US00RE36788E

United States Patent [19]

Mansvelt et al.

[11] E **Patent Number: Re. 36,788**

[45] **Reissued Date of Patent: Jul. 25, 2000**

[54] **FUNDS TRANSFER SYSTEM**

[75] Inventors: **Andre P. Mansvelt**, Johannesburg; **Serge C. P. Belamant**, Hurlingham, both of South Africa

[73] Assignee: **Visa International Service Association**, Foster City, Calif.

[21] Appl. No.: **08/916,701**

[22] Filed: **Aug. 22, 1997**

Related U.S. Patent Documents

Reissue of:

[64] Patent No.: **5,175,416**
Issued: **Dec. 29, 1992**
Appl. No.: **07/701,821**
Filed: **May 17, 1991**

[30] **Foreign Application Priority Data**

Sep. 6, 1990 [ZA] South Africa 907106

[51] **Int. Cl.**[7] **G06F 15/30**

[52] **U.S. Cl.** **235/379**; 235/380

[58] **Field of Search** 235/379, 380; 340/825.33; 902/25, 26, 27, 8, 22

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,007,355	2/1977	Moreno	235/61.7
4,215,421	7/1980	Giraud	364/900
4,277,837	7/1981	Stuckert	364/900

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0 172 670 A2	2/1986	European Pat. Off. .
0 256 768 A2	2/1988	European Pat. Off. .
0 355 372	12/1989	European Pat. Off. .
0 281 058 B1	2/1993	European Pat. Off. .
0 527 203	9/1994	European Pat. Off. .
2 413 721	7/1979	France .
2 530 053 B1	4/1986	France .
WO9117528	5/1991	France .
0355372	7/1989	Germany .
2 066 540	7/1981	United Kingdom .
WO83/0301	9/1983	WIPO .
WO83/03694	10/1983	WIPO .

OTHER PUBLICATIONS

EPO Opposition Division, Annex to Summons, Reference No. RAL/014/F6658, Application No. 90310934.6–2207/0421808, Mansvelt, Andre Peter, et al., Oct. 16, 1997.

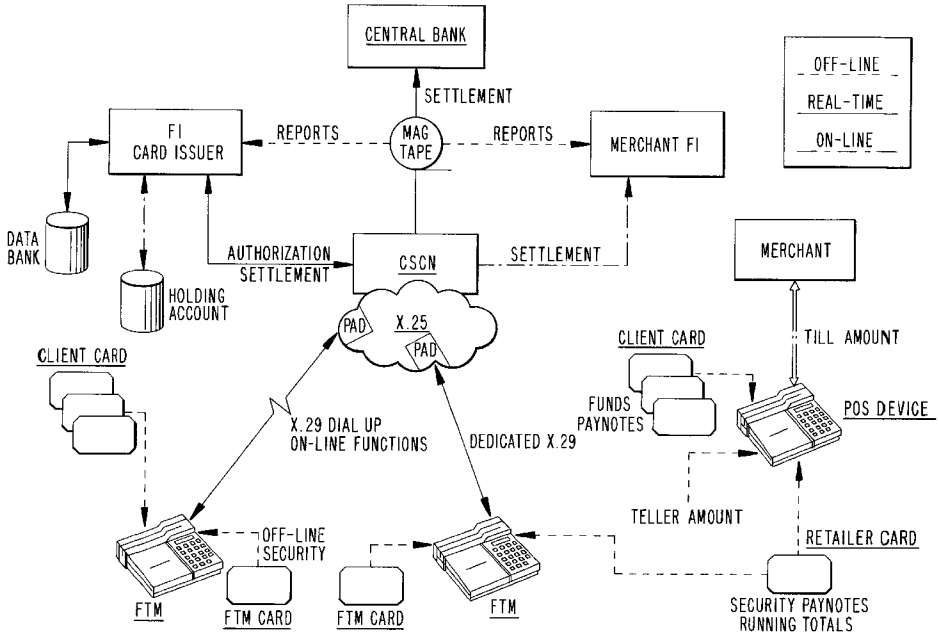
(List continued on next page.)

Primary Examiner—Karl D. Frech
Attorney, Agent, or Firm—Beyer & Weaver, LLP

[57] **ABSTRACT**

A method of transferring funds includes the steps of linking a first "smart card" to a first financial institution, debiting an account held at the financial institution and recording a corresponding credit value in the first smart card. The first smart card is then linked to a second, similar device, the credit value in the first device is reduced, and a corresponding credit value is recorded in the second device. The second device is then linked to a second financial institution, the credit value in the second device is reduced, and a corresponding credit value is recorded in an account held at the second financial institution. The first and second devices each store at least a portion of a program which is run in a synchronized interactive manner between the first devices. The invention extends to a system for implementing the method.

41 Claims, 7 Drawing Sheets



U.S. PATENT DOCUMENTS

4,305,059	12/1981	Benton	340/825.33
4,320,387	3/1982	Powell	340/825.34
4,341,951	7/1982	Benton	235/379
4,450,535	5/1984	de Pommery et al.	364/900
4,454,414	6/1984	Benton	235/379
4,467,139	8/1984	Mollier	178/22.08
4,549,075	10/1985	Saada et al.	235/380
4,556,958	12/1985	Ugon	364/200
4,625,276	11/1986	Benton et al.	364/408
4,709,136	11/1987	Watanabe	235/379
4,786,790	11/1988	Kruse et al.	235/380
4,802,218	1/1989	Wright et al.	380/23
4,877,947	10/1989	Mori	235/381
4,900,903	2/1990	Wright et al.	235/380
4,926,325	5/1990	Benton et al.	340/825.33
5,093,862	3/1992	Scwartz .	
5,434,395	7/1995	Storck et al. .	

OTHER PUBLICATIONS

Jerome Svigals, "Smart Cards, The New Bank Cards," 1987, MacMillan Publishing Company, New York, Revised Edition, Chapter 2 "Smart Cards for Financial Transactions," p. 60.

Roy Bright, "Smart Cards: Principles, Practice, Application," 1988, Ellis Horwood Limited, pp. 73–81, Ch. 6.

Herbert F.W. Schramm, "POS–Banking mit Chipkarten," 1987, Geldinstitute No. 1, pp. 70–71. (English translation included).

von W. Ott et al., "Kartenanwendungen im Fernmeldewesen," Der Fernmelde–Ingenieur, Aug./Sep. 1989, pp. 64–70. (English translation included).

"La Carte A Micro–Calculateur Multi–Applications MP–ADF," Bull CP8: TD 0143F.01, Aug. 1988. (English translation included).

S. Even et al., "Electronic Wallet," Jun. 1983.

Yrjönen et al., Chip Cards—Bank Notes of the Future, Paper to be presented at ESCAT 1988, Sep. 5–7, Helsinki, Finland.

Chip Card News Intamic, Dec. 1988, No. 26., including 3 articles.

Chip Card News, Apr. 1983, No. 5.

Prof. Shimon Even, Secure Off–Line Electronic Fund Transfer Between Nontrusting Parties, Oct. 1987, Smart Card 2000.

David Chaum, Provacy Protected Payments Unconditional Payer and/or Payee Untraceability, 1989, Smart Card 2000.

Beutelspacher, et al. Payment Applications with Multifunctional Smart Cards, 1989, Smart Card 2000.

Waidner, et al., Loss–Tolerant Electronic Wallet, 1991, Smart Card 2000.

Applications in the banking and financial sector, Ch. 6, pp. 73–81, no date.

Preussag AG, "Opposition (1)", Sep. 27, 1995, EPO.

Deutsche Telekom AG; "Opposition (2)", Sep. 26, 1995, EPO.

Ascom Autelca AG, "Opposition (3)", Sep. 26, 1995, EPO.

Giesecke & Devrient GmbH, "Opposition (4)", EPO.

Schlumberger Industries SA, "Opposition (5)", EPO.

Koninklijke PTT Nederland N.V., "Opposition (6)", EPO.

Elkington and Fife, "Response to the Communications of Notices of Opposition dated Mar. 1, 1996", Sep. 13, 1996, EPO.

EPO Opposition Division, "Annex to Summons", Oct. 16, 1997.

Elkington and Fife, "Patentee's Statement", Feb. 19, 1998, EPO.

EPO Opposition Division, Interlocutory Decision in Opposition Proceedings, Jun. 15, 1998, EPO.

EPO Opposition Division, "Minutes of Oral Proceedings", Jun. 15, 1998, EPO.

Michael Waidner, Birgit Pfitzmann, "Loss–Tolerant Electronic Wallet", 1991, Elsevier Science Publishers B.V.

"Notice of Appeal"; Ref. PJF/CB/0665800P; date: Jul. 13, 1998; author: none; Publisher: European Patent Office.

Klunker Schmitt–Nilson Hirsch, "Appeal of European Patent EP 0 421 808", Oct. 19, 1998, European Patent Office.

Cabinet Hirsch, Appeal of European Patent EP 0 421 808, Oct. 19, 1998, European Patent Office.

P. Remery et al.,"Le paiement electronique", 4, trimestre, 1988.

Prof. Shimon Even, "Secure Off–line Electronic Fund Transfer Between Nontrusting Parties", Smart Card 2000, 1989.

Chaum et al., "SmartCard 2000: The Future of IC Cards", Oct. 19, 1987, Elsevier Science Publishers, B.V.

Jerome Svigals, "SmartCards The New Bank Cards", 1985, MacMillan Publishing Company.

Jerome Svigals, "SmartCards The Ultimate Personal Computer", 1985, MacMillan Publishing Company.

Hawkes et al., "Integrated Circuit Cards, Tags and Tokens", 1990, BSP Professional Books.

Hiro Shogase, The Very Smart Card: A Plastic Packet Bank:, Oct. 1988, IEEE Spectrum.

