STUDIEN ZUM FINANZ-, BANK- UND VERSICHERUNGSMANAGEMENT

Hrsg.: Professor Dr. Reinhold Hölscher

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Band 4

CYBER MONEY

- Entwicklungstendenzen und Abwicklungstechniken im Internet -

von

Stefan Dreher

Kaiserslautern 1999

ISSN 1435-8484

Technische Universität Kaiserslautern
Lehrstuhl für Finanzdienstleistungen und Finanzmanagement
Postfach 3049
67653 Kaiserslautern

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

ARPA	Advanced Research Projects Agency
CEPS	Committee for European Payment Systems
DES:	Data Encryption Standard
DNS:	Domaine Name System
ECBS:	European Committee for Banking Standards
FTP:	File Transfer Protocol
FV:	First Virtual
GwG:	Geldwäschegesetz
HBCI-Standard:	Home Banking Computer Interface-Standard
HTML:	Hyper Text Markup Language
HTTP:	Hyper Text Transfer Protocoll
IP-Nummer:	Adresse eines Computers im Internet.
JAVA:	Programmiersprache
KWG:	Kreditwesengesetz
MIPS:	Million Instruktionen pro Sekunde
PIN:	Persönliche Identifikationsnummer
RSA:	Rivest, Shamir, Adleman.
SET:	Secure Electronic Transaction
SSL:	Secure Socket Layer. Verschlüsselungsverfahren
TAN:	Transaktionsnummer
TCP/IP:	Transfer Control Protocol/Internet Protocol
TOB:	T-Online Billing TOB
URL:	Uniform Resource Locator

Einleitung

In den letzten Jahren hat sich das Internet mit zunehmender Geschwindigkeit zu einem internationalen, virtuellen Marktplatz entwickelt, dem sogenannten Cyber Space. Cyber Space und Cyber Money sind typische Begriffe des beginnenden Informationszeitalters. „Cyber Space“ stammt ursprünglich aus der Feder von William Gibson, der in seinem Science Fiction Roman „Neuromancer“ aus dem Jahre 1984 diesen Begriff zum ersten mal erwähnte und somit dem Wort „Cyber“ seine aktuelle Bedeutung gab.

Cyber Money oder allgemeiner Digital Cash bietet in letzter Zeit genügend Spielraum für Spekulationen. So befinden sich die unterschiedlichsten Einschätzungen bezüglich der Auswirkungen von Elektronischem Geld auf die wirtschaftspolitischen Konsequenzen bzw. die volkswirtschaftlichen Folgen im Umlauf. Besonders bezüglich der Auswirkungen auf die Geldpolitik gibt es eine recht große Bandbreite an verschiedenen Meinungen und Argumenten.

Als Informationsforum und Werbeträger hat sich das Internet mittlerweile hinlänglich etabliert. Immer mehr Unternehmen wollen nun auch ihre Produkte im Netz anbieten. Dies kann jedoch nicht ohne geeignete Zahlungssysteme erfolgen. Die Erfahrung hat gezeigt, daß Online-Bestellungen mit anschließendem Versand per Nachnahme oder Rechnung nur bedingt geeignet sind. Da die verbindliche Unterschrift fehlt, gehen zu viele Bestellungen „ins Leere“. Noch problematischer ist die Vermarktung von digitalen Gütern. Hier sollte die Ware bereits vor der Online-Lieferung bezahlt sein.

Die vorliegende Studie wird zunächst die Rahmenbedingungen beleuchten, die für den Einsatz von elektronischem Geld im Internet benötigt werden. Dabei wird der Schwerpunkt auf das Wesen des Electronic Commerce und das Internet an sich gelegt. Ferner werden geldpolitische Anforderungen und das Agieren von Banken im Internet betrachtet. Im zweiten Teil werden dann die bekanntesten und vielversprechendsten Arten von Cyber Money vorgestellt, in ihren Grundzügen erläutert und bewertet. Der letzte Teil befaßt sich schließlich mit den Auswirkungen auf die am elektronischen Zahlungsverkehr im Internet beteiligten Parteien sowie den zu erwartenden Tendenzen und Möglichkeiten.

A. Rahmenbedingungen und Prämissen für den Einsatz von Cyber Money

Der erfolgreiche Einsatz von Cyber Money im Internet ist an eine Reihe von Bedingungen geknüpft, die im ersten Teil der Arbeit näher betrachtet werden sollen. Zum einen hängt die Entwicklung von Zahlungssystemen für das Internet sehr stark mit der des Electronic Commerce zusammen. Beide sind im Prinzip aufeinander angewiesen. Zum anderen muß ein Zahlungssystem auch den Anforderungen der Zentralbank bzw. deren Geldpolitik genügen. Neuere Systeme bauen deshalb direkt auf den gesetzlichen Bestimmungen auf.

I. Internet und Electronic Commerce

In den USA wird das Internet bereits als „die wirtschaftliche Infrastruktur des 21. Jahrhunderts“ angesehen. Selbst wenn dies auf den ersten Blick als gewagte These klingt, so wird dem Internet doch ein enormes Potential eingeräumt. Es ist zu erwarten, daß durch das Internet sowohl sämtliche Formen des Einzelhandels als auch der Markt für Dienstleistungen einem grundlegenden Wandel unterzogen werden. Sogenannte „Netz-Gurus“ prophezeien, daß Unternehmen auf mittelfristige Sicht ohne Präsenz im Internet nicht mehr bestehen können[1]. Die Entwicklung des virtuellen Marktplatzes wird auch durch die Deregulierung von herkömmlichen Märkten, dem Verschwinden von Regionen- und Branchengrenzen und der ständig wachsenden Informations- und Kommunikationsinfrastruktur gefördert. Die so entstehenden elektronischen Märkte werden von Fachleuten auch als der „sechste Kontinent“ bezeichnet, der in Zukunft als Standort für Electronic Commerce dienen wird[2].

1. Das Internet als Medium der virtuellen Welt

Der Grundstein der Internet-Entwicklung wurde während des kalten Krieges durch ein amerikanisches Rüstungsprojekt gelegt. Im Auftrag des US Verteidigungsministerium wurde das Internet zwischen 1959 und 1969 von der ARPA (Advanced Research Projects Agency) und einigen anderen Forschungseinrichtungen entwickelt[3]. Das Ziel war, ein Computernetz zu schaffen, welches selbst bei Ausfall einiger Teile des Systems noch funktionsfähig bleiben sollte[4]. Die wesentlichen Eigenschaften, die das Internet heute prägen, waren schon damals vorhanden:

---

1 Vgl. BECKER (Ohne Webseite, 1998), S. 19.
2 Vgl. BIRKELBACH (Cyber Finance, 1997), S. 40-41.
3 Zur Geschichte des Internet siehe auch http://info.isoc.org/zakon/internet/history/hit.htm.
4 Gedacht wurde hier an einen potentiellen Atomschlag der UdSSR.

- Datenaustausch zwischen verschiedenen Computersystemen,
- automatisches Umleiten von Informationen,
- die typische Internet Architektur (ein Netzwerk von Netzwerken)[5] sowie

das einheitliche Übertragungsprotokoll TCP/IP (Transfer Control Protocol/Internet Protocol).

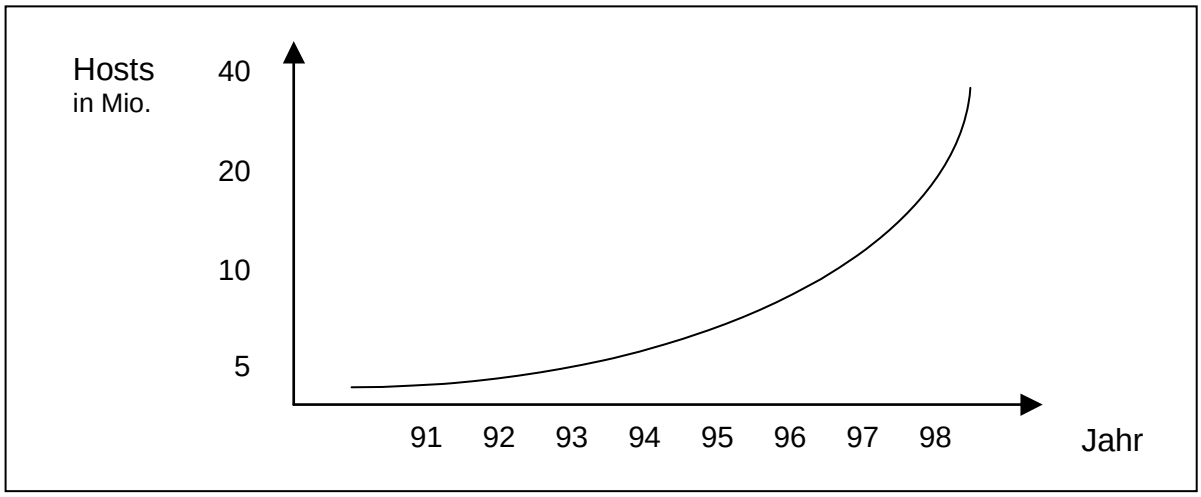

Abbildung 1: Weltweite Entwicklung der Hosts seit 1991[6]

Über TCP/IP können die ansonsten inkompatiblen Netzwerke miteinander verbunden werden. Dabei regelt das Internet Protokoll (IP) die richtige Adressierung der angeschlossenen Rechner und das TCP diverse Zusatzdienste wie die Datenflußkontrolle und die Wiederherstellung verlorener oder defekter Daten-Pakete. Für eine eindeutige Identifizierung aller im Netz befindlichen Rechner ist die sogenannte IP-Adresse verantwortlich. Diese ist aus jeweils vier Zahlen aufgebaut, z.B. 131.246.119.252. Die Zahlen geben dabei die hierarchische Netzstruktur an. Um eine anschaulichere Adressierung zu erhalten, wird die TCP/IP Nummer mit dem DNS (Domain Name System) verknüpft. Dieser ersetzt die IP-Nummer durch einen leicht zu merkenden Namen wie z.B. www.uni-kl.de. Die komplett ausgeschriebene Adresse (http://www.uni-kl.de) wird auch URL (Uniform Resource Locator) genannt.

Bestand das erste funktionierende Netz lediglich aus vier Rechnern, so wurde durch die Erlaubnis an einige Universitäten und Forschungseinrichtungen, sich mit dem Arpanet zu verbinden, die Anzahl schnell erhöht. Bereits 1973 wurden erste internationale Verbindungen nach Großbritannien und Norwegen aufgebaut. Ende 1975 waren bereits über 100 sogenannter Hosts an das Netzwerk angeschlossen und schon bald wurden die ersten Internetprovider gegründet. Bis 1991 wurde so eine Anzahl von ca. 500.000 Hosts erreicht, die bereits Mitte

[5] Vgl. LYNCH (Zahlungsverkehr, 1997), S. 25.
[6] Quelle: Internet Domain Survey.

1997 auf nahezu 20 Mio. exponentiell angestiegen ist[7]. Abbildung 1 gibt diese Entwicklung deutlich wieder. Heute umfaßt das Internet etwa 50.000 Netzwerke, wodurch der Datenverkehr im Backbone, dem sogenannten Rückgrat des Internets, exponentiell angestiegen ist. Ein Überblick über die aktuelle Struktur der europäischen Backbones kann im Internet eingesehen werden[8].

Innerhalb des Internets wurde schließlich das World Wide Web, kurz WWW als neuer Dienst neben e-mail und ftp (file transfer protocol) eingerichtet[9]. Das WWW, ursprünglich ebenfalls nur für Forschungszwecke gedacht, ist als Ansammlung von Hypertext-Dokumenten und –Verknüpfungen zu verstehen, die alle auf dem HTML (Hyper Text Markup Language) Standard beruhen. HTML ist eine sogenannte Auszeichnungssprache (Markup Language). Sie hat die Aufgabe, die logischen Bestandteile eines Dokuments zu beschreiben. Als Auszeichnungssprache enthält HTML daher Befehle zum Markieren typischer Elemente eines Dokuments, wie Überschriften, Textabsätze, Listen, Tabellen oder Grafikreferenzen[10]. Die Entwicklung von HTML-Browsern ermöglichte schließlich einfaches Betrachten von HTML-Dateien und Bewegen innerhalb des WWW. Die Errichtung des WWW im Internet ist vergleichbar mit der Umstellung von DOS auf Windows. Anstatt Befehlszeilen werden Mausklicks getätigt und Informationen werden graphisch anschaulich präsentiert[11]. Wenn heute also vom Internet geredet wird, ist vielmals nur das WWW gemeint, das mit seiner Informations- und Benutzervielfalt eine ideale Basis für eine kommerzielle Nutzung bzw. Electronic Commerce darstellt[12].

2. Entstehung des Electronic Commerce

Basis für Electronic Commerce ist ein elektronischer Marktplatz. Darunter wird eine Infrastruktur verstanden, die unter Verwendung von Informations- und Kommunikationstechnik ein Forum für Anbieter und Nachfrager zum Zwecke des Handels mit Waren und Dienstleistungen darstellt[13]. Hinzu kommen die Abwicklung des Geldverkehrs und die Geschäftsregeln in Online-Netzen[14]. Die grundlegende Struktur von Electronic Commerce läßt sich am besten durch eine technische, eine anwendungs- und eine umfeldbezogene Ebene charakterisieren.

---

7 Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 20.
8 Siehe unter http://www.ebone.net/structure/backbone.htm.
9 Entwickelt von Tim Berners-Lee im Europäischen Labor für Teilchenphysik CERN in Genf.
10 Siehe SELFHTML V. 7.0 von Stefan Münz (1998).
11 Vgl. SIETMANN (Electronic Cash, 1997), S. 25.
12 Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 30.
13 Vgl. PERNUL / RÖHM (Neuer Markt, 1997), S. 345.
14 Vgl. RAPP (Tendenzen, 1998), S. 12.

Die technische Ebene enthält die Bausteine Infrastruktur, Datenkommunikation, digitalisierte Inhalte und Abwicklung von Prozessen. Auf der anwendungsbezogenen Ebene lassen sich unter anderem Home-Shopping, Online-Spiele, Online-Marketing und Werbung nennen. Zum Umfeld lassen sich Faktoren wie Institutionalisierung, Kodifizierung und Abstimmung von rechtlichen, politischen und sozialen Belangen anführen[15].Die Entwicklung des Electronic Commerce wurde auch durch Internet-Provider wie AOL (America Online), CompuServe und T-Online begünstigt. Der Aufbau eigener Netzwerke mit einer Angebotspalette von Unterhaltung über Online-Shopping bis hin zum Internet-Banking sicherte zu Beginn reichlich Kundenzuwachs, der aus der steigenden Zahl der Internetnutzer rekrutiert werden konnte. Entsprechend gekennzeichnete gebührenpflichtige Dienste oder Inhalte werden ähnlich wie beim Telefon über die monatliche Abrechnung bezahlt. Dabei können sowohl fixe Beträge als auch kürzere Taktzyklen abgerechnet werden. Bei Nutzung des Online-Shopping kommt dem Verkäufer zugute, daß der Kunde bereits dem Provider mit Anschrift und Bankverbindung bekannt ist und er folglich ein geringeres Risiko beim Zahlungsvorgang trägt. Der Online-Dienst übernimmt somit die „Rolle des vertrauenswürdigen Dritten bei der Abrechnung von Leistungen zwischen Anbietern und Kunden“[16]. Erst der Ausbau des WWW zu einem immer attraktiver werdenden Medium brachte schließlich eine breite Basis an potentiellen Kunden für einen erfolgversprechenden Ausbau des Electronic Commerce. Mit der Zeit haben sich so diverse Geschäftsmodelle zur Nutzung des WWW gebildet, dabei lassen sich folgende als besonders häufig vertretene nennen[17:]

- Direktvertrieb von Produkten und Dienstleistungen,
- Werbung,
- Vermittlung und Makelei,
- Datenbankzugriffe bzw. –abfragen sowie
- Online-Transaktionen.

Unter diesen ist vor allem die Werbung als der erste Schritt zur Kommerzialisierung des Internet herauszuheben. Das sogenannte „Webvertising“ beschränkte sich zunächst auf die Netzpräsenz über die eigene Homepage, welches aber bald durch kostenpflichtige Verweise auf häufig frequentierten Seiten von Suchmaschinen oder anderen „Treffpunkten“ im Netz ausgebaut wurde. So gibt es mittlerweile Agenturen, die sich auf das Auffinden solcher Seiten

15 Vgl. SCHODER / STRAUSS (Electronic Commerce, 1997), S. 52-53.
16 PERNUL / RÖHM (Neuer Markt, 1997), S. 345.
17 Vgl. SIETMANN (Electronic Cash, 1997), S. 31-36.

und die Vermarktung von Links spezialisiert haben. Begehrte Seiten in Deutschland sind neben den üblichen Suchmaschinen bei einigen Fernsehsendern oder Zeitschriften zu finden, also bei Medien, zu denen der Verbraucher bereits Kontakt hat[18].

3. Verborgenes Potential

Ohne Zweifel wird durch das Internet eine neue Ära des globalen Wettbewerbs eingeläutet. Sowohl die zunehmende Präsenz von Unternehmen im Internet als auch die ständig steigende Quote von PCs mit Internetanbindung sprechen eine deutliche Sprache. Von den deutschen Großunternehmen sind bereits über 98% im Internet vertreten. Bei kleineren und mittelständischen Unternehmen ist die Präsenz eher schwankend und vor allen Dingen von der jeweiligen Branche abhängig. Dabei bietet das Internet gerade für kleinere Unternehmen nicht zu vernachlässigende Vorteile, da hier nicht die Größe sondern die Geschwindigkeit und die Flexibilität ausschlaggebend sind. Die jüngste IBM-Studie belegt, daß 85% der europäischen Unternehmen Nachteile erwarten, wenn sie nicht in Electronic Commerce investieren. Zwar erzielen neun von zehn Unternehmen, die über das Internet Geschäfte tätigen, noch keinen Gewinn, für sie zählt zum gegenwärtigen Zeitpunkt lediglich das Dabeisein[19].

Die Welthandelsorganisation (WTO) schätzt die Anzahl der Internet-User zur Zeit auf ca. 100 Millionen. Bis zur Jahrtausendwende soll nach Meinung von IBM die Zahl bereits auf ein Vielfaches angewachsen sein[20]. Umsätze in Höhe von rund 14 Mrd. DM im Jahre 1997 sind erst der Anfang von geschätzten Jahresumsätzen von ca. 500 bis 600 Mrd. DM weltweit ab dem Jahr 2000[21].

Dies würde für Industrieländer bedeuten, daß etwa ein Viertel der Wirtschaftstätigkeiten über das Internet abgewickelt wird. Umgerechnet auf den globalen Güter- und Serviceumsatz entspräche dies etwa 8 Prozent[22]. Für Deutschland prophezeit eine Untersuchung von A.T. Kearney Research eine Steigerung des Marktvolumens von derzeit 500 Mill. DM auf realistische 5 Mrd. DM innerhalb der nächsten fünf Jahre.

---

18 Vgl. STEINAU (Electronic Commerce, 1998), S. 54-64.

19 Vgl. IGLER (Mit virtuellem Geld, 1998), S. 55.

20 Gegenwärtig verdoppelt sich die Anzahl der Internet-Nutzer alle 12 bis 15 Monate.

21 Schätzungen diesbezüglich gehen jedoch weit auseinander. IBM z.B. erwartet in einer aktuellen Studie vom Dezember 98 ein weltweites Marktvolumen von 600 Milliarden US$ für 2002.

22 Vgl. BÜRKEL (Chancen, 1998), S. 327 und FLIEGE (Anonymer Zahlungsverkehr, 1998), S. 42.

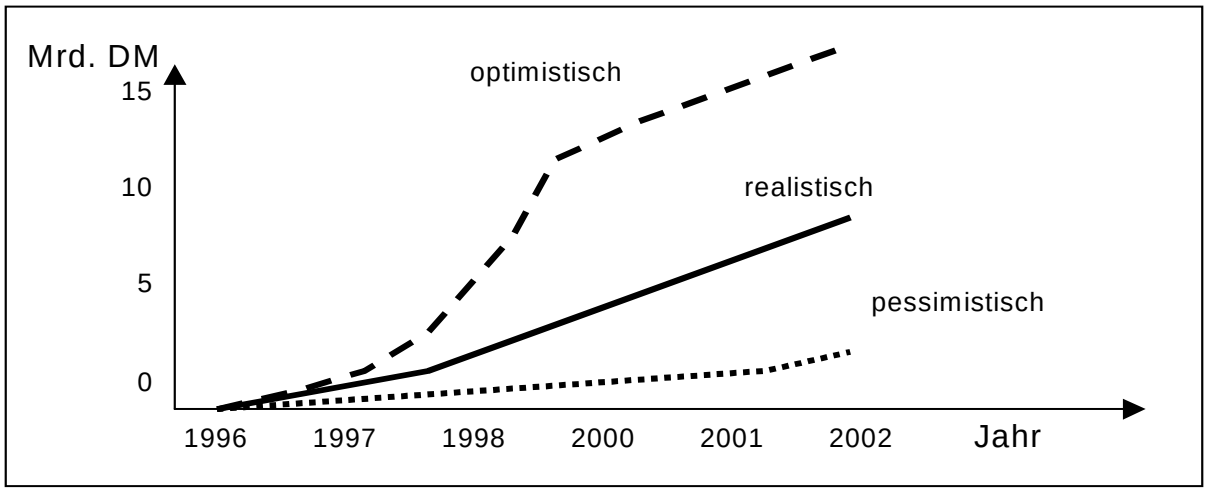

Abbildung 2: Entwicklungsszenarien für Electronic Commerce in Deutschland[23]

Dies gilt jedoch alles nur unter der Voraussetzung, daß es sichere und allgemein akzeptierte Zahlungsmittel gibt[24]. Die meisten Phasen eines Geschäfts lassen sich bereits über das Internet abwickeln. So besteht die Möglichkeit Kontaktaufnahme, Verhandlungen, Abmachungen und teilweise sogar die Lieferung digital zu betreiben, lediglich bei der Bezahlung gibt es Engpässe[25]. Der durch das Fehlen von internetfähigen Zahlungssystemen verursachte Medienbruch im Verkaufsprozeß wird in Abbildung 3 anschaulich dargestellt.

Als Beispiele für einen Vertrieb über das Internet wird unter anderem auch die Lebensmittelbranche genannt. Dinge des alltäglichen Gebrauchs sollen bequem über das Internet geordert werden können. Bezahlt wird dabei online über das Internet, geliefert wird noch am selben Tag per Kurier einer Servicekette[26]. Auch bereits etablierte Versandhäuser wie Quelle, Neckermann oder Otto bieten teilweise ihr komplettes Sortiment im Internet an[27].

[23] Quelle: A.T. Kearney Research.
[24] Vgl. LÜTGE (Viele Bits, 1997), S. 22.
[25] Vgl. PADOVAN / BUSSIEK (Grenzenloses Wirtschaften, 1998), S. 249.
[26] Für den Bereich Mannheim / Ludwigshafen ist dies bei Markant bereits möglich.
[27] Marktstatistiken zu etlichen Untersuchungen finden sich auch bei KRAUSE (Electronic Commerce, 1998), S. 62-70.

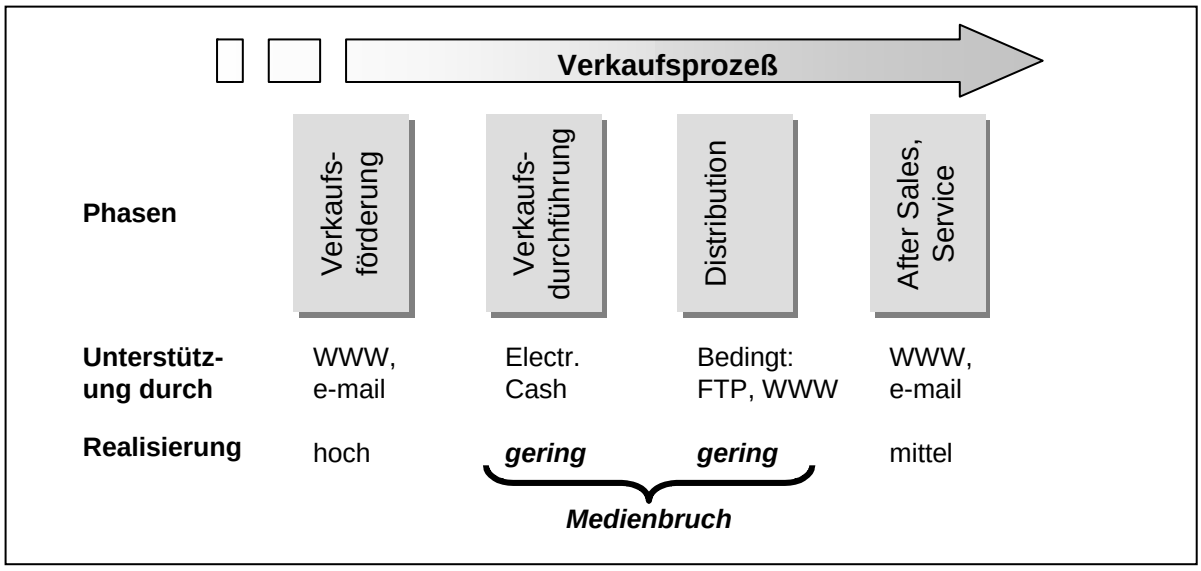

Abbildung 3: Der Verkaufsprozess und seine Unterstützung im Internet[28]

Für viele Branchen bietet das WWW vor allem die Chance, ein relativ kostengünstiges Filialnetz aufzubauen. Dabei muß nicht in Immobilien bzw. Ladengeschäfte investiert werden und der Personalbedarf bleibt relativ gering. Durch steigende Ansprüche an Qualität und Quantität werden vermehrt die elektronischen anstatt der physischen Informations- und Vertriebswege ausgebaut. Gestiegener Komfort und Bequemlichkeit zeigen sich auch in der räumlichen und zeitlichen Unabhängigkeit des Kunden. Es bieten sich bislang nicht gekannte Vergleichsmöglichkeiten, wobei regionale Barrieren durch Mausklicks überwunden werden[29].

Cyber Malls, virtuelle Kaufhäuser oder sonstige Online-Vertriebe gibt es bereits zuhauf. Das größte Hindernis für einen umsatzstarken Online-Handel bleibt jedoch der Mangel an adäquaten elektronischen Zahlungssystemen. Insofern hängt die weitere Entwicklung des Electronic Commerce nicht unwesentlich davon ab, inwieweit es gelingt, den Erwartungen des Kunden nach „Convenience“ bei der Bezahlung der Produkte und Dienstleistungen zu entsprechen[30].

II. Notwendigkeit von Zahlungsmitteln im Internet

Um mit den exponentiellen Wachstumsraten des Internet Schritt halten zu können, müssen die bisher existierenden Zahlungssysteme angepaßt werden. Eine Untersuchung des Handelsblattes konnte diesbezüglich nur sehr mühsame Möglichkeiten feststellen. Folglich haben herkömmliche Zahlungssysteme ihre Möglichkeiten so gut wie ausgeschöpft. Im folgenden Abschnitt dieser Studie soll auf die Grenzen herkömmlichen Geldes näher eingegangen werden

[28] Vgl. STOLPMANN (Elektronisches Geld, 1998), S. 34.
[29] Vgl. RAPP (Tendenzen, 1998), S. 13.
[30] Vgl. PERNUL / RÖHM (Neuer Markt, 1997), S. 345.

und daraus geldpolitische Anforderungen an elektronische Zahlungssysteme abgeleitet werden. Schließlich wird noch betrachtet, wieweit sich die deutschen Kreditinstitute bereits mit dem Medium Internet auseinandergesetzt haben.

1. Herkömmliches Geld und seine Grenzen

Die Geschichte des Geldes ist die Geschichte seines Verschwindens, seiner Entmaterialisierung. Die materielle Basis des Geldes verringerte sich mit jeder Weiterentwicklung. Teilweise wird auch vom *Entsubstantialisierungsprozeß* im Laufe der geldgeschichtlichen Entwicklung gesprochen[31].

