



PCT

- | | |
|--|---|
| <p>(51) International Patent Classification:
 <i>G07F 7/08</i> (2006.01) <i>G06Q 20/00</i> (2006.01)
 <i>G06Q 30/00</i> (2006.01)</p> <p>(21) International Application Number:
 PCT/IB2009/051252</p> <p>(22) International Filing Date:
 25 March 2009 (25.03.2009)</p> <p>(25) Filing Language: English</p> <p>(26) Publication Language: English</p> <p>(71) Applicant (for all designated States except US): NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FI-02150 Espoo (FI).</p> <p>(71) Applicant (for LC only): NOKIA, INC. [US/US]; 6021 Connection Drive, MS 2-5-520, Irving, Texas 75039 (US).</p> | <p>(72) Inventor; and
 (75) Inventor/Applicant (for US only): IMMONEN, Ari Tapani [FI/FI]; Kurkihirrentie 8K25, FI-02330 Espoo (FI).</p> <p>(74) Agents: LEYES, Charles A. et al.; Alston & Bird LLP, Bank of America Plaza, 101 S. Tryon Street, Suite 4000, Charlotte, NC 28280-4000 (US).</p> <p>(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.</p> |
|--|---|

[Continued on next page]

- (54) Title:** SYSTEMS, METHODS, APPARATUSES, AND COMPUTER PROGRAM PRODUCTS FOR GENERATION AND EXCHANGE OF DIGITAL CURRENCY

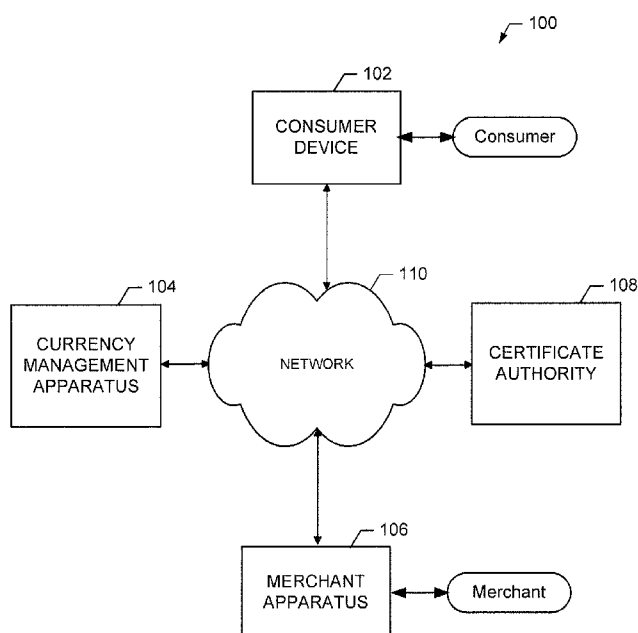


FIG. 1.

- (57) Abstract:** A method, apparatus, and computer program product are provided for generation and exchange of digital currency. A method may include entering into a transaction with a merchant. The method may further include accessing a unit of digital currency from a digital currency wallet. The unit of digital currency may be verifiable based at least in part upon a public key infrastructure. The method of may additionally include conveying the unit of digital currency to the merchant as at least partial payment for the transaction. Corresponding computer program products and apparatuses are also provided.



(84) **Designated States** (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

— *with international search report (Art. 21(3))*

SYSTEMS, METHODS, APPARATUSES, AND COMPUTER PROGRAM PRODUCTS FOR GENERATION AND EXCHANGE OF DIGITAL CURRENCY

TECHNOLOGICAL FIELD

Embodiments of the present invention relate generally to electronic commerce and, more particularly, relate to systems, methods, apparatuses, and computer program products for generation and exchange of digital currency.

5

BACKGROUND

The modern communications era has brought about a tremendous expansion of wireline and wireless networks. Computer networks, television networks, and telephony networks are experiencing an unprecedented technological expansion, fueled by consumer demand. Wireless and mobile networking technologies have addressed related consumer demands, while providing more flexibility and immediacy of information transfer.

In this regard, the modern communications era has enabled electronic commerce, which allows a consumer to purchase goods and services using a communication device in communication with a merchant over a network or other link. For example, a consumer may remotely purchase goods or services from an online vendor over the internet. In another example, a consumer may use a mobile computing device to engage in electronic commerce at a point of sale, such as in a supermarket or restaurant.

However, to date, electronic commerce has been limited in the form of payment that a consumer may use in electronic transactions for goods or services in transactions. In this regard, traditional electronic commerce transactions often involve a consumer electronically providing credit card information to a merchant, which may then verify the consumer's identity and/or the validity of the credit card with a credit card issuer prior to completing the transaction. Unfortunately, no robust and practical approximation exists in electronic commerce for a cash transaction, such as where a consumer enters a brick and mortar store and exchanges tangible currency for a good, such that an identity of the consumer need not be verified because the currency itself is known to be valid. In this regard, systems for certifying, verifying, and exchanging digital currency are not available to enable electronic commerce using digital currency.

Accordingly, it may be desirable to provide systems, methods, apparatuses, and computer program products for facilitating generation and exchange of digital currency.

30

BRIEF SUMMARY OF SOME EXAMPLES OF THE INVENTION

A method, apparatus, and computer program product are therefore provided for facilitating generation and exchange of digital currency. In this regard, a method, apparatus, and computer program product are provided that may provide several advantages to computing devices, computing device users, merchants, and financial service providers. Embodiments of the invention provide for the generation of digital currency that is verifiable using a public key infrastructure. Embodiments of the invention further facilitate transactions using digital currency. Some embodiments provide counterfeit protection schemes. Use of a centralized trust facilitator, such as a certificate authority, by embodiments of the invention further provides for scaling in that multiple currency management apparatuses managed by multiple financial institutions, multiple consumers, multiple consumer devices, multiple merchants, and/or multiple merchant apparatuses may be added to a system for facilitating generation and exchange of digital currency.

In a first exemplary embodiment, a method is provided, which includes entering into a transaction with a merchant. The method of this embodiment further includes accessing a unit of digital currency from a digital currency wallet. The unit of digital currency of this embodiment is verifiable based at least in part upon a public key infrastructure. The method of this embodiment additionally includes conveying the unit of digital currency to the merchant as at least partial payment for the transaction.

In another exemplary embodiment, a computer program product is provided. The computer program product includes at least one computer-readable storage medium having computer-readable program instructions stored therein. The computer-readable program instructions may include a plurality of program instructions. Although in this summary, the program instructions are ordered, it will be appreciated that this summary is provided merely for purposes of example and the ordering is merely to facilitate summarizing the computer program product. The example ordering in no way limits the implementation of the associated computer program instructions. The first program instruction of this embodiment is for entering into a transaction with a merchant. The second program instruction of this embodiment is for accessing a unit of digital currency from a digital currency wallet. The unit of digital currency of this embodiment is verifiable based at least in part upon a public key infrastructure. The third program instruction of this embodiment is for conveying the unit of digital currency to the merchant as at least partial payment for the transaction.

In another exemplary embodiment, an apparatus is provided. The apparatus of this embodiment includes a processor and a memory storing instructions that when executed by the processor cause the apparatus to enter into a transaction with a merchant. The instructions of this embodiment when executed by the processor further cause the apparatus to a unit of digital currency from a digital currency wallet. The unit of digital currency of this embodiment is verifiable based at least in part upon a public key infrastructure. The instructions of this embodiment when executed by the processor additionally cause the apparatus to convey the unit of digital currency to the merchant as at least partial payment for the transaction.