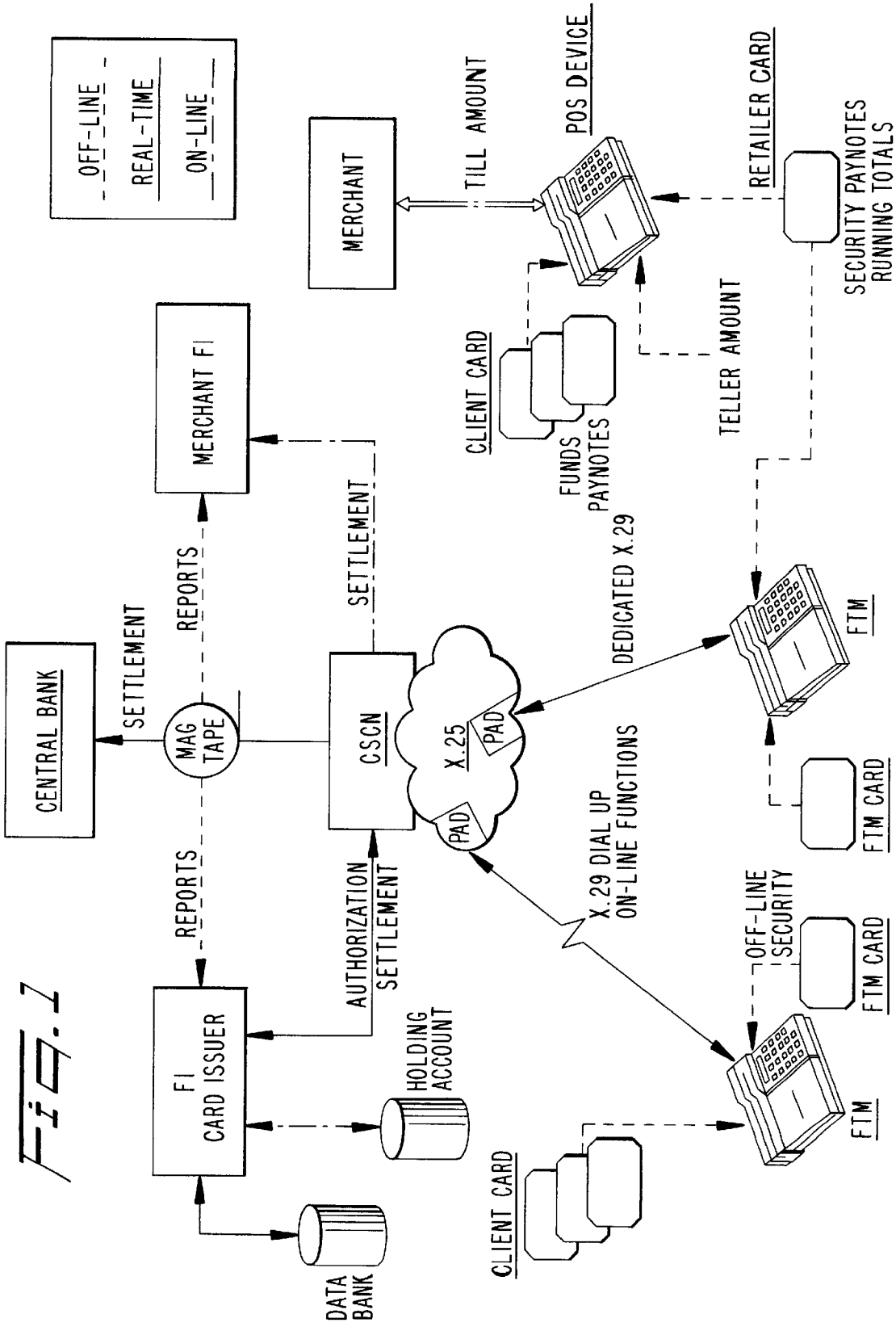

OFF-LINE
REAL-TIME
ON-LINE
MERCHANT
TILL AMOUNT
POS DEVICE
RETAILER CARD
SECURITY PAYNOTES
RUNNING TOTALS
MERCHANT FI
CLIENT CARD
FUNDS
PAYNOTES
TELLER AMOUNT
SETTLEMENT
REPORTS
SETTLEMENT
CENTRAL BANK
SETTLEMENT
MAG TAPE
CSCN
X.25
PAD
PAD
DEDICATED X.29
FTM
FTM CARD
X.29 DIAL UP
ON-LINE FUNCTIONS
OFF-LINE
SECURITY
FTM CARD
REPORTS
AUTHORIZATION
SETTLEMENT
FI
CARD ISSUER
HOLDING
ACCOUNT
FTM
CLIENT CARD
DATA
BANK

Fig. 1

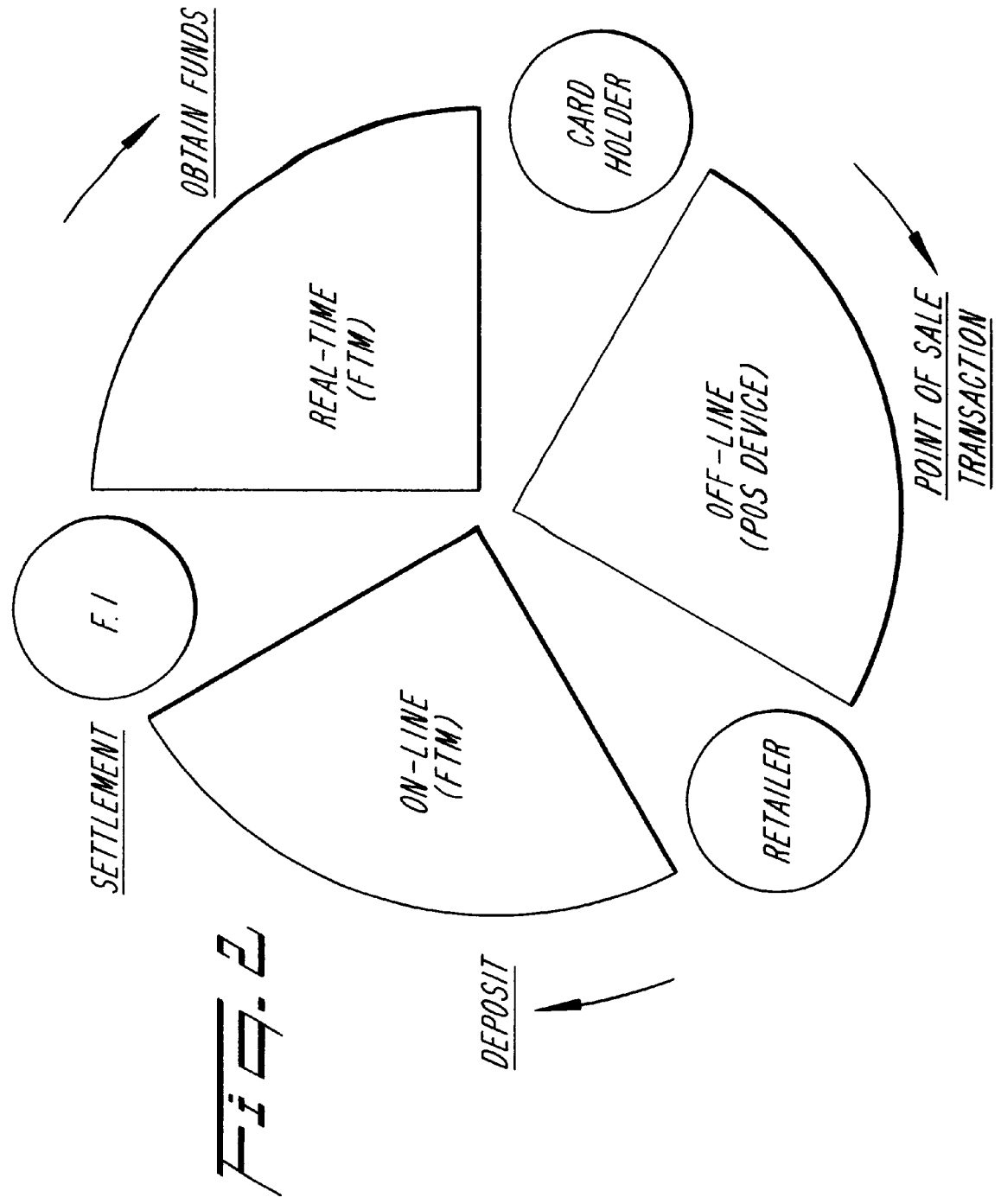

OBTAIN FUNDS
CARD HOLDER
REAL-TIME (FTM)
POINT OF SALE TRANSACTION
OFF-LINE (POS DEVICE)
F.I
SETTLEMENT
ON-LINE (FTM)
RETAILER
DEPOSIT

