





## Electronic Payment

Prof. Bart Preneel  
 COSIC – KU Leuven - Belgium  
 Firstname.Lastname(at)esat.kuleuven.be  
<http://homes.esat.kuleuven.be/~preneel>  
 December 2014


1



## Goals

- Understand how physical payment systems can be replaced by electronic payment systems
- Understand principles behind prepaid (e.g. Proton), debit (e.g. Maestro), credit (e.g. EMV)
- Understand electronic coins and micropayments


2



## Overview

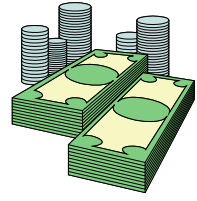
- Traditional payment
- Principle of electronic cash
- Electronic purse
- Credit card transactions
- Micropayments
- Electronic cash: on-line
- Electronic cash: off-line

3




## Traditional payment

- Cash
- Instruction:
  - check
  - credit card
  - debit card



4



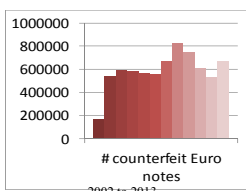
## Cash

- bearer instrument
- off-line payments
- low and medium value
- privacy, coins not traceable
- widely accepted

- bank: risk of forgery, cost of transport
- user: theft and loss, change, physical presence
- government: money laundering

5

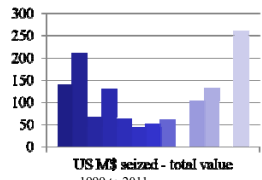
## €/ \$ Counterfeiting



# counterfeit Euro notes  
2002 to 2013

2014

- > 15 billion notes in circulation
- fraudulent: 670,000 or 1 in 22,000
- +/- € 800 billion genuine in 2011
- new 5/10 € bill in May '13/Sep '14
- UK pound: 1 in 4170 counterfeit!



US \$ seized - total value  
1999 to 2011

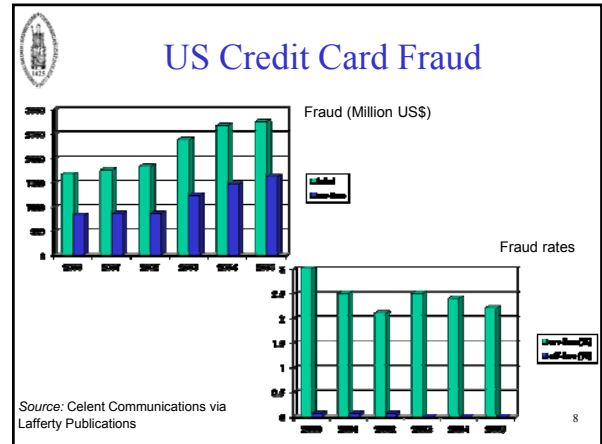
- 1995: \$15.5 million (1% digitally produced)
- 2005: \$61 million (45% digitally produced)
- Fraudulent: 1 to 2 in 10000
- \$1000 billion genuine in 2013
- redesign: 1928, 1990, 1996-2003, 2003-2013

