# Digital Cash

**Birgit Pfitzmann**

**Hopper Conference, 19.9.1997**


1 **Introduction**
2 **Properties (Functionality, Security, Privacy)**
3 **Important Proposals — Overview**
4 **Mechanisms**
5 **Outlook**


© Birgit Pfitzmann, Saarbrücken, 17.9.1997



## 1 Introduction

Like “real” money, only …

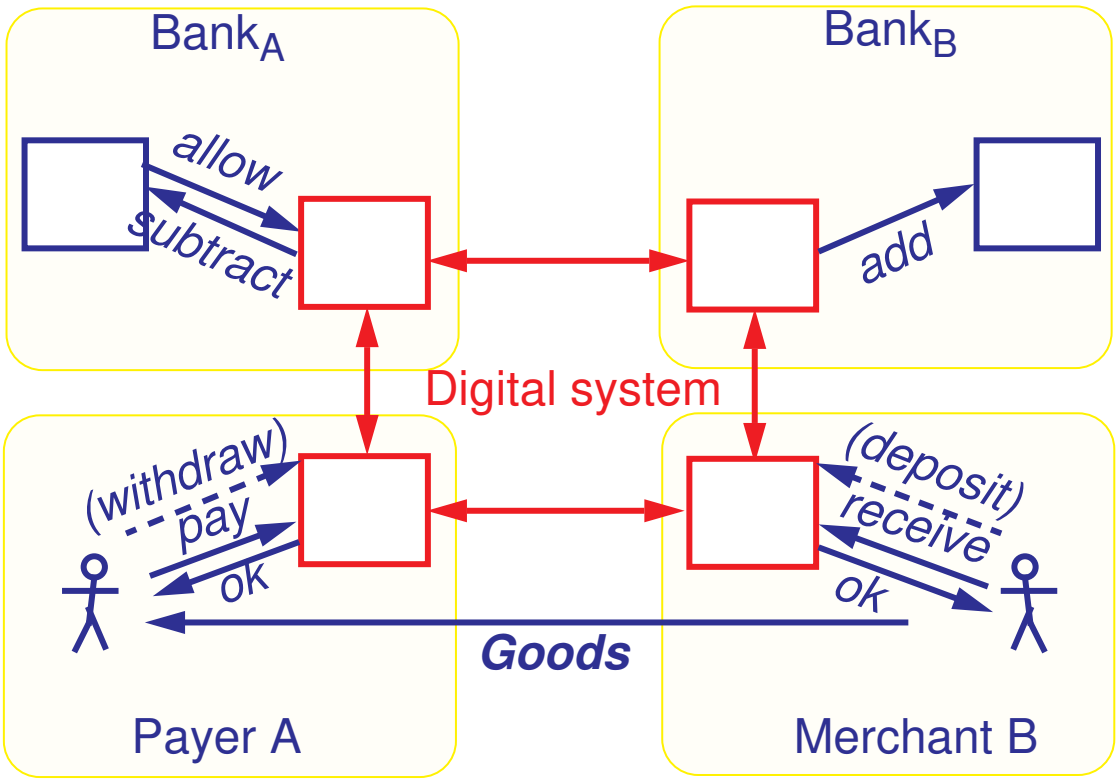
usable in networks,
faster,
cheaper

??

Many variants, none exactly like “real” money
Better don’t assume anything

# 2 Properties

## 2.1 Functionality






- Order of events:
  - „Prepaid“: *allow* before *pay* (separate withdrawal)

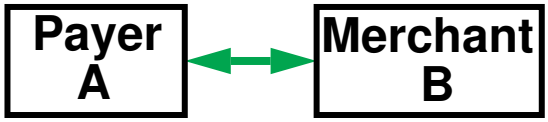
    E.g., cash
  - „Pay-now“:*allow* during *payment*

    E.g., bank transfer
  - „Pay-later“: *allow* afterwards.

