Raúl Rojas

Elektronisches Geld im globalen Datennetz

Kommerz im Internet

Das erstaunlich rasche Wachstum des Internets hat zu einem neuen Phänomen geführt: das globale Datennetz, ursprünglich nur für die Übertragung von wissenschaftlichen Daten entworfen, ist zum Medium für den Austausch von Waren und Diensten geworden. Das Netz ist zum wahren Markt evolviert, in dem, erstaunlicherweise, kein geeignetes Austauschmittel vorhanden ist. Es gibt keine sicheren statistischen Angaben über die im Internet getätigten Transaktionen, vor allem weil über das Netz meistens nur Angebote und Kataloge versandt werden; wirkliche Transaktionen werden dann durch Telefonanruf getätigt. Obwohl der neue virtuelle Marktplatz noch marginal zu den vorhandenen reellen Markplätzen ist, erlebt er ein Wachstum, das die noch vorhandenen Hindernisse beseitigen könnte. Die Firmen Visa und Mastercard schätzen deswegen, daß die Entwicklung des elektronischen Kommerzes bereits an einem »kritischen Scheideweg« angekommen ist (Visa, Mastercard 1996).

Wo es Waren gibt, entsteht früher oder später Geld – das allgemein akzeptierte Austauschmittel. Das ist jetzt der Fall im Internet, wo innerhalb von wenigen Monaten eine Lawine von verschiedenen elektronischen Geldvarianten entstanden ist. Die Situation ähnelt der Entstehung des Bankensystems in Europa während der Renaissance, als private Bankiers auf der Bildfläche erschienen sind und Papiernoten Münzen ersetzten. So wie später jede italienische Republik ihr Geld selbst druckte, so wie in Nordamerika im achtzehnten und neunzehnten Jahrhundert private Finanziers die Lücke füllten, die keine Zentralbank einzunehmen vermochte, so konkurrieren heute verschiedene Ansätze um die Vorherrschaft auf dem Gebiet der elektronischen Zahlungsmittel. D. Bennahum (1995) sieht darin eine Konfrontation, die dem wirklichen Krieg ähnelt – auf dem Spiel stehen möglicherweise Milliardenumsätze und die Gewinne, die die virtuellen Bankiers der Neuzeit als Vermittler einstreichen könnten. Die Teilnehmer reichen von großen etablierten Finanzinstitutionen wie Visa oder Citybank bis hin zu unbekannten Firmen, die bei dieser Goldgräberstimmung wie Pilze aus dem Boden geschossen sind. Es geht um enorme Beträge: Wür-

PROKLA. Zeitschrift für kritische Sozialwissenschaft, Heft 103, 26. Jg. 1996, Nr. 2, 227-240

den im Jahr 2000 25% der Rechnungen der Haushalte in den USA über das globale Datennetz bezahlt, würde sich dies auf 310 Mrd. US-Dollar im Jahr aufaddieren. Gerechnet wird auch mit großen Einsparungen, falls es gelingt, Münzen und Bargeld zu ersetzen. Drei Viertel aller Zahlungen werden gewöhnlich mit Bargeld beglichen. Die Kosten für Handel und Banken, die sich aus der Verwaltung des Bargeldes ergeben, sind für Europa auf 45 Mrd. US-Dollar geschätzt worden. Käufer, die statt Münzen Chipkarten verwenden, könnten zur Entstehung des *reibungslosen Kapitalismus* (Gates) beitragen.

Die große Frage bei dieser ganzen Entwicklung ist, wie die notwendigen Standards und die Interoperabilität der verschiedenen elektronischen Märkte garantiert wird. Dies ist keine einfach zu lösende Aufgabe, weil das Internet die nationalen Grenzen überschreitet. Es ist der Markt, der überall und doch nirgends ist. Wer soll Steuern auf die Transaktionen erheben? Wo werden die Geldflüsse letztendlich zum Ausgleich gebracht? Wer wird die Ausgabe des elektronischen Geldes überwachen? In welcher Währung werden die Transaktionen berechnet? Die Beauftragte des Büros für Technologieabschätzung in den USA, Linda García, hatte sicherlich recht, als sie bei einem Hearing im Amerikanischen Kongreß sagte, daß elektronisches Handeln »Raum und Zeit zwingt«. Es entsteht ein babylonischer Turm der Geldsysteme, der das präzise und über viele Jahre ausgearbeitete regulatorische Geflecht des internationalen Finanzsystems in einiger Zeit an unbekannte Ufer bringen wird.

Diese Problematik wollen wir in diesem Beitrag analysieren. Wir möchten aber zuerst erläutern, welche technischen Mittel sich hinter den vorgeschlagenen Methoden verbergen, um dann im letzten Teil des Aufsatzes auf die sozialen Konsequenzen zurückzukommen.

