

METHOD AND SYSTEM FOR MOBILE REMITTANCE

[0001] This application claims priority from U.S. Provisional Application No. 61/477,400, filed on April 20, 2011, titled "Method and System for Mobile Remittance," which is incorporated herein by reference in its entirety.

BACKGROUND OF THE INVENTION

1. Field of Invention

[0002] Aspects of the present invention relate to methods and systems for providing a remittance from one mobile device to another. More particularly, aspects of the current invention related to methods and systems for transferring funds from one mobile device to another when the mobile devices do not belong to the same network.

2. Description of Related Art

[0003] While mobile currency remittance and/or other mobile remittance of monetary/non-monetary value (e.g., credit) via Short Message Services (SMSs) are known in the art, there are currently several problems with the existing methods of mobile remittance. One problem is that such transfers depend on the originating user's mobile carrier or network and which other carriers have agreements to transfer funds, either nationally or internationally, with the originating carrier. That is, currently, mobile remittance may be achieved only among users of the same carrier or among users of carriers that have agreements with the originating carrier. Another problem in the art today relates to the security of the mobile transaction, as many such remittance transactions are inherently insecure. Further, the current methods for mobile remittance are cumbersome and involve multiple steps, including

organizing the sale of and purchasing cash cards or other prepaid cards, signing up authorized agents (such as banks or merchants, for example), and ensuring that the agents have access to funds to provide as part of the remittance transaction, among other steps. In addition, the current methods and systems for mobile remittance are difficult to use, especially in rural areas, where banks/Automated Teller Machines (ATMs) may not be as prevalent as in urban areas, and there is a risk that the mobile remittance may not reach the intended recipient.

[0004] There is a need in the art for methods and systems of mobile remittance that are network-agnostic and that allow transfer of funds across any network, regardless of whether these networks have or do not have direct funds transfer agreements between the initiating and receiving networks. There is another need in the art for mobile remittance transactions that are easy to use and secure, and that ensure that the mobile remittance reaches the intended recipient, regardless of whether the recipient is in an urban or rural area.

SUMMARY

[0004a] The invention is defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

[0005] In light of the above described problems and unmet needs, the techniques disclosed herein may solve the above-identified needs, as well as others, by providing methods and systems of mobile remittance that are network-agnostic and that allow transfer of funds across any network, regardless of whether these networks have or do not have funds transfer agreements among each other. In addition, the techniques disclosed herein may provide for mobile remittance transactions that are easy to use and secure, and that ensure that the

mobile remittance reaches the intended recipient, regardless of whether the recipient is in an urban or rural area.

[0006] Additional advantages and novel features will be set forth in part in the description that follows, and in part will become more apparent to those skilled in the art upon examination of the following or upon learning by practice.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Various example aspects of the systems and methods will be described in detail, with reference to the following figures, wherein:

[0008] Figs. 1A-H illustrate various exemplary techniques;

[0009] Figs. 2A-E illustrate various exemplary techniques;

[0010] Figs. 3A-C illustrate various exemplary techniques;

[0011] Fig. 4 presents an example system diagram of various hardware components and other features, for use in accordance with the techniques disclosed herein; and

[0012] Fig. 5 is a block diagram of various example system components, for use in accordance with the techniques disclosed herein.

DETAILED DESCRIPTION

[0013] These and other features and advantages are described in, or are apparent from, the following detailed description of various example aspects.

[0014] Referring to Fig. 1A, therein shown is a local "on" net mobile SMS remittance system 100, including a mobile network 120 within a given country A, a mobile network 130 within the same country A, a mobile network 140 within a different country B, and a mobile network 150 within country B. Fig. 1A illustrates a remittance t being transferred between a sender 110, who is a subscriber of the mobile network 120, and another subscriber of the same mobile network A.

[0015] Referring to Fig. 1 B, therein shown is a local "off" net mobile SMS remittance system 200, including a mobile network 220 within a given country A, a mobile network 230 within the same country A, a mobile network 240 within a different country B, and a mobile network 250 within country B. Fig. 1 B illustrates a remittance t_1 between two subscribers of different mobile networks 220 and 230.

