Elektronische Zahlungssysteme mit Schwerpunkt Digitales Geld

Seminar Sommersemester 2004

Seminararbeit im Studiengang Wirtschaftsmathematik
vorgelegt am: 09.07.2004
von: Marcus Rapp
Matrikelnummer: 426866

Abteilung Angewandte Informationsverarbeitung (SAI)
Prof. Dr. F. Schweiggert

Inhaltsverzeichnis

Abkürzungsverzeichnis

bzw.	beziehungsweise
d. h.	das heißt
i. Allg.	im Allgemeinen
sog.	so genannt
u. a.	unter anderem
z. B.	zum Beispiel
evtl.	eventuell
s.	siehe
o.ä.	oder ähnliches

1 Einführung

In den letzten Jahren hat sich das Internet von seiner hauptsächlichen Verwendung als Informationsbörse und Werbeträger weiter entwickelt zu einem virtuellen Marktplatz, der es Anbietern und Kunden erlaubt, Waren digital auszutauschen. Eines der wichtigsten Probleme stellt dabei das Fehlen von adäquaten Zahlungssystemen dar. In den letzten Jahren boten Softwarehersteller, Dienstleister und Banken in mehreren Pilotprojekten unterschiedliche digitale Zahlungssysteme an, die allerdings auf Grund geringer Akzeptanz wieder eingestellt wurden. Dabei waren einige dieser Systeme bereits sehr weit entwickelt, vor allem die später in dieser Arbeit noch näher behandelten elektronischen Münzen der niederländischen Firma DigiCash, das mit eigenem Protokoll und spezieller Software dem Kunden digitale Münzen auf der Festplatte zur Verfügung stellte.
Bei diesen Systemen handelt es sich in erster Linie um Ansätze, mit denen vor allem größere Zahlungen kostendeckend abgewickelt werden konnten, sog. Macropayments. Da das Internet aber wie oben erwähnt auch als Informationsbörse genutzt wird, wir auch immer mehr nach Möglichkeiten gesucht, um die Behandlung von Kleinstbeträge, sog. Micropayments, effizient zu gestalten. Bei diesen Micropaymentsystemen (z.B. für einen Zeitungsartikel, einen einzelnen Aktienkurs o.ä.) handelt es sich im Allgemeinen um Beträge, die im Cent-Bereich liegen.
Um sich ein Bild von den Anforderungen an ein digitales Münzsystem im Internet machen zu können, sollte man jedoch zunächst einmal einige grundlegenden Eigenschaften des Mediums Internet analysieren.
Das Internet ist ein unsicheres Computernetz, das es ermöglicht, den Datenverkehr abzuhören, was vor allem dann gefährlich wird, wenn es sich um sensible Daten wie z.B. Kreditkartennummern handelt. Allerdings lassen sich durch den Einsatz von kryptographischen Protokollen wie z.B. SSL[1] oder SET[2] Zahlungen über das Internet ohne größere Sicherheitsrisiken durchführen, womit jedoch die Problematik der fehlenden Anonymität beim Bezahlvorgang - eines der Hauptkriterien für ein elektronisches Münzsystem - nicht gelöst wird. Außerdem besteht über das Internet die Möglichkeit, eine fremden Identität anzunehmen, ohne dass der Kommunikationspartner dies merkt. Dies mag an einigen Stellen des Internets von eher geringer Problematik sein, wie z.B. in Chatrooms oder Newsgroups, bei Bezahlvorgängen aber ist die Gewährleistung von Authentizität absolut unverzichtbar.
In dieser Seminararbeit wird zunächst ein Überblick über verschiedene Zahlungssysteme gegeben, wobei auch Ansätze erwähnt werden, die sich in der Praxis nicht durchgesetzt haben. Das zweite Kapitel geht dann speziell auf elektronsiche Münzsysteme ein, erörtert die Anforderungen an ein solches System und deren jeweilige Umsetzung und führt kurz

[1] Secure Socket Layer

[2] Secure Electronic Transactions

in die Problematik von Wechselgeld bei derartigen Systemen ein. Den Abschluss dieses Kapitels bildet dann die Vorstellung des Micropayment Systems eCash der Firma DigiCash.

