Die Elektronische Brieftasche
oder
Die Abschaffung des physischen Geldes

J.A.Makowsky

Department of Computer Science

Technion - Israel Institut of Technology

Die Natur des Geldes

Im Laufe der Zeit hat Geld sich entmaterialisiert: Waren es ganz früher Goldmünzen, so hat die Erfindung des Buchdrucks langsam die Ablösung der Goldmünzen durch Papiergeld ermöglicht. Langsam ist hier das wichtige Wort. Der Goldstandard wurde erst im letzten Jahrzehnt aufgegeben. 500 Jahre sind verstrichen von der technischen Realisierbarkeit des Papiergeldes bis zur vollständigen Verwirklichung dieses Konzepts. Dazwischen war Papiergeld lange Zeit nur ein Hilfskonstrukt, das erlaubte, Gold schneller und bequemer zu handhaben, Papiergeld als Goldersatz, jederzeit einlösbar bei der Bank. Dass das Privileg, Geld zu drucken, vom Staat monopolisiert wurde ist übrigens ebenfalls eine neuere Entwicklung. Dabei ist nicht zu übersehen, dass dieses Monopol nur beschränkt der Realität entspricht: Verschiedene Kreditsysteme, Wechsel, Bankobligationen werden de facto wie Geld gehandhabt und nicht vergebens vermerkt die Encyclopedia Britannica unter dem Stichwort "MONEY", dass Geld das Medium des Zahlungsverkehrs sei, dass aber mit dessen Definition grundsätzliche Schwierigkeiten verbunden seien. Die wesentlichen Merkmale des Geldes sind sicher seine absolute Konvertibilität, seine Anonymität und seine unmittelbare Verfügbarkeit. Wechsel, Cheques und Kreditkarten unterscheiden sich von Geld, obzwar in verschiedenem Masse, gerade in diesen Eigenschaften vom Geld.

Es liegt nahe, die Erfindung des Buchdrucks mit den neuen Erfindungen auf dem Gebiet der elektronischen Daten- und Textverarbeitung zu vergleichen. Auch diese eröffnet uns ganz neue Möglichkeiten nicht zuletzt auf dem Gebiet finanzieller Transaktionen. Schon "lange" werden Lohnzahlungen dadurch vorgenommen, dass den Banken Magnetbänder überreicht werden, die alle Zahlungen elektronische Speichern und zu gegebenen Daten die entsprechenden Transaktionen

aktivieren. Und nicht nur Lohnzahlungen, sondern alle grossen Interbanktransaktionen werden so durchgeführt, wobei sogar der physische Transport des Magnetbandes ersetzt wird durch elektronischen Datenfluss mittels Kabel oder Laserstrahl. Liegt es da nicht nahe, sich zu überlegen, ob solche Veränderungen nicht auch für den individuellen Geldbenützer nutzbringend und wünschenswert sind.

Die elektronische Brieftasche

Wir wollen hier eine Erfindung vorstellen, die es prinzipiell ermöglicht, Geld, im herkömmlichen Sinne, ganz abzuschaffen und durch Taschencomputer zu ersetzen, die, wie die Magnetbänder im Grossverkehr mit den Banken, alle individuellen Transkationen ausführen und speichern. Das Projekt heisst ELMON (electronic money) und wird von Prof. Shimon Even an der Abteilung für Informatik des TECHNION (Israel Institute of Technology) in Zusammenarbeit mit der Research and Development Foundation des Technions vorangetrieben. Kernstück des Projekts ist die ELEKTRONISCHE BRIEFTASCHE (electronic wallet), die von Prof. Even und seinen beiden Schülern Dr. O.Goldreich und Dr. Y.Yacobi erfunden wurde. Die Elektronische Brieftasche ist in den USA, Japan, Canada, Israel und verschiedenen europäischen Ländern zum Patent angemeldet, in den USA ist das Patentverfahren bereits eingeleitet.

Die elektronische Brieftasche gleicht in Form und Grösse einem herkömmlichen Taschenrechner mit Tasten und Anzeigefeld. Ihre Energieversorgung wird durch Batterien gewährleistet. Zwei elektronische Brieftaschen können direkt, mittels Licht emmittierenden und Licht empfindlichen Transistoren, Daten aneinander abgeben. Ihre Geometrie ist so beschaffen, dass sie Kopf an Kopf aneinander passen und in dieser Position, und nur in dieser, Datenaustausch möglich ist. Sie wird an Individuen entweder durch die Bank, eine Kreditkartenorganisation oder die Regierung (im folgenden kurz die Bank genannt) abgegeben. Dem Benützer wird ein Passwort gegeben und dieses muss dem Gerät jedesmal eingegeben werden, bevor ihm Daten entnommen oder durch es Transaktionen ausgeführt werden.

Will ein stolzer Besitzer einer elektronischen Brieftasche einem anderen eine Summe, sagen wir 128.50 Sfr., bezahlen, so tippt er sein Passwort ein, gefolgt von 128.50 Sfr. and dem Befehl PAY. Der potentielle Empfänger tippt nun in sein Gerät Passwort, 128.50 Sfr. und RECEIVE.