[0016] Referring now to Fig. 1 C, therein shown is an international on net mobile SMS remittance system 300, including a mobile network 320 within a given country A, a mobile network 330 within the same country A, a mobile network 340 within a different country B, and a mobile network 350 within country B. Fig. 1 C illustrates a remittance t_2 between two subscribers' mobile networks 320 and 340 located in two different countries.

[0017] As can be seen for Figs. 1A-C, SMS remittance messages may be sent between two subscribers of any two networks, even networks supporting different carriers, as will be explained in more detail below, regardless of whether the networks have funds transfer agreements with each other or not.

[0018] The sender and recipient of the mobile SMS remittance may or may not have an account with a service provider, such as a remittance facilitation center.

[0019] Referring to Fig. 1D, therein shown is an example SMS telephonic transfer system 400 where the sender 410 has an account with the service provider, and the account has a positive value. According to various aspects, the sender 410 may send a SMS message from mobile network 420 in country A, for example, the SMS message including an M-Pin (a mobile pin number, for example), and an M-Credit (mobile credit, the specified amount of the transfer, for example) to a specific short code. It should be appreciated by those of ordinary skill in the art that this may be achieved via a web browser (e.g., via a Hypertext Transfer Protocol Secure (HTTPS) protocol), as an alternative to a mobile SMS message.

[0020] The SMS message may be forwarded to the service provider server 465 via, e.g., a Short Message Peer-to-Peer (SMPP) protocol 450 via the SMS hub 460, which may capture the sender's Mobile Subscriber Integrated Services Digital Network (MSISDN) number, may validate the sender via the MSISDN in the prepaid database 455, and may verify the balance in the sender's account. Upon a positive outcome of the validation of the sender and of the verification of the sender's

account balance, the service provider server may send a SMS message to the MSISDN of the designated recipient 470, whether a local recipient or a foreign recipient, containing a system-generated serial number and the M-Credit amount. The recipient 470, who may be located in country B, for example, receives the SMS message generated by the service provider server.

[0021] An example implementation of a SMS telephonic transfer system 500, where the sender 510 does not have an account with the service provider 565, is described in reference to Fig. 1E. In this example, the SMS telephonic transfer system 500 is described with respect to an American Express® gift card. However, those of ordinary skill in the art will recognize that any other credit card, bank card, gift card or prepaid card may alternatively be used with this implementation. In this implementation, the sender 510 may send an SMS message with the card number and a Personal Identification Number (PIN) of the card to a selection of short codes (this may also be achieved via a browser), which may represent various denominations to be transferred. For example, short code 2000 may represent a value of \$20, and short code 3000 may represent a value of \$30, among other short codes and values. Alternatively, the value of the transfer may be indicated in the SMS message of the sender 510 or otherwise communicated to the service provider's server 565 via, e.g., a Short Message Peer-to-Peer (SMPP) protocol 550 via the SMS hub 560. According to various aspects, the server 565 may store the sender's MSISDN and short code (and/or other indication of amount to be transferred) for billing settlements with the mobile carrier(s) in a database 555. The server may then send an SMS with a system generated serial number and amount to the MSISDN of the recipient 570.

[0022] Fig. 1 F is a flow chart illustrating a mobile device enabled fund transfer and cash out method.

According to various aspects, the method starts when a sender sends a remittance message to service provider server at S110, for example in the form of an SMS message sent from the senders mobile device, as discussed above. The message may include, for example, a mobile pin number and a credit amount corresponding to funds to be transferred to a recipient. When the service provider receives the message from the recipient, the service provider may validate the remittance message at S120, for example by capturing the sender's MSISDN and comparing the sender's MSISDN to a reference database, and by verifying the sender's balance in the sender's account. When the sender has been validated at S120, the service provider may send a message to the recipient that may contain a system-generated serial number and/or gift card or other cash card or credit card number and the amount of funds destined to the recipient in the form of a M-Credit amount at S130.

