368 (abgerufen am: 24. Oktober 2014).

224. SPOOREN, S., D. PAWLITZEK und N. POHLMANN. Passwort sicher erstellen, 2013. https://www.it-sicherheit.de/ratgeber/it_sicherheitstipps/tipp/passwort-sicher-erstellen/?cHash=d328b801a799fa212988e7ff10e1fdf9 (abgerufen am: 24. Oktober 2014).

225. YAPITAL FINANCIAL AG. Häufig gestellte Fragen, 2014. https://www.yapital.com/deu/privatenutzer/faq (abgerufen am: 24. Oktober 2014).

226. YAPITAL FINANCIAL AG. Yapital die neue Art des Bezahlens, 2014. https://www.yapital.com/deu/geschaeftskunden (abgerufen am: 24. Oktober 2014).

227. YAPITAL FINANCIAL AG. Nutzungsbedingungen, 2013. 25. Juni 2013. https://www.yapital.com/mediaObject/Legal-docs/Terms-of-use/Yapital-Consumer-Terms_GER_130524-V1.1/original/Yapital+Consumer+Terms_GER_130524+V1.1.pdf (abgerufen am: 24. Oktober 2014).

228. YAPITAL FINANCIAL AG. Akzeptanzstellen. Hier können Sie mit Yapital bezahlen, 2014. https://www.yapital.com/deu/privatenutzer/wo-sie-mit-yapital-bezahlen-koennen (abgerufen am: 24. Oktober 2014).

229. REWE GROUP-UNTERNEHMENSKOMMUNIKATION. REWE Group steigt im November mit Yapital ins Mobile Payment ein, 2013. 12. September 2013. http://www.rewe-group.com/presse/pressemeldungen/pressemeldung-detail/article/rewe-group-steigt-im-november-mit-yapital-ins-mobile-payment-ein/ (abgerufen am: 24. Oktober 2014).

230. GOUDINOUDIS, A. Yapital noch in diesem Jahr in allen deutschen Douglas-Filialen, 2014. 30. September 2014. http://yapital.info/2014/09/yapital-noch-in-diesem-jahr-in-allen-deutschen-douglas-filialen/ (abgerufen am: 24. Oktober 2014).

231. GOUDINOUDIS, A. System-Update bei GRAVIS: Gadgets ab sofort mit Yapital bezahlen, 2014. 22. September 2014. http://yapital.info/2014/09/system-update-bei-gravis-gadgets-ab-sofort-mit-yapital-bezahlen/ (abgerufen am: 24. Oktober 2014).

232. GOUDINOUDIS, A. Bezahlen über alle Kanäle: Kooperation zwischen Yapital und Wirecard, 2014. 04. Februar 2014. http://yapital.info/2014/02/bezahlen-uber-alle-kanale-kooperation-zwischen-yapital-und-wirecard/ (abgerufen am: 24. Oktober 2014).

233. GOUDINOUDIS, A. Kooperation mit Weltmarktführer: VeriFone-Terminals standardmäßig für Yapital Smartphone-Zahlungen gerüstet, 2014. 10. September 2014. http://yapital.info/2014/09/kooperation-mit-weltmarktfuhrer-verifone-terminals-standardmasig-fur-yapital-smartphone-zahlungen-gerustet/ (abgerufen am: 24. Oktober 2014).

234. GOUDINOUDIS, A. Yapital and Ingenico ease handling of cross-channel payments, 2014. 10. September 2014. http://yapital.info/en/2014/09/yapital-and-ingenico-ease-handling-of-cross-channel-payments/ (abgerufen am: 24. Oktober 2014).

235. GROSSKLAUS, P. Yapital löst gemeinsam mit POSPartner und BLE-Beacons das Funkloch-Problem im Mobile Payment, 2014. 13. Februar 2014. http://yapital.info/2014/02/yapital-lost-gemeinsam-mit-pospartner-und-ble-beacons-das-funkloch-problem-im-mobile-payment/ (abgerufen am: 24. Oktober 2014).