Fig. 2

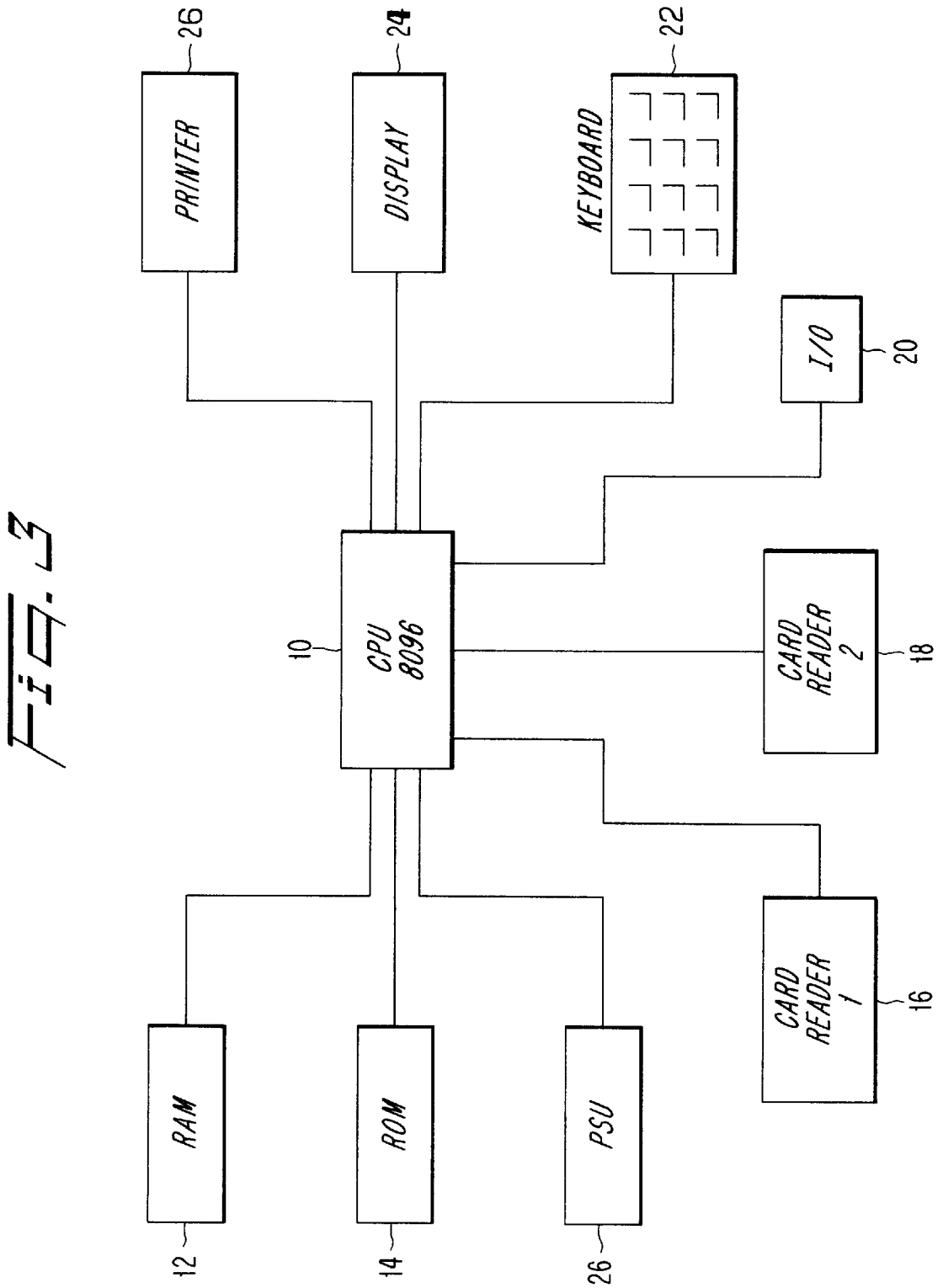

PRINTER
26
DISPLAY
24
KEYBOARD
22
I/O
20
CPU
8096
10
CARD
READER
2
18
CARD
READER
1
16
RAM
12
ROM
14
PSU
26

FIG. 3

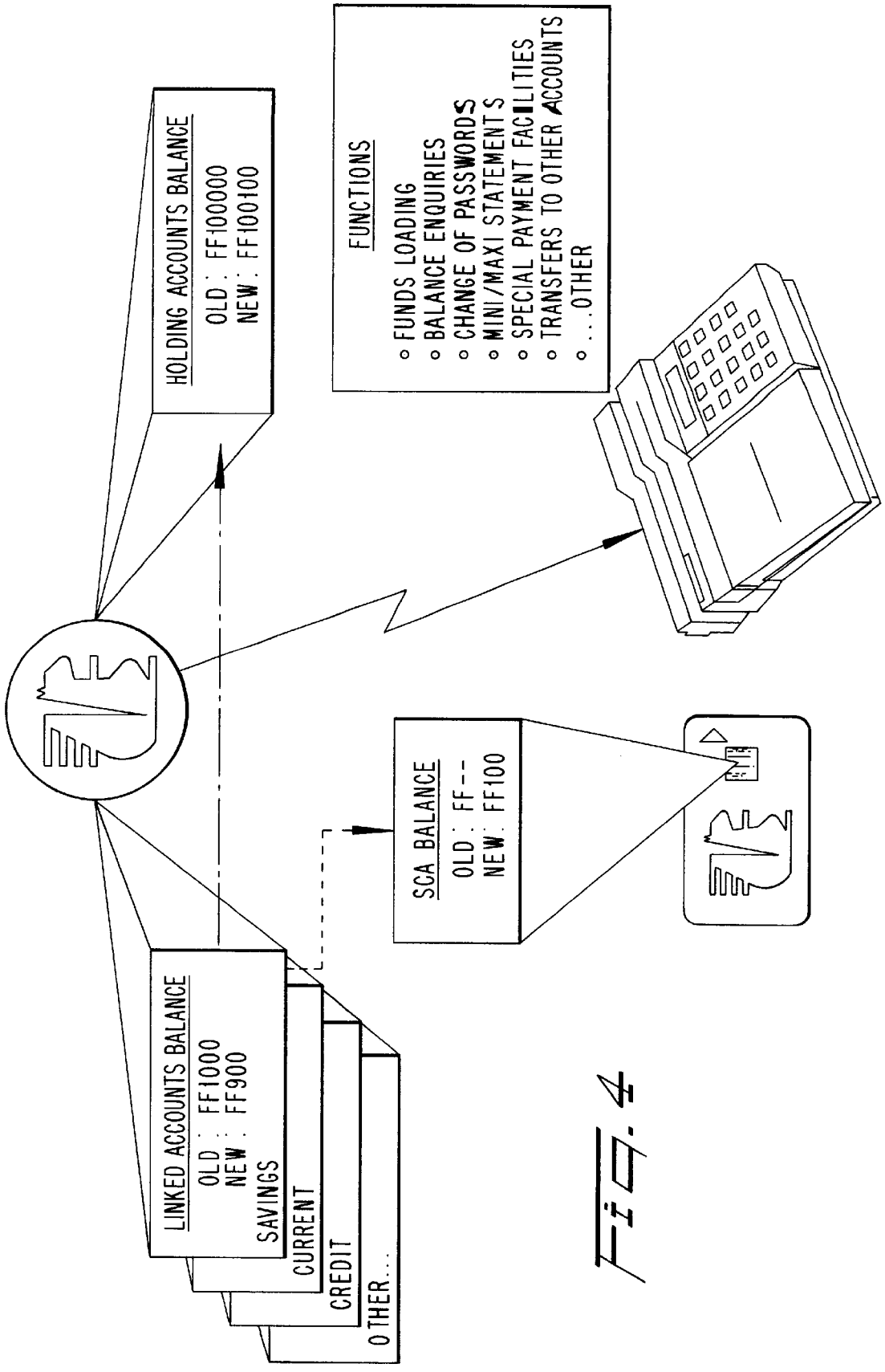

HOLDING ACCOUNTS BALANCE
OLD : FF100000
NEW : FF100100
FUNCTIONS
FUNDS LOADING
BALANCE ENQUIRIES
CHANGE OF PASSWORDS
MINI/MAXI STATEMENTS
SPECIAL PAYMENT FACILITIES
TRANSFERS TO OTHER ACCOUNTS
....OTHER
SCA BALANCE
OLD : FF--
NEW : FF100
LINKED ACCOUNTS BALANCE
OLD : FF1000
NEW : FF900
SAVINGS
CURRENT
CREDIT
OTHER....