Jetzt stecken sie die beiden Geräte zusammen und sofort wird der Inhalt des Zahlenden Gerätes um die eingegebene Summe verringert und die des anderen um eben diese Summe erhöht. Beide Parteien erhalten zusätzlich, und das ist hier fast das Wichtigste, einen Beleg der Transaktion, der als rechtsgültige Quittung anerkannt werden soll. Die rechtsgültigkeit wird durch kryptographische Unterschrift und Handschlagprotokolle erreicht. Periodisch muss der Inhaber einer elektronischen Brieftasche bei einer Bank sein Gerät auftanken, indem er es an einen passenden elektronischen Schalter anschliesst. Letzteres kann auch via Telefon und Heimcomputer mit Zusatzgerät geschehen. Beim Auftanken liest die Bank alle seit dem letzten Auftanken vorgenommenen Transaktionen ab und leitet sie an die zentrale Datenverarbeitung weiter. Gleichzeitig übermittelt die Bank der Brieftasche neue Daten, wie den neuen Kontostand in der Brieftasche, Datum, Zeit, einige Kryptographische Daten und die neue Gültigkeitsfrist, nach welcher die Brieftasche spätestens wieder aufgetankt werden muss oder aber ungültig wird. Auch diese Operationen können rechtsgültig belegt werden. Ein Benützer wird zum Auftanken genötigt sein wenn entweder die Brieftasche zu voll oder nahezu leer ist, das Transaktionsgedächtnis nahezu voll ist oder wenn der Ablauftermin naherückt. Die zentrale Clearingstelle überprüft die Transaktionsdaten mit den entsprechenden Daten der Transaktionspartner auf Konsistenz und selbst bei Verlust einer Brieftasche sind die Transaktionen rekonstruierbar.

Bargeld und Kreditkarte in Einem

Die Vorteile der elektronischen Brieftasche gegenüber herkömmlichen Geld, Cheques und Kreditkarten sind sofort ersichtlich: Bequemlichkeit in Grösse und Aufwand, leichte Kontrolle des Kontostands, Schnelligkeit der Transaktion etc. Sie vereint damit, vom buchhalterischen Standpunkt aus alle Vorteile von Bargeld und Kreditkarte. Hinzu kommt aber als wesentlichste Neuerung die erhöhte Sicherheit vor Missbrauch, Fälschung, Diebstahl und Betrug. Das hier beschriebene System unterscheidet sich besonders darin von der in Frankreich eingeführten "Smart Card", als der Benützer (Konsument) genau kontrollieren kann, wieviel Geld aus seiner elektronischen Brieftasche genommen wird. Zudem sind Kontrollen, wie Rückruf bei der Kreditkartenorganisation, nicht nötig, da Echtheit und Validität ebenfalls via kryptographische Unterschrift überprüft werden kann. Selbst bei einander unbekannten Ausstellern der elektronischen Brief-

tasche, z.B. eine von der X-Bank in Israel eine von der Y-Bank auf den Bermudas, muss lediglich überprüft werden, ob der Israelische, respektive Bermudesische Aussteller die richtige Codenummer trägt. Es muss hierbei hervorgehoben werden, dass die Brieftaschennummer, im Gegensatz zur Kreditkarten oder Kontonummer, bei jedem Auftanken, ohne Mehraufwand gewechselt werden kann, was die Sicherheit zusätzlich erhöht und es erlaubt, je nach Wunsch, verschiedene Grade der Anonymität der Benützer zu gewährleisten. Letzteres ist besonders wichtig, um die psychologischen Barrieren der Angst zu überwinden, die hinter jeder neuen Anwendung der elektronischen Datenverarbeitung bloss die kalte Hand des "grossen Bruders" vermuten.

Kryptographie und Datenschutz

Diese Sicherheit wird gewährleistet durch Verwendung von modernsten Kryptosystemen, die auf dem Prinzip des offenen Schlüssels basieren. Diese Kryptosysteme haben in den letzten zehn Jahren das gesamte Gebiet der Kryptographie revolutioniert. Sie wurden vorallem in den USA und in Israel entwickelt, wobei dasjenige von Prof. M. Rabin (Hebräische Universität Jerusalem und Harvard University Cambridge, Ma) hier verwendet wird. Prof. S. Even und seine Partner, Dr. O. Goldreich und Y.Yacobi, selbst gehören auch zu den Koryphäen auf dem Gebiet der elektronischen Kryptographie.

