Ist elektronisches Bargeld realisierbar?

Jan Holger Schmidt **Arnd Weber**[2]
Matthias Schunter[1]

Zusammenfassung

Die Vorteile von Bargeld sind Unverkettbarkeit (d.h. unbedingte Anonymität), geringe Transaktionskosten und Unwiderrufbarkeit der Zahlung. Um diese Vorteile auch dem elektronischen Handel zu erschließen, untersucht dieser Beitrag, ob elektronisches Bargeld entwikkelt werden kann, das die Vorteile von Bargeld mit den Vorteilen elektronischer Zahlungssysteme vereint. Nach einer Beschreibung der in unseren Benutzerbefragungen erhobenen Anforderungen an elektronisches Bargeld geben wir einen kurzen Überblick über die technischen Möglichkeiten. Anschließend beschreiben wir die Trade-offs zwischen den sich widersprechenden Anforderungen. Abschließend erklären wir, wieso bestehende elektronische Zahlungsmittel kein elektronisches Bargeld sind, und zeigen offene Fragen auf dem Weg zum elektronischen Bargeld auf.

1 Einleitung

Elektronisches Bargeld definieren wir als universell einsetzbare elektronische Werte[3]. Derzeit wird der Einsatz von Wertkarten, wie z.B. der Geldkarte, sowohl im herkömmlichen als auch im elektronischen Handel angestrebt, um die Transaktionskosten gegenüber herkömmlichen Kartenzahlungen zu senken. Um aber traditionelles Bargeld weitestgehend zu ersetzen, muß ein elektronisches Zahlungssystem sowohl einfach benutzbar und robust sein, als auch Unverkettbarkeit und offline Transferierbarkeit ermöglichen.

---

[1] Universität des Saarlandes, Fachbereich Informatik, Lehrstuhl Kryptographie und Sicherheit, D-66123 Saarbrücken, <max@krypt.cs.uni-sb.de, schunter@acm.org>.

[2] Albert-Ludwigs-Universität, Institut für Informatik und Gesellschaft, D-79098 Freiburg i. B., <aweber@iig.uni-freiburg.de>.

[3] Neben elektronischem Geld betrachten wir auch mögliche Pay-now Schemata und Debitsysteme.

Da solch ein System nicht existiert, stellt sich die Frage, ob es überhaupt möglich ist, elektronisches Bargeld zu entwickeln, das diese essentiellen Eigenschaften von traditionellem Bargeld bietet und daher das Potential hat, dieses in weiten Bereichen zu ersetzen.

1.1 Überblick

Nach der Beschreibung der Vorteile elektronischen Bargelds in Abschnitt 1.2 beschreiben wir die gewünschten Eigenschaften in Kapitel 2. Neben den essentiellen Eigenschaften von Bargeld sind dies wünschenswerte Eigenschaften wie Verlust- und Fehlertoleranz oder die Zahlungsmöglichkeit über Netzwerke. Anschließend beschreiben wir die technischen Möglichkeiten in Kapitel 3 und diskutieren in Kapitel 4, inwieweit diese die Erfüllung der Anforderungen ermöglichen. Abschließend skizzieren wir in Kapitel 5, warum existierende Systeme[4] kein Bargeld sind und zeigen auf, welche vielversprechenden Möglichkeiten wir auf dem Weg zum elektronischen Bargeld, welches diesen Namen verdient, sehen.

1.2 Erhoffte Vorteile von elektronischem Bargeld

Unsere Gespräche[5] mit Bankvertretern haben ergeben, daß elektronisches Geld noch keine Gewinne erwirtschaftet. Trotzdem bleibt ein Einsatz von elektronischem Bargeld aus folgenden Gründen wünschenswert:

- Geringere Handhabungskosten gegenüber Geldscheinen und Münzen,
- keine Probleme mit fehlendem Wechselgeld sowie
- erschwerte Fälschung.

---

[4] Für einen Überblick über existierende Systeme verweisen wir auf Asokan, Janson, Steiner, Waidner 1997, Furche, Wrightson 1997, Mahony, Peirce, Tewary 1998.

[5] Die Darstellung der Anforderungen und des Nutzens elektronischen Bargelds basiert auf Interviews mit Experten und Nutzern. Diese wurden innerhalb der Forschungsprojekte „Soziale Determinanten der Entwicklung alternativer POS-Zahlungssysteme”, gefördert von der Deutschen Forschungsgemeinschaft (vgl. Weber 1997b), sowie CAFE und SEMPER, gefördert von der Europäischen Union, vorgenommen. Vgl. Furger u.a. 1998 für die Nutzerinterviews.

Zusätzlich bietet elektronisches Bargeld die folgenden Vorteile gegenüber herkömmlichen elektronischen Zahlungsmitteln:

- Unbedingte Anonymität im Sinne unverkettbarer elektronischer Zahlungen[6],
- verringerte Kommunikationskosten durch off-line Zahlungen,
- Herausgeber von elektronischem Bargeld können zusätzliche Marktsegmente gewinnen,
- geleistete Vorauszahlungen an den Herausgeber zum Erhalt von elektronischem Bargeld können verzinst werden,
- wie bei herkömmlichen Barzahlungen können zum Vorteil der Händler Zahlungen nicht widerrufen werden.

Außerdem bietet elektronisches Bargeld auch die Vorteile von Paynow Systemen:

- Ausgabe an nicht kreditwürdige Personen möglich und
- Verringerung der Transaktionskosten durch Ersetzung von Kreditkartenzahlungen.

Diese Vorteile sind in ihre Gänze nur realisierbar, wenn traditionelles Bargeld in einem erheblichen Maße ersetzt werden kann und gleichzeitig Nutzbarkeit in offenen elektronischen Netzen gegeben ist.

