

SYSTEMS AND METHODS FOR FACILITATING AND CONDUCTING TRANSACTIONS

FIELD OF INVENTION

[001] The present invention relates broadly, but not exclusively, to systems and methods for facilitating and conducting transactions.

BACKGROUND

[002] Traditionally, if one party (a benefactor) wishes to transfer money to another party (a beneficiary), the benefactor can visit an automated teller machine (ATM) and withdraw cash and thereafter physically hand the cash over to the beneficiary. Alternatively, some ATMs allow a benefactor to electronically transfer money from the benefactor's account to a beneficiary's account. In recent times, Internet-banking websites and mobile applications installed on smart phones allow users to electronically transfer money from one account to another without needing to visit an ATM.

[003] However, not everyone may have access to computers or smart phones to perform online electronic money transfers. For example, the elderly may not have access to computers or smart phones, or may not be confident in using computers or smart phones to perform online electronic money transfers.

[004] The traditional method of visiting and withdrawing cash from an ATM, and thereafter physically handing the cash over to a beneficiary is not preferred as there are security concerns with physically handling large sums of money, especially among vulnerable persons such as the elderly and young children.

[005] A need therefore exists to provide systems and methods for facilitating and conducting transactions that seek to address at least some of the above problems.

SUMMARY

[006] According to a first aspect, there is provided a system for facilitating a transaction, comprising: a receiver module configured to receive a beneficiary account number and a transaction amount; a generator module configured to generate code data based on the beneficiary account number, the transaction amount and a timestamp; an encoder module configured to encode the code data in a machine-readable code, wherein the code data can be subsequently decoded for use during the transaction; and an identifier module configured to assign an identifier that is uniquely associated with the code data.

[007] According to a second aspect, there is provided a method for facilitating a transaction, comprising: receiving, at a receiver module, a beneficiary account number and a transaction amount; generating, using a generator module, code data based on the beneficiary account number, the transaction amount and a timestamp; encoding, using an encoder module, the code data in a machine-readable code, wherein the code data can be subsequently decoded for use during the transaction; and assigning, using an identifier module, an identifier that is uniquely associated with the code data.

[008] According to a third aspect, there is provided a system for conducting a transaction, comprising: a code decoder module configured to decode code data that is encoded in a machine-readable code, wherein the code data comprises a beneficiary account number, a transaction amount and a timestamp; and a processor module configured to: determine an identifier which is uniquely associated with the code data, wherein the code data is stored in association with the identifier in a database module that is communicatively connected to the processor module; and retrieve a benefactor account number that is stored in association with the identifier in the database module, wherein the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number.

[009] According to a fourth aspect, there is provided a method for conducting a transaction, comprising: decoding, using a code decoder module, code data that is encoded in a machine-readable code, wherein the code data comprises a beneficiary account number, a transaction amount and a timestamp; determining, using a processor module, an identifier which is uniquely associated with the code data, wherein the code data is stored in association with the identifier in a database module;

and retrieving, using the processor module, a benefactor account number that is stored in association with the identifier in the database module, wherein the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Embodiments and implementations are provided by way of example only, and will be better understood and readily apparent to one of ordinary skill in the art from the following written description, read in conjunction with the drawings, in which:

[0011] Figure 1 shows a flow chart illustrating a method for conducting a transaction, according to an example embodiment;

[0012] Figure 2 shows a flow chart illustrating a method for conducting a transaction, according to another example embodiment;

[0013] Figure 3 shows a flow chart illustrating a method for conducting a transaction, according to yet another example embodiment;

[0014] Figure 4 shows a flow chart illustrating a method for conducting a transaction, according to yet another example embodiment;

[0015] Figure 5 shows a schematic of a system for facilitating a transaction, according to an example embodiment;

[0016] Figure 6 shows a flow chart illustrating a method for facilitating a transaction, according to an example embodiment;

[0017] Figure 7 shows a schematic of a system for conducting a transaction, according to an example embodiment;

[0018] Figure 8 shows a flow chart illustrating a method for conducting a transaction, according to an example embodiment; and

[0019] Figure 9 shows a schematic diagram of a computer system suitable for use in executing at least some steps of the method for conducting or facilitating a

transaction and/or for realizing at least a part of the system for conducting or facilitating a transaction.