236. GROSSKLAUS, P. Etablierung als Standard: ConCardis nimmt Yapital ins Portfolio, 2014. 03. April 2014. http://yapital.info/2014/04/etablierung-als-standard-concardis-yapital/ (abgerufen am: 24. Oktober 2014).

237. GROSSKLAUS, P. Yapital öffnet sich für Partnerschaften mit Banken, 2014. 14. Mai 2014. http://yapital.info/2014/05/yapital-partnerschaften-mit-banken/ (abgerufen am: 24. Oktober 2014).

238. YAPITAL FINANCIAL AG. Kosten & Gebühren, 2014. https://www.yapital.com/yapital_webcontent/ajax/costs_b2c/costs_deu.png (abgerufen am: 24. Oktober 2014).

239. YAPITAL FINANCIAL AG. Kosten & Gebühren für Geschäftskunden, 2014. https://www.yapital.com/deu/geschaeftskunden/kosten-und-gebuehren (abgerufen am: 24. Oktober 2014).

240. SKOPOS INSTITUT FÜR MARKT- UND KOMMUNIKATIONSFORSCHUNG. Nutzung und Akzeptanz von QR-Codes. Hürth, 7. Jul. 2014.

241. YAPITAL FINANCIAL AG. Händlervertrag, 2014. https://www.yapital.com/yapital_webcontent/pdf/haendlervertrag_s.pdf (abgerufen am: 26. Oktober 2014).

242. CUSTOMWEB GMBH. Yapital-Zahlungsmodule, 2014. http://www.sellxed.com/shop/de/extensions/module/payment-service-provider/yapital.html (abgerufen am: 26. Oktober 2014).

243. YAPITAL FINANCIAL AG. Yapital Partner im Überblick, 2014. https://www.yapital.com/deu/geschaeftskunden/partner/ (abgerufen am: 26. Oktober 2014).

244. GROSSKLAUS, P. Rundumschutz beim Kauf mit Yapital: Nutzer kostenfrei versichert, 2014. 04. März 2014. http://yapital.info/2014/03/rundumschutz-beim-kauf-mit-yapital-nutzer-kostenfrei-versichert/ (abgerufen am: 26. Oktober 2014).

245. GROSSKLAUS, P. Neue Vertriebskanäle und Werbung im Wandel durch QR-Codes, 2014. 05. September 2014. http://yapital.info/2014/09/neue-vertriebskanale-und-werbung-im-wandel-durch-qr-codes/ (abgerufen am: 26. Oktober 2014).

246. STRUDTHOFF, M. Interview: Yapital erweitert sein Omnichannel Payment um interessante neue Funktionen, 2014. 04. März 2014. http://www.mobile-zeitgeist.com/2014/03/04/interview-yapital-erweitert-sein-omnichannel-payment-um-immer-mehr-neue-funktionen/ (abgerufen am: 26. Oktober 2014).

247. PAYMEY GMBH. Paymey - Berlin - Bank/Finanzinstitut, 2013. https://www.facebook.com/PAYMEYcom?sk=info (abgerufen am: 25. Juni 2014).

248. PAYMEY GMBH. PAYMEY - AGB, 2014. https://www.paymey.com/agb.html (abgerufen am: 29. Oktober 2014).

249. PAYMEY GMBH. Crowdfunding für PAYMEY 2, 2014. 31. März 2014. https://www.seedmatch.de/startups/paymey-2 (abgerufen am: 29. Oktober 2014).

250. PAYMEY GMBH. Erste Schritte mit PAYMEY, 2014. https://www.paymey.com/erste-schritte-mit-paymey.html (abgerufen am: 30. Oktober 2014).

251. WOHLAND, R. Welche Limits gelten für Privatkunden?, 2014. 28. Mai 2014. https://paymey.zendesk.com/hc/de/articles/201927777-Welche-Limits-gelten-f%C3%BCr-Privatkunden- (abgerufen am: 30. Oktober 2014).

252. PAYMEY GMBH. Im Handel einkaufen, 2014. https://www.paymey.com/im-handel-einkaufen.html (abgerufen am: 30. Oktober 2014).