    E.g., credit cards

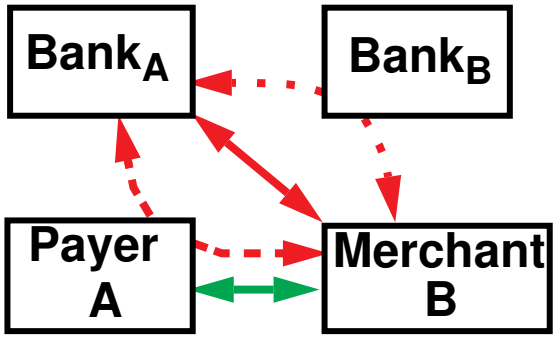
- Communication during payment

**Offline**




+ Less Communication
– Prevent double-spending?
  - Security modules: Smartcards ...
  - Check afterwards

**Online**




– Communication
+ No double-spending problem



- Universal?
  - Not: Merchant = Bank
  - Not: Merchant previously know
- Open? All buyers, merchants, banks, producers
- Extensions
  - Receipts
  - Personal log
  - Several currencies
  - Undo
  - prepaid: loss tolerance
  - offline: transferability

## 2.2 Security

Goal: Multi-party security

No need to trust other parties unreasonably!

- In particular: bank-insider fraud

Like normal legal security: Evidence needed

Note:

- Large computers / software nowadays necessarily insecure.
- Lack of evidence bad for both sides.

Currently not in all systems



## 2.3 Privacy

- Against outsiders: Encryption — independent
- Anonymity
  - Usually only for buyers and in payment
  - At least for small amounts, like cash
  - Security and anonymity no contradiction
    - Identification after fraud possible
    - Where necessary, external identification
    - Fair exchange under pseudonyms

- Anonymity from merchant only in shop or by anonymous communication

- Weaker anonymity:
  - Linkability (only for efficiency) — re-identification
  - Traceability for law enforcement
    - Often only merchant to be identified
    - Consider risk of large data collection — also economic
  - At least split merchant and bank data



## 3 Important Proposals — Overview

| | Online | Offline |
|---|---|---|
| **Not anonymous** | • Crypto-less: First Virtual or just-do<br>• Encryption: just do<br>• "Trusted" payment server<br>  • NetBill (CMU, VISA)<br>• Secure credit cards<br>  • CyberCash<br>  • iKP (IBM)<br>  • SET (VISA, Mastercard …) | • Counters in smartcards<br>  • Danmont, Proton ...<br>  • CLIP (Europay)<br>  • CEN IEP (Standardization)<br>  (• EMV (Europay, VISA, Mast.))<br>• Counters in "Wallet"<br>  • Mondex<br>(So far not used online ...) |
| **Anon.** | • "Exchangers"<br>  • Anonymous Creditcard (AT&T)<br>  • NetCash (ISI)<br>• Blind signatures<br>  • e-cash (DigiCash) | • Blind signatures<br>  • CAFE (EU project)<br>(So far not used online ...) |

## User has to trust her device

- Production, shipping
- Generate secrets in device itself
- Direct in- and outputs
- Device has to ask user in decisions
- Protection from / after theft



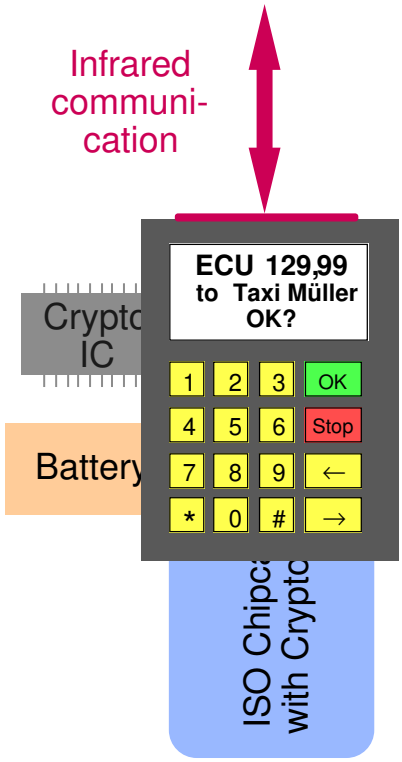
## Main problems currently:

- Shop scenario, even with smartcard:
  - PIN-entry into unknown device
  - PIN-entry watched
- Internet scenario: Operating system security of PC or multi-user station

  $\Rightarrow$ near future: smartcard + PC

⇒ Later: Full mobile devices

E.g., CAFE wallet




Device independence:

- arbitrary (multifunctional) mobile user device
  - Mobile phone
  - PDA
  - Watch, …
- arbitrary security module
  - more secure, stabler ...