DETAILED DESCRIPTION

[0020] Embodiments will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0021] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0022] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “receiving”, “scanning”, “calculating”, “determining”, “replacing”, “generating”, “initializing”, “outputting”, or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0023] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes, or may comprise a computer or other device selectively activated or reconfigured by a computer program stored in the computer. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer

suitable for executing the various methods / processes described herein will appear from the description below.

[0024] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the invention.

[0025] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the GSM mobile telephone system. The computer program when loaded and executed on such a computer effectively results in an apparatus that implements the steps of the preferred method.

[0026] Figure 1 shows a flow chart illustrating a method for conducting a transaction, according to an example embodiment. A user (a benefactor) wishes to transfer money to another user (a beneficiary). At step 102, the benefactor visits an automated teller machine (ATM) and inserts his ATM card. At step 104, the benefactor enters his personal identification number (PIN) for authentication purposes. At step 106, the benefactor enters the beneficiary's (i.e. fund recipient's) account number. At step 108, the benefactor enters the amount of funds that he wishes to transfer to the beneficiary.

[0027] At step 110, the ATM generates a code or token based on the beneficiary's account number, the amount of funds to be transferred (i.e. transaction amount) and a timestamp corresponding to the time and/or date of the fund transfer request. The code is preferably a machine-readable code and also preferably not

human-readable. For example, the code may be a barcode or a Quick Response Code (QR-code). Suitable machines or readers can read the information encoded in the barcode or QR-code, but humans are unable to directly read the information encoded in the barcode or QR-code just by looking at the barcode or QR-code.

[0028] In an implementation, the code may be generated by first generating corresponding code data based on the beneficiary account number, the transaction amount and the timestamp. The code data may be generated by appending the beneficiary account number, the transaction amount and the timestamp to each other. For example, if the beneficiary account number is “244-25931-9”, the transaction amount is “\$100” and the timestamp is “201609262030” (26 September 2016; 2030h), the generated code data may be “244-25931-9100201609262030”.

[0029] Thereafter, the code data is encoded in the machine-readable code. For example, a QR-code may be generated that has the code data “244-25931-9100201609262030” encoded therein.

[0030] The benefactor can then share this QR-code with the beneficiary. For example, the QR-code can be printed on a piece of paper or digitally transmitted as an image file. The advantage of the code being a machine-readable code and not human-readable is that third parties who inadvertently gain possession of the QR-code are not able to directly and quickly decode the sensitive data encoded in the QR-code. Moreover, appending the beneficiary account number, the transaction amount and the timestamp to each other typically results in a string of, on the face of it, unintelligible numerals, alphabets or characters. Third parties who inadvertently gain possession of the QR-code and decode the QR-code to obtain the code data may not immediately think that it represents sensitive data.

[0031] After the QR-code is shared with the beneficiary, he can receive the funds from the benefactor at his own convenience. Subsequently, at step 112, the beneficiary goes to an ATM (may not be the same ATM that the benefactor used to generate the QR-code) to scan the QR-code. It is assumed that the ATM has a suitable reader than is capable of reading and decoding the code data encoded in the QR-code.

[0032] Optionally, at step 114, a one-time password (OTP), which is a one-time-valid, dynamic pass-code, can be used to confirm the identity of beneficiary so that unauthorized persons do not receive the funds from the benefactor. For example,

an OTP may be sent to the beneficiary's mobile phone via a Short Message Service (SMS) message and the beneficiary has to provide the OTP at the ATM.

[0033] If the OTP entered by the beneficiary is correct, the fund transfer takes place at step 116. At step 118, the benefactor is notified that the transfer of funds to the beneficiary has been completed. The transaction amount is deducted from the benefactor's account and credited to the beneficiary's account.

[0034] Figure 2 shows a flow chart illustrating a method for conducting a transaction, according to another example embodiment. A user (a benefactor) wishes to give credit to another user (a customer) for use at a particular merchant's store. At step 202, the benefactor visits an automated teller machine (ATM) and inserts his ATM card. At step 204, the benefactor enters his personal identification number (PIN) for authentication purposes.