2 Wünschenswerte Eigenschaften

Wir beschreiben nun Eigenschaften von herkömmlichem Bargeld und existierenden elektronischen Zahlungsmitteln, welche aus Anwendersicht wünschenswert sind.

2.1 Eigenschaften herkömmlichen Bargelds

Um einen größeren Anteil der Bargeldtransaktionen zu ersetzen, muß elektronisches Bargeld dessen essentielle Eigenschaften aufweisen, da anderenfalls die Erwartungen der Anwender enttäuscht würden.

---

[6] Unverkettbarkeit unterbindet die Verkettung von Zahlungen bei bestehenden Wertkarten, bei denen z.B. Einkäufe mit derselben Wertkarte ein und derselben Person zugeordnet werden können.

Universelle Einsetzbarkeit: Universelle Einsetzbarkeit bedeutet, daß jeder das Geld nutzen kann und es von allen als Zahlungsmittel akzeptiert wird. Ein Benutzer einer der ersten Wertkarten in Biel (CH) sagte schon 1993 „Geld kann man überall gebrauchen, die Karte nicht. Man ist auf die Geräte angewiesen, die die Karte lesen können."[7] Ebenso sind Zahlungen mit Bargeld im wahrsten Sinne des Wortes kinderleicht und die Befragten erwähnten Situationen wie, „wenn ich einem kleinen Kind ein Geschenk machen will." Und wiesen darauf hin, „daß Kinder zunächst mit Bargeld den Umgang mit Geld lernen müssen." Ein weiterer Aspekt der Einsetzbarkeit ist die Tragbarkeit der Geräte, da elektronisches Bargeld ohne ein Gerät nicht nutzbar ist.

Off-line Verwendbarkeit: Barzahlungen können ohne Bank erfolgen. Da die meisten Nutzer nicht immer on-line sein werden, ist off-line Verwendbarkeit eine wünschenswerte Eigenschaft von elektronischem Bargeld.

Off-line Transferierbarkeit: Hierunter verstehen wir die Möglichkeit, erhaltene Werte direkt für weitere Zahlungen einzusetzen. Die Befragten nannten Situationen wie die Zahlung von Trinkgeldern, Zahlungen an Kinder, Straßenmusikanten, Spenden, Geschenke („How do you put a tenner in somebody's birthday card?"), Zahlungen an Nachbarn, („20p to buy a pint of milk") und kleine Zahlungen, wie für „ein Glas Bier" oder „un café". Auch Situationen wie der Verkauf eines gebrauchten Autos an Fremde konnten sich Befragte ohne Bargeld nicht vorstellen. Sie sahen, daß diese Möglichkeiten bei Wertkarten nicht gegeben sind: „Aber wenn ich auf der Karte sFr 1.000 habe, kann ich sie nicht weitergeben. Ich kann daraus nicht drei Karten machen, wovon ich eine weitergeben kann," sagte ein Teilnehmer des Versuches in

---

[7] Die Zitate zur Begründung unserer Thesen entstammen persönlichen Interviews mit 268 Kartennutzern in Deutschland, Frankreich, Großbritannien, Italien und der Schweiz.. Ihnen wurde u.a. die Frage gestellt „Stellen Sie sich einmal vor, in Ihrer Karte wäre so eine Art elektronisches Portemonnaie und Sie könnten damit alles und überall bezahlen. Damit wäre im Prinzip das Bargeld überflüssig. Würden Sie trotzdem noch mit Bargeld bezahlen wollen? (Wenn ja:) Bei welchen Anlässen?" Etwa die Hälfte gab an, weiterhin mit Bargeld bezahlen zu wollen und nannte Gründe, wie wir sie zitieren. Die Fragebögen, Antworten und Interpretationen sind in Furger u.a. 1998 im Detail wiedergegeben.

Biel und dachte weiter: „Wenn jeder ein Ablesegerät hätte, aber das kann ich mir nicht vorstellen."

Unverkettbarkeit: Die Befragten nannten mehrere Gründe wegen derer sie den Schutz der Privatsphäre des Bargeldes schätzen.[8] Einige Franzosen sah ihn als Teil des Grundrechts der „liberté personelle" an. Manche forderten einfach Vertraulichkeit: „Monetäre Angelegenheiten sind primär Privatangelegenheiten", „weil ich entscheiden will, wer wann was von mir erfährt", oder „[I would like to] minimise Big Brother's surveillance of my expenditure". Andere forderten Unverkettbarkeit zur Bezahlung von Gütern „which fell off the back of a lorry", oder für „cash for the babysitter". Daher werden einige Bereiche von Barzahlungen nur durch Zahlungssysteme mit einem starkem Schutz der Privatsphäre abgedeckt werden können. Im folgenden unterscheiden wir zwei Stufen: „Unverkettbarkeit" (Chaum 1981) bedeutet, daß Bank und Händler nicht feststellen können, ob zwei Zahlungen von einer Person getätigt wurden. „Pseudonymität" bedeutet, daß mehrere Zahlungen einer Person verkettet werden können und diese somit z.B. nach Bezahlung einer persönlichen Rechnung nicht mehr anonym sind, auch wenn anfangs dem Pseudonym kein Name zugeordnet war.