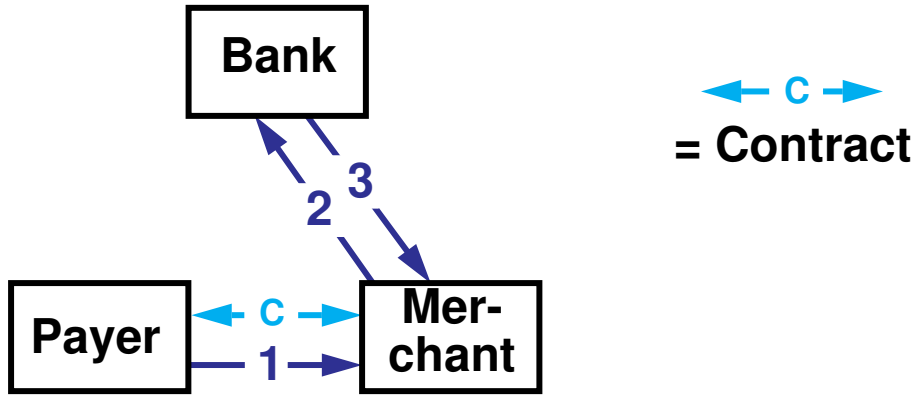


## 4.2 Message Authentication

- Symmetric (shared-key)
  - \+ fast
  - – no non-repudiation (evidence)
- Asymmetric (digital signatures)
  - – slower
  - \+ non-repudiation (evidence)
  - o public-key infrastructure needed

## 4.3 Non-Anonymous Online Systems

Typical example: Credit-card like, e.g., iKP



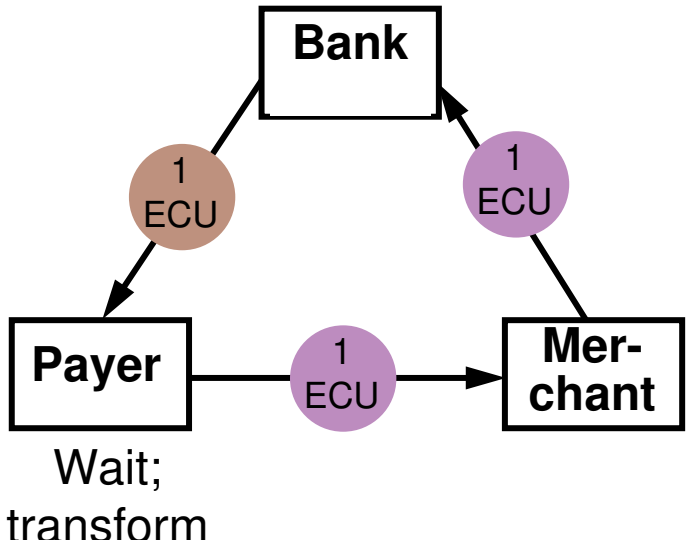

- Digital signatures, mainly in 1, 3 (in 3KP)
- 1 part of 2
- 1 encrypted against merchant, at least if only PIN-based



## 4.4 Anonymous Online Systems

Most secure class: blindly signed "coins", e.g., in e-cash.

- Information of certain form
- digitally signed by bank




- Perfect payer anonymity
- Amount coded in signature type
- Online-check: "Coin" not spent before?

## 4.5 Anonymous Offline Systems

- Almost always tamper-resistance + fall-back measures
- Cryptography still necessary: At least mutual identification of devices
- Most secure class again: blindly signed “coins”, e.g., CAFE
  - Trick: Identification after double-spending (if tamper-resistance broken):
    - Honest payers anonymous
    - Cheaters identified



## 5 Outlook

- More than one system:
  - Secure credit cards for large amounts
  - Cash-like for small amounts
  - Maybe “micropayments” separately
- Evolution, in particular devices

  $\Rightarrow$ Network and shop scenario will grow together
- Security never perfect
- For networks: entire market place necessary
- Export restrictions $\Rightarrow$ regional solutions important

Some sources: http://www.semper.org/~sirene/