Erst vor ca. 2500 Jahren wurde der Tauschhandel mit Naturalien teilweise durch die Verwendung von Münzen aus Metall oder Edelmetall ersetzt. Gute 2000 Jahre später tauchten dann die ersten Geldscheine auf, welche lange durch einen Goldgegenwert abgesichert waren. Erst die staatlich garantierte Annahmepflicht und Vertrauen in die Rechtsordnung konnte den sogenannten Goldstandard aufheben. Doch selbst im Industriezeitalter kam es vor allem beim Handel mit schwächeren Volkswirtschaften immer wieder zu Tauschgeschäften. Maschinen gegen Kaffee, Öl oder andere Rohstoffe. Größere Konzerne mußten eigens Abteilungen für den Barter-Trade unterhalten, welche die Tauschgüter in Geld zu konvertieren versuchten[32]. Hieraus ist ersichtlich, daß die Verwendung von Geld den Wirtschaftsprozeß erheblich vereinfachen kann.[33]

Das heute verwendete Geld besteht in der Regel aus Papier oder Metall, hat also eine physische Existenz. Jedoch hat bereits heute ein Großteil des Geldes virtuellen Charakter[34]. Sämtliche Guthaben auf Bankkonten oder Transaktionen zwischen diesen sind nichts anderes, als digitale Informationen. Der Bargeldanteil der Bundesrepublik Deutschland beläuft sich noch auf ca. 11% der Geldmenge M_3, der Rest ist Buch- bzw. Giralgeld[35]. Auch Computergeld wird als Giralgeld verstanden, da es sich von Buchgeld nur durch die technische Erfassung, nicht aber im Wesen unterscheidet[36]. Herkömmliche Zahlungssysteme wie Bargeld, Schecks oder Kartenzahlungen weisen in verschiedener Hinsicht eine Reihe von Nachteilen auf, die bei neuartigen Zahlungssytemen reduziert werden könnten[37]:

---

31 Vgl. HAHN (Währungsrecht, 1990).
32 Vgl. SIETMANN (Electronic Cash, 1997), S. 2 und JAHN (Geld, 1995), S. 24.
33 Vgl. SCHIERENBECK/HÖLSCHER (BankAssurance, 1998), S. 3
34 VAK (Unterwegs, 1995) unterscheidet 5 Perioden des Geldes.
35 Vgl. SIETMANN (Electronic Cash, 1997), S. 8.
36 Vgl. SCHAAL (Geldtheorie, 1998), S. 16.
37 Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 36-38.

- *Hohe Transaktionskosten*: Der Einzelhandel erfährt bei Bareinnahmen einen Verlust von 2 bis 4 Prozent durch Zählen, Sicherheit und Transport. Für die Bezahlung mit Kreditkarten werden ebenso Gebühren von ca. 1 bis 3 Prozent verlangt.
- *Zinsverluste*: Das Mitführen von Bargeld oder Geld auf der Geldkarte führt zu Zinsverlusten. Zwar kommt es auch bei digitalem Geld auf dem PC nicht zur Zinsbildung, es besteht jedoch die Möglichkeit einer schnelleren Rückführung in Giralgeld.
- *Geringe Transaktionsgeschwindigkeit*: Die Suche nach dem passenden Kleingeld oder Wechselgeld, die Online-Überprüfung bei Kreditkarten samt Unterschrift oder das Ausfüllen eines Scheckformulars können sehr zeitaufwendig sein.
- *Mangelnde Anonymität bei Kreditkarten*: Durch die relativ genauen Angaben des Verwendungszweckes bei der Kreditkartenabrechnung ist die theoretische Erstellung von Kundenprofilen möglich und wird zumindest in den USA auch teilweise praktiziert.
- *Steigende Herstellungskosten*: Um der geforderten Fälschungssicherheit zu entsprechen, müssen vor allem Banknoten immer raffinierter hergestellt werden[38]. Bei einer digitalen Währung sind die Entwicklungskosten wahrscheinlich höher, die Erstellung von Geldeinheiten aber fast kostenfrei.
- *Geringe Umweltfreundlichkeit*: Die Herstellung von Banknoten ist mit einem starken Verbrauch von Schwermetallen und anderen giftigen Substanzen verbunden. Zudem müssen Banknoten nach bereits relativ kurzer Zeit erneuert werden.
- *Sicherheitsmängel*: Der Verlust von Bargeld wird nicht ersetzt.
- *Fehlende Flexibilität*: Das Volumen von Bargeld steigt etwa proportional zu seinem Wert. Eine digitale Geldbörse bleibt immer gleich groß bzw. klein. Bargeld verlangt auch nach einer Mindestumlaufmenge, so daß stets Wechselgeld gewährleistet werden kann.
- *Schlechte Hygiene*: Gerade im Einzelhandel kann man oft beobachten, daß von den selben Personen sowohl kassiert als auch bedient wird.
- *Gebundenheit*: Keine Übertragung in offene Netze wie z.B. dem Internet.

Auf das Wesentliche reduziert beinhaltet Geld lediglich diverse Informationen: über Angebot und Nachfrage, also über den Wert und die Knappheit des Gutes sowie über die zeitliche und räumliche Dimension des Tausches. Je mehr Zahlungsvorgänge stattfinden und je höher die Summe der Zahlungen innerhalb einer Volkswirtschaft ist, desto störender werden umständli-

[38] Wasserzeichen, Metallapplikationen, Durchsichtsregister und 3D- oder Kipp-Effekte sind Beispiele dafür.

che Geldsysteme, so daß sich automatisch effizientere und schnellere Systeme entwickeln. Aus diesen Gründen werden auch Münzen und Banknoten allmählich durch digitale oder virtuelle Einheiten, sogenannte *Geldsurrogate* substituiert. Die bereits seit längerer Zeit geläufigen Kreditkarten und EC-Karten sowie die neuere Geldkarte zielen deutlich in diese Richtung[39].

2. Geldpolitische Anforderungen an Cyber Money

Zahlungsverkehr und Geldpolitik sind in der Bundesrepublik sowohl traditionell als auch rechtlich eng miteinander verknüpft. Grundsätzlich gelten für digitales Geld die selben Anforderungen wie für herkömmliches Geld. Eine Bewertung der verschiedenen Geldformen bezüglich ihrer Geldnähe wird in Abbildung 4 gezeigt.

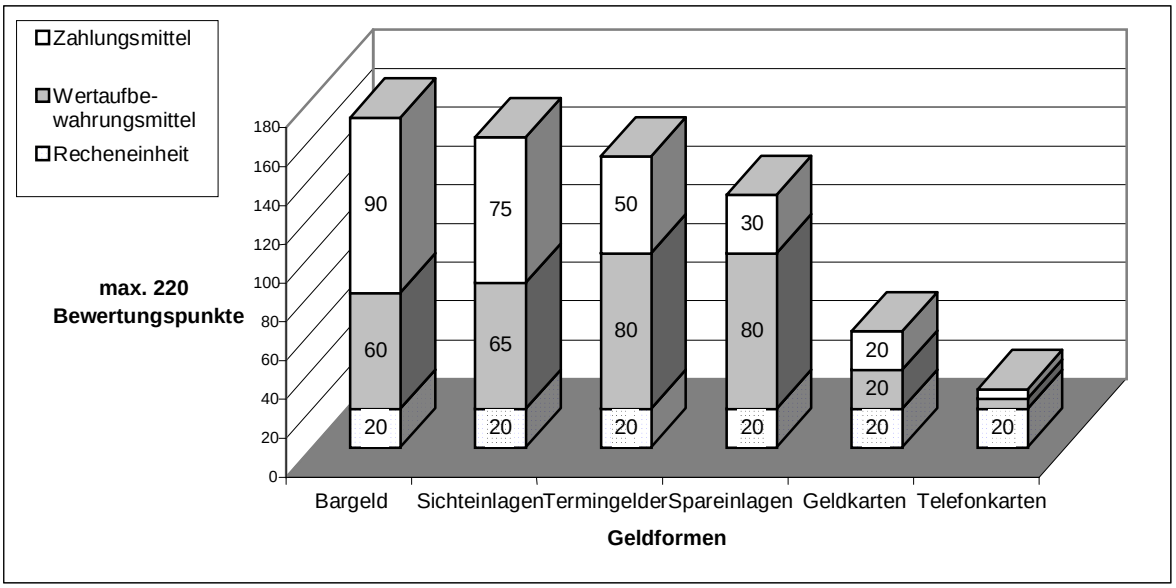

Abbildung 4: Geldnähe durch Erfüllung der Geldfunktion[40]

Die Erfüllung der wesentlichen Geldfunktionen ist zwingend, dabei lassen sich folgende Funktionen nennen[41]:

- *Funktion des Geldes als Wertmesser*: verantwortlich für Wertrelationen, Recheneinheit und das Preissystem.
- *Funktion des Geldes als Wertspeicher*: wichtig für die Bildung von Vermögen, für Investitionen und Konsum.

39 Vgl. GRAMLICH (Elektronisches Geld, 1997), S. 11.
40 Vgl. KLEIN (1997), S. 203.
41 Vgl. SCHAAL (Geldtheorie, 1998), S. 17-18; ISSING (Geldpolitische Bedeutung, 1997), S. 617; SCHIERENBECK/HÖLSCHER (BankAssurance, 1998), S. 3-6.

- *Funktion des Geldes als Wertüberträger*: als Garantie für die Fungibilität, der Tauschbarkeit, Teilbarkeit und gesetzliches Zahlungsmittel.

In gewisser Weise ähnelt die Entwicklung der verschiedenen Cyber Money Arten der Entwicklung des Bank- und Geldwesens im 17. Jahrhundert. Mehrere Anbieter von Cyber Money existieren nebeneinander im Internet. Der Verbraucher wird sich schließlich die Frage stellen, ob Cyber Money A auch beim Emittenten B akzeptiert wird und umgekehrt. Um dieses Problem zu vermeiden, wird in den heutigen Volkswirtschaften Geld stets von einem einzigen Emittenten, der Zentralbank, herausgegeben. Dieses Monopol gewährleistet eine Beschränkung der Geldmenge und sichert zumeist eine staatlich garantierte Annahmepflicht. Für Cyber Money lassen sich grundsätzlich drei wesentliche Gruppierungen als potentielle Anbieter nennen: Nichtbanken, Geschäftsbanken und Zentralbanken[42].

Von Nichtbanken werden in Deutschland bereits einige elektronische Werteinheiten wie Telefonkarten oder andere Wertkarten emittiert. Diese Arten werden als *„single-purpose“* bezeichnet, da Emittent und Akzeptant identisch sind. Volkswirtschaftliche Auswirkungen sind dabei zu vernachlässigen. Anders bei *„multi-purpose“* Geld. Da Emittent und Akzeptant hierbei nicht identisch sein müssen, erreichen diese Arten von Geld mehr „Geldnähe“. Problematisch wird dies unter dem Aspekt, daß Nichtbanken keinerlei Liquiditätskontrollen und Liquiditätssicherungen unterliegen. Durch das Konkursrisiko kann somit ein Umtausch in reale Geldeinheiten nicht jederzeit gewährleistet werden. Ein so entstehender Vertrauensverlust könnte einen Run auf die Emittenten auslösen und bei einer Kettenreaktion zu einer Krise des Geldwesens führen. Auch sind durch einen geringeren Einfluß der Zentralbank auf die Geldmenge inflationäre Tendenzen möglich. Die Geldschöpfung von Nichtbanken ist aus heutiger Sicht nicht mit der monetären Steuerung der Geldmenge vereinbar[43].

Die Emission von elektronischem Geld durch Geschäftsbanken entspricht in etwa einer Kreditvergabe (multiple Giralgeldschöpfung)[44] und hat somit direkten Einfluß auf die Geldmenge. Da jedoch Geschäftsbanken einer permanenten geldpolitischen Überwachung durch die Zentralbank unterliegen, bleibt die Geldmenge steuerbar. Die Mindestreserveverpflichtung garantiert eine ausreichende Liquidität und hohe Bonität. Jedoch nimmt mit zunehmender

[42] Vgl. JAHN (Geld, 1995), S. 24.
[43] Vgl. PADOVAN / BUSSIEK (Grenzenloses Wirtschaften, 1998), S. 248 und MÖKER (Elektronisches Geld, 1998), S. 190; siehe auch Kapitel II. 1. in Abschnitt C.
[44] Vgl. SCHAAL (Geldtheorie, 1998), S. 103.

Verbreitung von elektronischem Geld der Refinanzierungsbedarf der Banken bei der Zentralbank ab[45].

3. Deutsche Banken im Internet

Da Cyber Money nur durch Kreditinstitute herausgegeben wird, soll nun untersucht werden, inwieweit sich deutsche Banken mit dem Medium Internet befaßt haben.

In der Anfangszeit wurde das neue Medium Internet vorwiegend zum Aufbau von Know-how und als Marketingplattform verwendet. Auf der Suche nach neuen Tätigkeitsbereichen und Geschäftsmöglichkeiten wurde bald die Bedeutung eines geeigneten Internetbezahlsystems als entscheidender Faktor für die Entwicklung des Bankenbereichs im Electronic Commerce erkannt. Die verstärkte Nutzung des Internet sowohl durch Privatkunden als auch durch Unternehmen führt zu Strukturveränderungen, denen sich besonders die Banken stellen müssen[46]. Dadurch wird das Internet auch zu einem neuen Vertriebsweg für Finanzdienstleistungen[47]. Andersen Consulting sieht die Zukunft der Banken im Cyberspace in einer Virtualisierung der Produkte und Unternehmen unter Loslösung von der Materie. So wird aus anfaßbarem Geld Cyber Money in elektronischen Geldbörsen. Der Computer verwandelt sich zum Konto, Tresor, Kassiermaschine und Kontoführer in einem[48]. Die so entstehende virtuelle Bank zeichnet sich vor allem durch eine Präsenz im elektronischen Markt aus, die alle Eigenschaften einer echten Bank anbietet. Unterstützt durch klassische Finanzsoftware, elektronische Agentensysteme und mit persönlicher Beratung gekoppelt kann die virtuelle Bank sehr schnell zur Konkurrenz für konventionelle Banken werden[49].

Der Wandel von den ersten Web-Seiten bis zu den heutigen Angeboten von Banken im Internet ist gewaltig. Zu Beginn wurde einfach vorhandenes Prospektmaterial ins Netz gestellt, jedoch war mit solchen relativ langweiligen und technisch zurückhaltenden Seiten die Netzgemeinde nicht zu begeistern und der Erfolg blieb aus. Die anfängliche Euphorie der Banken schlug schnell in Ernüchterung um. Erst durch den Einsatz moderner Technologien, das Anbieten von weiteren Dienstleistungen und die Umstellung auf kurze, inhaltsstarke Texte, welche ständig aktualisiert werden müssen, begann sich ein Erfolg einzustellen. Diejenigen Institute, die bereits seit geraumer Zeit im Internet vertreten sind, wissen, wie aufwendig die inhaltliche, visuelle und technische Gestaltung guter Web-Seiten ist.

---

45 Vgl. HARTMANN (Die Europäische, 1997), S. 640.
46 Vgl. HAGEN / ZAGLER (Sicherer Zahlungsverkehr, 1998), S. 217.
47 Vgl. ERLINGHEUSER (Virtuelle Schalterhalle, 1998), S. 35-55; WANKE (Sachsen LB, 1998), S. 184.
48 Vgl. BRUER (Revolution, 1998), S. 59.
49 Vgl. STOCKMANN (Die virtuelle Bank, 1998), S. 273-279.

Vor diesem Hintergrund sind auch die gegründeten Joint Ventures mit diversen Anbietern von Cyber Money zu sehen. Dadurch wurde der Grundstein für eine Zusammenarbeit zwischen Sparkassen und Banken, Herstellern von Kreditkarten, Software-Herstellern und Händlern gelegt. Die Möglichkeit der sicheren Point-of-Sale-Zahlungen im Internet für deutsche Handelsunternehmen ist dabei eines der Hauptziele der Kooperation[50].

So bildet das Internet für Banken und Sparkassen nicht nur die Plattform für die Abwicklung von Electronic Commerce und Home-Banking, sondern muß auch als Grundlage für die Bereitstellung weiterer innovativer Dienste im Rahmen einer „virtuellen Bankfiliale" dienen. So werden neben Bankdienstleistungen eine Vielzahl von Non-Banking-Leistungen, sogenannte „added values", offeriert. Der Ausbau der virtuellen Schalterhalle zu einem multimedialen Ereignis, bei dem individuelle Beratung und Information um zusätzliche Angebote wie Audio- und Videokonferenzen sowie Cross-Selling-Angebote ergänzt werden, ist bei einigen Instituten schon zu beobachten[51].

III. Veränderungen der industriellen Risiken und daran angepaßte Versicherungsmodelle

1. Begriffsbestimmung und Abgrenzung

Ursprünglich definiert wurde der Begriff „Cyber Money" als Geldart, welche losgelöst von jedem Trägermedium in Computernetzen wie dem Internet als Zahlungsmittel verwendet werden kann. Dabei ist Cyber Money an keine reale Währung gebunden[52]. Auf diese Spezifikation hin wurde z.B. das eCash-System von DigiCash entwickelt, welches später noch genauer beschrieben wird. Dieser Ansatz ist allerdings aus heutiger Sicht nicht mehr sinnvoll, da nur Systeme auf Basis einer realen Währung praxistauglich sind. Vielmehr kann Cyber Money heute als Bezeichnung für *alle* Zahlungssysteme verstanden werden, über die im Internet bezahlt werden kann.

Um Sprachverwirrungen vorzubeugen, werden zu Beginn die verschiedenen Begriffe erläutert. Unter Cyber Money oder Digital Cash werden im Rahmen dieser Arbeit digitale Zahlungssysteme verstanden, mit denen per Karte oder als digitale Werteinheit auf einem PC im Internet bezahlt werden kann. Andere Formen des Zahlungsverkehrs wie das Internet-Banking über die Hausbank fallen nicht in diese Kategorie[53].

---

[50] Vgl. WEISS (Virtuelle Bank, 1998), S. 429 und VITT (Zukunftsvision, 1997), S. 237.
[51] Vgl. RAPP (Tendenzen, 1998), S. 14-15.
[52] Vgl. BORCHERT (Cyber Money, 1996), S. 41.
[53] Vgl. FRIEDRICH (Elektronisches, 1997), S. 2.

Unter elektronischem Geld oder E-Geld werden im allgemeinen von einem Kreditinstitut emittierte Werteinheiten verstanden, die wie Bargeld oder Buchgeld als Zahlungsmittel verwendet werden, ohne bei einer Transaktion eine Kontobewegung zu veranlassen. Die Werteinheiten sind daher wie Bargeld als vorausbezahlte Inhaberinstrumente zu sehen und verkörpern Kaufkraft in Form übertragbarer Forderungen gegen den Emittenten. Nur reine münzbasierte Systeme wie z.B. eCash können auch als Netzgeld bezeichnet werden[54]. Eine Übersicht über die verschiedenen Zahlungsmittel wird in Abbildung 5 dargestellt, wobei alle kursiv dargestellten Verfahren zu den Digital Cash-Systemen gezählt werden können.

Methode / Mittel	**Papier**	**Karte**	**Netz**
Übertrag	Überweisung	Kreditkarte	Homebanking
Belastung	Scheck	Debitkarte	Elektronische Lastschrift
Vorausbezahlt	Bargeld	Elektronische Geldkarte	Elektronisches Netzgeld

Abbildung 5: Anzahl der SmartCards in Deutschland

Eine allgemeingültige Abgrenzung der digitalen Zahlungsverfahren untereinander ist nicht vorhanden. Die später vorgestellten Cyber Money-Systeme lassen sich nach verschiedenen Kriterien abgrenzen.

Eine einfache Unterscheidung ist die in *kartenbasierte* und von körperlichen Trägermedien losgelöste *softwarebasierte* Systeme. Zu den Kartensystemen werden dann sowohl alle Verfahren mit Kreditkarte als auch mit SmartCards gezählt. Zu den softwarebasierten Verfahren zählen Zahlungsmittel, die in offenen Computernetzwerken durch Generieren von Münzen zum Einsatz kommen (Netzgeld). Ferner läßt sich eine Unterscheidung nach dem Zeitpunkt der tatsächlichen Zahlung vornehmen. So ist zwischen *pre-paid*, *pay-now* und *post-paid* zu unterscheiden. Unter pre-paid fallen die meisten SmartCard-Systeme wie z.B. die Geldkarte. Pay-now kommt z.B. bei Netzgeld vor, wenn die digitalen Münzen direkt von der Bank an den Händler weitergereicht werden. Kreditkartenbasierte Systeme schließlich sind als post-paid einzustufen, da die Abrechnung meist am Monatsende erfolgt. Insgesamt lassen sich über 20 verschiedene Digital Cash-Systeme nennen, die zum großen Teil jedoch nur als Varianten der Grundtypen anzusehen sind. Viele davon haben rein theoretischen Charakter und sind noch lange nicht marktreif[55].

[54] Vgl. MÖKER (Elektronisches Geld, 1998), S. 177.
[55] Vgl. GRAMLICH (Elektronisches Geld, 1997), S. 13.

Die Einteilung in dieser Arbeit wird nach verschiedenen Gesichtspunkten vorgenommen. Zum einen wird eine Differenzierung nach technischen Aspekten vorgenommen, d.h. Verfahren auf Basis von Kreditkarten, Schecks, Software und SmartCards werden getrennt, zum anderen wird eine besondere Betonung auf die für Europa und speziell Deutschland relevanten Verfahren wie eCash, SET und die Geldkarte gelegt.

2. Durch Cyber Money entstehende Problemfelder

Der Grund zur Entwicklung von Zahlungssystemen für das Internet ist eindeutig: mit den traditionellen Zahlungsmitteln läßt sich im Internet nicht bezahlen. Bargeld kann nicht über das Internet verschickt werden, Kreditkarten lassen sich nicht stofflich prüfen und Unterschriften nicht eigenhändig leisten. Für die Entwicklung von Cyber Money mußte das Rad jedoch nicht neu erfunden werden. Zumindest unbare Zahlungsmittel haben eine Gemeinsamkeit, die sich mit etwas Mühe auch in den virtuellen Raum übertragen läßt: sie weisen einen Dritten an, ein Konto zu belasten und den Gegenwert auf einem anderen Konto zu speichern. Da diese Methoden aber im Vergleich zu Bargeld Nachteile aufweisen, wurde auch versucht, digitale Münzen für das Internet zu entwickeln und zu emittieren. Die Emission von Cyber Money ohne staatliche Kontrollen kann jedoch zu unerwünschten Zuständen führen. Bei mehreren Cyber-Währungen ist es denkbar, daß einige eine gewisse Eigendynamik entwickeln, da sie nicht mehr eins zu eins an den Wert des realen Geldes gekoppelt sind. So könnten Währungen mit den unterschiedlichsten Bezeichnungen wie CyberGold, Diginotes oder Ähnliches zur offiziellen Währung in Konkurrenz treten[56].

Der durch mangelnde Regulierung entstehende Wettbewerb hätte für den Verbraucher einige ernste Probleme zur Folge. So ist es den meisten Bürgern weder möglich noch zumutbar, die Bonität aller emittierenden Institute zu beurteilen. Auch fehlen immer noch die rechtlichen Grundlagen für Geldgeschäfte im Internet. Da das Internet kein geographischer Rechtsraum ist, können Verstöße auch nicht geahndet werden. Im schlimmsten Fall kann eine unkontrollierte Entwicklung durch einen dominoartigen Zusammenbruch den ganzen Zahlungsverkehr erschüttern.

Ein weiterer Aspekt ist das hohe Risikopotential elektronischer Zahlungssysteme in Bezug auf die Geldwäsche. Das Erkennen von geldwäscherelevanten Transaktionen wird im Vergleich zu klassischen Schaltergeschäften für den Bankmitarbeiter aufgrund der hohen Automation immer schwieriger. Insbesondere wegen seiner teilweise uneingeschränkten Anonymi-

[56] Vgl. LÜTGE (Viele Bits, 1997), S. 22.

tät kann Digital Cash für Geldwäscher sehr attraktiv sein. Besonders SmartCards und Netzgeldsysteme erfüllen aufgrund ihrer hohen Anonymität die essentiellen Voraussetzungen nicht mehr, die im Geldwäschegesetz (GwG) gefordert werden und für eine effektive Bekämpfung der Geldwäsche zwingend sind. Geld kann bei diesen Systemen teilweise beliebig auf Dritte übertragen werden, ohne daß noch nachvollziehbar ist, wer wem wofür etwas überwiesen hat[57]. Zumindest für Deutschland ist durch die Änderung des KWG (Kreditwesengesetz) vom 1. Januar 1998 sichergestellt, daß das Herausgeben und Verwalten von elektronischen Zahlungseinheiten als Bankgeschäft definiert ist. Somit dürfen diese Geschäfte nur vom Bundesaufsichtsamt lizenzierte Banken betreiben[58].

[57] Vgl. FINDEISEN (Elektronisches Geld, 1998), S: 49.
[58] Vgl. §1 Abs. 1 Satz 2 Nr. KWG und §1 Abs. 1 Satz 2 Nr. 12 KWG.

B. Formen und Spezifikationen von Cyber Money-Systemen

Zur Bezahlung von Waren und Dienstleistungen im Internet lassen sich bislang folgende Zahlungssysteme differenzieren, die im Anschluß genauer beschrieben und untersucht werden:

- Elektronische Schecks,
- Zahlung mit Kreditkarte,
- Kontosysteme (hier nicht behandelt),
- Elektronisches Geld (Netzgeld) sowie
- SmartCards.

I. Internetbezahlsysteme auf der Basis von elektronischen Schecks und Kreditkarten

Elektronische Zahlungssysteme auf Basis von Schecks und Kreditkarten unterscheiden sich zwar deutlich in ihrem technologischen Aufbau, werden aber aufgrund ihrer Konzeption in einem Kapitel zusammengefaßt. Beide Verfahren wurden für den amerikanischen Markt und für amerikanische Zahlungsgewohnheiten entworfen[59]. Aufgrund dieser Tatsache eignen sie sich nur bedingt für den europäischen bzw. deutschen Markt. Zum einen besitzt die Kreditkarte in Amerika einen weit höheren Verbreitungsgrad als in Deutschland und zum anderen werden sehr viele Zahlungen in Amerika per Scheck anstelle der bei uns üblichen Überweisung oder Abbuchung beglichen[60]. Während die Bezahlung mit Schecks zu den accountbasierten Konzepten gehört, fällt die Kreditkarte unter die inhaberbasierten Verfahren mit Hardware. Beide Systeme sind nur im weitesten Sinne als Digital Cash-Systeme zu verstehen, da die eigentliche Abrechnung über die Kreditkartenemittenten bzw. Banken erfolgt. Aufgrund der hohen Transaktionskosten, die sich bei Zahlungssystemen auf Basis von Kreditkarten ergeben, sind hohe Sicherheitsstandards zwingend, da nur größere Beträge ökonomisch sinnvoll sind.

1. Aufbau und Funktionsweise von elektronischen Schecks

Das Konzept der elektronischen Schecks basiert auf der Idee, ein digitales Formular anstelle des herkömmlichen Formulars aus Papier zu verwenden. Zur Sicherheit wird eine digitale Unterschrift angehängt und mit Verschlüsselungsverfahren geschützt. Dadurch bleibt die

[59] In den USA wurden 1988 ca. 50 Milliarden Schecks ausgestellt, 1996 entfielen 77,5% aller unbaren Zahlungen auf Schecks, 19% auf Kreditkarten. Fast 50% des unbaren Zahlungsverkehrs in Deutschland entfällt auf Überweisungen, Lastschriften belegen noch weitere 40%. Der Rest verteilt sich auf Karten und Schecks.

[60] Vgl. BERNDT (Elektronisches Geld, 1995), S. 369.

Handhabung der elektronischen Schecks gegenüber konventionellen Schecks sehr ähnlich. Als Beispiele für Zahlungsverfahren mit Schecks lassen sich folgende Varianten nennen:

Das *NetCheque-Verfahren* wurde an der University of Southern California vom Institute for Information Science unter der Leitung von Clifford Neuman entwickelt. Ausgangspunkt ist das Prinzip des Verrechnungsschecks, welches auf ein elektronisches System übertragen wird. Der elektronische Scheck beinhaltet dabei alle Angaben, die ein Scheck aus Papier auch enthält: Kontonummer, Empfänger, Zahlungsbetrag, Währung, Verfallsdatum und zusätzlich die digitale Unterschrift zur Sicherstellung der Authentizität. Dadurch kann zwar keine Anonymität gewährleistet werden, jedoch ist das Verfahren mit ausreichender Sicherheit theoretisch auch für größere Beträge geeignet. Unterschiede zu normalen Schecks sind die digitale Signatur anstelle der Unterschrift sowie die Registrierung aller beteiligten Parteien bei einer zentralen Stelle. Diese neutrale Institution soll die Identität der Transaktionspartner bestätigen. Hierbei kann ein Kerberos-System[61] verwendet werden, welches per Algorithmus die Zugriffsautorisierung bestätigt.

Die Einreichung des Schecks bei der Bank kann wie in der Realität auch später erfolgen, sie ist also nicht Bestandteil des Bezahlungsvorgangs an sich. Das Risiko, einen ungedeckten Scheck zu erhalten, ist demnach ebenso gegeben. Einzig die Autorisierungsstelle garantiert die Identität des Geschäftspartners. Praktische Anwendung findet das System bislang nicht und hat lediglich Studien- bzw. Testcharakter. Der Zahlungsablauf ist in Abbildung 6 dargestellt[62].

[61] Autorisierungssoftware vom MIT.

[62] Vgl. KRAUSE (Electronic Commerce, 1998), S. 94 und KRISTOFERITSCH (Digital Money, 1998), S. 138.