[0035] At step 208, the benefactor enters the amount of credit or funds that he wishes to give to the customer. The ATM may display a list of merchants that accept credit in this manner. The benefactor inputs the chosen merchant's identity at the ATM. The ATM may have an account number or identifier associated with each merchant.

[0036] At step 210, the ATM generates a code or token based on the merchant's account number (hereinafter beneficiary's account number) or identifier, the amount of credit to be given by the benefactor to the customer (i.e. transaction amount) and a timestamp. The code is preferably a machine-readable code and also preferably not human-readable. For example, the code may be a barcode or a Quick Response Code (QR-code).

[0037] In an implementation, the code may be generated by first generating corresponding code data based on the beneficiary account number, the transaction amount and the timestamp. The code data may be generated by appending the beneficiary account number, the transaction amount and the timestamp to each other. For example, if the beneficiary account number is "244-25931-9", the transaction amount is "\$100" and the timestamp is "201609262030" (26 September 2016; 2030h), the generated code data may be "244-25931-9100201609262030". For added security, the code data is preferably encrypted using techniques known in the art.

[0038] Thereafter, the code data is encoded in the machine-readable code. For example, a QR-code may be generated that has the code data “244-25931-9100201609262030” encoded therein.

[0039] The benefactor can then share this QR-code with the customer. For example, the QR-code can be printed on a piece of paper or digitally transmitted as an image file. The advantage of the code being a machine-readable code and not human-readable is that third parties who inadvertently gain possession of the QR-code are not able to directly and quickly decode the sensitive data encoded in the QR-code.

[0040] After the QR-code is shared with the customer, he can visit the merchant's store at his own convenience to spend the credit. Subsequently, at step 212, the customer goes to the merchant's store to scan the QR-code at a point-of-sale (POS) terminal to pay for his purchase. It is assumed that the POS has a suitable reader than is capable of reading and decoding the code data encoded in the QR-code.

[0041] Optionally, at step 214, a one-time password (OTP), which is a one-time-valid, dynamic pass-code, can be used to confirm the identity of customer so that unauthorized persons are not able to utilize the credit from the benefactor. For example, an OTP may be sent to the customer's mobile phone via a Short Message Service (SMS) message and the customer has to provide the OTP at the ATM.

[0042] If the OTP entered by the customer is correct, the product payment (i.e. fund transfer) takes place at step 216. At step 218, the benefactor is notified that the fund transfer has been completed. In other words, the transaction amount is deducted from the benefactor's account and credited to the merchant's/beneficiary's account to pay for the products that the customer has purchased.

[0043] Figure 3 shows a flow chart illustrating a method for conducting a transaction, according to yet another example embodiment. A user (a benefactor) wishes to transfer money to another user (a beneficiary). At step 302, the benefactor visits an automated teller machine (ATM), and inserts his ATM card and enters his personal identification number (PIN) for authentication purposes. At step 304, the benefactor selects a “Code Generation” option at the ATM in order to initiate money transfer to

the beneficiary. At step 306, the benefactor enters (i) the beneficiary's (i.e. fund recipient's) account number, (ii) the amount of funds that he wishes to transfer to the beneficiary, and (iii) a validity period of the transaction. The validity period may be a default period (e.g. 3 days) and is calculated based on the time/date of the fund transfer request by the benefactor.

[0044] At step 308, the ATM generates a code based on (i) the beneficiary's (i.e. fund recipient's) account number, (ii) the amount of funds that he wishes to transfer to the beneficiary, and (iii) a timestamp corresponding to the time and/or date of the fund transfer request. The timestamp is used to calculate the validity period of the code. The code is preferably a machine-readable code and also preferably not human-readable. For example, the code may be a barcode or a Quick Response Code (QR-code). Suitable machines or readers can read the information encoded in the barcode or QR-code, but humans are unable to directly read the information encoded in the barcode or QR-code just by looking at the barcode or QR-code.

[0045] In an implementation, the code may be generated by first generating corresponding code data based on the beneficiary account number, the transaction amount and the timestamp. The code data may be generated by appending the beneficiary account number, the transaction amount and the timestamp to each other. For example, if the beneficiary account number is "244-25931-9", the transaction amount is "\$100" and the timestamp is "201609262030" (26 September 2016; 2030h), the generated code data may be "244-25931-9100201609262030". For added security, the code data is preferably encrypted using techniques known in the art.