6

### Common features \$/EURO

pattern detected by scanners and copiers

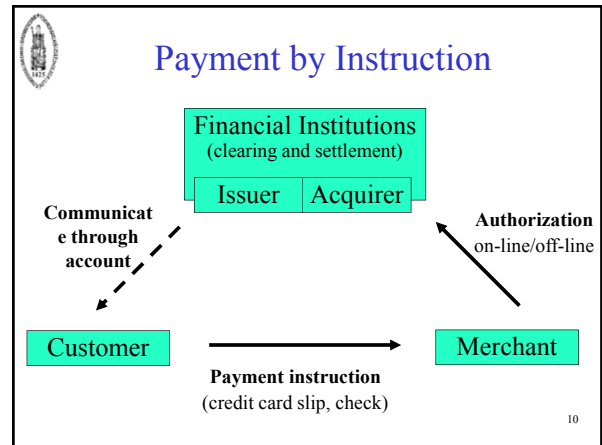
7



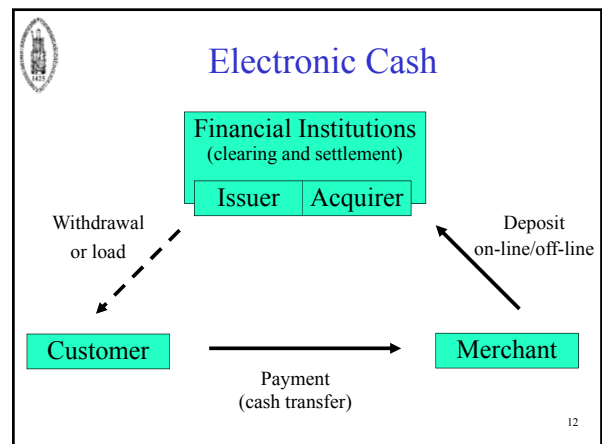
### Card fraud rates (Europe) 2000

Source: Lafferty Publications

Belgian Debit	0.02%	Smart Card & PIN
CB (France)	0.04%	Smart card & PIN
Maestro (Europay)	0.06%	Mag-stripe & PIN
UK Debit	0.14%	Mag-stripe & PIN
Visa EU Credit	0.04%	Mag-stripe & signature
Visa USA Credit	0.06%	Mag-stripe & signature
Europay Credit	0.10%	Mag-stripe & signature
Canada Credit	0.15%	Mag-stripe & signature
UK Credit	0.16%	Mag-stripe & signature
Cartes Bancaires Abroad	0.47%	Mag-stripe & signature



- ### Payment by Instruction
- Convenient
  - Reduced risk
  - Identify users: manual signatures, magstripe cards, smart cards
  - Traceable
  - Verification expensive:
    - credit/debit card: on-line, tamper resistant modules
    - check: off-line, delay, processing cost
- 11



### Electronic Cash

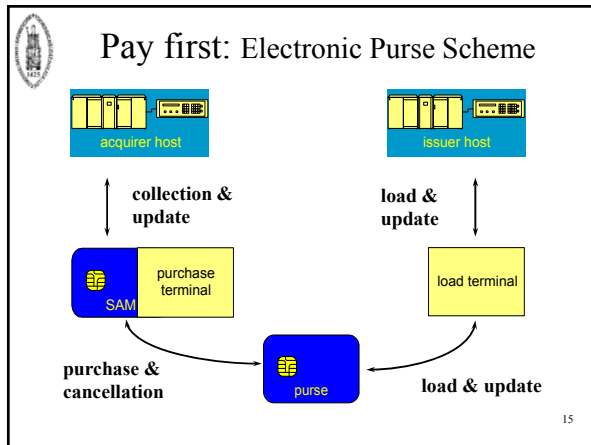
- Convenient, no physical presence
- Reduced risk
- Cost effective for low value
- Untraceable and unlinkable
- **More expensive than traceable systems, new technology**
- Verification inexpensive:
  - on-line: no tamper resistant modules
  - off-line: reduced risk, doublespending

13

### Payment = authenticated transfer of value

- (data origin) authentication
  - symmetric: MAC
  - asymmetric: digital signature
- transfer of value: replay!
  - Prevent replay: tamper resistance, challenge response
  - Detect replay: nonce, timestamp
- risk management

14



### Pay first: electronic purse (2)

- Customer: smart card with
  - counter: value
  - MAC key
  - RSA certificate
- Merchant: terminal
  - off-line
  - loads value from card
  - contains smart card
- Issuer/Acquirer:
  - database for reconciliation of all transactions

16

### Pay first: electronic purse (3)

- Load value: on-line to issuer
- Payment
  - off-line
  - check for blacklist
  - keys from both terminal and customer card
- Deposit: on-line (weekly)
- anonymity: issuer identifies user based on account number
- traceable and linkable
- relies on tamper resistance

17

### Pay first: electronic purse (4)


▪ 1 layer: Banksys

The diagram shows a central 'banksys' logo at the top, connected by lines to several 'chipkaart' (chip cards) below. An arrow points from the text 'Proton card: ID<sup>d</sup> mod n' and 'With d private key of Banksys' towards the chipkaarts.

Proton card:  $ID^d \text{ mod } n$   
 With d private key of Banksys

### Pay first: electronic purse (5)

- National schemes: Proton, Clip, Mondex
- CEPS: Common European Purse Specification
  - standards exist, not deployed
  - relies in part on public-key cryptography
- Limitations: no card to card payment. Why?

