December 2021

A SYSTEM AND METHOD FOR PROVIDING DIGITAL TRASACTION IN OFFLINE MODE TO PREVENT DOUBLE SPENDING PROBLEM

Gokul Anand Manimaran Mr
Visa

TITLE: “A SYSTEM AND METHOD FOR PROVIDING DIGITAL TRASACTION IN OFFLINE MODE TO PREVENT DOUBLE SPENDING PROBLEM”

Visa

#

Inventor: Gokul Anand Manimaran

TECHNICAL FIELD

The present subject matter is related, in general to offline digital transactions, and more particularly, but not exclusively to system and method for providing secured offline digital transaction in offline mode to prevent double spending problem.

BACKGROUND

In recent years cashless payment transactions are preferred over hard cash payment transactions. Because the cashless payment transactions are not conducted with money in the form of physical notes or coins, but rather through the transfer of digital information (usually an electronic representation of money) using credit cards, debit cards, mobile payments, digital currencies and the like. The cashless payment transactions are more vulnerable to hacking, fraud, double spending problem and the like. These issues cause increasing worry for many users to conduct cashless transactions specifically in offline mode (i.e., user is not connected to internet during cashless transaction). Because centralized entity (e.g., network server) which verifies the cashless transactions may not be reachable due to the offline nature of the transaction.

In view of the above, there is a need to build a complete offline transaction model to provide more reliable and secured cashless transaction to the users in offline mode.

The information disclosed in this background of the disclosure section is only for enhancement of understanding of the general background of the invention and should not be taken as an acknowledgment or any form of suggestion that this information forms the prior art already known to a person skilled in the art.

SUMMARY

The following presents a simplified summary of the present disclosure in order to provide a basic understanding of some aspects of the disclosure. This summary is not an extensive overview of the disclosure. It is not intended to identify key or critical elements of the disclosure or to delineate the scope of the disclosure. The following summary merely presents some concepts of the disclosure in a simplified form as a prelude to the more detailed description provided below.

In an embodiment, the present disclosure provides a system and method for providing a platform to perform cashless payment transaction in offline mode using virtual coins. The system may include network server which is configured to generate the virtual coins based on received customer request for generating the virtual coins. Each of the generated virtual coins includes unique virtual identification number to identify the user and Universally Unique Identifier (UUID) to identify individual coins. By this, the double spending problem can be prevented. Further, network server is configured to process payment transaction claim request received from the merchant via merchant device through the communication network.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this disclosure, illustrate exemplary embodiments and, together with the description, serve to explain the disclosed principles. In the figures, the left-most digit(s) of a reference number identifies the figure in which the reference number first appears. The same numbers are used throughout the figures to reference like features and components. Some embodiments of device or system and/or methods in accordance with embodiments of the present subject matter are now described, by way of example only, and with reference to the accompanying figures, in which:

Figure 1 shows an exemplary illustration of a platform to perform offline payment transactions within a particular ecosystem in accordance with some embodiments of the present disclosure**;**

Figure 2 illustrates a method flow diagram of onboarding offline currency process for offline payment transactions in accordance with some embodiments of the present disclosure;

Figure 3 illustrates a structural diagram of virtual coin in accordance with some embodiments of the present disclosure;

Figure 4 illustrates a method flow diagram for conducting offline payment transaction between customer device and merchant device in accordance with some embodiments of the present disclosure;

Figure 5 illustrates a method flow diagram for processing offline payment transaction by a network server in accordance with some embodiments of the present disclosure; and

Figure 6 shows a general-purpose computer system implementing network server for processing offline payment transactions, in accordance with embodiments of the present disclosure.

The figures depict embodiments of the disclosure for purposes of illustration only. One skilled in the art will readily recognize from the following description that alternative embodiments of the structures and methods illustrated herein may be employed without departing from the principles of the disclosure described herein.

DESCRIPTION OF THE DISCLOSURE

In the present document, the word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or implementation of the present subject matter described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments.

While the disclosure is susceptible to various modifications and alternative forms, specific embodiment thereof has been shown by way of example in the drawings and will be described in detail below. It should be understood, however that it is not intended to limit the disclosure to the particular forms disclosed, but on the contrary, the disclosure is to cover all modifications, equivalents, and alternative falling within the spirit and the scope of the disclosure.

The terms “comprises”, “comprising”, or any other variations thereof, are intended to cover a non-exclusive inclusion, such that a setup, device, or method that comprises a list of components or steps does not include only those components or steps but may include other components or steps not expressly listed or inherent to such setup or device or method. In other words, one or more elements in a device or system or apparatus proceeded by “comprises… a” does not, without more constraints, preclude the existence of other elements or additional elements in the device or system or apparatus.

The terms "an embodiment", "embodiment", "embodiments", "the embodiment", "the embodiments", "one or more embodiments", "some embodiments", and "one embodiment" mean "one or more (but not all) embodiments of the invention(s)" unless expressly specified otherwise.

The terms "including", "comprising", “having” and variations thereof mean "including but not limited to", unless expressly specified otherwise.

Present disclosure relates to a system and method for providing a platform to perform digital transaction in offline mode using virtual coins. The system may include network server which is configured to generate the virtual coins based on received customer request for generating the virtual coins. Each of the generated virtual coins includes unique virtual identification number to identify the user and Universally Unique Identifier (UUID) to identify individual . So that each coin cannot be spent more than once. By this, the double spending problem can be prevented. Thus, secured cashless transaction is performed in offline mode using the generated virtual coins. Further, network server is configured to process payment transaction claim request received from the merchant via merchant device through the communication network. The present disclosure provides the platform which allows participants or group of people of the same ecosystem to perform offline payment transactions using the virtual coins. Thereby, boosting private economy associated with the particular ecosystem. The present disclosure facilitates to track fraud or duplicate money claiming from the merchant. The customer will receive the receipt signed by the merchant during purchase and will submit this receipt and log when merchant comes back online. So, it can be traced back to the merchant.

The present disclosure also facilitates to track fraudulent activities or when customers phone data is lost by sending the phones IMEI (International Mobile Equipment Identity) data, SIM (subscriber identification module) data and nearby cell tower data. The present invention facilitates offline transaction model to boost private economy so that individual or group of people be able to thrive successfully in their lives.