Fig. 4

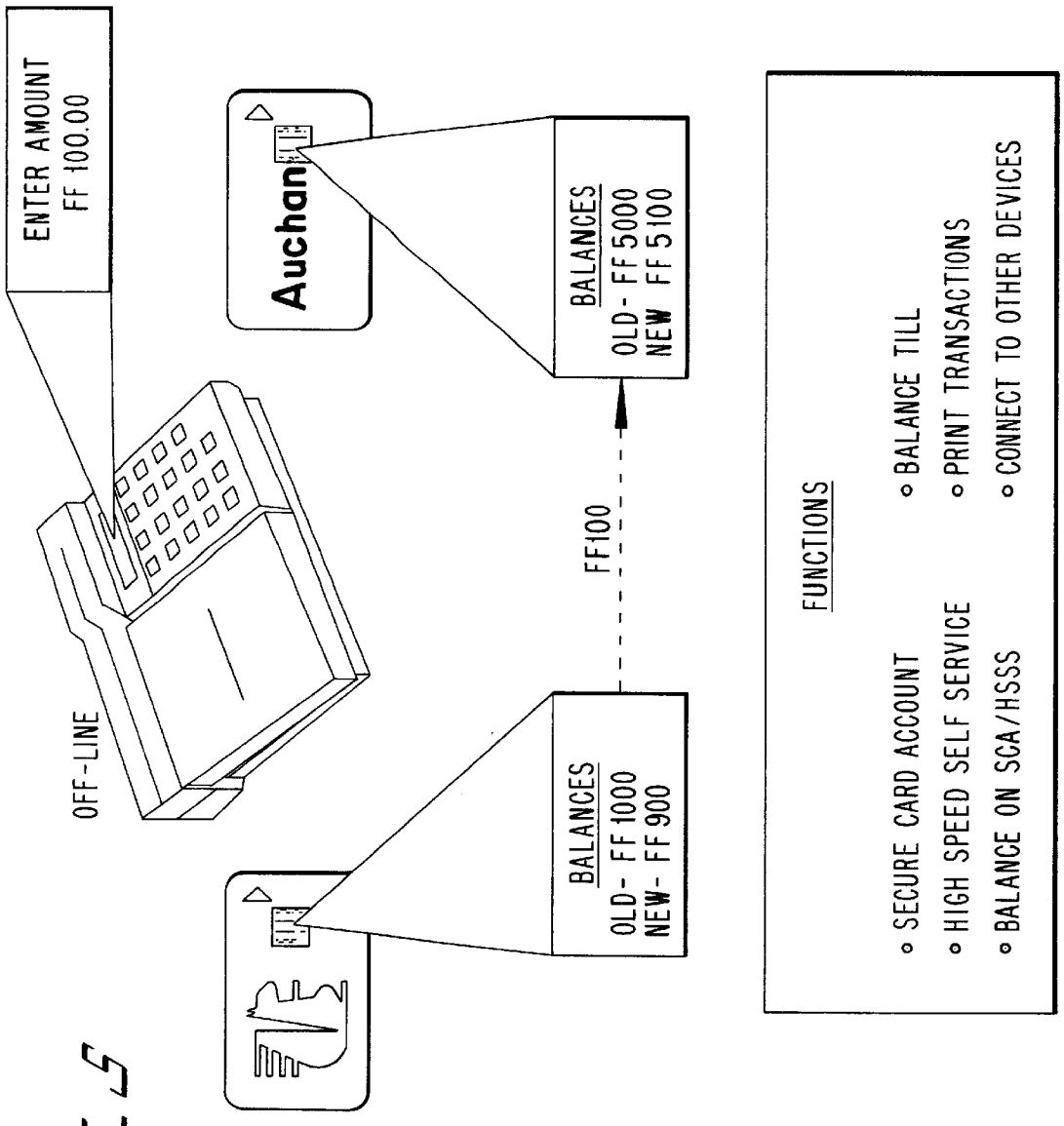

ENTER AMOUNT
FF 100.00
OFF-LINE
Auchan
BALANCES
OLD- FF 5000
NEW FF 5100
FF100
BALANCES
OLD- FF 1000
NEW- FF 900
FUNCTIONS
o SECURE CARD ACCOUNT
o HIGH SPEED SELF SERVICE
o BALANCE ON SCA/HSSS
o BALANCE TILL
o PRINT TRANSACTIONS
o CONNECT TO OTHER DEVICES

Fig. 5

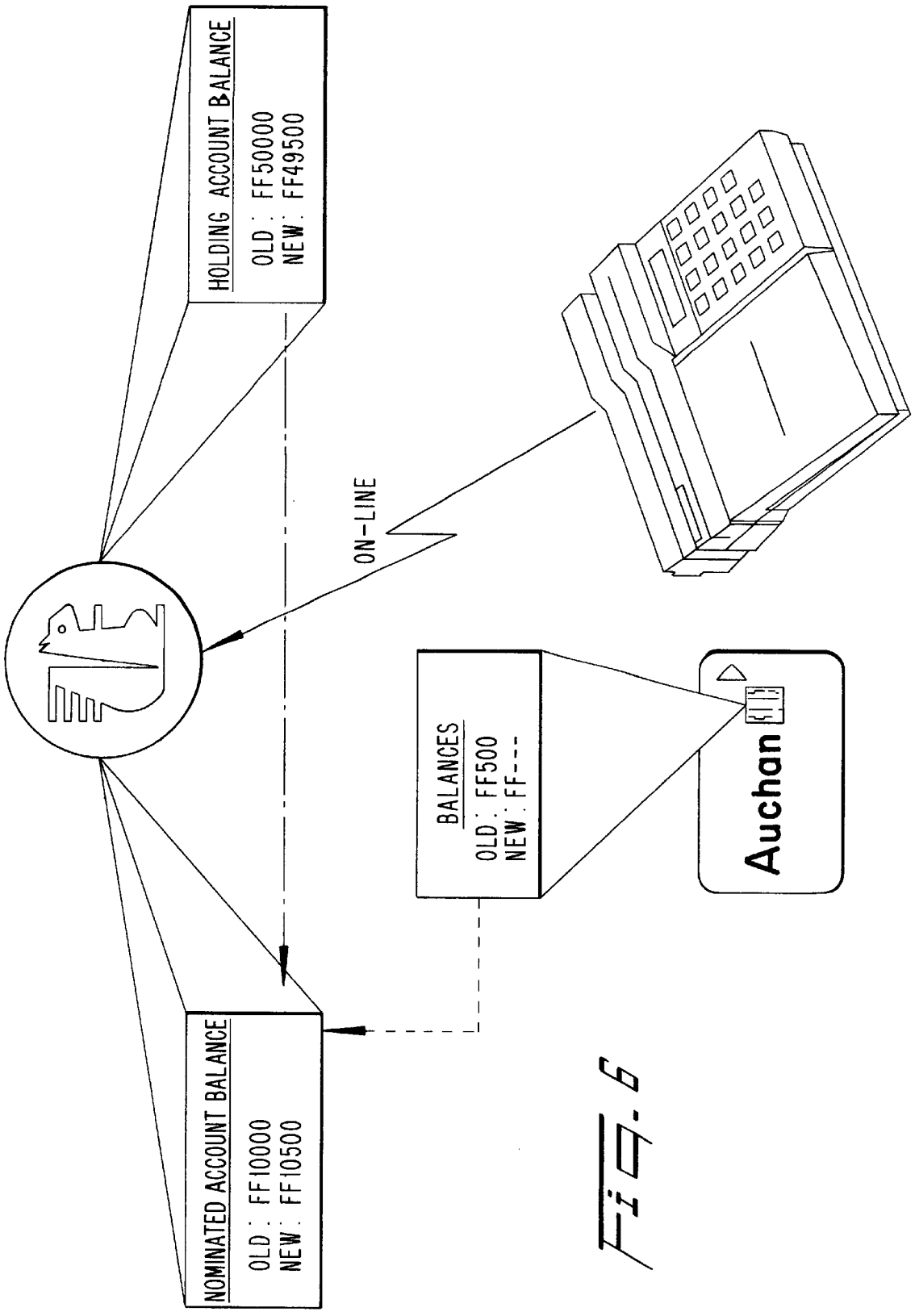

HOLDING ACCOUNT BALANCE
OLD : FF50000
NEW : FF49500
ON-LINE
BALANCES
OLD : FF500
NEW : FF---
Auchan
NOMINATED ACCOUNT BALANCE
OLD : FF10000
NEW : FF10500