[0046] Thereafter, the code data is encoded in the machine-readable code. For example, a QR-code may be generated that has the code data "244-25931-9100201609262030" encoded therein.

[0047] At step 310, a transaction reference is generated. The transaction reference is an identifier that is uniquely associated with the code data. At step 312, the code data is stored in association with the transaction reference in a database module (issuer database) that is communicatively connected to the ATM. The benefactor's account number may be stored in association with the transaction reference in the database module. The benefactor's account number may be obtained from the ATM since the benefactor's account number is known after the benefactor presents his ATM card at step 302.

[0048] At step 314, the ATM displays a notification that the request to transfer money to the beneficiary has been approved.

[0049] At step 316, the benefactor shares the QR-code with the beneficiary. The advantage of the code being a machine-readable code and not human-readable is that third parties who inadvertently gain possession of the QR-code are not able to directly and quickly decode the sensitive data encoded in the QR-code.

[0050] After the QR-code is shared with the beneficiary, he can receive the funds from the benefactor at his own convenience. Subsequently, at step 318, the beneficiary goes to an ATM (may not be the same ATM that the benefactor used to generate the QR-code) to scan the QR-code. It is assumed that the ATM has a suitable reader that is capable of reading and decoding the code data encoded in the QR-code.

[0051] At step 320, the identity of the beneficiary's bank can be determined based on the code data that is decoded from the QR-code. In particular, the beneficiary's bank account number that is part of the code data can be used to identify the beneficiary's bank. This is possible because the first few digits of an account number may indicate a bank's identity. Alternatively, the format of bank account numbers varies across different banks. For example, some may have 10 digits, some may have 16 digits, some may have a dash after the first three digits, etc.

[0052] At step 322, integration with an application programming interface (API) may be implemented to track the transaction reference that is stored in the database module. As mentioned above, the code data (i.e. beneficiary account number, transaction amount and timestamp) and benefactor account number are stored in association (i.e. linked) to a unique identifier (transaction reference) in the database module. The code data that is encoded in the QR-code is decoded and the unique identifier associated with the decoded code data can be determined. After the unique identifier has been determined, the benefactor account number that is stored in association with the unique identifier can also be determined. In this manner, the essential data required for a fund transfer (i.e. beneficiary account number, transaction amount and benefactor account number) is known.

[0053] Optionally, at step 324, a one-time password (OTP), which is a one-time-valid, dynamic pass-code, can be used to confirm the identity of beneficiary and/or

whether the beneficiary account is legitimate so that unauthorized persons do not receive the funds from the benefactor. For example, an OTP may be sent to the beneficiary's mobile phone via a Short Message Service (SMS) message and the beneficiary has to provide the OTP at the ATM.

[0054] If the OTP entered by the beneficiary is correct, the fund transfer takes place at step 326. The fund transfer is performed securely using known techniques. The benefactor is notified that the transfer of funds to the beneficiary has been completed. The transaction amount is deducted from the benefactor's account and credited to the beneficiary's account.

[0055] If the beneficiary does not complete the transaction (i.e. does not scan the QR-code at the ATM at step 318) within the validity period (e.g. 3 days), the QR-code "expires", i.e. the transaction will not be authorized. If the transaction is not authorized, the beneficiary and/or benefactor may be notified accordingly.

[0056] Figure 4 shows a flow chart illustrating a method for conducting a transaction, according to yet another example embodiment. A user (a benefactor) wishes to give credit to another user (a customer) for use at a particular merchant's store. At step 402, the benefactor visits an automated teller machine (ATM), and inserts his ATM card and enters his personal identification number (PIN) for authentication purposes. At step 404, the benefactor selects a "Code Generation" option at the ATM in order to give credit to the customer for use at a particular merchant's store. At step 406, the benefactor enters (i) the merchant's account number (hereinafter beneficiary's account number), (ii) the amount of credit or funds that he wishes to give to the customer (hereinafter transaction amount), and (iii) a validity period of the credit. The validity period may be a default period (e.g. 3 days) and is calculated based on the time/date of the credit provision request by the benefactor.