Transparenz: Dem Nutzer sollte es möglich sein, auf einen Blick festzustellen, wieviel Geld er noch bei sich trägt. „Kinder sehen beim Bargeld die Menge". Es bleiben aber auch Unannehmlichkeiten erspart, daß man beispielsweise nicht erst nach langem Schlange stehen vor der

---

[8] Zur Frage der Unverkettbarkeit stellten wir 137 der Befragten die Frage „Viele der Transaktionen, die mit Zahlungskarten getätigt werden, werden in Datenbanken gespeichert. Es wäre technisch möglich, jede Transaktion anonym zu machen, aber das wäre mit Mehrkosten verbunden. Wieviel wären Sie bereit dafür pro Jahr mehr zu bezahlen?" Etwa ein Drittel erklärte sich bereit, hierfür einen Betrag zwischen DM 20 und 50 zu zahlen. Anderen 139 Kartennutzern stellten wir die Frage „Heute werden persönliche Daten, welche aus Kartenzahlungen stammen, in Datenbanken gespeichert. Mit unserem System wäre dies nicht mehr der Fall, denn Sie hätten sozusagen elektronische Münzen und Banknoten in Ihrem Portemonnaie. Wäre es für Sie wichtig, daß beim Bezahlen mit elektronischen Zahlungssystemen die Anonymität der Transaktionen wie beim Bargeld bewahrt wird?" Rund die Hälfte fand dies wichtig oder sehr wichtig. Wir zitieren aus den Kommentaren der Befragten.

Kasse feststellt, daß der Betrag auf der Karte nicht zum Zahlen der Rechnung genügt.

Kontrolle über die Geldbörse: In der Regel überreichen Kunden dem Händler nicht die gesamte Geldbörse, damit dieser sich bedient. Daher sollte dies bei elektronischem Bargeld auch nicht vorausgesetzt werden. Das Terminal sollte auch nicht unbedingt die Möglichkeit haben, manipuliert erscheinende Geräte einfach aus dem Verkehr zu ziehen. Dies ist insbesondere dann sinnvoll, wenn auf dem Träger noch weitere Funktionen (z.B. Möglichkeit zur digitalen Signatur oder Zugangskontrollen) sind, auf die ein Kunde nicht verzichten will oder kann.

Lange Gültigkeitsdauer: Elektronische Wertkarten haben derzeit, im Gegensatz zu Bargeld, eine eingeschränkte Gültigkeitsdauer. Bei elektronischem Bargeld muß auf eine ausreichend lange Gültigkeitsdauer geachtet werden.

Robustheit: Elektronisches Bargeld muß robust gespeichert werden. Benutzer erwarten mindestens die Robustheit von Plastikkarten, die in vielen Ländern und Klimata lesbar sind.

Preis-/Leistungsverhältnis: Zusatzkosten müssen durch Zusatznutzen gerechtfertigt sein. Da Bargeld für Nutzer scheinbar keine Kosten verursacht, werden Zusatzkosten den Nutzern nur schwer vermittelbar sein. Ebenso würde ein Disagio bei der Transfers unter privaten Nutzern kaum akzeptiert werden („Schwundgeld”).

Sicherheit: Abgesehen von dem Risiko des Herausgebers, Schaden durch Betrug zu erleiden, soll auch dem Benutzer Sicherheit gegenüber dem Herausgeber gewährt werden.

2.2 Weitere wünschenswerte Eigenschaften

Zusätzlich zu den essentiellen Eigenschaften von Bargeld werden von einem elektronischen Zahlungsmittel weitere Eigenschaften erwartet werden:

Kein Wechselgeldproblem: Nutzer erwarten, daß bei elektronischem Bargeld kein Wechselgeldproblem auftritt, d.h., daß jeder Betrag problemlos bezahlt werden kann.

Zahlungen über Netzwerke: Elektronische Zahlungssysteme sollten sichere Zahlungen auch über unsichere Netzwerke ermöglichen.

Verlust- und Fehlertoleranz: Sicherheit bei Verlust, Diebstahl und Funktionsstörung ist ein Verkaufsargument für Kreditkarten und würde auch bei elektronischem Bargeld begrüßt.

Internationale Verwendung: Einsetzbarkeit bei grenzüberschreitenden Zahlungen wird heute schon von Kreditkarten ermöglicht.

Einfaches Nachladen: Falls Nachladen nur am Bankautomat ermöglicht wird, werden viele Nutzer dort weiter herkömmliches Bargeld abheben, welches universell einsetzbar ist. Analog sollte das Nachladen von elektronischem Bargeld nicht mehr Zeit als das Abheben von herkömmlichem Bargeld benötigen.

Benutzerfreundlichkeit: Zahlungssysteme sollten einfach zu verstehen und zu benutzen sein.

3 Technologien für elektronisches Bargeld

Dieser Abschnitt gibt einen kurzen Überblick über existierende Technologien, die den Aufbau elektronischer Zahlungssysteme ermöglichen. Bevor wir auf spezielle Systeme eingehen, skizzieren wir grundlegende Technologien.

3.1 Basistechnologien

3.1.1 Manipulationsschutz der Hardware

Chipkarten mit Manipulationsschutz (engl. *tamper resistance*) sollen verhindern, daß elektronisches Bargeld unerlaubt vervielfältigt wird. Mit entsprechender Ausrüstung kann jedoch, ggf. durch leicht zugängliche Instrumente in Universitätslaboratorien, manipulationsgeschützte Hardware gebrochen werden (Anderson, Kuhn 1996). Zwar existieren stärker gesicherte Systeme auf dem Markt, aber sie erfordern größere Module als Chipkarten.

3.1.2 Blinde Signaturen

Unverkettbarkeit läßt sich durch „blinde" digitale Signaturen erreichen. Das Bargeld wird zwar vom Herausgeber signiert, aber er kann die Signatur bei eingelöstem Bargeld nicht wiedererkennen (Chaum 1983).