Das Kernstück der elektronischen Brieftasche ist denn auch ein Mikrochip welches alle arithmetischen und kryptographischen Operationen zu vollziehen im Stande ist. Das schliesst die Multiplikation 1024-stelliger Zahlen in Sekundenbruchteilen mit ein, die für die gewünschte Sicherheit nötig ist, wenn das gesamte monetäre System der Bank davon abhängig ist. Die elektronische Brieftasche ist so konstruiert, dass jeder Versuch, in das Innere des Gerätes zu gelangen, automatisch alle relevante Information auf dem Chip zerstört. Aber selbst wenn es gelingen sollte, eine Brieftasche zu fälschen, so würden alle Kopien beim Verfallsdatum des Originals auch verfallen. Der Mikrochip ist auch mit einem Gedächtnis ausgerüstet, das erlaubt bis zu hundert Transaktionen zu speichern und das die kryptographischen Programme und Protokolle enthält, die von der Bank umprogrammiert werden können. Es ist auch vorgesehen, dass die Brieftasche sowohl als Uhr als auch als Taschenrechner benützt werden kann. Es ist auch möglich, sie zusätzlich als Taschenkalender auszurüsten.

Der Weg zur Realisierung

Es sieht also tatsächlich aus, als ob alle technischen Probleme gelöst oder lösbar seien, und sie sind es auch. Die Erfinder sind zuversichtlich, dass sie mit einem Aufwand von 2 1/2 Millionen US-Dollar und zwei Jahren Arbeit einen Prototyp herstellen können, der versuchsweise dem Publikum abgegeben werden könnte. Ist die neue Form von Geld einmal im Umlauf, so glauben sie, wird ihr Erfolg nicht mehr aufzuhalten sein. Alle Bestandteile des Mikrochips existieren bereits in verschiedener Form in den Designbibliotheken (Cell Libraries) und sogar auf dem Markt, und müssen nur noch geeignet zusammengestellt und dann miniaturisiert werden. Diese Arbeit ist nicht zu unterschätzen, stellt aber keine Anforderungen innovativer Art, die über das in der Mikroelektronik übliche technische Niveau hinausgeht.

Für die technische Produktion der elektronischen Brieftasche kommen vorwiegend Hersteller herkömmlicher Taschenrechner oder elektronischer Uhren in Frage. Je nach Geschmack kann das Äussere rein funtionell bestimmt sein oder aber schmuckmässig ausgestattet werden. Brieftasche für den Tag nüchtern sachlich, für den Abend diskret elegant mit Diamanten verziert. Man stelle sich vor wie Japanische Elektronik mit Schweizer Juwelierkunst hier zusammen ein neues Produkt lancieren könnten....

Und warum ist die elektronische Brieftasche noch nicht auf ihrem Siegeszug durch die Welt, fragte ich Prof. Even in seinem Büro. Er gestand, dass er und seine Kollegen sich der marktpolitischen und psychologischen Probleme der Erfindung voll bewusst sind. Versuche, elektronisches Geld im eigentlichen Sinne in Umlauf zu bringen gab es bis jetzt zwar noch keine. Trotzdem wollte Prof. Even kurz die elektronische Brieftasche mit anderen, ähnlichen Ideen vergleichen. Die Banken benützen nun schon seit mehreren Jahren das System SWIFT (und andere) zur elektronischen Geldüberweisung. Diese System benützen alle kryptographische Protokolle welche Authentizität und Geheimhaltung garantieren, aber der Empfänger hat keinen Beleg, der vor Gericht rechtsgültig wäre. Im Interbankverkehr ist dies ja auch nicht nötig, da die Banken untereinander mehr Vertrauen aufbringen, als dies im Individualverkehr üblich und sinnvoll ist.

Troztdem ist die Idee elektronischen Geldes nicht neu. 1982 hat in den USA W.S. Powell eine "Gelduhr" patentieren lassen. Äusserlich gleicht diese Uhr dem hier beschriebenen System

insofern, wie ein Armbandrechner einem Taschenrechner gleicht. Sie unterscheidet sich aber von der elktronischen Brieftasche insofern, als sie keine kryptographischen Methoden verwendet, um Sicherheit zu gewährleisten. Zudem ist sie als Armbanduhr eben weniger handlich als das hier beschriebene, zwar grössere, aber ergonomischere Modell.

Professor Even glaubt, dass ein entscheidender Impuls für die Verbreitung seiner Erfindung vorallem von Seiten der Verbraucherorganisationen kommen sollte. Haben nämlich diese einmal verstanden, dass die elektronische Brieftasche vorallem dem Individuellen Benützer zum Vorteil gereicht und ihn vor Wuchergebühren und anderen Problemen mit Kreditkarten schützt, so werden diese sich von selbst zu Gunsten seiner Erfindung einsetzen. Pilotversuche können von Banken oder gar von Regierungen durchgeführt werden. Aber selbst eine Kreditkartenorganisation könnte dadurch versuchen, ihre Konkurrenten auszuboten. Das grösste Hindernis an der Einführung kryptographisch sicherer Systeme ist die Skepsis der meisten Menschen gegenüber mathematisch beweisbaren, der sinnlichen Wahrnehmung aber entzogenen Sicherheitsvorkehrungen. Das gilt ganz allgemein, sei es im militärischen oder im zivilen Bereich, aber ganz besonders wenn es um soetwas persönliches geht, wie unser gutes Geld.