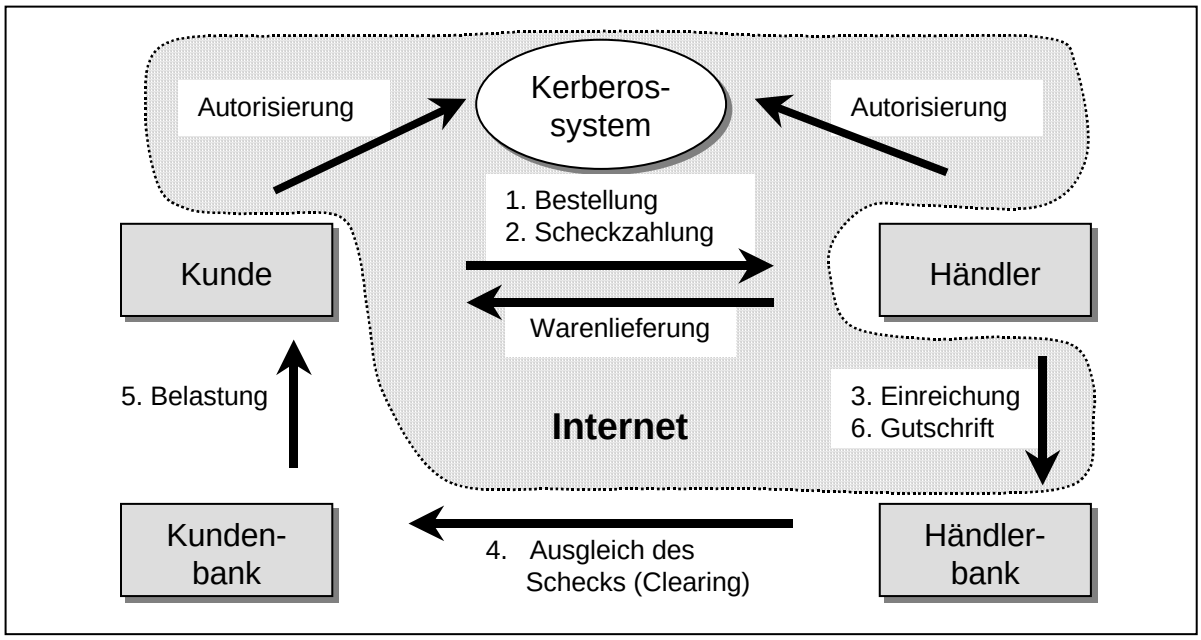

Abbildung 6: Der Zahlungsvorgang bei NetCheque

Als Vorteile des Verfahrens sind die einfache Bedienbarkeit, die gute Skalierbarkeit der Beträge (Micro- bis Macropayments) und der flexible Einsatz zu nennen. So können Privatpersonen sowohl Sender als auch Empfänger von elektronischen Schecks sein (Peer-to-Peer-Transaktionen). Die Transaktionsgeschwindigkeit ist kurz, da keine Online-Bestätigung erfolgt[63]. Nachteile des Systems sind in der unverschlüsselten Übertragung des Schecks zu sehen, da dadurch leicht die Bankverbindungen der beteiligten Personen „ausspioniert" werden können. Lediglich die digitalen Unterschriften werden mit symmetrischen Verfahren verschlüsselt. Die Autorisierung über Kerberos gilt als weitgehend sicher. Alle beteiligten Parteien benötigen jedoch ein Konto bei einer Bank, welche die NetCheque Technologie unterstützt und über die alle anfallenden Gebühren abgerechnet werden[64].

NetBill ist durch Zusammenarbeit der Carnegie Mellon University mit Visa International und Microsoft entstanden. Ziel war, ein internettaugliches Zahlungsverfahren für Microbeträge ab 1 Pf. (bzw. Cent) zu entwickeln. Aufgrund der Systemkonzeption ist das Verfahren nur für immaterielle Güter geeignet, die sich per Internet übermitteln lassen. Der Ablauf einer Transaktion bei NetBill ist in Abbildung 7 dargestellt.

63 Vgl. SCHUSTER u. A. (Digital Cash, 1997), S. 55-57 und STOLPMANN (Elektronisches Geld, 1997), S. 60-63.
64 Vgl. HIMMELSPACH u. A. (Analyse, 1996), S.24-26 und HIRT (Electronic, 1997), S. 21-22.

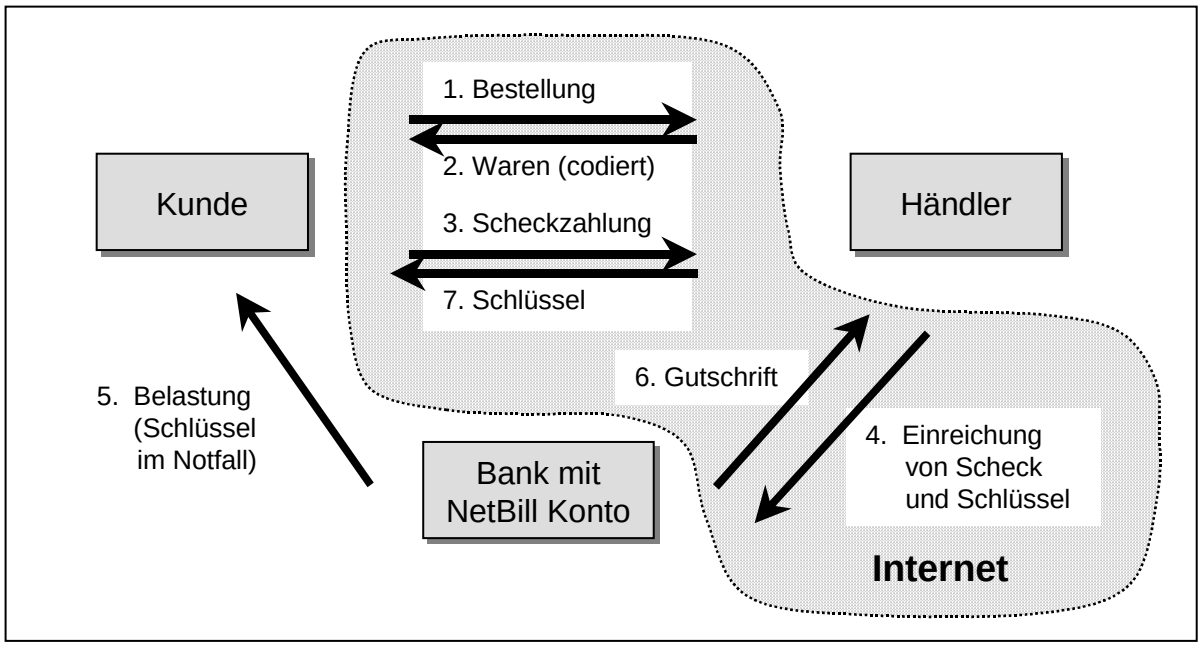

Abbildung 7: Die Durchführung einer Transaktion über NetBill

Eine wesentliche Eigenschaft von NetBill ist, daß die Lieferung bei Bezahlung garantiert werden kann. Der Kunde erhält seine digitale Ware bereits vor Bezahlung, jedoch in verschlüsselter Form. Stimmt die Prüfsumme des Produkts mit der des Händlers überein, kann der Kunde seinen digitalen Scheck übermitteln. Im Gegenzug erhält er vom Händler den Schlüssel zur Decodierung seiner Ware. Aus Sicherheitsgründen wird der Schlüssel auch bei der Bank hinterlegt, so daß das Risiko der Geschäftstransaktion gleichmäßig zwischen Kunde und Händler aufgeteilt ist[65].

Somit ist NetBill hervorragend geeignet, um beispielsweise Gebühren für Shareware-Produkte einzuziehen. Die gegenseitige Authentisierung von Kunde und Händler sowie die asymmetrische Verschlüsselung der Ware schränkt dabei zusätzlich die Möglichkeiten des Mißbrauchs ein. Problematisch sind allerdings die durch den hohen Kommunikationsaufwand entstehenden Transaktionskosten. Zwar ist vorgesehen, daß mehrere Transaktionen gebündelt werden, ob die Kosten auch für Micropayments niedrig genug bleiben, ist fraglich. Zudem müssen beide Geschäftspartner ein spezielles Kundenkonto (NetBill-Account) bei der selben Bank führen, welches vorausbezahlt bzw. gedeckt sein muß. Diese Bank ist auch für die Berechnung von Gebühren verantwortlich. Weiterhin ist die Beschränkung auf Produkte wie Software, Rechenleistung oder Information hinderlich für einen breiten Einsatz mit hoher Akzeptanz[66].

[65] Vgl. WEISSHUHN (Digitale Zahlungsverfahren, 1998), S. 150 und KRAUSE (Electronic Commerce, 1998), S. 92.
[66] Vgl. STOLPMANN (Elektronisches Geld, 1997), S. 75-78 und KRISTOFERITSCH (Digital Money, 1998), S. 136-137.

2. Kreditkarten in Digital-Cash-Systemen

Ein großer Teil aller Zahlungen für Waren, Dienstleistungen und Informationen im Internet werden heute über die gängigen Kreditkarten abgewickelt. Wie bereits erwähnt, sind diese Verfahren keine Digital Cash-Systeme im engeren Sinne, da sie lediglich versuchen, bewährte Technologien sicher in den virtuellen Raum zu übertragen. Voraussetzung ist also ein Kreditkartenvertrag mit einem der unten aufgeführten Anbieter bzw. deren Vertragspartner. Generell eignen sich kreditkartenbasierte Zahlungssysteme vor allem für Zahlungen im Macropayment-Bereich. Hierzu sind eine Reihe von Systemen entwickelt worden, die im folgenden beschrieben werden.

First Virtual (FV) spielt unter den Unternehmen, die sich mit Online-Zahlungsmitteln befassen, eine herausragende Rolle. Zum einen hat es als erstes Unternehmen ein auf Kreditkarten basierendes Zahlungssystem mit hohem Sicherheitsstandard für das Internet entwickelt, zum anderen ist es das erste Finanzinstitut weltweit, welches sich ausschließlich auf die Abwicklung von Online-Finanztransaktionen spezialisiert hat.

Am Anfang steht zunächst eine recht aufwendige Registrierung von Händlern und Kunden bei First Virtual. Dabei werden über einen sicheren Übertragungskanal (nicht das Internet) alle zahlungsrelevanten Kreditkarteninformationen[67] übertragen. Im Gegenzug erhält der Kunde eine persönliche Identifikationsnummer (PIN), die ihn eindeutig identifizierbar macht und regelmäßig erneuert wird. Für spätere Zahlungsabläufe wird nur diese FV-PIN übertragen, nicht jedoch die Kreditkartendaten des Kunden. Der Zahlungsvorgang bei First Virtual stellt sich wie in Abbildung 8 gezeigt dar[68].

Vorteilhaft bei der Bezahlung über First Virtual ist, daß keine zusätzliche Software bei den Kunden und Händlern installiert werden muß, da nur über Email kommuniziert wird. Auch bleibt auf Wunsch die Anonymität des Kunden gewahrt, da der Händler die FV-PIN keiner Person zuordnen kann. Der Diebstahl der FV-PIN bietet auch für potentielle Betrüger keinen Angriffspunkt, da jede Transaktion vom Kunden per Email bestätigt werden muß. Tritt der Verdacht eines versuchten Mißbrauchs auf, kann die FV-PIN auf Wunsch des Kunden jederzeit ausgetauscht werden. Die sensitiven Kreditkartendaten werden auf einem nicht über das Internet zugänglichen Rechner gespeichert[69].

---

67 Nur Kreditkarten von Visa und Mastercard werden akzeptiert.

68 Vgl. LUKAS (Cyber Money, 1997), S. 137-139 und KRAUSE (Electronic Commerce, 1998), S. 92.

69 Vgl. WEISSHUHN (Digitale Zahlungsverfahren, 1998), S. 151-152 und KRISTOFERITSCH (1998), S. 141-142.

Das Fehlen von Verschlüsselungsmechanismen hat jedoch auch seine Schwächen. Da Emails keine sichere Übertragung gewährleisten, kann zumindest die Bestätigung der Transaktion mit den Daten über den Kaufvorgang abgefangen werden. Zudem kommt es zu einer doppelten finanziellen Belastung des Kunden. Zum einen bezahlt er Gebühren an seinen Kreditkartenanbieter, zum anderen werden bei First Virtual Jahresbeiträge sowie Gebühren pro Transaktion fällig. Die Händler sparen zwar die Provision an die Kreditkartengesellschaften, werden dafür aber ebenfalls von First Virtual zur Kasse gebeten. Durch dieses Abrechnungsverfahren ist die Bezahlung von Micropayments über First Virtual nicht sinnvoll.

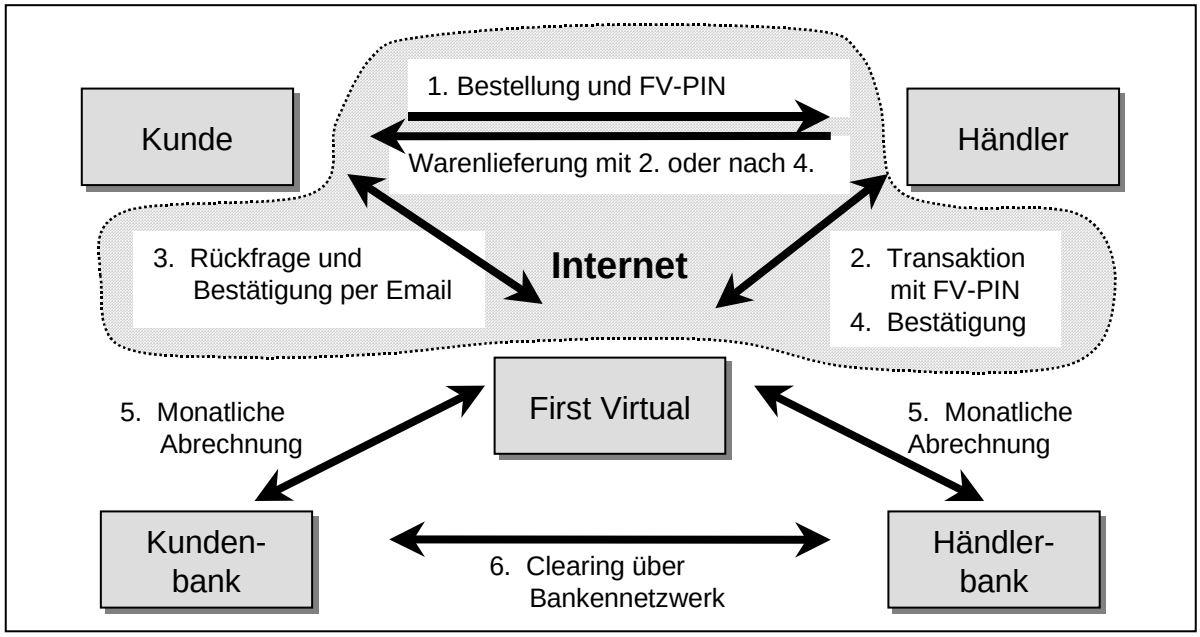

Abbildung 8: Der Zahlungsvorgang bei First Virtual

Trotz der hohen Kosten erfreut sich das Verfahren in den USA relativ großer Beliebtheit. Im Vergleich zu anderen Verfahren ist die Praxistauglichkeit und Akzeptanz von First Virtual recht hoch[70].

Das dem Verfahren von First Virtual ähnliche *CyberCash* wird von der gleichnamigen Firma CyberCash angeboten. Dieses Verfahren ist bereits seit 1995 für Internetzahlungen verfügbar. Voraussetzung ist eine kostenlose Software namens „Wallet“ sowie wiederum eine Kreditkarte, wobei bei CyberCash jedoch mehrere Anbieter akzeptiert werden[71]. Ein Screenshot der Wallet ist in Abbildung 9 zu sehen. Nach einmaliger Konfiguration kann das System umgehend eingesetzt werden. Händler, welche die CyberCash-Lösung als Zahlungsmittel akzeptieren wollen, müssen sich entweder direkt bei CyberCash oder bei einem Lizenznehmer regist-

[70] Vgl. STOLPMANN (Elektronisches Geld, 1997), S. 63-66 und SCHUSTER u. A. (Digital Cash, 1997), S. 53-55.

[71] Diese enthält auch Funktionen zur Auswahl anderer Zahlungsverfahren von CyberCash wie CyberCheque, CyberCoin und electronic direct debit (edd).

rieren lassen und erhalten eine spezielle Händler-Software (CashRegister). Diese ist sowohl für die Kommunikation zwischen Kunde und Händler als auch zwischen Händler und CyberCash zuständig[72].

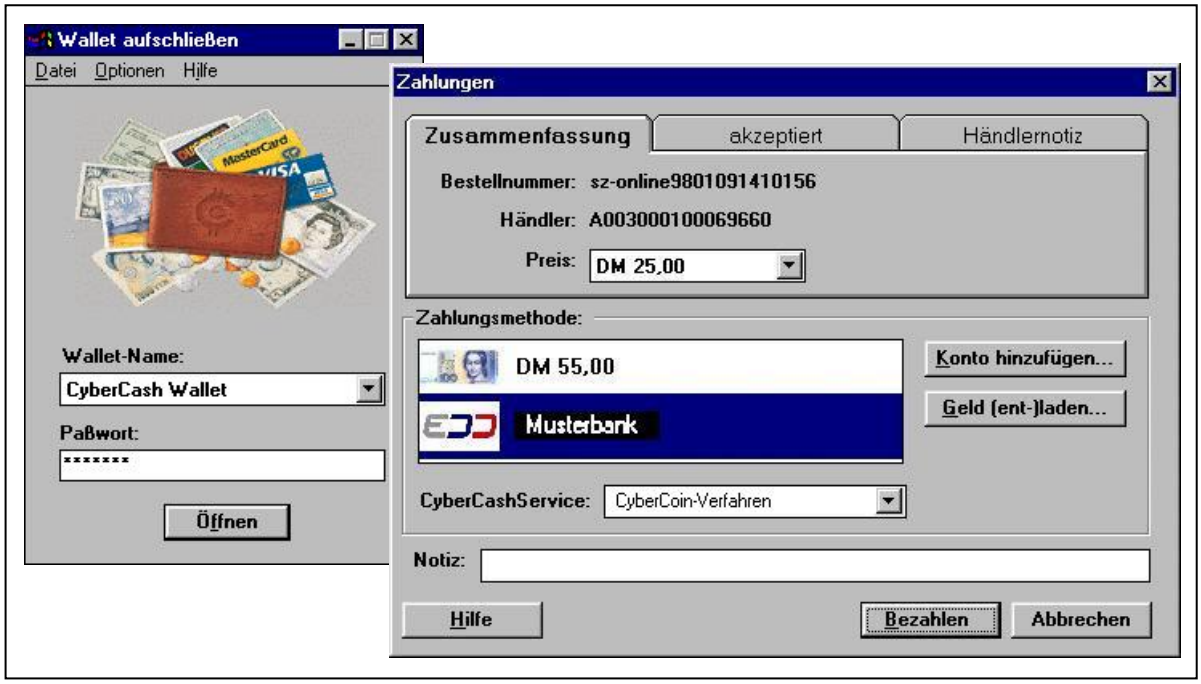

Abbildung 9: Anmeldefenster und Wallet-Oberfläche bei CyberCash

Verschlüsselt wird über eine sehr sichere RSA Codierung mit einem 1024 Bit Schlüssel. Dank einer Ausnahmegenehmigung darf dieser Sicherheitsstandard auch außerhalb der USA auf diesem hohen Niveau gehalten werden. Somit beruht das System von CyberCash weniger auf einem neuen Zahlungsverfahren als vielmehr auf einem sicheren Übertragungsprotokoll. Das Zahlungsprotokoll nach dem klassischen CyberCash-Verfahren wird in Abbildung 10 dargestellt. Sämtliche Schritte werden dabei automatisch durchgeführt. Der gesamte Vorgang dauert zwischen 15 und 90 Sekunden[73].

Insgesamt ist die Bezahlung über CyberCash sehr anwenderfreundlich, da eine aufwendige Registrierung entfällt. Die Online-Verifikation erweist sich ebenfalls als wichtiger Vorteil des CyberCash Verfahrens. Wie die anderen kreditkartenbasierten Zahlungssysteme ist CyberCash vor allem für den Macropayment-Bereich geeignet, da die Transaktionskosten auch aufgrund der Online-Verarbeitung vergleichsweise hoch sind. Anonymität wird gewährleistet, weil der Händler die Zahlungsdaten nicht entschlüsseln kann. Er benötigt jedoch aufgrund des Warentransfers eine Anschrift. Im Unterschied zu First Virtual und Open Market sind mit

[72] Vgl. POLYSIUS (Der Point of Sale, 1998), S. 31-34 und KRISTOFERITSCH (Digital Money, 1998), S. 140-141.
[73] Vgl. STOLPMANN (Elektronisches Geld, 1998), S. 66-70.

CyberCash auch materielle Güter erwerbbar. Kritiker argumentieren, daß im Vergleich zu First Virtual sensitive Zahlungsdaten über das Internet übertragen werden. Trotz der Verschlüsselung durch die CyberCash-Wallet gibt es theoretisch Mittel und Wege, an diese Daten auf unbefugte Weise zu gelangen[74].

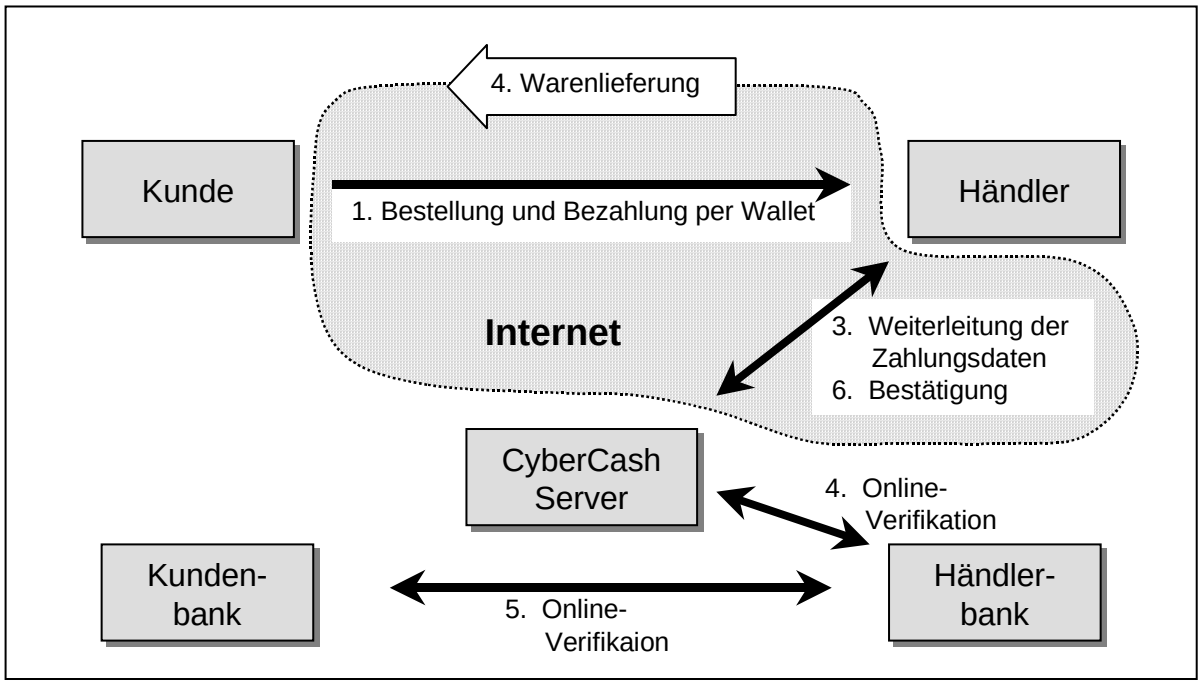

Abbildung 10: Transaktionsschritte beim CyberCash Verfahren

Die Akzeptanz und Praxistauglichkeit von CyberCash ist in den USA vergleichsweise hoch. So konnte CyberCash auch einige deutsche Lizenznehmer finden, unter anderem die Sachsen-LB und die Dresdner Bank, bei denen auch weitere Spezifikationen über das System zu finden sind[75]. Mittlerweile wurde jedoch das CyberCash-Verfahren dem SET Standard angepaßt, so daß die Kreditkartenbezahlung über CyberCash nicht mehr exakt wie oben erwähnt durchgeführt wird. Das SET (secure electronic transaction) Zahlungsprotokoll ist ein offener Standard und für verschiedene Systeme konzipiert[76]. Da durch SET der aktuellste Standard verkörpert wird und das Verfahren umfangreicher als die anderen ist, wird es in einem eigenen Kapitel behandelt.

Die Stuttgarter Firma *TeleCash*, eine gemeinsame Tochter von IBM und der Deutschen Telekom gehört hierzulande zu den Pionieren bei Online-Zahlungsverfahren. Lange bevor die sicheren 128-Bit-Verschlüsselungen aus den USA für den Export freigegeben wurden, hat TeleCash zusammen mit der Brokat Informationssysteme GmbH eine eigene Lösung entwi-

[74] Vgl. SCHUSTER u. A. (Digital Cash, 1997), S. 44-47 und WANKE (Sachsen LB, 1998), S. 184-185.
[75] Unter www.cybercash.de/ccsystem/features.htm ist der Ablauf einer CyberCash-Transaktion im Detail dargestellt.
[76] Vgl. WASMEIER (Cash auf Draht, 1998), S. 98.

ckelt. Die Kreditkartendaten werden verschlüsselt und dem Händler vorenthalten. Dieser ergänzt lediglich seine Angaben und reicht den Zahlungsauftrag weiter. Nach erfolgreicher Autorisierung durch TeleCash wird die Bezahlung über die Netzwerke der Kartengesellschaften veranlaßt. Eine sichere Verschlüsselung wird durch ein Java-Applet gewährleistet. Dieses muß zwar bei jeder Sitzung neu geladen werden, ist aber auch nur 100 KByte groß[77].

3. Einheitlicher Standard durch SET

Mit SET (Secure Electronic Transaction) steht ein von Visa, Mastercard und anderen Organisationen gemeinsam entwickeltes Zahlungsprotokoll zur Verfügung. Version 1.0 wurde im Mai 1997 offiziell verabschiedet. SET ist als Anwendungsprotokoll zu verstehen und baut auf den bewährten Protokollen SSL (secure sockets layer) und S-HTTP (secure hypertext transfer protocol) auf. Insbesondere wurden auch die Erfahrungen verschiedener anderer Zahlungssysteme und –protokolle einbezogen. So wurde das von Visa und Microsoft entworfene STT (secure transaction technology) sowie der von Mastercard, IBM und Netscape entwickelte SEPP (secure electronic payment protocol) Ansatz berücksichtigt[78].

Nur dadurch konnte ein offenes System zur sicheren Übertragung von Kreditkartendaten über das Internet geschaffen werden. So ist auch mit einer breiten Unterstützung der Systemanbieter, Händler, Kunden und Banken zu rechnen. Vor allem Detailverbesserungen und die Bemühungen um einen weit verbreiteten Industriestandard sind die Eigenschaften, die SET auszeichnen. Drei zentrale Funktionen lassen sich dabei gesondert nennen:

- die verschlüsselte Übertragung der Daten zwischen Kunde und Händler,
- die Authentifizierung aller Vertragspartner bei der Transaktion sowie
- Sicherheitsmechanismen zur Gewährleistung der Integrität der Daten.

Im folgenden soll auf die genannten Punkte näher eingegangen werden.

SET verwendet eine Kombination von RSA- und DES-Verschlüsselung sowie digitale Unterschriften für eine sichere und authentische Übertragung. Nachrichten (z.B. Bestellformulare) werden mit einem zufällig erzeugten 56-Bit DES-Schlüssel symmetrisch verschlüsselt. Der DES-Schlüssel wird mit dem öffentlichen RSA-Schlüssel[79] des Empfängers kodiert und der DES-Nachricht beigelegt (vergleichbar mit einem Umschlag). Die Kreditkartendaten werden mit dem öffentlichen RSA-Schlüssel der Bank kodiert. Somit kann der Empfänger nur die

[77] Vgl. KÖHLER (Electronic Commerce, 1998), S. 58-60 und WASMEIER(Cash auf Draht, 1998), S. 97.
[78] Vgl. KRITOFERITSCH (Digital Money, 1998), S. 114.
[79] Da nur Kreditkarten- und Schlüsselinformationen mit RSA kodiert werden, liegt eine Exportgenehmigung für den recht wirkungsvollen RSA Schlüssel vor.

eigentliche Nachricht berechnen, nicht jedoch die Kreditkartendaten. Vor dem Versenden wird jede SET-Nachricht mit einer digitalen Signatur versehen, die mit dem RSA-Schlüssel des Absenders verschlüsselt wird.

Beim RSA-Verfahren wird der öffentliche Schlüssel des Kommunikationspartners vorausgesetzt. Dieser wird bei SET in Form von Zertifikaten an jede unterschriebene Nachricht angehängt, so daß sie nach jedem Empfang geprüft werden können. Diese Zertifikate enthalten die Daten und die Signatur der ausstellenden Zertifizierungsstelle. Das Zertifikat des Kunden dient somit als Nachweis der Authentizität. Das Zertifikat des Händlers weist ihn als legitimen Vertragspartner aus.