253. PAYMEY GMBH. Online einkaufen, 2014. https://www.paymey.com/online-einkaufen.html (abgerufen am: 30. Oktober 2014).

254. EBAY INC. eBay Inc. plant Trennung von eBay und PayPal in unabhängige börsennotierte Unternehmen in 2015, 30. Sep. 2014. 30. September 2014. http://presse.ebay.de/pressrelease/4649 (abgerufen am: 24. November 2014).

255. PAYPAL INC. Third-Party Shopping Carts – The Cart Upload Command, 2014. https://developer.paypal.com/webapps/developer/docs/classic/paypal-payments-standard/integration-guide/cart_upload/

256. PAYPAL INC. PayPal-Datenschutzgrundsätze, 2014. 14. Mai 2014. https://www.paypal.com/de/webapps/mpp/ua/privacy-full (abgerufen am: 31. Oktober 2014).

257. KASPERSKY LABS. Finanzielle Cyberbedrohungen im Jahr 2013, Teil 1: Phishing, 2014. 02. April 2014. http://www.viruslist.com/de/spam/analysis?pubid=200883849 (abgerufen am: 31. Oktober 2014).

258. PAYPAL INC. Kostenlose Tools: Sicherheitsschlüssel, 2014. https://www.paypal.com/de/cgi-bin/webscr?cmd=xpt/Marketing/securitycenter/general/PPSecurityKey-outside (abgerufen am: 31. Oktober 2014).

259. RIXECKER, K. PayPal: Sicherheitsexperten umgehen Zwei-Faktor-Authentifizierung, 2014. 25. Juni 2014. http://t3n.de/news/paypal-sicherheitsexperten-553437/ (abgerufen am: 31. Oktober 2014).

260. GUTEFRAGE.NET GMBH. 250€ Paypalguthaben geklaut (PayPal, Diebstahl), 2012. 06. April 2012. http://www.gutefrage.net/frage/250-paypalguthaben-geklaut#answers (abgerufen am: 31. Oktober 2014).

261. CHIP DIGITAL GMBH. PayPal Account gehackt - Was nun?, 2011. 29. Juni 2014. http://forum.chip.de/recht/paypal-account-gehackt-1531241.html (abgerufen am: 31. Oktober 2014).

262. KOWOLLIK, B. WDR 2 Quintessenz - Paypal-Betrug, 2014. 14. Januar 2014. http://www.wdr2.de/service/quintessenz/paypal104.html (abgerufen am: 31. Oktober 2014).

263. CHIP DIGITAL GMBH. PayPal gehackt: Cleverer Trick verdoppelt Guthaben, 2014. 16. Juni 2014. http://www.chip.de/news/PayPal-gehackt-Cleverer-Trick-verdoppelt-Guthaben_70359402.html (abgerufen am: 31. Oktober 2014).

264. WEKWERTH, M. PayPal und die Kontosperrung: Unterlassungsklage in Deutschland, 2011. 08. Dezember 2011. http://www.wekwerth.de/news/allgemein/paypal-kontosperrung-unterlassungsklage-in-deutschland/ (abgerufen am: 31. Oktober 2014).

265. SCHNURER, G. Vorsicht Kunde! - Erfasst, verknüpft und gesperrt. PayPal Kunden leben "sicherer", 2010. 06. November 2010. http://www.heise.de/video/artikel/Vorsicht-Kunde-Erfasst-verknuepft-und-gesperrt-PayPal-Kunden-leben-sicherer-1510769.html (abgerufen am: 31. Oktober 2014).

266. BAUM, A. Immer wieder Ärger mit PayPal. Mainz: ZDF, 2010.

267. ZEIT ONLINE GMBH. Kreditkartenbetrug: PayPal lässt Einkäufe mit gestohlenen Kreditkarten zu, 2010. 27. September 2010. http://www.zeit.de/digital/internet/2010-09/paypal-internet-sicherheit (abgerufen am: 31. Oktober 2014).