[0057] At step 408, the ATM generates a code based on (i) the beneficiary's account number, (ii) transaction amount, and (iii) a timestamp corresponding to the time and/or date of the credit provision request. The timestamp is used to calculate the validity period of the code. The code is preferably a machine-readable code and also preferably not human-readable. For example, the code may be a barcode or a Quick Response Code (QR-code). Suitable machines or readers can read the information encoded in the barcode or QR-code, but humans are unable to directly

read the information encoded in the barcode or QR-code just by looking at the barcode or QR-code.

[0058] In an implementation, the code may be generated by first generating corresponding code data based on the beneficiary account number, the transaction amount and the timestamp. The code data may be generated by appending the beneficiary account number, the transaction amount and the timestamp to each other. For example, if the beneficiary account number is “244-25931-9”, the transaction amount is “\$100” and the timestamp is “201609262030” (26 September 2016; 2030h), the generated code data may be “244-25931-9100201609262030”. For added security, the code data is preferably encrypted using techniques known in the art.

[0059] Thereafter, the code data is encoded in the machine-readable code. For example, a QR-code may be generated that has the code data “244-25931-9100201609262030” encoded therein.

[0060] At step 410, a transaction reference is generated. The transaction reference is an identifier that is uniquely associated with the code data. At step 412, the code data is stored in association with the transaction reference in a database module (issuer database) that is communicatively connected to the ATM. The benefactor's account number may be stored in association with the transaction reference in the database module. The benefactor's account number may be obtained from the ATM since the benefactor's account number is known after the benefactor presents his ATM card at step 402.

[0061] At step 414, the ATM displays a notification that the request to give credit to the customer has been approved.

[0062] At step 416, the benefactor shares the QR-code with the customer. The advantage of the code being a machine-readable code and not human-readable is that third parties who inadvertently gain possession of the QR-code are not able to directly and quickly decode the sensitive data encoded in the QR-code.

[0063] After the QR-code is shared with the customer, he can visit the merchant's store at his own convenience to spend the credit. Subsequently, at step 418, the customer goes to the merchant's store to scans the QR-code at a point-of-sale (POS) terminal when paying for his purchases. It is assumed that the POS has a

suitable reader than is capable of reading and decoding the code data encoded in the QR-code.

[0064] At step 420, the identity of the merchant (i.e. beneficiary's) bank can be determined based on the code data that is decoded from the QR-code. In particular, the beneficiary's bank account number that is part of the code data can be used to identify the beneficiary's bank. This is possible because the first few digits of an account number may indicate a bank's identity. Alternatively, the format of account numbers varies across different banks. For example, some may have 10 digits, some may have 16 digits, some may have a dash after the first three digits, etc.

[0065] At step 421, a merchant's database is accessed to store the transaction reference number (that is uniquely associated with the code data) for each transaction. The transaction reference is linked with an Issuer for integration of the transaction.

[0066] At step 422, integration with an application programming interface (API) may be implemented to track the transaction reference that is stored in the database module at step 412. As mentioned above, the code data (i.e. beneficiary account number, transaction amount and timestamp) and benefactor account number are stored in association (i.e. linked) to a unique identifier (transaction reference) in the database module. The code data that is encoded in the QR-code is decoded and the unique identifier associated with the decoded code data can be determined. After the unique identifier has been determined, the benefactor account number that is stored in association with the unique identifier can also be determined. In this manner, the essential data required for a fund transfer (i.e. beneficiary account number, transaction amount and benefactor account number) is known.

[0067] Optionally, at step 424, a one-time password (OTP), which is a one-time-valid, secure dynamic pass-code, can be used to confirm the identity of customer so that unauthorized persons are not able to utilize the credit from the benefactor. For example, an OTP may be sent to the customer's mobile phone via a Short Message Service (SMS) message and the customer has to provide the OTP at the ATM.

[0068] If the OTP entered by the customer is correct, the transaction (i.e. payment for products) takes place at step 426. The benefactor is notified that the fund transfer / purchase of products by the customer has been completed. In other words, the transaction amount is deducted from the benefactor's account and credited to the merchant's (i.e. beneficiary's) account.