Mit der dualen Signatur werden zwei Nachrichten einander eindeutig zugeordnet. Dadurch wird erreicht, daß Bestellung und Zahlungsanweisung fest miteinander verknüpft sind, ohne daß der Händler Einsicht in die Kreditkartendaten und die Bank Einsicht in die Bestelldaten erhält[80]. Der eigentliche Ablauf einer SET-Transaktion stellt sich wie folgt dar:

1. Auswahl der zu bestellenden Produkte über das WWW.
2. Ausfüllen des Bestellformulars und Versand über das WWW an den Händler. Die Bestell- und Zahlungsdaten werden dabei automatisch getrennt verschlüsselt und signiert.
3. Der Händler entschlüsselt die Bestelldaten, fügt den verschlüsselten Zahlungsinformationen seine eigene digitale Signatur hinzu und leitet sie an den SET-Server weiter.
4. Der SET-Server der Händlerbank dekodiert die Zahlungsinformationen, vergleicht die Signaturen und veranlaßt eine Online-Verifikation.
5. Bei positiver Verifikation wird das Konto des Kunden automatisch belastet.
6. Der Händler erhält eine Bestätigung über die erfolgte Zahlung (oder Ablehnung).
7. Der Händler veranlaßt den Warentransfer.

Jeder dieser Schritte wird dabei durch die oben erwähnten Verschlüsselungsverfahren kodiert, so daß nur verschlüsselte Informationen über das Internet geleitet werden. Grafisch läßt sich der Ablauf einer SET-Transaktion wie in Abbildung 11 darstellen[81].

[80] Vgl. SCHUSTER u. A. (Digital Cash, 1997), S. 39-41.
[81] Vgl. STOLPMANN (Elektronisches Geld, 1998), S: 72-75.

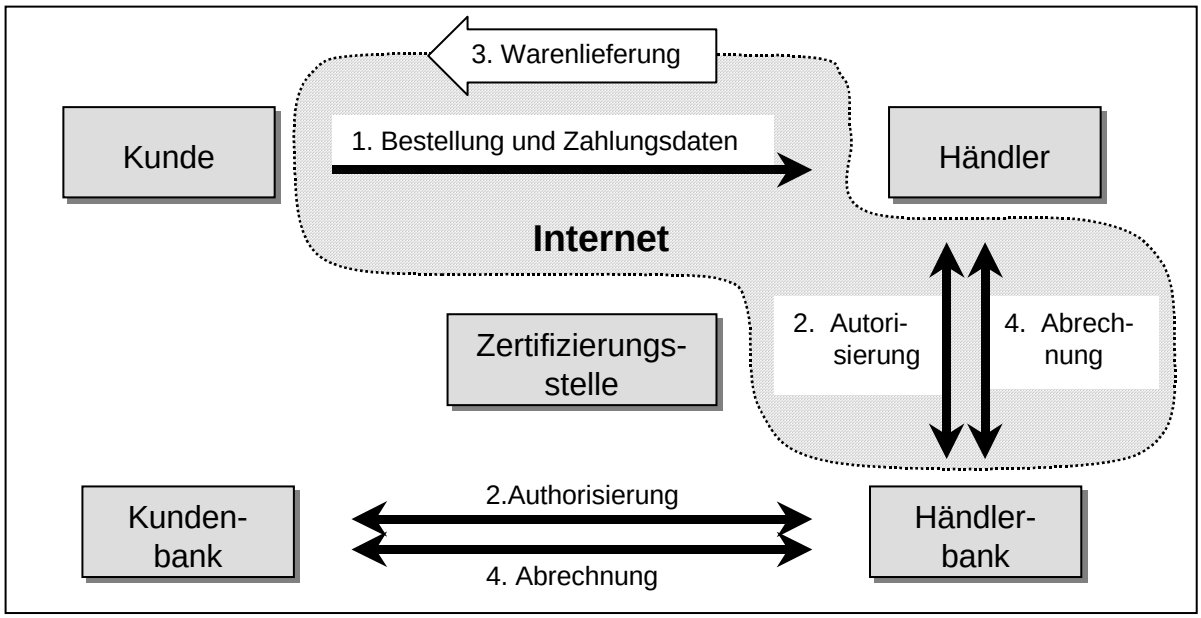

Abbildung 11: Vereinfachte Darstellung einer SET-Transaktion

Prinzipiell eignet sich das SET-Protokoll auch zur Übertragung von anderen Zahlungsdaten, z.B. einer Bankverbindung. Aufgrund der breiten Unterstützung durch alle namhaften Organisationen ist SET geeignet, der zukünftige Standard für elektronische Zahlungssysteme auf Debit- und Kreditbasis im Internet zu werden. Die Konzeption als offene, plattformunabhängige Architektur und eine kostenlose Lizenzvergabe werden dies noch zusätzlich begünstigen[82].

Trotz allem wird an SET kritisiert, daß zu Beginn die Kreditkartendaten in den Computer eingegeben werden müssen und dort auch zwischengespeichert werden. Hierbei besteht prinzipiell eine Angriffsmöglichkeit für Hacker, Viren oder andere Manipulationen. Dieses Problem ist jedoch nur mit zusätzlicher Hardware zu beheben[83].

Wie bei anderen Zahlungssystemen mit Kreditkarte sind auch mit SET aus wirtschaftlichen Gesichtspunkten nur Macropayments sinnvoll. Zudem wird über das Kreditkartensystem nur monatlich abgerechnet, was in einigen Fällen nachteilig sein kann. Positiv anzumerken ist, daß sich SET als ein zunächst ausschließlich an Kreditkarten orientierter Standard nun auch für andere Zahlungsvarianten öffnet. Einige Anbieter von elektronischen Lastschriftverfahren wollen ihr System auf den SET-Standard umstellen[84].

---

82 Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 113-118 und KÖHLER (Electronic Commerce, 1998), S. 53-56.

83 C-SET (chip-secured electronic transactions) ist ein europäisches Projekt, bei dem die sensiblen Daten auf einer Smart Card gespeichert werden sollen.

84 Vgl. SCHUSTER u. A. (Digital Cash, 1997), S. 35-43 und WEISSHUHN (Digitale Zahlungsverfahren, 1998), S. 145-147.

II. Digitales Geld auf der Basis von Software und elektronischen Münzen

Digitales Bargeld ist als Zahlungsmittel im Internet von großer Bedeutung für die Entwicklung des Electronic Commerce. Dabei sollen die Eigenschaften und Funktionalität realen Bargeldes möglichst naturgetreu digital abgebildet werden. Genau wie „echtes" Geld haben auch digitale Münzen einen inhärenten Wert. Sie sind keine Schuld- oder Gutscheine, deren Wert von einer dritten Partei gedeckt wird. Da aber digitales Geld durch Bits dargestellt wird, kann es beliebig oft kopiert werden. Elektronisches Bargeld muß deshalb Mechanismen besitzen, welche unerlaubte Vervielfältigungen verhindern und Fälschungen erkennen. Die im folgenden vorgestellten Digital Cash-Systeme auf reiner Softwarebasis kommen ohne die Verwendung von zusätzlichen Hardwareelementen aus. Die Konzeption ist somit bei allen Modellen gleich: die Möglichkeit zur Bezahlung von Kleinstbeträgen muß ökonomisch möglich sein. Da bei einigen Systemen die Beträge nicht limitiert sein müssen, treten DC-Systeme auf Softwarebasis in direkte Konkurrenz zu allen anderen Systemen[85].

1. Münzbasierte Zahlungssysteme

Zahlungssysteme mit digital erzeugten Münzen wollen Bargeld so gut wie möglich im virtuellen Raum abbilden, um die bereits erwähnten Funktionen von echtem Geld auch im Internet zu bieten. Dies hat teilweise zur Folge, daß zur Bezahlung von Waren genau die richtige Stückelung an digitalen Münzen in der Wallet sein müssen, wie dies zum Beispiel bei richtigem Bargeld nötig ist. Der Unterschied bei der digitalen Lösung ist zudem, daß man kein Wechselgeld erhält, d.h. der Betrag muß genau übertragen werden. Wichtigster Aspekt bei den vorgestellten Lösungen ist jedoch immer die dem Bargeld ähnliche hohe Anonymität[86].

Bereits 1989 gründete David Chaum das Unternehmen *DigiCash*, welches Hard- und Softwarelösungen für elektronische Zahlungssysteme anbietet. Alle Lösungen garantieren Sicherheit und Anonymität mit Hilfe von moderner Kryptologie. *eCash* wird dabei als Lösung für offene Netze wie das Internet propagiert.

Das in eCash verwendete kryptologische Verfahren ist für Online-Zahlungen ausgelegt, d.h. die digitalen Münzen werden nach Erhalt sofort bei der Bank auf Gültigkeit überprüft. Die digitalen Münzen werden nach dem sogenannten „Blinding-Verfahren" erstellt. Auf dem eigenen PC werden Münzen mit einer zufälligen Seriennummer generiert und mit einem bestimmten Faktor (blinding factor) verrechnet (bildlich: in einen Umschlag gesteckt). Diese

[85] Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 128.
[86] Vgl. STOLPMANN (Elektronisches Geld, 1998), S: 53-60 und KRISTOFERITSCH (Digital Money, 1998), S. 125-133.

werden anschließend bei der Bank eingereicht, wo die Münzen mit einer digitalen Unterschrift versehen werden, ohne daß jedoch die Bank die Seriennummer der Münze einsehen kann. Die Bank gleicht den Kontostand des Kunden an und sendet die Münzen zurück. Der „Umschlag“ wird entfernt und die anonyme digitale Münze kann für einen Einkauf verwendet werden[87]. Eine Zahlung mit eCash läuft folgendermaßen ab (vgl. Abbildung 12):

1. Der Benutzer hebt mit seiner kostenlosen Kundensoftware von seinem eCash Bankkonto online digitales Geld auf die Festplatte seines Rechners. Dabei kommt das Blinding-Verfahren zum Einsatz.
2. Beim Einkauf im Internet sendet seine Kundensoftware die digitalen Münzen an den Händler, der diese online an seine Bank weiterleitet.
3. Die Bank prüft die Unterschrift der Münzen und registriert die Seriennummer. Der Betrag wird auf dem Konto des Händlers gutgeschrieben.

Der Händler wird über die Gültigkeit der Aktion informiert und kann die Ware ausliefern.

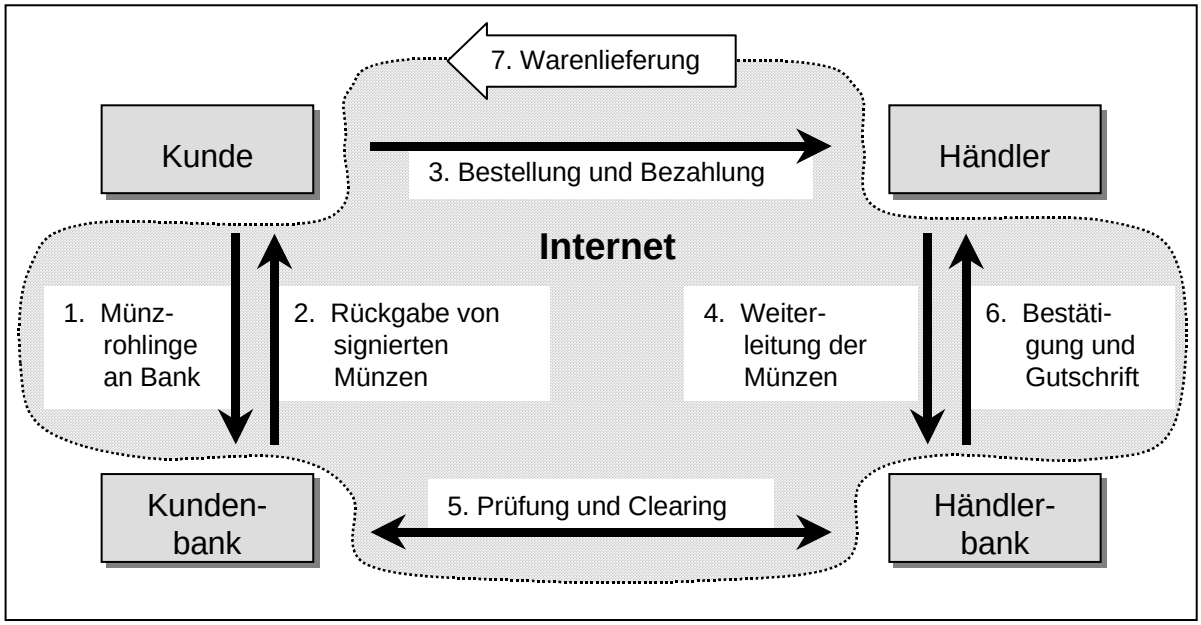

Abbildung 12: Der Zahlungsvorgang mit eCash

Durch die oben beschriebene Blinding-Funktion bleibt der Käufer gegenüber der Händlerbank anonym. Es kann kein Käuferprofil erstellt werden, indem die ausgegebenen Münzen der gekauften Ware gegenüber gestellt werden. Im Zweifelsfalle kann der Kunde seinen Blinding-Faktor bekannt geben und damit seine Transaktionen nachweisen. eCash ist somit das einzige Verfahren, das vollständige Anonymität bieten kann. Mit Hilfe eines Recovery-Mechanismus

[87] Vgl. DRESEN (Abgewogen, 1998), S. 96-98 und THIESSEN (Elektronische Zahlungsmittel, 1998), S. 218.

ist auch eine nachträgliche Erstattung durch einen Festplattencrash verlorener Münzen möglich. Die Sicherheit der Münzen ist dadurch gewährleistet, daß jede Münze nur für einen Zahlungsvorgang benutzt werden kann und dann bei der Bank eingereicht wird. Hier würde sich auch ein Ansatz zur Besteuerung von Umsätzen über das Internet ergeben. Da die digitalen Einnahmen nicht vor der Bank verheimlicht werden können, ist auch bereits ein Ansatz zur Verhinderung der Geldwäsche in das System implementiert. Es ist auch ein Transfer der digitalen Einheiten zwischen Privatpersonen möglich, sofern beide eine Cyberwallet besitzen[88]. Da eCash im Prinzip eine eigene Währung darstellt, fällt sie unter die Zuständigkeitsbereich der Zentralbanken. Daher sollte eCash, wie im Kapitel über Geldpolitik erwähnt, nur von Kreditinstituten emittiert werden dürfen. Diese müssen für die ausgegebenen Einheiten auch entsprechende Garantien übernehmen. Konzipiert ist eCash für den Micropayment-Bereich. Ob dies mit der Online-Überprüfung der Münzen vereinbar ist, wird sich in Feldversuchen herausstellen. Bei einem breiten Einsatz von eCash kann die Online-Verifikation jedoch zu einem Hemmschuh werden. Herkömmliche Technik wird dabei sehr schnell an ihre Grenzen geraten, da jede einzelne Münze kryptographisch erzeugt und nach Gebrauch archiviert werden muß. Mit zunehmender Anzahl an im Umlauf befindlichen Münzen steigt automatisch die Dauer der Echtheitsüberprüfung an. Angriffsmöglichkeiten für Hacker bietet lediglich die Wallet-Software. Die digitalen Münzen sind mit einem starken RSA-Schlüssel kodiert und bieten nur wenig Angriffspunkte, zumal der Wert jeder einzelnen Münze im Verhältnis zum Aufwand, diese zu fälschen, sehr gering ist. Die fest vorgegebene Wertstückelung der Münzen kann sich ebenfalls nachteilig auswirken, da bei zwar ausreichender Geldmenge jedoch ohne passende Münzen erst wieder neues Geld erstellt werden muß. In Deutschland wird e-Cash von der Deutschen Bank in einem Feldversuch getestet[89].

NetCash ist wie NetCheque ein Produkt der University of Southern California. Es wurde als anonymes elektronisches Geld konzipiert, welches sich in die globale Infrastruktur und Kontenführung der Banken integrieren läßt. Das System baut auf dem bereits vorgestellten NetCheque auf. Die Dotierung von NetCash ist Dollar. Eine Stückelung der Münzen ist nicht vorgegeben, da Münzen mit beliebigem Wert erhalten werden können. Gegenüber eCash besitzt es eine deutlich reduzierte Anonymität, da auch ohne Zustimmung des Kunden Zahlungsdaten mit Informationen über die Bestellung ermittelt werden können. Da der herausge-

[88] Vgl. KÖHLER (Electronic Commerce, 1998), S. 66-68 und WASMEIER (Cash auf Draht, 1998), S. 100-101.
[89] Vgl. REICH (Ecash, 1997) und SCHUSTER u. A. (Digital Cash, 1997), S. 57-62.

benden Bank die Seriennummern der Münzen und die Kunden bekannt sind, kann sie nach Rückgabe durch einen Händler Rückschlüsse auf die Verwendung ziehen[90].

Der vereinfachte Ablauf einer Transaktion geschieht wie folgt (siehe auch Abbildung 13):

1. Der Kunde läßt sich von einem Currency-Server Münzen ausgeben und bezahlt im Gegenzug z.B. mit einem NetCheque oder direkt von seinem Konto.
2. Die Münzen werden bei einer Bestellung mit dem öffentlichen Schlüssel des Händlers verschlüsselt und übergeben.
3. Der Händler tauscht die Münzen sogleich bei seiner Bank um und erhält nach Validierung auf Wunsch neue Münzen.

Die Händlerbank leitet die Münzen an die ausgebende Bank um sie dort prüfen zu lassen und den Betrag zu verrechnen.

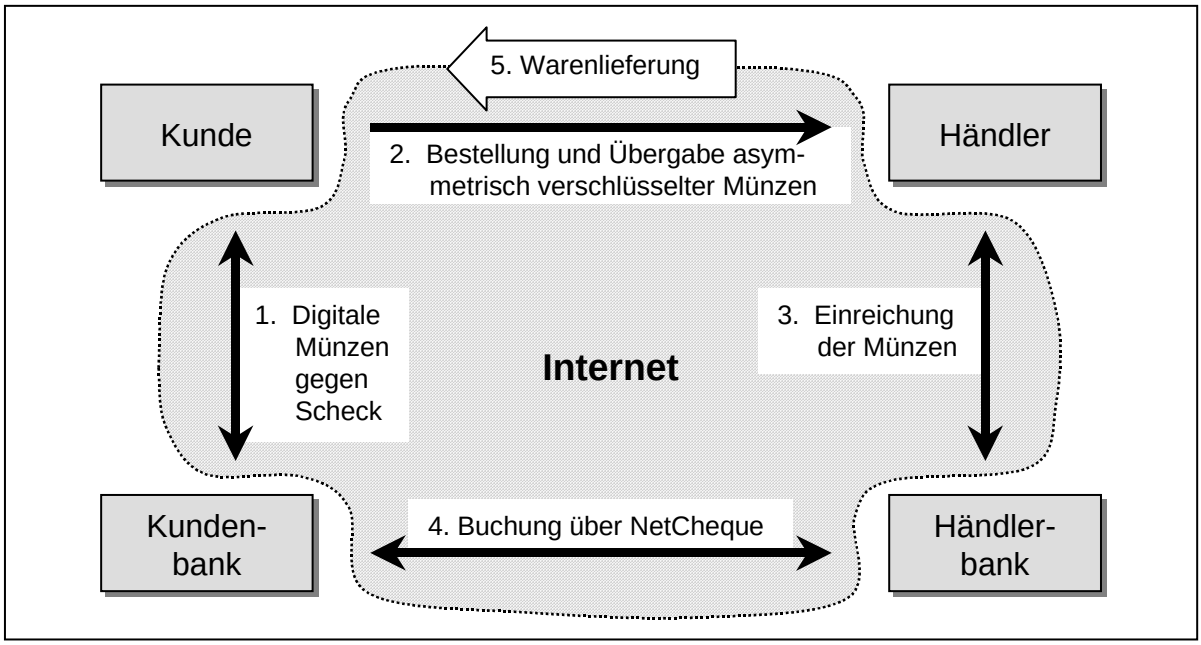

Abbildung 13: Transaktionsfluß bei NetCash

Um mehrfaches Bezahlen mit der selben Münze zu vermeiden, werden alle Seriennummern der ausgestellten, aber nicht eingereichten Münzen in einer Datenbank gespeichert. Die Nummern werden markiert, sobald die Münze eingereicht wurde. Erhaltene Münzen sollten deswegen sofort bei der Bank eingelöst werden[91].

Der Vollständigkeit wegen werden noch kurz zwei weitere Zahlungssysteme im Micropayment-Bereich erwähnt, die jedoch noch in der Entwicklung bzw. Testphase sind. Sowohl

[90] Vgl. KRAUSE (Electronic Commerce, 1998), S. 93-94 und STOLPMANN (Elektronisches Geld, 1998), S. 26.
[91] Vgl. SCHUSTER u. A. (Digital Cash, 1997), S. 62-64 und KRISTOFERITSCH (Digital Cash, 1998), S. 133-135.

PayWord als auch *MicroMint* werden am MIT getestet. Beide Verfahren sind nur für Kleinstbeträge konzipiert und relativ einfach aufgebaut. Die Systeme benötigen keine umfangreiche Verschlüsselungen. Die Währungen sind gerade so kompliziert, daß eine unerlaubte Entschlüsselung gerade etwas mehr kostet, als das erbeutete Geld wert ist[92]

2. Kontobasierte Zahlungssysteme

Kontobasierte Zahlungssysteme können aufgrund ihrer Konzeption (Bildung eines Schattenkontos) keine absolute Anonymität bieten. Die durch ihre relativ einfache Struktur bedingten niedrigen Transaktionskosten machen sie jedoch für Zahlungen im Micropayment-Bereich interessant.

Ebenfalls von CyberCash ist das *CyberCoin-System*. Dieses wird wie die bereits beschriebenen Verfahren CyberCash und CyberCheque in die Wallet-Software integriert. Bei CyberCash wurde erkannt, daß verschiedene Zahlungsvarianten angeboten werden müssen, die sich für unterschiedliche Zwecke eignen. Für Micropayments sind die CyberCoins, für Macropayments CyberCash, bzw. falls keine Kreditkarte vorhanden ist, CyberCheque vorgesehen. Für die Verwendung des Verfahrens ist kein spezielles Konto nötig, der Transfer erfolgt via CyberCash vom Girokonto der Hausbank[93].

Da das CyberCoin-Verfahren nur für Beträge von umgerechnet 5 Pfennig bis etwa 20 DM konzipiert wurde, ist eine Beschränkung der digitalen Münzen auf einen monatlichen Höchstbetrag möglich. Dies soll als zusätzlicher Schutz des Anwenders vor Mißbrauch dienen. Für größere Beträge steht, wie bereits erwähnt, das Kreditkarten-Verfahren zur Verfügung. Als Einsatzgebiet von CyberCoin wird insbesondere die Bezahlung von digitalisierten Gütern mit geringen Preisen, sogenannten Softgoods gesehen. Transaktionen sind jedoch nur mit Händlern möglich, die das CyberCoin-System lizensiert haben.

Im Gegensatz zu eCash und NetCash werden bei CyberCoin keine digitalen Münzen auf dem PC gespeichert. Die eigentlichen Finanzwerte werden ausschließlich auf dem gesicherten Bankserver gespeichert, beim Anwender werden nur sogenannte Log-Dateien angelegt. Dadurch wird sowohl der Diebstahl als auch das Double-Spending von Münzen im CyberCoin-System quasi unmöglich. Der Nachteil ist eine reduzierte Anonymität, da über alle Transaktionen Log-Dateien angelegt werden. Der Kunde bleibt jedoch auf Wunsch zumindest

---

92 Vgl. SCHUMANN / ROSENTHAL (So gut wie Bargeld, 1997), S. 46 und KRAUSE (Electronic Commerce, 1998), S. 95.

93 Vgl. BIBOW / WICHMANN (Elektronisches Geld, 1998), S. 11-13 und DRESEN / DUNNE (Fürs Netz, 1998), S. 116.

dem Händler gegenüber anonym[94]. Die Zahlungsanweisung wird analog zum vorgestellten CyberCash-Verfahren über das Internet verschlüsselt übertragen. Ohne Zwischenschaltung eines Bankservers ist jedoch keine Transaktion möglich.

Ein Ladevorgang mit CyberCoins läuft folgendermaßen ab (Abbildung 14):

1. Der Kunde gibt online an, welchen Betrag er in seine Wallet (bzw. auf das Schattenkonto bei der Bank) übertragen möchte.
2. Nach erfolgreicher Sicherheitsüberprüfung werden die Coins gutgeschrieben.
3. Die Zahlungsaufträge werden an das Kreditinstitut mit dem Schattenkonto weitergeleitet.
4. Falls das Kontokorrent-Konto des Kunden bei einer an CyberCash angeschlossenen Bank ist, wird das Schattenkonto direkt belastet, ansonsten wird der Geldbetrag per Lastschrift eingezogen.

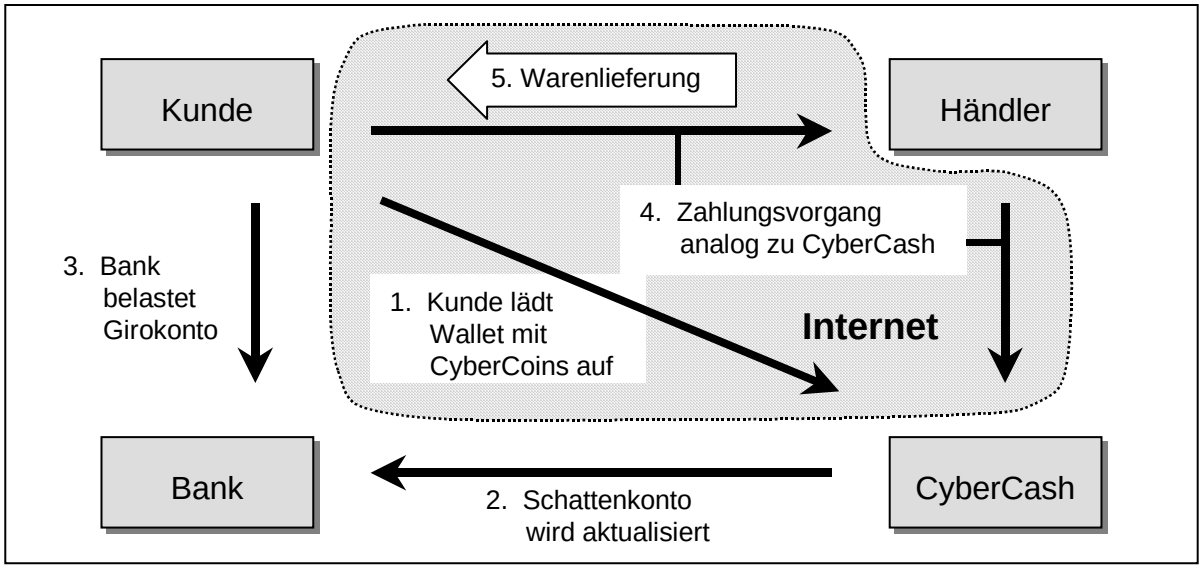

Abbildung 14: Ladevorgang bei CyberCoin

Der weitere Zahlungsablauf und Warentausch mit dem Händler wird analog zum CyberCash-Verfahren durchgeführt. Anfang Oktober 1997 wurde von CyberCash, der Dresdner Bank und der Sachsen LB ein Joint Venture zur Einführung von CyberCoin in der Bundesrepublik gegründet[95].

Millicent wurde Ende 1995 von Digital Equipment (DEC) vorgestellt. Konzipiert ist Millicent zur Bezahlung von Kleinstbeträgen bis hin zu Bruchteilen von Pfennigen (Picopayments). Mit Millicent können nur Produkte bezahlt werden, die auch über das Internet vertrieben werden. Gebühren für den Kunden werden in Höhe von 1% des Umsatzes erhoben. Das System wird

[94] Vgl. KÖHLER (Electronic Commerce1998), S. 64-66 und STOLPMANN (Elektronisches Geld, 1998), S. 71-72.
[95] Vgl. SIETMANN (Electronic Cash, 1997), S. 112-124 und SCHUSTER u. A. (Digital Cash, 1997), S. 44-47.

derzeit von der Suchmaschine Infoseek getestet. Die Millicent-Geldbörse soll in den Internet-Browser integriert werden, so daß keine zusätzliche Software nötig ist. Aufgrund ausschließlicher Verwendung von Kleinstbeträgen können die Sicherheitsanforderungen auf ein Minimum reduziert werden. Der Aufwand zum Mißbrauch steht somit nicht im Verhältnis zu dessen Ertrag. Als Kryptographiealgorithmus wird eine schnell berechenbare Einweg-Hash-Funktion verwendet. So reicht bereits eine geringe Rechnerleistung für eine schnelle Verschlüsselung aus[96].