3.1.3 Vertrauenswürdige Benutzergeräte

Damit Benutzer überprüfen können, was das Zahlungsmodul der Bank übermittelt, bietet sich das „wallet with observer" Konzept an (Chaum 1992). Hierbei kann sich der Anwender eine elektronische Brieftasche eines beliebigen Herstellers kaufen. Module von mehreren Herausgebern garantieren jeweils die Sicherheit eines Herausgebers. Um Transparenz zu gewährleisten und dem Anwender eine sichere Eingabe seiner PIN zu ermöglichen, benötigt solch eine Brieftasche eine Anzeige und eine Tastatur.

3.1.4 Anonymität im Netzwerk

Trotz Anwendung von blinden Signaturen ist der Zahlende anhand des Datenflusses identifizierbar. Dies kann durch anonyme Terminals oder anonyme Dienste im Netz (Chaum 1981) verhindert werden.

3.1.5 Verlusttoleranz

Speichern die Benutzer Backup-Informationen, so kann selbst ein System, das Unverkettbarkeit gewährleistet, verlusttolerant sein (Pfitzmann, Waidner 1997).

3.2 Technologien für Münzsysteme

Wir unterscheiden zwischen Münz- und den unten beschriebenen Zählersystemen. Wie konventionelle Münzen haben auch elektronische einen festen Nennwert. Eine digitale Signatur stellt sicher, daß die Münzen nur vom Herausgeber akzeptiert werden. Blinde Signaturen gewährleisten Unverkettbarkeit. Solche Münzen weisen eine hohe Sicherheit auf, führen aber auch zu einem Wechselgeldproblem, welches durch Erweiterungen reduziert werden kann.

3.2.1 Erkennung von Mehrfachverwendung

Es existiert keine Softwarelösung, die unerlaubtes Vervielfältigen von elektronischem Geld verhindert. Aus diesem Grund wird bei einer Zahlung bisher entweder manipulationsgeschützte Hardware verwendet oder mittels einer on-line Verbindung zum Herausgeber überprüft, ob das Geld schon verwendet wurde und damit ungültig ist (z.B. eCash). Enthalten elektronische Münzen die verschlüsselte Identität des Besitzers, so läßt sich bei Mehrfachverwendung der Betrüger herausfinden. Dadurch können off-line Systeme zusätzlich geschützt werden. Die

Kodierung kann dabei so erfolgen, daß die Identifikation ausschließlich bei Mehrfachverwendung möglich ist und blinde Signaturen ansonsten die Unverkettbarkeit sicherstellen (Chaum, Fiat, Naor 1990).

3.2.2 Nullwertige Münzen für off-line Transferierbarkeit

Um eine Identifikation von Betrügern bei transferierbaren elektronischen Münzen zu ermöglichen, bindet der Empfänger der Münze während des Zahlungsvorgangs eine nullwertige Münze an die gezahlte (van Antwerpen 1990). Diese nullwertige Münze enthält die kodierte Identität des Empfängers. Durch die Bindung muß auch diese nullwertige Münze beim nächsten Transfer zusammen mit der Wertmünze weitergereicht werden. Somit ist sichergestellt, daß der Herausgeber den Empfänger identifizieren kann, falls dieser die Münze (und somit auch die nullwertige) unerlaubt mehrfach verwendet. Unumgänglich wächst deshalb bei jedem Transfer der benötigte Speicherplatz pro Zahlung (Chaum, Pedersen 1993).

3.2.3 Teilbarkeit zur Lösung des Wechselgeldproblems

Wie bei konventionellen Münzen führt auch bei elektronischen der feste Nennwert zu Schwierigkeiten beim Bezahlen von exakten Beträgen. Akzeptiert man bei einer Zahlung Wechselgeld, so wird man gleichzeitig zum Zahlungsempfänger. Damit ist Wechselgeld keine Lösung des Problems in Systemen, die Unverkettbarkeit nur für den Zahlenden gewährleisten. Okamoto und Ohta (1992, vgl. Chan, Frankel, Tsiounis 1998) schlugen deshalb teilbare Münzen vor, die inkrementell bis zur dem Nennwert zahlbar sind. Ein Nachteil ist, daß die Unverkettbarkeit reduziert wird, da Fragmente einer Münze miteinander verkettet werden können. Das Wechselgeldproblem kann auch durch die unten gezeigte Kombination von Münz- und Zählersystemen reduziert werden.

3.3 Technologien für Zählersysteme

In Zählersystemen wird der Betrag von elektronischem Geld, den eine Person besitzt, durch einen Zähler repräsentiert. Manipulationsgeschützte Hardware und Authentikationsschemata sind notwendig, um unberechtigte Veränderungen des Zählerstandes durch die Benutzer zu verhindern. Wird in allen Zahlungsmodulen der gleiche Schlüssel verwendet, so kann auch Unverkettbarkeit gewährleistet werden. Die Verwendung von unterschiedlichen Schlüsseln für die einzelnen Anwender erhöht die Sicherheit eines Zählersystems. Da jeder Schlüssel dann ein Pseudonym für seinen Benutzer ist, erlaubt ein solches System höchstens Pseudonymität.

Eine weitere Möglichkeit zur Erreichung von mehr Sicherheit ist, den Wert der Zähler beim Herausgeber zu verfolgen. Solche Schattenkonten erlauben es, die Mehrfachverwendung von Werten festzustellen und bieten zusätzlich Verlust- und Fehlertoleranz.

3.4 Hybride Schemata aus Zählern und Münzen

3.4.1 Zähler in Verbindung mit nullwertigen Münzen

Elektronische Münzen (bzw. Schecks) können die Sicherheit von Zählersystemen etwas steigern (Bos, Chaum 1990), indem Zahlungen zusätzlich durch eine entsprechende Anzahl an nullwertigen Münzen autorisiert werden müssen (z.B. je eine nullwertige Münze zur Autorisierung von je 2 EURO). Selbst bei unerlaubter Manipulationen am Zähler ist ohne weitere Abhebung von nullwertigen Münzen der Schaden pro manipuliertem Gerät begrenzt.