Fig. 6

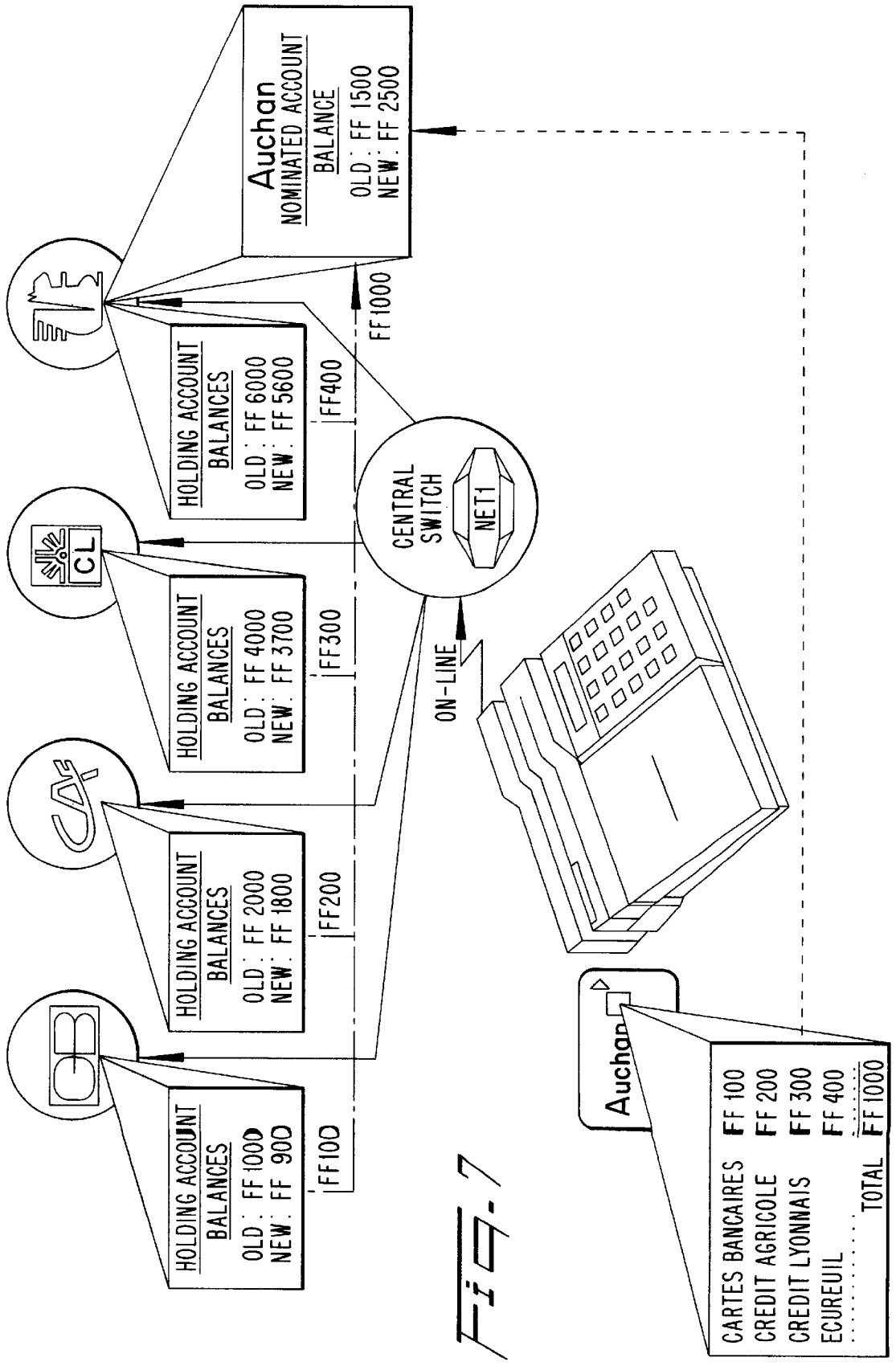

Auchan
NOMINATED ACCOUNT
BALANCE
OLD: FF 1500
NEW: FF 2500
FF1000
HOLDING ACCOUNT
BALANCES
OLD: FF 6000
NEW: FF 5600
FF400
HOLDING ACCOUNT
BALANCES
OLD: FF 4000
NEW: FF 3700
FF300
HOLDING ACCOUNT
BALANCES
OLD: FF 2000
NEW: FF 1800
FF200
HOLDING ACCOUNT
BALANCES
OLD: FF 1000
NEW: FF 900
FF100
CENTRAL SWITCH
NET1
ON-LINE
Auchan
CARTES BANCAIRES FF 100
CREDIT AGRICOLE FF 200
CREDIT LYONNAIS FF 300
ECUREUIL FF 400
TOTAL FF 1000

Fig. 7

FUNDS TRANSFER SYSTEM

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

This application claims priority of South African Patent Application No. 907106 filed Sep. 6, 1990 in the Republic of South Africa, in the name of inventors Mansvelt and Belamant.

BACKGROUND OF THE INVENTION

This invention relates to a method of and a system for transferring funds.

At present, remote banking generally involves the use of magnetic stripe cards, together with cheques or cash. The cards are encoded with information identifying holders of the cards. The information stored on the card is typically a primary account number (PAN). Typically, the card is inserted into an automatic teller machine (ATM) and a personal identification number (PIN) is entered by the cardholder. In some cases, the ATM verifies that the entered PIN corresponds with a PIN calculated by the ATM and then allows a transaction such as a withdrawal or deposit of funds to take place. If the ATM is on-line to the relevant financial institution, the account of the cardholder may be debited immediately a withdrawal takes place, or the ATM may store the transaction information, with the cardholder's account being debited at a later stage, utilising track **3** on the card. In any event, direct debiting or crediting of an account is generally limited to a two way transaction between a financial institution and an account holder at the financial institution.

Cheques, credit cards, debit cards and cash are also utilised for the purchasing of goods and services. However, these systems are cumbersome and risky and, if provided as on-line services, are relatively unreliable and expensive.

SUMMARY OF THE INVENTION

According to the invention a method of transferring funds includes the steps of linking a first portable data storage and processing device to a first financial institution; debiting an account held at the financial institution and recording a corresponding credit value in the first portable data storage and processing device; linking the first portable data storage device to a second, similar device; reducing the credit value in the first device and recording a corresponding credit value in the second device; linking the second portable data storage and processing device to a second financial institution; reducing the credit value in the second device; and recording a corresponding credit value in an account held at the second financial institution.

Preferably, the first and second devices each store at least a portion of a program which is run in a synchronised interactive manner between the first and second devices.

A terminal means may be provided which receives the first and second devices and permits data transfer therebetween, the terminal means operating under the control of a stored program to facilitate interaction of the first and second devices.

The first and second financial institutions may be one and the same or different banks, building societies or other similar institutions.

The first and second portable data storage and processing devices are preferably "smart cards" comprising electronic data storage and processing circuitry on a credit card-like substrate, operating under the control of stored software.

The first device may be allocated to an individual registered at the first financial institution, while the second device may be allocated to a retailer or other commercial entity, the magnitude of the reduction in the credit value stored in the first device corresponding to the value of a transaction between the individual and the retailer or commercial entity.

The second device may total the credit values recorded therein, so that the credit value recorded at the second financial institution corresponds to the total of all credit values recorded in the second device in a predetermined period. Further according to the invention a system for transferring funds includes first and second portable data storage and processing devices; first terminal means for linking the first device to a first financial institution; second terminal means for linking the second device to a second financial institution; and third terminal means adapted to receive the first and second devices and to permit data transfer between them, so that a credit value stored in the first device which corresponds to a debit from an account held at the first financial institution can be reduced by a desired amount and a corresponding credit value can be recorded in the second device, the second device being adapted to transfer the credit value stored therein to an account held at the second financial institution.

Preferably, the first and second devices each store at least a portion of a program which is run in a synchronised interactive manner between the first and second devices.

The first and second portable data storage and processing devices are preferably "smart cards" comprising electronic data storage and processing circuitry on a credit card-like substrate, operating under the control of stored software.

The first and second terminal means are preferably adapted to link the respective smart cards to the respective financial institutions via a digital or analogue data network.

The third terminal means is preferably a card reader device adapted to receive both smart cards and to allow data transfer therebetween.

Preferably, the card reader device operates under the control of a stored program which facilitates the interaction of the first and second smart cards.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic illustration of a funds transfer system according to the invention;

FIG. **2** is a schematic illustration of a basic mode of operation of the system of FIG. **1**;

FIG. **3** is a basic schematic block diagram of a card reader device used in the system of FIG. **1**; and

FIGS. **4** to **7** illustrate schematically several different operations possible with the system of FIG. **1**.

DESCRIPTION OF AN EMBODIMENT

The funds transfer system illustrated schematically in the drawings is designed to allow the direct transfer of funds

from a first financial institution to a cardholder, from the cardholder to a retailer, and from the retailer to a second financial institution, via an analogue or digital data network. In order to allow the necessary data to be transferred in a convenient manner, use is made of "smart cards". Such devices are well known and comprise a credit card-like substrate on which is mounted an integrated circuit containing a central processing unit (CPU) and associated random access memory (RAM) and read-only memory (ROM), as well as an electrically erasable programmable read-only memory (EEPROM). Contacts on the surface of the substrate allow a suitable card reader device to apply power to the computer on the card and permit data transfer to and from the computer.

The operation of the system is illustrated in a highly simplified form in the diagram of FIG. **2**. In the first leg of the process, a card holder obtains funds from an account held at a financial institution (FI). This is carried out in real time or on-line via a funds transfer machine (FTM) which is linked to the financial institution via the data network. The cardholder selects an amount to be credited to his personalised smart card (referred to hereinafter as a client card), and a credit balance on his credit card is increased, while the balance in his account at the financial institution is debited correspondingly.

The cardholder can now use his client card to conduct financial transactions of different kinds, in either an on-line or an off-line manner. Typically, as shown in FIG. **2**, the client card will be used by the cardholder in a transaction in which goods are purchased from a retailer. The retailer is provided with a point of sale (POS) device which is a self-contained, battery powered smart card reading device. To conduct a transaction, both the client card and a personalised smart card of the retailer (hereinafter called a retailer card) are both inserted into the POS device, which operates under the control of a stored program to allow communication between the client card and the retailer card. The amount of the transaction is entered into the POS device. This amount is then presented to the client card, which reduces the credit value stored in its EEPROM by the amount of the transaction, and forwards this amount to the retailer card which increases a credit value stored therein by the same amount.

Once the transaction is completed, the client card of the cardholder is removed from the POS device while the retailer card remains in the device. The retailer will typically conduct a number of different transactions with different cardholders during the course of a business day, and an accumulating total credit value will be stored in the retailer card. At intervals, typically at the end of each working day, the retailer will remove the retailer card from the POS device and insert it into a dedicated funds transfer machine (FTM) which is linked to a second financial institution (that is, the financial institution at which the retailer holds an account) via the electronic data network. The transaction information stored on the retailer card is transferred to the retailer's financial institution, which identifies the accounts of the various cardholders who have conducted transactions with the retailer, and which then credits the retailer's account with the total value of the transactions, and debits the financial institution's cardholder account with the value of the respective transaction. A magnetic tape record of the data transmissions conducted over the data network allows the respective financial institutions to generate printed statements for the cardholders and the retailer, if necessary. The cardholder can also use his card in an on-line manner, via an on-line funds transfer machine, to settle accounts, credit his card with a salary payment or another deposited amount, or conduct similar on-line transactions.

The advantage of an electronic funds transfer system of the kind described above in broad terms is that both conventional currency, such as cash or cheques, and conventional credit transactions, such a those employing credit cards, can be replaced. Delays in processing financial transactions are reduced or eliminated, while the use of cards on which a credit balance is stored ensures the availability of funds and reduces the risks associated with cash or credit transactions. Numerous other benefits arise from the use of an electronic data network, allowing a reduction in record-keeping and administration and reducing the likelihood of errors.

The operation of the funds transfer system will now be described in greater detail. A crucial part of the system is a card reader device which is adapted to receive two smart cards simultaneously, and effectively to allow communication between the cards. The card reader device is essentially conventional except for the provision of a second card reader slot and associated input/output circuitry. A suitable device is a type P500 terminal manufactured by Crouzet Sextant Avionique of France.

The circuitry of the card reader device is illustrated schematically in FIG. **3**, and is based around an Intel type 8096 microprocessor **10**. Associated with the microprocessor **10** is a random access memory (RAM) **12** and a read-only memory (ROM) **14**. First and second smart card readers **16** and **18** and an input/output (I/O) interface **20** comprising an RS232 interface are connected to the microprocessor **10**. Finally, a keypad **22**, a liquid crystal display (LCD) **24** and a miniaturised paper printer **26** are also controlled by the microprocessor **10**. The device is powered by a power supply circuit **28** comprising a rechargeable battery pack which allows the card reader to be operated for up to 30 days before replacement or recharging of the battery is necessary.

