Avoin Arkkitehtuuri Oy -
syysseminaari
16.9.2004

E – raha

Esa Kerttula, prof.
Lappeenrannan teknillinen yliopisto

Prof-Tel Oy
www.proftel.fi

Sisältö

- nykyiset maksujärjestelmät, ongelmat ja haasteet
- rahan (maksuvälineiden) kehitykseen vaikuttavia megatrendejä
- mitä on e-raha (e-cash, e-money)
  - suhde muihin e-maksumenetelmiin
  - esimerkkejä ja kokemuksia
- vaatimuksia e-rahalle
  - toiminnot ja teknologia
  - tietoturva, yksilönsuoja
  - lainsäädäntö, EU
  - vähän e-rahan taustalla olevasta crypto-teknologaista
- ongelmia ja haasteita, tulevaisuuden näkymiä

1. Nykyiset maksujärjestelmät

- Maksujärjestelmiä operoitu osana pankkipalveluja
  - perinteisesti pankeille varattu, etuoikeutettu asema (ainakin toistaiseksi)
  - maksujärjestelmät pankeille taloudellisesti kriittinen voimavara
  - vaikka järjestelmät toimineet huomaamattomasti ja luotettavasti, niissä on myös heikkouksia, mitkä voivat uhata jopa nykyisten palveluntarjoajien asemaa (pidemmällä aikavälillä)
- Erityisesti yleiset maksujärjestelmien palvelumallit (standardit) "vanhanaikaisia" ja kustannukset käyttäjille "keinotekoisen" korkeat
  - poikkeuksena pankkien sisäinen liikenne ja "high value" –transaktiot
  - huolestuttavampaa on, että jopa kansallisella tasolla maksu-järjestelmät yhä fragmentoituneempia
  - seurauksena, että pankkipalvelujen tehokkuus kärsii (legacy systems) ja jakelukustannukset korkeat verrattuna potentiaalisiin uusiin teknologioihin

- Boston Consulting Group:
  - worldwide domestic payments running at $1,800 Trillion per year (2001)
  - revenues (or costs to their users) to banking systems $200 Billion per year
  - additionally $168 Trillion cross-border transactions generating an additional $28 Billion per year in revenue
  - the total social costs (bank revenue plus payor and payee non-banking expences) higher still
    - for US alone totally $225 Billion per year, or
    - representing 3 % of GDP, or
    - over $3000 annually for family of four, or
    - another way to looking: the average cost of payment absorbs about 5 % of the value of an average consumer purchase

- pankkijärjestelmät globaalisti jäykkiä ja mono-polistisia (Suomi edistyksellinen ja edelläkävijä)
  - maksujärjestelmät suurin este sähköisen kaupankäynnin (e-commerce) yleistymiselle
  - 80 % kaikista Internet-ostoista maksettava luottokortilla
    - kustannustehottomin maksuväline
    - turvaton korttisiirto Internetissä
    - tilitykset paperimuodossa kokonaan Netin ulkopuolella (esim. APACS, concensus business)
    - ”settlement-days” (2-3 pankkipäivää), vrt. settlement in e-payments (max. few hours)
    - ei koske isoja transaktioita (lähes reaaliaikainen)
- ⇒ tilaa uusille e-payment -järjestelmille
- vrt. puhelin- ja postijärjestelmien monopolien purkautuminen ja uudet liiketoimintamallit

Payment costs

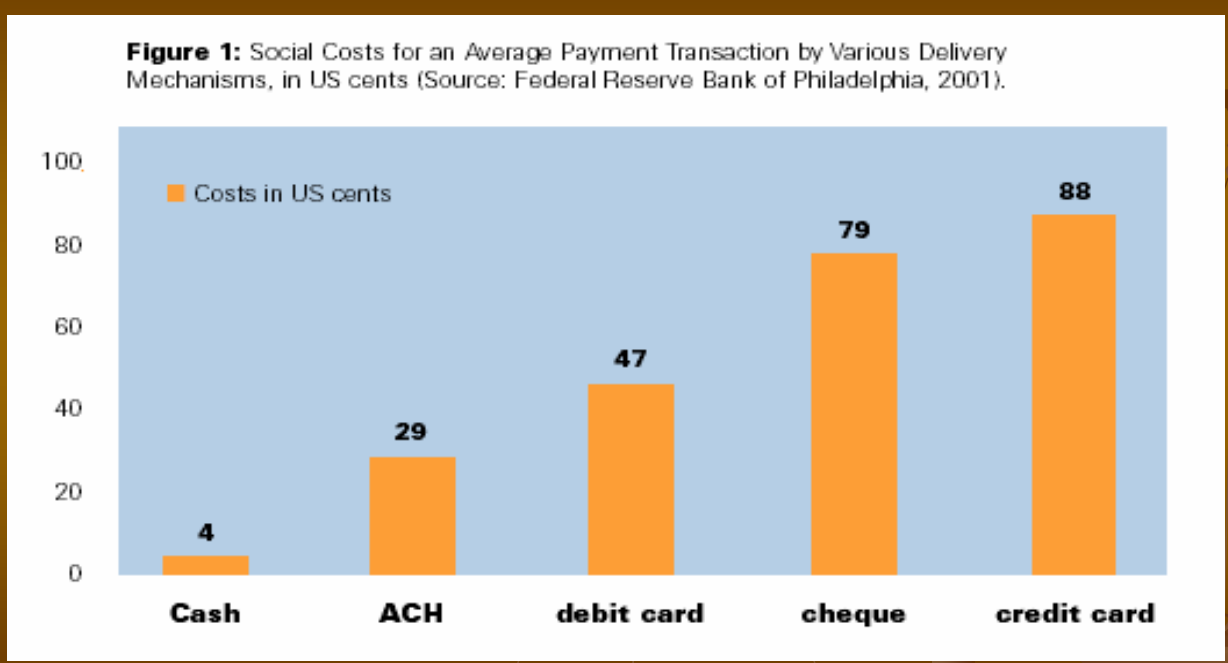
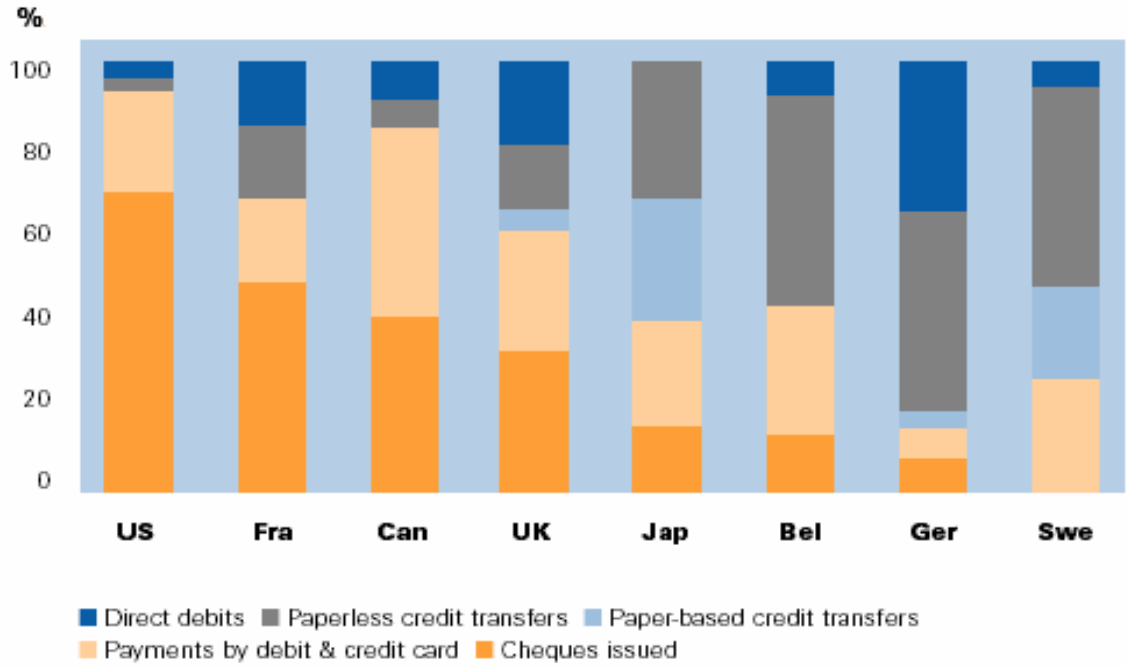