[0069] If the customer does not complete the transaction (i.e. does not purchase products at the merchant's store) within the validity period (e.g. 3 days), the code "expires", i.e. the transaction will not be authorized and notified to the customer.

[0070] Figure 5 shows a schematic of a system 500 for facilitating a transaction, according to an example embodiment. The transaction may be a fund transfer request. For example, a user (a benefactor) wishes to transfer money to another user (a beneficiary). In the following description, the term "module" (e.g. receiver module, generator module, etc.) can refer to software, a hardware element, or a combination of both.

[0071] The system 500 comprises a receiver module 502, a generator module 504, an encoder module 506 and an identifier module 508. The receiver module 502 is configured to receive a beneficiary account number and a transaction amount (i.e. amount of money to be transferred), for example from an ATM input module 540. The generator module 504 is configured to generate code data based on the beneficiary account number, the transaction amount and a timestamp. The timestamp may correspond to the time and/or date of the fund transfer request. The generator module 504 may generate the code data by appending the beneficiary account number, the transaction amount and the timestamp to each other, as described above.

[0072] The encoder module 506 is configured to encode the code data in a machine-readable code (e.g. a Quick Response Code (QR-code)). The code data can be subsequently decoded for use during the transaction. The identifier module 508 is configured to assign an identifier that is uniquely associated with the code data.

[0073] In an implementation, the system 500 may further include a transmitter module 510 configured to transmit the identifier and the corresponding code data to a remote database module 550 that is communicatively connected to the system 500. The identifier is preferably stored in association with the code data and a benefactor account number in the remote database module 550.

[0074] Figure 6 shows a flow chart illustrating a method 600 for facilitating a transaction, according to yet another example embodiment. The transaction may be a fund transfer request. For example, a user (a benefactor) wishes to transfer money to another user (a beneficiary). At step 602, a beneficiary account number and a transaction amount (i.e. amount of money to be transferred) are received at a receiver module (such as the receiver module 502 described above) from e.g. an ATM input module. At step 604, a generator module (such as the generator module 504 described above) is used to generate code data based on the beneficiary account number, the transaction amount and a timestamp, e.g. by appending the beneficiary account number, the transaction amount and the timestamp to each other.

[0075] At step 606, an encoder module (such as encoder module 506 described above) is used to encode the code data in a machine-readable code such as a Quick Response Code (QR-code). The code data can be subsequently decoded for use during the transaction. At step 608, an identifier module (such as identifier module 508 described above) is used to assign an identifier that is uniquely associated with the code data. The method 600 may include storing, in a database module, the identifier in association with the code data and a benefactor account number.

[0076] Figure 7 shows a schematic of a system 700 for conducting a transaction, according to an example embodiment. The transaction may be a fund transfer request. For example, a user (a benefactor) wishes to transfer money to another user (a beneficiary). The system 700 includes a code decoder module 702 and a processor module 704. The code decoder module 702 is configured to decode code data that is encoded in a machine-readable code. The code data comprises a beneficiary account number, a transaction amount and a timestamp.

[0077] The processor module 704 is configured to determine an identifier which is uniquely associated with the code data. This is possible as the code data is stored in association with the identifier in a database module 750 that is communicatively connected to the processor module 704. The processor module 704 is further configured to retrieve a benefactor account number that is stored in association with the identifier in the database module 750. In this manner, the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number to complete the transaction.

[0078] The processor module 704 may be further configured to determine a validity period of the code data based on the timestamp, such that the transaction amount can only be deducted from the account associated with the benefactor account number during the validity period.

[0079] The processor module 704 may be further configured to receive a one-time-valid, dynamic passcode; and determine a validity of the dynamic passcode such that the transaction amount can only be deducted from the account associated with the benefactor account number on a condition that the dynamic passcode is valid.

[0080] Figure 8 shows a flow chart illustrating a method 800 for conducting a transaction, according to an example embodiment. The transaction may be a fund transfer request. For example, a user (a benefactor) wishes to transfer money to another user (a beneficiary). At step 802, a code decoder module (such as the code decoder module 702 described above) is used to decode code data that is encoded in a machine-readable code. The code data comprises a beneficiary account number, a transaction amount and a timestamp.