[0023] According to various aspects, once the recipient receives the SMS message with the system-generated serial number and/or gift card or other cash card number and the M-Credit amount at S130, the recipient may approach an authorized agent and provide the system-generated serial number to the authorized agent at S140. According to various aspects, the recipient may provide the agent with only the system-generated serial number. At S150, after receiving the system-generated serial number, the agent may send the system-generated serial number to the service provider's server via SMS or web browser, for example, in order to obtain a funding credit corresponding to the amount of the remittance. Once the server

receives the serial number, the server may validate the serial number at S160 to confirm that the agent-provided serial number corresponds to the transaction initiated by the sender. Once the serial number is validated at S160, the server may send a portion of a PIN number, e.g., the first four digits of an 8 digit PIN to the recipient (alternatively referred to herein as the "recipient key"), and the last four digits to the agent (alternatively referred to herein as the "agent key"), in two separate messages, at S170. It should be noted that the 8 digit PIN may actually comprise any number of digits, and any subset of those digits may be sent to the recipient and/or the agent, respectively, at S170. Once the recipient receives the portion of the PIN, the recipient may then provide the received 4 digits to the agent at S180 in order to obtain the remittance. According to various aspects, when the agent receives the recipient key, or recipient portion of the PIN at S180, the agent may then send the complete 8 digit PIN, for example via SMS, to the service provider at S190. As a result, the server may transfer the funds to the agent's Mobile wallet (M-wallet) as a mobile credit or M-Credit, along with a commission, for example, at S195. It should be noted that absent both the recipient key and the agent key, the service provider may not transfer the funds to the agent, and the transaction may not be completed. When the agent receives the fund, the agent may provide the funds directly to the recipient, for example, in the form of cash, and may keep the commission.

[0024] In an alternative example cash out method, once the recipient receives the SMS message with the system-generated serial number and/or gift card or other cash card number and the M-Credit amount, the recipient may enter the serial

number at an authorized ATM or bank, thus bypassing the agent. The ATM bank may contact the service provider server to validate the serial number and the recipient's MSISDN. Once the verification is complete, the service provider server may provide a one-time PIN number (e.g., 6-digits) to the recipient. Upon entry of the appropriate PIN number, the ATM/bank may then dispense the correct amount to the recipient.

[0025] In accordance with some aspects, although the above discussion indicates that the service provider server communicates with the agent, the service provider may also communicate with main distributors (e.g., in-country partners), who in turn communicate with agents and/or recipients, when the agents are international agents and the in-country partners may be in a better position to communicate with the agents. Most or all members in the distribution hierarchy, which may include in-country partners and agents, may have M-wallets (e.g., a virtual pre-paid card), each of which has an initial value of \$0. The cash-out amount with commission may be credited to the M-wallet of the agent and to the in-country partner, if applicable, after the transaction is completed. The agents may be paid from the next level up, e.g. the in-country partner of the service provider, or from a lateral fellow-agent. Thus, the M-credits travel up the hierarchy, from the recipients to the service provider, while the funds travel down the hierarchy, from the service provider to the recipients. Payouts or settlements within the hierarchy may be scheduled on any agreed-upon basis (e.g., daily, weekly, monthly).

[0026] An example payout/settlement will now be described in reference to Fig.1G. According to various

aspects, if an agent 610 does not wish to wait for the settlement date (e.g., daily, weekly, monthly), the agent 610 may send a request for cash/credit advance out of the agent's M-wallet to a predetermined SMS code (e.g., "R,35" to request a \$35 advance) to the service provider. The service provider may generate, based on the SMS message, a serial number and amount, similar to the remittance flow described above, but without participation of a sender (i.e., the requesting agent is the sender and the recipient in this variation). The requesting agent (e.g., the gas station operator) may then approach a fellow agent (e.g., the grocer) for cash out. A similar cash out mechanism as in the remittance process described above may be applicable here, except that the agent may request a part or the entire payment amount in goods and/or services from the other agent, such as, e.g., 2lbs of rice and the remainder in cash. In this case, the grocer fellow agent may realize a profit margin on the requested 2lbs of rice in addition, for example, to the commission. The service provider may also receive a fee from the requesting agent for the transaction.