Kernstück von Millicent ist die Verwendung eines Broker-Systems und sogenannter *„Scripts"*. Scripts sind Nachrichten, die Informationen über den aktuellen Kontostand, die Kontobezeichnung sowie über das Verfallsdatum Auskunft geben. Zusätzlich sind sie mit einer Seriennummer versehen, um Double-spending zu verhindern.

Jedes Script enthält ein Zertifikat mit einer PIN des Kunden, welche potentiellen Diebstahl erschwert, da das Zertifikat erst kurz vor dem Bezahlen erstellt wird. Scripts gelten jedoch nur jeweils für einen Händler. Damit man nicht bei jedem Händler ein Konto eröffnen muß und zur Reduzierung des Verwaltungsaufwandes, werden sogenannte Broker zwischengeschaltet. Bei diesen Brokern wird ein Geldbetrag deponiert und im Gegenzug erhält der Kunde ein Script. Vor der Bestellung tauscht der Kunde bei seinem Broker spezifische Händler-Scripts in der gewünschten Höhe. Mit diesen kann er nun seine Bestellung begleichen (siehe Abbildung 15). Die Händler lösen die erhaltenen Scripts später bei den Brokern gegen echtes Geld ein[97].

[96] Vgl. STOLPMANN (Elektronisches Geld, 1998), S. 78-80 und KRISTOFERITSCH (Digital Money, 1998), S. 135-136.
[97] Vgl. KÖHLER (Electronic Commerce, 1998), S. 68-69.

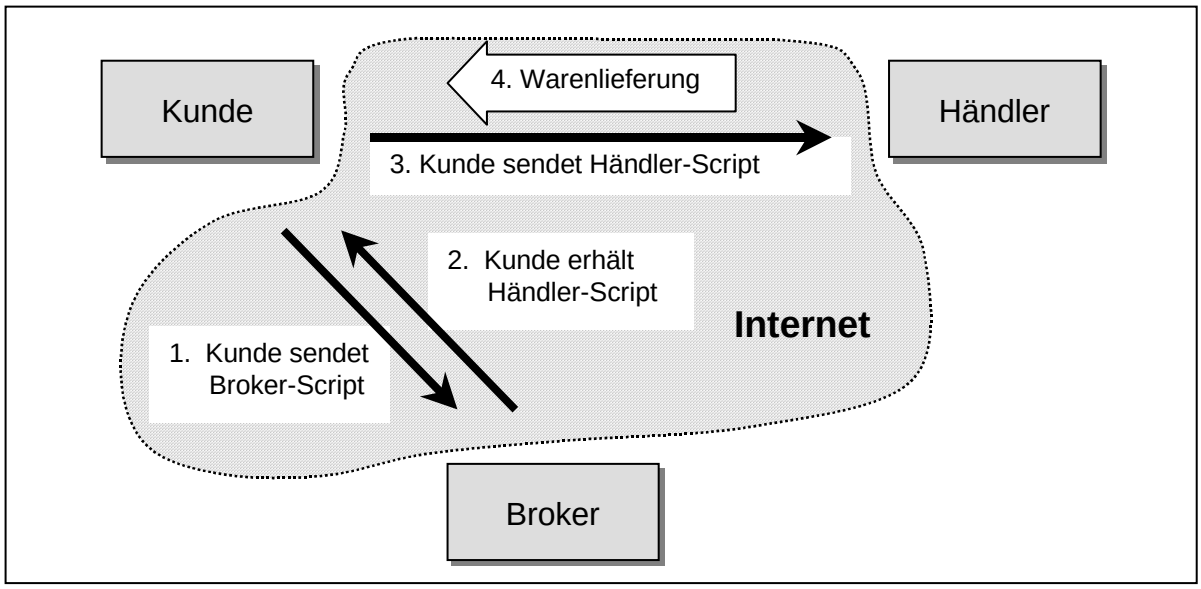

Abbildung 15: Der Zahlungsvorgang mit Millicent

Anonymität wird bei Millicent nicht angestrebt. Da die Kunden jedoch über diverse Broker ihre Scripts erwerben können, gibt es keine zentrale Stelle, bei der ein Kundenprofil erstellt werden könnte. Die Kundenaccounts verlieren zudem nach einer gewissen Zeit ihre Gültigkeit und werden gelöscht. Die Offline-Prüfung der Scripts bei den Händlern bietet zwar keine hundertprozentige Sicherheit, ist jedoch aufgrund der geringen Beträge akzeptabel. Um als vollwertiges Internetbezahlsystem anerkannt zu werden, ist eine Kombination von Millicent mit einem anderen Digital Cash-System nötig.

Der eindeutige Vorteil des Millicent-Systems, was auch Ziel der Entwicklung war, liegt in den im Vergleich zu den anderen Systemen unschlagbar geringen Transaktionskosten. Auch die Skalierbarkeit, d.h. die Ausbaufähigkeit auf eine sehr große Anzahl von Nutzern ist durch die dezentrale Konzeption gewährleistet. Durch die befristete Gültigkeit der Accounts wird erreicht, daß stets nur aktuelle Konten geführt werden[98].

III. Zahlungssysteme auf der Basis von SmartCards

SmartCards bieten beinahe unbegrenzte Einsatzmöglichkeiten. Sie werden bereits bei der Zeiterfassung oder als Münzersatz in öffentlichen Telefonen verwendet. Durch die Telekommunikation und das Internet werden SmartCards Bestandteil der Computer-Peripherie. In Mobiltelefonen und elektronischen Geldbörsen sowie als Zugangskontrolle beim Homebanking kommen sie zum Einsatz. Durch ihre Maßnahmen zum Schutz von Signaturen genügen SmartCards auch erhöhten Sicherheitsanforderungen. SmartCards lassen sich definieren als

[98] Vgl. KRAUSE (Electronic Commerce, 1998), S. 92 und SCHUSTER u. A. (Digital Cash, 1997), S. 70-72.

„um entsprechende Chip- und Prozessortechnologie erweiterte Plastikkarten, die mit Hilfe kryptographischer Verfahren elektronisches Geld speichern können. Sie zeichnen sich ferner durch breite Nutzungsmöglichkeiten aus, d.h. es können verschiedene Anwendungen auf einer Karte enthalten sein“ [99].

1. Technischer Aufbau und Funktionsweise von SmartCards

SmartCards sind intelligente Multifunktionskarten, die einen Chip enthalten, auf dem alle Bestandteile eines Computers zu finden sind. Je nach Ausführung sind ein wiederbeschreibbarer 16 KByte großer EEPROM-Speicher[100], 1 bis 16 KByte RAM[101], 16 KByte ROM[102] sowie eine eigene CPU[103] mit einer Rechenleistung von etwa 1 Million Instruktionen pro Sekunde (MIPS) vorhanden. Lediglich die Energieversorgung und das Benutzerinterface fehlen bzw. sind extern vorhanden. Wie auf jedem Computer läuft auch auf einer SmartCard ein Betriebssystem. Alle Chipkarten sollten hinsichtlich ihrer Technik und Spezifikation der internationalen Norm ISO/IEC 7816 entsprechen. Diese regelt unter anderem auch die Kontaktbelegung des Kartenchips (siehe Abbildung 16).

Je nach Ausstattung verfügen einige Varianten über einen kryptographischen Coprozessor, der die erhebliche Rechenleistung zur asymmetrischen Verschlüsselung aufbringt. Dabei müssen Rechenoperationen mit sehr langen natürlichen Zahlen effizient verarbeitet werden. Die Erzeugung einer digitalen Signatur auf der Karte selbst hat den Vorteil, daß der geheime Schlüssel des Karteninhabers auf der Karte abgespeichert ist, ohne von außen ausgelesen werden zu können. Die Daten können auf verschiedene Weise geschützt werden. Statt einer herkömmlichen PIN werden neuerdings auch biometrische[104] Merkmale zur Authentifizierung verwendet. Zudem verfügt jede Karte über eine nicht veränderbare Seriennummer, welche die Karte dem Benutzer eindeutig zuordnet.

Einfachere Versionen sind die sogenannten Speicherchipkarten mit konkreten Anwendungen wie z.B. die Krankenversichertenkarte. Sie sind billiger und verfügen über keine programmierbare CPU sondern nur über ein wiederbeschreibbares EEPROM. Die bekannte Telefonkarte speichert das Guthaben in Feinsicherungen, die nach Benutzung unwiderruflich durchbrennen.

---

[99] KRISTOFERITSCH (Digital Money, 1998), S. 42.
[100] Electrically erasable programmable ROM, vgl. FASTENRATH, S. 43.
[101] Random access memory, vgl. ebenda.
[102] Read only memory, vgl. ebenda.
[103] Central processing unit, vgl. ebenda.
[104] Z.B. der Fingerabdruck oder das Irisbild.

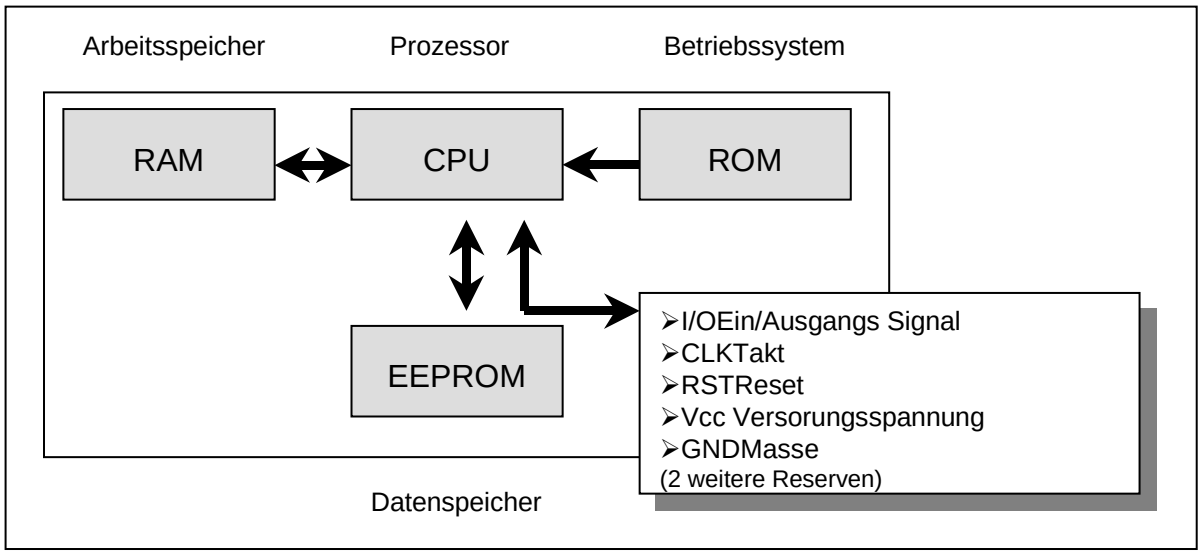

Abbildung 16: Elemente einer SmartCard und ihre Kontaktfelder

Anwendungen für SmartCards werden über sogenannte Applets implementiert. Diese werden vorwiegend in der Programmiersprache Java geschrieben, da diese einfache Schnittstellen und eine breite Akzeptanz bietet. Über die JavaCard-Virtual-Machine werden Applets direkt für das jeweilige Kartenbetriebsystem übersetzt. Durch den Java Standard werden die SmartCards multifunktional, ohne daß dadurch viel Software nötig ist. So ist es ohne weiteres möglich, mehrere Anwendungen auf einer SmartCard zu integrieren (z.B. Geldkarte, Telefonkarte, Ausweise, Zugangskontrolle oder Adressbuch). Ein sogenannter Space-Manager teilt den freien Speicherbereich in Schubladen mit fester Größe ein[105].

In den meisten Fällen werden die Daten mit Hilfe eines Kartenlesers übertragen. Je nach Sicherheitsanforderung muß darauf geachtet werden, daß die Karten von möglichen physikalischen Verbindungen nach außen durch einen Verschlußmechanismus (Shutter) getrennt werden. Für gewisse Anwendungen wie Zugangskontrollen oder Bezahlung von Kleinstbeträgen an Automaten ist auch die Verwendung von kontaktlosen Chipkarten möglich. Damit ist z.B. die Abfertigung einer größeren Anzahl von Personen pro Zeiteinheit oder ein störungsfreier Betrieb unter rauhen Bedingungen möglich.

Kartenleser für SmartCards sind mittlerweile in einer erheblichen Variantenzahl und mit einer Preisspanne von zehn bis über tausend Mark auf dem Markt. Angefangen von Einschüben für das 3,5“-Diskettenlaufwerk über Lesevorrichtungen in Tastaturen bis hin zu externen Geräten. Die Chipkartenleser lassen sich in vier Klassen unterteilen:

[105] Vgl. WALTER (Von der Mikrotransaktion, 1998), S. 14-15 und GLADIS (Krötenwanderung, 1998), S. 128-130.

- Klasse 1 beinhaltet einfache Geräte, welche Chipkarten beschreiben und lesen können. In hohen Auflagen sind solche Geräte schon für unter 20,- DM zu bekommen.
- Chipkartenleser der Klasse 2 müssen eine Tastatur für die Eingabe der PIN besitzen.
- Leser der Klasse 3 benötigen zusätzlich noch ein Display zur Kontrolle der Zahlung.
- Die höchsten Anforderungen werden an Kartenleser der Klasse 4 gestellt, die neben Tastatur und Display noch eine zusätzliches „Crypto-Modul“ aufweisen müssen.

Für eine Bezahlung mit der Geldkarte via Internet kommen nur Kartenleser in Frage, die vom ZKA (Zentraler Kreditausschuß) zugelassen sind. Diese müssen dann der Klasse 4 entsprechen, sofern die Karte auch über das Internet aufgeladen werden soll. Für einen einfachen Zahlungsvorgang würde jedoch bereits ein Gerät der Klasse 1 ausreichen[106]

2. Beispiele für SmartCard-Anwendungen

Primär wurden SmartCards für die Abwicklung von Micropayments im realen Wirtschaftsleben konzipiert. Die Einbindung von SmartCards in Internetzahlungssysteme kann auf zwei verschiedene Arten erfolgen:

- Bei Stand-Alone-Lösungen wird eine Software für die SmartCard-Hardware erzeugt, die ein sicheres Lesen und Schreiben über Internet gewährleistet.
- Im Rahmen von Hybrid-Versionen wird versucht, SmartCard-Technologie in bereits existierende Digital Cash-Lösungen zu integrieren. Inwiefern sich die in diesem Kapitel vorgestellten Verfahren bereits für eine konkrete Online-Zahlung eignen, ist nicht belegt. Einige der Verfahren befinden sich noch immer in der Testphase.

Mondex ist eines der wenigen SmartCard-Systeme, das bereits in mehreren Pilotprojekten getestet wurde. Entwickelt wurde Mondex von Mitarbeitern der National Westminster Bank. Das Projekt begann 1995 mit einem Feldversuch in Swindon[107], Großbritannien, und ist inzwischen noch in Hongkong, Indonesien, auf den Philippinen und in Kanada im Einsatz[108]. Mittlerweile wird Mondex in über 55 Ländern verwendet und die Anzahl der Karten soll bis Ende 1998 bei über einer Million liegen. Im Sommer 1997 wurde unter der Leitung von Mastercard eine erste Internet-Anbindung erprobt. Der Verbindungsaufbau zum Internet erfolgte dabei ausschließlich über GSM-Mobiltelefone[109].

---

[106] Vgl. FASTENRATH u. A. (Smart, 1998), S. 42-47 und BEYKIRCH (Chipgeld, 1998), S. 148-151.
[107] Vgl. KRÖNIG (Abschied, 1995).
[108] Vgl. LUKAS (Cyber Money, 1997), S. 6972.
[109] Vgl. POWELL-JONES (Monex,1998), S. 28.

Die Nutzung von Mondex im Alltag ist recht weit fortgeschritten. Die Karte läßt sich wie Bargeld benutzen und ist für Beträge bis 500 Pfund gültig. Über einen portablen Kartenleser im Taschenrechnerformat werden die Transaktionen durchgeführt. Die Karte kann an speziellen Bankautomaten oder per Telefon aufgeladen werden. Mittels PIN ist die Karte „abschließbar", was als Diebstahlschutz dienen soll. Die Konzeption als Mehrwegkarte erlaubt es den Anwendern, auch Peer-to-Peer-Transaktionen vorzunehmen, d.h. ohne Zwischenschaltung einer Clearingstelle Geld an andere Kartenbesitzer zu übertragen.

Ein weiterer Aspekt ist die Tauglichkeit für mehrere Währungen. Als Multi-Currency-Karte ausgelegt, kann die Mondex-Karte bis zu fünf Währungen verwalten. Eine Händlerkarte unterscheidet sich nur durch den höheren maximalen Betrag, die benötigte Hardware bleibt identisch[110].

Variabel angelegt ist ebenfalls das Sicherheitssystem. Dieses besteht aus zwei Teilsystemen, die unterschiedlich aktiviert und erneuert werden können. Genaue Sicherheitsmerkmale wurden jedoch nicht bekannt gegeben. Beim Zahlungsvorgang kommunizieren die Chips untereinander, ohne daß eine Bank oder Clearingstelle beteiligt ist. Die Geldschöpfung geht von einer Mondex-Master-Karte aus, die das elektronische Geld an andere Ausgabestellen weiterleitet, an denen die Kunden ihre Karten laden können. Durch dieses System soll die Geldschöpfung kontrolliert werden[111].

Durch seine Peer-to-Peer-Eigenschaft bietet das Mondex-System einen hohen Grad an Bedienerfreundlichkeit. Sowohl Händler als auch Kunden profitieren davon. Da nicht jede Transaktion bei der Bank eingereicht werden muß, können gerade Händler dadurch ihre Kosten erheblich senken. Die größere Nähe zu richtigem Bargeld spricht hingegen die Kunden an, die dadurch wesentlich flexibler im Umgang mit der Karte sein können[112].

Allerdings sprechen viele Gründe auch gegen eine breite Verwendung von Mondex. Zum einen ist das Sicherheitssystem komplett auf der Karte verankert und stellt somit ein nicht unerhebliches Risiko dar. Durch die Möglichkeit der direkten Übertragbarkeit auf andere Karten könnten bei größeren Umlaufmengen Fälschungen nur schwer entdeckt werden. Zum anderen begünstigt die freie Verfügbarkeit Geldwäsche und Steuerhinterziehung[113].

CAFE (Conditional Access for Europe) ist ein seit 1992 von der EG gefördertes Verfahren mit dem Ziel, bis zum Jahr 2000 Bargeld und Ausweise auf SmartCards zu realisieren. Es

[110] Vgl. KRAUSE (Electronic Commerce, 1998), S: 97 und KÖHLER (Electronic Commerce, 1998), S. 71.
[111] Vgl. SIETMANN (Electronic Cash, 1997), S. 65-69.
[112] Vgl. POWELL-JONES (Monex, 1998), S. 28-29.
[113] Vgl. THOME / SCHINZER (Electronic Commerce, 1997), S. 125.

existieren Parallelen zum DigiCash-Verfahren bei der Verwendung von verdeckten Signaturen. Dies sichert einerseits die Anonymität und verhindert andererseits die Mehrfachausgabe der selben digitalen Münze[114].

Aufgebaut ist das System sowohl aus der Karte, in der die Werteinheiten gespeichert werden, als auch aus der Geldbörse selbst, die über eine Infrarotverbindung mit dem Terminal kommuniziert. Die Sicherheit des Systems basiert auf einem Public-Key-Verfahren mit digitalen Signaturen. Peer-to-Peer-Transaktionen sollen ebenfalls möglich sein. In die Geldbörse integriert ist der sogenannte „Guardian", ein kryptographischer Prozessor, ohne den keine Transaktion möglich ist. Er versieht nicht nur jede Zahlung mit einer digitalen Signatur, sondern integriert auch die Identität des Nutzers in die Seriennummer der Münze. Im Betrugsfalle kann die Identität jedoch aufgehoben werden[115]. Das Sicherheitsniveau des CAFE-Projekts gilt als sehr hoch. Inwiefern der Pilotversuch in Brüssel eine Praxistauglichkeit zeigte und wieweit diese auf das Internet übertragbar ist, ist nicht bekannt.

Die Firma TeleCash hat zudem ein Verfahren namens *TC-Moneybytes* auf Basis der deutschen Geldkarte entwickelt. Über einen Adapter für das Diskettenlaufwerk kann die Smart-Card mit dem PC kommunizieren[116]. In Kapitel 1. II. in Abschnitt C wird das Verfahren mit anderen Systemen verglichen.

Als Zahlungssysteme auf Basis von SmartCards ohne realisierte Internet-Anbindung lassen sich ferner folgende Beispiele nennen:

- Die *Quick-Karte* ist das Österreichische Gegenstück zur Geldkarte. Es bestehen zwar einige konzeptionelle Unterschiede, etwa der Verzicht auf die Führung eines Schattenkontos, eine Internet-Anbindung wird jedoch ähnlich wie bei der Geldkarte funktionieren[117].
- Eine Mischung aus Geldkarte und Mondex stellt das von Visa veröffentlichte *VisaCash* dar. Bei einem umfangreichen Test während der olympischen Spiele in Atlanta wurden über 200.000 Transaktionen mit einem Gesamtumsatz von 1,1 Milliarden US$ registriert[118]. Als Akzeptanzstellen wurden PCs, Kioske, Mobiltelefone, Hand-held-PCs und TV set-top Boxen spezifiziert. Auf Wunsch wird auch die Visa Kreditkarte integriert, so daß ein breites Einsatzspektrum gegeben ist. Die Karte ist nach dem Visa-Open-Platform-Card Standard ausgelegt, der dem Java-Standard angepaßt wurde. Weltweit laufen bereits

[114] Vgl. ebenda, S. 125.
[115] Vgl. KÖHLER (Electronic Commerce, 1998), S. 72 und KRISTOFERITSCH (Digital Money, 1998), S. 145-147.
[116] Vgl. KRAUSE (Electronic Commerce, 1998), S. 97.
[117] Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 147-149.
[118] Vgl. KRAUSE (Electronic Commerce, 1998), S: 97.

über 70 Pilotprojekte mit der neuen Visa-SmartCard. Weitere Testversuche in Japan und Frankreich sind geplant[119].

Danmønt war 1991 das weltweit erste Kartensystem auf dem Geldwerte gespeichert werden konnten. In Dänemark erfreut sich diese Karte großer Beliebtheit, da mit ihr in öffentlichen Telefonen, an Automaten, in Transportsystemen und an Kiosken bezahlt werden kann. Es sind über ein halbe Million Karten im Umlauf, die hauptsächlich an Automaten zum Einsatz kommen[120].

3. Die deutsche Geldkarte im Internet

Durch die sukzessive Umstellung aller im Umlauf befindlichen EC-Karten sind mittlerweile über 45 Millionen bankübergreifende SmartCards mit dem Geldkartenchip im Umlauf[121]. Durch das starke Bewerben der Geldkarte durch die Banken ist eine breite Einsatzmöglichkeit abzusehen. Mit ihrer Eignung für Kaufbeträge von zehn Pfennig bis zu 400 Mark nimmt die Geldkarte bei den Internetbezahlsystemen eine Zwischenstellung ein. Eine endgültige Verwendung der Geldkarte im Internet scheitert bisher noch an der Freigabe bzw. Zertifizierung durch den ZKA. Der Wettlauf um die beste Geldkartenlösung und die Gunst der Banken hat bereits begonnen. Hard- und Software-Hersteller bieten inzwischen einige Lösungen an, die aber wohl alle noch nicht den hohen Anforderungen des ZKA genügen.

Der konventionelle Ladevorgang der Geldkarte erfolgt am Geldautomaten. Der Betrag wird vom Girokonto auf das Börsenverrechnungskonto der jeweiligen Bank gebucht. Im Rahmen der Einführung des HBCI (Home Banking Computer Interface) wird es auch möglich sein, die Geldkarte über das Internet aufzuladen[122]. Ein vereinfachtes Schema einer Internettransaktion mit der Geldkarte ist in Abbildung 17 dargestellt.

---

[119] Siehe www.visa.com.

[120] Vgl. KRAUSE (Electronic Commerce, 1998), S. 97.

[121] Im Vergleich zu etwa 15 Millionen Kreditkarten in Deutschland.

[122] Vgl. STEIN (Homebanking, 1998), S. 39-43.

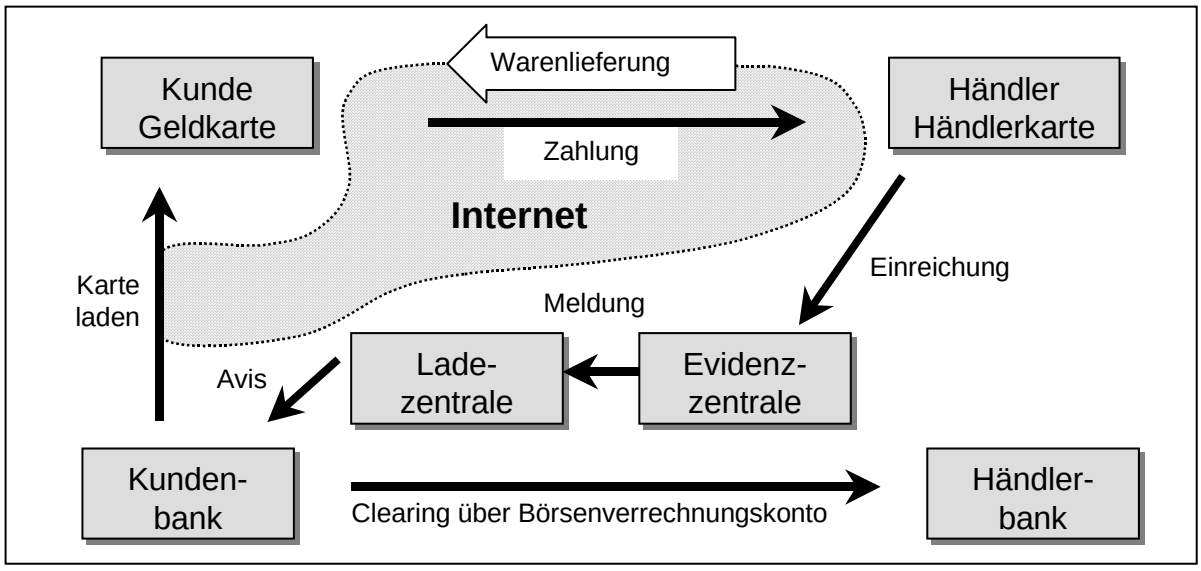

Abbildung 17: Geldkarten-Zahlungen via Internet

Zahlungsvorgänge über das Internet mit der Geldkarte unterscheiden sich von herkömmlichen in einem wesentlichen Punkt: Händler und Karteninhaber befinden sich an verschiedenen Punkten. Aus diesem Grund muß das einzelne Akzeptanzterminal durch ein geteiltes ersetzt werden.

Der eine Chipkartenleser befindet sich beim Kunden, der andere beim Händler. Die notwendige Kommunikation erfolgt über Internet-Protokolle. Auf Kundenseite muß ein Java-tauglicher Browser, in den die Geldkarten-Anwendung implementiert wird, sowie ein Lesegerät vorhanden sein. Der Händler benötigt die entsprechenden Gegenstücke, d.h. ein Kartenterminal sowie die Software für Händler. Die Software kann in die Internet-Kasse integriert werden, die unter Umständen bereits andere Zahlungssysteme enthält. Je nach Größe des Händlers kann auch ein Dienstleister zwischen Händler und Evidenzzentrale geschaltet werden, der die Verwaltung der Kartenserver übernimmt.

Die Kommunikation zwischen Kunden- und Händlerkarte während des eigentlichen Zahlungsvorgangs ist in jedem Fall durch die kartengestützte Kryptographie geschützt. Hierbei kommen verschiedene Verfahren und Protokolle zum Einsatz. Nach erfolgter Transaktion zeigt das Java-Applet im Kundenbrowser Zahlbetrag, Zeitpunkt, Händlerkartennummer sowie Restbetrag auf der Geldkarte an. Dies kann als Quittung und für spätere Reklamationen ausgedruckt werden. Über die Händlerkartennummer besteht die Möglichkeit, die reale Anschrift des Händlers zu erfahren.

Ein Vorteil der Geldkarte ist die relativ hohe Anonymität. Absolute Anonymität wird zwar nur bei nicht kontogebundenen Wertkarten erreicht, die Geldkarte bietet jedoch trotz Schattenkonto einen ausreichenden Schutz. Allein die Tatsache, daß keine sensiblen Daten wie

Kreditkartennummern über das Internet übertragen oder Werteinheiten auf dem relativ unsicheren PC gespeichert werden, bringt für den Anwender psychologische Vorteile[123].

Nicht nur für Kunden sondern auch für Internet-Händler ist die Geldkarte interessant. Während Kreditkarteninstitute bis zu 4% des Umsatzes verlangen, kosten Transaktionen mit der Geldkarte minimal 2 Pfennig, maximal jedoch nur 0,3% des Umsatzes. Auch beim eigentlichen Bezahlvorgang entstehen nur sehr geringe Übertragungskosten, da keine Online-Verifizierung nötig ist. Durch diese insgesamt sehr niedrigen System-Gebühren ist das Verfahren auch sehr gut für Zahlungen im Micropayment-Bereich geeignet.