Figure 2: Use of cashless payment systems, by country, 1998.
(Volume in percent of total cashless payments) (Source: Bank for International Settlements).

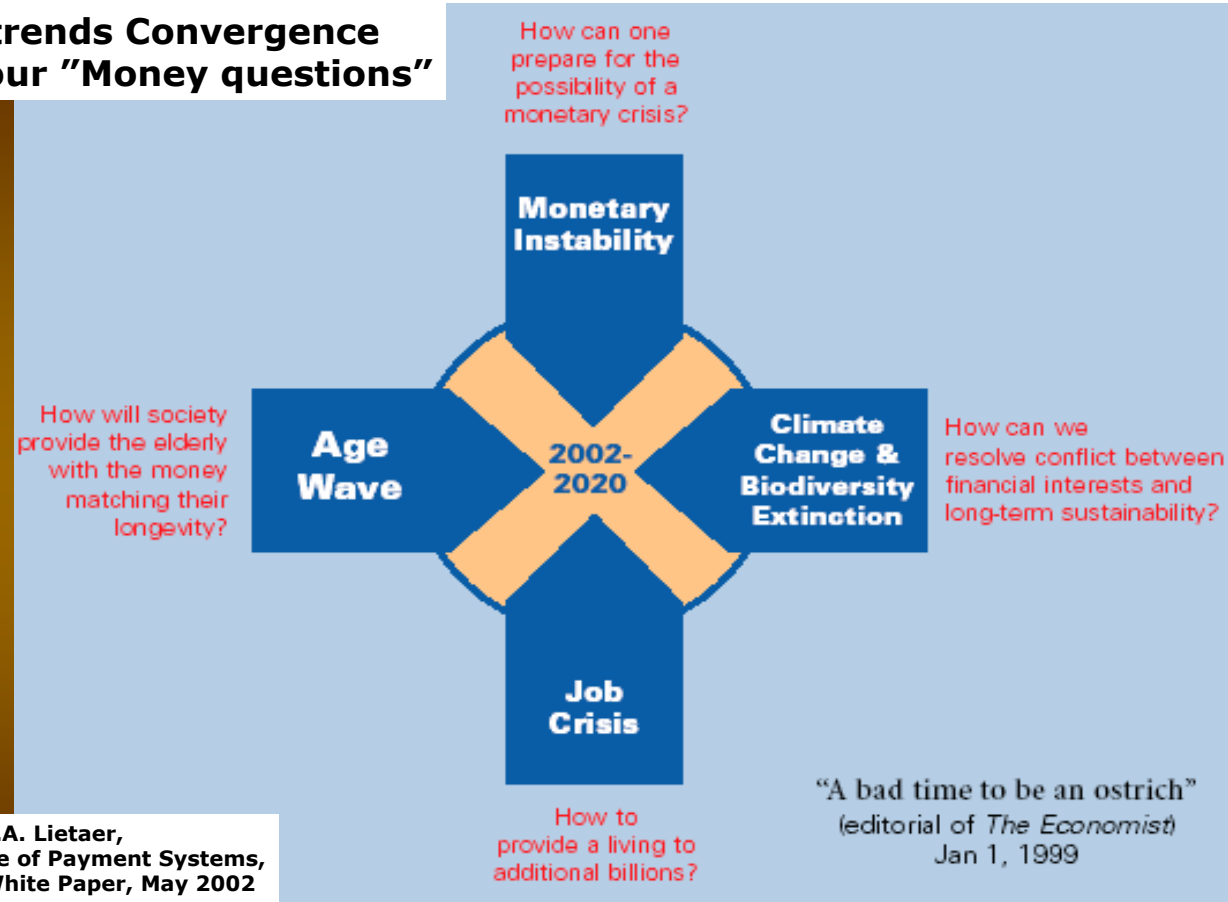


- **E-payments**
  - jo lyhyellä aikavälillä (1-5 vuotta) *e-market* evoluutio tulee generoimaan erilaisia *e-payment* –ratkaisuja, VÄISTÄMÄTÖN PAKKO !
  - tehokkaampia, täysin digitaalisia
  - painetta jo B2C –markkinasegmentissä riippumatta tuottaako e-payment –ratkaisuja pankit vai ei, esim.
    - stored value cards
    - PayPal (globaali)
    - mobiilit maksujärjestelmät
    - maailmalla satoja pilotteja ja akateemisia e-cash – ja muita e-payment -ehdotuksia
    - pohjoismaat kehittyneitä
      - esim. Nordea, OKO, Sampo

- B2B markkina kuitenkin tulee toimimaan strategisena vääntövartena
  - 3-5 vuoden kuluessa
  - yrityksille MUST
- *e-payment* –kehityksessä on erotettava
  - legal tender currency -kehityssuunta
    - kansalliset valuutat vaihtovälineenä
  - commercial private currencies -kehityssuunta
    - commercial loyalty currencies (Frequent Flyer Miles, kanta-asiakaskortit, jne)
    - *e-barter* -currencies
  - complementary currencies –kehityssuunta
    - normaali rahan kanssa rinnakkainen maksuväline
  - social purpose currencies -kehityssuunta