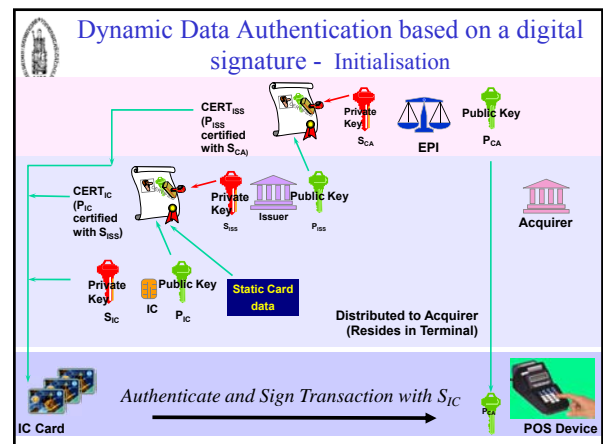
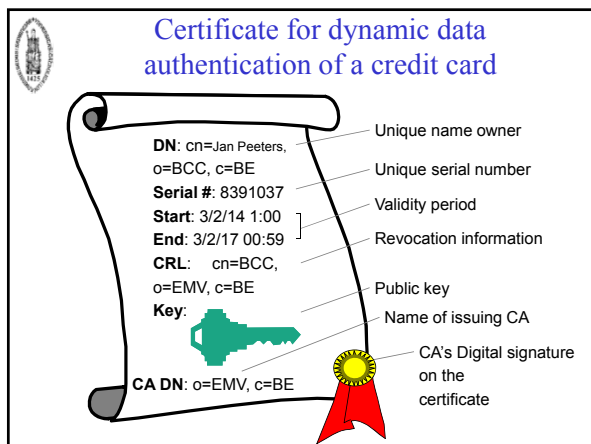
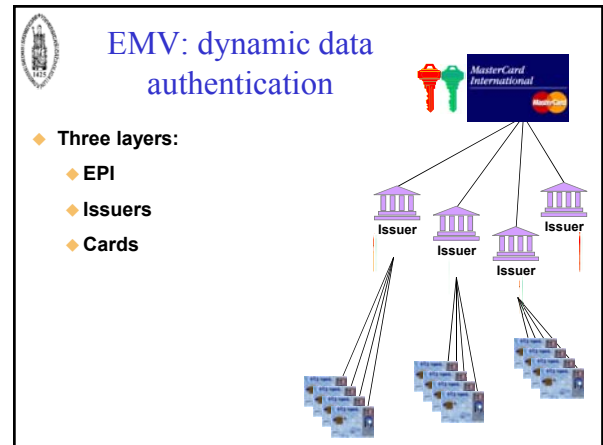
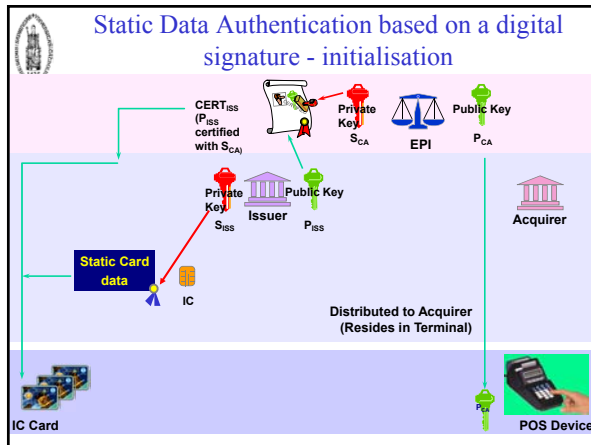


19

### Pay later: EMV

- Magstripe with PIN (on-line) or manual signature (off-line)
- Smart card with DES and RSA certificate
  - off-line PIN verification
  - on-line card verification above threshold (risk management)
- Smart card with RSA (dynamic)
  - needs PKI (card scheme-issuer-card)
  - off-line verification in terminal
  - on-line for high risk

20



### Credit cards today

- Magstripe/hologram/embossing (US) (no chip)
- SDA: Static Data Authentication (UK)
  - 3-DES based MAC + static RSA signature
  - vulnerable to cloning
- DDA: Dynamic Data Authentication
  - 3-DES based MAC
  - Dynamic RSA signature of random string for entity authentication
- CDA: Combined Data Authentication
  - 3-DES based MAC
  - RSA signature on random string and on payment details
  - more secure; still the issue of mafia fraud

25

### Micropayments

- Only 1 expensive payment
  - authorisation/commitment using digital signature
- Sub-payments are cheap
  - off-line computation of hash value
- Sub-payment and deposit very small
  - hash value (100 bits)
- Lamport chain idea:
 

$$x_0 \xrightarrow{f} x_1 \xrightarrow{f} x_2 \xrightarrow{f} x_3 \xrightarrow{f} x_{t-1} \xrightarrow{f} x_t$$