Mehrfachverwendung: Wegen des geringen Speicherplatzes auf Chipkarten kann auch eine begrenzte Mehrfachverwendung der nullwertigen Münzen erlaubt werden (CAFE 1996[9]). Abhängig davon, wie oft die Münze mehrfach verwendet werden darf, liegen die Sicherheit und Unverkettbarkeit zwischen der eines Münzsystems und der eines Systems mit Zählern.

Zahlung in Ticks: Finden alle Zahlungen an denselben Empfänger statt, wie beispielsweise pro Zeitintervall in einem Telefonat, so genügt dafür eine nullwertige Münze (Signatur). Nach einer Initialisierungsphase benötigen aufeinanderfolgende Zahlungen kaum Rechenzeit (Pedersen 1997).

3.4.2 Münzpools in Verbindung mit Zählern

Eine Lösung des Wechselgeldproblems, die auch Unverkettbarkeit garantiert, besteht darin, die Benutzergeräte bei der Ausgabe mit einem großen Vorrat an Münzen mit unterschiedlichen Nennwerten aus-

---

[9] In CAFE konnten Schecks zweimal verwendet werden. Dadurch konnten mit einer Chipkarte bis zum nächsten Ladevorgang 70 Zahlungen getätigt werden.

zustatten (z.B. EURO 1000 in verschiedenen Stückelungen). Dabei wird die Teilmenge dieses privaten Münzpools, welche der Benutzer abgehoben hat und somit auch ausgeben darf (z.B. EURO 75.24; anfänglich 0), durch einen Zähler kontrolliert[10]. Hierbei garantiert der Manipulationsschutz, daß nur diese Teilmenge ausgegeben werden kann. Sollte dieser gebrochen werden, so kann der Benutzer zwar alle Münzen aus seinem privaten Münzpool ausgeben, ohne identifiziert zu werden, aber muß für weiteren Zahlungen neue Münzen beim Herausgeber nachladen und deren Gegenwert einzahlen oder sich ein neues Modul holen und auch dieses brechen. Damit besteht der maximale Schaden pro Gerät für den Herausgeber in der Menge an Münzen im privaten Pool.

4 Trade-offs bei der Entwicklung von elektronischem Bargeld

Hier untersuchen wir, welche wesentlichen Abwägungen getroffen werden müssen, wenn elektronisches Bargeld alle gewünschten Charakteristika aufweisen soll.

4.1 Trade-offs mit Kosten

Ein elektronisches Zahlungssystem ist nur dann akzeptabel, wenn die Kosten durch die entstehenden Vorteile gerechtfertigt sind. Viele Eigenschaften – wie komfortable Benutzergeräte mit Anzeige – sind mit Kosten verbunden, die bei entsprechenden Vorteilen aber auch getragen werden sollten. Diese Kosten können auch durch die Herausgeber übernommen werden, die sich dadurch eine gewinnbringende Kundenbindung erhoffen. Wir sind der Ansicht, daß bisher keine ausreichenden Studien durchgeführt wurden, die belegen, wieviel die Benutzer und Herausgeber für den Einsatz mächtiger Systeme zu zahlen bereit sind.

Unverkettbarkeit führt zu komplexen Systemen: Unverkettbarkeit erfordert kompliziertere Protokolle, sowie in Netzwerken anonyme Dienste oder Terminals.

---

[10] Diese Idee stammt von David Chaum.

Robuste und zuverlässige Systeme sind mit zusätzlichen Kosten verbunden: Selbst aufwendig konstruierte robuste Systeme werden nie so unversehrt mögliche Schäden überstehen wie konventionelles Bargeld. Dies gilt insbesondere für Geräte mit Nutzerinput und -output. Andererseits sind auch weniger robuste, günstigere Geräte akzeptabel, wenn das System eine ausreichende Verlust- und Fehlertoleranz bietet.

Das Wechselgeldproblem für sichere, unverkettbare elektronische Münzen ist schwer zu lösen: Eine Zahlung soll nicht dadurch verhindert werden, daß keine passenden Nennwerte verfügbar sind. Nur Münzen von kleinstem Nennwert (z.B. ein Cent) zu verwenden, würde zu überhöhtem Speicherbedarf und Rechenkapazität führen. Auch für Münzpools wird mehr Speicher benötigt. Teilbare Münzen wiederum reduzieren die Unverkettbarkeit und Zähler, die nicht zu einem Wechselgeldproblem führen, die Sicherheit.

Verlusttoleranz erfordert zusätzlichen Aufwand: Um Verlusttoleranz zu gewährleisten, müssen Backup-Informationen verwaltet werden.

4.2 Trade-offs mit Sicherheit

Perfekte Sicherheit ist unmöglich: Abgesehen von dem Risiko, daß ein Zahlungssystem mit sehr hohem Aufwand gebrochen wird, existieren auch Risiken, daß geheime Schlüssel oder Baupläne von Chips mit Manipulationsschutz gestohlen werden. Sollte elektronisches Bargeld weit verbreitet sein, so ist dies nicht alleine ein Risiko des Herausgebers, sondern auch eines für die Volkswirtschaft.

Vertrauen in Zahlungssystem ist unabdingbar: Nur wenn ein Vertrauen in die Systeme aufgebaut werden kann, finden sie auch Anwendung. Neue Verfahren sind nicht leicht zu verstehen und bedürfen somit Zeit, bis ein entsprechendes Vertrauen aufgebaut ist (Pfitzmann et al. 1997).