2 Überblick Zahlungssysteme

Elektronische Zahlungssysteme lassen sich ganz allgemein in die Gruppen Macro- und Micropayment unterteilen, wobei die Zuordnung eines Zahlungssystems zu einer dieser beiden Gruppen abhängig ist vom jeweiligen Zahlungsumfang. Zahlungen bis maximal 5 Euro werden für gewöhnlich zu Micropayment, alles darüber zu Macropayment gerechnet. Im Folgenden werden nun die wichtigsten Systeme dieser beiden Gruppen kurz vorgestellt, wobei als Grundlage dieses Kapitels „die Einführung in Zahlungssysteme“ der Abteilung Informationswissenschaft der Universität Konstanz gedient hat.[3]

2.1 Macropayment

2.1.1 Kreditkartensysteme

Die Kreditkarte ist im Internet das noch immer am häufigsten benutzte Zahlungsmittel. Diesen Umstand hat sie natürlich der weiten Verbreitung der Karten selbst, aber auch der einfachen Integrierbarkeit in Internetshops zu verdanken. Dabei wird mit SET ein Protokoll verwendet, das sichere Transaktionen beim Bezahlen mit Karten über offene Netze gewährleistet. SET widmet sich ausschließlich dem Zahlungsvorgang selbst und nicht dem gesamten Einkaufvorgang vom Füllen des Warenkorbs bis zur Lieferung der Waren. Hierbei übertragene Daten müssen gesondert abgesichert werden. SET ist ein offener technischer Standard, der von Visa und MasterCard 1996 mit den folgenden Zielen ins Leben gerufen wurde:

1. Sicherheit bei Zahlungen
   Bei der Sicherheit wurde Wert auf Vertraulichkeit und Integrität von Bezahl- und Bestelldaten sowie die Authentifizierung von Kunden, Händler und Händlerbank gelegt.

2. Interoperabilität
   Interoperabilität soll durch eine offen Spezifikation erreicht werden, so dass Software unterschiedlichster Hersteller im globalen Markt interoperieren können.

[3] nachzulesen unter [UniKonstanz].

3. Akzeptanz am Markt
   Akzeptanz am Markt erhofft man sich durch leichte Implementierbarkeit des Protokolls, Effizienz sowie durch möglichst geringen Änderungsbedarf bei der Ausstattung von Kunden, Händler, Händlerbanken und deren Beziehungen untereinander.

Die Händler profitieren von der Eigenschaft, dass SET-Zahlungen garantiert sind und nicht, wie normale Kreditkartenzahlungen storniert werden können. Für Kunden ist besonders interessant, dass die Händler ihre Kreditkartennummer nicht erhalten und dass die Händler vor Erhalt eines SET-Zertifikats Kontrollen unterzogen werden. Leider ist der Integrationsaufwand in ein Shopsystem, im Vergleich zu einfachen Kreditkartenzahlungen, meist deutlich höher. Da die Kreditkartenzahlungen immer mit nicht zu vernachlässigenden Gebühren verbunden sind, lohnen sie sich jedoch erst ab einem bestimmten Betrag.

2.1.2 Elektronisches Geld

Herkömmliches Münzgeld unterscheidet sich von Kreditkarten in zwei wesentlichen Punkten: Zum einen ermöglicht es anonymes Bezahlen, zum anderen kann jeder die Echtheit von Münzgeld feststellen und nicht nur die Bank. Könnte man dies digital umsetzen, so würden sich die teueren Online-Verbindungen zur Bank erübrigen, da sich jeder Händler selbst von der Echtheit des Geldes überzeugen könnte.
Der auf Grund seiner sehr guten Sicherheitseigenschaften wohl vielversprechendste Vorschlag für ein elektronisches Münzsystem war *ECash* von der Firma Digicash, die von November 1997 bis Mai 2001 ein Pilotprojekt zusammen mit der Deutschen Bank durchgeführt hatte. *ECash* war eine internetspezifische Umsetzung des anonymen elektronischen Bargeld-Systems, das von D.Chaum entwickelt wurde. Auf Grund seiner sehr innovativen Implementierung wird auf dieses System inKapitel 2 noch näher eingegangen.
Als weiteres Beispiel für eine vollständige Implementierung eines elektronischen Münzsystems sei hier noch das System *Netcash* von der University of Southern California erwähnt, das jedoch verglichen mit *ECash* nur eine geringe Anonymität der Kunden gewährleisten konnte.
Welche weiteren Anforderungen an elektronische Münzsysteme gestellt werden, neben der bereits erwähnten Anonymität des Kunden und der Verifizierbarkeit der Münzen, wird in Kapitel 2 ausführlich erläutert.