A boot program is stored in the ROM **14**, which initialises the card reader when it is turned on. An operating system and software controlling the operation of the card reader is downloaded into the RAM **12** via the I/O interface **20**, and must be reloaded if power is removed from the device.

The above described card reader device is used as a stand-alone point of sale (POS) device allowing communication between the client cart of a cardholder and the retailer card of the retailer. An essentially similar machine is used as a funds transfer machine (FTM) to allow communication between the client card and the cardholders financial institution, and to allow communication between the retailer card and the retailers financial institution. In this case however a modem is included in the device to link it to the electronic data network and thus to the respective financial institutions. In either case, the stored computer program in the RAM controls the operation of the device and generates prompts and other information which is displayed on the liquid crystal display **24** in use.

The first leg of a typical sequence of transactions will now be described, in which a cardholder transfers funds from an account held at his financial institution to his own client card. This is done using a card reader device as described above, configured as a funds transfer machine (FTM). Using the keypad **22**, the cardholder selects a "Funds transfer" option and enters the amount to be transferred and the type of account to be debited. A display is generated on the liquid crystal display **24**, prompting the cardholder to enter this card into the card reader device. Power is now applied to the card reader in the device, which applies power to the circuitry on the card itself. The microprocessor on the card initialises itself and outputs data to the card reader device indicating its operating parameters, including the baud rates, clock speed and data format which it uses. The card also outputs an identification code to the card reader device, indicating that it is a client card of the correct type.

Once the handshaking procedure between the client card and the FTM control card (as described in Appendices 1 and 2) is completed correctly, the transaction can continue. The cardholder is prompted to enter a password, which is checked with a corresponding code stored in a secure memory area on the card. If the correct password is not entered within three attempts, the card is disabled. Assuming that the correct password is entered, a file information table in the card memory is read, providing details, inter alia, of the current credit balance stored in the card.

The FTM now compiles a message for transmission via the data network, which includes critical fields such as the amount to be transferred, a transaction sequence number (TSN) and a unique sequence number (USN). The message is transmitted via the data network to the financial institution at which the cardholder holds an account. Assuming that there are sufficient funds in the cardholder's account to meet the request, the financial institution debits the cardholder's account and moves the funds to a holding account. The amount of the transfer, together with the TSN and the USN, is encrypted under the issuer key of the financial institution and transmitted back to the data network, which encrypts this encrypted data further with a data network key. The database of the data network is also updated with details of the transaction.

The message is routed back to the FTM, which extracts the encrypted portion of the data and transmits it, together with the data and account type, to the client card. The client card decrypts the encrypted data using the random key and the issuer key (both of which are stored securely on the card) and will check that the TSN and the USN in the decrypted data match the original TSN and USN. Assuming that a match occurs, the transaction is then written to the client card transaction file, and the current credit balance is updated on the card.

The FTM now runs a utility program on the client card which sends an 8 byte encrypted message to the FTM containing the TSN, the USN, and a code indicating whether the transaction was good or bad. The TSN stored in the card is incremented. The above data is encrypted with the data network key and is transmitted via the network to the financial institution for confirmation of the transaction. The display of the FTM now prompts the cardholder to remove his client card.

The result of the above transaction is that an amount of funds corresponding to the figure entered by the cardholder into the FTM is deducted from the credit balance of his account at the financial institution and transferred to a holding account of the financial institution. The credit balance stored on the client card is updated by the same amount, and can now be used to conduct further transactions. A state table of the above described transaction is shown in Appendix 1.

The above described transaction takes place between the financial institution and a so-called secure card account (SCA) which can only be accessed via a high security encryption/decryption procedure. The client card also makes provision for a high speed self service (HSSS) account which is limited to a relatively low maximum credit balance and which does not require the use of a password to be debited. This account can be used, for example, when using vending machines or the like, where relatively small amounts are involved. A state table showing how funds are transferred from the secure card account (SCA) to the high speed self service (HSSS) account is shown in Appendix 2.

Assuming now that cardholder wishes to conduct a transaction with a retailer, such as the purchase of goods or services, the card reader terminal illustrated in FIG. **3** is used, configured as a point of sale (POS) device. When this device is turned on by the retailer, the display prompts the retailer to enter the retailer card into the appropriate slot at the bottom of the machine. The card outputs its identity code to the device, which verifies that it is a retailer card, and a handshaking procedure is carried out as described above with reference to the funds transfer machine.

The retailer card has a merchant information file which stores, inter alia, the merchant's name, a "hot card" file and transaction batch numbers. The main menu of the software stored in the terminal is now displayed, and offers a choice of "Sales" or "Utilities". Assuming that "Sales" is selected, a second menu appears, offering a choice of "Purchase" or "Card balance". The latter option allows the retailer to check the running total credit balance stored in his card.

Assuming that the "Purchase" option is selected, the display will then prompt the retailer to enter the amount of the transaction. This can be done directly via the keypad **22**, or via the input/output interface **20**, if the card reader terminal is connected to a till. The display now prompts the cardholder to enter his client card into the second card reader, and a handshaking procedure once again takes place to ensure that the correct type of card is being used.

The sequence of events is described in the state table of Appendix 3, and includes the generation of a random key by the client card which is then used in the subsequent messages for this transaction. The retailer card checks to see whether the credit balance stored thereon is below the permissable maximum and that the amount of the transaction will not cause the balance to exceed the maximum. Information from the client card is now read into the RAM **12** of the terminal, including the client identification code and balance information. Once the security measures (up to and including Utility 4 in Appendix 3) have been carried out, the terminal prompts the card holder to indicate whether a secure card account (SCA) transaction or a high speed self service (HSSS) transaction is desired. The terminal now runs

a utility to check whether the client card is on the "hot card" list stored on the retailer card, and if so, aborts the transaction, and switches off the client card.

The terminal now prompts the cardholder to enter his password. If the correct password is recognised, a flag is set in the RAM of the card. The amount of the transaction, the date, the retailer identity, and the transaction batch number are now transferred directly to the client card in an unencrypted form. The microprocessor of the client card checks that the flag in the RAM is correctly set to indicate the use of the correct password, and checks the identity of the retailer card to ensure that it is in fact a retailer card. The transaction information is then stored in the RAM of the card. The transaction information is now written to the transaction file on the client card and the balance in the client card is updated (that is, reduced) and stored in a non volatile memory area of the card. If the amount of the transaction is greater than the stored balance (that is, an impermissible transaction) the card is put into a CPU loop so that it "hangs", and cannot be reset except by aborting the transaction. Once the transaction has been encrypted and recorded, the RAM of the card is cleared.

The terminal now transmits the encrypted transaction information to the retailer card, and the cardholder's identification number and the record sequence number are checked, both to ensure a valid transaction and to ensure correct decryption. The accumulated credit balance on the retailer card is now updated. Similarly to the client card, the card will "hang" if the total balance exceeds the maximum permissible limit. The amount of the transaction, the client card unique sequence number (USN), and the financial institution issuer code are now encrypted with the key of the data network, and this information is stored in a non volatile area on the retailer card. The total number of SCA transactions is incremented, and the transaction information is written to the retailer card transaction file. This information is further encrypted with the card reader terminal key, as contained on the retailer card.

The encrypted information is now transferred to the RAM **12** of the card reader terminal, and a transaction record is printed using the printer **26**. On the same record, an encrypted record of the transaction is printed, in a 16 byte format, to ensure, if necessary, that the retailer has not modified the POS device software. The cardholder is now prompted to remove his card, and the original main menu is displayed.

The result of the above transaction is that the credit balance on the client card is reduced by the amount of the transaction, and the accumulated credit balance on the retailer card is increased correspondingly. The printed transaction record, including its encrypted data, allows errors to be traced. The entire transaction takes place on an off-line basis, using only the two smart cards (the client card and the retailer card) and the stand-alone card reader terminal.

In the case of a high speed self service (HSSS) transaction, a simplified procedure is followed. A state table of such a transaction is shown in Appendix 4.

The next step in the operation of the system is for the retailer to settle the transactions, whether SCA or HSSS transactions, recorded on his retailer card. The settlement procedure is once again an on-line procedure, requiring the use of a funds transfer machine (FTM). This may be a dedicated device located on the premises of the retailer, or may be located elsewhere.

Using the keypad of the FTM, the retailer chooses the "settlement" option, and is prompted via the display to insert his card. The FTM then conducts the usual handshaking procedure between the FTM card inserted into the machine and the retailer card. A utility on the retailer card is now run which outputs the batch total, date, batch number, number of transactions and the retailer card USN, all encrypted under the data network key. This data is then transmitted to the data network through the pre-initialised communications link, typically a XXX pad. Transactions which are encrypted using the data network key are sent to the data network on a one to one basis, and are confirmed by the network. The network decrypts the received data and conducts a number of validity checks, for example, by checking the sum of all transaction amounts against the total in the batch data.

The batch number and the new batch data are now encrypted by the data network with the data network key, and transmitted back to the FTM. The FTM transfers this data to the retailer card, and the retailer card decrypts the data and checks that the batch numbers remain the same. The retailer card then increments the batch number and updates it, enters the batch date, and resets all totals to zero. The transaction address on the file information table (FIT) on the card is reset to the first address position, and a bit flag is set which allows the transaction file to be overwritten by the data network hot card file. A utility is then run to write the hot card file to the transaction file. Finally, the FTM prompts the retailer to remove the retailer card. The batch transaction data is transmitted via the data transfer network to the financial institution of the retailer, updating the retailer's account by crediting it with the total value of the transactions. The network also sends a message to the financial institution of each cardholder who conducted a transaction in the particular batch concerned, authorising a transfer of funds from the holding account of the cardholder's financial institution to the retailer's financial institution. A state table illustrating the above settlement procedure appears in Appendix 5.