In another exemplary embodiment, an apparatus is provided, which includes means for entering into a transaction with a merchant. The apparatus of this embodiment further includes means for accessing a unit of digital currency from a digital currency wallet. The unit of digital currency of this embodiment is verifiable based at least in part upon a public key infrastructure.

5 The apparatus of this embodiment additionally includes means for conveying the unit of digital currency to the merchant as at least partial payment for the transaction.

The above summary is provided merely for purposes of summarizing some example embodiments of the invention so as to provide a basic understanding of some aspects of the invention. Accordingly, it will be appreciated that the above described example embodiments are
10 merely examples and should not be construed to narrow the scope or spirit of the invention in any way. It will be appreciated that the scope of the invention encompasses many potential embodiments, some of which will be further described below, in addition to those here summarized.

15 BRIEF DESCRIPTION OF THE DRAWING(S)

Having thus described embodiments of the invention in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. 1 illustrates a system for facilitating generation and exchange of digital currency according to an exemplary embodiment of the present invention;

20 FIG. 2 is a schematic block diagram of a mobile terminal according to an exemplary embodiment of the present invention;

FIG. 3 illustrates a block diagram of a consumer device according to an exemplary embodiment of the invention within the context of the system of FIG. 1;

25 FIG. 4 illustrates a block diagram of a currency management apparatus according to an exemplary embodiment of the invention within the context of the system of FIG. 1;

FIG. 5 illustrates a block diagram of a merchant apparatus according to an exemplary embodiment of the invention within the context of the system of FIG. 1;

FIG. 6 illustrates a block diagram of a certificate authority according to an exemplary embodiment of the invention within the context of the system of FIG. 1;

30 FIG. 7 illustrates a flowchart according to an exemplary method for using digital currency according to an exemplary embodiment of the invention;

FIG. 8 illustrates a flowchart according to an exemplary method for implementing a counterfeit protection scheme according to an exemplary embodiment of the invention;

35 FIG. 9 illustrates a flowchart according to an exemplary method for generating and issuing digital currency according to an exemplary embodiment of the invention; and

FIG. 10 illustrates a flowchart according to an exemplary method for receiving digital currency as payment for a transaction according to an exemplary embodiment of the invention.

DETAILED DESCRIPTION

Some embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like reference numerals refer to like elements throughout.

Embodiments of a System for Facilitating Generation and Exchange of Digital Currency

FIG. 1 illustrates a block diagram of a system 100 for facilitating generation and exchange of digital currency according to an exemplary embodiment of the present invention. As used herein, "exemplary" merely means an example and as such represents one example embodiment for the invention and should not be construed to narrow the scope or spirit of the invention in any way. It will be appreciated that the scope of the invention encompasses many potential embodiments in addition to those illustrated and described herein. As such, while FIG. 1 illustrates one example of a configuration of a system for facilitating generation and exchange of digital currency, numerous other configurations may also be used to implement embodiments of the present invention.

In at least some embodiments, the system 100 includes various entities, including one or more consumer devices 102, one or more currency management entities 104, one or more merchant apparatuses 106, and a certificate authority 108, which are configured to communicate over a network 110. The network 110 may comprise a wireline network, wireless network (e.g., a cellular network, wireless local area network, wireless wide area network, and/or the like), or some combination thereof, and in an exemplary embodiment comprises or is otherwise embodied as the internet. The network 110 may comprise a structured network and/or an ad-hoc network. Interfaces between the entities of the system 100 over the network 110 may be made on an on-demand basis to facilitate various functions described herein. For example, the consumer device 102 may be configured to interface with the merchant apparatus 106 on an ad-hoc basis when within some proximate range of the merchant apparatus 106, such as through a radio frequency connection, infrared connection, Blue Tooth connection, and/or the like. As such, one or more of the entities of the system 100 may not be in constant communication with other entities of the system 100 over the network 110.

The consumer device 102 may comprise any computing device configured to enable a consumer to receive, store, and/or send digital currency and to enable a consumer using the consumer device 102 to engage in a transaction (e.g., for a good or service) using digital currency. In this regard, the consumer device 102 may be embodied as a server, desktop computer, laptop computer, mobile terminal, mobile computer, mobile phone, mobile communication device, game device, digital camera/camcorder, audio/video player, television device, radio receiver, digital video recorder, positioning device, any combination thereof, and/or the like. In an exemplary

embodiment, the consumer device 102 is embodied as a mobile terminal, such as that illustrated in FIG. 2

In this regard, FIG. 2 illustrates a block diagram of a mobile terminal 10 representative of one embodiment of a consumer device 102 in accordance with embodiments of the present invention. It should be understood, however, that the mobile terminal 10 illustrated and hereinafter described is merely illustrative of one type of consumer device 102 that may implement and/or benefit from embodiments of the present invention and, therefore, should not be taken to limit the scope of the present invention. While several embodiments of the electronic device are illustrated and will be hereinafter described for purposes of example, other types of electronic devices, such as mobile telephones, mobile computers, portable digital assistants (PDAs), pagers, laptop computers, desktop computers, gaming devices, televisions, and other types of electronic systems, may employ embodiments of the present invention.

As shown, the mobile terminal 10 may include an antenna 12 (or multiple antennas 12) in communication with a transmitter 14 and a receiver 16. The mobile terminal may also include a controller 20 or other processor(s) that provides signals to and receives signals from the transmitter and receiver, respectively. These signals may include signaling information in accordance with an air interface standard of an applicable cellular system, and/or any number of different wireline or wireless networking techniques, comprising but not limited to Wireless-Fidelity (Wi-Fi), wireless local access network (WLAN) techniques such as Institute of Electrical and Electronics Engineers (IEEE) 802.11, and/or the like. In addition, these signals may include speech data, user generated data, user requested data, and/or the like. In this regard, the mobile terminal may be capable of operating with one or more air interface standards, communication protocols, modulation types, access types, and/or the like. More particularly, the mobile terminal may be capable of operating in accordance with various first generation (1G), second generation (2G), 2.5G, third-generation (3G) communication protocols, fourth-generation (4G) communication protocols, and/or the like. For example, the mobile terminal may be capable of operating in accordance with 2G wireless communication protocols IS-136 (Time Division Multiple Access (TDMA)), Global System for Mobile communications (GSM), IS-95 (Code Division Multiple Access (CDMA)), and/or the like. Also, for example, the mobile terminal may be capable of operating in accordance with 2.5G wireless communication protocols General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and/or the like. Further, for example, the mobile terminal may be capable of operating in accordance with 3G wireless communication protocols such as Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access 2000 (CDMA2000), Wideband Code Division Multiple Access (WCDMA), Time Division-Synchronous Code Division Multiple Access (TD-SCDMA), and/or the like. The mobile terminal may be additionally capable of operating in accordance with 3.9G wireless communication protocols such as Long Term Evolution (LTE) or Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and/or the like. Additionally, for example, the mobile terminal may be capable of operating in accordance with fourth-generation (4G) wireless communication protocols and/or the like as well as similar wireless communication protocols that may be developed in the future.

