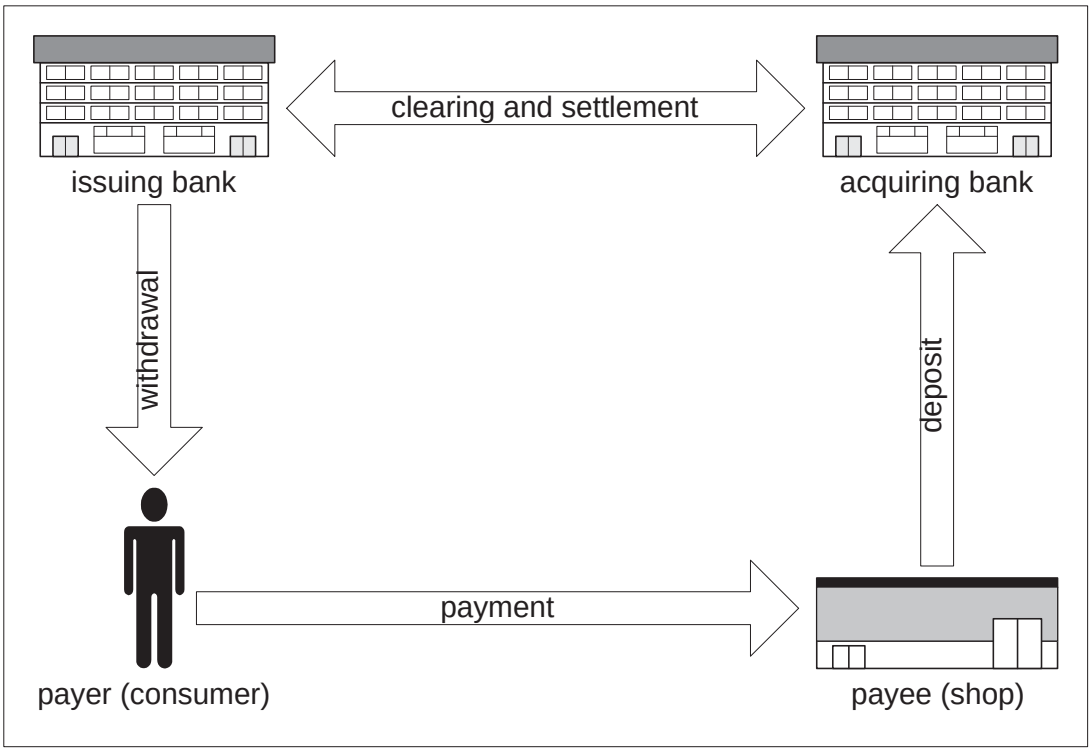
Cryptography 2, Part 2, Lecture 6
Electronic Payment Systems