2.2 Micropayment

In Kapitel 2.1 wurden Verfahren erläutert, die zum Handel ab einem bestimmten Geldbetrag über das Internet sehr gut geeignet sind. Auf Grund

ihrer relativ hohen Kosten eignen sie sich jedoch nicht für die Bezahlung kleinerer Beträge. Für das sog. Micropayment gibt es mehrere Ansätze, die alle die veränderten Anforderungen im Vergleich zu Macropayment-Systemen berücksichtigen. So kann wegen der nur geringen Geldbeträge auf einen Großteil der Sicherheitfunktionen verzichtet werden, was zum einen die fixen Transaktionskosten verringern hilft, d.h. eine billigere Abwicklung gewährleistet, und zum anderen durch den Verzicht auf eine Bonitätsprüfung Vorteile in Geschwindigkeit und Einfachheit mit sich bringt. Außerdem ist bei nur geringen Zahlungsbeträgen keine Preisgabe der Identität erwünscht, d.h. das Micropayment-System sollte Anonymität des Zahlungsverkehrs unterstützen. Im Folgenden werden nun zwei Systeme kurz vorgestellt.

2.2.1 Mobile Payment (Paybox)

Bei diesem System können Zahlungen per Mobiltelefon durchgeführt werden, wobei auch Privattransaktionen zwischen zwei Paybox-Benutzern möglich sind. Eine typische Paybox Transaktion verläuft nach folgendem Muster:

1. Kunde wählt Paybox an und gibt seine Mobilfunknummer an.
2. Server des Händlers übermittelt Daten zu Paybox-Server.
3. Paybox-Server ruft Kunden an und übermittelt Händler und Betrag.
4. Kunde bestätigt Zahlung mit 4-stelliger PIN.
5. Bei korrekter PIN meldet Paybox-Server dem Händler erfolgreiche Zahlung.

Die Vorteile dieses Systems sind zum einen die Sicherheit durch Benutzung des Mobiltelefons, der relativ große Kunden- bzw. Händlerkreis und die Möglichkeit, Zahlungen zwischen Mitgliedern durchzuführen.
Als Nachteile seien erwähnt, dass es derzeit nur deutsche Händler gibt, die Paybox unterstützen und die Notwendigkeit eines Mobiltelefons.[4]

2.2.2 Firstgate Click & Buy

Firstgate[5] Click & Buy hat sich nach nur vier Jahren deutschlandweit als marktführende Lösung im Bereich der einfachen Tarifierung und sicheren Abrechnung für Internet-Inhalte und -Services etabliert.
Auf Grund der einfachen Handhabung und der relativ hohen Sicherheit

[4]Für nähere Informationen s. [Paybox].

[5]Firstgate Internet AG wurde im Januar 2000 von Norbert Stangl gegründet.

bei gleichzeitiger geringer Kostenbelastung wird Click & Buy mittlerweile von ca. 2800 Anbietern als Internet-Payment-Lösung verwendet, darunter namhafte Anbieter wie Stiftung Warentest, Financial Times Deutschland, Börse Online, Deutsche Post, UNICEF u.a.
Um Click & Buy verwenden zu können, ist nur eine kurze Anmeldung auf der Internetseite von Firstgate durchzuführen. Beim Bezahlvorgang werden die gezahlten Beträge erst im Nachhinein vom Konto des Kunden abgebucht. Des weiteren kann der Kunde entscheiden, ob das Geld per Lastschriftverfahren oder per Kreditkarte abgebucht wird. Alle den Bezahlvorgang betreffenden Transaktionen werden in Zusammenarbeit mit der Deutschen Bank durchgeführt und erfolgen verschlüsselt, was ein hohes Sicherheitsniveau gewährleistet.[6]