Some Narrow-band Advanced Mobile Phone System (NAMPS), as well as Total Access Communication System (TACS), mobile terminals may also benefit from embodiments of this invention, as should dual or higher mode phones (e.g., digital/analog or TDMA/CDMA/analog phones). Additionally, the mobile terminal 10 may be capable of operating according to Wireless Fidelity (Wi-Fi) or Worldwide Interoperability for Microwave Access (WiMAX) protocols.

It is understood that the controller 20 may comprise circuitry for implementing audio/video and logic functions of the mobile terminal 10. For example, the controller 20 may comprise a digital signal processor device, a microprocessor device, an analog-to-digital converter, a digital-to-analog converter, and/or the like. Control and signal processing functions of the mobile terminal may be allocated between these devices according to their respective capabilities. The controller may additionally comprise an internal voice coder (VC) 20a, an internal data modem (DM) 20b, and/or the like. Further, the controller may comprise functionality to operate one or more software programs, which may be stored in memory. For example, the controller 20 may be capable of operating a connectivity program, such as a web browser. The connectivity program may allow the mobile terminal 10 to transmit and receive web content, such as location-based content, according to a protocol, such as Wireless Application Protocol (WAP), hypertext transfer protocol (HTTP), and/or the like. The mobile terminal 10 may be capable of using a Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit and receive web content across the internet or other networks.

The mobile terminal 10 may also comprise a user interface including, for example, an earphone or speaker 24, a ringer 22, a microphone 26, a display 28, a user input interface, and/or the like, which may be operationally coupled to the controller 20. Although not shown, the mobile terminal may comprise a battery for powering various circuits related to the mobile terminal, for example, a circuit to provide mechanical vibration as a detectable output. The user input interface may comprise devices allowing the mobile terminal to receive data, such as a keypad 30, a touch display (not shown), a joystick (not shown), and/or other input device. In embodiments including a keypad, the keypad may comprise numeric (0-9) and related keys (#, *), and/or other keys for operating the mobile terminal.

As shown in FIG. 2, the mobile terminal 10 may also include one or more means for sharing and/or obtaining data. For example, the mobile terminal may comprise a short-range radio frequency (RF) transceiver and/or interrogator 64 so data may be shared with and/or obtained from electronic devices in accordance with RF techniques. The mobile terminal may comprise other short-range transceivers, such as, for example, an infrared (IR) transceiver 66, a Bluetooth™ (BT) transceiver 68 operating using Bluetooth™ brand wireless technology developed by the Bluetooth™ Special Interest Group, a wireless universal serial bus (USB) transceiver 70 and/or the like. The Bluetooth™ transceiver 68 may be capable of operating according to ultra-low power Bluetooth™ technology (e.g., Wibree™) radio standards. In this regard, the mobile terminal 10 and, in particular, the short-range transceiver may be capable of transmitting data to and/or receiving data from electronic devices within a proximity of the mobile terminal, such as within 10 meters, for example. Although not shown, the mobile terminal may be capable of transmitting

and/or receiving data from electronic devices according to various wireless networking techniques, including Wireless Fidelity (Wi-Fi), WLAN techniques such as IEEE 802.11 techniques, and/or the like.

The mobile terminal 10 may comprise memory, such as a subscriber identity module (SIM) 38, a removable user identity module (R-UIM), and/or the like, which may store information elements related to a mobile subscriber. In addition to the SIM, the mobile terminal may comprise other removable and/or fixed memory. The mobile terminal 10 may include volatile memory 40 and/or non-volatile memory 42. For example, volatile memory 40 may include Random Access Memory (RAM) including dynamic and/or static RAM, on-chip or off-chip cache memory, and/or the like. Non-volatile memory 42, which may be embedded and/or removable, may include, for example, read-only memory, flash memory, magnetic storage devices (e.g., hard disks, floppy disk drives, magnetic tape, etc.), optical disc drives and/or media, non-volatile random access memory (NVRAM), and/or the like. Like volatile memory 40 non-volatile memory 42 may include a cache area for temporary storage of data. The memories may store one or more software programs, instructions, pieces of information, data, and/or the like which may be used by the mobile terminal for performing functions of the mobile terminal. For example, the memories may comprise an identifier, such as an international mobile equipment identification (IMEI) code, capable of uniquely identifying the mobile terminal 10.

Referring now to FIG. 3, which illustrates a block diagram of a consumer device 102 according to an exemplary embodiment of the invention within the context of the system 100, in an exemplary embodiment, the consumer device 102 includes various means, such as a processor 120, memory 122, communication interface 124, user interface 126, and currency wallet manager 128 for performing the various functions herein described. These means of the consumer device 102 as described herein may be embodied as, for example, hardware elements (e.g., a suitably programmed processor, combinational logic circuit, and/or the like), a computer program product comprising computer-readable program instructions (e.g., software or firmware) stored on a computer-readable medium (e.g. memory 122) that is executable by a suitably configured processing device (e.g., the processor 120), or some combination thereof.

The processor 120 may, for example, be embodied as various means including one or more microprocessors with accompanying digital signal processor(s), one or more processor(s) without an accompanying digital signal processor, one or more coprocessors, one or more controllers, processing circuitry, one or more computers, various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit) or FPGA (field programmable gate array), or some combination thereof. Accordingly, although illustrated in FIG. 3 as a single processor, in some embodiments the processor 120 comprises a plurality of processors. In an exemplary embodiment, the processor 120 is configured to execute instructions stored in the memory 122 or otherwise accessible to the processor 120. These instructions, when executed by the processor 120, may cause the consumer device 102 to perform one or more of the functionalities of the consumer device 102 as described herein. As such, whether configured by hardware or software methods, or by a combination thereof, the processor

120 may represent an entity capable of performing operations according to embodiments of the present invention while configured accordingly. Thus, for example, when the processor 120 is embodied as an ASIC, FPGA or the like, the processor 120 may comprise specifically configured hardware for conducting one or more operations described herein. Alternatively, as another
5 example, when the processor 120 is embodied as an executor of instructions, the instructions may specifically configure the processor 120 to perform one or more algorithms and operations described herein.

The memory 122 may include, for example, volatile and/or non-volatile memory. Although illustrated in FIG. 3 as a single memory, the memory 122 may comprise a plurality of memories.
10 The memory 122 may comprise volatile memory, non-volatile memory, or some combination thereof. In this regard, the memory 122 may comprise, for example, a hard disk, random access memory, cache memory, flash memory, a compact disc read only memory (CD-ROM), digital versatile disc read only memory (DVD-ROM), an optical disc, circuitry configured to store information, or some combination thereof. The memory 122 may be configured to store
15 information, data, applications, instructions, or the like for enabling the consumer device 102 to carry out various functions in accordance with exemplary embodiments of the present invention. For example, in at least some embodiments, the memory 122 is configured to buffer input data for processing by the processor 120. Additionally or alternatively, in at least some embodiments, the memory 122 is configured to store program instructions for execution by the processor 120. The
20 memory 122 may store information in the form of static and/or dynamic information. In this regard, the memory 122 may comprise, for example, a virtual currency "wallet" that stores digital currency. This stored information may be stored and/or used by the currency wallet manager 128 during the course of performing its functionalities.