Figure 1 shows an exemplary environment (100) for performing offline payment transactions within the particular ecosystem in accordance with some embodiments of the present disclosure. The exemplary environment (100) may indicate offline payment transaction setup between, but not limited to, individuals, group of people, private sector, and the like. In one embodiment, the individuals, the group of people, and the private sector may be related to region or area hit by flood, severe storm, earthquake, and the like within the particular ecosystem. The exemplary environment (100) comprises the offline payment transaction setup between individuals such as a customer (101) and a merchant (102), a customer device (103), a merchant device (104), a communication network (106), and a network server (107), customer's bank (111) and merchant's bank (112). The customer (101) may request to the network server (107) for virtual coins in exchange for amount (e.g., 500 rupees) through communication network (106) using an application (105) installed in the customer device (103). The customer device (103) may be a smartphone, a computer, a phone, a tablet, and so on. The customer (101) may receive virtual coins in exchange for the amount by the network server (107) via the communication network (106). The received virtual coins may be stored in wallet associated with the application (105) installed in the customer device (103). The customer (101) may pay virtual coins to the merchant (102) in exchange for a good or service via the customer device (103), without connecting to internet.

The merchant device (104) is configured receive offline payment from the customer (101) via the customer device (103). The merchant device (104) is configured to stay online (i.e., by connecting to the internet) to prevent fraud. The merchant device (104) may be a smartphone, a computer, a phone, a tablet, and so on. Upon receiving the virtual coins against purchase from the customer (101), the merchant (102) may request to the network server (107) to process the payment transaction claim request via the merchant device (104) through communication network (106). The customer (102) and the merchant (102) have to register themselves with the application (105) by providing information. The information may include name, account number, bank name, phone number and the like.

In an example embodiment, consider the customer (101) may purchase goods and/or services through online merchant website or by visiting merchant facility (not shown in Figure.1) such as retail store. The goods and/or services may include, but not limited to, clothes, electronic products, transportation, consultancy and so on. Upon purchasing, the customer (101) has to pay bill generated against the purchase. The customer (101) pays the bill using virtual coins by accessing the application (105). The application (105) associated with the customer (101) is configured to store the virtual coins with specific denomination, while paying the bill, respective bill amount in the form of virtual coins is transmitted to the merchant device (104) in offline mode (i.e., without connecting to the internet). The denomination of virtual coins may be in the form of rupees, dollars, euros, and the like. The merchant device (104) receives the virtual coins from the customer (101). The merchant (102) may claim received virtual coins by requesting to the network server (107) by connecting to the internet. The network server (107) may process the received payment transaction claim request by sending request to the customer's bank (111). The customer's bank (111) is configured to verify the received payment transaction claim request. Based on the successful verification to the received payment transaction claim request, the transaction payment is remitted to the merchant's bank (112) via network server (107).

The network server (107) may include at least one Central Processing Unit (also referred to as "CPU" or "processor") (108) and a memory (110) storing instructions executable by the processor (108). The processor (108) may comprise at least one data processor for executing program components to execute user requests or system-generated requests. The memory (110) is communicatively coupled to the processor (108). The memory (110) stores instructions, executable by the processor (108), which, on execution, may cause the network server (107) to provide the virtual coins in exchange for amount upon receiving the request from the customer (101), configured to process payment transaction claim request received from the merchant (102) via merchant device (104) through the communication network.

The network server (107) further comprises an Input/ Output (I/O) interface (109). The I/O interface (109) is coupled with the processor (108) through which an input signal or/and an output signal is communicated. The input signal and the output signal may represent data received by the network server (107) and data transmitted by the network server (107), respectively. In an embodiment of the present disclosure, the network server (107) may be configured to receive and transmit data via the I/O interface (109). The received data may comprise the customer (101) request related to generating the virtual coins, customer authentication response from the customer bank (111), the payment transaction claim request response from the customer's bank (111), and the like. The transmitted data may include customer (101) authentication request to customer's bank (111), response to customer (101) request related to generating the virtual coins, the payment transaction claim request to customer's bank (111), the payment transaction claim request response transmitted to the merchant's bank (112) (i.e., to initiate the remittance to the merchant (102) account), and the like.

In an embodiment, the network server (107) may communicate with the customer's bank (111) and merchant's bank (112) via communication network (106). The network server (107) and the customer's bank (111) and merchant's bank (112) may communicate over the communication network (106) via Application Program Interfaces (APIs). The communication network (106) may include, without limitation, a direct interconnection, Local Area Network (LAN), Wide Area Network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Ultra-Wide Band, etc.

In some embodiments, a software related to the application (105) may provision each of the customer, the merchant to complete transactions, such as requesting for generation of the virtual coins, payment transaction claim request (i.e., by the merchant), and so on. In some embodiments, the software may be an add-on to a web browser. In some embodiments, the customer device (103) may communicate with the merchant device (104) via one or more Application Programming Interfaces (APIs).

Figure 2 illustrates a method flow diagram of onboarding offline currency process for offline payment transactions in accordance with some embodiments of the present disclosure. At step.1 the customer (101) accesses the application (105) installed in the customer device (103) to request for virtual coins. At step.2 the customer (101) selects or decides amount to be converted into virtual coins and adds the selected amount to wallet associated with application (105). For example, the customer (101) may select 500 rupees from the account and may decide to convert the selected 500 rupees into virtual coins to further perform the offline payment transaction using created virtual coins. The customer (102) requests to network server (107) to generate the virtual coins for the selected amount. At step 3 &4 the network server (107) checks for the corresponding customer's bank upon receiving the request for generating the virtual coins. The customer's bank (111) may be identified by the network server (107) based on the received customer request. The customer request for generating the virtual coins may include selected amount and bank details of customer (101) such as bank name, bank account number, customer Permanent Account Number (PAN), bank code and so on. Upon detecting the customer's bank, request for customer (102) authentication may be sent to customer's bank (111) by the network server (107). At step.5 the customer's bank (111) verifiers detail associated with the customer (102) and send the authentication response to the network server (107). The detail associated with the customer may include customer name, customer account number, phone number, account balance, account type and so on. At step.6, based on the successful authentication, the network server (107) may generate the virtual coins for the selected amount by the customer (102). At step.7, each generated virtual coin may include unique virtual identification number and Universally Unique Identifier (UUID). The network server (107) may store all generated virtual coins virtual identification number (virtual-id) and UUID in database associated with network server (107). At step.8, the network server (107) encrypts the generated virtual coins. At step.9, the network server (107) may send the encrypted virtual coins to the customer (101) via the communication network (106). In an embodiment, the encryption may be performed by using private and public key algorithms. At step.10, the customer (101) may encrypt the generated virtual coins with private key associated with the customer (101) and stores the encrypted virtual coins in the wallet associated with the application (105) which is installed in the customer device (103).