Der elektronische Marktplatz

Bis vor kurzem gab es keine sicheren demoskopischen Zahlen über das Internet und über sein Potential als zukünftiger Markt für Waren und Dienstleistungen. Vorhanden war nur eine Reihe von Netzumfragen und viele anekdotische Hinweise darauf, daß das Internet im Begriff war, zu einem echten Markt zu werden. Netzumfragen (d.h. solche, bei denen die Formulare über das Netz verschickt werden) haben jedoch den Nachteil, daß sie wenig repräsentativ für die Gesamtbevölkerung sein können. Neuere Erhebungen, die von einem Konsortium von amerikanischen Firmen finanziert wurden, zeigen jedoch, daß das Internet bereits zu einem interessanten Marktplatz geworden ist. Die von CommerceNet und Nielsen Media Research durchgeführte Haushaltsumfrage kam zu folgenden Ergebnissen (bezogen auf die USA und Kanada):

- 17% (hochgerechnet ca. 37 Millionen) der Personen über sechzehn Jahre haben Zugriff auf Internet (egal ob sie es regelmäßig nutzen oder nicht);
- 11% (ca. 24 Millionen) der Personen über sechzehn Jahre benutzten das Internet in den letzten drei Monaten;
- etwa 8% (ca. 18 Millionen) der Personen über sechzehn Jahre benutzten das World-Wide-Web (WWW) in den letzten drei Monaten;
- Internet-Benutzer sind im Durchschnitt 5 Stunden und 28 Minuten pro Woche im Internet (die meisten jedoch weniger als eine Stunde);
- Männer stellen 66% der Internet-Benutzer und verbrauchen 77% der Computerzeit;
- etwa 14% (ca. 2,5 Millionen) der WWW-Benutzer haben bereits Waren oder Dienstleistungen über das Internet gekauft.

Diese Ergebnisse (die in den USA teilweise skeptisch aufgenommen wurden) lassen sich natürlich nicht ohne weiteres auf Europa und andere Länder übertragen, aber durch das explosive Wachstum des Internets werden die demoskopischen Zahlen für Europa in wenigen Monaten auch ähnlich aussehen. Die Realität wird sicherlich die jetzige Statistik überholen.

Jetzt stellt sich natürlich die Frage nach der Zahlungsmethode, wenn diese breite Masse von Internet-Benutzern bereits Waren elektronisch bestellen kann. Das einfachste Schema besteht darin, die schon vorhandene Infrastruktur des Kredikartenverkehrs zu verwenden. Die traditionellen Kredikartenfirmen haben aber lange Zeit gezögert in den Internet-Markt einzusteigen. Der Grund liegt auf der Hand: Anders als die Geldautomaten oder die Point-of-sale-Geräte, die in dem privaten Netz der Banken integriert sind, besteht das Internet aus sehr verschiedenen Teilnetzen mit unterschiedlichen technischen Standards. Das Internet ist aber vor allem ein offenes Netz. Typische Internet-Übertragungen stellen ein nicht zu unterschätzendes Sicherheitsproblem dar, da eine elektronische Botschaft im Durchschnitt über 10 Rechner läuft und somit ohne großen Aufwand abgehört und kopiert werden kann. Das Internet ist in dieser Hinsicht unsicherer als ein Telefonanruf, der nur Käufer und Verkäufer verbindet (vorausgesetzt, die Telefongesellschaft lauscht nicht). Dies hat jedoch die Entstehung des ersten Internet-basierten Telebanking Systems nicht verhindert: im August 1995 öffnete die Security First Network Bank ihre Türen, deren Konten von den US-Bundesbehörden versichert sind.

Inzwischen ist im Internet eine neue Art der finanziellen Vermittlung zwischen Kunden und Kreditkartenfirmen entstanden. Kleine finanzielle Vermittler übernehmen die Funktion der sicheren Übertragung der Kreditkartennummer. Die einfachste Methode dafür ist die von First Virtual Holdings entwickelte, die im Oktober 1994 an den Markt (ans Netz) ging (Borenstein et al. 1995). Käufer und Verkäufer benötigen eine Registrierungsnummer (PIN) bei First Virtual – der Käufer deponiert seine Kredit-

kartennummer, der Verkäufer eine Kontonummer für Überweisungen. Der Käufer bestellt per elektronischer Post oder mittels des WWW's und der Verkäufer gibt die Rechnung an First Virtual weiter, diese fragt den Käufer zurück, ob die Transaktion durchgeführt werden soll (über E-Mail) und leitet die entsprechende Kreditkartenzahlung in die Wege. Einziger Vorteil des Systems ist, daß keine Kreditkartennummer, sondern nur der vereinbarte PIN über das Netz fließt. Die finanziellen Vermittler sind eine Art verlängerter Arm der Kreditkartenfirmen und tragen zur Erhöhung der Transaktionskosten bei. In diesem Fall wollen wir nicht von elektronischem Geld sprechen, da nur die üblichen Kreditmechanismen verwendet werden. Andere Firmen, wie z.B. CyberCash, verschlüsseln die Kreditkartennummer des Kunden und leiten diese Information an die Kreditkartenfirmen. Der Käufer und der Verkäufer benötigen spezielle Software von CyberCash (eine elektronische »Brieftasche«), die die entsprechenden Kommunikationsprotokolle umsetzt. Der Verkäufer kann die Kreditkarten-Daten des Kunden nicht entziffern, sondern leitet sie an CyberCash, das die entzifferten Daten in das Netz der Banken und Kreditkartenfirmen bringt. Die Autorisierung für eine Transaktion sollte 15 bis 20 Sekunden dauern.
Sicherlich ist diese Art der finanziellen Vermittlung in Gefahr; spätestens dann, wenn Mastercard und Visa selbst ins Internet voll einsteigen. Daß aber der Markt in diese Richtung drängt, erkennt man aus den Erfahrungen von First Virtual, die mit ihrer Low-Tech-Lösung im Jahre 1995 alle sechs Wochen eine *Verdopplung* der Kundenbasis erlebte. Die Funktion der Vermittler könnte jedoch in der Zukunft darin bestehen, die Kreditkartenfirmen vor Internet und seinen technischen Unwägbarkeiten abzuschotten. Die Hauptschwierigkeit beim heutigen Kommerz im Internet sind die unterschiedlichen Standards, fehlerhafte Software und sogar ungeplante Ausfälle der Netzknoten (Borenstein et al. 1996). Außerdem sind, da die Benutzerbasis des Internet sich Jahr für Jahr verdoppelt, zu jedem gegebenen Zeitpunkt mehr als die Hälfte der Netzteilnehmer völlig unerfahrene Benutzer. Die Kreditkartenfirmen könnten deswegen entscheiden, die Internet-Dienstleistungen unabhängigen Tochtergesellschaften zu überlassen.