The communication interface 124 may be embodied as any device or means embodied in
25 hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 122) and executed by a processing device (e.g., the processor 120), or a combination thereof that is configured to receive and/or transmit data from/to a remote device (e.g., another consumer device 102, a currency management apparatus 104, a merchant apparatus 106, a certificate authority 108, and/or the like) over the
30 network 110. In at least one embodiment, the communication interface 124 is at least partially embodied as or otherwise controlled by the processor 120. In this regard, the communication interface 124 may be in communication with the processor 120, such as via a bus. The communication interface 124 may include, for example, an antenna, a transmitter, a receiver, a transceiver and/or supporting hardware or software for enabling communications with other entities
35 of the system 100. The communication interface 124 may be configured to receive and/or transmit data using any protocol that may be used for communications between computing devices of the system 100. The communication interface 124 may additionally be in communication with the memory 122, user interface 126, and/or currency wallet manager 128, such as via a bus.

The user interface 126 may be in communication with the processor 120 to receive an
40 indication of a user input and/or to provide an audible, visual, mechanical, or other output to the

user. As such, the user interface 126 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen display, a microphone, a speaker, and/or other input/output mechanisms. The user interface 126 may be in communication with the memory 122, communication interface 124, and/or currency wallet manager 128, such as via a bus.

5 The currency wallet manager 128 may be embodied as various means, such as hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 122) and executed by a processing device (e.g., the processor 120), or some combination thereof and, in one embodiment, is embodied as or otherwise controlled by the processor 120. In embodiments where the currency wallet manager
10 128 is embodied separately from the processor 120, the currency wallet manager 128 may be in communication with the processor 120. The currency wallet manager 128 may further be in communication with the memory 122, communication interface 124, and/or user interface 126, such as via a bus.

FIG. 4 illustrates a block diagram of a currency management apparatus 104 according to
15 an exemplary embodiment of the invention within the context of the system 100. The currency management apparatus 104 may comprise one or more computing devices configured to generate and issue digital currency to a consumer device 102. In this regard, the currency management apparatus 104 may comprise, for example, one or more server computing devices. The currency management apparatus 104 may, for example, be managed by a bank, credit card company, or
20 other financial institution that may, for example, issue digital currency to a consumer out of the consumer's deposit account and/or from the consumer's line of credit. In an exemplary embodiment, the currency management apparatus 104 includes various means, such as a processor 130, memory 132, communication interface 134, user interface 136, and currency manager 138 for performing the various functions herein described. These means of the currency management apparatus 104 as described herein may be embodied as, for example, hardware
25 elements (e.g., a suitably programmed processor, combinational logic circuit, and/or the like), a computer program product comprising computer-readable program instructions (e.g., software or firmware) stored on a computer-readable medium (e.g. memory 132) that is executable by a suitably configured processing device (e.g., the processor 130), or some combination thereof.

30 The processor 130 may, for example, be embodied as various means including one or more microprocessors with accompanying digital signal processor(s), one or more processor(s) without an accompanying digital signal processor, one or more coprocessors, one or more controllers, processing circuitry, one or more computers, various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit)
35 or FPGA (field programmable gate array), or some combination thereof. Accordingly, although illustrated in FIG. 4 as a single processor, in some embodiments the processor 130 comprises a plurality of processors. The plurality of processors may be embodied on a single computing device or distributed among a plurality of computing devices. The plurality of processors may be in operative communication with each other and may be collectively configured to perform one or
40 more functionalities of the currency management apparatus 104 as described herein. In an

exemplary embodiment, the processor 130 is configured to execute instructions stored in the memory 132 or otherwise accessible to the processor 130. These instructions, when executed by the processor 130, may cause the currency management apparatus 104 to perform one or more of the functionalities of the currency management apparatus 104 as described herein. As such, whether configured by hardware or software methods, or by a combination thereof, the processor 130 may represent an entity capable of performing operations according to embodiments of the present invention while configured accordingly. Thus, for example, when the processor 130 is embodied as an ASIC, FPGA or the like, the processor 130 may comprise specifically configured hardware for conducting one or more operations described herein. Alternatively, as another example, when the processor 130 is embodied as an executor of instructions, the instructions may specifically configure the processor 130 to perform one or more algorithms and operations described herein.

The memory 132 may include, for example, volatile and/or non-volatile memory. Although illustrated in FIG. 4 as a single memory, the memory 132 may comprise a plurality of memories, which may be embodied on a single computing device or distributed across a plurality of computing devices. The memory 132 may comprise volatile memory, non-volatile memory, or some combination thereof. In this regard, the memory 132 may comprise, for example, a hard disk, random access memory, cache memory, flash memory, a compact disc read only memory (CD-ROM), digital versatile disc read only memory (DVD-ROM), an optical disc, circuitry configured to store information, or some combination thereof. The memory 132 may be configured to store information, data, applications, instructions, or the like for enabling the currency management apparatus 104 to carry out various functions in accordance with exemplary embodiments of the present invention. For example, in at least some embodiments, the memory 132 is configured to buffer input data for processing by the processor 130. Additionally or alternatively, in at least some embodiments, the memory 132 is configured to store program instructions for execution by the processor 130. The memory 132 may store information in the form of static and/or dynamic information. This stored information may be stored and/or used by the currency manager 138 during the course of performing its functionalities.

The communication interface 134 may be embodied as any device or means embodied in hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 132) and executed by a processing device (e.g., the processor 130), or a combination thereof that is configured to receive and/or transmit data from/to a remote device (e.g., a consumer device 102, merchant apparatus 106, certificate authority 108, and/or the like) over the network 110. In at least one embodiment, the communication interface 134 is at least partially embodied as or otherwise controlled by the processor 130. In this regard, the communication interface 134 may be in communication with the processor 130, such as via a bus. The communication interface 134 may include, for example, an antenna, a transmitter, a receiver, a transceiver and/or supporting hardware or software for enabling communications with other entities of the system 100. The communication interface 134 may be configured to receive and/or transmit data using any protocol that may be used for

communications between computing devices of the system 100. The communication interface 134 may additionally be in communication with the memory 132, user interface 136, and/or currency manager 138, such as via a bus.

The user interface 136 may be in communication with the processor 130 to receive an indication of a user input and/or to provide an audible, visual, mechanical, or other output to the user. As such, the user interface 136 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen display, a microphone, a speaker, and/or other input/output mechanisms. In an exemplary embodiment in which the currency management apparatus 104 is embodied as one or more servers, the user interface 136 may be limited, or even eliminated. The user interface 136 may be in communication with the memory 132, communication interface 134, and/or currency manager 138, such as via a bus.

The currency manager 138 may be embodied as various means, such as hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 132) and executed by a processing device (e.g., the processor 130), or some combination thereof and, in one embodiment, is embodied as or otherwise controlled by the processor 130. In embodiments where the currency manager 138 is embodied separately from the processor 130, the currency manager 138 may be in communication with the processor 130. The currency manager 138 may further be in communication with the memory 132, communication interface 134, and/or user interface 136, such as via a bus.

FIG. 5 illustrates a block diagram of a merchant apparatus 106 according to an exemplary embodiment of the invention within the context of the system 100. The merchant apparatus 106 may comprise one or more computing devices configured to facilitate a transaction between a merchant and a consumer using a consumer device 102. In this regard, the merchant apparatus 106 may comprise, for example, a point of sale system, such as may be located at a checkout point of a brick and mortar merchant. In some embodiments, the merchant apparatus 106 comprises one or more server devices configured to facilitate a transaction with a remote consumer device 102, such as over the internet. In an exemplary embodiment, the merchant apparatus 106 includes various means, such as a processor 140, memory 142, communication interface 144, user interface 146, and transaction manager 148 for performing the various functions herein described. These means of the merchant apparatus 106 as described herein may be embodied as, for example, hardware elements (e.g., a suitably programmed processor, combinational logic circuit, and/or the like), a computer program product comprising computer-readable program instructions (e.g., software or firmware) stored on a computer-readable medium (e.g. memory 142) that is executable by a suitably configured processing device (e.g., the processor 140), or some combination thereof.