268. SPIEGEL ONLINE. Wachsender Druck: Paypal stoppt Geldfluss an WikiLeaks, 2010. 04. Dezember 2010. http://www.spiegel.de/netzwelt/netzpolitik/wachsender-druck-paypal-stoppt-geldfluss-an-wikileaks-a-732856.html (abgerufen am: 1. November 2014).

269. WAU-HOLLAND-STIFTUNG. Wau-Holland-Stiftung auf Twitter, 2010. 04. Dezember 2010. https://twitter.com/wauland/status/10987193778569216 (abgerufen am: 1. November 2014).

270. BRINKMANN, B. Paypal empört Online-Händler – Warum deutsche Firmen unter dem US-Embargo gegen Kuba leiden, 2012. 27. August 2012. http://www.sueddeutsche.de/wirtschaft/us-embargo-gegen-kuba-ho-ho-wo-ist-die-buddel-rum-1.1125589 (abgerufen am: 1. November 2014).

271. SAWALL, A. und A. SEBAYANG. Kuba-Blockade: Rossmann wirft Paypal nach Drohungen raus, 2011. 08. September 2011. http://www.golem.de/1109/86314.html (abgerufen am: 1. November 2014).

272. PAYPAL (EUROPE) S.À R.L. ET CIE, S.C.A. PayPal-Nutzungsbedingungen, 2014. 17. Juni 2014. https://www.paypal.com/de/webapps/mpp/ua/useragreement-full (abgerufen am: 1. November 2014).

273. PAYPAL (EUROPE) S.À R.L. ET CIE, S.C.A. PayPal für Händler - einfach Zahlungen akzeptieren & Umsatz steigern, 2014. https://www.paypal.com/de/webapps/mpp/merchant (abgerufen am: 1. November 2014).

274. PAYPAL INC. Beacon, 2014. https://www.paypal.com/us/webapps/mpp/beacon (abgerufen am: 1. November 2014).

275. BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK. Übersicht: Bezahlsystem-Anbieter. Berlin, 2010.

276. KLEES, M. Der Internet-Zahlungsverkehr aus Sicht der Verbraucher in D-A-CH – Ergebnisse der Umfrage IZV11. Eine Zusammenfassung der Studie des ECC über den Online-Payment-Markt in Deutschland, Österreich und der Schweiz. Köln.

277. Wie eröffne oder schließe ich ein PayPal-Konto?, 2014. https://www.paypal.com/de/webapps/helpcenter/helphub/article/?solutionId=FAQ1443&m=HTQ (abgerufen am: 4. November 2014).

278. Wie bestätige ich mein Bankkonto?, 2014. https://www.paypal.com/de/webapps/helpcenter/helphub/article/?solutionId=FAQ513&topicID=FIRST_STEPS_CONFIRMATION&m=TCI (abgerufen am: 4. November 2014).

279. PAYPAL DEUTSCHLAND. Nutzen Sie unsere PayPal App wie ein Portemonnaie, 2014. https://www.paypal.com/de/webapps/mpp/pay-in-stores (abgerufen am: 4. November 2014).

280. EICHENSEHER, A. Orderbird und PayPal weiten smartes Restaurant, 2014. 01. August 2014. http://www.gizmodo.de/2014/08/01/orderbird-und-paypal-weiten-smartes-restaurant-bezahlen-aus.html (abgerufen am: 4. November 2014).

281. SHOPWARE AG. Plugin: PayPal Payment, 2014. http://wiki.shopware.com/Plugin-PayPal-Payment_detail_1496.html (abgerufen am: 4. November 2014).

282. EISENBRAND, R. Bitcoin-Wahnsinn: Wie wir einmal eine Story schreiben wollten und dabei 5.000 Euro verdient haben, 2014. 03. Juni 2014. http://www.onlinemarketingrockstars.de/wie-wir-einmal-mit-bitcoins-5000-euro-verdient-haben/ (abgerufen am: 1. Juli 2014).

283. PAYMIUM. Frequently Asked Questions, 2014. 03. November 2014. https://paymium.com/page/help (abgerufen am: 6. November 2014).