Figure.3 illustrates a structural diagram of virtual coin in accordance with some embodiments of the present disclosure. Referring back to Figure.2, at step.6, the network server (107) is configured to generate the virtual coins based on the customer (101) request. Each of the virtual coin may include two parts. First part is related to data part and second part is related to security. The data part may include denomination, customer (101) virtual identification number, UUID number. The denomination indicates the particular economy type associated with the eco system. The denomination may include rupees, dollars, euros, and the like. This denomination may be selected by the customer (101) based on the associated numbers. For example, number 1 is associated with rupees, number 2 is associated with dollars, number 3 is associated with euros and the like. If the customer wishes to convert the amount in rupees based on their eco system (e.g., India), then the customer (102) may select number 1 from list. The customer virtual-id is a unique id for each customer. So that no one else can impersonate another user. For example, the customer virtual-id may include, but not limited to, six digit number such as xxx-xxx. 'x' indicates any integer number. The UUID number is unique for each virtual coin. For example, the UUID includes 16 byte string. From the UUID, each virtual coin is uniquely identified from another, so that same virtual coin can't be spent again and again. By this, double spending problem can be prevented. The second part is security part in which the network server (107) digitally signs to authenticate the virtual coin. So that, the merchant (104) can trust the virtual coins paid by the customer (101).

Figure 4 illustrates a method flow diagram for conducting offline payment transaction between customer device and merchant device in accordance with some embodiments of the present disclosure. At step.1, upon purchasing goods/services from the merchant facility, the customer (101) may pay the bill using virtual coins by accessing the application (105) installed in the customer device (103). Initially, the virtual coins may be encrypted and stored in the wallet associated with the application (105) of customer (101). At step.2, once the customer (101) initiates the payment transaction against the purchase using virtual coins, the virtual coins may be decrypted and transmitted to merchant device (104) using wallet (i.e., offline wallet), without connecting to the internet. At step 3. The merchant (102) accesses the application (105) installed in the merchant device (104) to verify the received virtual coins against sold items to the customer (101). For authentication, the merchant (102) verifies that whether the customer (101) sent virtual coins are digitally signed by the network server (107) or not. At step.4, Upon successful verification, the merchant (102) encrypts the virtual coins with merchant (102) private key. If the verification is unsuccessful, then the initiated payment transaction against the purchase may be disapproved. At step.5, the merchant device (104) stores the encrypted virtual coins in the wallet. Now referring to Figure.5, the merchant device (104) sends payment transaction claim request to the network server (107) to claim the received virtual coins via communication network (106), by connecting to the internet. The payment transaction claim request may include encrypted virtual coins along with customer (101) name and bank details. The encrypted virtual coins may include the customer virtual-id and UUID. The network server (107) decrypts the received encrypted virtual coins using merchant (102) public key. The network server (107) further validates the customer virtual-id and UUID associated with each of the received virtual coins. Upon successful validation of each of the virtual coins, the network server (107) requests to customer's bank (111) to deposit the corresponding money to the merchant's bank (112). Now referring back to Figure.4, upon depositing requested payment transaction amount in the merchant's bank, the merchant device (104) may generate the bill and approves the transaction at step.5 and step. 6. The transaction approval may include notification or alert message to the customer (101) to indicate the approval status of the payment transaction. When the requested payment transaction amount in the merchant's bank is deposited subsequently, the corresponding virtual coins from the wallet associated with the customer (101) is deleted at step.7. In some scenarios, the customer device (103) data may be lost, then the encrypted virtual coins data can be claimed against the purchase. The virtual coins data may include virtual-ids and UUIDs. UUID is 16 bytes. So, the customer (101) may print the data related to the virtual coin and the same can be used for claim. For example, the printing data may include- 16*(net offline transaction) byte. Roughly 0.016 MB of data per 1000 currency units.#

The present invention provides secured cashless payment transaction in offline mode by providing the virtual coins based the customer request. Each of the virtual coins includes unique virtual-id and UUID. So that each coin cannot be used more than once. By this. the double spending problem can be prevented. The present disclosure also promotes private economy by providing an offline transaction model which allows participants or group of people of the same ecosystem to perform offline payment transactions. Thereby private economy can be boosted, so that individual or group of people be able to thrive successfully in their lives. For example, the offline payment transaction may occur between the individuals such as donor and merchant or group of people. The donor may donate the money to the merchant using virtual coins (i.e., private money). The merchant can claim the money at the end of the day. The normal money will be transferred to his account. But this private money can only be redeemed back to his wallet. So that he can pay this to other merchants or donate to other users. The present disclosure also facilitates to track fraudulent activities or when customers phone data is lost or duplicate money claiming from the merchant. Thereby providing more secured transactions.

Computing System

Figure 6 illustrates a block diagram of an exemplary computer system 600 for implementing embodiments consistent with the present disclosure. In an embodiment, the computer system 600 is used to implement the network server for providing a platform to cashless payment transaction in offline mode using virtual coins. The computer system 600 may include a central processing unit ("CPU" or "processor") 602. The processor 602 may include at least one data processor for executing processes in Virtual Storage Area Network. The processor 602 may include specialized processing units such as, integrated system (bus) controllers, memory management control units, floating point units, graphics processing units, digital signal processing units, etc.

The processor 602 may be disposed in communication with one or more input/output (I/O) devices 609 and 610 via I/O interface 601. The I/O interface 601 may employ communication protocols/methods such as, without limitation, audio, analog, digital, monaural, RCA, stereo, IEEE-1394, serial bus, universal serial bus (USB), infrared, PS/2, BNC, coaxial, component, composite, digital visual interface (DVI), high-definition multimedia interface (HDMI), radio frequency (RF) antennas, S-Video, VGA, IEEE 802.n /b/g/n/x, Bluetooth, cellular (e.g., code-division multiple access (CDMA), high-speed packet access (HSPA+), global system for mobile communications (GSM), long-term evolution (LTE), WiMax, or the like), etc.