[0027] In this manner, the recipients themselves may be motivated to sign up as agents, which may require a database entry of the agent's MSISDN for verification purposes, as their subsequent remittance/payout transactions may be more efficient. The more agents sign up, the more the system may grow, and an ever-expanding mobile commerce ecosystem, as shown in Fig. 1H, may be created. In Fig. 1H, the recipient 720 may receive a mobile remittance from a relative, for example. Recipient 720 may then cash that mobile remittance through an agent 710, and the remittance amount may be transferred to the M-wallet of the agent 710.

According to various aspects, the recipient 720 may wish to become an agent 710, thereby decreasing the service provider overhead, as the transfers may now be from the M-wallet of the recipient-become-agent 720 to the M-wallet of another agent 710, for example. Thus, an intra-distribution system may expand.

[0028] Agent recruitment may be achieved via a potential agent sending a SMS message to a specific short code for agent registration. Upon receipt of the SMS message, the service provider may respond with an SMS containing an Agent ID (AID) and a message to contact the service provider. The service provider may create a new record with the new AID and the agent's MSISDN. To complete the registration, the new agent may contact the service provider to provide more information, although this may not be necessary, in accordance with some aspects, and the agent's record may be updated. Additional information, such as a starter kit including stickers, decal and instruction manual, among other starter kit items, may then be sent to the new agent.

[0029] Figs. 2A-E illustrate various implementations. In Fig. 2A, a shopper 610 who may be, for example, online via a network such as, e.g., the Internet, may utilize a credit card 630 to place an order at a retailer's website 620. According to various aspects, the retailer may not have the ability to process the credit card 630. Accordingly, Figs. 2B-C illustrate a transaction involving the credit card 630 and the bank 640 that issued the credit card 630, where the bank 640 communicates with a payment gateway 650 . As illustrated in Fig. 1 C, the payment gateway 650 may communicate with the bank 640 to request

payment from the card issuing bank 640, and may keep the payment in a virtual account 660. According to various aspects, and as illustrated in Fig. 2D, the funds provided from the bank 640 and located in the virtual account 660 in the form of virtual funds may then be sent to a server 670, where the server 670 may be similar to the servers 465 and 565 discussed above. Accordingly, when the server 670 receives the virtual funds transferred by the bank 640 via the payment gateway 650, the server 670 may then, as illustrated in Fig. 2E, provide the virtual funds to a device 680 of the merchant, such as, e.g., a mobile device 680 of the merchant, via a mobile transaction as described above. As a result, the merchant may then utilize the device 680 to convert the virtual funds to real funds via, for example, an agent, or an ATM machine, as discussed above with respect to Fig. 1 F, even when the merchant may not have the ability to process a credit card, as is sometimes the case in remote and under-developed parts of the world.

[0030] Figs. 3A-C illustrate various implementations. In Fig. 3A, a shopper 710 who may be, for example, online via a network such as, e.g., the Internet, may utilize an affiliated prepaid card 730 to place an order at a retailer's website 720. According to various aspects, the affiliated pre-paid card 730 may be card funded via a server, where the funds have been verified, and the identity of the shopper 710 using the pre-paid card 730 has been validated, by the server. As such, funds from the prepaid card 730 may be transferred to the payment gateway 750, which may keep the payment in a virtual account. According

to various aspects, and as illustrated in Fig. 3B, the funds provided from the prepaid card 730 and located in the virtual account in the form of virtual funds may then be sent to a server 770, where the server 770 may be similar to the servers 465 and 565 discussed above.

Accordingly, when the server 770 receives the virtual funds transferred by the prepaid card 730 via the payment gateway 750, the server 770 may then, as illustrated in Fig. 3C, provide the virtual funds to a device 780 of the merchant, such as, e.g., a mobile device 780 of the merchant, via a mobile transaction. As a result, the merchant may then utilize the device 780 to convert the virtual funds to real funds via, for example, an agent, or an ATM machine, as discussed above with respect to Fig. 1 F.

[0031] Some variations may be directed toward one or more computer systems capable of carrying out the functionality described herein. An example of such a computer system 200 is shown in Fig. 4.