[0081] At step 804, a processor module (such as the processor module 704 described above) is used to determine an identifier which is uniquely associated with the code data. This is possible as the code data is stored in association with the identifier in a database module.

[0082] At step 806, the processor module is used to retrieve a benefactor account number that is stored in association with the identifier in the database module. In this manner, the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number to complete the transaction.

[0083] The method 800 may include determining, using the processor module, a validity period of the code data based on the timestamp. The transaction amount can only be deducted from the account associated with the benefactor account number during the validity period.

[0084] The method 800 may include receiving, at the processor module, a one-time-valid, dynamic passcode; and determining, using the processor module, a validity of the dynamic passcode. The transaction amount can only be deducted from the account

associated with the benefactor account number on a condition that the dynamic passcode is valid.

[0085] Figure 9 shows a schematic diagram of a computer system / system 900 suitable for use in executing at least some steps of the method for conducting or facilitating a transaction and/or for realizing at least a part of the system (e.g. the generator module 504, the processor module 704, etc.) for conducting or facilitating a transaction. The following description of the computing device 900 is provided by way of example only and is not intended to be limiting.

[0086] As shown in Figure 9, the example computing device 900 includes a processor 904 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 900 may also include a multi-processor system. The processor 904 is connected to a communication infrastructure 906 for communication with other components of the computing device 900. The communication infrastructure 906 may include, for example, a communications bus, cross-bar, or network.

[0087] The computing device 900 further includes a main memory 908, such as a random access memory (RAM), and a secondary memory 910. The secondary memory 910 may include, for example, a hard disk drive 912 and/or a removable storage drive 914, which may include a magnetic tape drive, an optical disk drive, or the like. The removable storage drive 914 reads from and/or writes to a removable storage unit 918 in a well-known manner. The removable storage unit 918 may include a magnetic tape, optical disk, or the like, which is read by and written to by removable storage drive 914. As will be appreciated by persons skilled in the relevant art(s), the removable storage unit 918 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0088] In an alternative implementation, the secondary memory 910 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 900. Such means can include, for example, a removable storage unit 922 and an interface 920. Examples of a removable storage unit 922 and interface 920 include a removable memory chip (such as an EPROM or PROM) and associated socket, and other removable storage units 922 and interfaces 920 which allow software and data to be transferred from the removable storage unit 922 to the computer system 900.

[0089] The computing device 900 also includes at least one communication interface 924. The communication interface 924 allows software and data to be transferred between computing device 900 and external devices via a communication path 926. In various embodiments, the communication interface 924 permits data to be transferred between the computing device 900 and a data communication network, such as a public data or private data communication network. The communication interface 924 may be used to exchange data between different computing devices 900 which such computing devices 900 form part an interconnected computer network. Examples of a communication interface 924 can include a modem, a network interface (such as an Ethernet card), a communication port, an antenna with associated circuitry and the like. The communication interface 924 may be wired or may be wireless. Software and data transferred via the communication interface 924 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being received by communication interface 924. These signals are provided to the communication interface via the communication path 926.

[0090] Optionally, the computing device 900 further includes a display interface 902 which performs operations for rendering images to an associated display 930 and an audio interface 932 for performing operations for playing audio content via associated speaker(s) 934.

[0091] As used herein, the term "computer program product" may refer, in part, to removable storage unit 918, removable storage unit 922, a hard disk installed in hard disk drive 912, or a carrier wave carrying software over communication path 926 (wireless link or cable) to communication interface 924. Computer readable storage media refers to any non-transitory tangible storage medium that provides recorded instructions and/or data to the computing device 900 for execution and/or processing. Examples of such storage media include floppy disks, magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, USB memory, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 900. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 900 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0092] The computer programs (also called computer program code) are stored in main memory 908 and/or secondary memory 910. Computer programs can also be received via the communication interface 924. Such computer programs, when executed, enable the computing device 900 to perform one or more features of embodiments discussed herein. In various embodiments, the computer programs, when executed, enable the processor 904 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 900.

[0093] Software may be stored in a computer program product and loaded into the computing device 900 using the removable storage drive 914, the hard disk drive 912, or the interface 920. Alternatively, the computer program product may be downloaded to the computer system 900 over the communications path 926. The software, when executed by the processor 904, causes the computing device 900 to perform functions of embodiments described herein.