Using the I/O interface 601, the computer system 600 may communicate with one or more I/O devices 609 and 610. For example, the input devices 609 may be an antenna, keyboard, mouse, joystick, (infrared) remote control, camera, card reader, fax machine, dongle, biometric reader, microphone, touch screen, touchpad, trackball, stylus, scanner, storage device, transceiver, video device/source, etc. The output devices 610 may be a printer, fax machine, video display (e.g., cathode ray tube (CRT), liquid crystal display (LCD), light-emitting diode (LED), plasma, Plasma Display Panel (PDP), Organic light-emitting diode display (OLED) or the like), audio speaker, etc.

The processor 602 may be disposed in communication with a communication network 611 via a network interface 603. The network interface 603 may communicate with the communication network 611. The network interface 603 may employ connection protocols including, without limitation, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc. The communication network 611 may include, without limitation, a direct interconnection, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, etc. Using the network interface 603 and the communication network 611, the computer system 600 may communicate with at least one user device 612 via communication network 611 to provide preference based campaign page. The network interface 603 may employ connection protocols include, but not limited to, direct connect, Ethernet (e.g., twisted pair 10/100/1000 Base T), transmission control protocol/internet protocol (TCP/IP), token ring, IEEE 802.11a/b/g/n/x, etc.

In an embodiment, the computer system 600 may receive offline payment transaction request by the customer device 612. The computer system 600 may receive request for generating virtual coins from the customer. Further, the computer system 600 may also receive payment transaction claim request from the merchant via merchant device 613 through the communication network 611.

The communication network 611 includes, but is not limited to, a direct interconnection, an e-commerce network, a peer to peer (P2P) network, local area network (LAN), wide area network (WAN), wireless network (e.g., using Wireless Application Protocol), the Internet, Wi-Fi, and such. The first network and the second network may either be a dedicated network or a shared network, which represents an association of the different types of networks that use a variety of protocols, for example, Hypertext Transfer Protocol (HTTP), Transmission

Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), etc., to communicate with each other. Further, the first network and the second network may include a variety of network devices, including routers, bridges, servers, computing devices, storage devices, etc.

In some embodiments, the processor 602 may be disposed in communication with a memory 605 (e.g., RAM, ROM, etc. not shown in **Figure 6**) via a storage interface 604. The storage interface 604 may connect to memory 605 including, without limitation, memory drives, removable disc drives, etc., employing connection protocols such as, serial advanced technology attachment (SATA), Integrated Drive Electronics (IDE), IEEE-1394, Universal Serial Bus (USB), fibre channel, Small Computer Systems Interface (SCSI), etc. The memory drives may further include a drum, magnetic disc drive, magneto-optical drive, optical drive, Redundant Array of Independent Discs (RAID), solid-state memory devices, solid-state drives, etc.

The memory 605 may store a collection of program or database components, including, without limitation, user interface 606, an operating system 607, web browser 608 etc. In some embodiments, computer system 600 may store user/application data, such as, the data, variables, records, etc., as described in this disclosure. Such databases may be implemented as fault-tolerant, relational, scalable, secure databases such as Oracle ® or Sybase®.

The operating system 607 may facilitate resource management and operation of the computer system 600. Examples of operating systems include, without limitation, APPLE MACINTOSH® OS X, UNIX®, UNIX-like system distributions (E.G., BERKELEY SOFTWARE DISTRIBUTION^{TM} (BSD), FREEBSD^{TM}, NETBSD^{TM}, OPENBSD^{TM}, etc.), LINUX DISTRIBUTIONS^{TM} (E.G., RED HAT^{TM}, UBUNTU^{TM}, KUBUNTU^{TM}, etc.), IBM^{TM} OS/2, MICROSOFT^{TM} WINDOWS^{TM} (XP^{TM}, VISTA^{TM}/7/8, 10 etc.), APPLE® IOS^{TM}, GOOGLE® ANDROID^{TM}, BLACKBERRY® OS, or the like.

In some embodiments, the computer system 600 may implement a web browser 608 stored program component. The web browser 608 may be a hypertext viewing application, such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc. Secure web browsing may be provided using Hypertext Transport Protocol Secure (HTTPS), Secure Sockets Layer (SSL), Transport Layer Security (TLS), etc. Web browsers 608 may utilize facilities such as AJAX, DHTML, Adobe Flash, JavaScript, Java, Application Programming Interfaces (APIs), etc. In some embodiments, the computer system 600 may implement a mail server stored program component. The mail server may be an Internet mail server such as Microsoft Exchange, or the like. The mail server may utilize facilities such as ASP, ActiveX, ANSI C++/C#, Microsoft .NET, Common Gateway Interface (CGI) scripts, Java, JavaScript, PERL, PHP, Python, WebObjects, etc. The mail server may utilize communication protocols such as Internet Message Access Protocol (IMAP), Messaging Application Programming Interface (MAPI), Microsoft Exchange, Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), or the like. In some embodiments, the computer system 600 may implement a mail client stored program component. The mail client may be a mail viewing application, such as Apple Mail, Microsoft Entourage, Microsoft Outlook, Mozilla Thunderbird, etc.

Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer-readable storage medium refers to any type of physical memory on which information or data readable by a processor 602 may be stored. Thus, a computer-readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) 602 to perform steps or stages consistent with the embodiments described herein. The term “computer-readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., be non-transitory. Examples include Random Access Memory (RAM), Read-Only Memory (ROM), volatile memory, non-volatile memory, hard drives, Compact Disc (CD) ROMs, DVDs, flash drives, disks, and any other known physical storage media.