Nachteilig im Vergleich zu Kreditkarten ist der momentan auf 400 DM begrenzte Kaufbetrag der Karte. Kreditkarten namhafter Firmen autorisieren bis zu 10.000 DM. Hierbei stellt sich allerdings die Frage, ob Zahlungen dieser Größenordnungen über das Internet sinnvoll bzw. realistisch sind. Weiterhin ist bei Internetzahlsystemen auf Basis von Kreditkarten kein Lesegerät notwendig. Um mit der Geldkarte im Internet bezahlen zu können, ist somit erst die Anschaffung eines ca. 50 bis 100 DM teuren Kartenlesers notwendig[124].

[123] Vgl. KÖHLER (Electronic Commerce, 1998), S. 70 und WASMEIER (Cash auf Draht, 1998), S. 98-99.
[124] Vgl. BEYKIRCH (Chipgeld, 1998), S. 148-151 und GLADIS (Krötenwanderung, 1998), S. 128-130.

C. Beurteilung der Cyber Money-Systeme und Einschätzung der zukünftigen Entwicklung

Die Wandlung des Internet vom Informationsmedium zum elektronischen Marktplatz führt zu einer Veränderung der Rahmenbedingungen für alle Beteiligten. An die Technik und die Standards des Internet werden plötzlich völlig neue Anforderungen gestellt, die teilweise nicht ohne Weiteres zu erfüllen sind. Die Banken sehen sich neuen Wettbewerbern gegenüber, die ihnen in ihrer traditionellen Funktion als Anbieter von Zahlungssystemen Konkurrenz machen. Die Verbraucher oder Kunden schließlich müssen sich mit den neuen Medien erst noch vertraut machen. Im letzten Abschnitt dieser Arbeit werden nun Auswirkungen und Abschätzungen der Entwicklung von Internetzahlungssystemen bezüglich aller Beteiligten untersucht.

I. Durch das Internet determinierte technische Rahmenbedingungen

1. Sicherheit durch Kryptographie und digitale Signaturen

Da ohne ausreichende Verschlüsselung ein sicherer Gebrauch von digitalen Zahlungssystemen nicht möglich ist, soll in diesem Abschnitt das Wesen der Kryptographie und Zertifikate näher erläutert werden. Zu lösende Probleme sind zum einen eine absolut sichere Übertragung der Daten und zum anderen die zweifelsfreie Identität des Absenders.

Die *Kryptographie* oder *Kryptologie* ist ein Teilbereich der Mathematik. Die Verschlüsselungsalgorithmen basieren auf komplexen mathematischen Verfahren und der zugrundeliegenden Zahlentheorie[125]. Entwickelt wurde das Gebiet der Kryptographie durch die Geheimdienste verschiedener Länder. Erst durch die zunehmende Verbreitung elektronischer Medien für den privaten und kommerziellen Bereich wurde die Verschlüsselungstechnik veröffentlicht.

Prinzipiell lassen sich zwei unterschiedliche Verschlüsselungsprinzipien nennen. Die Verschlüsselung mit einem einzigen geheimen Schlüssel wird als *secret-key* oder *symmetrisch* bezeichnet. Häufigster Vertreter dieser Art ist das DES-Verfahren. Der Nachteil der secret-key Verfahren ist offensichtlich. Sowohl Empfänger als auch Sender benutzen denselben Schlüssel, der für eine Kommunikation erst ausgetauscht werden muß. Die Sicherheit wird erheblich gefährdet, wenn der Schlüssel dabei über das Internet ausgetauscht wird. Vorteil der

[125] Vgl. LYNCH (Zahlungsverkehr, 1997), S. 78.

symmetrischen Verfahren ist die geringere Rechenleistung, die zur Verschlüsselung benötigt wird.

Bei den *Public-key-Verfahren* werden zwei Schlüssel verwendet, wovon einer öffentlich und der andere geheim ist. Alle Daten werden mit dem öffentlichen Schlüssel codiert, können jedoch nur mit dem geheimen Schlüssel entziffert werden. Die Verfahren werden auch als *asymmetrisch* bezeichnet. Das bekannteste asymmetrische Verfahren ist der RSA-Algorithmus.

Bei vielen Zahlungssystemen kommt ein sogenanntes Hybridverfahren zum Einsatz. Da die asymmetrische Verschlüsselung großer Datenmengen sehr hohe Rechenleistung erfordert, wird oft nur mit einem symmetrischen Verfahren verschlüsselt, der Schlüssel jedoch mit einem asymmetrischen Verfahren übertragen.

Als problematisch sind die von den USA auferlegten Exportbeschränkungen für kryptographische Verfahren zu sehen. Dadurch können Sicherheitsdifferenzen zwischen amerikanischen und europäischen Zahlungssystemen entstehen. Gerade kreditkartenbasierte Systeme, die sich auch für eine Bezahlung in Übersee eignen, sollten ein einheitlich hohes Sicherheitsniveau aufweisen. Die Beschränkung des Sicherheitsniveau oder sogar Verbote von Verschlüsselungen mit ausreichender Länge ist mit dem Verbot von Briefumschlägen oder der Hinterlegung von Safe-Kombinationen bei Behörden vergleichbar. Die fadenscheinige Begründung, diese Maßnahmen seien zur besseren Bekämpfung von Verbrechen notwendig, kann nicht wirklich ernst genommen werden[126].

Um das Problem der zweifelsfreien Identität zu lösen, gibt es die Möglichkeit der Nutzung einer *digitalen Signatur*, d.h. einer allgemein akzeptierten, elektronischen Unterschrift. Diese Signatur muß nur ein einziges Mal bei einer dazu autorisierten Stelle beantragt werden. Bereits im Juli ´97 wurde vom Bundestag das weltweit erste Gesetz zur digitalen Signatur verabschiedet, nach Meinung vieler Fachleute jedoch mit einem fast zu perfektionistischen Ansatz. Ausdrücklich wurde dabei Raum für staatlich nicht kontrollierte Zertifizierungsstellen gelassen. Ein behördlich beglaubigtes Zertifikat hat jedoch den Vorteil größerer Glaubwürdigkeit und breiterer Verwendbarkeit. Die meisten aktuellen Verfahren zur digitalen Signatur basieren auf asymmetrischen Verschlüsselungen. Der Empfänger eines Dokumentes kann die Echtheit durch Dechiffrieren mit dem öffentlichen Schlüssel des Absenders zweifelsfrei überprüfen. Personenspezifische öffentliche Schlüssel werden von den Zertifizierungsstellen (auch

[126] Vgl. KRISTOFERITSCH (Digital Money, 1998), S. 85.

Trust Center oder Certificate Authority genannt) verwaltet. Diese können bei Bedarf abgefragt oder bei Gefahr des Mißbrauchs gesperrt werden. Der geheime Schlüssel ist nur dem Inhaber selbst bekannt, wodurch der Verschlüsselungsvorgang der Leistung einer Unterschrift gleich kommt. Größere Dokumente müssen dabei nicht vollständig verschlüsselt werden, sondern lediglich mit einem digitalen „Fingerabdruck“ versehen werden.

Abgesehen von den technischen, organisatorischen und rechtlichen Problemen bleibt es fraglich, ob eine solche Lösung international durchsetzbar ist und wer wann bereit ist, regelmäßig Geld für eine elektronische Identität auszugeben, um damit innerhalb des Internet rechtskräftige Geschäfte zu tätigen. Für Deutschland wurde zu Beginn dieses Jahres in Mainz eine Kontroll- und Genehmigungsbehörde eingerichtet, welche die digitalen Signaturen verwaltet. Die Jahresgebühren für eine Chipkarte mit elektronischer Identität belaufen sich auf etwa 150,- DM.

2. Direkter Vergleich der vorgestellten Verfahren

Obwohl alle vorgestellten Verfahren für denselben Zweck, die sichere Bezahlung über das Internet, entwickelt worden sind, könnten die Ansätze in ihrer Architektur und den Detailausprägungen nicht unterschiedlicher sein. Insbesondere bezüglich der Basis der Verfahren (Kreditkarte, SmartCard, Konto, Software) und der Höhe der vorgesehenen Zahlungsbeträge mit den daraus resultierenden Transaktionskosten, sind deutliche Unterschiede bei den Systemen festzustellen. Gemeinsamkeiten treten unabhängig von der technischen Umsetzung darin auf, daß oft eine neutrale Institution zwischen Kunde und Händler vermittelt und für Sicherheit der Transaktion sorgt.

Die Versuche, elektronische Schecks durchzusetzen, scheiterten an dem im Vergleich zur Kreditkarte höheren Risiko für den Empfänger der Zahlung. In Europa wurden die Verfahren überhaupt nicht getestet, weswegen sie hier auch nicht mit den anderen Verfahren verglichen werden. Im Folgenden werden also nur diejenigen Systeme bewertet, die auch aktuelle Verwendung finden. In den beiden Tabellen werden die vorgestellten Verfahren anhand verschiedener Kriterien bewertet. Dabei wird noch einmal zwischen guthaben- und kreditkartenbasierten Verfahren unterschieden, um eine bessere Vergleichbarkeit zu erzielen.

	eCash	**Geldkarte**	**CyberCoins**	**MilliCent**
Status des Verfahrens in Deutschland	Pilotversuch Deutsche Bank	Anbieter warten auf Zertifizierung	Pilotversuch	Pilotversuch
geeignet für Beträge von	0,10 – 400 DM	0,01 – 400 DM	0,05 – 20 DM	Pfennigbruchteile bis 5 DM
Speicherort des Guthabens	PC-Festplatte	Chip der Geldkarte	Server der Bank	Server des Brokers
Preis Kundensoftware	kostenlos	50 – 100 DM für Kartenleser	kostenlos	kostenlos
Preis Händlersoftware	kostenlos	anbieterabhängig	kostenlos	noch nicht bekannt
Gebühren	keine Angaben	0,3%, mindestens 2 Pfennig	keine Angaben	keine Angaben
Anonymität	ja	eingeschränkt	eingeschränkt	eingeschränkt
Widerruf möglich	nein	nein	nein	ja
Wiederherstellung im Verlustfall	ja	nein	ja	ja
Sicherheit	sehr hoch	sehr hoch	hoch	hoch
Skalierbarkeit	aufwendig	gut	einfach	einfach
Peer-to-Peer	ja	nein	nein	nein

Abbildung 18: Vergleich guthabenbasierter Verfahren

Es ist deutlich zu erkennen, daß bisher nur Systeme auf Basis von Kreditkarten kommerziell einsetzbar sind. Diese sind aber wiederum nur für größere Beträge geeignet und können nur eine eingeschränkte Anonymität vorweisen. Hinzu kommt die recht hohe Belastung des Kunden durch Gebühren. Die guthabenbasierten Systeme sind zwar über die Pilotversuche noch nicht hinausgekommen, können jedoch hinsichtlich Geldnähe und Transaktionskosten einige Pluspunkte aufweisen.

	TeleCash	CyberCash USA	CyberCash GmbH	SET
Status des Verfahrens in Deutschland	kommerziell verfügbar	kommerziell verfügbar	in Vorbereitung	Pilotversuch abgeschlossen
Dauer einer Transaktion	15 – 90 Sek.	15 – 90 Sek.	15 – 90 Sek.	15 – 90 Sek.
Geeignet für Beträge von	ab ca. 20 DM	ab ca. 10 $	ab ca. 20 DM	ab ca. 20 DM
Preis Kundensoftware	kostenlos	kostenlos	kostenlos	kostenlos
Preis Händlersoftware	in Einrichtung enthalten	in Einrichtung enthalten	in Einrichtung enthalten	anbieterabhängig
Einrichtung Händler-account	1000 – 7500 DM	300 – 800 $	keine Angaben	keine Angaben
Gebühren	0,10 – 0,49 DM	0,10 – 0,20 $	keine Angaben	keine Angaben
monatliche Mindest-gebühren	150 – 200 DM	40 – 70 $	keine Angaben	keine Angaben
Anonymität	eingeschränkt	eingeschränkt	obliegt der Händlerbank	obliegt der Händlerbank
Widerruf möglich	ja	ja	ja	ja
Sicherheit	hoch	hoch	hoch	sehr hoch
Skalierbarkeit	gut	aufwendig	aufwendig?	gut
Peer-to-Peer	nein	nein	nein	nein

Abbildung 19: Vergleich kreditkartenbasierter Verfahren

Cyber Money-Systeme, bei denen digitalen Werteinheiten auf dem PC gespeichert werden, weisen ein auf die Unzuverlässigkeit des PCs zurückführendes Vertrauensdefizit auf. Berichte über sogenannte „Bugs“, Millennium-Probleme und Internet-Viren sind für eine breite Einführung solcher Verfahren nicht gerade förderlich.

3. Technische Varianten, Möglichkeiten und Trends

Im Zuge der laufenden Pilotprojekte und dem damit verbundenen Praxistest haben sich für einige Systeme Varianten oder Verbesserungsvorschläge herauskristallisiert, die im Folgenden näher erläutert werden.

Thin Wallets und *Multi-Purpose-Wallets* stellen die erste Möglichkeit dar. Herkömmliche Wallets mit einem Umfang von 3 bis 4 MByte (sogenannte „Fat-Wallets“) haben sich beim Download und der Installation auf Kundenseite als sehr unbeliebt erwiesen. Die Bereitstellung der Software auf konventionelle Weise (z.B. per Post) würde bei den Anbietern jedoch zu hohen Supportkosten führen. Der Trend geht daher teilweise zu sogenannten „Thin-Wallets“. Diese haben eine Größe von etwa 50 KByte und lassen sich somit leicht als Applets in die Browser integrieren. Kritik wurde dahingehend geäußert, daß eine verstärkte Verwal-

tung des Systems auf dem Betreiber-Server ein Rückschritt bezüglich der Sicherheit bedeuten könnte[127].

Auch sogenannte Multi-Purpose-Wallets finden immer mehr Verwendung. In Ihnen können mehrere unterschiedliche Zahlungssysteme, im Idealfall auch von verschiedenen Anbietern, integriert werden. Dadurch kann die relativ enge Verwendungsbandbreite einzelner Zahlungssysteme auf leichte Weise erweitert werden.

Für den deutschen Markt bietet sich als Alternative zu den kreditkartenbasierten Systemen das *elektronische Lastschriftverfahren* (electronic direct debit oder edd) über Internet an. Tele-Cash, CyberCash und das SET-Konsortium arbeiten an entsprechenden sicheren Lösungen. Die durchschnittliche Dauer, bis der Händler den Betrag auf dem Konto hat, ist im Vergleich zur Kreditkarte sogar kürzer. Zudem ist das Risiko für den Händler bei Widerruf der Zahlung durch den Kunden geringer, da die Kreditkartengesellschaften den Einsatz der Kundenauthentifizierung bislang nicht anerkennen. Da in Deutschland für jeden Lastschriftvorgang eine Kundenunterschrift vorliegen muß, wird als Kunstgriff eine virtuelle Buchungskarte (Direct Debit Card) verwendet. Für diese Karte leistet der Kunde einmalig einen schriftlichen Einziehungsauftrag. Unklar ist jedoch noch die rechtliche Bindung des Kunden bei dieser Variante[128].

Im Bereich der Abrechnung über Provider hat T-Online eine weitere Variante entwickelt, die nun auch den Abruf kostenpflichtiger Informationen über das Internet (also außerhalb des Provider-Netzes) ermöglicht. Das *T-Online Billing* (TOB) wird analog zum herkömmlichen Verfahren über T-Online abgerechnet. Der Kunde wird jedoch vom Billing-Server anhand seiner ihm dynamisch zugewiesenen IP-Adresse erkannt und erhält einen Hinweis über die anfallenden Kosten. Dabei werden Gebühren von 1 Pfennig bis zu 1,30 DM pro Minute berechnet. Dem Anbieter werden die angesammelten Gebühren regelmäßig überwiesen. Der Kunde bleibt während des Vorgangs anonym und mit knapp 3 Millionen T-Online Teilnehmern bietet das Verfahren eine hohe Zahl potentieller Kunden.

Weitere Perspektiven bestehen in neuen *Verwendungsformen für die deutsche Geldkarte*. Ein gesteigertes Interesse könnte die Geldkarte durch die kürzlich vereinbarte Zusammenarbeit von ZKA und der Deutschen Telekom erlangen. Ab Herbst 1999 sollen alle Telefonzellen für eine Bezahlung mit der Geldkarte eingerichtet sein. Einerseits wird zwar befürchtet, daß Telefonieren mit der Geldkarte teurer sein wird als mit herkömmlichen Telefonkarten, andererseits

[127] Vgl. WASMEIER (Cash auf Draht, 1998), S. 99.
[128] Vgl. ebenda, S. 98.

ist es auch möglich, daß die Telekom über jede Entlastung dankbar ist, da Zahlungsverkehrssysteme aufwendig und kostenintensiv sind.

Unter der Leitung des ZKA soll zudem ein europäisches Gremium entstehen, welches die Herstellung einer Interoperabilität der bestehenden elektronischen Geldbörsen zur Aufgabe hat. Hierbei ist auch eine Zusammenarbeit mit Visa und dem spanischen Geldbörsenemittent SERMEPA geplant.

Die Geldbörsenspezifikationen sollen dann über CEPS (Committee for European Payment Systems) und ECBS (European Committee for Banking Standards) zum Standard werden. Dies würde einen breiten Einsatz der Geldkarte im Internet ebenfalls sehr begünstigen.

Eine weitere Variante, die zur Zeit erprobt wird, ist *eCash auf SmartCards*. Mit der „Global-NetCard“ wollen IBM und die Deutsche Bank sozusagen eCash zum Mitnehmen anbieten. Hierbei zeigt sich auch deutlich der Unterschied zu den kontenbasierten Systemen: Die einzelnen digitalen Münzen können auf einem beliebigen Speicher gelagert werden, theoretisch sogar auf einem Blatt Papier.

Probleme ergeben sich allerdings noch im Detail. Der Speicherplatz auf der SmartCard ist noch sehr begrenzt, so daß nur eine geringe Anzahl von Münzen untergebracht werden kann. Da eine digitale Münze von eCash etwa 500 Zeichen umfaßt und somit rund 0,5 KByte groß ist, passen lediglich 20 Münzen auf die Karte. Von IBM wurde ein Verfahren entwickelt, die Münzgröße auf ein Viertel zu reduzieren, so daß immerhin 80 bis 90 Münzen Platz auf einem Chip finden. Weiter gibt es Überlegungen, die Staffelung der Münzbeträge zu vergrößern, um damit einen höheren Maximalbetrag zu realisieren.

Die geplanten Zahlungen an Offline-Automaten bringt ebenfalls Probleme mit sich. Da die Online-Prüfung der Münzen bezüglich Double-Spending Bestandteil des eCash-Systems ist, muß auf anderem Weg verhindert werden, daß geklonte Münzen in Umlauf kommen. Wird durch eine zusätzliche Signatur die Sicherheit erhöht, geht die Anonymität verloren und das Verfahren hat nur noch entfernt mit dem ursprünglichen eCash zu tun[129].

Falls es in absehbarer Zeit zu einem breiten Einsatz elektronischer Zahlungsmittel im Internet kommt, wird dies auch nachhaltige technische Auswirkungen auf das Internet selbst haben. Die rasante Entwicklung im Internet und Electronic Commerce beruhte bisher allein auf Basis des PCs als Endgerät. Durch die aktuelle Entwicklung werden immer mehr Geräte für das Internet tauglich gemacht. So werden in naher Zukunft Fernsehgeräte, Telefone oder andere

[129] Vgl. DRESEN (Abgewogen, 1998), S. 97.

Medien Zugang zum Internet haben. Dies soll vor allem eine Erleichterung für technisch weniger versierte Nutzer bringen, die sich nicht mit den Tücken eines PCs auseinandersetzen wollen[130]. Auch das Internet ist in seiner heutigen Form nur ein Vorbote davon, was in den kommenden Jahren erwartet werden kann. Die meisten Technologien, die heute im Internet zum Einsatz kommen, sind lediglich Übergangstechnologien. So ist schon heute die Konzeption eines leistungsfähigeren „Internet 2" in Arbeit und die im Internet bewährte Sprache HTML wird bereits durch eine neue mit dem Namen XML ergänzt[131].

II. Banken und Institutionen im Umfeld von Cyber Money

1. Geldpolitische Auswirkungen auf den Zahlungsverkehr und Maßnahmen der Zentralbanken

Durch die zunehmende Verwendung von elektronischem Geld anstelle von Bargeld oder herkömmlichen Zahlungsweisen kommt es zu einer Verschiebung im Zahlungsverkehr. Diese Verschiebung von Bargeld hin zu elektronischem Geld hat für die Banken unterschiedliche Auswirkungen. Für die Bundesbank bedeutet dies zum einen eine verkürzte Notenbankbilanz mit einer niedrigeren Seigniorage, also weniger Gewinne aus der Banknotenausgabe[132]. Zum anderen werden die Steuerungsmöglichkeiten der Geldmenge beschränkt. Untersuchungen der Universitäten Greifswald und Hannover zufolge könnte ein Verlust von 350 Millionen Mark durch die geringere Geldschöpfung entstehen. Da die Erzielung einer möglichst hohen Seigniorage nicht zu den Hauptzielen der Notenbank gehört, kann der drohende Verlust auch nicht als Begründung zur Ausdehnung des Banknotenmonopols herangezogen werden[133].

Drastische Strukturveränderungen durch den Einsatz von elektronischem Geld ergeben sich auch bei den Geschäftsbanken. Zum einen entfallen nicht unbeträchtliche Kosten der Bargeldverarbeitung (wie z.B. Sortieren, Zählen und Aufbewahren), zum anderen ergeben sich Konsequenzen für die Zinserträge: die Bargeldhaltung der Verbraucher sinkt und somit nehmen auch die Abflüsse aus dem Giralgeldkreislauf und die Barreserven der Banken ab. Dies bewirkt ein Ansteigen des Kreditvergabespielraums und vermindert die Mindestreserve[134]. Durch zunehmende Ausgabe von Netzgeld nimmt somit der Refinanzierungsbedarf bei der Zentralbank ab. Das betrifft sowohl die notwendige Beschaffung von Bargeld für die Bankkunden als auch die Pflicht zur Erfüllung der Mindestreservepflicht auf Sichteinlagen.

---

130 Vgl. SIETMANN (Electronic Cash, 1997), S. 49.
131 Vgl. BECKER (Secure Commerce, 1998), S. 225.
132 Vgl. ISSING (Geldpolitische Bedeutung, 1997), S. 619 und MÖKER (Elektronisches Geld, 1998), S. 189.
133 Vgl. FRIEDRICH (Elektronisches, 1997), S. 10 und RADETZKY (Kleingeld, 1998), S. 60.
134 Vgl. SÖLLNER / WILFERT (Elektronisches Geld, 1996), S. 396-397.

Einer Studie von britischen Marktforschern zufolge wird der Anteil des Bargelds am Zahlungsverkehr in den nächsten Jahren jedoch nicht wesentlich sinken. Als ein Grund dafür wird ein gut ausgebautes Netz an Geldausgabeautomaten genannt. Für die Banken ist eine Reduzierung der Bargeldtransaktionen nach heutigen Transaktionskosten auch nicht unbedingt wünschenswert. So sind die Kosten einer elektronischen Überweisung oder für Kartentransaktionen etwa dreimal so hoch wie die einer Bargeldtransaktion. Die Kosten für Schecks und papiergebundene Transaktionen liegen sogar noch darüber. Die Gesamtkosten des Zahlungsverkehrs würden sich allein deswegen erhöhen, da die meisten Bargeldtransaktionen außerhalb des Bankensystems stattfinden. Bei einem Anstieg bargeldloser Zahlungssysteme würden sich somit automatisch die Kosten des Zahlungsverkehrs bei den Kreditinstituten erhöhen[135].

Die geldpolitischen Auswirkungen von Cyber Money lassen sich somit in folgenden Punkten zusammenfassen:

- *Rationalisierung*: Der Einsatz von Geld vereinfacht in einer arbeitsteiligen Wirtschaft zwar den Güteraustausch, verursacht selbst jedoch Kosten. Werden durch neue Medien Transaktionen zu niedrigeren Kosten möglich, ist es ökonomisch rational, diese als Zahlungsmittel zu verwenden.
- *Floatnutzen*: Gewinne aus dem sogenannten Bodensatz oder Float sind zwar nur schwer quantifizierbar, stehen jedoch den Kreditinstituten zur Verfügung. Bei breiter Nutzung von Digital Cash-Systemen könnte der Floatgewinn an Bedeutung gewinnen und je nach Marktsituation könnten die Kunden am Zinsgewinn beteiligt werden.
- *Refinanzierungsbedarf*: Mit zunehmender Verbreitung von elektronischem Geld wird in wachsendem Maße Bargeld verdrängt. Der geschätzte Geldbedarf von der Zentralbank nimmt damit tendenziell ab. Auch das Mindestreservesoll der Banken vermindert sich, da durch die Ausgabe von Netzgeld die mindestreservepflichtigen Bilanzpositionen reduziert werden.
- *Abwicklung des Zahlungsverkehrs*: Um einen Vertrauensverlust aufgrund von Fälschungen oder Systemschwächen zu vermeiden, muß großer Wert auf Sicherheit, Funktionsfähigkeit und Integrität des Zahlungsverkehrs gelegt werden.
- *Geldmengenbegriff*: Damit die nachfragewirksame Geldmenge richtig erfaßt werden kann, müssen die elektronischen Zahlungsmittel in den relevanten Geldaggregaten enthalten sein. Dies setzt eine korrekte statistische Erfassung voraus.

[135] Vgl. RIEKEBERG (Geldkarte, 1998), S. 36.

Solange jedoch wie bei der deutschen Geldkarte jede Transaktion über das Internet wieder in den Bankenkreislauf überführt wird, gibt es auch keine wirklichen Probleme bei der Geldmengensteuerung bzw. –erfassung. Durch eine Beschränkung von elektronischem Geld auf genau einen Geschäftsvorfall, landen die digitalen Münzen nach jeder Transaktion wieder bei der Bank oder Zentralbank. Dadurch kann sogar ein besserer Überblick über den Geldfluß erreicht werden, als dies bisher der Fall ist. Somit ließe sich das Volumen des Netzgeldes auch quantitativ genau bestimmen und über bekannte geldpolitische Instrumente steuern. Die Einführung der Geldkarte wurde bereits durch die Erweiterung der Geldmengenaggregate berücksichtigt[136].

Die Kopplung einer virtuellen Währung an eine reale Währung sowie die Verwendung innerhalb des Währungsgebietes ist allerdings zwingend. Nur so ist ein regionales und funktionales Offshore-Booking zu vermeiden. Dies würde bedeuten, daß Waren innerhalb eines Zahlungsgebietes mit Zahlungsmitteln von außerhalb beglichen werden. Eine Gegenüberstellung von Waren und Geldmenge wäre dann nicht mehr möglich und eine Geldpolitik ineffizient. Auch eine Besteuerung nach herkömmlichen Methoden wäre dann nur noch unter Aufhebung der Anonymität des Systems gewährleistet[137].

Bei einer zunehmenden Verbreitung von elektronischem Geld durch Geschäftsbanken hat die Bundesbank daher folgende Maßnahmen vorgeschlagen[138]:

- Erweiterung der statistischen Meldepflicht,
- Erhöhung des Mindestreservesatzes,
- Änderung bzw. Erweiterung der Mindesreservebasis,
- Einführung einer Deckungspflicht auf die Gegenwerte sowie
- Umstellung des geldpolitischen Intrumentariums.

Die europäischen Zentralbanken haben sich ausdrücklich die Option auf eine Monopolisierung der Herausgabe von elektronischem Geld offengehalten. Dadurch würde elektronisches Geld automatisch zum gesetzlichen Zahlungsmittel und alle Akzeptanzprobleme würden vermieden. Das Banknotenmonopol würde somit um eine neue Form von Zentralbankgeld erweitert.

[136] Vgl. HARTMANN (Ein Modell, 1997), S. 478.
[137] Vgl. BORCHERT (Cyber Money, 1996), S. 42-43.
[138] Vgl. MÖKER (Elektronisches Geld, 1998), S. 201.

Dabei könnte sich eine Herausgabe von elektronischem Geld nur auf die Werteinheiten selbst, d.h. auf die Geldseite beziehen und die technische und anwendungsorientierte Seite den verschiedenen Systembetreibern überlassen werden. Um einer unkontrollierten Ausbreitung von elektronischem Geld Einhalt zu gebieten, kann die Zentralbank notfalls die Schutzvorschriften für das Banknotenmonopol auf elektronisches Geld ausdehnen[139].