The processor 140 may, for example, be embodied as various means including one or more microprocessors with accompanying digital signal processor(s), one or more processor(s) without an accompanying digital signal processor, one or more coprocessors, one or more controllers, processing circuitry, one or more computers, various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit)

or FPGA (field programmable gate array), or some combination thereof. Accordingly, although illustrated in FIG. 5 as a single processor, in some embodiments the processor 140 comprises a plurality of processors. The plurality of processors may be embodied on a single computing device or distributed among a plurality of computing devices. The plurality of processors may be in
5 operative communication with each other and may be collectively configured to perform one or more functionalities of the merchant apparatus 106 as described herein. In an exemplary embodiment, the processor 140 is configured to execute instructions stored in the memory 142 or otherwise accessible to the processor 140. These instructions, when executed by the processor 140, may cause the merchant apparatus 106 to perform one or more of the functionalities of the
10 merchant apparatus 106 as described herein. As such, whether configured by hardware or software methods, or by a combination thereof, the processor 140 may represent an entity capable of performing operations according to embodiments of the present invention while configured accordingly. Thus, for example, when the processor 140 is embodied as an ASIC, FPGA or the like, the processor 140 may comprise specifically configured hardware for conducting one or more
15 operations described herein. Alternatively, as another example, when the processor 140 is embodied as an executor of instructions, the instructions may specifically configure the processor 140 to perform one or more algorithms and operations described herein.

The memory 142 may include, for example, volatile and/or non-volatile memory. Although illustrated in FIG. 5 as a single memory, the memory 142 may comprise a plurality of memories,
20 which may be embodied on a single computing device or distributed across a plurality of computing devices. The memory 142 may comprise volatile memory, non-volatile memory, or some combination thereof. In this regard, the memory 142 may comprise, for example, a hard disk, random access memory, cache memory, flash memory, a compact disc read only memory (CD-ROM), digital versatile disc read only memory (DVD-ROM), an optical disc, circuitry
25 configured to store information, or some combination thereof. The memory 142 may be configured to store information, data, applications, instructions, or the like for enabling the merchant apparatus 106 to carry out various functions in accordance with exemplary embodiments of the present invention. For example, in at least some embodiments, the memory 142 is configured to buffer input data for processing by the processor 140. Additionally or alternatively, in at least some
30 embodiments, the memory 142 is configured to store program instructions for execution by the processor 140. The memory 142 may store information in the form of static and/or dynamic information. This stored information may be stored and/or used by the transaction manager 148 during the course of performing its functionalities.

The communication interface 144 may be embodied as any device or means embodied in
35 hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 142) and executed by a processing device (e.g., the processor 140), or a combination thereof that is configured to receive and/or transmit data from/to a remote device (e.g., a consumer device 102, currency management apparatus 104, certificate authority 108, and/or the like) over the network 110. In at least one embodiment, the
40 communication interface 144 is at least partially embodied as or otherwise controlled by the

processor 140. In this regard, the communication interface 144 may be in communication with the processor 140, such as via a bus. The communication interface 144 may include, for example, an antenna, a transmitter, a receiver, a transceiver and/or supporting hardware or software for enabling communications with other entities of the system 100. The communication interface 144
5 may be configured to receive and/or transmit data using any protocol that may be used for communications between computing devices of the system 100. The communication interface 144 may additionally be in communication with the memory 142, user interface 146, and/or transaction manager 148, such as via a bus.

The user interface 146 may be in communication with the processor 140 to receive an
10 indication of a user input and/or to provide an audible, visual, mechanical, or other output to the user. As such, the user interface 146 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen display, a microphone, a speaker, and/or other input/output mechanisms. In an exemplary embodiment in which the merchant apparatus 106 is embodied as one or more servers, the user interface 146 may be limited, or even eliminated. The user interface 146 may be
15 in communication with the memory 142, communication interface 144, and/or transaction manager 148, such as via a bus.

The transaction manager 148 may be embodied as various means, such as hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 142) and executed by a processing device (e.g., the
20 processor 140), or some combination thereof and, in one embodiment, is embodied as or otherwise controlled by the processor 140. In embodiments where the transaction manager 148 is embodied separately from the processor 140, the transaction manager 148 may be in communication with the processor 140. The transaction manager 148 may further be in communication with the memory 142, communication interface 144, and/or user interface 146,
25 such as via a bus.

FIG. 6 illustrates a block diagram of a certificate authority 108 according to an exemplary embodiment of the invention within the context of the system 100. The certificate authority 108 may comprise one or more computing devices (e.g., one or more servers) configured to facilitate implementation of a public key infrastructure (PKI) used by devices of the system 100. In this
30 regard, the certificate authority 108 may be managed by a certificate authority trusted by other devices and entities of the system 100, such that the certificate authority 108 is configured to issue certificates verifying a party's identity to devices of the system 100 and/or to verify the validity of a unit of digital currency issued by the currency management entity 104. The certificate authority 108 may be managed by, for example, a national treasury, or other government entity responsible
35 for the issuance of a currency. In an exemplary embodiment, the certificate authority 108 includes various means, such as a processor 150, memory 152, communication interface 154, user interface 156, certificate manager 158, and currency verifier 160 for performing the various functions herein described. These means of the certificate authority 108 as described herein may be embodied as, for example, hardware elements (e.g., a suitably programmed processor,
40 combinational logic circuit, and/or the like), a computer program product comprising computer-

readable program instructions (e.g., software or firmware) stored on a computer-readable medium (e.g. memory 152) that is executable by a suitably configured processing device (e.g., the processor 150), or some combination thereof.

5 The processor 150 may, for example, be embodied as various means including one or more microprocessors with accompanying digital signal processor(s), one or more processor(s) without an accompanying digital signal processor, one or more coprocessors, one or more controllers, processing circuitry, one or more computers, various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit) or FPGA (field programmable gate array), or some combination thereof. Accordingly, although
10 illustrated in FIG. 6 as a single processor, in some embodiments the processor 150 comprises a plurality of processors. The plurality of processors may be embodied on a single computing device or distributed among a plurality of computing devices. The plurality of processors may be in operative communication with each other and may be collectively configured to perform one or more functionalities of the certificate authority 108 as described herein. In an exemplary
15 embodiment, the processor 150 is configured to execute instructions stored in the memory 152 or otherwise accessible to the processor 150. These instructions, when executed by the processor 150, may cause the certificate authority 108 to perform one or more of the functionalities of the certificate authority 108 as described herein. As such, whether configured by hardware or software methods, or by a combination thereof, the processor 150 may represent an entity capable
20 of performing operations according to embodiments of the present invention while configured accordingly. Thus, for example, when the processor 150 is embodied as an ASIC, FPGA or the like, the processor 150 may comprise specifically configured hardware for conducting one or more operations described herein. Alternatively, as another example, when the processor 150 is embodied as an executor of instructions, the instructions may specifically configure the processor
25 150 to perform one or more algorithms and operations described herein.