Unverkettbarkeit läßt mehr mögliche Lücken für Betrüger: In Systemen mit Unverkettbarkeit kann selbst bei auffälligen Transaktionen nicht nachgeprüft werden, von wem sie stammen. Betrug kann auch erst dann sicher festgestellt werden, wenn beim Herausgeber ein höherer Gesamtbetrag an elektronischem Bargeld eingelöst wurde, als dieser je ausgestellt hat.

Mehr Sicherheit führt zu komplexeren Systemen: Zahlungssysteme jeweils auf den aktuellsten Sicherheitsstand zu bringen, ist mit regelmäßigen Kosten verbunden. Insbesondere bei alleiniger Sicherung durch Manipulationsschutz müssen, bedingt durch immer neue Angriffstechniken, die Benutzer regelmäßig mit neuen Modulen ausgestattet werden. Kryptographische Verfahren erfordern komplexe Zahlungsprotokolle und leistungsfähige Geräte. Der Einsatz sicherer elektronischer Münzsysteme führt zum Wechselgeldproblem. Die Zahlung mit Münzen nimmt auch mehr Rechenkapazität in Anspruch, als lediglich einen Zählerstand zu ändern. Zählersysteme weisen andererseits eine geringere Sicherheit auf. Unverkettbare Transferierbarkeit in einem Zählersystem würde dem Herausgeber kaum ermöglichen, Betrug festzustellen – geschweige denn, Betrüger zu identifizieren. Durch die Kombination von Münz- und Zählersystemen läßt sich allerdings ein Kompromiß finden.

Systeme, die viele Eigenschaften aufweisen, sind weniger sicher: Je komplexer ein System wird, desto wahrscheinlicher ist es, daß während der Entwicklung Schwachstellen übersehen wurden. Damit ist eine paradoxe Situation erreicht. Sichere Systeme werden komplexer und benötigen gegebenenfalls Erweiterungen wie teilbare Münzen zur Lösung des Wechselgeldproblems, was wiederum zu mehr Sicherheitsrisiken führt.

Die Kontrolle der Geldbörse durch den Benutzer entspricht nicht den Sicherheitsvorstellungen des Herausgebers: Im Gegensatz zu den Benutzern, die ihr Zahlungsgerät/Karte nicht entbehren wollen, mag es im Interesse des Herausgebers sein, suspekte Zahlungsmodule einzuziehen. Dies wäre für den Herausgeber beispielsweise in pseudonymen Systemen sinnvoll, wenn eine nicht erklärbare Differenz zum Schattenkonto festgestellt wird.

Herausgeber bieten keine unbegrenzte Gültigkeit von elektronischem Bargeld an: Herausgeber wollen nicht über viele Jahre dem Anwender garantieren, den Gegenwert seines elektronischen Geldes auszuzahlen, da zwischenzeitlich das Zahlungssystem gebrochen worden sein könnte. Um das Risiko im Griff zu haben, limitieren die Herausgeber die Gültigkeit des elektronischen Bargelds auf wenige Jahre. Dies ist allerdings nicht im Interesse der Anwender, deren Geld ungültig wird, oder die „abgelaufenes" Bargeld in einer on-line Verbindung zum Herausgeber austauschen müssen. Gegen eine lange Gültigkeit spricht aber auch die Notwendigkeit, während des Gültigkeitsszeitraums Informationen zu speichern, die Verlusttoleranz ermöglichen, oder die es dem Hersteller gestatten, Mehrfachverwender zu identifizieren.

4.3 Trade-offs mit Benutzerfreundlichkeit

Benutzerfreundlichkeit führt zu widersprüchlichen Anforderungen: Benutzerfreundliche Zahlungssysteme sollten dem Benutzer eine große Funktionalität bieten, was zu unkomfortablen Auswirkungen in anderen Bereichen führt. So ist Transferierbarkeit für den Anwender sicherlich wünschenswert. Systeme mit Transferierbarkeit führen aber zu komplexen Protokollen und bei Münzsystemen zu anwachsendem Speicherbedarf, wie ein Experte in unseren Interviews berichtete: „and then you need a little carriage to drag it behind you". Je mehr Speicherplatz und Rechenkapazität benötigt wird, desto größer werden die Zahlungsmodule. Um zu verhindern, daß der Benutzer ein zusätzliches Gerät mit sich tragen muß, kann die Zahlungsfunktion auch in Mobiltelefone oder Armbanduhren integriert werden.

Unbegrenzte off-line Transferierbarkeit mit Identifizierung von Mehrfachverwendern in einem System, das Unverkettbarkeit garantiert, ist nicht möglich: Die Anzahl möglicher Transfers ist begrenzt durch die für das anwachsende elektronische Bargeld zur Verfügung stehende Speicherkapazität. Die Benutzer müssen Bargeld zurückgeben, das die maximal zulässige Anzahl von Transfers erreicht haben. Dies bedeutet, die Anwender müssen zwischen transferierbarem und nicht weiter für Zahlungen geeignetem Geld unterscheiden.

Die Benutzerfreundlichkeit ist begrenzt: Die einfache Verwendbarkeit von konventionellem Bargeld kann mit elektronischem Bargeld kaum erreicht werden, da Geräte und Elektrizität benötigt werden.

Ein System, welches off-line Zahlungen und Verlusttoleranz gestattet, kann keine lange Gültigkeit erlauben: Bei off-line Verwendbarkeit kann der Herausgeber erst dann verlorenes Geld zurückerstatten, wenn es nicht mehr gültig ist. Es ist nämlich für den Herausgeber nicht feststellbar, ob das Geld wirklich verloren ist, oder an eine andere Person off-line gezahlt wurde. Damit ist ein Konflikt zwischen Verlusttoleranz, die kurze Gültigkeitszeiten verlangt, und off-line Zahlungen, für die eine lange Gültigkeit wünschenswert ist, gegeben.