Benne de Weger
b.m.m.d.weger@tue.nl

TU/e

June 11, 2012

Payment Model

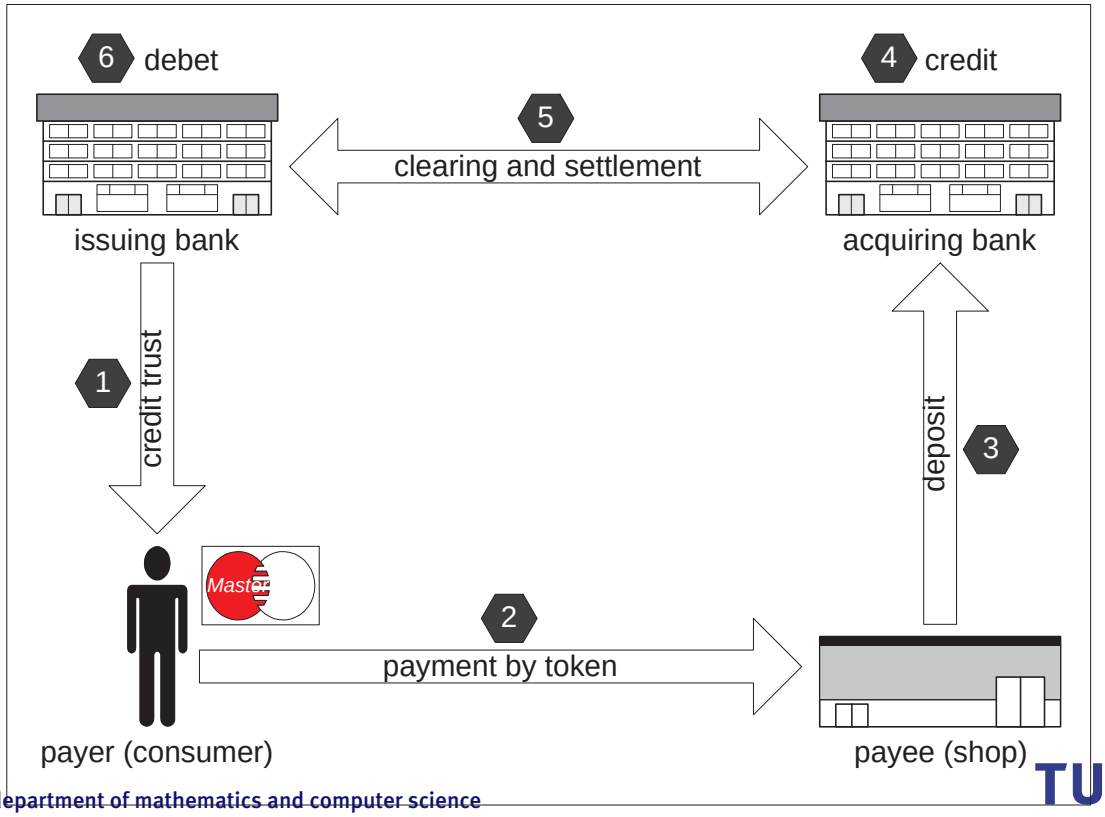


Properties / Requirements of payment systems

- creation of money only by designated parties
  - counterfeiting: illegal creation of 'new' money
  - copying, forging: illegal copying, forging of existing money
- users can only receive, possess (and protect ownership of) money, and transfer (pay, spend) existing money
- money transfer may require one-sided or two-sided authentication
- payment data may be confidential
- anonymity, untraceability and unlinkability of transfers may be required

