Programmable Banknotes

A new concept for electronic cash

Klaus Diepold

12.07.2005

TECHNISCHE
UNIVERSITÄT
MÜNCHEN

Lehrstuhl für
Datenverarbeitung

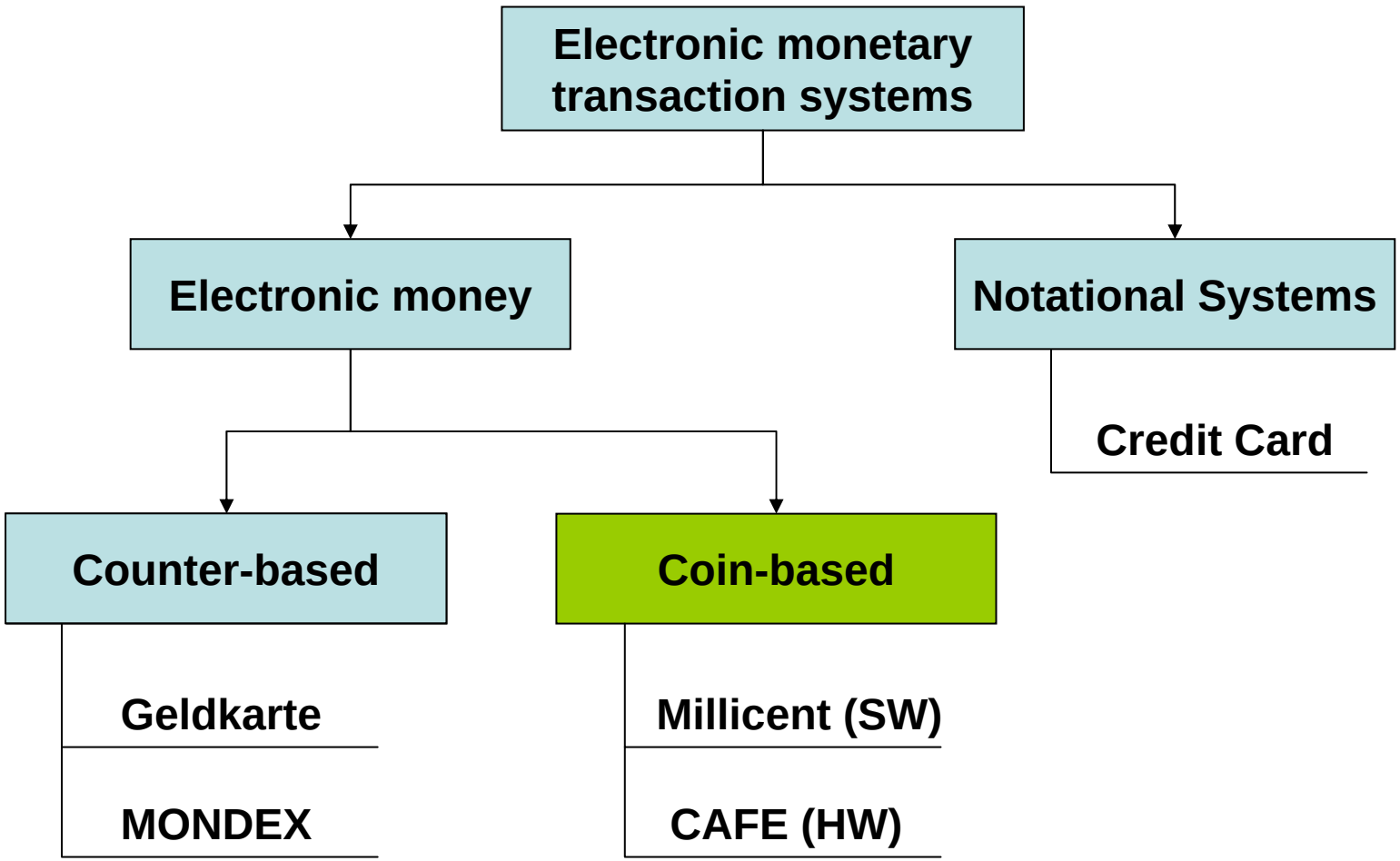
Acknowledgement

- Michael Pramateftakis
  - PhD Thesis TUM, June 2005
  - Programmable Banknotes – An Alternative Approach to Electronic Money
  - www.ldv.ei.tum.de/page51
- Supervisor: Prof. J. Swoboda