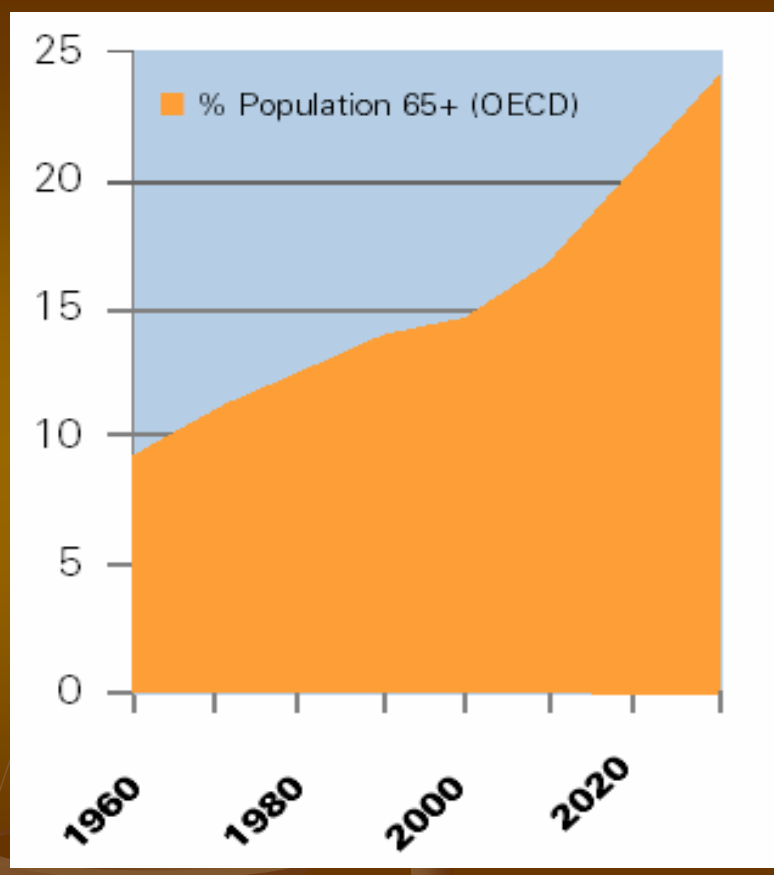
2. Rahajärjestelmien (valuutta) kehitykseen vaikuttavia megatrendejä

Megatrends Convergence
The four "Money questions"



Source: B.A. Lietaer,
The Future of Payment Systems,
UNISYS White Paper, May 2002

Population of 65 years or older (OECD) (1960-2030)

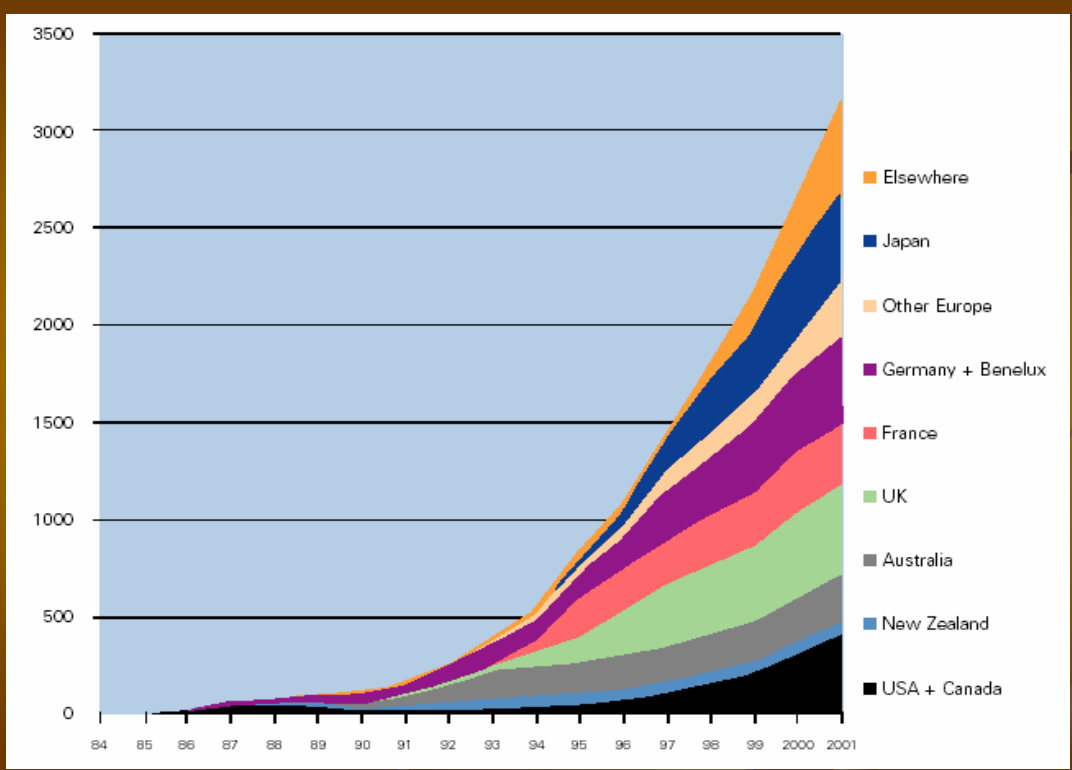


Source: B.A. Lietaer,
The Future of Payment Systems,
UNISYS White Paper, May 2002

Social purpose currencies

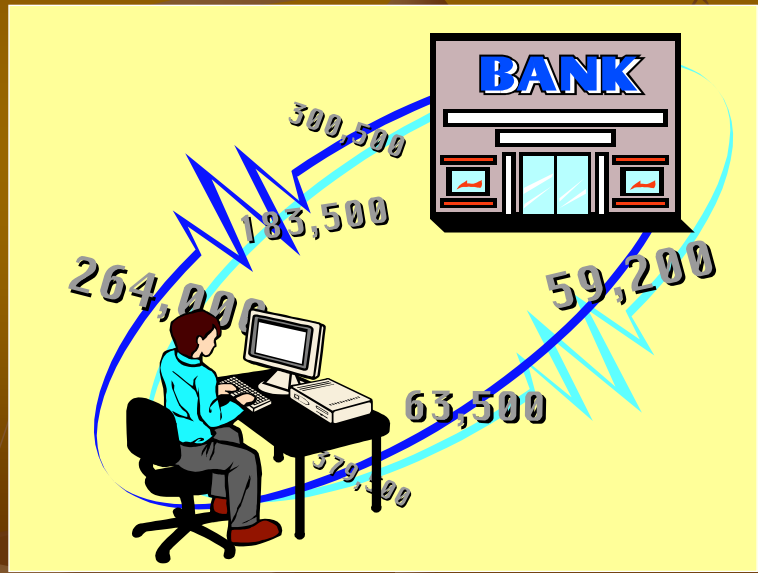
- yli 3000 järjestelmää ympäri maailmaa 15 vuoden aikana
  - ovat todistaneet että ”money” ei ole arvoneutraali
  - vaikuttamassa jopa yhteiskunnallisiin pitkän aikavälin megatrendeihin
- 95 % järjestelmistä tietokoneistettuja
- voivat ratkaista käytännön sosiaalisia ongelmia kuormittamatta suuremmin verottajaa ja valtion budjettia
- yleensä pienimuotoisia ja paikallisia järjestelmiä
  - ehkä kehittynein Sveitsin WIR (80,000 jäsentä, joista 25 % pieniä ja keskisuuria yrityksiä, vuotuinen vaihto US $2 Billion)
  - *Hureai Kippu* -raha (Japani), 300 järjestelmää, vanhukset käyttäjinä
    - käytetään mm. korvauksiin normaalivakuutuksen lisäksi

Number of Social Purpose Complementary Monetary Systems in some countires in 2001 (Source, *Future of Money*)