Digitales Geld

Andere Netz-Entrepreneurs haben Systeme vorgeschlagen, die echtes digitales Geld darstellen und die nicht an das Kreditkartengeschäft gekoppelt sind. Es wird dabei zwischen zwei Varianten des digitalen Geldes unterschieden: a) *Off-line-Geld* wird erzeugt (als eine Folge von Zahlen) und in speziellen Chipkarten gespeichert, die dieses Geld dann an andere Geräte übertragen können. Die Übertragung entspricht dem Akt des Geld-Ausgebens. Das ist die Methode, die z.B. von Mondex, einer Tochter der Nat-

West Bank in Großbritannien, vorgeschlagen wird. b) *On-line-Geld* dagegen wird interaktiv zwischen Kunden und Banken produziert. Bevor On-line-Geld akzeptiert wird, überprüft der Verkäufer bei der Bank, ob das Zahlungsmittel echt ist. Dies setzt voraus, daß alle Transaktionen innerhalb des Netzes verlaufen. On-line-Geld kann des weiteren *anonym* bzw. *teilweise anonym* ausgegeben werden.
Digitales Geld soll dieselben Funktionen wie traditionelles Geld übernehmen. Nach Okamoto und Ohta (1991) soll digitales Geld unbedingt folgende Eigenschaften besitzen. Es sollte a) ein sicheres Austauschmittel (unfälschbar); b) anonym (für spurlose Transaktionen); c) tragbar; d) unbegrenzt haltbar (bis es absichtlich vernichtet wird); e) allgemein anerkannt und f) off-line-fähig sein (d.h. es sollte möglich sein, das Geld auch ohne Verbindung zu einem Zentralrechner auszugeben). Außerdem sollte es einfach zu benutzen sein und in verschiedenen Denominationen existieren.
Digitales Geld ist aber nicht mehr an etwas Materielles gebunden, wie ein Geldschein, der schwierig zu fälschen ist, sondern es ist eine reine Zahl, eine Folge von Nullen und Einsen. Zahlen sind unbegrenzt haltbar und tragbar, sie existieren ja nur »virtuell«. Sie können aber nur allgemein als Geld akzeptiert werden, wenn es gelingt zu verhindern, daß sie nach Belieben erzeugt werden. Hier ist die Stelle, wo die moderne Kunst der Verschlüsselung geheimer Botschaften zum Zuge kommt. Wir müssen über Kryptographie reden, um das digitale Bargeld verstehen zu können.

Kryptographie und Digitale Signaturen

Kryptographie bildet die Grundlage eines jeden sicheren Systems für finanzielle Transaktionen (Kryptos bedeutet »verborgen« auf Griechisch). Kryptographische Methoden erlauben Information auf solche Weise zu chiffrieren, daß es für einen möglichen Angreifer praktisch unmöglich ist, aus dem chiffrierten den ursprünglichen Text zu rekonstruieren. Kreditkartennummer, Verträge oder »Signaturen« sollten auf öffentlichen Datennetzen, wie dem Internet, nicht im Klartext sondern nur chiffriert übertragen werden. Es sollte verhindert werden, daß Händler oder Dritte Kreditkartennummern aus dem Netz lesen und speichern, um damit möglicherweise betrügerische Transaktionen zu initiieren. Eigentlich sollten öffentliche Datennetze damit einen höheren Sicherheitsgrad als das übliche Verfahren der Telefonbestellungen erreichen können. Dies ist notwendig, da ein einziger erfolgreicher computerisierter Angreifer die Sicherheit von Tausenden von Bankkonten in Frage stellen könnte.
Moderne kryptographische Methoden arbeiten mit einem Schlüssel, der eine eindeutige Chiffrierung der Nachricht erlaubt. Besteht die Nachricht z.B. aus 1000 Nullen und Einsen, so kann der Sender (Alice) mit dem

Empfänger (Bob) vorher einen Schlüssel austauschen, der aus 1000 zufällig gewählten Bits besteht. Der Schlüssel darf keinem anderen bekannt sein. Alice chiffriert die Nachricht Bit für Bit dann so, daß, wenn das Schlüsselbit 1 ist, das Komplement des Nachrichtenbits übertragen wird (1 statt 0, oder 0 statt 1) und wenn das Schlüsselbit 0 ist, das unveränderte Nachrichtenbit übertragen wird. Ein möglicher Angreifer sieht über die Leitung nur eine Zufallsfolge von Nullen und Einsen und kann die Nachricht nicht rekonstruieren. Der Empfänger, also Bob, weiß jedoch, welche Bits vertauscht und welche ohne Änderungen übertragen wurden (da er den Schlüssel kennt) und kann die Nachricht ohne weiteres reproduzieren. Dieses Verfahren bietet absolute Sicherheit, hat aber den Nachteil, daß jedesmal ein neuer Schlüssel generiert und ausgetauscht werden muß. Soll der Schlüssel über ein Kommunikationsnetz übertragen werden, befinden wir uns wieder beim Anfangsproblem der sicheren Datenübertragung.