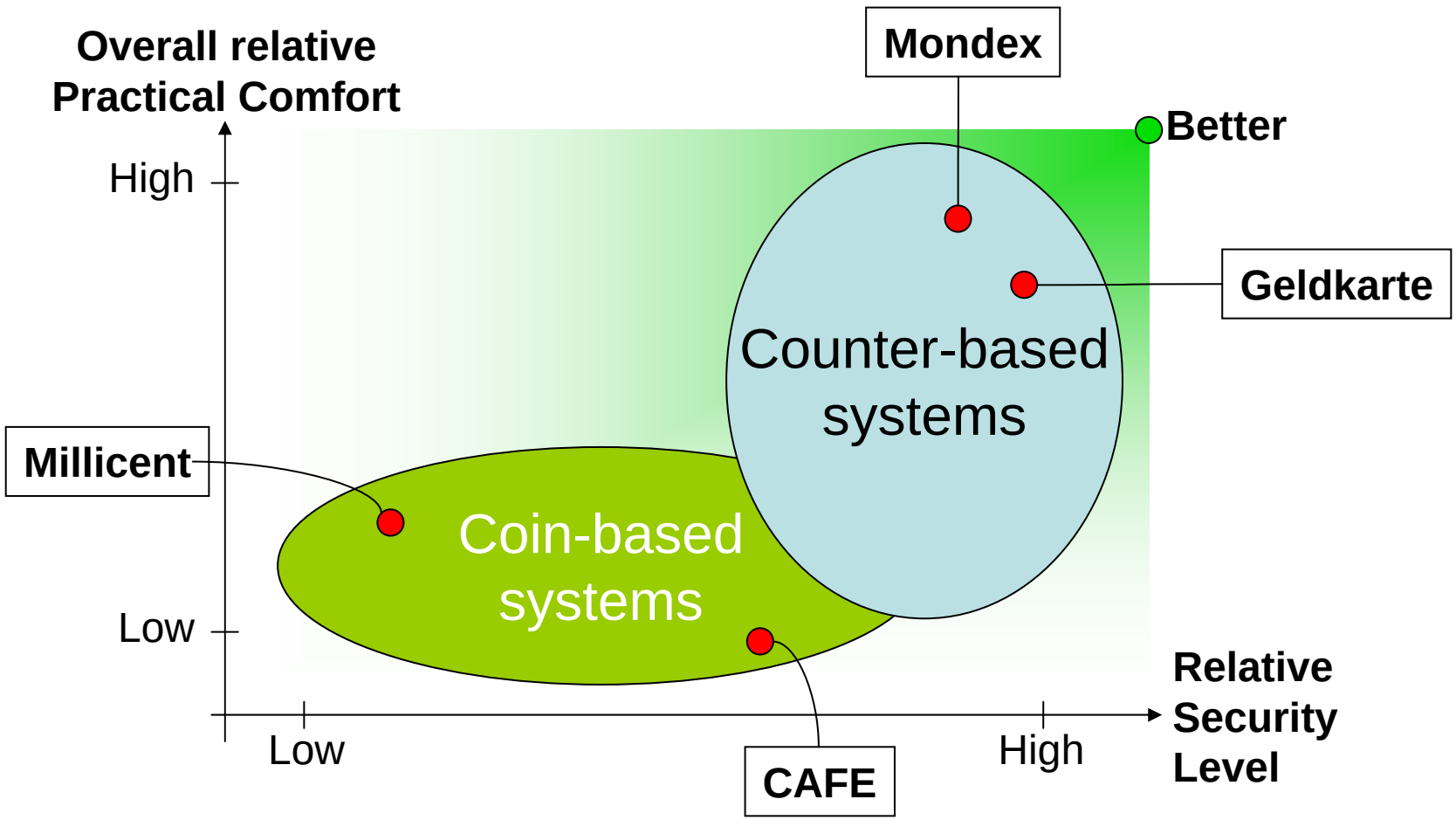
Overview

- The Current State of Electronic Money
- The Concept for Programmable Banknotes
- Closing Comments

Electronic Money



Concept Comparison



Requirements

The **ideal** electronic money system should provide:

	Coin-based	Counter-based
• Independence	✓	✗
• Security	✓	✓
• Untraceability	✓	✓
• Offline ability	✓	✗
• Transferability	✗	✓
• Divisibility	✗	✓