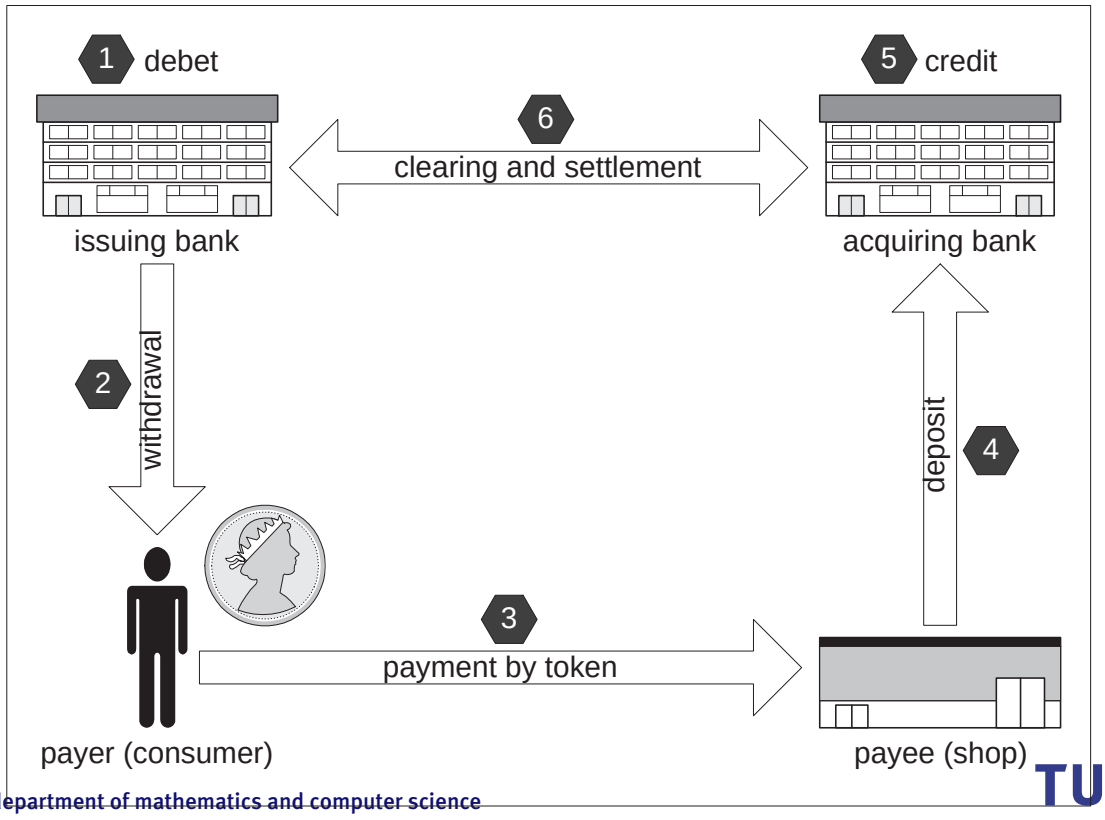
Credit Payment Model

account based, credit before debet



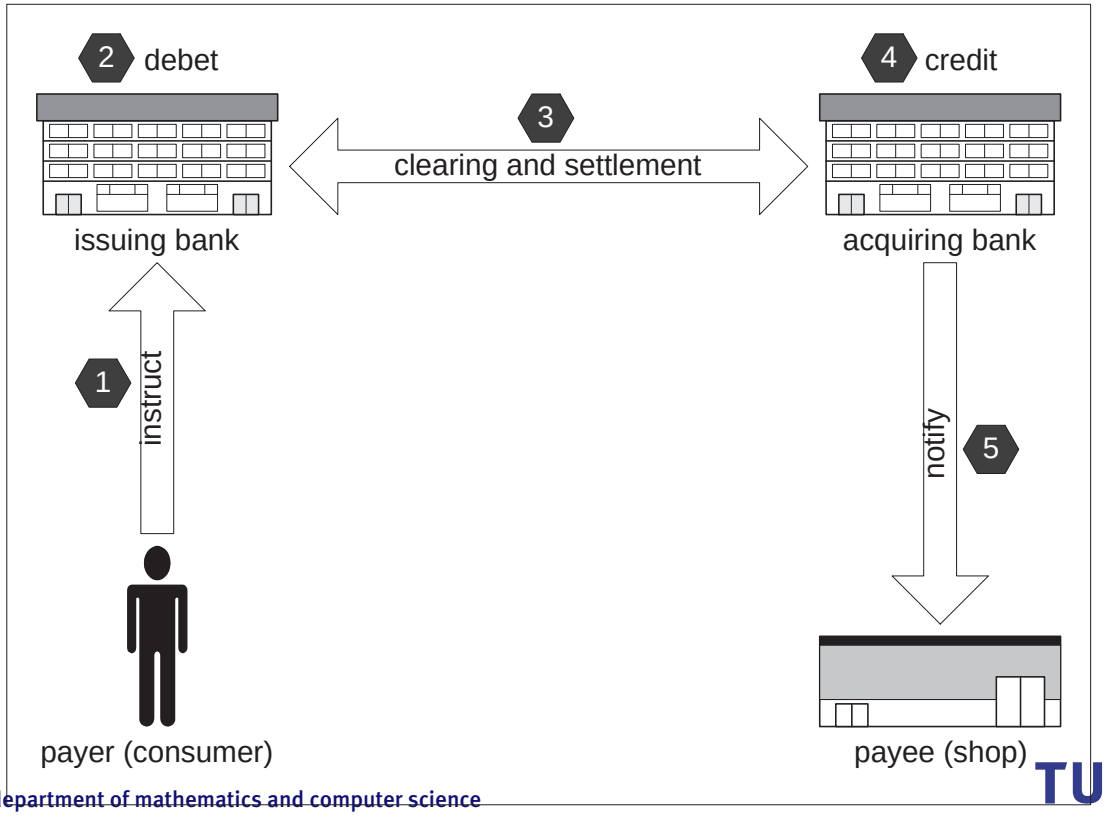
Debet Payment Model

cash based, debet before credit



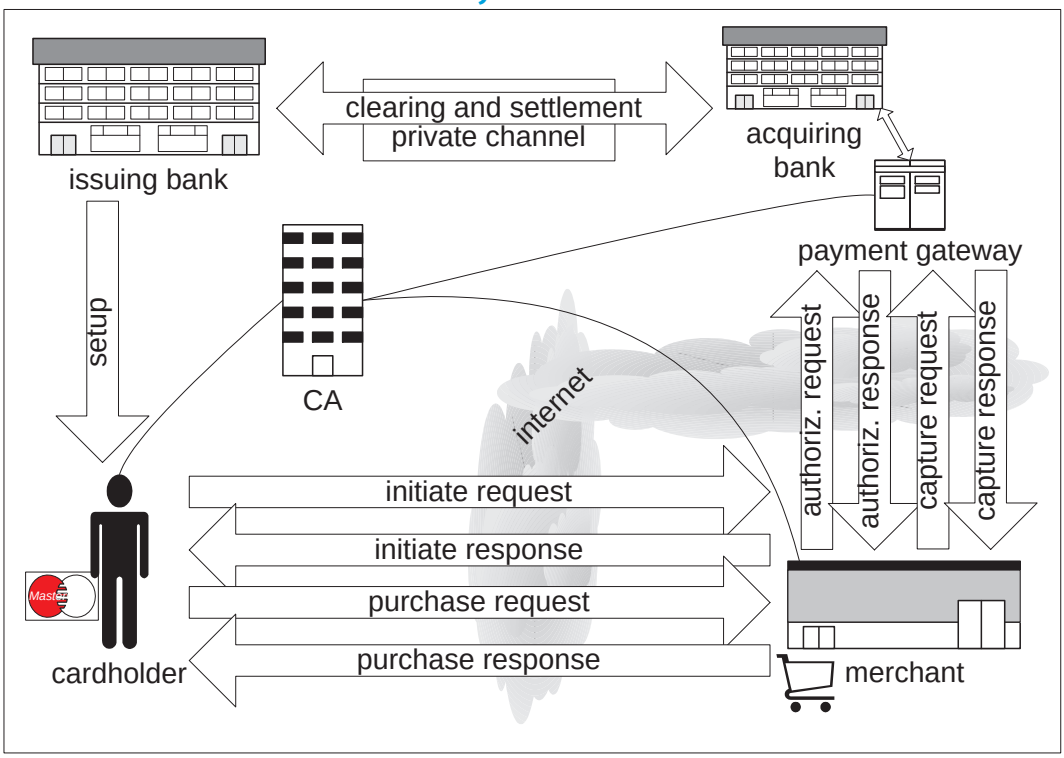
Indirect Payment Model

e.g. internet banking, incasso



SET - Secure Electronic Transactions

online credit card based system



SET - dual signatures

dual signature

- OI - Order Information: order reference + transaction ID
- PI - Payment Information: credit card number + transaction ID
- customer creates signature on $\texttt{hash}(\texttt{hash}(\text{OI}) \| \texttt{hash}(\text{PI}))$
- merchant receives OI, $\texttt{hash}(\text{PI})$ and then can verify the signature
- acquiring bank receives PI, $\texttt{hash}(\text{OI})$ and then can verify the signature
- (message from customer to acquiring bank sent encrypted via merchant)
- merchant does not learn credit card number
- acquiring bank does not learn order information

Digital Cash

Requirements

- unforgeability - only creating bank can create valid coins - by digital signature from creating bank
- uncopyability - replaced by the weaker unreusability (no 'double spending')
- untraceability - coins cannot be traced back to spender
- unlinkability - coin spendings cannot be related to the same (unknown) spender

eCash - Online Digital Cash

inventor

David Chaum (DigiCash, Amsterdam)

setup

- user gets bank public key and Initial Authentication Key
- user registers his own public key by signed message to bank

coinage

- RSA modulus $N = pq$
- Denominations D_i, e.g. 1 cent, 2 cents, 4 cents, etc.
- each D_i has a public RSA-exponent e_i and a private exponent d_i