Dieses Grundproblem hat zu der Entwicklung von Chiffriermethoden geführt, die mit einem kürzeren Schlüssel arbeiten, die wiederholt für einzelne Blöcke der Nachricht verwendet werden. Es gibt symmetrische und asymmetrische Methoden. Symmetrische Verfahren arbeiten mit einem einzigen Schlüssel, der sowohl dem Sender als auch dem Empfänger bekannt sein muß. Der Schlüssel, mit dem die Nachricht chiffriert wird, ist auch der Schlüssel mit dem die Nachricht dechiffriert wird. Im Juli 1977 hat das National Bureau of Standards der USA nach langen Beratungen mit der National Security Agency das DES-Verfahren (Data Encryption Standard) zur offiziellen kryptographischen Methode für unklassifizierte binäre Daten erklärt. DES wurde somit in die Rolle des de-facto-Standards für kommerzielle Datensicherheit erhoben. Eine 64-Bit-Nachricht wird mit DES in eine 64-Bit-Chiffre verwandelt. In sechzehn aufeinanderfolgende Stufen werden die ursprünglichen Bits der Nachricht permutiert und ersetzt. Der Schlüssel, der die genaue Form der Permutationen und Ersetzungen festlegt, besteht aus 64 Bits, wobei nur 56 effektiv für die Chiffrierung verwendet werden. Die von DES erzeugte Chiffre kann mit einem Kasten verglichen werden, der die Daten verbirgt. Der vereinbarte Schlüssel kann den Kasten schließen und nur dieser Schlüssel kann den Kasten wieder aufmachen. Der Empfänger der Nachricht ist nach der Dekodierung sicher, daß nur der andere Besitzer der Schlüssel die Daten hat chiffrieren können, während der Sender sicher ist, daß nur der Empfänger den Kasten aufmachen kann.

DES wird heutzutage für die Verschlüsselung von kommerziellen Daten und auch für die Übertragung finanzieller Transaktionen verwendet. Spezielle, von dem National Bureau of Standards überprüfte Schaltungen, können in Echtzeit mehrere Millionen Bits pro Sekunde chiffrieren.

Der große Nachteil von Systemen, die einen einzigen Schlüssel verwenden, ist erstens, daß der Schlüssel ausgetauscht werden muß und zweitens,

daß für die sichere Kommunikation von einer Person mit 100 anderen Personen 100 Schlüssel ausgetauscht werden müssen. Will man z.B. die Kommunikation zwischen Käufer und Verkäufer chiffrieren, müßte jeder Käufer mit jedem Verkäufer einen persönlichen Schlüssel vereinbaren, ein offensichtlich aussichtsloses Unterfangen. Hier kommen kryptographische asymmetrische Verfahren mit zwei Schlüsseln zum Zuge. Sie wurden Mitte der siebziger Jahre eingeführt und haben das gesamte Gebiet der Kryptographie revolutioniert.

Die sogenannte »Public Key«-Kryptographie verwendet für die Chiffrierung und Dechiffrierung zwei unterschiedliche Schlüssel. Wesentlich dabei ist, daß die Nachricht in einem Kasten verborgen werden kann und daß er mit jedem der beiden Schlüssel zugeschlossen werden kann. Der Kasten kann aber nur *mit dem jeweils anderen* Schlüssel wieder aufgemacht werden. Bob kann z.B. Kopien des einen Schlüssels an jede andere Person geben (dieser Schlüssel wird dann als »public«, also öffentlich bezeichnet). Jeder kann etwas für Bob chiffrieren. Aber nur Bob kann den geschlossenen Kasten (d.h. die Chiffre) wieder aufmachen und zwar mit dem anderen, seinem »privaten« Schlüssel. Auf diese Weise braucht jede Person nur zwei Schlüssel. Der öffentliche Schlüssel wird wie im Telefonbuch allgemein zugänglich gemacht, der private Schlüssel wird dagegen geheim gehalten.

Das sogenannte RSA-Chiffriersystem (Rivest et al. 1978) arbeitet mit zwei Schlüsseln A und B. Kern des Verfahrens ist die Exponentiation des Datenblocks auf eine sehr hohe Potenz und das Durchführen einer sogenannten Modulo-Operation. Der öffentliche Schlüssel A dient als Exponent für die Chiffrierung. Das RSA-Verfahren hat sich in den letzten Jahren (in verschiedenen Ausprägungen) zum Standard auf dem Gebiet der Public-Key-Kryptographie entwickelt.