3. Mitä on e-raha

- Sähköiset maksujärjestelmät
- esimerkkejä



Maksujärjestelmät, yhteenveto

Maksu-tapa	Perinteinen maksuväline ja tapahtuman todentaminen	Sähköinen maksuväline	Esimerkki sähköisestä maksuvälineestä
Luotto	Myyjän ylläpitämä tilivelkaluettelo; tilinomistajan allekirjoitus	Kanta-asiakaskortin hallinta (numero + allekirjoitus)	S-etukortti, K-Plussa
	Luottokortti; kortin haltijan allekirjoitus veloitustositteeseen	Luottokortin numero + digitaalinen nimikirjoitus tai SET-varmenne	Luottokortit First Virtual
	Velkakirja (osamaksu/vekseli); velallisen allekirjoitus todistajin velkakirjassa		
Tilisiirto	Pankkisiirto; tilin käyttäjän allekirjoitus tilissiirtolomakkeeseen	Tunnusluku salasanalla ja yhteyskohtaiset, vaihtuvat tunnukset	Merita Solo, OP Kultaraha
	Shekki; tilin käyttäjän allekirjoitus shekkilomakkeeseen	(ei käytössä Suomessa)	(ei käytössä Suomessa)
Käteinen	Raha; maksuvälineen anonyymi luovutus	Elektroninen kukkaro	E-Cash, Mondex
	Postiennakko		
Muut		Esim. teleoperaattorin pitämä tilivelkaluettelo soitetuista puheluista; teleoperaattorin järjestelmään kirjautunut puhelu	

What is E-Money?

- E-Money or "electronic Money" is not "money" at all, but refers to payment products in which value transfer occurs in electronic media such as *mag stripes, computer chips, databases, and the internet*
- Many consider Charge and Credit Cards to be the first "E-money"
- Today, when we speak of E-money we mean new payment products that mirror traditional products in electronic media

What is E-Money?

- **"Old Economy" Forms**
- **"Pay Before"** - Cash, Travelers Cheques
- **"Pay Now"** - Debit Cards, Checks
- **"Pay Later"** - Charge and Credit Cards

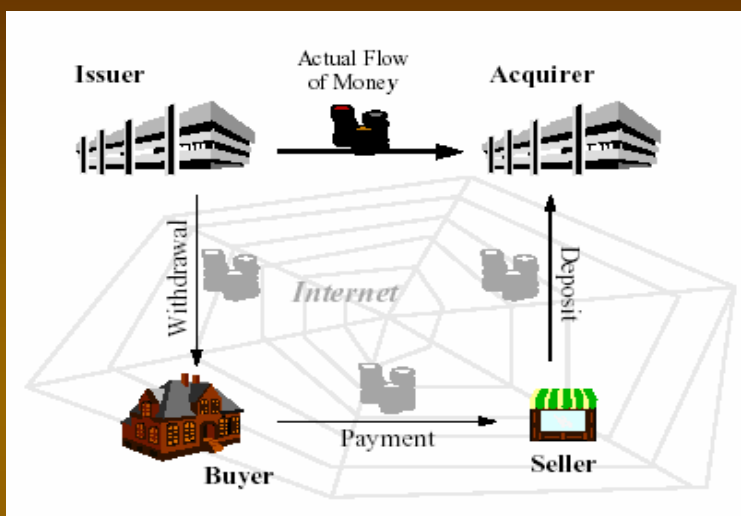
"New Economy" Forms

- **"Pay Before"** - Stored value cards, e-cash
- **"Pay Now"** - Internet Debit, Net-Checks
- **"Pay Later"** - Internet Credit products

What is Stored Value?

- A kind of e-Money – the "Pay Before" version
  - Typically, a consumer who purchases a Stored Value product, pays funds in advance, and those funds are held by the issuer of the product and are depleted as they are used.
  - Some Stored Value products aren't sold to consumers – they are like store coupons which are given to a consumer with some points/value preloaded, as an incentive for that consumer to shop at a particular store.

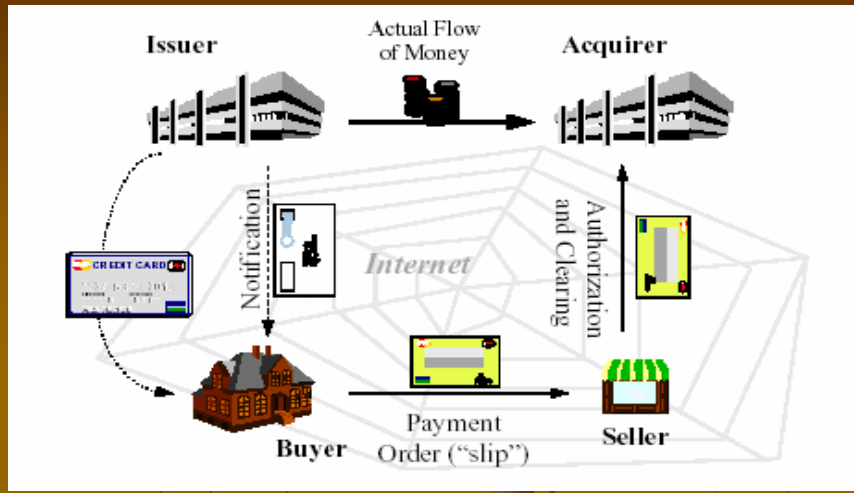
Cash-like Payment Systems



Before purchase money is withdrawn from the customer´s account and converted into electronic form

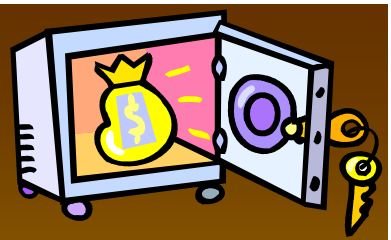
Examples:
- **e-cash**
- **certified bank checks**
- **e-purse (smart cards)**

Cheque-like Payment Systems



- "Pay now" systems: customer account charged at time of payment (e.g. EC card)
- "Pay later" systems: merchant account credited before customer account is charged (e.g. credit cards)

4. Vaatimuksia e-rahalle – building blocks



- Most payment systems are based on
  - asymmetric or symmetric cryptosystems
  - digital signatures
  - certificates (PKI)
  - secure hash-functions
  - security protocols
- Some on anonymity technologies
  - blinded signatures (e.g. that of Chaums)
  - digital credentials (e.g. that of Brands)
- Application of standards

Challenges

- e-cash
  - anonymity of customer
  - un-linkability of transactions
  - un-traceability of transactions
  - double spending of money
  - micro-payments
  - SSCD (Secure Signature Creation Device)
- infrastructure
  - EMV
  - ID management
    - e.g. Liberty Alliance
    - in B2B e.g. Tupas in Finland
    - PKI, e.g. FinEID
  - networking
    - Internet, mobile, Digital TV, voice

Esim. Elektroninen shekki

1) A new electronic check system with reusable refunds (presented by Hong Jiang)

Real-life check	E-check in this paper 1)
Not anonymous	Anonymous
Transactions are linkable	Transactions are unlinkable
Usually paid in the exact price of goods	Paid in a (pre-decided) check value and receive a refund check as change.
Post-paid	Pre-paid

Real-life cash	E-check in this paper
Fixed face values	Users decide the check values
Lifetime extends beyond a single transaction	Just for one transaction.
Can be used by any person, not resistant to theft.	Can only be used by the owner, resistant to theft.

Desirable properties

An ideal payment system is a divisible-cash system with the following properties:

- One coin is used for each payment.
- Subcoins are unlinkable.
- Protocols are computationally efficient.