The described operations may be implemented as a method, system or article of manufacture using standard programming and/or engineering techniques to produce software, firmware, hardware, or any combination thereof. The described operations may be implemented as code maintained in a “non-transitory computer readable medium”, where a processor 602 may read and execute the code from the computer readable medium. The processor 602 is at least one of a microprocessor and a processor capable of processing and executing the queries. A non-transitory computer readable medium may include media such as magnetic storage medium (e.g., hard disk drives, floppy disks, tape, etc.), optical storage (CD-ROMs, DVDs, optical disks, etc.), volatile and non-volatile memory devices (e.g., EEPROMs, ROMs, PROMs, RAMs, DRAMs, SRAMs, Flash Memory, firmware, programmable logic, etc.), etc. Further, non-transitory computer-readable media may include all computer-readable media except for a transitory. The code implementing the described operations may further be implemented in hardware logic (e.g., an integrated circuit chip, Programmable Gate Array (PGA), Application Specific Integrated Circuit (ASIC), etc.).

The illustrated steps are set out to explain the exemplary embodiments shown, and it should be anticipated that ongoing technological development will change the manner in which particular functions are performed. These examples are presented herein for purposes of illustration, and not limitation. Further, the boundaries of the functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternative boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed. Alternatives (including equivalents, extensions, variations, deviations, etc., of those described herein) will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein. Such alternatives fall within the scope and spirit of the disclosed embodiments. Also, the words "comprising," "having," "containing," and "including," and other similar forms are intended to be equivalent in meaning and be open ended in that an item or items following any one of these words is not meant to be an exhaustive listing of such item or items, or meant to be limited to only the listed item or items. It must also be noted that as used herein and in the appended claims, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise.

Furthermore, one or more computer-readable storage media may be utilized in implementing embodiments consistent with the present disclosure. A computer readable storage medium refers to any type of physical memory on which information or data readable by a processor may be stored. Thus, a computer readable storage medium may store instructions for execution by one or more processors, including instructions for causing the processor(s) to perform steps or stages consistent with the embodiments described herein. The term “computer readable medium” should be understood to include tangible items and exclude carrier waves and transient signals, i.e., are non-transitory. Examples include random access memory (RAM), read-only memory (ROM), volatile memory, non-volatile memory, hard drives, CD ROMs, DVDs, flash drives, disks, and any other known physical storage media.

Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. Accordingly, the disclosure of the embodiments of the disclosure is intended to be illustrative, but not limiting, of the scope of the disclosure.

With respect to the use of substantially any plural and/or singular terms herein, those having skill in the art can translate from the plural to the singular and/or from the singular to the plural as is appropriate to the context and/or application. The various singular/plural permutations may be expressly set forth herein for sake of clarity.

ABSTRACT

Present disclosure provides a system and method for providing a platform to perform digital transaction in offline mode using virtual coins. The system may include network server (107) which is configured to generate virtual coins when the customer (102) requests for generating virtual coins. Each virtual coin includes unique virtual identification number and Universally Unique Identifier (UUID that ensures each coin cannot be spent more than once, preventing double spending problem. Thus, secured cashless transaction is performed in offline mode using the generated virtual coins. Further, network server (107) is configured to process payment transaction claim request received from the merchant (102) via merchant device (104) through the communication network (106). The present disclosure provides the platform which allows participants or group of people of the same ecosystem to perform offline payment transactions using the virtual coins. Thereby, boosting private economy associated with the particular ecosystem.

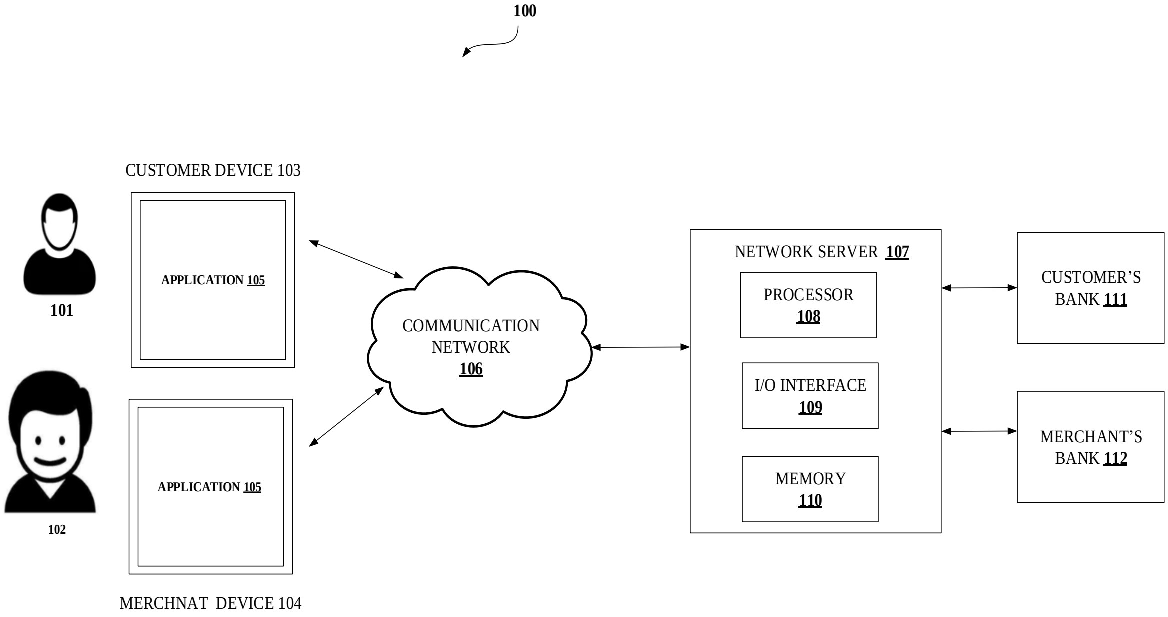
100
CUSTOMER DEVICE 103
APPLICATION 105
101
APPLICATION 105
102
MERCHNAT DEVICE 104
COMMUNICATION NETWORK 106
NETWORK SERVER 107
PROCESSOR 108
I/O INTERFACE 109
MEMORY 110
CUSTOMER'S BANK 111
MERCHANT'S BANK 112