3 Digitales Geld / Elektronische Münzsysteme

3.1 Einführung

Die Ausführungen in diesem Kapitel orientieren sich an [DuD5/2003] und an [Furche, Wrightson].
Prinzipiell sollen digitale Zahlungsmittel die gleichen Eigenschaften besitzen wie andere Zahlungsmittel auch. Allerdings wird ausschlielich durch den Austausch digitaler Daten bezahlt. Elektronisches Bargeld ist dabei als direktes Gegenstück zu konventionellen Münzen oder Papiergeld aufzufassen, es besteht aber aus einer Bitfolge, die in Form einer Datei auf der Festplatte gespeichert wird. Wie bei jeder Datei ist es auch hier möglich, diese zu kopieren, wobei die Kopie nicht vom Original zu unterscheiden ist. Beim Bezahlen mit elektronischen Münzen muss also sichergestellt werden, dass eine Bitfolge nur beim ersten Einreichen gültig ist und beim zweiten Mal als Fälschung erkannt und zurückgewiesen wird. Es ergeben sich folgende (ideale) Anforderungen und Eigenschaften an digitales Geld:

3.2 Allgemeine (Sicherheits-)Anforderungen / Eigenschaften

3.2.1 Verifizierbarkeit

Die Art der Verifizierbarkeit legt fest, mit welchem Verfahren überprüft werden kann, ob eine Zahlung durch den Kunden auch wirklich erfolgen kann. Damit soll verhindert werden, dass der Kunde z.B. mehrmals mit

[6] Für weitere Informationen s. [Firstgate].

derselben elektronischen Münze Einkäufe tätigt oder sein Konto nicht mehr gedeckt ist. Dabei wird unterschieden zwischen

- *Online*: Sobald der Kunde seine Zahlungsinformationen schickt, werden die elektronischen Münzen auf Gültigkeit überprüft. Erst danach bekommt der Kunde die bestellte Ware geliefert.
- *Offline*: Hierbei liefert der Händler zunächst die bestellte Ware an den Kunden. Erst anschließend wird dann versucht, den Kaufpreis einzulösen. Bei diesem Verfahren existiert für den Händler natürlich die Gefahr, kein Geld zu erhalten. Die Bezahlung mit einer elektronischen Münze geschieht hier - im Gegensatz zum Online-Verfahren - ohne Zuhilfenahme der Bank.
- *Outband*: Vertrauliche Zahlungsinformationen werden hier nicht über das Internet, sondern über den Postweg versendet. Dieses Verfahren wurde jedoch nur von First Virtual, einem Internet-Abrechnungssystem für Kreditkartenzahlungen angewandt.

3.2.2 Anonymität

Bei anonymen Zahlungssystemen muss ausgeschlossen sein, dass der Händler oder irgendeine andere dritte Instanz außer dem Kunden in der Lage ist, Zahlungen zuzuordnen. Dies kann mit Hilfe kryptographischer Methoden erreicht werden. Das am häufigsten verwendete Verfahren ist die von D. Chaum entwickelte *blinde Signatur*. Hierbei erhält der Signierer keinerlei Informationen darüber, welchen Datensatz er signiert hat und wie seine Signatur aussieht. Allerdings ist zu beachten, dass der Empfänger sich vor der Signatur auf den Inhalt des Datensatzes festzulegen hat, der im Nachhinein nicht mehr verändert werden kann. Dies hat zur Folge, dass es sich bei der blinden Signatur nicht um eine Blanko-Unterschrift handelt. Die blinde Signatur ist analog zu herkömmlichen Signaturen fälschungssicher, für jeden verifizierbar und kann nicht geleugnet werden.
Als Alternative zu blinden Signaturen bietet sich der Einsatz von *Zero-Knowledge-Protokolle* an. Hierbei übergibt der Kunde dem Händler nicht wie gewohnt eine digitale Münze, sondern überzeugt ihn statt dessen mit einem Zero-Knowledge-Protokoll davon, dass er eine digitale Münze besitzt. Dazu müssen nur soviel persönliche Informationen zusätzlich preisgegeben werden, damit ein evtl. Double-Spending nachträglich aufgedeckt werden kann. Der Vorteil dieser Methode besteht darin, dass hier weit mehr Sicherheitsbeweise bekannt sind und die Sicherheitsanalyse i. Allg. einfacher ist als bei blinden Signaturen.