Eine interessante Anwendung der asymmetrischen Kryptographie sind digitale Signaturen. Wenn man heute ein Dokument unterschreibt, kann die Unterschift bei einer digitalen Übertragung (z.B. per Fax) retuschiert oder verfälscht werden. Eine digitale Signatur ist aber viel schwieriger zu fälschen. Dabei wird folgende Methode verwendet: Nehmen wir an, daß Alice ein Dokument übertragen und unterschreiben will. Nach dem Dokument sendet sie einen Klartext, z.B. ihren Namen N, und den chiffrierten dazugehörigen Text A(N). Alice verschlüsselt N mit ihrem privaten Schlüssel A. Bob entschlüsselt A(N) mit Hilfe des öffentlichen Schlüssels B von Alice (den er kennt). Falls das Resultat identisch mit N ist, kann er sicher sein, daß Alice diese Information erzeugt hat, da nur sie über den zum öffentlichen Schlüssel B komplementären privaten Schlüssel A verfügt. Kann der Chiffrieralgorithmus nicht geknackt werden, kann auch die digitale Unterschrift nicht verfälscht werden. Normalerweise wird der Text N eine enge

Beziehung zum unterschriebenen Dokument haben, so daß die digitale Unterschrift nicht ausgeschnitten und mit einem anderen Dokument übertragen werden kann.
Asymmetrische Kryptographie bietet deshalb eine einfache Methode für den Austausch von geheimen Nachrichten zwischen Netzteilnehmern. Das Verfahren ist umso sicherer, je länger die Schlüssel sind. Der Nachteil der asymmetrische Kryptographie ist der Aufwand für die notwendigen Berechnung. Heutige Chipkarten (Karten mit einem eingebauten Mikroprozessor) können sehr schnell mit dem DES-Verfahren umgehen, nicht aber mit den Public-Key-Algorithmen. Karten der sogenannten dritten Generation werden deswegen einen speziellen Prozessor nur für die RSA-Berechnungen enthalten.

Digitales Bargeld – blinde digitale Signaturen

David Chaum hat die Möglichkeiten des elektronischen Geldes einen Schritt weiter gedacht (Chaum 1985, 1992). Ein Nachteil des Zahlungsverkehrs auf der Basis von Schecks oder Bankkarten ist, daß die Banken oder Kreditkartenfirmen die Kaufgewohnheiten der Individuen beobachten können. Die Anonymität des Bargeldes bei kommerziellen Transaktionen geht verloren. Es wäre aber wünschenswert, den Zahlungsverkehr so zu gestalten, daß keiner, nicht mal die Banken, Informationen über bestimmte Personen sammeln könnten. Dies bedeutet, daß die traditionellen asymmetrischen Verfahren erweitert werden müssen.
Chaum ist es gelungen, einen Typus von Transformationen zu finden, der kommutativ mit dem Public-Key Chiffrierverfahren ist. Bevor wir dies weiter erläutern, stellen wir Chaums Idee des digitalen Bargeldes dar.
Falls Alice bei Bob etwas für 100 DM kaufen möchte, kann sie einen Scheck mit diesem Betrag ausschreiben, der ihre Zahlungsverpflichtung dokumentiert. Alice kann den Scheck chiffrieren und beides an Bob abgeben: den Klartext und die Chiffre. Die Chiffre ist in diesem Fall ihre digitale Signatur. Diese kann von Bob oder von der Bank anhand des öffentlichen Schlüssels von Alice überprüft werden. Die Zahlung kann erfolgen, aber die Bank hat die Transaktion beobachtet. Die Transaktion kann geschützt werden, wenn Alice folgendermaßen vorgeht: sie informiert die Bank, daß sie einen Scheck über 100 DM abgeben will. Die Nummer x für den Scheck, eine Zahl von z.B. 100 Ziffern, wählt sie selber mit der Hilfe eines Zufallszahlengenerators. Sie holt die digitale Unterschrift von der Bank als Garantie, daß Geld vorhanden ist, wobei die Bank über verschiedene digitale Unterschriften verfügt, je eine für Transaktionen über zum Beispiel 1, 5, 10 oder 100 DM. Bevor Alice aber den Scheck an die Bank reicht, verbirgt sie dessen Nummer in einem digitalen »Umschlag«. D.h.

die Daten des Schecks werden so verändert, daß die Bank den Scheck nicht lesen kann. Die Bank unterschreibt mit der 100-DM-Signatur (Verschlüsselung mit dem privaten Schlüssel der Bank für 100 DM), belastet Alices Konto mit 100 DM und gibt das Resultat der Berechnung zurück an Alice. Diese entfernt den digitalen Umschlag und hat jetzt einen Scheck, der überall akzeptiert wird, weil er, versehen mit der Unterschrift der Bank, äquivalent zum Bargeld geworden ist.

Chaum nennt dieses Verfahren »blinde« Signaturen, da die Bank nicht weiß, was sich in dem digitalen Umschlag verbirgt. Mathematisch gesehen ist das, was Alice an die Bank gibt, nicht der Klartext x, sondern eine Variante $g(x)$. Die Bank antwortet mit dem chiffrierten Text $f(g(x))$. Da f und g kommutativ sind, entspricht dies $g(f(x))$. Alice kann die Operation g invertieren, so daß sie ohne weiteres $f(x)$ berechnen kann. Die Funktion g kann eine Multiplikation mit einer Zufallszahl und die Inverse von g die Division mit derselben Zahl sein. Die Bank hat x mit ihrem privaten Schlüssel chiffriert, ohne x zu kennen. Darin liegt der Kern der Methode. Alice kann x und $f(x)$ an den Verkäufer weitergeben. Mit dem öffentlichen Schlüssel der Bank kann der Verkäufer $f(x)$ dechiffrieren, das Resultat mit x vergleichen und überprüfen, ob die Bank tatsächlich unterschrieben hat. Der Verkäufer muß aber sofort (über das Netz) das Geld bei der Bank deponieren, da sonst die Gefahr besteht, daß Alice das Geld zweimal ausgibt. Die Bank führt eine Datenbank über alle in Zahlung gegebenen digitalen Schecks (in diesem Fall wahre digitale Banknoten) und verhindert auf diese Weise die doppelte Ausgabe des digitalen Bargeldes. Das erzeugte digitale Geld ist also auf jedem Fall On-line-Geld. Es ist anzumerken, daß die Bank weiß, welche Noten an wen bezahlt wurden, nicht aber, wer sie ausgegeben hat.