Figure 1

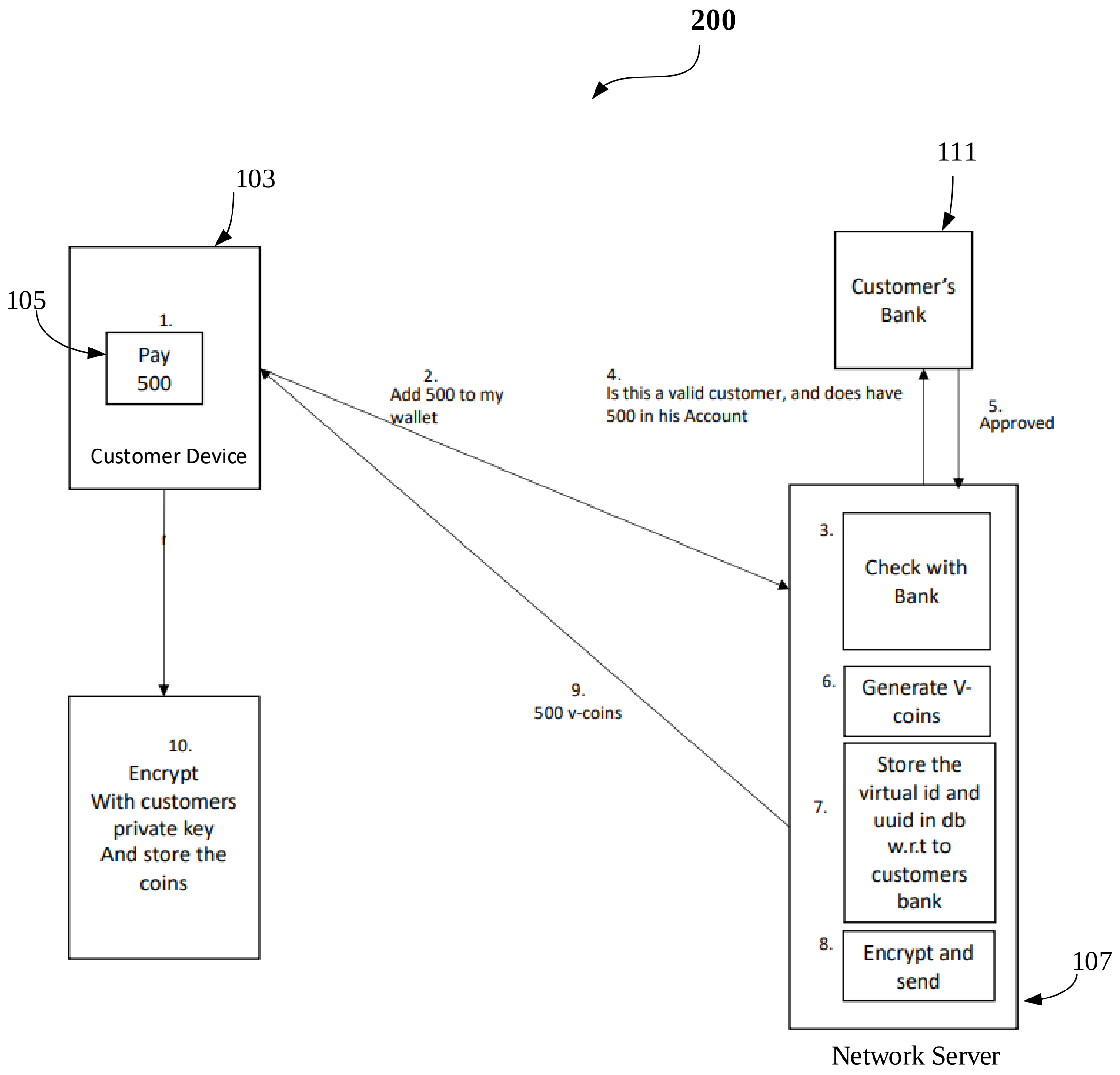
200
103
105
111
107
1.
Pay 500
Customer Device
2.
Add 500 to my wallet
4.
Is this a valid customer, and does have 500 in his Account
Customer's Bank
5.
Approved
3.
Check with Bank
6.
Generate V-coins
7.
Store the virtual id and uuid in db w.r.t to customers bank
8.
Encrypt and send
9.
500 v-coins
10.
Encrypt With customers private key And store the coins
Network Server

Figure 2

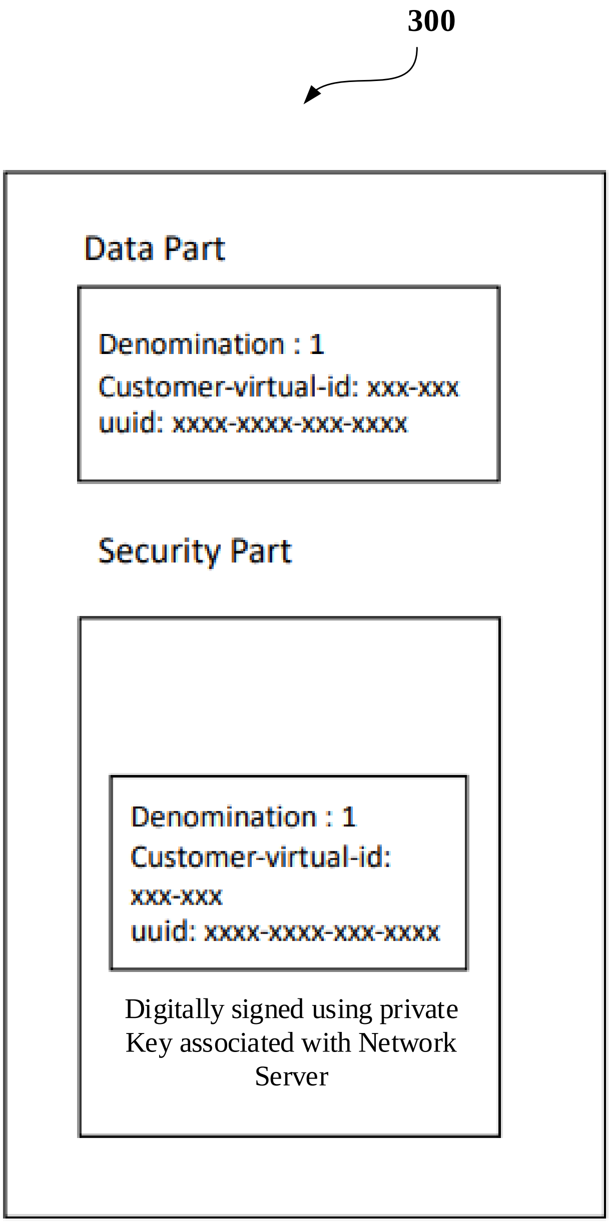
300
Data Part
Denomination : 1
Customer-virtual-id: xxx-xxx
uuid: xxxx-xxxx-xxx-xxxx
Security Part
Denomination : 1
Customer-virtual-id:
xxx-xxx
uuid: xxxx-xxxx-xxx-xxxx
Digitally signed using private Key associated with Network Server