The memory 152 may include, for example, volatile and/or non-volatile memory. Although illustrated in FIG. 6 as a single memory, the memory 152 may comprise a plurality of memories, which may be embodied on a single computing device or distributed across a plurality of computing devices. The memory 152 may comprise volatile memory, non-volatile memory, or
30 some combination thereof. In this regard, the memory 152 may comprise, for example, a hard disk, random access memory, cache memory, flash memory, a compact disc read only memory (CD-ROM), digital versatile disc read only memory (DVD-ROM), an optical disc, circuitry configured to store information, or some combination thereof. The memory 152 may be configured to store information, data, applications, instructions, or the like for enabling the certificate authority
35 108 to carry out various functions in accordance with exemplary embodiments of the present invention. For example, in at least some embodiments, the memory 152 is configured to buffer input data for processing by the processor 150. Additionally or alternatively, in at least some embodiments, the memory 152 is configured to store program instructions for execution by the processor 150. The memory 152 may store information in the form of static and/or dynamic

information. This stored information may be stored and/or used by the certificate manager 158 and/or currency verifier 160 during the course of performing their respective functionalities.

The communication interface 154 may be embodied as any device or means embodied in hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 152) and executed by a processing device (e.g., the processor 150), or a combination thereof that is configured to receive and/or transmit data from/to a remote device (e.g., a consumer device 102, currency management apparatus 104, merchant apparatus 106, and/or the like) over the network 110. In at least one embodiment, the communication interface 154 is at least partially embodied as or otherwise controlled by the processor 150. In this regard, the communication interface 154 may be in communication with the processor 150, such as via a bus. The communication interface 154 may include, for example, an antenna, a transmitter, a receiver, a transceiver and/or supporting hardware or software for enabling communications with other entities of the system 100. The communication interface 154 may be configured to receive and/or transmit data using any protocol that may be used for communications between computing devices of the system 100. The communication interface 154 may additionally be in communication with the memory 152, user interface 156, certificate manager 158, and/or currency verifier 160, such as via a bus.

The user interface 156 may be in communication with the processor 150 to receive an indication of a user input and/or to provide an audible, visual, mechanical, or other output to the user. As such, the user interface 156 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen display, a microphone, a speaker, and/or other input/output mechanisms. In an exemplary embodiment in which the certificate authority 108 is embodied as one or more servers, the user interface 156 may be limited, or even eliminated. The user interface 156 may be in communication with the memory 152, communication interface 154, certificate manager 158, and/or currency verifier 160, such as via a bus.

The certificate manager 158 may be embodied as various means, such as hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 152) and executed by a processing device (e.g., the processor 150), or some combination thereof and, in one embodiment, is embodied as or otherwise controlled by the processor 150. In embodiments where the certificate manager 158 is embodied separately from the processor 150, the certificate manager 158 may be in communication with the processor 150. The certificate manager 158 may further be in communication with the memory 152, communication interface 154, user interface 156, and/or currency verifier 160, such as via a bus.

The currency verifier 160 may be embodied as various means, such as hardware, a computer program product comprising computer readable program instructions stored on a computer readable medium (e.g., the memory 152) and executed by a processing device (e.g., the processor 150), or some combination thereof and, in one embodiment, is embodied as or otherwise controlled by the processor 150. In embodiments where the currency verifier 160 is embodied separately from the processor 150, the currency verifier 160 may be in communication

with the processor 150. The currency verifier 160 may further be in communication with the memory 152, communication interface 154, user interface 156, and/or certificate manager 158, such as via a bus.

One or more entities of the system 100 (e.g., the consumer device 102, currency management apparatus 104, merchant apparatus 106, and/or certificate authority 108) may be configured to implement a public key infrastructure. In this regard, entities of the system 100 may possess a public-private key pair. The certificate authority 108 may serve as a trusted party trusted by the consumer device 102, currency management apparatus 104, and merchant apparatus 106. Accordingly, the certificate manager 158 may be configured to issue a digital certificate to entities of the system 100 binding an entity's public key to an identity associated with the entity. In this regard, the certificate manager 158 may be configured to issue a digital certificate on a public key for the consumer device 102 that binds the public key of the consumer device 102 to the consumer's identity. Similarly, the certificate manager 158 may be configured to issue a digital certificate on a public key of the merchant apparatus 106 that binds the public key of the merchant apparatus 106 to the merchant's identity. The certificate manager 158 may be further configured to issue a digital certificate on a public key of the currency management entity 104. The certificate manager 158 may be configured to store issued digital certificates and/or public keys for entities of the system 100 in the memory 152, from which the digital certificates and/or public keys may be accessed by entities of the system 100 for use for verification of digitally signed data in accordance with the public key infrastructure.

Generation of Digital Currency

The currency manager 138 of the currency management apparatus 104 may be configured to generate units of digital currency. A unit of digital currency generated by the currency manager 138 may be signed with a digital signature generated by the currency manager 138 using the private key of the currency management apparatus 104. The currency manager 138 may sign the unit of digital currency for a predefined value (e.g., a denomination of currency), such that a unit of digital currency possesses a defined value. The currency manager 138 may generate digital currency in denominations correlating to the currency which it is digitizing. For example, if generating digital currency correlating to the American dollar, the currency manager 138 may be configured to generate units of digital currency having \$1 and \$5 denominations, but not units of digital currency having \$3 or \$4 denominations. The currency manager 138 may further be configured to generate quantities of various denominations of digital currency so as to generate a value set usable for consumers in their daily transactions. The generated denominations of digital currency may, similar to tangible currency denominations, allow change to be made using various combinations of units of digital currency. Accordingly, for example, if a consumer conveys a unit of digital currency valued at \$1 to a merchant for a product valued at \$0.93, a combination of units of digital currency generated and issued by the currency manager 138 may allow for a consumer to receive \$0.07 in change from a merchant for the difference

between the value of digital currency provided as payment and the value of the product received in exchange.

Some embodiments of the invention implement a counterfeit protection scheme through assignment of a unique serial number to units of digital currency. Accordingly, in such
5 embodiments, no two units of digital currency have the same serial number. The currency manager 138 may be configured to allocate the serial numbers from a set of serial numbers generated by the currency manager 138 and/or from a set of serial numbers provided to the currency management apparatus 104 by the certificate authority 108. A digital signature generated by the currency manager 138 for a unit of digital currency may cover the serial number
10 for the unit of digital currency.

Prior to issuing a unit of digital currency (e.g., to a consumer device 102 or to a merchant apparatus 106), the currency manager 138 may, in embodiments implementing a counterfeit protection scheme, be configured to send a generated unit of digital currency to the certificate authority 108. The currency verifier 160 may be configured to allocate a serial number to the unit
15 of digital currency (e.g., if not already allocated by the currency manager 138). The currency verifier 160 may then store an entry for the serial number in the memory 152 along with information that may be used to subsequently verify validity of the unit of digital currency based at least in part upon the serial number.