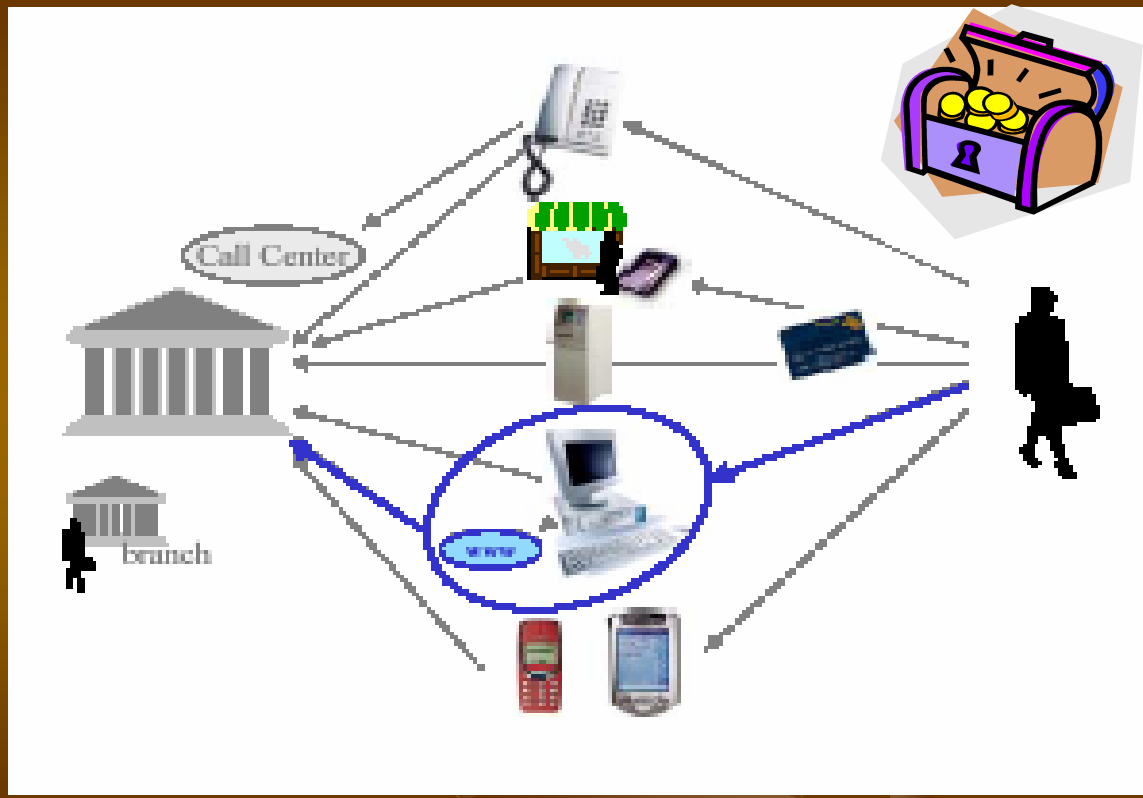
Not feasible with current technology . . .

Desirable properties

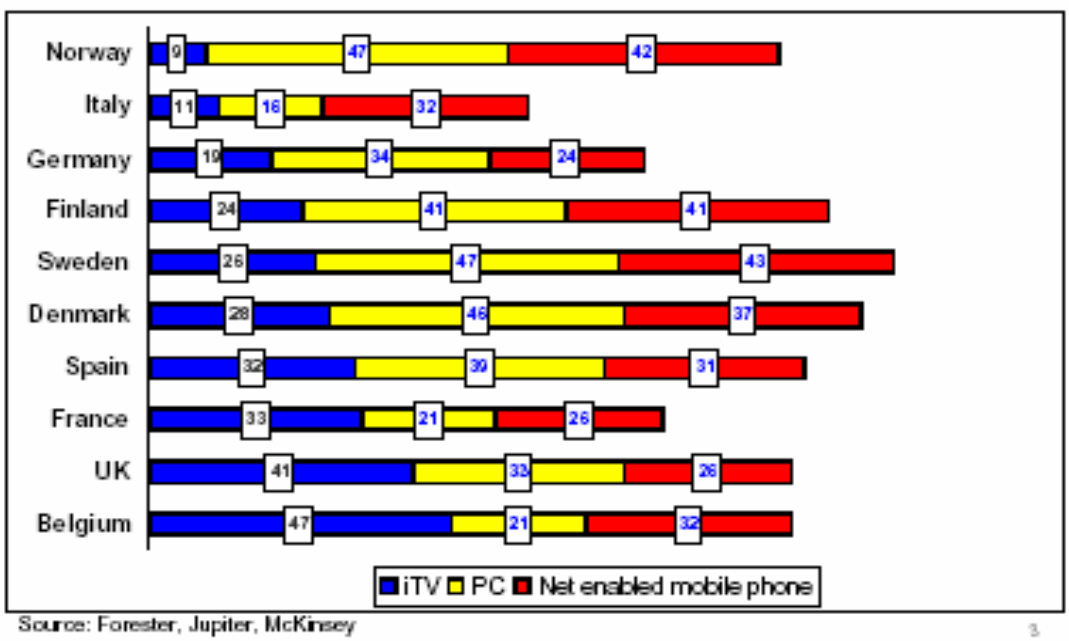
This paper describes an alternative solution:
A check system with an efficient reusable refund mechanism.

- A refund is unlinkable to the paid check.
- A refund check is reusable as payment
- Receiving a refund is efficient.

Esimerkkejä



Internet access in 2002, by device



Source: Forester, Jupiter, McKinsey

What is PayPal?

PayPal enables any business or consumer with email to send and receive online payments securely, conveniently and cost-effectively

- An account-based network which integrates with traditional payment systems
- The first global real-time payment system – available in 39 countries
- Focus on the underserved small business market, including online auctions
- Revenue derived primarily from Gross Merchant Sales (GMS)
- High variable revenue and low variable expense business model
- User-driven growth creates minimum reliance on traditional sales and marketing expenses
- Network effects which build on a large installed base – 15 million accounts

How Does PayPal Work?

Email Payments

PayPal

- Consumer signs up and enters credit card or bank account information
- Consumer enters email address of Merchant and dollar amount of payment

You've got money!