Figure.3

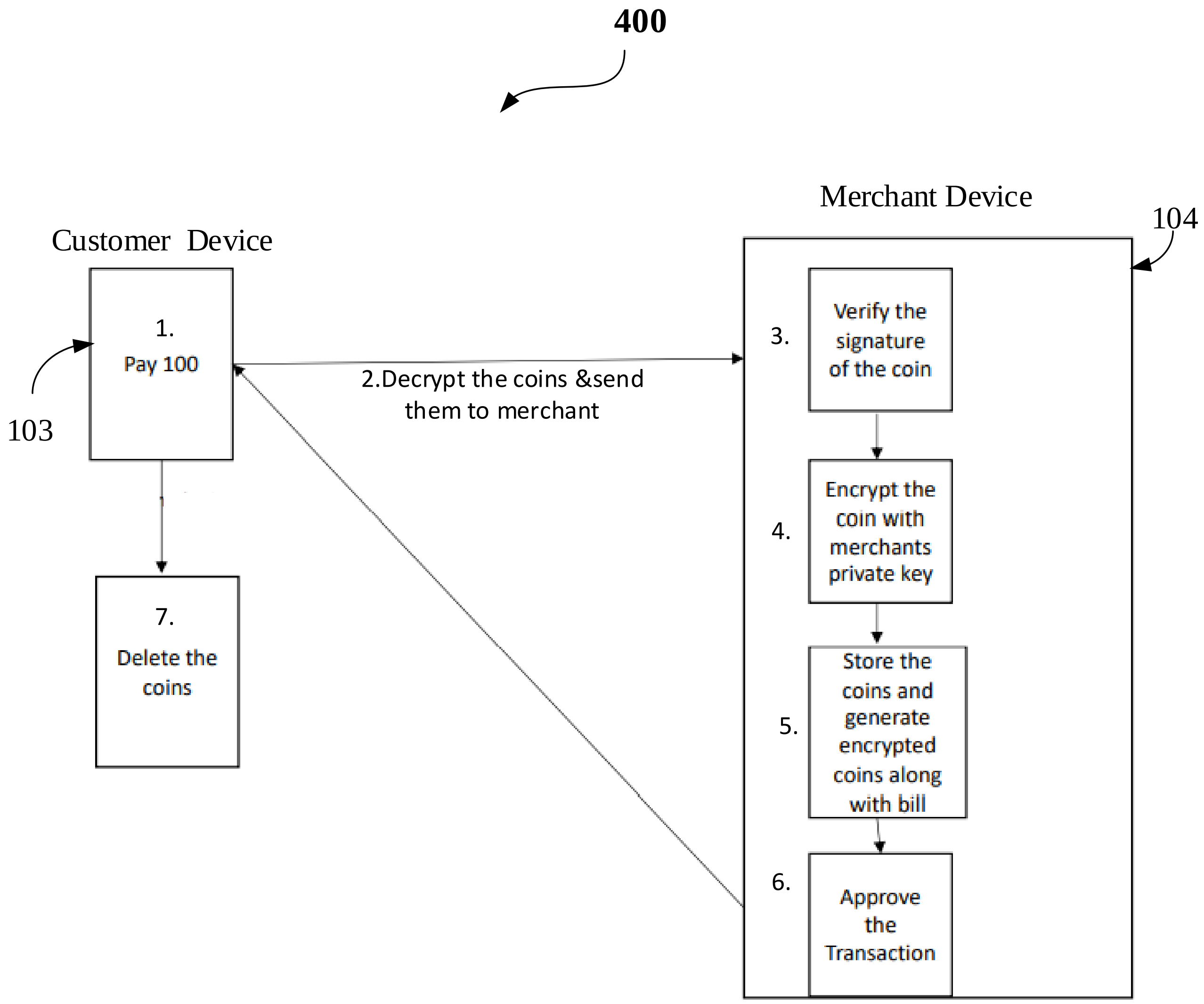
400
Merchant Device
104
Customer Device
1.
Pay 100
103
2.Decrypt the coins &send them to merchant
3.
Verify the signature of the coin
4.
Encrypt the coin with merchants private key
5.
Store the coins and generate encrypted coins along with bill
6.
Approve the Transaction
7.
Delete the coins