Für David Chaum ist Anonymität des Zahlungsverkehrs ein sehr wichtiger Bestandteil der bürgerlichen Rechte. Dostojewski drückte einen ähnlichen Gedanken aus, als er schrieb: »Geld ist vermünzte Freiheit«. Deswegen sucht Chaum nach Lösungen für das komplizierteste Problem: die Verwaltung der Banknoten in der Zirkulation. Eine mögliche Alternative wäre, Alice mit einer elektronischen Brieftasche auszustatten, die vertrauenswürdig in dem Sinne ist, daß sie keine Doppelausgabe der generierten Noten erlaubt. Dafür muß die Elektronik für den Benutzer unzugänglich sein, sie muß sich sogar selbst zerstören, falls jemand versucht, Daten abzuzweigen oder die Elektronik zu verändern. Die Produktion solcher unangreifbarer Chips wird z.Z. eifrig untersucht. Das System von Mondex ist in diesem Sinne weniger raffiniert als das von Chaum und seiner Firma Digicash, da in den elektronischen Brieftaschen Geld geladen wird, das von der Bank generiert wurde. Beim Digicash-System entscheidet der Benutzer über die Seriennummer seiner »Münzen«. Jede Brieftasche wird damit zur Notenpresse und die Bank überwacht nur die Transaktionen. Beide Syste-

me benötigen jedoch, für die effiziente Abwicklung von Zahlungen, solche unangreifbaren elektronischen Zusätze.
Das NetCash-System von Medvinsky und Neuman (1993) ist sehr ähnlich zum Digicash-System von Chaum. Der wesentliche Unterschied ist aber, daß beide Autoren die Kommunikation zwischen den »currency servers« weiter spezifiziert haben. Im NetCash-System arbeiten mehrere solche Server und emittieren unterschiedliche Arten elektronischen Geldes. Der Wechsel von einer elektronischen Währung in die andere wird über die Server reguliert, was bestimmte zusätzliche Sicherheitsanforderungen an die Protokolle stellt. Das »verteilte Zahlungssystem« operiert mit ähnlichen Techniken wie verteilte Computersysteme.

Wachstum und Regulation des elektronischen Geldsystems

Der konservative Nationalökonom F. A. von Hayek hat sein Leben lang für eine Privatisierung der Geldausgabe plädiert: »Money does not have to be created legal tender by government: like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually suppressed it« (Hayek 1978). Hayek würde sicherlich elektronisches Geld als einen erneuten Beweis seiner Thesen ansehen. Jeder kann E-Geld produzieren und es entscheidet schließlich der Markt, ob das produzierte Geld als Zahlungsmittel anerkannt wird oder nicht.
Die Geldausgabe ist ein von der Zentralbank strikt regulierter Prozeß. In früheren Zeiten konnten Geldzeichen, d.h. Banknoten, nur zu dem Betrag emittiert werden, den die vorhandenen Goldreserven erlaubten. Es entspricht aber der Natur des Geldes, daß diese Golddeckung nicht zwingend notwendig ist. Eine Banknote kann die Bank als Kredit für Alice verlassen und zurückkehren als Einzahlung von Bob, der Alice bestimmte Waren verkauft hat. So lange der Hin- und Rückfluß der Banknoten dieser Logik folgen, so lange die Kette der Zahlungen nicht abbricht, so lange braucht die Goldreserve nicht angetastet zu werden und die Goldreserve kann rein fiktiv sein. Die Zentralbank sorgt dafür, daß die Zahlungskette nicht abreißt, indem sie Geld knapp hält und damit seinen Wert schützt. Deswegen können private Banken auch nicht beliebig viel Geld (in Form von Kreditlinien) in Umlauf bringen. Die von den Banken in Umlauf gebrachte Geldmenge darf einen bestimmten konstanten Faktor in bezug auf ihre Reserven nicht übersteigen. Dieser Faktor wird von der Zentralbank festgelegt, er wird in Zeiten der Inflation reduziert, um Geld aus der Wirtschaft zu entziehen und in Zeiten der Depression erhöht, um die ökonomische Aktivität mit einer Finanzspritze zu stimulieren. Die Zentralbank beobachtet die Geldmenge sowie eine Reihe anderer Indikatoren und entscheidet dann über ihre eigene Strategie.

Stellen wir uns aber jetzt vor, daß digitales Geld in einem öffentlichen Netz erzeugt wird. Dies wurde im Fall von Digicash in einem weltweiten Versuch gemacht, bei dem es darum ging, die Sicherheit des Systems zu testen. Es handelte sich natürlich um künstliches Geld, das nicht für echte Transaktionen verwendet wurde. Der Versuch hat aber bewiesen, daß das System funktioniert. Solange die Wirtschaft ein Zahlungsmittel akzeptiert, interessiert nicht, ob dieses Zahlungsmittel aus reinen Zahlen oder aus aufwendig gedruckten Scheinen besteht: beides ist Geld. Die Umlaufgeschwindigkeit des digitalen Geldes kann aber die Umlaufgeschwindigkeit der Banknoten um ein Vielfaches übersteigen. Digitales On-line-Geld kann sich in wenigen Millisekunden in Bewegung setzen. Tausende von Erzeugungs-Vernichtungs-Zyklen können in wenigen Minuten durchlaufen sein. Die traditionellen Überwachungsinstrumente der Zentralbanken scheitern an dieser Stelle, da die wöchentliche Überwachung der Geldmenge nicht mehr ausreicht.