[0032] Computer system 200 includes one or more processors, such as processor 204. The processor 204 is connected to a communication infrastructure 206 (e.g. , a communications bus, cross-over bar, or network). Various software aspects are described in terms of this example computer system. After reading this description, it will become apparent to a person skilled in the relevant art(s) how to implement these techniques using other computer systems and/or architectures.

[0033] Computer system 200 can include a display interface 202 that forwards graphics, text, and other data from the communication infrastructure 206 (or from a frame buffer not shown) for display on a display unit 230. Computer system

200 also includes a main memory 208, preferably random access memory (RAM), and may also include a secondary memory 210. The secondary memory 210 may include, for example, a hard disk drive 212 and/or a removable storage drive 214, representing a floppy disk drive, a magnetic tape drive, an optical disk drive, etc. The removable storage drive 214 reads from and/or writes to a removable storage unit 218 in a well-known manner. Removable storage unit 218, represents a floppy disk, magnetic tape, optical disk, etc., which is read by and written to removable storage drive 214. As will be appreciated, the removable storage unit 218 includes a computer usable storage medium having stored therein computer software and/or data.

[0034] In alternative aspects, secondary memory 210 may include other similar devices for allowing computer programs or other instructions to be loaded into computer system 200. Such devices may include, for example, a removable storage unit 222 and an interface 220. Examples of such may include a program cartridge and cartridge interface (such as that found in video game devices), a removable memory chip (such as an erasable programmable read only memory (EPROM), or programmable read only memory (PROM)) and associated socket, and other removable storage units 222 and interfaces 220, which allow software and data to be transferred from the removable storage unit 222 to computer system 200.

[0035] Computer system 200 may also include a communications interface 224. Communications interface 224 allows software and data to be transferred between computer system 200 and external devices. Examples of communications interface 224 may include a modem, a network interface (such as an Ethernet card),

a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, etc. Software and data transferred via communications interface 224 are in the form of signals 228, which may be electronic, electromagnetic, optical or other signals capable of being received by communications interface 224. These signals 228 are provided to communications interface 224 via a communications path (e.g., channel) 226. This path 226 carries signals 228 and may be implemented using wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link and/or other communications channels. In this document, the terms "computer program medium" and "computer usable medium" are used to refer generally to media such as a removable storage drive 214, a hard disk installed in hard disk drive 212, and signals 228. These computer program products provide software to the computer system 200.

[0036] Computer programs (also referred to as computer control logic) are stored in main memory 208 and/or secondary memory 210. Computer programs may also be received via communications interface 224. Such computer programs, when executed, enable the computer system 200 to perform the features of the present techniques, as discussed herein. In particular, the computer programs, when executed, enable the processor 210 to perform these techniques. Accordingly, such computer programs represent controllers of the computer system 200.

[0037] In a technique implementing software, the software may be stored in a computer program product and loaded into computer

system 200 using removable storage drive 214, hard drive 212, or communications interface 220. The control logic (software), when executed by the processor 204, causes the processor 204 to perform the functionality as described herein. In another aspect, the techniques may be implemented primarily in hardware using, for example, hardware components, such as application specific integrated circuits (ASICs). Implementation of the hardware state machine so as to perform the functions described herein will be apparent to persons skilled in the relevant art(s).

[0038] In yet another aspect, these techniques are implemented using a combination of both hardware and software.

[0039] Fig. 5 shows a communication system 300 involving use of various features. The communication system 300 includes one or more assessors 360, 362 (also referred to interchangeably herein as one or more "users") and one or more terminals 342, 366 accessible by the one or more assessors 360, 362. In one aspect, operations, for example, input and/or accessed by an accessor 360 via terminal 342, such as personal computers (PCs), minicomputers, mainframe computers, microcomputers, telephonic devices, or wireless devices, such as personal digital assistants ("PDAs") or a hand-held wireless devices coupled to a remote device 343, such as a server, PC, minicomputer, mainframe computer, microcomputer, or other device having a processor and a repository for data and/or connection to a repository for data, via, for example, a network 344, such as the Internet or an intranet, and couplings 345, 364. The couplings 345, 364 include, for example, wired, wireless, or fiberoptic links. In

another aspect, the methods and systems disclosed herein may operate in a standalone environment, such as on a single terminal.