26

### Micropayments (2)

Customer
payee

Generate random  $x_0$   
 Compute  $x_t = f^t(x_0)$   $\xrightarrow{x_t, \text{SIG}(x_t)}$  Authorize  $t$  payments

---

Compute  $x_{t-i} = f^{t-i}(x_0)$   $\xleftarrow{i}$   $\xrightarrow{x_{t-i}}$  Check  $f^i(x_{t-i}) = x_t$

$x$ : 96..128 bit string,  $f$  one-way function

27

### Micropayments: Micromint

- idea of Rivest and Shamir
- collision resistant hash function  $h$ 
  - finding collisions is hard.....
  - unless you perform a massively parallel pre-computation
- coin = collision pair
  - $(x, x')$  with  $x \neq x'$  and  $h(x) = h(x')$
- easy to check validity
- update function  $h$  on a regular basis


28

### Micropayments: Micromint

- $n$ -bit hash function
  - If you evaluate the hash function in  $r$  points, you expect  $r^2/2^{n+1}$  collisions if  $r \ll 2^n$
  - Cost of finding 1 collision ( $r=1$ ):  $2^{n/2}$  steps
  - Cost per collision:  $r/(r^2/2^{n+1}) = 2^{n+1}/r$
- Example:  $n=120, r = 2^{72}$ 
  - cost of finding a single collision:  $2^{60.5}$  steps
  - With  $r = 2^{72}$ , expect  $2^{23}$  collisions; cost for each collision is only  $2^{72-23} = 2^{49}$  steps
  - So making a coin is much cheaper for the government (large scale, precomputation) than for an attacker

29

### Micropayments: Bitcoin (2009)



- Designed by Satoshi Nakamoto
- Distributed generation and verification
- Transactions
  - irreversible
  - inexpensive
  - over anonymous peer-to-peer network
  - broadcasted within seconds and verified within 10 to 60 minutes by inclusion in hash chain
  - double spending prevention using a central database (chain mechanism)
- Pseudonymous (believed by many to be anonymous)... but
  - A. Biryukov, D. Khovratovich, I. Pustogarov: Deanonimisation of Clients in Bitcoin P2P Network. ACM Conference on Computer and Communications Security 2014: 15-29

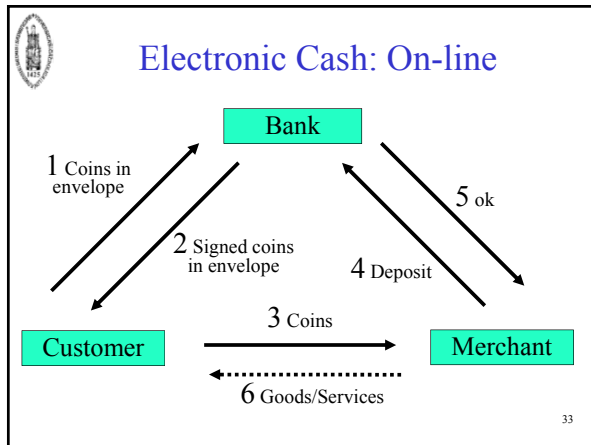
30

### Micropayments: Bitcoin (2009)

- **Bitcoins**
  - can be mined by anyone but economies of scale
  - finding **nonce** such that  
SHA-2(SHA-2 (previous hash || transaction data || **nonce**))  
has a required number (d) of leading zeroes
    - proof of work: hard to compute but easy to check
    - if more solutions are found, d is increased
    - currently massive hardware investment
  - hard limit of about 21 million
  - divisible to 8 decimal places yielding a total of approx.  $21 \times 10^{14}$  units
  - system assumes that longest chain is correct chain (majority of computational power can create new “true” chain)

### Micropayments: Bitcoin (ctd)

- **Bitcoins**
  - transferred from one public key to another using a digital signature computed with the private key of the payer
  - one user can have of course many key pairs
  - not anonymous: public keys can be clustered and many can be linked to identities
- **Incidents**
  - June 2012: massive devaluation
  - June 2012: Mt. Gox hacked - largest Bitcoin exchange (which trades Bitcoins for real world dollars and vice versa)
  - September 2012: Bitfloor hacked - \$250,000 USD in Bitcoins inappropriately transferred to a single account)
  - August 2013: bug in Random Number Generator in Java on Android results in theft of Bitcoins
  - February 2014: Mt. Gox temporarily closed



### Electronic coins (1) on-line

- Coin C is RSA signature:
  - $C = \underline{x}^d \text{ mod } n$
  - with  $\underline{x}$  = encoded version of 160-bit string x
- verify signature using  $(e, n)$  (note  $e \cdot d = 1 \text{ mod } \lambda(n)$ )
- detect double-spending on-line
- denominations: different values of e
  - $e_1=3$ : 1 cent;  $e_2=5$ : 2 cents;  $e_3=7$ : 4 cents,...
- No anonymity!