284. BITCOIN DEUTSCHLAND AG. Geschäftsbedingungen der Bitcoin Deutschland AG, 2014. https://www.bitcoin.de/de/agb (abgerufen am: 6. November 2014).

285. BITCOIN DEUTSCHLAND AG. Trust-Level-Kriterien, 2013. 07. August 2013. https://www.bitcoin.de/de/infos#trust-level (abgerufen am: 5. Dezember 2014).

286. BITMIXER.IO. How does it works?, 2013. 20. Dezember 2013. https://bitmixer.io/how.html (abgerufen am: 6. November 2014).

287. BIRYUKOV, A., D. KHOVRATOVICH und I. PUSTOGAROV. Deanonymisation of Clients in Bitcoin P2P Network. In: G.-J. AHN, M. YUNG und N. LI, Hg. the 2014 ACM SIGSAC Conference, S. 15-29.

288. BITCOIN WIKI. Weaknesses, 2014. 04. September 2014. https://en.bitcoin.it/wiki/Weaknesses (abgerufen am: 6. November 2014).

289. SCHERSCHEL, F. Bitcoin-Dienstleister wider die 51-Prozent-Bedrohung, 2014. 17. Juli 2014. http://www.heise.de/security/meldung/Bitcoin-Dienstleister-wider-die-51-Prozent-Bedrohung-2262208.html (abgerufen am: 6. November 2014).

290. KANNENBERG, A. "Bitcoin-Brothers": Berliner Startup will das Mining umkrempeln, 2014. 05. November 2014. http://www.heise.de/newsticker/meldung/Bitcoin-Brothers-Berliner-Startup-will-das-Mining-umkrempeln-2442025.html (abgerufen am: 6. November 2014).

291. KANNENBERG, A. Studie stellt Bitcoin-Verlust bei Mt. Gox in Zweifel, 2014. 28. März 2014. http://www.heise.de/newsticker/meldung/Studie-stellt-Bitcoin-Verlust-bei-Mt-Gox-in-Zweifel-2156255.html (abgerufen am: 6. November 2014).

292. KANNENBERG, A. Bitcurex, Coinex und Canadian Bitcoins: Erneut Angriffe auf Bitcoin-Börsen, 2014. 19. März 2014. http://www.heise.de/newsticker/meldung/Bitcurex-Coinex-und-Canadian-Bitcoins-Erneut-Angriffe-auf-Bitcoin-Boersen-2150037.html (abgerufen am: 6. November 2014).

293. KAUFMANN, S. Digitale Währung: Bitcoin-Börse schließt nach Hacker-Angriff, 2014. 05. März 2014. http://www.berliner-zeitung.de/wirtschaft/digitale-waehrung-bitcoin-boerse-schliesst-nach-hacker-angriff,10808230,26479644.html (abgerufen am: 6. November 2014).

294. THOMA, J. Transaktionsfehler: Angreifer legen Bitcoin-Börsen lahm, 2014. 12. Februar 2014. http://www.golem.de/news/transkationsfehler-angreifer-legen-bitcoin-boersen-lahm-1402-104509.html (abgerufen am: 6. November 2014).

295. SPIEGEL ONLINE. Virtuelle Währung: Hack-Attacken bremsen Bitcoin-Rallye, 2013. 04. April 2013. http://www.spiegel.de/netzwelt/web/hacker-angriff-auf-bitcoin-dienst-instawallet-kurs-steigt-nicht-mehr-a-892438.html (abgerufen am: 6. November 2014).

296. CAP, C.H. Bitcoin – das Open-Source-Geld [online]. HMD - Praxis der Wirtschaftsinformatik, 2012, (283), 84-93. https://www.wiso-net.de/document/HMD__293CF66480B28C2ACFC0AE7CE943B303

297. VAN DER LAAN, W.J., G. ANDRESEN, J. GARZIK, G. MAXWELL und P. WUILLE. Glossar, 2014. 07. November 2014. https://bitcoin.org/de/glossar#bestaetigung (abgerufen am: 7. November 2014).