Nutzerinput und -output stehen im Gegensatz zur Gerätegröße: Für die Benutzer ist es angenehmer, eine kleine Karte mit sich zu führen, als ein Gerät im Taschenrechnerformat mit eigener Tastatur und Anzeige.

5 Existierende Systeme

Wenn man herkömmliches Bargeld ersetzen möchte, so sind nach unseren Befragungen off-line Transferierbarkeit und Unverkettbarkeit nötig. Heute gibt es keine einzige Implementierung, die diese Charakteristika bietet. Internet-Zahlungsmittel wie eCash kann man nicht off-line verwenden.[11] Existierende Wertkarten bieten keine Unverkettbarkeit, und nur Mondex bietet Transferierbarkeit, allerdings nicht für Händler. Lediglich der CAFE-Prototyp (CAFE 1996) bot Unverkettbarkeit, aber nur eine begrenzte Transferierbarkeit zu „Geschwister"-Karten (für die Übertragung von Eltern zu Kindern zum Händler).

6 Konsequenzen

In den europäischen Wertkartenprojekten wurde sichtbar, daß es sehr schwierig ist, das herkömmliche Bargeld zu ersetzen. Außer bei Mondex gibt es keine Transferierbarkeit. Gelegentlich wurde versucht, durch Kartenleser die Transparenz zu erhöhen. Nutzbarkeit auf Netzwerken war kaum möglich.[12] Aus unseren eigenen Befragungen wissen wir, daß die Nutzer diesen Mangel an Funktionalität sehen. Wenn man also nur einige Charakteristika anbietet, kann man auch nur die Nutzung in einzelnen Nischen erwarten, jedoch keine Abschaffung des Bargeldes.

---

[11] Bei Digicash eCash ist eine on-line Überprüfung notwendig. Wie bei allen existierenden Internet-Zahlungsmitteln ist keine Unverkettbarkeit gegeben, weil der Inhaber ja eine TCP/IP Adresse angeben muß, um eine Verbindung mit dem Zahlungsempfänger herzustellen.

[12] Im EU-Projekt SEMPER wurde die KPN-Wertkarte Chipper für Zahlungen über das Internet benutzt. Vgl. <http://www.semper.org>.

6.1.1 Elektronische Brieftaschen

Zukünftige Systeme elektronischen Bargeldes könnten allerdings ihren Namen in einem höheren Grade verdienen. Elektronische Brieftaschen könnten über mehrere Megabytes E^2PROM, Display und Tastatur verfügen, was mehrere Probleme auf einmal lösen könnte: Man kann Transferierbarkeit anbieten, viele Münzen speichern, das Guthaben anzeigen und die PIN auf dem eigenen Gerät eingeben. Nicht vertrauenswürdige Terminals könnten kein Geld entnehmen. Das Wallet-Oberver Konzept kann realisiert werden. Unwiderrufliche Zahlungen wären möglich. Mit einem kontaktlosen Interface könnten billige Terminals möglich werden, so daß sogar kleine Summen kostengünstig bezahlt werden könnten.

Leider wurden bislang wenig Erfahrungen mit elektronischen Brieftaschen gesammelt. Vielmehr muß festgestellt werden, daß die Kartenindustrie und die Banken sich in einem „lock-in” (Arthur 1989) befinden, indem sie sich auf (Chip-)Karten festgelegt haben. Würden die Nutzer für elektronische Brieftasche zahlen wollen? Erste qualitative Interviews mit 139 Kartennutzern in fünf europäischen Ländern zeigen, daß es eine Zahlungsbereitschaft von EURO 15 bis 50 für derartige Geräte gibt, wenn sie mehrere Karten ersetzen, also auch Postpay-Funktion haben (Furger et al. 1998). Den Gesprächspartnern wurden Prototypen gezeigt, und ihre Feedback war ermutigend:

> *„Wenn ich so ein Superding in der Hand habe, würde ich es natürlich vielseitig einsetzen.”*
>
> *„Could be something like a Swatch, the latest trend to have.”*
>
> *„That's the future, this kind of thing.”*

Abb. 1: Designstudie für eine multifunktionale Brieftasche mit Infrarotschnittstelle, Menütasten und Schublade für mehrere Sicherheitsmodule (Özalp 1996).

Bislang wurde jedoch noch kein größerer Versuch unternommen.[13] Die Lage mag sich noch ändern, wenn Mobiltelefone oder Organizer zunehmend für Zahlungen benutzt werden oder um sonstige Dokumente sicher digital anzuzeigen und zu signieren (vgl. das deutsche Signaturgesetz, Bundesregierung 1997). Mit der Benutzung existierender Gerätetypen würden die marginalen Kosten für die Zahlungs- oder Signaturfunktion minimiert (vgl. Pfitzmann et al. 1997, Weber 1997a).

6.1.2 Münzen in Chipkarten

Da Zahlungssystembetreiber ihre Karten weiterentwickeln wollen, sollte man untersuchen, ob mit teilbaren oder mehrfach verwendbaren Münzen nicht doch ein zählerloses System gebaut werden kann, bei dem nur einige wenige Transaktionen verkettbar sind. Verlusttoleranz wird jedoch immer noch schwer zu realisieren sein. Allerdings hätte man recht niedrige Kosten für Geräte auf der Kundenseite. Neue flexible Kartendisplays könnten die Transparenz auf der Kundenseite erhöhen.

6.1.3 Andere Lösungsansätze

Neben den zwei erwähnten Ansätzen wäre ein dritter Lösungsansatz, einen stärkeren Manipulationsschutz zu verwenden, und weniger auf Signaturen zu vertrauen. Es gibt Systeme mit batteriegestütztem RAM, gegen die keine Attacken bekannt sind (z.B. Cryptoboards von IBM). Heute sind solche Geräte dicker als normale Karten und sehr teuer, da in kleinen Losgrößen produziert. Aber dies könnte sich ändern. Eine vierte Möglichkeit wäre nach neuen kryptographischen Techniken zu suchen.