- e_i are small distinct primes

eCash - withdrawal

coins

- coin number: 160 bit random number x, selected by user
- unblinded coin of denomination D_i: $C = f(x)^{d_i} \pmod N$
- formatting function: $f(x) = x_t \| x_{t-1} \| \cdots \| x_1 \| x_0$, with $x_0 = x$ and $x_{i+1} = \texttt{hash}(x_0 \| x_1 \| \cdots \| x_i)$

withdrawal

	payer		bank
coin number:	$x \in_R \{0,1\}^{160}$		
blinding factor:	$r \in_R \mathbb{Z}_N^*$		
blinding:	$M = f(x) r^{e_i} \pmod N$		
		$\xrightarrow{ID_{\text{payer}}, M, D_i}$	
			debit account of payer with D_i
blind signature:			$S = M^{d_i} \pmod N$
		$\xleftarrow{S}$	
unblinding:	$C = S/r \pmod N$		
verification:	$C^{e_i} \stackrel{?}{=} f(x) \pmod N$		

eCash - payment

payment

by encrypted transfer of coins to merchant or bank

verification

bank verifies by computing $C^{e_i} \pmod N = f(x)$
which should have the correct formatting
then stores serial number in database of spent coins

properties

blinding guarantees anonymity / untraceability / unlinkability

eCash - deviating protocol

unforgeability?

bank signs random looking data

deviating protocol producing valid coin

- ask bank to sign $M_1 = f(x_1)^{e^2} f(x_2)^{e^1}$ for denomination D_1
- bank debits for D_1 and returns $S_1 = M_1^{d_1}$
- ask bank to sign $M_2' = \rho^{e_2} S_1$ for denomination D_2 and random ρ
- bank debits for D_2 and returns $\rho S_2 = \rho S_1^{d_2}$, revealing $S_2 = S_1^{d_2}$
- compute t_1, t_2 such that $e_1 t_1 + e_2 t_2 = 1$
- now $C_1 = f(x_1)^{d_1} = f(x_1)^{t_1} f(x_2)^{-t_2} S_2^{e_2 t_2}$ is a valid coin
- so is $C_2 = f(x_2)^{d_2} = f(x_1)^{-t_1} f(x_2)^{t_2} S_1^{e_1 t_1}$
- but total value is exactly the paid $D_1 + D_2$