298. THOMA, J. Bitcoins: Mehr als 4,5 Millionen britische Pfund im Müll, 2013. 28. November 2013. http://www.golem.de/news/bitcoins-mehr-als-4-5-millionen-pfund-im-muell-1311-103025.html (abgerufen am: 7. November 2014).

299. DELL. Dell now accepts bitcoin, 2014. http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing (abgerufen am: 6. November 2014).

300. KANNENBERG, A. Expedia experimentiert mit Bitcoinzahlungen, 2014. 11. Juni 2014. http://www.heise.de/newsticker/meldung/Expedia-experimentiert-mit-Bitcoinzahlungen-2219669.html (abgerufen am: 6. November 2014).

301. RIZZO, P. Expedia Exec Says Bitcoin Spending Has Exceeded Estimates, 2014. 02. Juli 2014. http://www.coindesk.com/expedia-exec-bitcoin-payments-have-exceeded-estimates/ (abgerufen am: 6. November 2014).

302. GROßMANN, J. Reisen mit Bitcoin, 2013. 02. Dezember 2013. http://www.geo.de/GEO/reisen/reisewissen/internet-waehrung-reisen-mit-bitcoin-76510.html (abgerufen am: 7. November 2014).

303. BITCOIN WIKI. Transaction fees, 2014. 20. Juni 2014. https://en.bitcoin.it/wiki/Transaction_fee (abgerufen am: 7. November 2014).

304. COINBASE INC. What is Coinbase and how much does it cost to use?, 2014. 23. Oktober 2014. https://support.coinbase.com/customer/portal/articles/585625-what-is-coinbase-and-how-much-does-it-cost-to-use- (abgerufen am: 7. November 2014).

305. COINBASE INC. What fees does Coinbase charge for merchant processing?, 2014. 24. Oktober 2014. https://support.coinbase.com/customer/portal/articles/1277919-what-fees-does-coinbase-charge-for-merchant-processing- (abgerufen am: 7. November 2014).

306. BITPAY INC. Pricing, 2014. https://bitpay.com/pricing (abgerufen am: 7. November 2014).

307. COINKITE INC. Bitcoin Debit Card, 2014. https://coinkite.com/faq/card (abgerufen am: 8. November 2014).

308. BITPAY INC. Bitcoin for eCommerce, 2014. https://bitpay.com/bitcoin-for-ecommerce (abgerufen am: 8. November 2014).

309. COINKITE INC. Bitcoin Point of Sale, Payment and Exchange Terminal, 2014. https://coinkite.com/faq/terminal (abgerufen am: 8. November 2014).

310. LIU, A. Ripple Labs Releases Downloadable Ripple Client, 2014. 07. Mai 2014. https://ripple.com/ripple-labs-releases-downloadable-ripple-client/ (abgerufen am: 11. November 2014).

311. RIPPLE LABS INC. Creating a Ripple Wallet, 2014. 11. September 2014. https://support.ripplelabs.com/hc/en-us/articles/203247853-Creating-a-Ripple-Wallet (abgerufen am: 12. November 2014).

312. SNAPSWAP EU. SnapSwap Ripple Gateway Signup, 2014. 08. November 2014. https://snapswap.eu/#/signup (abgerufen am: 12. November 2014).

313. SCHWARTZ, D., N. YOUNGS und A. BRITTO. The Ripple Protocol Consensus Algorithm, 2014.

314. RIPPLE LABS INC. Reserves, 2014. 15. September 2014. https://wiki.ripple.com/Reserves (abgerufen am: 12. November 2014).

315. RIPPLE LABS INC. Transaction Fee, 2014. 15. September 2014. https://wiki.ripple.com/Transaction_fee (abgerufen am: 12. November 2014).

316. INTERNATIONAL RIPPLE BUSINESS ASSOCIATION. Ripple Gateways, 2014. http://www.xrpga.org/gateways.html (abgerufen am: 12. November 2014).