7 Ist elektronisches Bargeld realisierbar?

Selbst mit heutigen Techniken ist es möglich, in neue Zahlungsmittel Charakteristika wie Unverkettbarkeit, Transparenz und off-line Benutzbarkeit zu integrieren. Unverkettbare Systeme zum Beispiel wären

[13] In CAFE wurden nur wenige Transaktionen via Infrarot getätigt. Im Versuch der UBS in St. Moritz (1990) wurde ebenfalls eine Wertkarte mit Brieftasche (Adapter) benutzt, und zwar mit Radio-Interface. Beide Interfaces waren nicht sehr robust.

unserem heutigen Bargeld ähnlicher als existierende Kartensysteme. Wie die Diskussion der Trade-offs gezeigt habt, ist es jedoch eine Herausforderung für die Forschung, ein System zu bauen, das tatsächlich den Namen „elektronisches Bargeld” verdient.

8 Danksagungen

Die Autoren möchten David Chaum, Franco Furger, Tatsuaki Okamoto, Birgit Pfitzmann, Ingo Pippow, Jan Reichert, und Michael Waidner für viele anregende Diskussionen danken. Die Nutzerbefragungen wurden für das CAFE-Projekt gemacht. Die Autoren danken den Interviewern und den 300 Befragten (vgl. Furger et al. 1998, Weber 1995, Weber 1997b). Die vorliegende Arbeit wurde teilweise vom ACTS-Projekt SEMPER unterstützt, repräsentiert jedoch nur die Ansicht der Autoren.

9 Literatur

Anderson, Ross; Kuhn, Markus: Tamper Resistance - a Cautionary Note. The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, S. 1-11

Antwerpen, C. van: Electronic Cash. Master's thesis, Centre for Mathematics and Computer Science (CWI). Amsterdam 1990

Arthur, Brian: Competing Technologies, Increasing Returns, and Lock-In by Historical Events. In: Economic Journal 1989, S. 116-131

Asokan, N.; Janson, Phillipe; Steiner, Michael; Waidner, Michael: The State of the Art in Electronic Payment Systems. In: IEEE Computer 30/9 (1997), S. 28-35

Bos, Jurjen; Chaum, David; SmartCash: A Practical Electronic Payment System. Report CS-R9035, Centrum voor Wiskunde en Informatica. Amsterdam 1990

Bundesregierung, die: Signaturgesetz. In der Fassung vom 8. Oktober 1997. Verfügbar unter <http://www.bsi.de>

CAFE: The CAFE Consortium: Technical Specifications: Architecture and Protocols - Final Report Volume IIA, CAFE (Esprit 7023) Deliverable PTS9364, April 1996

Chan, Agnes; Frankel, Yair; Tsiounis, Yiannis: Easy Come - Easy Go Divisible Cash. Eurocrypt' 98, LNCS 1403, Springer-Verlag. Berlin 1998, S. 561-575

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. In: CACM 1981, S. 84-88

Chaum, David: Blind Signatures for Untraceable Payments. In: Advances in Cryptology, Proceedings of Crypto ‘82. New York 1983, S. 199-205

Chaum, David; Fiat, Amos; Naor, Moni: Untraceable Electronic Cash. In: Crypto '88, LNCS 403, Springer-Verlag. Berlin 1990, S. 319-327

Chaum, David: Achieving Electronic Privacy. In: Scientific American (August 1992), S. 96-101

Chaum, David, Pedersen, Torben: Transferred Cash Grows in Size. In: Eurocrypt '92, LNCS 658, Springer-Verlag. Berlin 1993, S. 390-407

Furche, Andreas; Wrightson, Graham: Computer Money: Zahlungssysteme im Internet; dpunkt Verlag. Heidelberg 1997

Furger, Franco; Paul, Gerd; Weber, Arnd: Survey Results. CAFE Project Report, 1998. Available at <http:/www.iig.uni-freiburg.de/~aweber/>

Mahony, Donal; Peirce, Michael; Tewari, Hitesh: Electronic Payment Systems, Artech House, London1998

Özalp, Nilgün: Entwurf von Benutzerendgeräten für elektronische Zahlungssysteme. Diplomarbeit, Fachhochschule Hildesheim/Holzminden 1996

Okamoto, Tasuaki; Ohta, Kazuo: Universal Electronic Cash. In: Crypto '91, LNCS 576, Springer-Verlag. Berlin 1992, S. 324-337

Pedersen, Torben: Electronic Payments of Small Amounts. In: Security Protocols 1996, LNCS 1189, Springer-Verlag, Berlin 1997, S. 59-68

Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael: Trusting Mobile User Devices and Security Modules. In: Computer 30/2 (1997), S. 61-68

Pfitzmann, Birgit; Waidner, Michael: Strong Loss Tolerance of Electronic Coin Systems. In: ACM Transactions on Computer Systems 15/2 (1997), S. 194-213

Schmidt, Jan; Schunter, Matthias, Weber, Arnd: Can Cash be Digitalised? In: Günter Müller, Kai Rannenberg (Hrsg.): Multilateral Security for Global Communication. Bonn 1999, i.E.

Weber, Arnd: Zur Notwendigkeit sicherer Implementation digitaler Signaturen in offenen Systemen. In: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997 (a), S. 465-478

Weber, Arnd: Soziale Alternativen in Zahlungsnetzen. Campus. Frankfurt, New York 1997 (b)

Weber, Arnd; Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael: Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet. Frankfurt 1995 (Project CAFE)