The information stored by the currency verifier 160 in association with a serial number may
20 comprise a random code generated by the currency verifier 160. The currency verifier 160 may further add the random code to the unit of digital currency. This random code may comprise a random numeric string, character string, alphanumeric string, and/or the like that may be used to facilitate verification of validity of a unit of digital currency when used for a transaction. In this regard, the random code may be allocated for a unit of digital currency having a unique serial
25 number for use in a single future transaction. Accordingly, when subsequently verifying a unit of digital currency having a serial number and a random code that is used in a transaction, the currency verifier 160 may be configured to access stored information associated with the serial number of the unit of digital currency from the memory 152 and determine whether the random code most recently allocated to the unit of digital currency by the currency verifier 160 correlates
30 with the random code contained in the unit of digital currency. If there is a correlation between the random code in the unit of digital currency and the random code last allocated to the unit of digital currency (e.g., the random codes are the same), the currency verifier 160 may validate the unit of digital currency. The currency verifier 160 may then replace the random code with a new random code for use in a subsequent transaction. Accordingly, counterfeit protection may be achieved in
35 that a unit of digital currency with an assigned unique serial number and comprising a random code may not be copied to enable use for multiple transactions because each random code may be valid only for a single transaction and may then be replaced with a new random code following the transaction.

The information stored by the currency verifier 160 in association with a serial number may
40 alternatively comprise one or more usage steps indicative of a transaction history of the unit of

digital currency. For example, the currency verifier 160 may be configured to store at least a partial usage history of a unit of digital currency in the memory 152. A stored usage step may represent a single transaction involving the unit of digital currency and may, for example, comprise an identity of one or more parties to a transaction, a timestamp indicating when the transaction took place, and/or other transaction-related information that may be used to trace the unit of digital currency. Thus, upon receipt of a newly generated unit of digital currency from a currency management apparatus 104, the currency verifier 160 may be configured to store in association with the serial number allocated to the unit of digital currency, an identity of the currency management apparatus 104, an identity (e.g., a digital certificate issued by the certificate authority 108) for a party (e.g., a consumer, consumer device 102, merchant, merchant apparatus 106, and/or the like) to which the currency management apparatus 104 is issuing the unit of digital currency, a timestamp indicating a time of issuance of the digital currency, and/or the like. As will be further described, when verifying the validity of a unit of digital currency having a serial number that is being conveyed in a transaction, the currency verifier 160 may be configured to access stored information associated with the serial number of the unit of digital currency from the memory 152 and determine whether the party conveying the unit of digital currency correlates with a stored usage step for the serial number and/or whether the unit of digital currency comprises one or more usage steps correlating to the usage step(s) stored in the memory 152. If there is a correlation, the currency verifier 160 may validate the unit of digital currency. The currency verifier 160 may then store a new usage step in association with the serial number to reflect the most recent transaction so that the unit of digital currency may be validated in a future transaction. Accordingly, counterfeit protection may be achieved in that a counterfeit unit of digital currency may not have an identical usage history as a valid unit of digital currency having the same serial number.

Once having stored information and an associated serial number in embodiments implementing a counterfeit protection scheme, the currency verifier 160 may be configured to generate a digital signature on the unit of digital currency, using a private key of the certificate authority 108. This digital signature may be generated on the entire digital currency package, which may include the associated serial number and, if applicable, the random code. The currency verifier 160 may then send the unit of digital currency back to the currency management apparatus 104, which may then issue it to another party.

Issue of Digital Currency

The currency manager 138 may further be configured to issue units of digital currency to another party (e.g., a consumer, a consumer device 102, merchant, merchant apparatus 106, and/or the like) trusted by the currency management apparatus 104. For example, a trusted party may comprise a computing device (e.g., a consumer device 102 or merchant apparatus 106) associated with a customer (e.g., a consumer or merchant) of a party (e.g., a bank) managing operation of the currency management apparatus 104. The identity of the trusted party may be verifiable by the currency manager 138 using a public key infrastructure. In this regard, the

currency manager 138 may be configured to verify the identity of a party that sent a message, request, a unit of digital currency, and/or other digital data to the currency management apparatus 104 based at least in part upon a digital signature included by the transmitting party and a digital certificate issued by the certificate authority 108 that binds the party's private key to the party's identity.

For example, in order to retrieve one or more units of digital currency from the currency management apparatus 104, the currency wallet manager 128 may be configured to establish an identity of a consumer using the consumer device 102 and/or an identity of the consumer device 102 to the currency management apparatus 104 by generating and sending a message to the currency management apparatus. The message may comprise a digital signature generated by the currency wallet manager 128 using the private key of the consumer device 102. The currency manager 138 may then verify the identity of the consumer (e.g., that the consumer is who he says he is and/or that the consumer has an account with or is otherwise known to the currency management apparatus 104) and/or the identity of the consumer device 102 using a digital certificate issued on the consumer device's 102 public key by the certificate authority 108 in accordance with the public key infrastructure. The digital certificate may be included in the message sent by the currency wallet manager 128, may be retrieved from the certificate authority 108, and/or may be pre-stored in the memory 132.

The message sent by the currency wallet manager 128 to establish an identity may be linked with a request for one or more units of digital currency. If not, the currency wallet manager 128 may be configured to send a subsequent message to the currency management apparatus 104 requesting one or more units of digital currency. The request may comprise a request to have the value of the requested unit(s) of digital currency be deducted, for example, from a deposit account (e.g., a checking account, savings account, and/or the like) of the consumer, a line of credit (e.g., a credit card) of the consumer, and/or the like. The request may further specify specific denomination(s) of units of digital currency and quantities thereof requested.

In response to a request for units of digital currency, the currency manager 138 may access appropriate unit(s) of digital currency to satisfy the request from the memory 132. If sufficient units of digital currency to satisfy the request are not already available, the currency manager 138 may generate unit(s) of digital currency as previously described. The currency manager 138 may then issue the appropriate requested unit(s) of digital currency to the consumer device 102. In issuing requested unit(s) of digital currency to a consumer device 102, the currency manager 138 may be configured to send the unit(s) of digital currency to the consumer device 102. Alternatively, in embodiments implementing certain counterfeit protection schemes, when issuing unit(s) of digital currency, the currency manager 138 may be configured to send the issued unit(s) of digital currency to the certificate authority 108 so that the certificate authority 108 may implement and/or enforce the counterfeit protection scheme(s). Accordingly, the currency verifier 160 may receive unit(s) of digital currency issued by the currency management apparatus 104 and then record an appropriate usage step in association with respective serial number(s) for the unit(s) of digital currency or insert a random code into the digital currency unit(s). The currency

verifier 160 may then either send the unit(s) of digital currency back to the currency management apparatus 104 so that the currency manager 138 may send the one or more unit(s) of digital currency to the consumer device 102 or may forward the unit(s) of digital currency to a consumer device 102 (e.g., the consumer device 102 of the consumer requesting digital currency) indicated to the certificate authority 108 by the currency manager 138.