- Merchant receives an email indicating that Consumer has sent money
- Merchant may withdraw the cash, leave it in his PayPal account or send it to someone else

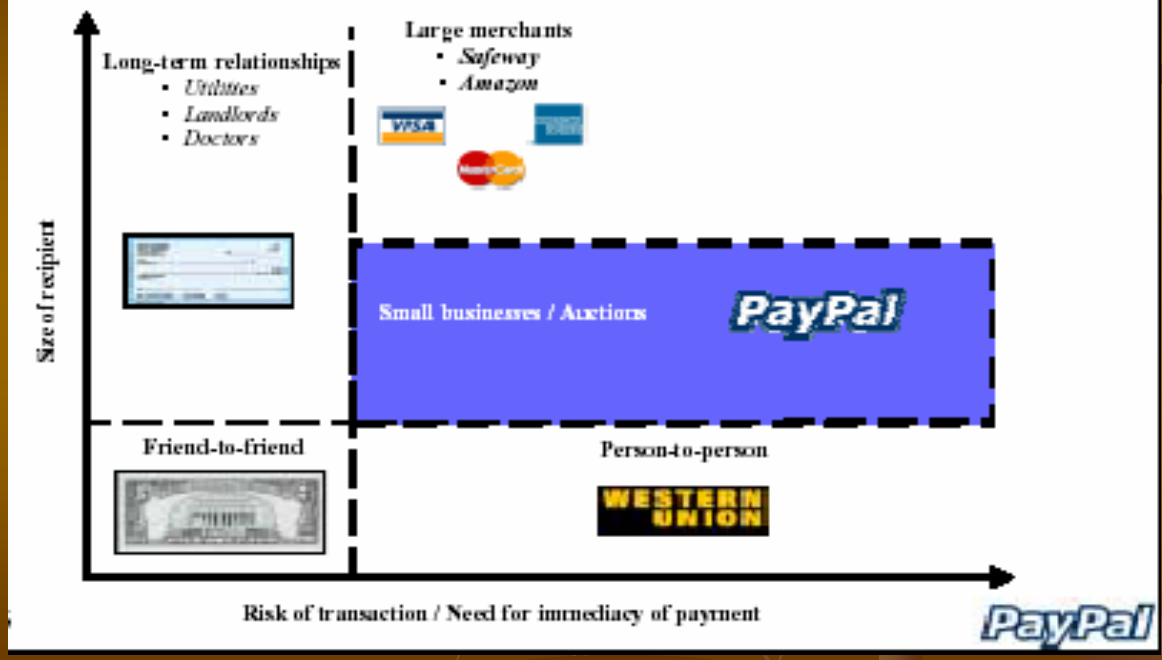
Web Accept Payments

PayPal CLICK HERE TO PAY

- Consumer, not yet a PayPal user, visits the website of Merchant, and selects goods or services to purchase
- From a pop-up window, Consumer opens a PayPal account and makes credit-card funded payment on one easy form

The Payments Market Landscape

Underserved Small Business Market Results in Attractive Margins



Why will Mobile Commerce happen?

- Always available
- Always with me
- Knows when / where I am
- Authenticates me

- Knows me / what I want
- It's mine
- It's unobtrusive

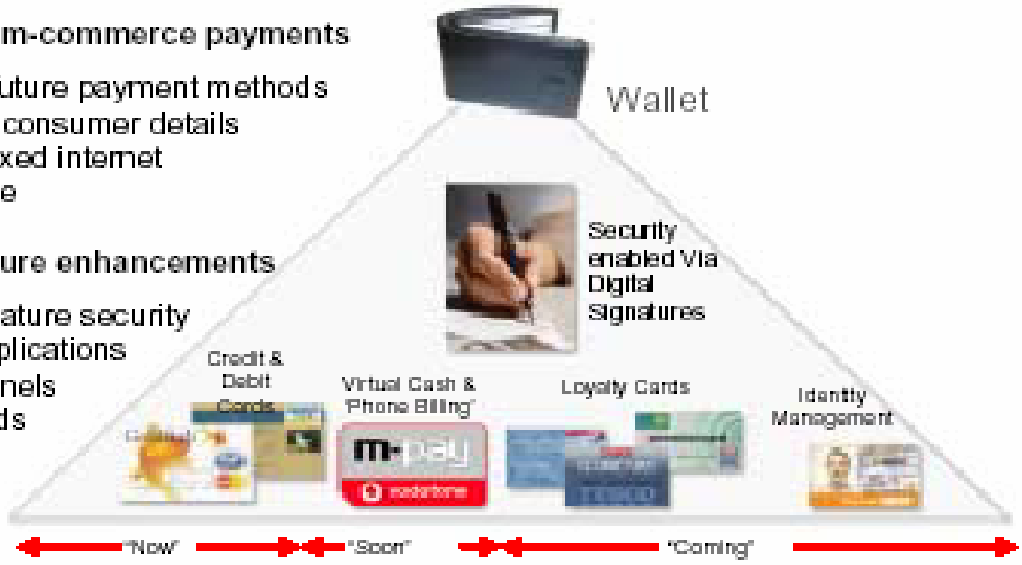
M-Payment Strategy

Convenient m-commerce payments

- current & future payment methods
- address & consumer details
- mobile & fixed internet
- pan-Europe

Possible future enhancements

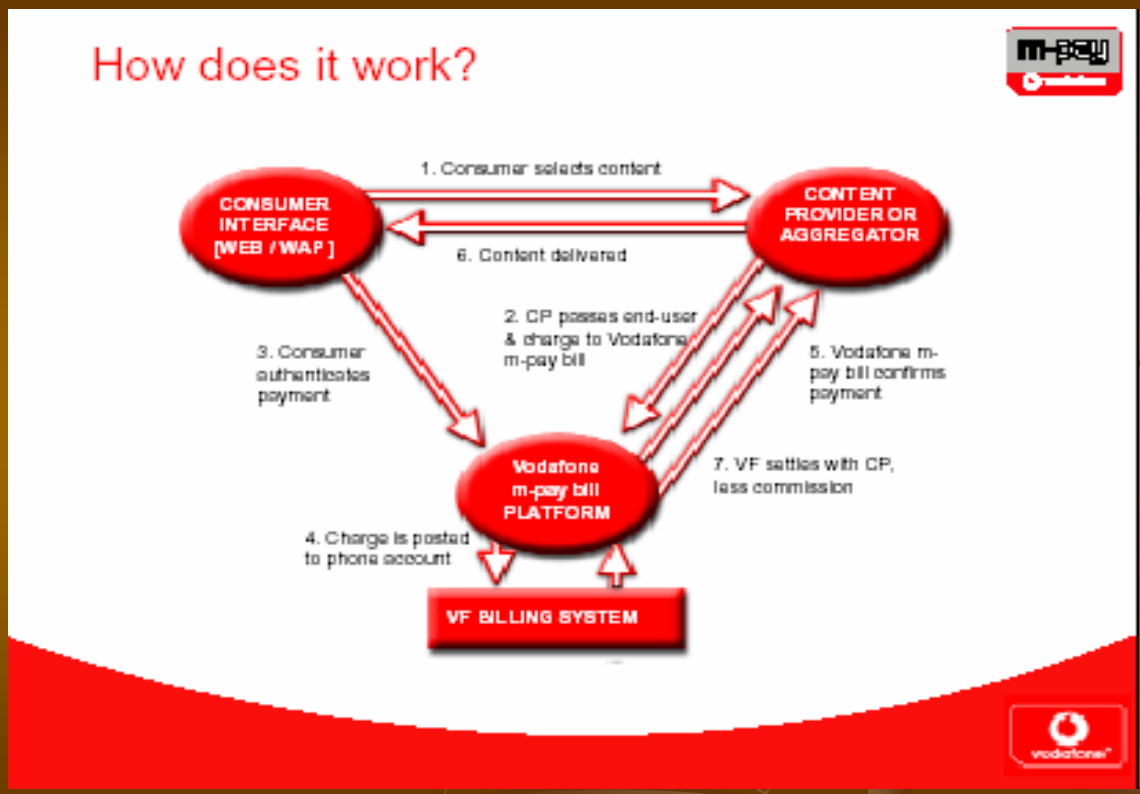
- digital signature security
- identity applications
- other channels
- loyalty cards