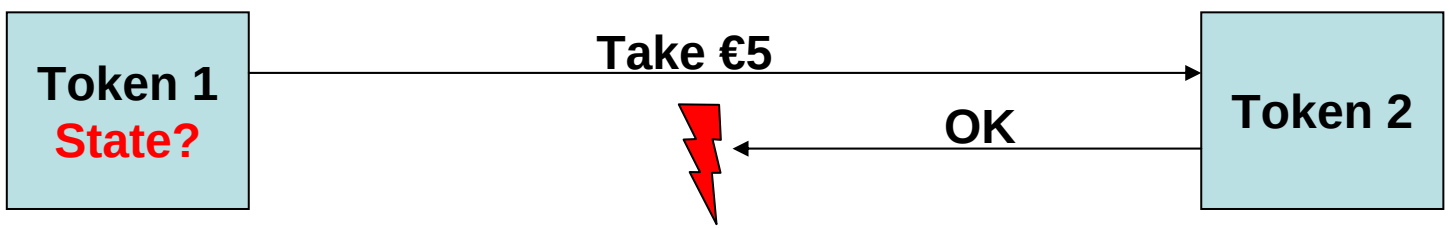
Conceptual Problems

Coin-based systems:

- Coins can be copied arbitrarily.
- Doublespending is detected after it happened.

Counter-based systems:

- Insecure environment / network.
- Transaction integrity protection difficult.



Current State

Coin-based systems:

- Disadvantages have to be taken as is.
- Low popularity, especially with providers.

Counter-based systems:

- No transaction directly between users possible
- Restriction to transactions with trusted terminals only (z.B. Geldkarte).
- Payment system
- No replacement for cash

Overview

- The Current State of Electronic Money
- The Concept for Programmable Banknotes
- Closing Comments

Programmable Banknotes

Observation:

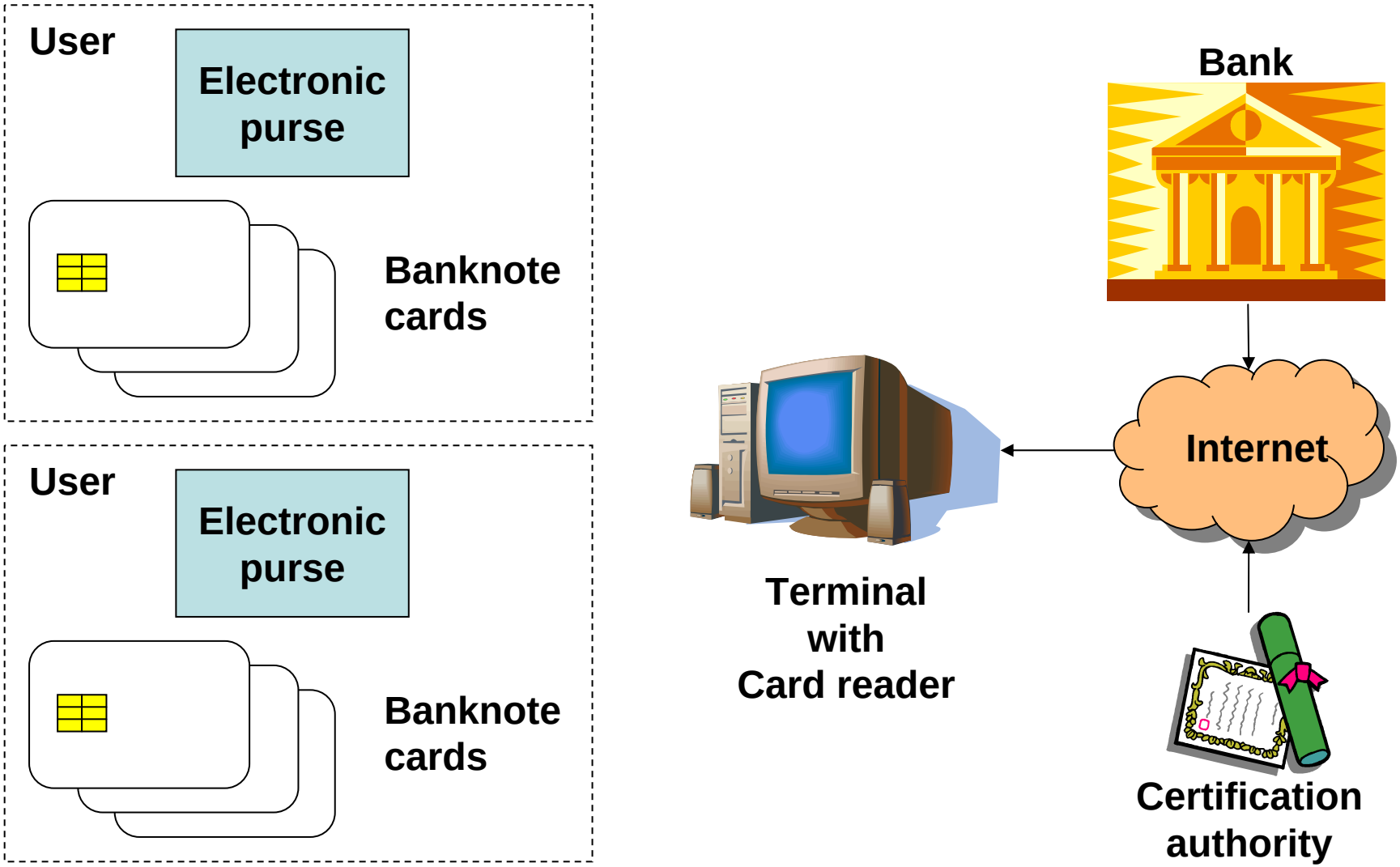
- Vulnerable point in counter-based systems: Communication network.