Weitere Probleme sind die Souveränität der Geldausgabe und die grenzüberschreitenden Finanzflüsse. Die DM-Emission wird von der Bundesbank reguliert. Eine private Bank in Singapur kann aber entscheiden, Finanzinstrumente, die in DM notiert werden, zu emittieren, d.h. wahre elektronische Mark auszugeben. Die Bundesbank würde die Kontrolle über die Geldmenge verlieren, wenn viele ausländische Banken denselben Weg beschreiten würden. Das Problem wird aber zuerst die amerikanischen Finanzbehörden treffen, da der US-Dollar als Weltgeld eine privilegierte Stellung einnimmt und sein elektronischer Schatten überall zu finden sein wird. Bleibt das Problem der unkontrollierten Finanzflüsse. Wenn elektronisches Geld anonym über öffentliche Netze transferiert werden kann, dann gibt es eigentlich keinen Grund mehr, das eigene Konto nicht in dem Land zu halten, das die besten Zinsen zahlt. Steuern auf Zinsen könnten ganz vermieden werden, wenn nur das Geld auf der richtigen elektronischen Oase plaziert wird.

Ökonomen haben auch davor gewarnt, den vom Internet-Handel auf die Staatsfinanzen ausgehenden Effekt zu unterschätzen. In den USA sind Firmen, die Waren von einem Staat in einen anderen über Katalog verkaufen, von der Verkaufssteuer befreit. Den Staatsfinanzen entgehen auf diese Weise jedes Jahr Steuereinnahmen in Höhe von über 3,3 Mrd. US-Dollar. Es wird dafür plädiert, auch den Internet-Handel von der Steuer zu befreien, was zu einem weiteren »ökonomischen Kannibalismus« zwischen den Bundesstaaten führen könnte (CCER 1995). Es ist sowieso nicht klar, wie im globalen Datennetz überhaupt Steuern erhoben werden können.

Quo vadis digitales Geld?

Gerade die Finanzinstitute, die das Internet am Anfang als ein nettes, aber schließlich uninteressantes Experiment belächelt haben, versuchen heute mit aller Macht, die verlorene Zeit wieder wettzumachen. Zwei interessante Allianzen sind im Laufe der Jahre 1994 und 1995 entstanden: Visa entschied sich für die Definition eines Kommerzprotokolls in Zusammenarbeit mit Microsoft (*Secure Transaction Technology*, freigegeben in September 1995), während Mastercard dasselbe Projekt zusammen mit IBM und Netscape in Angriff nahm (*Secure Electronic Payment Protocol*, freigegeben in November 1995). Beide Konsortien haben jedoch letztendlich eingesehen, daß ein gemeinsamer Standard notwendig ist und haben Ende Februar 1996 das *Secure Electronic Transaction*-Protokoll (SET) angekündigt und für Kommentare freigegeben. SET arbeitet mit dem Public-Key Verfahren und benutzt unterschiedlich lange Schlüssel. Die Schlüssel werden von einer Hierarchie von Behörden mit einem Sicherheitssiegel (Zertifikat) vergeben. Der umfangreichste Teil des Protokolls behandelt die Ausstellung und Rückführung von Zertifikaten.

Das SET-Protokoll von Visa und Mastercard ist im Laufe seiner Entwicklung zu einem sehr umfangreichen Dokument geworden. Beide Firmen sind zentrale Akteure auf dem internationalen Finanzmarkt: zusammen haben sie etwa 800 Millionen Karten in Umlauf gebracht, die Umsätze über 700 Mrd. US-Dollar im Jahr 1995 generiert haben. Beide verfügen über ein weltumspannendes Netz von Geldautomaten, die auch im neuen Protokoll berücksichtigt worden sind. In dem Moment, in dem das endgültige Dokument verabschiedet wird, wird es über Nacht zum Standard für Kreditkartentransaktionen über öffentliche Datennetze. Die Softwareindustrie müßte dann mit Produkten reagieren, die den neuen Standard implementieren.

Ein Problem ist jedoch die Sicherheit des Schlüssels in einem symmetrischen Verfahren. Eine Gruppe von Kryptoanalysten hat berechnet, wie schwierig es ist, unterschiedlich lange Schlüssel für das DES-Verfahren durch Ausprobieren aller Möglichkeiten herauszufinden (Blaze et al. 1996). Sie kamen zu dem Ergebnis, daß es möglich ist, mit einer Investition von Zehntausend Dollar in spezielle schnelle Chips, einen 56-Bit-Schlüssel (wie für DES) in 18 Monaten zu berechnen. Mit einer Investition von 10 Millionen Dollar für spezielle Hardware wäre es möglich, den DES-Schlüssel in 6 Minuten zu berechnen. Deswegen empfehlen sie, die Bitlänge des Schlüssels bereits heute bis auf 75 Bits zu erweitern. Ein für die nächsten 20 Jahre sicheres System sollte sogar 90-Bit-Schlüssel verwenden. Die von der amerikanischen Regierung für den Export freigegebene Software, die mit 40-Bit-Schlüssel arbeitet, bietet deshalb praktisch keine Sicherheitsgarantie mehr. Dies wurde bestätigt, als zwei Studenten im Sommer 1995 die 40-Bit-

Schlüssel von Netscape mit einem Netzwerk von Workstations knacken konnten. Auch der RSA-Algorithmus ist bereits für Schlüssel von bis zu 425-Bit-Länge geknackt worden: Anfang 1994 wurden 600 Computer verwendet, um einen solchen Schlüssel zu berechnen. Schlüssel mit bis zu 512 Bits sollten bereits 10 bis 15 Jahre Computerzeit (in einem Netz) brauchen, um geknackt zu werden. Gewöhnlich werden deswegen heute 512, 768 oder 1024 Bits für den Schlüssel verwendet.