[0094] It is to be understood that the embodiment of Figure 9 is presented merely by way of example. Therefore, in some embodiments one or more features of the computing device 900 may be omitted. Also, in some embodiments, one or more features of the computing device 900 may be combined together. Additionally, in some embodiments, one or more features of the computing device 900 may be split into one or more component parts.

[0095] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

CLAIMS

1. A system for facilitating a transaction, comprising:
 - a receiver module configured to receive a beneficiary account number and a transaction amount;
 - a generator module configured to generate code data based on the beneficiary account number, the transaction amount and a timestamp;
 - an encoder module configured to encode the code data in a machine-readable code, wherein the code data can be subsequently decoded for use during the transaction; and
 - an identifier module configured to assign an identifier that is uniquely associated with the code data.
2. The system as claimed in claim 1, further comprising a transmitter module configured to transmit the identifier and the corresponding code data to a remote database module that is communicatively connected to the system.
3. The system as claimed in claim 2, wherein the identifier is stored in association with the code data and a benefactor account number in the remote database module.
4. The system as claimed in any one of the preceding claims, wherein the generator module is configured to generate the code data by appending the beneficiary account number, the transaction amount and the timestamp to each other.
5. The system as claimed in any one of the preceding claims, wherein the machine-readable code comprises a Quick Response Code (QR-code).
6. A method for facilitating a transaction, comprising:
 - receiving, at a receiver module, a beneficiary account number and a transaction amount;
 - generating, using a generator module, code data based on the beneficiary account number, the transaction amount and a timestamp;
 - encoding, using an encoder module, the code data in a machine-readable code, wherein the code data can be subsequently decoded for use during the transaction; and
 - assigning, using an identifier module, an identifier that is uniquely associated with the code data.

7. The method as claimed in claim 6, further comprising storing, in a database module, the identifier in association with the code data and a benefactor account number.

8. The method as claimed in claim 6 or 7, wherein the step of generating the code data comprises appending the beneficiary account number, the transaction amount and the timestamp to each other.

9. The method as claimed in any one of claims 6 to 8, wherein the machine-readable code comprises a Quick Response Code (QR-code).

10. A system for conducting a transaction, comprising:

a code decoder module configured to decode code data that is encoded in a machine-readable code, wherein the code data comprises a beneficiary account number, a transaction amount and a timestamp; and

a processor module configured to:

determine an identifier which is uniquely associated with the code data, wherein the code data is stored in association with the identifier in a database module that is communicatively connected to the processor module; and

retrieve a benefactor account number that is stored in association with the identifier in the database module, wherein the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number.

11. The system as claimed in claim 10, wherein the processor module is further configured to determine a validity period of the code data based on the timestamp, and wherein the transaction amount can only be deducted from the account associated with the benefactor account number during the validity period.

12. The system as claimed in claim 10 or 11, wherein the processor module is further configured to:

receive a one-time-valid, dynamic passcode; and

determine a validity of the dynamic passcode, wherein the transaction amount can only be deducted from the account associated with the benefactor account number on a condition that the dynamic passcode is valid.

13. A method for conducting a transaction, comprising:
 - decoding, using a code decoder module, code data that is encoded in a machine-readable code, wherein the code data comprises a beneficiary account number, a transaction amount and a timestamp;
 - determining, using a processor module, an identifier which is uniquely associated with the code data, wherein the code data is stored in association with the identifier in a database module; and
 - retrieving, using the processor module, a benefactor account number that is stored in association with the identifier in the database module, wherein the transaction amount can be deducted from an account associated with the benefactor account number and credited to an account associated with the beneficiary account number.
14. The method as claimed in claim 13, further comprising:
 - determining, using the processor module, a validity period of the code data based on the timestamp, wherein the transaction amount can only be deducted from the account associated with the benefactor account number during the validity period.
15. The method as claimed in claim 13 or 14, further comprising:
 - receiving, at the processor module, a one-time-valid, dynamic passcode; and
 - determining, using the processor module, a validity of the dynamic passcode, wherein the transaction amount can only be deducted from the account associated with the benefactor account number on a condition that the dynamic passcode is valid.