317. INTERNATIONAL RIPPLE BUSINESS ASSOCIATION. Exchangers, 2014. http://www.xrpga.org/exchangers.html (abgerufen am: 12. November 2014).

318. INTERNATIONAL RIPPLE BUSINESS ASSOCIATION. Market Makers, 2014. http://www.xrpga.org/market-makers.html (abgerufen am: 12. November 2014).

319. INTERNATIONAL RIPPLE BUSINESS ASSOCIATION. Merchants, 2014. http://www.xrpga.org/merchants.html (abgerufen am: 12. November 2014).

320. TOP RATE ENTERPRISES L.P. SmartyCash Visa Card, 2014. http://smartycash.biz/ (abgerufen am: 12. November 2014).

321. RIPPLE LABS INC. Activating Your Wallet, 2014. 15. Oktober 2014. https://support.ripplelabs.com/hc/en-us/articles/202964876-Activating-Your-Wallet (abgerufen am: 12. November 2014).

322. SNAPSWAP INC. SmartyCash Visa Card Fees Schedule, 2014. 12. November 2014. http://help.snapswap.vc/knowledgebase/articles/396454 (abgerufen am: 12. November 2014).

323. RIPPLE LABS INC. Merchant Integration Guide, 2014. 15. September 2014. https://wiki.ripple.com/Merchant_Integration_Guide (abgerufen am: 27. November 2014).

324. RIPPLE LABS INC. Merchant Integration Manual, 2014. 15. September 2014. https://wiki.ripple.com/Merchant_Integration_Manual (abgerufen am: 13. November 2014).

325. THE ROCK TRADING LTD. FAQ - Frequently Asked Questions, 2014. https://www.therocktrading.com/en/pages/faq (abgerufen am: 13. November 2014).

326. GAITATZIS, T. Ripple Wallet, 2013. 10. Juni 2013. https://play.google.com/store/apps/details?id=com.phonebank.ripplewallet (abgerufen am: 13. November 2014).

327. RIPPLE LABS INC. Rippled, 2014. 28. Oktober 2014. https://wiki.ripple.com/Rippled (abgerufen am: 27. November 2014).

328. MAGENTO. Ripple (JSON-RPC), 2014. 24. Februar 2014. http://www.magentocommerce.com/magento-connect/ripple-json-rpc.html (abgerufen am: 13. November 2014).

329. BLOCKR.IO. Bitcoin Block Explorer. Bitcoin Blockchain Market and Price, 2014. 17. September 2014. http://btc.blockr.io/ (abgerufen am: 10. November 2014).

330. BLOCKR.IO. Peercoin Block Explorer. Peercoin Blockchain Market and Price, 2014. 17. September 2014. http://ppc.blockr.io/ (abgerufen am: 10. November 2014).

331. COINMARKETCAP. Virtuelle Währungen - Digitale Zahlungsmittel nach Marktkapitalisierung 2014. Zitiert nach de.statista.com, 2014. 03. November 2014. http://de.statista.com/statistik/daten/studie/296205/umfrage/marktkapitalisierung-digitaler-zahlungsmittel/ (abgerufen am: 10. November 2014).

332. PEERCOIN. Payment Integration Guide, 2014. http://www.peercoin.net/payment-integration-guide (abgerufen am: 10. November 2014).

333. *IPSOS. Zahlungsverhalten in Deutschland. Erfüllung der Kriterien für Zahlungsinstrumente durch die einzelnen Instrumente aus Nutzersicht, 2010. http://de.statista.com/statistik/daten/studie/13137/umfrage/erfuellung-einzelner-kriterien-durch-zahlungsinstrumente/ (abgerufen am: 13. Juni 2014).*

334. *SCHMIDT, H. Samsung zieht Konkurrenz in Deutschland weiter davon, 2014. 13. April 2014. http://netzoekonom.de/2014/04/13/samsung-zieht-konkurrenz-in-deutschland-weiter-davon/ (abgerufen am: 17. November 2014).*

335. *GRUNEWALD, A. Unser mobiler Planet: Deutschland. Hamburg, Mai 2012.*