Allerdings ist hierzu anzumerken, daß sich keine „gesicherten Aussagen über das Geldangebotsverhalten der Finanzintermediäre und ihre Beeinflussung der Geldpolitik der Zentralbank treffen lassen. ... [Auch] konnten bisher wesentliche Störungen der Wirkungen geldpolitischer Maßnahmen nicht festgestellt werden. ... Sollte es sich in Zukunft herausstellen, daß das autonome Geldangebotsverhalten der Finanzintermediäre die Geldpolitik der Bundesbank erheblich durchkreuzt, so müßten neue geldpolitische Instrumente zu ihrer Kontrolle eingesetzt werden“[140].

Als Fazit läßt sich feststellen, daß Bargeld für Kreditinstitute vor allem wegen der Refinanzierungskosten bei der Zentralbank sehr teuer ist. Das gilt aber auch für elektronisches Bargeld. Vor diesem Hintergrund scheint es nur logisch, daß die Kreditinstitute zuerst ihre auf Buchgeld basierenden Zahlungsangebote optimieren und der Einführung von elektronischem Bargeld eher zögernd gegenüber stehen[141].

2. Feldversuche und Unterstützung der Verfahren durch deutsche Banken

Wie bereits im Zusammenhang mit den jeweiligen Systemen angedeutet, werden bei verschiedenen Banken Cyber Money-Systeme in Pilotprojekten getestet. CyberCash hat mit der Sachsen-LB und der Dresdner Bank zwei deutsche Lizenznehmer gefunden. Diese haben in einem Pilotprojekt die CyberCash GmbH gegründet, als Joint-Venture mit der amerikanischen CyberCash Inc. (Virginia). An diesem Versuch nahmen zu Beginn neben circa 30 Händlern auch 5000 Mitarbeiter und Privatkunden der beiden Banken teil[142].

eCash wird in einem Pilotversuch der Deutschen Bank getestet. Genaue Zahlen über die Teilnehmer sind nicht bekannt, doch ist anzunehmen, daß zwischen 50 und 100 Händler sowie einige tausend Kunden an dem Versuch teilnehmen. Die Dauer der Testphase wurde bereits mehrfach verlängert.

---

139 Vgl. FRIEDRICH (Elektronisches, 1997), S. 16.
140 SCHAAL (Geldtheorie, 1998), S. 116.
141 Vgl. KLEIN (Cyber Money, 1997), S. 210.
142 Vgl. DRESEN / DUNNE (Fürs Netz, 1998), S: 110-116.

Über Ergebnisse der Feldversuche der deutschen Banken ist leider nicht viel zu erfahren. Die Pilotprojekte werden in der Öffentlichkeit oft geschönt dargestellt, d.h. die Zahlen der Händler und Nutzer werden deutlich zu hoch angegeben. Viele Anbieter klagen zudem über zu geringe Umsätze, die den Aufwand (noch) nicht rechtfertigen. Da sowohl Frist als auch Anzahl der Teilnehmer bereits mehrfach verlängert bzw. erhöht wurden, liegt der Schluß nahe, daß noch keine konkreten Strategien und Ergebnisse gefunden oder die bisherigen nicht befriedigend sind. So wurde der Beginn des Produktivbetriebs der neuen Zahlungssysteme mehrfach hinausgeschoben. Hinzu kommt erschwerend, daß einige der ersten Anbieter von Digital-Cash-Systemen mittlerweile trotz diverser Lizenzvereinbarungen vom Konkurs bedroht sind. Nicht ganz unbeteiligt ist dabei die Bankgesetzgebung, die zwar Cyber Money nicht kennt, für die Einführung jedoch einige Hürden darstellt.

Als strategischer Vorteil für die Kreditinstitute könnte sich der Einsatz der Geldkarte im Internet herausstellen. Aufgrund der technischen Infrastruktur der ec-Karte mit dem integrierten Geldkarten-Chip wird eine künstliche Markteintrittsbarriere für Non- und Nearbanks geschaffen. Wenn es den Banken gelingt, die erforderliche technologische Kompetenz bereitzustellen, können sie eine Rolle als Infrastrukturanbieter beim Electronic Commerce einnehmen. Neben dem klassischen Homebanking können so auch neue Wachstums- und Ertragspotentiale erschlossen werden[143].

Momentan scheitert jedoch ein weiterer Ausbau der Geldkarte für das Internet an der fehlenden Zulassung des ZKA. Einige technisch ausgereifte Verfahren für die Geldkarte stehen bereits zur Verfügung, lediglich die Zertifizierung fehlt. Das ZKA hat bisher drei generische Anforderungen an die Geldkarte gestellt:

Der angezeigte Betrag muß mit dem transferierten Betrag übereinstimmen,

- die Authentizität des Händlers muß gewährleistet sein und
- die Transaktionsprotokolle müssen manipulationssicher sein.
- Standards oder Abnahmeroutinen für konkrete Lösungen gibt es vom ZKA bisher nicht.

Der Fall der deutschen Geldkarte macht deutlich, daß verschiedene Interessengruppen für eine Verzögerung des Interneteinsatzes verantwortlich sind. Der ZKA verweigert die Zulassung aufgrund nicht geklärter Sicherheitsanforderungen der Chipkartenleser. Wie im zweiten Teil dieser Arbeit bereits beschrieben, sind vier Klassen von Chipkartenlesern zu unterscheiden. Für eine einfache Bezahlung mit der Geldkarte reicht ein Gerät der Klasse 1 aus. Nur wenn

[143] Vgl. RAPP (Tendenzen, 1998), S. 14.

die Karte über das Internet auch aufgeladen werden soll, ist ein Gerät der Klasse 4 vorgeschrieben, da dieser Vorgang als extrem sicherheitskritisch eingestuft wird. Es sollte jedoch dem Kunden überlassen werden, ob er ein Gerät für mehr als 100,- DM anschaffen möchte, nur um seine Karte per Internet aufzuladen. Einige der immer höheren Sicherheitsanforderungen an die Geldkarte werden andererseits auch von den größeren Privatbanken gestellt. Denn sowohl die Deutsche Bank als auch die Dresdner Bank unterhalten selbst Cyber Money-Projekte wie z.B. eCash oder CyberCoin und haben diesbezüglich ebenfalls Interesse an einer Freigabe durch den ZKA[144].

Als Ergebnis kann festgehalten werden, daß keines der in Deutschland zur Diskussion stehenden Verfahren einstimmige Unterstützung von den Banken erhält. Die Investitionen in die favorisierten Verfahren sind inzwischen wohl zu hoch, als daß man sich auf eines der Systeme einigen könnte.

3. Höhere Anforderungen an die Kreditinstitute für eine Steigerung des Kundennutzens

Da die Währungspolitik eine zentrale Aufgabe in unserer Gemeinschaft darstellt, darf die Verwendung von Digital Cash nicht allein von den Bedürfnissen des Wirtschaftsverkehrs abhängen. Eine hoheitliche Überwachung ist unverzichtbar. Daher ist eine Erweiterung des Kreises der Bankgeschäfte und eine Unterstellung von Near-banks unter eine spezifische Wirtschaftsaufsicht sinnvoll.

Laut §3 des Bundesbankgesetzes hat die Bundesbank eine Überwachungsfunktion über den Zahlungsverkehr insgesamt und über die einzelnen Systeme in Deutschland. Dabei wird auch das Verhalten der Kreditinstitute bezüglich Bonität und Liquidität beobachtet. Für eine wirksame Kontrolle im Umgang mit elektronischem Geld ist jedoch eine einzelne Bankenaufsichtsbehörde nicht ausreichend. Vielmehr ist eine grenzüberschreitende Kooperation dieser Stellen durch völkerrechtliche Verträge erforderlich[145].

Von der EU-Kommission wurden am 29.7.98 zwei Richtlinienentwürfe für die Herausgabe von E-Geld und den Status der herausgebenden Institute vorgelegt. Darin wird die „Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geldinstituten“ und die „Koordinierung der Rechts- und Verwaltungsvorschriften über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute“ geregelt. Dabei wird die Herausgabe von E-Geld nicht als Einlagengeschäft betrachtet, das herkömmlichen Kreditinstituten vorbehalten werden soll. Allerdings

[144] Vgl. GLADIS (Krötenwanderung, 1998), S. 130.
[145] Vgl. GRAMLICH (Elektronisches Geld, 1997), S. 18.

werden für E-Geldinstitute schwächere Aufsichtsregelungen als ausreichend betrachtet. Gewisse Mindestanforderungen bezüglich Anfangskapital, Eigenmittel, Management und Aufsicht werden jedoch gestellt. Um Wettbewerbsverzerrungen zu vermeiden, sollen die E-Geldinstitute gleichzeitig in die bestehenden Bankrechtskoordinierungs-Richtlinien einbezogen werden[146]. Als Gründe der Reglementierung von elektronischem Geld führt die „Arbeitsgruppe für EU-Zahlungssysteme und Netzgeld" an[147]:

- Schutz der Bezugsbasis des bestehenden geldpolitschen Instrumentariums,
- Schutz der Verbraucher bei Insolvenz des Emittenten,
- Schutz des öffentlichen Vertrauens in das allgemeine Zahlungssystem sowie
- Sicherung des fairen Wettbewerbs unter den Emittenten.

Der Stellenwert der Banken wird im Rahmen einer Einführung von Cyber Money noch einmal unterstrichen. Dies wird auch durch die Novellierung des Kreditwesengesetzes deutlich. Der Ausbau des elektronischen Zahlungsverkehrs ist noch lange nicht abgeschlossen. Sowohl Verbraucheraufklärung als auch die Entwicklung des Verbraucherverhaltens bezüglich der neuen Medien sind dabei nicht vorrangig. Eher die Rationalisierung der Bankgeschäfte, die vom Geschäftskundenbereich nun auch immer stärker das Privatkundengeschäft umfaßt, steht dabei im Vordergrund.

Daher ist es für die Banken bereits jetzt erforderlich, Erfahrung in der virtuellen Abwicklung von Güterströmen und Leistungen zu gewinnen. Nur so können sie bei einem zukünftig breiten Einsatz von Digital Cash ihre Wettbewerbsvorteile Vertrauen und Sicherheit im Geschäft mit Firmenkunden und Konsumenten wahren. Denn eines läßt sich bereits jetzt feststellen: die gewohnte Kundenbindung wird sich mit der Einführung von leicht vergleichbaren Angeboten im Internet schnell ändern. Durch die neue Preissensitivität muß das Kundengeschäft grundsätzlich neu bewertet werden[148].

Die besondere Herausforderung für die Banken wird das Erkennen der optimalen Nutzung des Mediums Internet sein. Dabei sollte ein „best value" für den Kunden in Zusammenarbeit mit bankexternen Unternehmen sowohl im technischen Umfeld (z.B. Provider) als auch im inhaltlichen Umfeld (z.B. Informationsanbieter, Nachrichtendienste) erzielt werden. Als klassische Dienstleistungsanbieter sind Banken und Sparkassen besonders von den Merkmalen der Informationsgesellschaft betroffen. Viele ihrer Produkte lassen sich schon heute problemlos

146 Vgl. BÖHLE / RIEHM (EZI-N, 1998), Newsletter Nr. 20.
147 Vgl. BÜSCHGEN (Bankbetriebslehre, 1998), S. 428-429.
148 Vgl. WANKE (Sachsen LB, 1998), S. 219.

digitalisieren und über das Internet vertreiben. Selbst komplexe Bankprodukte werden davon betroffen sein. Die vielbeschworene Loyalität des Kunden zur Hausbank wird dadurch weiter abnehmen und es wird zu einer Anonymisierung der Kunde-Bank-Beziehung kommen. Durch die Transparenz der Bankdienstleistungen im Internet wird sich das Preis-Leistungs-Bewußtsein der Kunden noch verstärken[149].

III. Cyber Money aus Kunden- und Anwendersicht

Auf Verbraucherseite entstehen bezüglich den vorgestellten Zahlungssystemen Konflikte zwischen Bedienerfreundlichkeit, Systemsicherheit und der gebotenen Anonymität. Bei absoluter Anonymität ist eine reduzierte Sicherheit in Kauf zu nehmen, zudem ist die Beweislage im Zweifelsfalle erheblich komplizierter. Die Punkte Sicherheit, Anonymität und Bedienerfreundlichkeit bilden eine Art magisches Dreieck, das nur schwer optimiert werden kann[150].

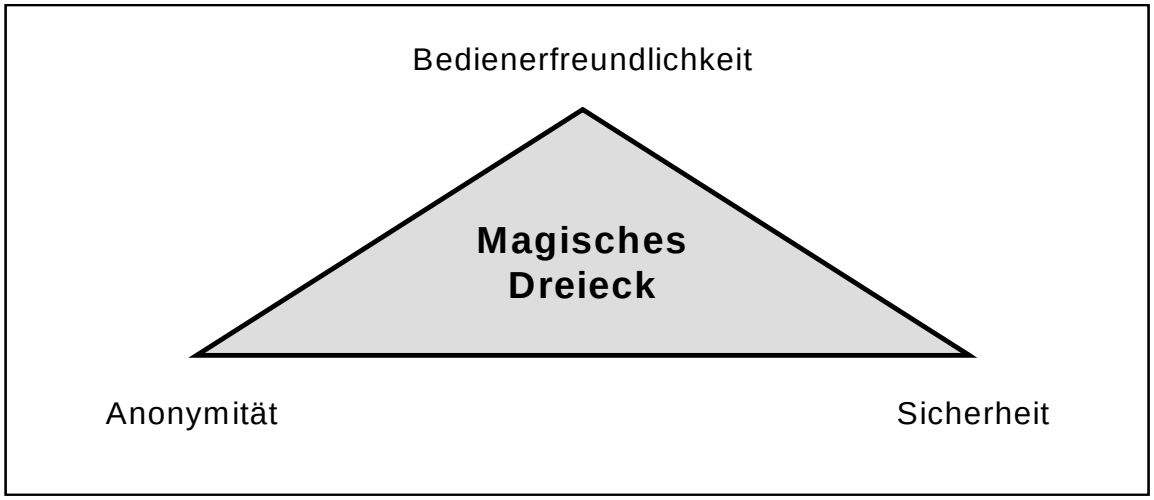

Abbildung 20: Anforderungen an ein Cyber Money-System

Die Aspekte der Sicherheit wurden bereits im Abschnitt C. I. 1. behandelt. Im folgenden wird nun die Bedienungsfreundlichkeit und Anonymität aus Verbrauchersicht betrachtet.

1. Bedienung und Akzeptanz durch die Anwender von Cyber Money

Unter Berücksichtigung aller vorgestellten Ideen, die als zukünftige Zahlungsmöglichkeiten im Internet diskutiert werden, bleibt abzuwarten, welche Lösung sich letztendlich durchsetzen wird. Ob eine Lösung wie die Geldkarte, die eine kostenintensive Hardware-Komponente enthält, sich gegen reine Softwarelösungen wie eCash oder CyberCash durchsetzen kann, oder ob nicht doch Systeme auf Basis der Kreditkarte die besten Chancen haben, ist noch nicht abzusehen.

[149] Vgl. WEISS (Virtuelle Bank, 1998), S. 427-428und RAPP (Tendenzen, 1998), S. 15.
[150] Vgl. LÜTGE (Viele Bits, 1997), S. 23.

Die Merkmale, die ein Zahlungssystem im Internet grundsätzlich erfüllen sollte, um den Ansprüchen von Anbietern und Verbrauchern zu genügen, stehen bereits jetzt schon fest[151]:

- Unabhängigkeit von physischen Orten,
- von maßgeblichen Institutionen anerkannte Sicherheit,
- Geheimhaltung des Benutzers,
- Vertrautheit mit der Zahlungsweise,
- hohe Zuverlässigkeit,
- zügige Abwicklung,
- breite Akzeptanz,
- Währungsunabhängigkeit,
- internationale Verrechnungsmöglichkeit sowie
- Teilbarkeit in kleinere Einheiten.

Die Erfahrung erfolgreicher amerikanischer Online-Händler zeigt, daß zumindest die US-Kundschaft keine komplexen High-Tech Zahlungslösungen annimmt, sondern eher Systeme, die einen angemessenen Kompromiß zwischen Sicherheit und Bequemlichkeit darstellen. Umständliche Authentifizierungsmaßnahmen und lange Transaktionszeiten haben sich bei der US-Kundschaft als äußerst unbeliebt erwiesen. Gerade noch akzeptiert wird eine automatische Prüfung der Rechnungsanschrift zur Kreditkarte mit dem sogenannten AVS (Adress Verification System). Dadurch wird die Wahrscheinlichkeit eines Kartenmißbrauchs deutlich verringert, was den US-Händlern offensichtlich genügt.

Ein Abwägen von Chancen und Risiken findet bei deutschen Online-Händlern noch nicht in gleichem Maße statt. Eine Bezahlung ohne schriftliche Anmeldung über das Internet ist noch immer die Ausnahme. Geliefert wird entweder per Vorkasse oder bei konventionellen Gütern per Nachnahme. Dies wirkt eher geschäftshemmend und unterdrückt ein spontanes Internet-Einkaufserlebnis[152].

Untersuchungen haben gezeigt, daß die Kunden bereit sind, bedienerfreundliches Home-Banking sowie Electronic Commerce zu akzeptieren, wenn sie damit Zeit und Geld sparen

[151] Vgl. SEIPP (Shopping, 1998), S. 46.
[152] Vgl. WASMEIER (Cash auf Draht, 1998), S. 96.

können[153]. Die Kosten der Nutzung eines Internetzahlungssystem setzen sich dabei aus verschiedenen Komponenten zusammen[154]:

- *Variable Kosten pro Transaktion*: diese bestehen zum einen aus den Online-Kosten und zum anderen aus systemabhängigen Kosten pro Transaktion oder einer Umsatzpauschale zusammen.
- *Fixe Kosten*: je nach System können Fixkosten pro Monat oder Jahr anfallen, die meisten Anbieter werden aber keine solchen Gebühren erheben.

Dabei werden die Kosten je nach System variabel zwischen Kunden und Händler aufgeteilt. Meistens ist nur für die Händler eine Lizenzgebühr vorgesehen, um auf Verbraucherseite eine breite Akzeptanz zu finden. In der Einführungsphase eines Systems fallen für den Kunden zumeist keine Kosten an. Ferner ist die Frage zu stellen, ob Systeme mit der Möglichkeit einer wirtschaftlichen Zahlung von Kleinstbeträgen, vom Kunden überhaupt nachgefragt werden. Zwar besteht auf Anbieterseite Interesse, gewisse digitale Güter nur gegen einen Betrag abzugeben, doch darf bezweifelt werden, ob der Internetbenutzer auch für jede Kleinigkeit bezahlen wird. Die gewünschte Information oder Ware ist „um die Ecke“ vielleicht bereits umsonst zu bekommen, frei nach dem im Internet gängigen Motto: „Bezahlt wird nicht!“. Viele Anbieter sehen auch genau darin ihr eigentliches Problem: den Kunden davon zu überzeugen, daß Dienstleistung Geld kostet[155].

Ein weiterer Aspekt für ein Internetbezahlsystem ist auch die Spontanität, welche das System dem Nutzer ermöglicht. Muß z.B. die Geldkarte vor einer Bezahlung im Internet zuerst bei einer Bankfiliale aufgeladen werden, so kann dies sicherlich nicht als spontan bezeichnet werden. Kreditkarten bieten hier einen eindeutigen Vorteil. Jedoch sind kreditkartenbasierte Zahlungssysteme nur für Anwender sinnvoll, die bereits im Besitz einer solchen sind. Die Anschaffung einer Kreditkarte zur ausschließlichen Nutzung bei Internetzahlungen ist durch die hohen Transaktionskosten und die jährlichen Gebühren nicht gerechtfertigt.

Ein viel diskutierter Vorschlag zur Steigerung der Attraktivität der Geldkarte besteht beispielsweise in der Verzinsung des Kartenguthabens bis zur tatsächlichen Ausgabe. Im Gegensatz zum Bargeldverkehr stehen die Beträge der Geldkarte auf den Schattenkonten den Instituten zinslos zur Verfügung. Bei einer angenommenen Nutzung der Karte von 10% der Bevölkerung und einem durchschnittlichen Ladebetrag von 100 DM würden den Banken somit

[153] Vgl. LYNCH (Zahlungsverkehr, 1997), S. 131.
[154] Vgl. STOLPMANN (Elektronisches Geld, 1998), S.29.
[155] Vgl. RADETZKY (Monex, 1998), S. 17.

rund 800 Millionen DM für die Verzinsung am Tagesgeldmarkt zur Verfügung stehen. Diese Erlöse könnten zur Nutzensteigerung der Geldkarte gegenüber dem Bargeld zumindest teilweise an die Kunden weitergegeben werden[156].

Wie im realen Zahlungsverkehr wird sich in der virtuellen Welt sehr wahrscheinlich ebenfalls auf Dauer ein Portfolio an Zahlungsmitteln etablieren. Standardisierte Wallet-Software mit multiplen Zahlungssystemen werden in Zukunft durch einfaches Anklicken einen Zahlungsvorgang auslösen, ohne daß der Kunde noch merkt, welche Bezahlvariante sich dahinter verbirgt[157]. Neben der Zahlung mit der Kredit- oder Geldkarte werden auch digitale Münzen und elektronische Lastschriftverfahren, ähnlich der Bezahlung mit der EC-Karte, zur Verfügung stehen. Die Kreditwirtschaft muß die einzelnen Produkte klar positionieren und ihre Einsatzfelder definieren. So kann für jede Zahlung das optimale Verfahren gewählt werden, denn keines der bisher bekannten Verfahren kann sowohl Anonymität des Verbrauchers, Sicherheit bei großen Beträgen, Wirtschaftlichkeit bei kleinen Beträgen, grenzüberschreitende Zahlungen und ein breite Akzeptanz sowie einfache Bedienbarkeit in sich vereinen[158].

2. Anonymität und Datenschutz contra Sicherheit

Die Gewährleistung der Anonymität ist für viele Verbraucher das wichtigste Kriterium bei Cyber Money-Systemen. Solange das Geld eine „digitale Spur" hinterläßt, ist es kein perfektes Geld. Die Gefahr, daß über solche Daten nicht erwünschte Käuferprofile erstellt werden, ist zu groß. Der gläserne Kunde wäre die Folge[159].

Wenn von Internetzahlungssystemen Anonymität gefordert wird, so kann dies gegenüber mehreren Beteiligten gemeint sein. Zum einen muß Anonymität gegenüber Dritten, d.h. völlig Unbeteiligten gewährt sein. Damit soll Mißbrauch ausgeschlossen werden. Zum anderen ist auch eine zumindest ausreichende Anonymität gegenüber dem Service-Provider und der Bank erforderlich. Dies soll vorrangig dem Kunden Schutz gegenüber Datenmißbrauch geben, notfalls aber eine Offenlegung der Transaktionen ermöglichen. Ferner ist bei Bedarf Anonymität gegenüber dem Vertragspartner wünschenswert[160].

Im zweiten Abschnitt der Arbeit wurde bereits die Anonymität der Systeme beurteilt. Die Frage nach einer befriedigenderen Anonymität eines Zahlungssystems ist durchaus berechtigt und darf nicht unterschätzt werden. Szenarien über die totale Kontrolle des Menschen gibt es

[156] Vgl. RIEKEBERG (Geldkarte, 1998), S. 37.
[157] Vgl. THIESSEN (Elektronische Zahlungsmittel, 1998), S. 222.
[158] Vgl. SEIPP (Shopping, 1998), S. 47.
[159] Vgl. JAHN (Geld, 1995), S. 24.
[160] Vgl. FLIEGE (Anonymer Zahlungsverkehr, 1998), S. 44-47.

bereits genügend. Worauf sich der Kunde bei Nutzung einer der zahlreichen Kredit-, EC-, GeldKarten oder SmartCards einläßt, kann er nur selten mit ausreichender Gewißheit überblicken. Abbildung 21 verdeutlicht die Verbreitung einiger typischer Smart-Card-Anwendungen.

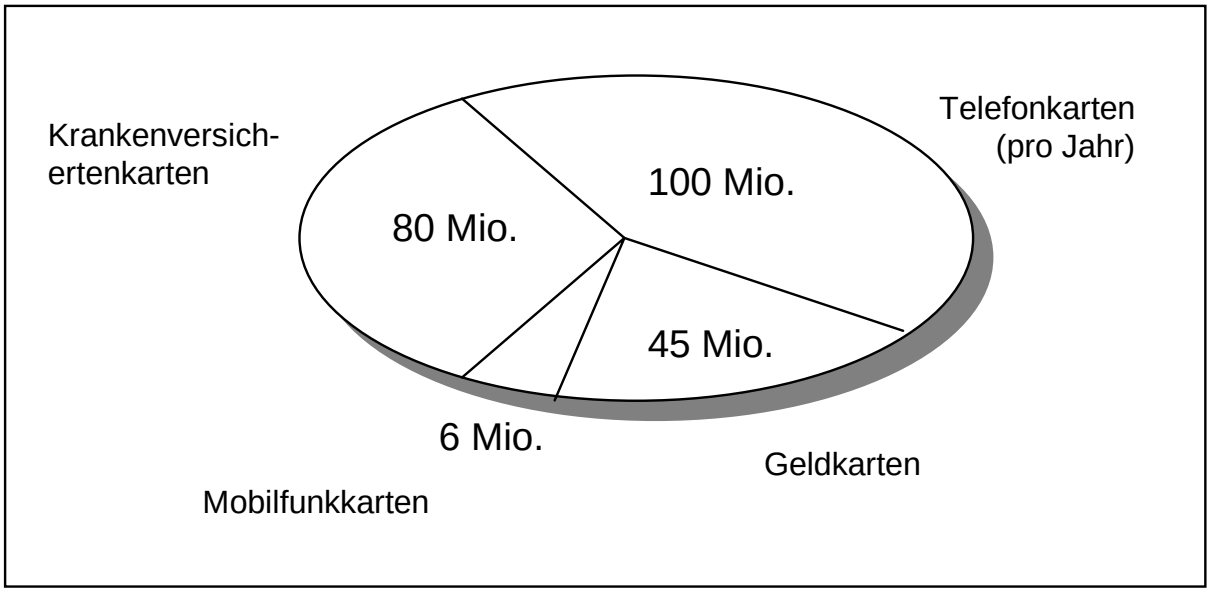

Abbildung 21: Anzahl der SmartCards in Deutschland

Bei jedem Bezahlvorgang hinterläßt der Kunde eine digitale Spur. Diese enthält Daten über seine Person, was und wieviel er wann und wo eingekauft hat. In vielen Fällen werden diese Daten bewußt von den Karteninstituten gesammelt und ausgewertet bzw. an Dritte verkauft. American Express gab in einer Presseerklärung offen zu, daß das Geschäft der Zukunft nicht mit den Kreditkarten sondern durch den Handel mit Käuferprofilen gemacht wird[161].

Nach den seit etwa einem Jahr gültigen Tele- und Medienvorschriften dürfen Nutzungsprofile nur anonym, d.h. ohne Rückschluß auf eine Person erstellt werden. Die Verwendung solcher Profile kann auf sehr unterschiedliche Arten erfolgen. Zum einen ist somit ein sehr zielgenaues Marketing möglich, indem potentielle Kunden direkt erreicht werden, zum anderen können aber auch Risiken ausgeschlossen werden, d.h. bestimmte Personenkreise werden gezielt als Geschäftspartner oder Kunden ausgeschlossen.

Bei der deutschen Geldkarte kann der Kunde zumindest dem Händler gegenüber anonym bleiben, da dieser nur die Geldkartennummer erfährt. Bekommt der Kunde Zweifel an der Richtigkeit der letzten Transaktionen, so kann er die Logdatei der Karte mit Informationen über die letzten drei Ladevorgänge und die letzten fünfzehn Zahlungen an einem Sonderfunktionsterminal ausdrucken lassen. Selbst bei einem Hardware-Defekt der Karte mit Restgutha-

[161] Vgl. GROTE (Profit, 1998), S. 108.

ben ist über das Schattenkonto bei der Evidenzzentrale eine Rekonstruktion möglich. Hier werden die Kartennummer und der verfügbare Betrag gespeichert, nicht jedoch die Historie, wie dieser zustande gekommen ist. Die Evidenzzentrale alleine könnte also kein Kundenprofil erstellen. Eine Reklamationsbearbeitung und somit Aufhebung der Anonymität ist nur per Unterschrift möglich[162]. Die Geldkarte ist somit entgegen den Beteuerungen des ZKA nicht als völlig anonym einzustufen, da die personenbezogenen Daten mit den Zahlungsdaten des Börsenverrechnungskontos bei der Evidenzzentrale gespeichert werden. Lediglich sogenannte *„White Cards"*, Geldkarten die nicht in die EC-Karte des Kunden integriert sind, bieten hier absolute Anonymität.