3.2.3 Einmaligkeit

Diese Forderung an elektronische Münzsysteme soll das sogenannte *Double-Spending* verhindern, d.h. es darf nicht möglich sein, dass der Besitzer

einer elektronischen Münze diese kopiert und erneut bei einem Zahlungsvorgang verwendet. Zur Vermeidung des Double-Spending wurden zwei unterschiedliche Verfahren entwickelt.
Durch kryptographische Methoden lässt sich die unerlaubte Mehrfachverwendung von elektronischen Münzen nicht von vornherein verhindern. Es besteht jedoch die Möglichkeit, die Identifikationsnummer (z.B. Kontonummer) des Double-Spenders zu ermitteln. Dazu wird die Identität des Münzbesitzers so in die Münze eingebettet, dass die Bank bei einem Double-Spending Vergehen nachträglich die Identität des Verursachers bestimmen kann. Die Anonymität wird dadurch nicht verletzt, da bei jedem Bezahlvorgang jeweils nur ein Teil der Identität preisgegeben wird. Erst nach einer zweiten Bezahlung, bei der der Kunde einen anderen Teil seiner Identität preisgeben muss, kann die Bank die Teile zur kompletten Identität zusammensetzen.
Als zweites Verfahren zur Vermeidung von Double-Spending existiert eine Hardware-gestützte Lösung. Dazu werden die Münzen in einem zusätzlichen Gerät, dem so genannten Observer, gespeichert. Dadurch wird dem Kunden der direkte Zugriff auf die elektronischen Münzen verwehrt und ein Kopieren unmöglich gemacht.

3.2.4 Authentizität

Bei elektronischen Zahlungsverfahren sind die Verfahren zur gegenseitigen Authentisierung, d.h. zur Überprüfung der Identität eines Benutzers bzw. einer Bank, von essentieller Bedeutung. Als mögliches System bietet sich z.B. die Vergabe einer PIN-Nummer an, wobei es sich hierbei um eine wenig verlässliche Zugangskontrolle handelt, da die (geheime) PIN-Nummer oftmals schriftlich mit der Karte mitgeführt wird. Des weiteren liefern die meist verwendeten vierziffrigen PINs nur 10000 mögliche Kombinationen, welche mit entsprechendem technischem Gerät leicht durchprobiert werden können.
Als bessere Methode des Identitätsnachweises gilt die elektronische Unterschrift (Signatur). Sie wird zur Feststellung der Echtheit von elektronisch übermittelten Nachrichten verwendet. Eine digitale Signatur ist das elektronische Äquivalent zur handschriftlichen Unterschrift und hat die Eigenschaft, dass sie jeweils nur von einer einzigen Person korrekt erzeugt werden kann. Durch Überprüfen der digitalen Signatur lässt sich feststellen, ob die zugehörige Nachricht verändert wurde. Die heutzutage am häufigsten benutzten elektronischen Unterschriftensysteme basieren auf dem RSA[7]-Algorithmus, der wohl bekanntesten Public-Key-Verschlüsselungs-Methode. [8]

[7] benannt nach seinen Erfindern Rivest, Shamir und Adleman.

[8] nähere Informationen zum RSA-Verfahren sind nachzulesen in [Furche, Wrightson], S.111ff.

3.2.5 Fälschungssicherheit

Fälschungssicherheit wird dadurch erreicht, dass die digitalen Münzen nur von den dazu autorisierten Instanzen erzeugt werden können, die diese Datensätze mit digitalen Signaturen versehen. Hierbei kann wiederum das RSA-Verfahren verwendet werden, es gibt jedoch auch andere Ansätze, wie z.B. die ElGamal-Signatur. [9]