Die Sicherheit des digitales Geldes hängt jedoch nicht nur von der Länge der kryptographischen Schlüssel ab. Das System ist so vertrauenswürdig wie das schwächste Glied in der Kette. Sogar die Software, die die Transaktionen von der Kundenseite ausführt, sollte überprüft werden und ein Sicherheitssiegel bekommen. Sonst könnte spezielle Software die Tastatureingaben der Kunden beobachten und Kartennummer oder Schlüssel (über das Netz) beiseite schaffen.

Eine Variante für Zahlungen im Internet, die auch die Banken ins Spiel bringt, ist die von dem amerikanischen *Financial Services Technology Consortium* (FSTC) studierte Infrastruktur für elektronische Zahlungen. Die Hauptidee ist das Bankennetz, das seit Jahren effizient funktioniert, für die Abwicklung aller sicherheitsrelevanten Geschäfte zu verwenden und das öffentliche Netz nur für die Einreichung von Bestellungen und Bestätigungen zu benutzen, d.h. das Internet wird als eine Art schnelleres Fax benutzt. Käufer und Verkäufer unterhalten sich mit ihren jeweiligen Banken und diese bearbeiten den finanziellen Teil.

Eine weitere Reihe von Fragen können aber zu diesem Zeitpunkt noch nicht beantwortet werden. Wird digitales Geld, direkt von den Banken kontrolliert, sich so weit ausbreiten, daß es zum echten Konkurrenten der Kredikarten wird? Wird sich die Off-line- oder die On-line-Variante des digitalen Geldes durchsetzen? Für die erste Option spricht die Tragbarkeit und Bedienungsfreundlichkeit der ausgedachten Systeme; für die zweite Option spricht die erhöhte Sicherheit. Ein offenes Problem sind auch die sogenannten »micropayments«, d.h. Gebühren die unter einem Pfennig bleiben. Sie könnten für die Übertragung bestimmter Informationen erhoben werden (Literatursuche, Stadtinformationssysteme usw.) sind aber nur umständlich mit Kreditkarten zu begleichen. Digitales Geld ist hier angebracht, jedoch erhöhen zu viele Mikrozahlungen den Verwaltungsaufwand unermeßlich, zumindest mit den heutigen Protokollen.

Viele Fragen, noch wenige Antworten – wir befinden uns erst am Anfang des Entstehens des elektronischen Finanzsystems der Zukunft. Welche Formen dieses annehmen wird, können wir noch nicht mit Sicherheit sagen. Interessanterweise können es die traditionellen Akteure, Banken und klassische Finanzinstitutionen auch nicht. Die selbstorganisierende Natur des internationalen Datennetzes ist mit den Selbstorganisationsprozessen

des globalen Marktes in Berührung gekommen. Die Geschichte kennt kein ähnliches Beispiel einer solchen Kollision.

Literatur

Bennahum, D. S. (1995): The trouble with e-cash, in: *Marketing Computers*, Vol. 15, N. 4, April 1995, S. 25.

Blaze, M. et al. (1996): Minimal Key Lengths for Symmetric Cyphers to Provide Adequate Commercial Security, Januar 1996, unveröffentlicht.

Borenstein, N. et al. (1995): Perils and Pitfalls of Practical CyberCommerce – The Lessons of First Virtual's First Year, in: *Frontiers in Electronic Commerce*, Austin, Texas, Oktober.

CCER (1995): Prop 13 Meets the Internet: How State and Local Government Finances are Becoming Road Kill on the Information Superhighway, Center for Community Economic Research, University of California, Berkeley, Pressemitteilung.

Chaum, D. (1992): Achieving Electronic Privacy, in: *Scientific American*, August, S. 96–102.

Chaum, D. (1985): Security Without Identification: Transaction Systems to Make Big Brother Obsolete, in: *Communications of the ACM*, Vol. 28, No. 10, Oktober, S. 1030-1044.

Hayek, F.A. von (1978): Denationalisation of Money – The Argument Refined, Institute of Economic Affairs.

Medvinsky, G.; Neuman, B. C. (1993): NetCash: A Design for Practical Electronic Currency on the Internet, in: *First ACM Conference on Computer and Communications Security*.

Okamoto, T.; Ohta, K. (1991): Electronic Digital Cash, in: J. Feigenbaum (Hrsg.), *Advances in Cryptology*, CRYPTO'91, Springer-Verlag, S. 324–350.

Rivest, R.; Shamir, A.; Adleman, L. (1978): A Method for obtaining digital signatures and public-key cryptosystems, in: *Communications of the ACM*, Vol. 21, No. 2, S. 120–126.

Visa, Mastercard (1996): Secure Electronic Transaction (SET) – Technical Specifications, Entwurf für Kommentare, Februar.