[0040] While this invention has been described in conjunction with the example aspects outlined above, various alternatives, modifications, variations, improvements, and/or substantial equivalents, whether known or that are or may be presently unforeseen, may become apparent to those having at least ordinary skill in the art. Accordingly, the example aspects, as set forth above, are intended to be illustrative, not limiting. Various changes may be made without departing from the scope of the appended claims. Therefore, the claims are intended to embrace all known or later-developed alternatives, modifications, variations, improvements, and/or substantial equivalents.

WHAT IS CLAIMED IS:

1. A method of securely transferring funds using a server apparatus by means of mobile device messages, the server apparatus being programmed to:

- receive a first mobile device message from a sender's mobile device, the first message including an identifier of a recipient's mobile device and data indicative of a credit amount corresponding to funds to be transferred;

- process the first message to capture an identifier of the sender's mobile device from data received along with the first message;

- compare the captured identifier to a reference database in a repository to validate the sender;

- in response to validation of the sender, automatically send a second message to the recipient's mobile device using the identifier of the recipient's mobile device in the first mobile device message, the second message including a transaction identifier; for the transaction identifier from the second message to be subsequently provided from the recipient's mobile device to a third party;

- receive a third message from the third party, the third message including the transaction identifier;

- validate the transaction identifier received from the third party to identify the transaction, and in response to successful validation of the transaction identifier by the server apparatus, automatically generate a recipient key and a third party key;

- use a communication interface of the server apparatus to send a first key message to the recipient on the recipient's mobile device, the first key message having the recipient key, and send a second key message to the third party, the second key message having the third party key; for the recipient key to be subsequently provided from the recipient to the third party; and

- receive, from the third party, the recipient key and the third party key and transfer the funds to an account for the third party as a credit in response to receipt of the recipient key and the third party key.

2. The method of claim 1, wherein transferring the funds to the recipient is performed via the third party.
3. The method of claim 1, wherein the server apparatus comprises a server for one of the mobile devices.
4. The method of claim 1, wherein the first message comprises at least one of a bank card number, a gift card number, and a pre-paid card number.
5. The method of claim 1, wherein the second message comprises at least one of a serial number, a gift card number, a cash card number, and a credit card number.
6. The method of claim 5, wherein the portion of the second message comprises the serial number.
7. The method of claim 1, further comprising providing the funds from the third party to the recipient.
8. The method of claim 1, wherein transferring funds to an account for the third party as a credit comprises transferring a commission to the third party.
9. A system for transferring funds using mobile devices, the system comprising: a server apparatus;
a user interface functioning via the server apparatus; and
a repository accessible by the server apparatus;
wherein the server apparatus is configured to perform the method of claim 1.
10. The system of claim 9, wherein the server apparatus is housed on a terminal selected from a group consisting of a personal computer, a minicomputer, a main frame computer, a microcomputer, a hand held device, and a telephonic device.

11. The system of claim 9, wherein the server apparatus is selected from a group consisting of a personal computer, a minicomputer, a microcomputer, and a main frame computer.

12. The system of claim 11, wherein the server apparatus is coupled to a network that comprises the Internet.

13. A computer program product comprising a computer-readable medium having control logic embodied in the medium for implementing the method of claim 1.

14. A method of transferring funds using a mobile device, the method comprising:

receiving, from a first person's mobile device, a first message at a server apparatus, the first message including an identifier of a second person's mobile device and data indicative of a credit amount corresponding to funds to be transferred;

processing the first message to capture an identifier of the sender's mobile device from data received along with the first message;

comparing the captured identifier to a reference database in a repository to validate the sender;

in response to successful validation, sending a second message from the server to the identified second person's mobile device, the second message comprising a number;

at the server, receiving the number from an authorised ATM or bank, the number having been entered thereat whereby the server verifies the number;

in response to verification, the server sending a one-time PIN to the second person's mobile device for the second person to enter the one-time PIN to the ATM or bank for the ATM or bank to dispense funds to the second person.