3.3 Wechselgeld

Im vorhergehenden Kapitel wurden die Anforderungen an elektronische Münzsysteme und ihre jeweilige Umsetzung vorgestellt. Damit kann nun herkömmliches Bargeld schon sehr gut digital nachgebildet werden. Allerdings fehlt noch eine Lösung für die Wechselgeld-Problematik. Denn der bisherige Geldkreislauf elektronischer Münzsysteme sieht vor, dass der Kunde passend bezahlen kann und der Händler das Geld anschließend einlöst. Es muss also eine Möglichkeit für die Ausgabe von Wechselgeld gefunden werden, die die Tatsache berücksichtigt, dass digitale Münzen zur Ahndung von Double-Spending Informationen über ihren Besitzer enthalten, der auch als einziger in der Lage ist, diese Münzen auszugeben. Als einfachste und offensichtlichste Lösung der Wechselgeld-Problematik gilt der Vorschlag, nur Münzen eines einzigen Basiswertes zu erzeugen, z.B. 1-Cent-Münzen, mit denen dann jeder Geldbetrag exakt bezahlt werden kann. Damit wäre das Problem vollständig gelöst, allerdings müsste dann jeder Benutzer sehr viele Münzen erzeugen lassen, speichern und übertragen. Deshalb wird dieses Ansatz sehr schnell ineffizient.
In den folgenden beiden Kapiteln werden nun die zwei wesentlichen Strategien zur Lösung der Wechselgeld-Problematik vorgestellt.

3.3.1 Übertragbarkeit

Bei dem Ansatz mit übertragbaren Münzen besteht die Möglichkeit, dass Benutzer untereinander Guthaben austauschen können, ohne dass die Bank zur Verrechnung der Transaktion herangezogen werden muss. Allerdings müssen bei diesem Ansatz Einbußen in der Systemsicherheit, speziell bei der Anonymität, hingenommen werden. Das größere Problem stellt jedoch das lineare Anwachsen des Datensatzes einer digitalen Münze mit jeder Übertragung dar, so dass bei diesem Ansatz dieselben Probleme entstehen wie bei der im vorigen Kapitel kurz vorgestellten Idee mit den 1-Cent-Münzen.

[9] Für weiterführende Informationen s. [ElGamal].

3.3.2 Teilbarkeit

Die Teilbarkeit von digitalen Münzen ist eine Eigenschaft, die traditionelle Bargeldsysteme nicht erfüllen können. Darunter versteht man die Möglichkeit, eine Banknote in eine beliebige Anzahl kleinerer Banknoten zu tauschen, so dass die Summe dieser Banknoten dem Wert der ursprünglichen Banknote entsprechen. Die jeweilige Signatur der Münzen betreffend stellt die Teilbarkeit kein Problem dar, da sich signierte Datensätze auf Grund der mathematischen Eigenschaften mancher digitaler Signaturen so aufteilen lassen, dass man zwei neue Datensätze mit neuen Signaturen erhält. Problematisch an diesem Ansatz ist jedoch wie bei der Übertragbarkeit die nicht mehr vollständig vorhandene Anonymität und der Effizienzverlust im Vergleich zu Basissystemen ohne diese Zusatzfunktionalität.

3.4 DigiCash

Das eCash System ist eine Entwicklung des amerikanischen Mathematikers und Kryptologen Dr. David Chaum von DigiCash und wurde von eCash Technologies weitergeführt. Es wurde in einem Pilotprojekt zusammen mit der deutschen Bank im Oktober 1997 eingeführt, auf Grund mangelnden Interesses seitens der Kunden jedoch im Mai 2001 für gescheitert erklärt. [10] eCash basiert auf digitalen Münzen, die das Pendant zu herkömmlichem Bargeld darstellen. Diese eCash Münzen sind zunächst nichts anderes als Datenblöcke, die den Wert der Münze, eine Seriennummer und eine digitale Unterschrift enthalten.
Der Kunde erzeugt sich zunächst mit einer speziellen Software seine digitalen Münzen, die dann von der Bank mittels blinder Signatur (s.3.2.2) signiert und vom Konto des Kunden abgebucht werden. Dadurch ist gewährleistet, dass die Benutzung des digitalen Geldes durch den Kunden vollkommen anonym bleibt (eine Zuordnung von Seriennummer und Kunde ist nicht möglich). Mit diesen Münzen kann der Kunde dann bei anderen eCash Kunden und Händlern bezahlen oder sie wieder bei seiner Bank einlösen. Die Gültigkeit der eCash Münzen kann von den Beteiligten einfach durch Einlösen der Münzen bei der Bank berprüft werden, welche wiederum die Gültigkeit anhand der blinden Signatur verifiziert.
Die Kommunikation zwischen den einzelnen Komponenten wird durch asymmetrische Verschlüsselung abgesichert, wobei jeder Teilnehmer (Händler, Kunde, Bank) über ein zertifiziertes Schlüsselpaar verfügt. Andernfalls könnte das digitale Geld abgefangen werden und von Angreifern benutzt werden, da der Wert direkt mit der Münze in Beziehung steht. Ferner wird das Zertifikat des Nachrichtenempfängers zwecks Authentifizierung benötigt. So kann sichergestellt werden, dass der Partner für die

[10] Vgl. [Heise].