Simple Solution:

- “Replace” insecure connection with secure hardware, thus “regaining control”.

Programmable Banknotes

Lehrstuhl für
Datenverarbeitung



Supported Transactions

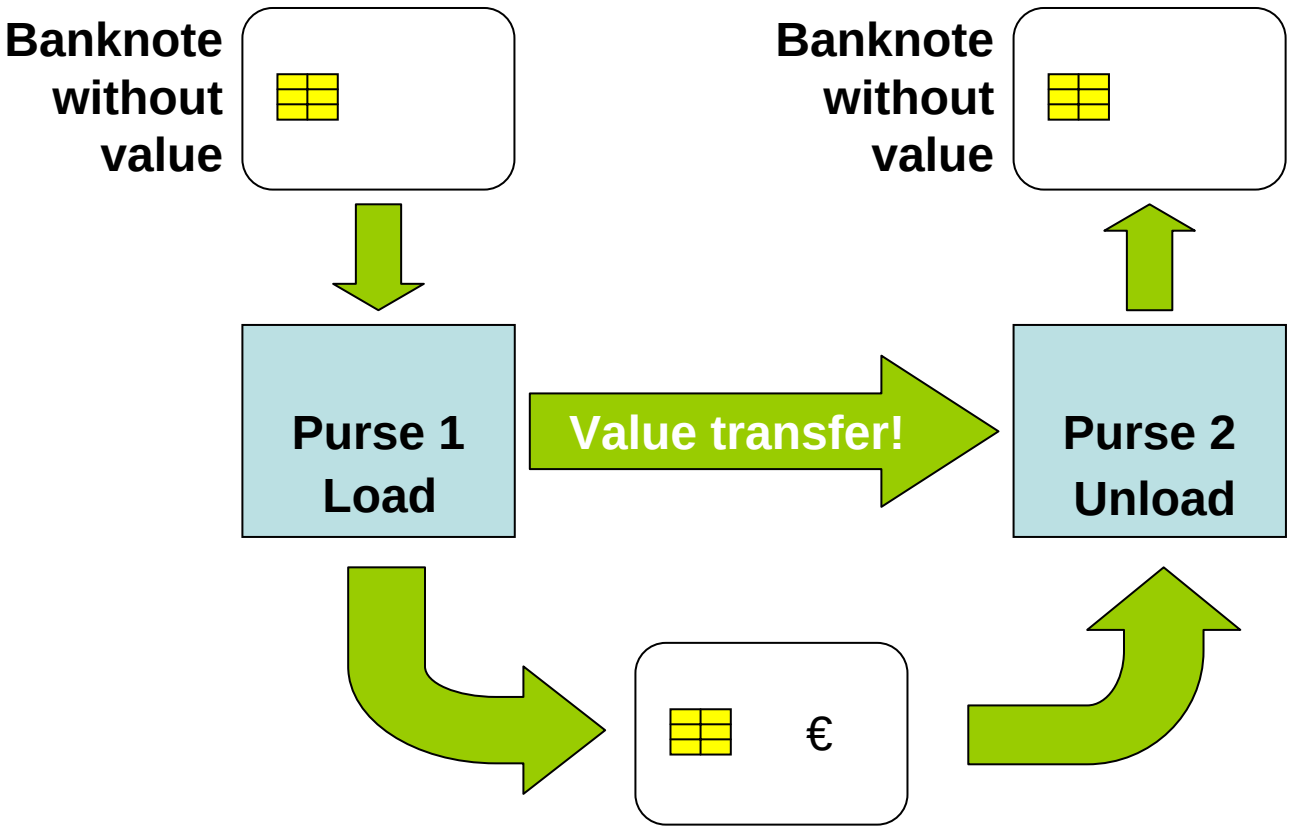
Two kinds of transaction:

- Offline transaction
  - transaction directly between users
- Online transaction
  - transaction over a network.

Sufficient for offering all features of a complete electronic money system.

Offline Transaction

Offline Transaction Model:



Offline Transaction

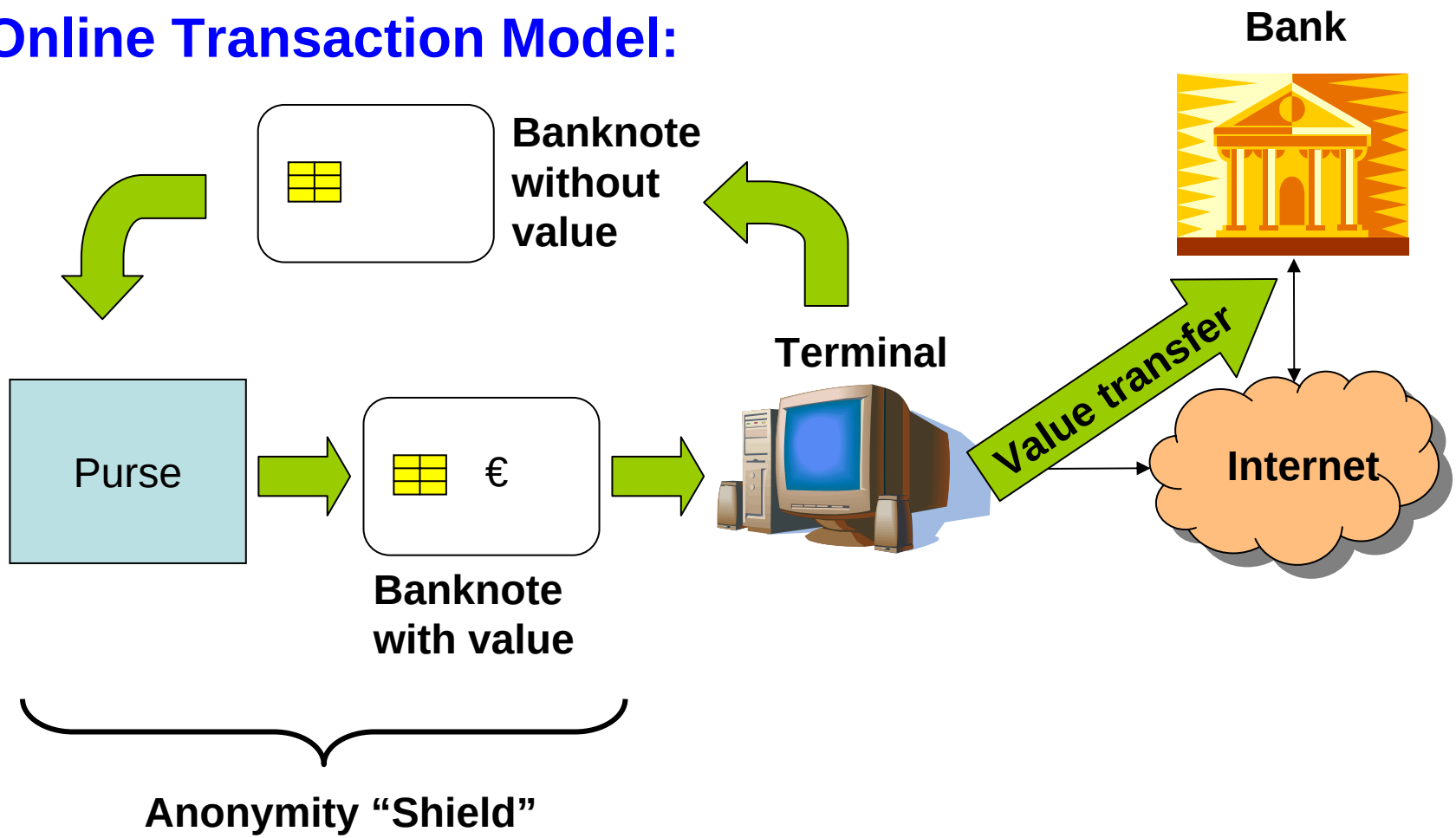
- No insecure channel.
- Cards remain within the user's purse for as long as needed.
  - One entity controls the system card-purse.
  - Correct load/unload can be checked before card is handed over.
- Only authentic purses may communicate with authentic cards.
- Model of cash exchange.