### Electronic coins (2) + anonymity

Generate x  
Compute  $\underline{x}$   
Generate r  
Blinding factor

$y = (r^e \underline{x}) \text{ mod } n$

Bank

Compute  $z = y^d = (r \underline{x}^d) \text{ mod } n$

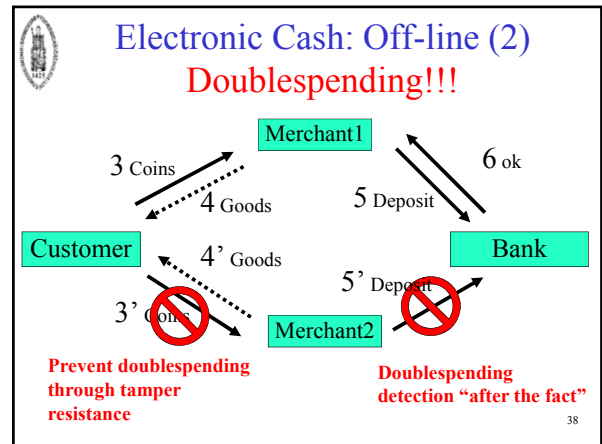
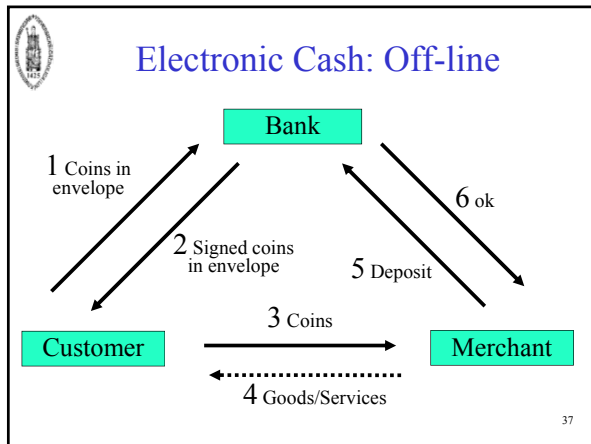
$z = y^d$

Compute  $C = z/r \text{ mod } n = \underline{x}^d \text{ mod } n$   
Check  $C^e = \underline{x} \text{ mod } n$

x 160-bit string,  $\underline{x}$  and r “random” values in  $[0, n-1]$

### Electronic coins (3)

- Payment message:
  - $E_{\text{Pub\_shop}}(\text{ID}_{\text{shop}} \parallel \text{ID}_{\text{trans}} \parallel C_1 \parallel C_2 \parallel \dots \parallel C_i)$
  - $E_{\text{Pub\_shop}}$  prevents stealing of spent coins
  - $\text{ID}_{\text{trans}}$  random transaction identifier
- Payer is untraceable
- Coins of payer are unlinkable
- Payee is NOT anonymous: allows for some audit



### Electronic cash: Offline (3)

- Doublespending detection after the fact requires more sophisticated blinding protocols (restrictive blinding, Brands93)
  - One payment allows user stay anonymous, but identity leaks after 2 payments

39

### Extensions

- revokable cash
- divisible coins
- fault and loss tolerance
- anonymous fingerprinting
- unlinkable credentials:
  - one can show that one is 18 years old, without revealing one's identity

40

### More information and some links

- [www.visa.com](http://www.visa.com): Travelmoney
- [www.mastercard.com](http://www.mastercard.com)
- D. Chaum, S. Brands, Minting electronic cash, IEEE Spectrum, February 1997 (introductory article)
- P. Wayner, Digital cash: Commerce on the net, Morgan Kaufmann, 1997
- D. O'Mahony, M. Peirce, H. Tewari, Electronic payment systems, Artech House, 1997
- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, <http://bitcoin.org/bitcoin.pdf>, consulted on February 1, 2013
- Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Internet Measurement Conference. pp. 127-140. ACM (2013)

41