Figure 4

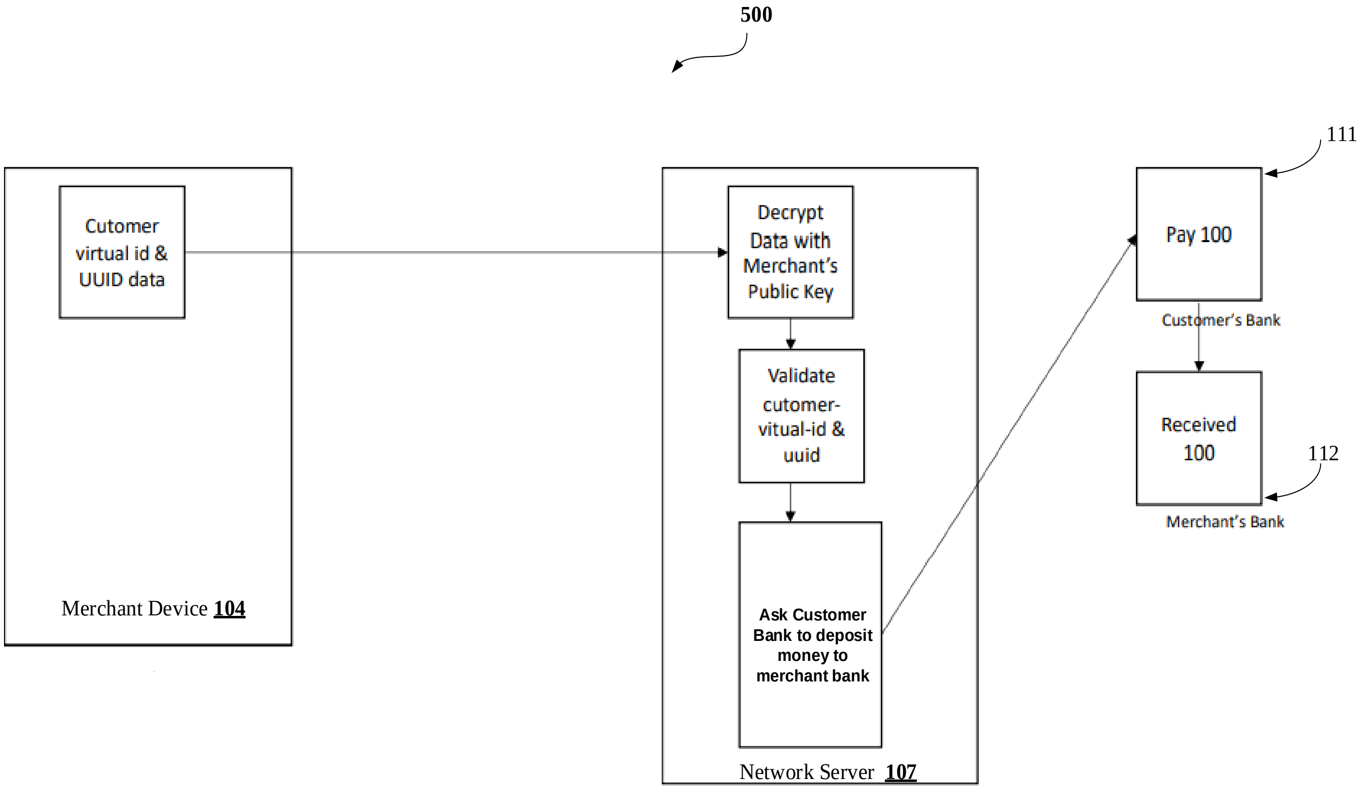
500
111
Cutomer virtual id & UUID data
Merchant Device 104
Decrypt Data with Merchant's Public Key
Validate cutomer-vitual-id & uuid
Ask Customer Bank to deposit money to merchant bank
Network Server 107
Pay 100
Customer's Bank
Received 100
112
Merchant's Bank

Figure 5

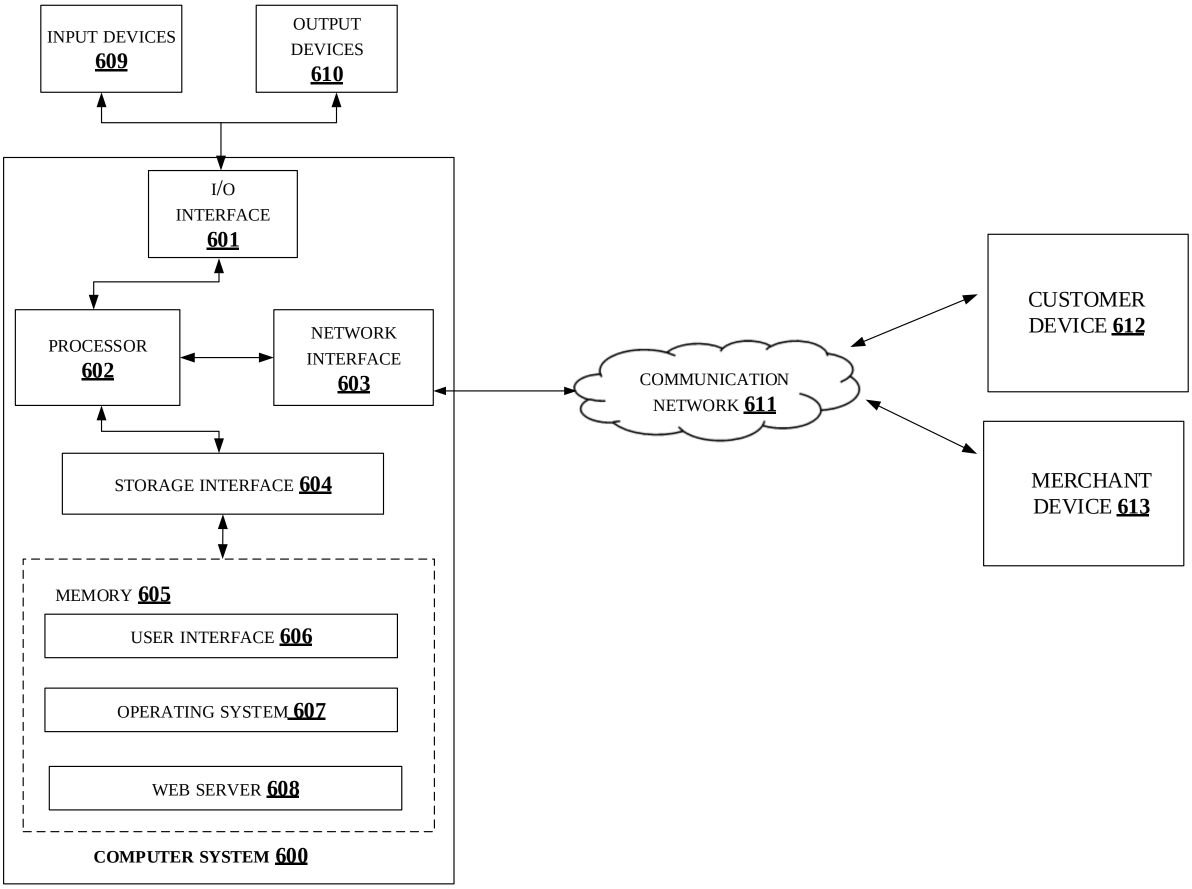
INPUT DEVICES 609
OUTPUT DEVICES 610
I/O INTERFACE 601
PROCESSOR 602
NETWORK INTERFACE 603
STORAGE INTERFACE 604
MEMORY 605
USER INTERFACE 606
OPERATING SYSTEM 607
WEB SERVER 608
COMPUTER SYSTEM 600
COMMUNICATION NETWORK 611
CUSTOMER DEVICE 612
MERCHANT DEVICE 613

Figure 6