It will be apparent from the above description that the entire chain of financial transactions is accomplished by the direct transfer of information between the financial institutions concerned and the client and retailer smart cards. By the use of high levels of encryption, a high security level is achieved. This is made possible mainly by the use of intelligent cards which can communicate with one another, via an intelligent terminal device, which permits the necessary high standard of encryption/decryption and other security procedures to be achieved. Diagrams illustrating the various transactions are shown in FIGS. **4** to **7**.

An important aspect of the invention is the running of a program (application) which is effectively split between the two (or more) CPU's of the smart cards. The running of these CPU's is facilitated and synchronised by the card reader terminal, which itself runs a stored program. However, the transaction is controlled by the programs stored on the cards themselves, while the terminal merely allows direct communication between the cards, consistent with the operating protocol of the cards.

Although the funds transfer system of the invention has be described in relation to a conventional, typical series of transactions, it will be appreciated that the applicability of the system is wider than the specific example given above. The described system can be used to operate savings, transmission and current accounts, as well as credit accounts (including general credit accounts and specific credit accounts such as petrol or garage type accounts). The system is also applicable to the running of mortage bond accounts, subscription deposit accounts, or foreign exchange accounts, for example.

APPENDIX 1

Client (Utility)	FTM (Control)
UTIL_1: Function: Generate random number. Encrypt random number. card type and currency with transaction key. Output. Dependencies: None	
	UTIL_2: Function: Input. Decrypt with transaction key. Encrypt random number and card type with random key. Dependencies: Utility card must be client card. UTIL_3: Function: Output. Dependencies: None.
UTIL_2: Function: Input. Decrypt with random key. Dependencies: Random number must match random number generated in UTIL_1.	
UTIL_9: Function: Input. Decrypt with Metrolink key and issuer key. Write transaction. Update balance. Clear RAM. Dependencies: Control card presented in UTIL_2 must be FTM card. Password must have been presented. Client transaction sequence numbers must match. Transactions amount cannot overflow SCA balance.	

APPENDIX 2

Client (Utility)	FTM (Control)
UTIL_1: Function: Generate random number. Encrypt random number. card type and currency with transaction key. Output. Dependencies: None	
	UTIL_2: Function: Input. Decrypt with transaction key. Encrypt random number and card type with random key. Dependencies: Utility card must be client card. UTIL_3: Function: Output. Dependencies: None.
UTIL_2: Function: Input. Decrypt with random key. Dependencies: Random number must match random number generated in UTIL_1.	
UTIL_7: Function: Input. Write transaction. Update balances. Clear RAM. Dependencies: Control card presented in UTIL_2 must be FTM card. Password must have been presented. Transaction amount cannot be greater than SCA balance. Transaction amount cannot overflow HSSS balance.	

APPENDIX 3

Client (Utility)	Retailer (Control)
UTIL_1: Function: Generate random number. Encrypt random number. card type and currency with transaction key. Output. Dependencies: None	
	UTIL_4: Function: Input. Decrypt with transaction key. Encrypt random number, record sequence number & card type with random key. Dependencies: Retailer card can not be full. Utility card must be client card. Currencies must match. UTIL_5: Function: Output. Dependencies: None.
UTIL_2: Function: Input. Decrypt with random key. Dependencies: Random number must match random number generated in UTIL_1. UTIL_4: Function: Input. Handle information. Dependencies: Password must have been presented. Control card presented in UTIL_2 must be retailer card. UTIL_6: Function: Write transaction. Update balance. Encrypt amount, client card unique sequence number and record sequence number with random key. Output. Clear RAM. Dependencies: Paynote amount presented to card in UTIL_4 must be greater than zero. Paynote amount cannot be greater than SCA balance.	
	UTIL_6: Function: Input. Decrypt with random key. Update balance. Write transaction. Encrypt amount, client card unique sequence number and issuer code with metrolink 1 key. Dependencies: Utility card presented in UTIL_4 must be client card. Record sequence number must match. Paynote amount cannot overflow batch total. UTIL_5: Function: Output. Dependencies: None.

APPENDIX 4

Client (Utility)	Retailer (Control)
UTIL_1: Function: Generate random number. Encrypt random number. card type and currency with transaction key. Output. Dependencies: None	
	UTIL_4: Function: Input. Decrypt with transaction key. Encrypt random number, record sequence number & card type with random key. Dependencies: Retailer card can not be full. Utility card must be client card. Currencies must match. UTIL_5: Function: Output. Dependencies: None.
UTIL_2: Function: Input. Decrypt with random key. Dependencies: Random number must match random number generated in UTIL_1. UTIL_4: Function: Input. Handle information. Dependencies: Control card presented in UTIL_2 must be retailer card. UTIL_6:	

APPENDIX 4-continued

Client (Utility)	Retailer (Control)
Function: Write transaction. Update balance. Encrypt amount, client card unique sequence number and record sequence number with random key. Output. Dependencies: Paynote amount presented to card in UTIL_4 must be greater than zero. Paynote amount cannot be greater than HSSS balance.	
	UTIL_6: Function: Input. Decrypt with random key. Update balance. Write transaction. Encrypt amount, client card unique sequence number and issuer code with metrolink 1 key. Dependencies: Utility card presented in UTIL_4 must be client card. Record sequence number must match. Paynote amount cannot overflow batch total.
	UTIL_5: Function: Output. Dependencies: None.

APPENDIX 5

Retailer (Utility)	FTM (Control)
	UTIL_1: Function: Generate random number. Encrypt random number and card type with transaction key. Output. Dependencies: None
UTIL_1: Function: Input. Decrypt with transaction key. Dependencies: None	
UTIL_2: Function: Encrypt batch number, batch total and batch date with metrolink key. Encrypt batch number. retailer card unique sequence number & total number of transactions with metrolink key. Output. Dependencies: Control card presented in UTIL_1 must be FTM card.	
UTIL_3: Function: Input. Decrypt with metrolink key. Reset batch. Dependencies: Batch number must match batch number encrypted in UTIL_2.	

We claim:

1. A method of transferring funds including the steps of:

linking a first portable data storage and processing device to a first financial institution, the first portable data storage device storing at least a portion of a program;

debiting an account held at the financial institution and recording a corresponding credit value in the first portable data storage and processing device;

linking the first portable data storage device to a second, similar device via a terminal means, the second portable data storage device storing at least a portion of a program which is run in a synchronized, interactive manner with the portion of the program stored in the first portable data storage device;

reducing the credit value in the first device and recording a corresponding credit value in the second device;

linking the second portable data storage and processing device to a second financial institution;

reducing the credit value in the second device;

and recording a corresponding credit value in an account held at the second financial institution.

2. A method according to claim **1** wherein the terminal means receives the first and second devices and permits data transfer therebetween, the terminal means operating under the control of a stored program to facilitate interaction of the first and second devices.

3. A method according to claim **1** wherein the first and second financial institutions are one and the same bank, building society or another similar institution.

4. A method according to claim **1** wherein the first and second financial institutions are different banks, building societies or other similar financial institutions.

5. A method according to claim **1** wherein the first and second portable data storage and processing devices are "smart cards" comprising electronic data storage and processing circuitry on a credit card-like substrate, operating under the control of stored software.

6. A method according to claim **1** wherein the first device is allocated to an individual registered at the first financial institution, while the second device is allocated to a retailer or other commercial entity, the magnitude of the reduction in the credit value stored in the first device corresponding to

the value of a transaction between the individual and the retailer or commercial entity.

7. A method according to claim **1** wherein the second device totals the credit values recorded therein, so that the credit value recorded at the second financial institution corresponds to the total of all credit values recorded in the second device in a predetermined period.

8. A system for transferring funds including:

first and second portable data storage and processing devices, each storing at least a portion of a program which is run in a synchronized, interactive manner between the first and second devices;

first terminal means for linking the first device to a first financial institution;

second terminal means for linking the second device to a second financial institution;

and third terminal means adapted to receive the first and second devices and to permit data transfer between them, so that a credit value stored in the first device which corresponds to a debit from an account held at the first financial institution can be reduced by a desired amount and a corresponding credit value can be recorded in the second device, the second device being adapted to transfer the credit value stored therein to an account held at the second financial institution.

9. A system according to claim **8** wherein the first and second portable data storage and processing devices are "smart cards" comprising electronic data storage and processing circuitry on a credit card-like substrate, operating under the control of stored software.

10. A system according to claim **9** wherein the first and second terminal means are adapted to link the respective smart cards to the respective financial institutions via a data network.

11. A system according to claim **9** wherein the third terminal means is a card reader device adapted to receive both smart cards and to allow data transfer therebetween.

12. A system according to claim **11** wherein the card reader device operates under the control of a stored program which facilitates the interaction of the first and second smart cards.

13. A method of transferring funds comprising:

linking a first smart card to a first financial institution, said first smart card storing at least a portion of a program;

debiting a first account held at said first financial institution and recording a corresponding credit value in said first smart card;

linking said first smart card to a second, similar smart card via a terminal means, said second smart card storing at least a portion of said program which is run in a synchronized, interactive manner with the portion of said program stored in said first smart card, said program being consistent with a value transfer protocol of said smart cards;

reducing said credit value in said first smart card and recording a corresponding credit value in said second smart card;

linking said second smart card to a second financial institution;

reducing said credit value in said second smart card; and

recording a corresponding credit value in an account held at said second financial institution.

14. A method as recited in claim 13 wherein said terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value and receives said first and second smart cards and permits data transfer therebetween, said terminal means facilitating interaction of said first and second smart cards.