Gesellschaftliche Auswirkungen lassen sich durch die Verwendung von elektronischem Geld bereits feststellen. Kreditkarten stehen in den USA mittlerweile für Seriosität und Kreditwürdigkeit. Eine Barzahlung ist somit schon fast verdächtig. Auch in Deutschland lassen sich Tendenzen diesbezüglich feststellen. Allein die Existenz von SmartCards, digitalem Geld oder Cyber Money wird die Gesellschaft nicht verändern. Erst die Art und Weise, wie die Systeme letztendlich verwendet werden, hat gesellschaftliche Auswirkungen[163]. Mit zunehmendem Einsatz von elektronischem Geld werden zwangsweise auch immer mehr Daten produziert. Die Gefahr, daß diese trotz Datenschutz und Bürgerrechte verglichen, verkauft und für Fahndungszwecke verwendet werden, ist groß. Bereits heute ist Datenschutz und informationelle Selbstbestimmung nicht selbstverständlich[164].

[162] Vgl. BEYKIRCH (Chipgeld, 1998), S. 151.
[163] Vgl. GROTE (Gar nicht smart, 1998), S. 111-113.
[164] Vgl. KOLLMANN (Elektronisches Geld, 1998), S. 23.

Ausblick

Der Durchbruch zu einem auf breiter Basis angelegten Online-Handel mit sicheren und standardisierten Zahlungssystemen im Internet ist noch nicht geschafft. Es scheint, als ob Electronic Commerce sozusagen ein „Henne-Ei-Problem“ darstellt: Erst wenn ein allen Anforderungen genügendes Zahlungssystem vorhanden ist, werden genügend Anwender für eine attraktive Nachfrage im Internet vorhanden sein. Umgekehrt kann sich ein solches Zahlungssystem erst entwickeln, wenn eine ausreichende Zahl von Kunden und Händlern bereit ist, Zeit und Geld in den Aufbau eines solchen Systems zu investieren.

In der nun angebrochenen Übergangszeit der Währungsunion bis zur endgültigen Einführung des Euro im Jahre 2002 könnten elektronische Zahlungssysteme durch den Mangel an echten Euro-Münzen und Scheinen einen unverhofften Schub erleben. Somit kann die Währungsunion eine gute Chance für eine stärkere Verbreitung von digitalem Geld werden, da lediglich elektronische Formen des Euro zur Verfügung stehen.

Die meisten der in dieser Arbeit vorgestellten Verfahren sind über einen Testlauf bzw. einen Pilotversuch nicht hinausgekommen. Keines der vorgestellten Zahlungssysteme wird jedoch dem Anspruch, den der Begriff Cyber Money impliziert, gerecht. Echtes elektronisches Geld mit Wertaufbewahrungs- und allgemeinen Zahlungsmittelfunktionen, die per Internet von Benutzer zu Benutzer wandern können und akzeptiert werden, gibt es bisher nur in Ansätzen. Viel mehr als eine einmalige Übertragung von Kaufkraft an wenige ausgewählte Subjekte ist nicht möglich. Zum einen scheitert die Entwicklung anspruchsvollerer Systeme an unterschiedlichen Interessen der Wettbewerber, zum anderen setzen auch Sicherheit und technische Machbarkeit Grenzen.

Die Zeitspanne bis zu einer breiten Nutzung virtuellen Geldes als Ersatz für Bargeld reicht somit von 5 bis 7 Jahren für SmartCard-Systeme bis zu über 50 Jahre für ausschließlich elektronische Zahlungssysteme. Trotz der Verwendung aktuellster Literatur und verschiedener anderer Quellen mit hoher Aktualität ist eine aussagekräftige Einschätzung der Entwicklung im Bereich der digitalen Zahlungsmittel für das Internet kaum abzusehen.

Literaturverzeichnis

AMBROS, H. (Virtual, 1995):

Virtual reality – virtual banking, Wien 1995.

BECKER, C. (Ohne Webseite, 1998):

Ohne Webseite ist ein Unternehmen tot, in: VDI Nachrichten, Nr. 34 vom 21. 08.1998, S. 19.

BECKER, L.(Secure Commerce, 1998):

Secure Commerce & Communication – Die kommerzielle Vision des Internet, in: Internet Banking – Der Bankbetrieb im Umbruch; LANGE, T. A. (Hrsg.), Wiesbaden 1998, S. 205-226.

BERENTSEN, A. (Digitales Geld, 1998):

Digitales Geld, Geldmenge und Geldpolitik, in: BRILL, A. / VRIES, M. DE (HRSG.): Virtuelle Wirtschaft: virtuelle Unternehmen, virtuelle Produkte, virtuelles Geld und virtuelle Kommunikation, Opladen/Wiesbaden 1998, S. 251-264.

BERENTSEN, A. (Digital Money, 1998):

Digital Money, Liquidity and Monetary Policy, Arbeitspapier der University of California, Berkley und der Universität Bern, in: Kyklos, Nr. 51/98, S. 89-117.

BERNDT, H. (Elektronisches Geld, 1995):

Elektronisches Geld – Geld der Zukunft?, in: Sparkasse, Nr. 8/95, S. 369-372.

BEYKIRCH, H.-B. (Chipgeld, 1998):

Chipgeld – Wie die Geldkarte funktioniert, in: iX – Magazin für professionelle Informationstechnik, Nr. 12/98, S. 148-151.

BIBOW, J. / WICHMANN, T. (Elektronisches GELD, 1998):

Elektronisches Geld: Funktionsweise und wirtschaftspolitische Konsequenzen, aus: Beiträge aus dem Institut für Statistik und Ökonometrie der Universität Hamburg, Nr. 19/98.

BIRKELBACH, J. (Cyber Finance 1997):

Cyber Finance – Finanzgeschäfte im Internet, Wiesbaden 1997, S. 35-52 und S. 117-128.

BÖHLE, K. / RIEHM, U. (Bezahlen, 1997):

Bezahlen im Internet – sechs Einführungen konkurrieren um Lesergunst, in: VDI Nachrichten, Nr. 8 vom 20.2.1998, S. 32.

BÖHLE, K. / RIEHM, U. (HRSG.) (EZI-N, 1998):
EZI-N Elektronische Zahlungssysteme im Internet – Newsletter, URL: http://www.itas.fzk.de/deu/PROJEKT/Pez/ezin***.htm.

BORCHERT, M. (Cyber Money, 1996):
Cyber Money – eine neue Währung, in: Sparkasse, Nr. 1/96, S. 41-43.

BRUER, A. (Revolution, 1998):
Revolution des Finanzgeschäfts, Stuttgart 1998, S. 24-59.

BÜRKEL, W. (Chancen, 1998):
Chancen des Internet, in: Die Bank, Nr. 5/98, S. 327.

BÜHL, A. (Cyber Money, 1998):
Cyber Money oder die Verflüchtigung des Geldes, in: BRILL, A. / VRIES, M. DE (Hrsg.): Virtuelle Wirtschaft: virtuelle Unternehmen, virtuelle Produkte, virtuelles Geld und virtuelle Kommunikation, Opladen/Wiesbaden 1998, S. 224-240.

BÜSCHGEN, H. E. (Bankbetriebslehre, 1998):
Bankbetriebslehre, Bankgeschäfte und Bankmanagement, 5. Aufl., Wiesbaden 1998, S. 428-439.

BUNDESMINISTERIUM DER JUSTIZ (Bekanntmachung, 1998):
Bekanntmachung zur digitalen Signatur nach dem Signaturgesetz und der Signaturverordnung, vom 14. September 1998, in: Bundesanzeiger, Nr. 204a/98.

CREDE, A. (Electronic commerce, 1998):
Electronic commerce and the banking industry: the requirement and opportunities for new payment systems using the internet, URL: http://wwwjcmc.huji.ac.il/vol1/issue3/crede.htm

DRESEN, S. (Abgewogen, 1998):
Abgewogen – ecash, Cybercash und Millicent im Vergleich, in: iX – Magazin für professionelle Informationstechnik, Nr. 5/98, S. 96-98.

DRESEN, S. / DUNNE, T. (Fürs Netz, 1998):
Fürs Netz geprägt – wie Cyber Cash funktioniert, in: iX – Magazin für professionelle Informationstechnik, Nr. 4/98, S. 110-116.

ERLINGHEUSER, B. (Virtuelle Schalterhalle, 1998):
Virtuelle Schalterhalle – Die Bank von morgen, in: LANGE, T. A. (Hrsg.): Internet Banking – Der Bankbetrieb im Umbruch, Wiesbaden 1998, S. 35-58.

EUROPÄISCHE ZENTRALBANK (Bericht, 1998):

Bericht über elektronisches Geld, übersetzt durch die Deutsche Bundesbank, August 1998.

FASTENRATH, B. / REINERS, T. / WABNITZ, S.-H. (Smart, 1998):

Smart is beautiful – Standard, Java und mehr, in: iX – Magazin für professionelle Informationstechnik, Nr. 9/98, S. 42-47.

FINDEISEN, M. (Elektronisches Geld, 1998):

Elektronisches Geld ist attraktiv für Geldwäscher, in: Bank Magazin, Nr. 2/98, S. 48-49.

FLIEGE, C. (Anonymer Zahlungsverkehr, 1998):

Anonymer Zahlungsverkehr mit elektronischem Geld, in: Computer und Recht, Nr. 1/98, S. 41-46.

FRIEDRICH, H.-J. (Elektronisches, 1997):

Elektronisches Karten- und Netzgeld (E-Geld) aus der Sicht einer Notenbank, Vortrag auf der I.I.R. Konferenz „Zahlungssysteme im Umbruch“, Frankfurt 1997.

FROITZHEIM, U. (Digitales Geld, 1998):

Digitales Geld – letzter Schliff, in: Wirtschaftswoche, Nr. 15/98, S. 98-100.

GLADIS, R. (Krötenwanderung, 1998):

Krötenwanderung – EBusiness mit Geldkarten, in: c´t special 98, Geld online 3, S. 128-130.

GOLL, M. (Digitales Geld, 1998):

Digitales Geld auf dem Weg zum allgemein gültigen Zahlungsmittel?, in: Connection Newsflash, März 98.

GOTTA, F. (Cyber Money, 1996):

Cyber Money – die Währung im Internet, in: Die Welt vom 18.01.1996, S.3.

GRAMLICH, L (Elektronisches Geld, 1997):

Elektronisches Geld – Gefahr für Geldpolitik und Währungshoheit?, in: Computer und Recht, Nr. 1/97, S. 11-18.

GROTE, A. (Gar nicht smart, 1998):

Gar nicht smart – bringen Chipkarten die schöne neue Welt?, in: c´t special 98, Geld online 3, S. 111-113.

GROTE, A. (Profit, 1998):

Profit durch Profile – Online-Anbieter werten personenbezogene Daten ihrer Kunden aus, in: c´t special 98, Geld online 3, S. 107-11.

HAHN, H.J. (Währungsrecht, 1990):

Währungsrecht, München 1990.

HAGEN, J. U., ZAGLER, H. (Sicherer Zahlungsverkehr, 1998):

Sicherer Zahlungsverkehr im Elctronic Commerce, in: Die Bank, Nr. 4/98, S. 217-219.

HARTMANN, M. (Ein Modell, 1997):

Ein Modell zu wirksamen Kontrolle von elektronischem Geld im Internet (Cyber Money), in: Sparkasse, Nr. 10/97, S. 475-478.

HARTMANN, W. (Die Europäische, 1997):

Die Europäische Integration im Zahlungsverkehr aus Sicht der Deutschen Bundesbank, in: Zeitschrift für das gesamte Kreditwesen, Nr. 13/97, S. 639-641.

HIMMELSPACH, A. / RUNGE, A. / SCHUBERT, P. / ZIMMERMANN, H.-D. (Analyse, 1996):

Analyse und Bewertung von elektronischen Zahlungssystemen, Bericht Nr.: BusinessMedia/52, Version 1.0 10/96, Universität St. Gallen.

HIRT, M. (Electronic, 1997):

Electronic Payments-Systems im Internet: ein neues Geschäftsfeld für Banken, Publikation der Swiss Banking School Nr. 157, Bern 1997.

JAHN, T. (Geld, 1995):

Geld ist alles was gilt, in: die Zeit, 1.12.1995, Nr. 49, Wirtschaft, S. 24.

IGLER, M. (Mit virtuellem Geld, 1998):

Mit virtuellem Geld einkaufen, in: Management Berater, Januar 1998, S. 54-55.

ISSING, O. (Geldpolitische Bedeutung, 1997):

Die geldpolitische Bedeutung des Zahlungsverkehrs, in: Zeitschrift für das gesamte Kreditwesen, Nr. 13/97, S. 617-621.

KLEIN, S. (Cyber Money, 1997):

Cyber Money ohne Bankenlobby, in: Jahrbuch der Telekommunikation und Gesellschaft – die Ware Information, Heidelberg 1997, S.203-210.

KOLLMANN, K. (Elektronisches Geld, 1998):

Elektronisches Geld und Verbraucher – Themen und Schwerpunkte einer deutschen Konferenz über Sicherheit bei den elektronischen Zahlungsformen, in: Arbeit & Wirtschaft, Nr. 4/98, S. 22-23.

KOSSEL, A. / WRONSKI H.-J. (Bare Bytes, 1997):
Bare Bytes – online bezahlen im Internet, in: c´t, Nr. 16/97, S. 66-69.

KRAUSE, J. (Electronic Commerce, 1998):
Electronic Commerce – Geschäftsfelder der Zukunft heute nutzen, München 1998.

KRISTOFERITSCH, G. (Digital Money, 1998):
Digital Money - Electronic Cash - Smart Cards: Chancen und Risiken des Zahlungsverkehrs via Internet, Wien 1998.

KÖHLER, T. (Electronic Commerce, 1998):
Electronic Commerce: Elektronischer Handel in der Praxis, Bonn 1998.

KRÖNIG, J. (Abschied, 1998).:
Abschied vom Portemonnaie, in: die Zeit, 1.12.95, Nr. 49, Wirtschaft.

LANGE, T. A. (Internet Banking, 1998):
Internet Banking – Eine Potentialanalyse, in: LANGE, T. A. (Hrsg.): Internet Banking – Der Bankbetrieb im Umbruch, Wiesbaden 1998, S. 15-34.

LUKAS, S. (Cyber Money, 1997):
Cyber Money: Künstliches Geld im Internet und elektronische Geldbörsen, Berlin 1997.

LÜTGE, G. (Viele Bits, 1997):
Viele Bits für eine Mark, in: die Zeit, 12.12.1997, Nr. 51, Wirtschaft, S. 22-23.

LYNCH, D. C., LUNDQUIST, L. (Zahlungsverkehr, 1997):
Zahlungsverkehr im Internet, München/Wien 1997.

MEISTER, E. (Cyber Geld, 1996):
Cyber Geld, Prepaid-Card und Euro – Konsequenzen für den Geld- und Werttransport, Rede auf der Jahresmitgliederversammlung der Bundesvereinigung Deutscher Geld- und Werttransportunternehmen, 28.11.1996, Frankfurt am Main.

MÖKER, U. (Elektronisches Geld, 1998):
Elektronisches Geld aus Sicht einer Zentralbank, in: LANGE, T. A. (Hrsg.): Internet Banking – Bankbetrieb im Umbruch, Wiesbaden 1998, S. 173-202.

MÜLLER, M. (Dämon Cybermoney, 1995):
Dämon Cybermoney, in: die Zeit, 1.12.95, Nr. 49, Wirtschaft.

O.V.:

Cyber Cash – sicheres Bezahlen im Internet, URL: http://www.dresdner-bank.de/f_firmen/b_office/c_cash/fbca_all.htm.

O.V.:

Die EZB fordert eine Mindestreserve für elektronische Geld, in: FAZ, 1.9.1998, Nr. 202/98, S. 19.

O.V.:

Geldpolitische Auswirkungen des „digitalen Geldes“, URL: http://www.home.t-online.de/home/06995530471-0001/ausw.htm.

O.V.:

Verbraucher wollen mehr Sicherheit beim digitalen Geld; Studie von inTouch, URL: http://www.intouch.de/download/pi_studie.htm.

PADOVAN, B. / BUSSIEK, T. (Grenzenloses Wirtschaften, 1998):

Grenzenloses Wirtschaften in offenen Netzwerken: Neue Anforderungen an den Wertaustausch, in: BRILL, A. / VRIES, M. DE (Hrsg.): Virtuelle Wirtschaft: virtuelle Unternehmen, virtuelle Produkte, virtuelles Geld und virtuelle Kommunikation, Opladen/Wiesbaden 1998, S. 241-250.

PERNUL, G. / RÖHM, A. W. (Neuer Markt, 1997):

Neuer Markt – neues Geld?, in: Wirtschaftsinformatik, Nr. 39, 4/97, S. 345-355.

POLYSIUS, K. U. (Der Point of Sale, 1998):

Der Point of Sale im Internet: Cybercash als deutscher Standard?, in: cards Karten cartes, Nr. 1/98, S. 31-34.

POWELL-JONES, O. (Mondex, 1998):

Mondex hat keine Akzeptanzprobleme, in: cards Karten cartes, Nr. 4/98, S. 27-29.

RADETZKY, G. VON (Mondex, 1998):

Kleingeld im Internet – Abwicklung von Geschäften unter 5 DM, in: is report, Nr. 6/98, S. 16-17.

RADETZKY, G. VON (Kleingeld, 1998):

Kleingeld im Internet – Bezahlung mit Chiffre oder Chip, in: Datenverarbeitung, Steuer, Wirtschaft, Recht (DSWR), 3/98, S. 58-60.

RAPP, A. (Tendenzen, 1998):
Tendenzen und Visionen im Internetbanking, in: Bank und Markt, Nr. 3/98, S. 10-15.

REICH, T. (Ecash, 1998):
Ecash: Zahlungsmittel im Internet?, in: JurPC, Internet-Zeitschrift für Rechtsinformatik, URL: http://www.jura.uni-sb.de/jurpc/aufsatz/19970035.htm, 1997.

RIEKEBERG, M. (Geldkarte, 1998):
Geldkarte aus Verbrauchersicht unbrauchbar?, in: cards Karten cartes, Nr. 4/98, S. 33-37.

SCHAAL, P. (Geldtheorie, 1998):
Geldtheorie und Geldpolitik, 4. überarb. Und erw. Aufl., München 1998.

SCHIERENBECK, H. / HÖLSCHER, R. (BankAssurance, 1998):
BankAssurance, Institutionelle Grundlagen der Bank- und Versicherungsbetriebslehre, 4. Auflage, Stuttgart 1998.

SCHODER, D. / STRAUSS, R. E. (Electronic Commerce, 1997):
Electronic Commerce, in: BROßMANN, M. / FLIEGER, U. (Hrsg.): Business Multimedia: Innovative Geschäftsfelder strategisch nutzen, Wiesbaden 1997, S. 51-65.

SCHMEH, K. (Cyber Zaster, 1996):
Cyber Zaster – Ohne Moos nix los, in: Pl@net – das Internetmagazin, Nr. 8/96, S. 38-40.

SCHUMANN, M. / ROSENTHAL, F. (So gut wie Bargeld, 1997):
So gut wie Bargeld – Zahlungsmodelle für Geldtransaktionen in Online-Netzen, in: Geldinstitute, Nr. 6/97, S. 46-51.

SCHUSTER, R. / FÄRBER, J. / EBERL, M. (Digital Cash, 1997):
Digital Cash: Zahlungssysteme im Internet, München 1997.

SEIPP, P. (Shopping, 1998):
Shopping ohne Grenzen – wie man auch im Internet sicher zahlen kann, in: Geldinstitute, Nr. 4-5/98, S. 46-47.

SIETMANN, R. (Electronic Cash, 1997):
Electronic Cash: Der Zahlungsverkehr im Internet, Stuttgart 1997.

SÖLLNER, F. / WILFERT, A. (Elektronisches Geld, 1996):
Elektronisches Geld und Geldpolitik, in: List Forum für Wirtschafts- und Finanzpolitik 22, Nr. 3/96, S. 389-405.

STEIN, M. (Homebanking, 1998):
Homebanking mit HBCI: Wo sind die Einsatzgebiete, in: bank und markt, Nr. 11/98, S. 39-43.

STEINAU, H. / SCHNEIDER, M. / WIDRAT, S. (Electronic Commerce, 1998):
Electronic Commerce – Wie sich im Internet doch Geld verdienen läßt, in: Impulse, Nr. 3/98, S. 54-64.

STOCKMANN, C. (Die virtuelle Bank, 1998):
Die virtuelle Bank: Eine Begriffsklärung, in: Wirtschaftsinformatik, Nr. 40, 4/98, S. 273-280.

STOCKMANN, C. (Elektronische Bankfilialen, 1997):
Elektronische Bankfilialen und virtuelle Banken: Das Privatkundengeschäft von Universalbanken im elektronischen Markt, Diss., wirtschaftswissenschaftliche Fakultät der Universität Regensburg, 1997.

STOLPMANN, M. (Elektronisches Geld, 1997):
Elektronisches Geld im Internet – Grundlagen, Konzepte, Perspektiven, Köln 1997.

THIESSEN, F. (Elektronische Zahlungsmittel, 1998):
Elektronische Zahlungsmittel im Vormarsch, in: Zahlungsverkehr, Beiblatt Nr. 5/98, S. 217-222.

THOME, R. (Elektronischer Marktplatz, 1998):
Elektronischer Marktplatz: Wer dort nicht anbietet, wird nicht mehr gefunden, in: bank und markt, Nr. 9/98, S. 31-38.

THOME, R. / SCHINZER, H. (Electronic Commerce, 1997):
Electronic Commerce – Anwendungsbereiche und Potentiale der digitalen Geschäftsabwicklung, München 1997.

VAK, K. (Unterwegs, 1995):
Unterwegs zum abstrakten Symbolsystem Geld, in: BOLLMANN, S. (Hrsg.): Kursbuch neue Medien, Mannheim 1995, S. 301-310.

VITT, A. (Zukunftsvision, 1997):
Zukunftsvision Cybergeld: Finanzdienste und ihre Erfahrung, in: MÜNKER, S. / ROESLER, A. (Hrsg.): Mythos Internet, Frankfurt 1997, S. 236-247.

WALTER, M. (Zukunftsvision, 1997):
Von der Mikrotransaktion zur Smart Card, in: Finanzen für Unternehmen und Unternehmer, Nr. 11/98, S. 14-15.

WANKE, A. (Sachsen LB, 1998):

Sachsen LB CyberCash – die neue Dimension des Geldes, in: Der langfristige Kredit, Nr. 5/98, S. 184-185.

WASMEIER, M. (Cash auf Draht, 1998):

Cash auf Draht – Elektronisches Geld und andere Online-Bezahlungsverfahren, in: c´t special 98, Geld online 3, S. 96-101.

WEISS, M. (Virtuelle Bank, 1998):

Virtuelle Bank – Zeitgeistphänomen oder Geschäftsfeld der Zukunft?, in: Zeitschrift für das gesamte Kreditwesen, Nr. 8/98, S. 427-429.

WEISSHUHN, A. (Digitale Zahlungsverfahren, 1998):

Digitale Zahlungsverfahren im Internet, in Lange, T. A. (Hrsg.): Internet Banking – Der Bankbetrieb im Umbruch, Wiesbaden 1998, S. 131-154.

WRIGHTSON, G. / FURCHE, A. (Central Bank, 1997):

Central Bank Control of Computer Money, in Hipp, C. (Hrsg.): Geld, Finanzen, Banken und Versicherungen, Karlsruhe 1997, S. 341-349.

ZERDICK, A. / PICOT, A. / SCHRAPE, K. (HRSG.) (Internet-Ökonomie, 1999):

Die Internet-Ökonomie – Strategien für die digitale Wirtschaft, Berlin / Heidelberg 1999.

ZIESCHANG, T. (Fisch und Chips, 1998):

Fisch und Chips – Wie sicher sind SmartCards?, in: iX – Magazin für professionelle Informationstechnik, Nr. 9/98, S. 48-52.

Glossar

Applet: Programmdatei, die vom Webserver auf Anforderung zum Browser gesendet wird und im PC des Nutzers bestimmte Aktionen ausführt.

Arpanet: Im Auftrag der Arpa (Advanced Research Projects Agency) entwickeltes militärisches Kommunikationsnetz. Basierend auf einem Rechnerverbund mit Vermittlungsknoten, somit Vorgänger des heutigen Internets.

Asymmetrische Verschlüsselung: Kryptographisches Verfahren unter Verwendung eines Schlüsselpaares. Nachrichten, die mit dem einen Schlüssel kodiert werden, können nur mit dem dazugehörigen zweiten Schlüssel dekodiert werden.

Backbone: Elektronische Hauptverkehrsader eines Kommunikationsnetzwerkes. Bietet sehr schnelle Verbindungen bei großer Kapazität.

Browser: Navigationssoftware zur Darstellung von Webseiten. Der NCSA Mosaic war der erste graphische Web-Browser; Netscape Navigator und Microsoft Internet Explorer sind heute am weitesten verbreitet.

Chipkarte: Plastikkarte im Scheckkartenformat, auf der ein fingernagelgroßer Chip integriert ist. Speichermedium für Daten und digitales Geld.

DES: Data Encryption Standard. Der am häufigsten verwendete internationale Standard für symmetrische Verschlüsselung mit fester Schlüssellänge von 56 Bit.

DNS: Domaine Name System. System, das die Adresse eins Computers in eine Form von vier Zahlen übersetzt, die durch Punkte (dots) getrennt sind.

Domain: Bereich, zu dem ein Computer gehört.

Encryption: Codierung von Daten, so daß nur ein Empfänger, der einen Codeschlüssel hat, die Daten lesen kann.

Geldsurrogate: Geldsubstitute, near monies oder geldnahe Titel, Qualität hängt von Akzeptanz, Liquidierungsgrad, Risiko und Verzinsung ab.

Hash-Funktion: Sehr rechenintensives Verschlüsselungsverfahren. Die Hash-Funktion erzeugt eine Prüfsumme fester Länge, welche digital unterschrieben und an die Nachricht angehängt wird. Der Empfänger wendet die gleiche Funktion an und vergleicht das Ergebnis.

HBCI-Standard: Home Banking Computer Interface-Standard, einheitliche Schnittstelle zwischen Bankrechner, Chipkarten und Heim-PCs.

Homepage: Erste Seite eines Angebots im WWW, Ausgangspunkt für weitere Seiten und Verzweigungen.

Host: Bezeichnung für einen an ein Computernetzwerk angeschlossenen Rechner.

http: Hyper Text Transfer Protocoll, Standard zur Übertragung von WWW-Seiten.

Hyperlink: Verweis von einer Stelle in einem HTML-Dokument auf eine andere Stelle im selben oder in einem anderen Dokument.

IP-Nummer: Adresse eines Computers im Internet.

JAVA: Programmiersprache, die sich aufgrund ihrer unabhängigen Konzeption für eine Fülle von Anwendungen eignet, insbesondere für Anwendungen des WWW.

Kerberos: Autorisierungsalgorithmus zur Identifizierung beider Parteien bei elektronischen Übertragungen. Entwickelt vom Massachusetts Institute of Technology (MIT).

Plug-in: Programm, das wie ein Baustein an ein anderes angefügt werden kann und diesem neue Funktionen, wie z.B. Filmwiedergabe, zugänglich macht.

Protocol: Regelwerk für die Übermittlung von Daten in einem Netzwerk. Z.B.: TCP/IP oder HTTP.

Provider: Anbieter, der einen Zugang zum Internet verschafft und auch Inhalte auf eigenen Webservern darstellt.

RSA: Rivest, Shamir, Adleman. Beliebtester asymmetrischer Verschlüsselungsalgorithmus, nach den drei Entwicklern benannt.

SSL: Secure Socket Layer. Verschlüsselungsverfahren, das in den USA einen Verschlüsselungsgrad von 128 Bit erreicht, aber einem von der NSA durchgesetzen Exportverbot unterliegt. Freigegeben ist nur eine 40 Bit Variante.

TAN: Transaktionsnummer. Absicherungstechnik, die heute im Home Banking allgemein verbreitet ist.

Webserver: Computer, der auf Anforderung eines Browsers Daten ins Internet verendet

Bisher in dieser Reihe erschienen:

Band 1: *Hölscher, Reinhold / Kremers, Markus / Rücker, Uwe-Christian:*
Industrieversicherungen als Element des modernen Risikomanagements, Ergebnisse einer empirischen Untersuchung, 1996

Band 2: *Hölscher, Reinhold / Rücker, Uwe-Christian / Heller, Alexander / Strohhecker, Marcus:*
Wirtschaftlichkeitsanalysen zu aeroben und anaeroben Verfahren bei der Abwasserreinigung in der Weinwirtschaft, 1996

Band 3: *Hölscher, Reinhold:*
Bankbetriebliche Marktpreisrisiken im Grundsatz I, 1998

Band 4: *Dreher, Stefan:*
Cyber Money, Entwicklungstendenzen und Abwicklungstechniken im Internet, 1999

Die Studien zum Finanz-, Bank- und Versicherungsmanagement können unter folgender Adresse bezogen werden:

Technische Universität Kaiserslautern
Lehrstuhl für Finanzdienstleistungen und Finanzmanagement
Postfach 3049
67653 Kaiserslautern

Telefon: 0631 / 205-4109
Telefax: 0631 / 205-3621

E-Mail: lff@wiwi.uni-kl.de
URL: http://lff.wiwi.uni-kl.de