What does Vodafone m-pay bill do?

it allows Vodafone UK consumers to make remote micropayments by charging to their phone account

- micropayments of 5p to £5
- suitable for use on GSM, GPRS, 3G and the internet
- separating the cost of the content from the cost of carriage
- allowing Content Providers to set their prices and promotional deals

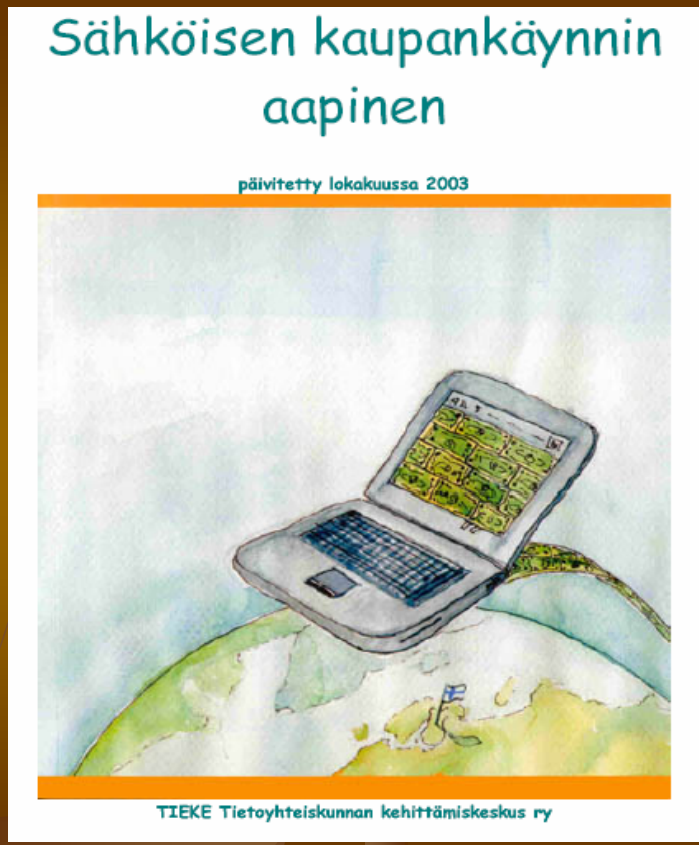


Lainsäädännöstä lyhyesti

Lähde: FiCom

- **Vuonna 2000 Euroopan unionissa hyväksyttiin sähköistä rahaa koskeva direktiivi.**
- **Direktiivin tarkoituksena oli tehdä ero talletustoiminnan ja sähköisen rahan välille ja antaa muillekin kuin pankeille mahdollisuus sähköisen rahan liikkeelle laskemiseen.**
- **Komissio miettii nyt, sovelletaanko sähkörahadirektiiviä myös matkaviestinyrityksiin. Suomessa taas on käynnissä juuri voimaan tulleen luottolaitoslain arviointi.**
- **Niin kutsuttuihin prepaid-liittymiin puheaika maksetaan etukäteen eli liittymään talletetaan arvoa, joka voidaan tulkita sähköiseksi rahaksi.**
- **Direktiivin säätämisen aikaan oli jo tavanomaista tarjota jälkikäteen laskutettavien puhelinliittymien rinnalla prepaid-liittymiä. Silloin ei ollut esillä eikä edes mielletty, että prepaid-liittymät rinnastettaisiin sähköiseen rahaan.**

Lisälukemista



Hieman e-rahan taustalla olevista uusista crypto-teknologioista

- **esitetään vain ”sokeutettu allekirjoitus”**
- **akateemisessa mailmassa esitetty satoja erilaisia ja uusiin innovaatioihin perustuvia toinen toistaan sofistikoidumpia e-cash –menetelmiä**
  - **kaikissa käytetään diskreettiä matematiikkaa ja monipuolisia crypto-protokollia**
  - **paljon patentteja**

Sokea-allekirjoitus

- Perustuu Chaumin -80 alussa kehittämään periaatteeseen
- Menetelmällä pystytään allekirjoituttamaan sanoma toisella osapuolella ilman, että itse sanomasta annetaan hänelle mitään informaatiota.
  - kirjoittaja ei tiedä mitä allekirjoitti, mutta pystyy todistamaan että on/ ei ole allekirjoittanut sitä
- Sovelluksia:
  - elektroninen raha
  - aikaleimapalvelut
  - anonyymit kirjautumiset

Chaumin sokea allekirjoitus

- Oletetaan., että A haluaa allekirjoituttaa B:llä asiakirjan ***m***
  - B:n julkinen avain on (***n, e***) ja salainen (***n, d***)
- A generoi satunnaisluvun ***r*** siten, että ***s.y.t (r,n) = 1***
  - => luvuilla *r* ja *n* ei ole yhteisiä tekijöitä
- A lähettää sanoman B:lle $m' = r^e m \bmod n$
  - => sanoma on "sokeutettu" satunnaisluvulla ***r***
- B allekirjoittaa sanoman $s' = (m')^d = (r^e m)^d \bmod n$
  - Koska $s' = r\, m^d \bmod n$ pystyy A selvittämään sanoman ***m*** allekirjoituksen poistamalla sokeutuksen $s = s'\, r^{-1} \bmod n$
- A:n sanomassa on aito B:n allekirjoitus ***s***, koska $s = s'/r = (r\, m^d) \bmod n = m^d \bmod n$

Sokean allekirjoituksen sovelluksia

- Sähköisen rahan omistaja yksilöi elektronisen rahan ja sokeuttaa sen Chaumin menetelmällä ja lähettää rahan takaisin pankkiinsa
- Pankki veloittaa summan asiakkaan tililtä ja leimaa rahan omalla salaisella avaimellaan ja palauttaa rahan takaisin asiakkaalle
- Asiakkaan järjestelmä poistaa sokeutuksen, jolloin hänellä on hallussaan pankin leimaamia rahaa, jonka alkuperäistä omistajaa ei voida jäljittää (rahan anonyymiys)
- Pankin saadessa rahan takaisin pankin on hyväksyttävä se

- Security Without Identification: Transaction Systems to Make Big Brother Obsolete. David Chaum in Communications of the ACM, Vol. 28, No. 10, pages 1030-1044; October 1985.