Offline Transaction

- Cards can only contain authentic money, because they were loaded by an authentic purse.
  - No need for separate money authentication.
- Complete anonymity.
  - No personal information of user on the cards.

Online Transaction

Online Transaction Model:



Online Transaction

- No need for direct card handover.
- Transaction over a network.
  - Connection to network through a terminal.
  - Network is insecure, outside of transaction partners' control.
- An observer is introduced, e.g. a bank.
  - The system provides anonymity even in this case.

Online Transaction

- One end of the network connection is always trusted (the bank).
- The terminal and the bank only see a card.
  - User anonymity is protected.
- The receiver performs a similar procedure and obtains the money by loading a card.
  - Receiver is also anonymous.

Overview

- The Current State of Electronic Money
- The Concept for Programmable Banknotes
- Closing Comments

System Features

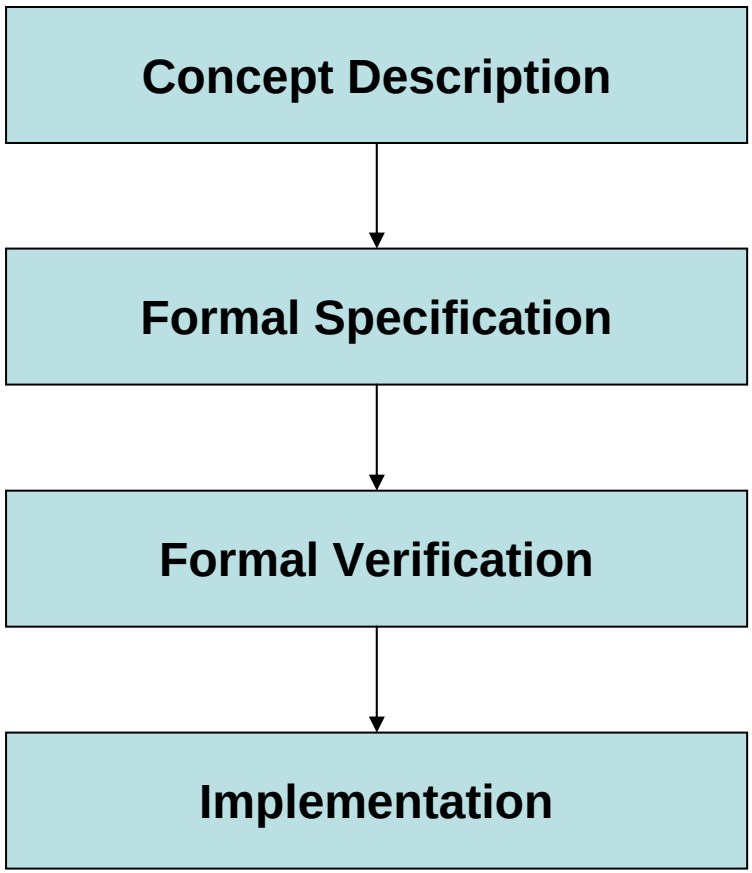
All features of conventional electronic money systems are supported:

- Load/unload and currency exchange through transaction with a bank.
- Payment through transaction with any other partner.

Additional feature:

- User-to-User transaction
  - Enables programmable banknotes to replace cash.

Further System Aspects



Goal for system design:

- Be as close as possible to requirements of Common Criteria and ITSEC.

Prototype Implementation

- Implemented on a Zeitcontrol Basiccard ZC4.5D rev F.
- Card capabilities:
  RSA, DES, SHA-1
  30KB EEPROM, 1KB RAM
- Banknote card application takes up 3KB
- Offline transaction takes 2-4 sec

Programmable Banknotes

Lehrstuhl für
Datenverarbeitung

Thank you for your attention!