Brands' offline digital cash

inventor

Stefan Brands

goal

double spend detection (or even prevention)

setup

- group $G_q \subset \mathbb{Z}_p^*$ of order $q | p-1$ with generators g, g_1, g_2
- bank key pair: $x \in_R \mathbb{Z}_q$, $h = g^x$
- signature: $\mathrm{Sig}(A, B) = (z, a, b, r)$ satisfying
  $g^r = h^c a, \quad A^r = z^c b, \quad c = \mathtt{hash}(A, B, a, b, r)$
- coin: triple $A, B, \mathrm{Sig}(A, B)$

Brands' offline digital cash

opening an account

	payer		bank
payer secret:	$u_1 \in_R \mathbb{Z}_q$		
payer identity:	$I = g_1^{u_1}$		
		$\xrightarrow{I, ID_{\text{payer}}}$	
			store ID_{payer}, I
			$z = (Ig_2)^x$
		$\xleftarrow{z}$	

withdrawal

- creation of coin in collabotation of payer and bank
- payer identity is in there, but hidden

Brands' offline digital cash

withdrawal

	payer		bank
bank witness:			$w \in_R \mathbb{Z}_q$
			$a = g^w, b = (Ig_2)^w$
		$\xleftarrow{a,b}$	
identity blinding factor:	$s \in_R Z_q^*$		
payer witness:	$x_1, x_2 \in_R \mathbb{Z}_q$		
	$u, v \in_R \mathbb{Z}_q$		
identity blinded by payer:	$A = (Ig_2)^s, z' = z^s$		
commitment to secrets:	$B = g_1^{x_1} g_2^{x_2}$		
parts of signature:	$a' = a^u g^v, b' = b^{su} A^v$		
challenge:	$c' = \text{hash}(A, B, z', a', b')$		
blinded challenge:	$c = c'/u \pmod q$		
		$\xrightarrow{c}$	
response:			$r = cx + w \pmod q$
		$\xleftarrow{r}$	
verification:	$g^r \stackrel{?}{=} h^c a, (Ig_2)^r \stackrel{?}{=} z^c b$		
part of signature:	$r' = ru + v \pmod q$		
coin signature:	$\text{Sig}(A, B) = (z', a', b', r')$		
coin:	$\text{coin}_{A,B} = \{A, B, \text{Sig}(A, B)\}$		

Brands' offline digital cash

payment

	payer		merchant
send coin:		$\xrightarrow{\text{coin}_{A,B}}$	
challenge:			$d = \text{hash}(A, B, \text{ID}_{\text{mchnt}}, \text{time})$
		$\xleftarrow{d}$	
response:	$r_1 = du_1 s + x_1 \pmod q$, $r_2 = ds + x_2 \pmod q$		
		$\xrightarrow{r_1, r_2}$	
verification:			verify coin signature, $g_1^{r_1} g_2^{r_2} \stackrel{?}{=} A^d B$

zero-knowledge proof

merchant should verify that the payer is entitled to this coin

Brands' offline digital cash

deposit

	merchant		bank
		$\xrightarrow{\text{coin}_{A,B}, r_1, r_2, \text{time}}$	
verification:			verify coin signature, recompute challenge d, $g_1^{r_1} g_2^{r_2} \stackrel{?}{=} A^d B$ do double spend detection

merchant's assurance

merchant is sure he will receive money from the bank, even if coin is spent twice

Brands' offline digital cash

double spend detection by bank

- bank stores $(A, \text{time}, r_1, r_2)$
- when coin is spent twice, A will already be in the database
- if identical r_1, r_2, the merchant is trying to deposit twice
- if different r_1, r_2, the payers identity can be recovered by
- $$\frac{r_1 - r_1'}{r_2 - r_2'} = \frac{(du_1 s + x_1) - (d' u_1 s + x_1)}{(ds + x_2) - (d's + x_2)} = \frac{(d - d')u_1 s}{(d - d')s} = u_1$$
- identity is $I = g_1^{u_1}$
- but identity remains hidden if coin is spent only once

Brands' offline digital cash

double spend prevention

is possible with a more complicated variant, introducing a smartcard as a tamperproof 'observer' of the payer