Security without Identification

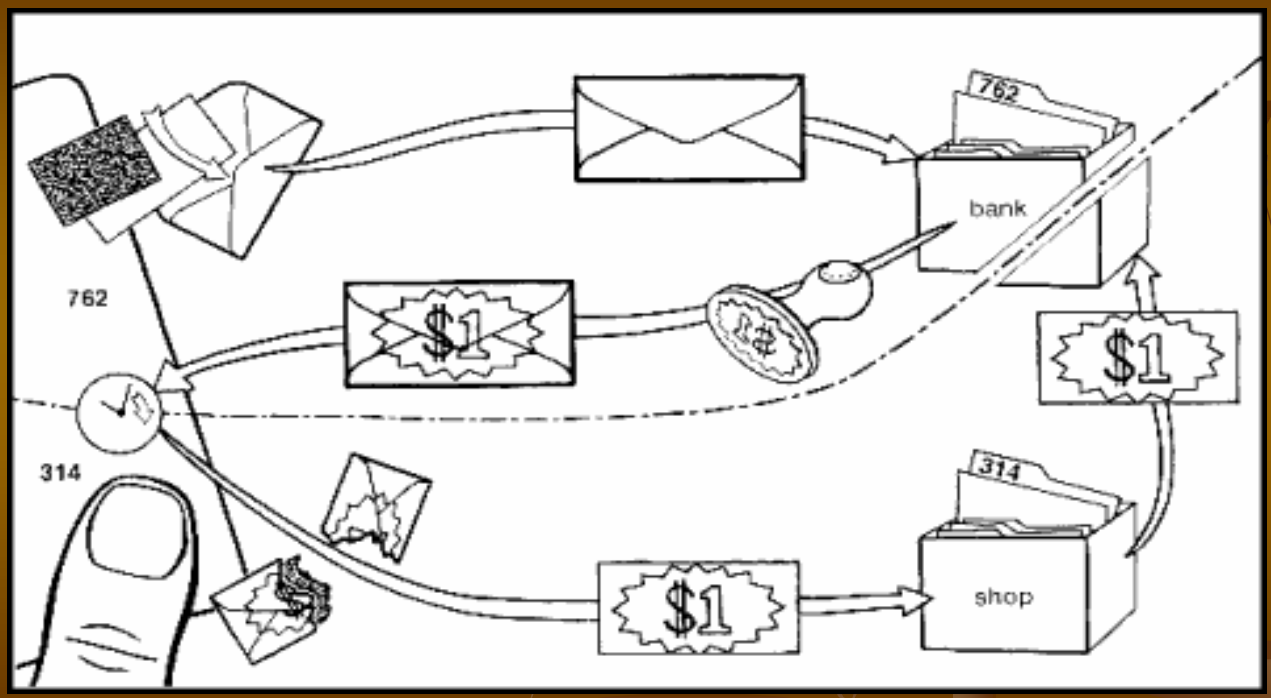
Card Computers to make Big Brother Obsolete

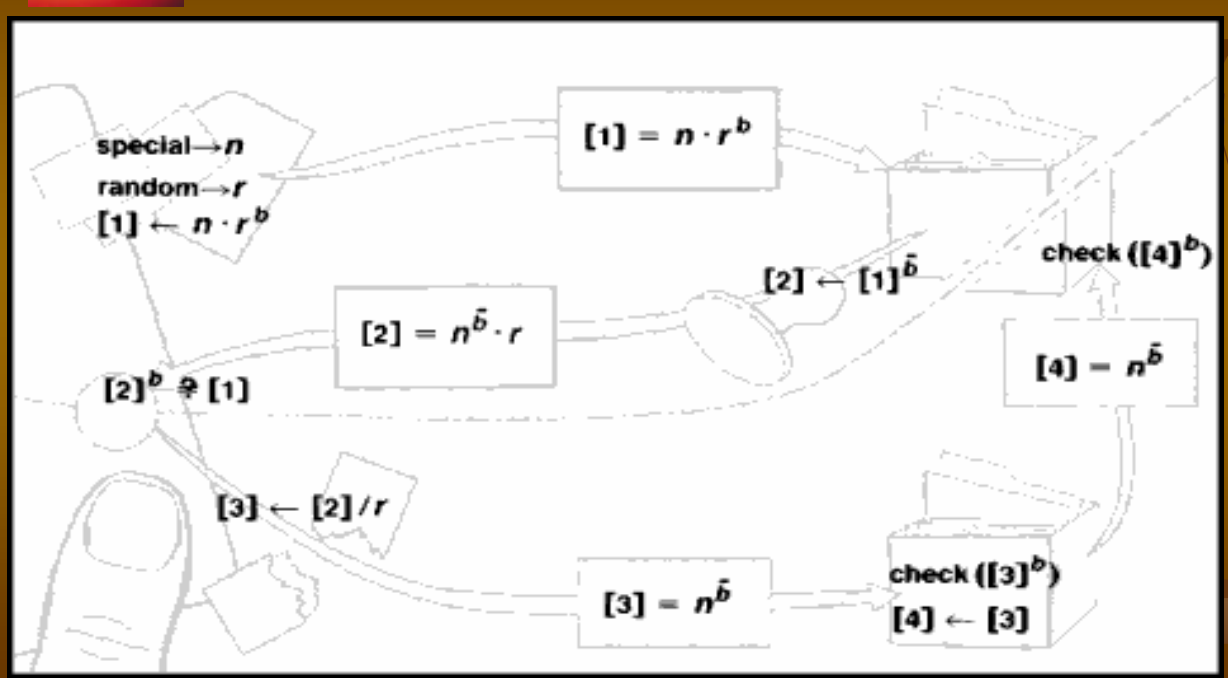
by David Chaum

You may soon use a personal "card computer" to handle all your payments and other transactions. It can protect your security and privacy in new ways, while benefitting organizations and society at large.

Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. Already, public and private sector organizations acquire extensive personal information and exchange it amongst themselves. Individuals have no way of knowing if this information is inaccurate, outdated, or otherwise inappropriate, and may only find out when they are accused falsely or denied access to services. New and more serious dangers derive from computerized pattern recognition techniques: even a small group using these and tapping into data gathered in everyday consumer transactions could secretly conduct mass surveillance, inferring individuals' lifestyles, activities, and associations. The automation of payment and other consumer transactions is expanding these dangers to an unprecedented extent.

Organizations, on the other hand, are attracted to the efficiency and cost-cutting opportunities of such automation. Moreover, they too are vulnerable, as when cash, checks, consumer credit, insurance, or social services are abused by individuals. The obvious solution for organizations is to computerize in ways that use more pervasive and interlinked records, perhaps in combination with national identity cards or even fingerprints. But the resulting potential for misuse of data would have a chilling effect on individuals. Nevertheless, this is essentially the approach of the electronic payment and other automated systems now being tried. Although these systems will require massive investment and years to complete, their underlying architecture is already quietly being decided and their institutional momentum is growing.


762
bank
762
$1
$1
314
314
$1
shop


special→n
random→r
[1] ← n · r^b
[1] = n · r^b
[2] ← [1]^b̄
check ([4]^b)
[2] = n^b̄ · r
[4] = n^b̄
[2]^b ≠ [1]
[3] ← [2] / r
[3] = n^b̄
check ([3]^b)
[4] ← [3]

5. Ongelmia ja haasteita, tulevaisuudesta

- mikä taho tulee toimimaan ”driverina” ?
  - pankit
  - hallinnot
  - yksityiset organisaatiot
  - vaihtoehtoisten maksujärjestelmien rooli ?
- kuka maksaa kustannukset
  - käyttäjä ?
  - kauppias
  - infran tarjoaja (pankit, operaattorit)
- standardit ja teknologia
  - mikä teknologia voittaa ?
- e-payment tulee kuitenkin varmasti (myös e-cash)
  - milloin, kehitys hidasta ?

Viva the cashless society!

Well, let’s at least
start thinking about it ...


SPARE
CHANGE
NO
SMART
CARDS


SMART
CARDS
NO
SPARE
CHANGE