Bestellung bzw. den Geldtransfer auch wirklich die Person ist, für die sie sich ausgibt.
Durch die Seriennummer der digitalen Münzen (mind. 100-stellige Zahl) wird sichergestellt, dass diese nicht doppelt ausgegeben werden können. Nach jeder Benutzung der Münzen werden diese zur Überprüfung bei dem eCash-Server eingereicht, wo die jeweiligen Seriennummern dann gespeichert werden, wodurch eine unerlaubte Mehrfachverwendung einer digitalen Münze erkannt werden kann. Das Problem, dass bei zunehmender Anzahl von Benutzern die zu verwaltenden Datenmengen sehr groß werden können, wird zumindest zum Teil dadurch gelöst, dass die Münzen mit einem Gültigkeitsdatum versehen werden.
Besonderes Merkmal von eCash gegenüber anderen Zahlungssystemen ist die Anonymität der Münzen. Weder der Händler noch die Bank können zurückverfolgen, wer die eCash Münzen generiert hat. Aus diesem Grund ist der Einsatz von eCash insbesondere dort sinnvoll, wo der Kunde nicht seine Adresse zur Lieferung von Waren angeben muss, also z.B. beim Download von Daten. Da der Empfänger von eCash Münzen diese unmittelbar bei der Bank einlöst, ist die Zahlung garantiert. Die Transaktionskosten werden beim Einlösen der eCash Münzen bezahlt, beim Erstellen der Münzen fallen keine Kosten an. Da die Transaktionskosten deutlich geringer als bei Kreditkarten ausfallen, sind eCash Zahlungen auch bei Kleinstbeträgen sinnvoll.
Das System von DigiCash hat jedoch auch einige Nachteile, so sind z.B. die Online-Überprüfungen der Münzen relativ teuer, und durch die gewährleistete Anonymität entstehen Sicherheitslücken. Des weiteren ist die Installation und Benutzung des Systems recht komplex und der Rechenaufwand, bedingt durch das asymmetrische Verfahren, relativ hoch.[11]

4 Fazit

Keines der in den letzten Jahren eingeführten digitalen Münzsysteme hat es über die Testphase hinaus geschafft sich als neue gängige Internetwährung zu etablieren. Das Hauptproblem dabei lag jedoch nicht primär an den Systemen selbst, sondern an der jeweils relativ kleinen Benutzergruppe der Systeme im Vergleich zur Gesamtgröße der Internet-Gemeinde. Die Folge daraus war, dass die Systeme für potentielle Verkäufer uninteressant waren. Dadurch wurde jedoch wieder die Anzahl der Benutzer klein gehalten, denn es gab nur wenig Möglichkeiten, mit diesen Systemen im Internet Einkäufe zu tätigen.

[11] für weitere Informationen s. [Schneppe].

Literatur

[Furche, Wrightson]
Furche, A., Wrightson, G. : Computer Money, Internet- und Kartensysteme, 1. Auflage.
dpunkt-Verlag für digitale Technologie GmbH, Heidelberg, 1996.

[ElGamal]
ElGamal, T.: A Public Key Cryptosystem And A Signature Scheme Based On Discrete Logarithms, Springer Verlag, 1984.

[DuD5/2003]
DuD, Datenschutz und Datensicherheit, Schwerpunkt Anonymität und Pseudoanonymität in Anwendungen, Ausgabe 5/2003, Vieweg.

[UniKonstanz]
http://www.inf-wiss.uni-konstanz.de/CURR/summer98/imk/Internet-Zahlungssysteme/zahlungssysteme.html, 02.07.2004

[Paybox]
http://www.paybox.net, 02.07.2004.

[Firstgate]
http://www.firstgate.de, 02.07.2004.

[Heise]
http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/16934&words=Ecash, 02.07.2004.

[Schneppe]
http://ulrich.schneppe.bei.t-online.de/s1916/start.htm#inhaltsverzeichnis, 02.07.2004.