15. A method as recited in claim 13 wherein said first smart card is allocated to an individual registered at said first financial institution and said second smart card is allocated to a commercial entity, and wherein the magnitude of the reduction in said credit value stored in said first smart card corresponds to the value of a transaction between said individual and said commercial entity, whereby the direct transfer of currency from said individual to said commercial entity is allowed.

16. A method as recited in claim 13 wherein said value transfer protocol ensures implementation of a predetermined transaction sequence to effect the transfer of credit value from said first smart card to said second smart card.

17. A method as recited in claim 16 wherein said first and second smart cards exchange messages during said transaction sequence and wherein subsequent messages carry information from previous messages, whereby implementation of said predetermined transaction sequence is ensured.

18. A method as recited in claim 13 further comprising:

sending a first random challenge from said first smart card to said second smart card, thereby ensuring to said first smart card that said second smart card is valid; and

sending a second random challenge from said second smart card to said first smart card, thereby ensuring to said second smart card that said credit value in said first smart card has been reduced.

19. A method as recited in claim 13 wherein at least one of said smart cards is embodied within an integrated circuit mounted on a substrate and wherein contacts on a surface of said substrate allow said terminal means to apply power to said integrated circuit and to permit data transfer to and from said integrated circuit.

20. A method of transferring funds comprising:

linking a first smart card to a first financial institution, said first smart card storing at least a portion of a program;

debiting a first account held at said first financial institution and recording a corresponding credit value in said first smart card;

linking said first smart card to a second, similar smart card via a terminal means, said second smart card storing at least a portion of said program which is run in a synchronized, interactive manner with the portion of said program stored in said first smart card;

exchanging messages between said first and second smart cards, each reply message being dependent upon information received from an earlier message;

determining whether each received message is valid using said information received from an earlier message, wherein when it is determined that a message is not valid, said program terminates;

reducing said credit value in said first smart card and recording a corresponding credit value in said second smart card;

linking said second smart card to a second financial institution;

reducing said credit value in said second smart card; and

recording a corresponding credit value in a second account held at said second financial institution.

21. A method as recited in claim 20 wherein said terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value and receives said first and second smart cards and permits data transfer therebetween, said terminal means facilitating interaction of said first and second smart cards.

22. A method of transferring funds comprising:

linking a first smart card to a first financial institution, said first smart card storing at least a portion of a program;

debiting a first account held at said first financial institution and recording a corresponding credit value in said first smart card;

linking said first smart card to a second, similar smart card via a terminal means, said second smart card storing at least a portion of said program;

running said program in a synchronized, interactive manner between said smart cards;

a step for performing the function of ensuring that said first and second smart cards are valid and are continuously linked during said running, whereby fraud is reduced;

reducing said credit value in said first smart card and recording a corresponding credit value in said second smart card;

linking said second smart card to a second financial institution;

reducing said credit value in said second smart card; and

recording a corresponding credit value in a second account held at said second financial institution.

23. A method as recited in claim 22 wherein said terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value and receives said first and second smart cards and permits data transfer therebetween, said terminal means facilitating interaction of said first and second smart cards.

24. A smart card for transferring funds, said smart card being arranged for effecting the following:

linking a first smart card to a first financial institution, said first smart card storing at least a portion of a program;

debiting a first account held at said first financial institution and recording a corresponding credit value in said first smart card;

linking said first smart card to a second, similar smart card via a terminal means, said second smart card storing at least a portion of said program which is run in a synchronized, interactive manner with the portion of said program stored in said first smart card, said program being consistent with a value transfer protocol of said smart cards;

reducing said credit value in said first smart card and recording a corresponding credit value in said second smart card;

linking said second smart card to a second financial institution;

reducing said credit value in said second smart card; and

causing a corresponding credit value to be recorded in a second account held at said second financial institution.

25. A smart card as recited in claim 24 wherein said terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value, and wherein said terminal means receives said first and second smart cards and permits data transfer therebetween and facilitates interaction of said first and second smart cards.

26. A smart card as recited in claim 24 wherein said first smart card is allocated to an individual registered at said first financial institution and said second smart card is allocated to a commercial entity, and wherein the magnitude of the reduction in said credit value stored in said first smart card corresponds to the value of a transaction between said individual and said commercial entity, whereby the direct transfer of currency from said individual to said commercial entity is allowed.

27. A smart card as recited in claim 24 being further arranged wherein said value transfer protocol ensures implementation of a predetermined transaction sequence to effect the transfer of credit value from said first smart card to said second smart card.

28. A smart card as recited in claim 24 being further arranged wherein said first and second smart cards exchange messages during said transaction sequence and wherein subsequent messages carry information from previous messages, whereby implementation of said predetermined transaction sequence is ensured.

29. A smart card as recited in claim 24 being further arranged for effecting the following:

sending a first random challenge from said first smart card to said second smart card, thereby ensuring to said first smart card that said second smart card is valid; and

sending a second random challenge from said second smart card to said first smart card, thereby ensuring to said second smart card that said credit value in said first smart card has been reduced.

30. A smart card as recited in claim 24 being embodied within an integrated circuit mounted on a substrate and having contacts on a surface of said substrate to allow said terminal means to apply power to said integrated circuit and to permit data transfer to and from said integrated circuit.

31. A system for transferring funds comprising:

first and second smart cards, each storing at least a portion of a program which is run in a synchronized, interactive manner between said first and second smart cards, said program being consistent with a value transfer protocol of said smart cards;

first terminal means for linking said first smart card to a first financial institution;

second terminal means for linking said second smart card to a second financial institution; and

third terminal means adapted to receive said first and second smart cards and to permit data transfer between them, so that a credit value stored in said first smart card which corresponds to a debit from an account held at said first financial institution can be reduced by a desired amount and a corresponding credit value can be recorded in said second smart card, said second smart card being adapted to transfer said credit value stored therein to an account held at said second financial institution.

32. A system as recited in claim 31 wherein said third terminal means is a single unit including a keypad for

entering said credit value and a display for displaying said credit value and receives both smart cards and allows data transfer therebetween, said third terminal means facilitating interaction of said first and second smart cards.

33. A system as recited in claim 31 wherein said first smart card is allocated to an individual registered at said first financial institution and said second smart card is allocated to a commercial entity, and wherein the magnitude of the reduction in said credit value stored in said first smart card corresponds to the value of a transaction between said individual and said commercial entity, whereby the direct transfer of currency from said individual to said commercial entity is allowed.

34. A system as recited in claim 31 wherein said value transfer protocol ensures implementation of a predetermined transaction sequence to effect the transfer of said credit value from said first smart card to said second smart card.

35. A system as recited in claim 34 wherein said first and second smart cards exchange messages during said transaction sequence and wherein subsequent messages carry information from previous messages, whereby implementation of said predetermined transaction sequence is ensured.

36. A system as recited in claim 31

wherein said first smart card is further adapted to send a first random challenge to said second smart card, thereby ensuring to said first smart card that said second smart card is valid; and

wherein said second smart card is further adapted to send a second random challenge to said first smart card, thereby ensuring to said second smart card that said credit value in said first smart card has been reduced.

37. A system according to claim 31 wherein at least one of said smart cards is embodied within an integrated circuit mounted on a substrate and contacts on a surface of said substrate allow said terminal means to apply power to said integrated circuit and to permit data transfer to and from said integrated circuit.

38. A system for transferring funds comprising:

first and second smart cards, each storing at least a portion of a program which is run in a synchronized, interactive manner between said first and second smart cards;

said program stored on said smart cards being arranged to perform the following when run,

exchanging messages between said first and second smart cards, each reply message being dependent upon information received from an earlier message, and

determining whether each received message is valid using said information received from an earlier message, wherein when it is determined that a message is not valid, said program terminates;

first terminal means for linking said first smart card to a first financial institution;

second terminal means for linking said second smart card to a second financial institution; and

third terminal means adapted to receive said first and second smart cards and to permit data transfer between them, so that a credit value stored in said first smart card which corresponds to a debit from an account held at said first financial institution can be reduced by a desired amount and a corresponding credit value can be recorded in said second smart card, said second smart card being adapted to transfer said credit value stored therein to an account held at said second financial institution.

39. A system as recited in claim 38 wherein said third terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value and receives both smart cards and allows data transfer therebetween, said third terminal means facilitating interaction of said first and second smart cards.

40. A system for transferring funds comprising:

first and second smart cards, each storing at least a portion of a program which is run in a synchronized, interactive manner between said first and second smart cards;

means for performing the function of ensuring that said first and second smart cards are valid and are continuously linked during said program, whereby fraud is reduced;

first terminal means for linking said first smart card to a first financial institution;

second terminal means for linking said second smart card to a second financial institution; and

third terminal means adapted to receive said first and second smart cards and to permit data transfer between them, so that a credit value stored in said first smart card which corresponds to a debit from an account held at said first financial institution can be reduced by a desired amount and a corresponding credit value can be recorded in said second smart card, said second smart card being adapted to transfer said credit value stored therein to an account held at said second financial institution.

41. A system as recited in claim 40 wherein said third terminal means is a single unit including a keypad for entering said credit value and a display for displaying said credit value and receives both smart cards and allows data transfer therebetween, said third terminal means facilitating interaction of said first and second smart cards.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : Re. 36,788
DATED : July 25, 2000
INVENTOR(S) : Mansvelt et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page,
Item [73] Assignee: delete "**Visa International Service Association,** Foster City, Calif." and insert "**Net1 Holdings S.A.R.L.,** Luxembourg."

Signed and Sealed this

Twenty-eighth Day of August, 2001

Attest:

Nicholas P. Godici

Attesting Officer

NICHOLAS P. GODICI
Acting Director of the United States Patent and Trademark Office