The currency wallet manager 128 may then be configured to receive unit(s) of digital currency sent by the currency manager 138 and/or forwarded by the currency verifier 160. The currency wallet manager 128 may be configured to verify validity of a received unit of digital currency based at least in part upon the public key infrastructure. In this regard, the currency wallet manager 128 may be configured to verify a digital signature of the currency management apparatus 104 included in the unit of digital currency by the currency manager 138 using a digital certificate issued on the public key of the currency management apparatus 104 by the certificate authority 108. Additionally or alternatively, the currency wallet manager 128 may be configured to verify a digital signature of the certificate authority 108 included in the unit of digital currency. The currency wallet manager 128 may access the digital certificate(s) from a message in which the unit of digital currency was sent to the consumer device 102 (e.g., if included by the currency manager 138), from the certificate authority 108, and/or from the memory 122 (e.g., if pre-stored in the memory 122). In some embodiments, the currency wallet manager 128 may be configured to send a received unit of digital currency to the certificate authority 108 so that the currency verifier 160 may verify validity of the unit of digital currency. In such embodiments, if a counterfeit protection scheme is implemented, the currency verifier 160 may be configured to verify the unit of digital currency by determining whether a correlation exists between verification information (e.g., a random code, usage step information describing the issuance of the unit of digital currency from the currency management apparatus 104 to the consumer device 102, and/or the like) included with the unit of digital currency and information stored in memory 152 for the corresponding serial number for the unit of digital currency.

The currency wallet manager 128 may be configured to then store a received unit of digital currency in a digital currency wallet, such as in the memory 122, for subsequent use in a transaction.

It will be appreciated that the transaction manager 148 of the merchant apparatus 106 may be similarly configured to establish an identity of the merchant and/or of the merchant apparatus 106 to the currency management apparatus 104 and request and receive units of digital currency issued to the merchant apparatus 106 (e.g., to a merchant associated with the merchant apparatus 106) by the currency management apparatus 104. Accordingly, the transaction manager 148 may be configured to implement at least some of the functionality described above in connection with the currency wallet manager 128.

Use of Digital Currency in a Transaction

The consumer may cause the currency wallet manager 128 to enter into a transaction with the merchant, such as through consumer interaction with the user interface 126. The transaction

may be of any type and have any terms that may be negotiated and/or agreed upon between a consumer and merchant. The transaction may occur, for example, on location at a merchant's brick and mortar store or may occur remotely, such as through consumer access of a website provided by the merchant via the merchant apparatus 106. The transaction manager 148 may be configured to send transaction terms, payment options and/or payment information to the consumer device 102. The currency wallet manager 128 may then cause the payment information and/or payment options to be displayed to the consumer on a display of the user interface 126, such that the consumer may use the user interface 126 to select payment options, such as by selecting one or more units of digital currency from the digital currency wallet to convey to the merchant apparatus 106 as at least partial payment for the transaction.

The currency wallet manager 128 may then be configured to access one or more units of digital currency from the digital currency wallet in memory 122. The currency wallet manager 128 may further generate a message conveying the one or more units of digital currency to the merchant apparatus 106. The currency wallet manager 128 may generate a digital signature to include in the message using the private key of the consumer device 102 and may include a digital certificate of the consumer device 102 in the message.

In some embodiments, the currency wallet manager 128 may convey a unit of digital currency to the merchant by sending the message conveying the unit of digital currency to the merchant apparatus 106. The transaction manager 148 may be configured to verify validity of a unit of digital currency conveyed by the consumer device 102 based at least in part upon the public key infrastructure. In this regard, the transaction manager 148 may be configured to verify a digital signature of the currency management apparatus 104 included in the unit of digital currency by the currency manager 138 using a digital certificate issued on the public key of the currency management apparatus 104 by the certificate authority 108. Additionally or alternatively, the transaction manager 148 may be configured to verify a digital signature of the certificate authority 108 included in the unit of digital currency by the currency verifier 160. The transaction manager 148 may access the digital certificate for the currency management apparatus 104 and/or for the certificate authority 108 from the message conveying the unit of digital currency (e.g., if included by the currency wallet manager 128), from the certificate authority 108, and/or from the memory 142 (e.g., if pre-stored in the memory 142). If the unit of digital currency comprises a serial number, the transaction manager 148 may be further configured to verify that the serial number is unique among other units of digital currency conveyed in the transaction and/or other units of digital currency that may be stored in the merchant's digital currency wallet in the memory 142. In this regard, the transaction manager 148 may be configured to verify, for example, that the consumer is not conveying multiple units of digital currency having identical serial numbers (e.g., counterfeit units of digital currency). Additionally or alternatively, the transaction manager 148 may be configured to send a conveyed unit of digital currency to the certificate authority 108 so that the currency verifier 160 may verify validity of the unit of digital currency.

In other embodiments, such as those implementing a counterfeit protection scheme, the currency wallet manager 128 may be configured to send the message conveying the unit of digital

currency to the certificate authority 108 as an intermediary so that the currency verifier 160 may verify the validity of conveyed unit(s) of digital currency prior to forwarding to the conveyee merchant apparatus 106 indicated in the message. The currency wallet manager 128 may include an indication of the identity of the merchant apparatus 106 (e.g., the digital certificate of the merchant apparatus 106, an internet protocol address of the merchant apparatus 106, domain name of the merchant apparatus 106, and/or the like) in the conveyance message so that the certificate authority 108 may send validated unit(s) of digital currency to the appropriate conveyee (e.g., the merchant). The currency verifier 160 may then verify that the serial number of the unit of digital currency is a valid serial number for an issued unit of digital currency and may determine whether the issued unit of digital currency having that serial number has the value of the received unit of digital currency.

The currency verifier 160 may then be configured to verify the unit of digital currency by determining whether a correlation exists between verification information (e.g., a random code, usage step information, and/or the like) included with the unit of digital currency and information stored in memory 152 for the corresponding serial number for the unit of digital currency. If the unit of digital currency comprises a random code and the random code matches the random code associated with the digital currency unit's serial number, the currency verifier may verify that the unit of digital currency is valid and may then generate a new random code and replace the existing random code with the new random code. The currency verifier 160 may store the new random code in association with the serial number for the unit of digital currency in the memory 152. The currency verifier 160 may then send the validated unit of digital currency to the merchant apparatus 106.

In some embodiments, the certificate authority 108 and a conveyee in a transaction (e.g., the merchant apparatus 106 or a consumer device 102) may be configured to implement a PKI enabled handshaking in order to prevent a party from mimicking the certificate authority 108. In this regard and using the merchant apparatus 106 as an example conveyee, the currency verifier 160 may generate an interim random code for a conveyed unit of digital currency and store the interim random code in association with the unit of digital currency in memory 152. The currency verifier 160 may then sign the unit(s) of digital currency conveyed to the merchant apparatus 106 with the private key of the certificate authority 108 and send the conveyed digital currency to the merchant apparatus 106. The currency verifier 160 may encrypt at least a portion of the message sent to the merchant apparatus 106 using the public key of the merchant apparatus 106. The transaction manager 148 may then receive the conveyed unit(s) of digital currency and if encrypted, may decrypt the digital currency unit(s) and identify the sender. In order to further establish the validity of a received unit of digital currency and/or the sender, the transaction manager 148 may send the unit of digital currency to the certificate authority 108. The currency verifier 160 may then receive the returned unit of digital currency, which includes an interim random code, and verify validity of the unit of digital currency based at least in part upon the interim random code. The currency verifier 160 may then generate a final transaction random code and replace the interim random code with the final transaction random code. The currency

verifier 160 may save the final transaction random code in association with the serial number of the digital currency unit for future validation of the digital currency unit. The currency verifier 160 may then send the digital currency unit including the final transaction code back to the merchant apparatus 104. Accordingly, the transaction manager 148 may be configured to verify that the digital currency unit conveyed to the merchant apparatus 104 has been validated by the actual trusted certificate authority 108 and not an imposter.

In some embodiments wherein the transaction manager 148 is configured to send a received unit(s) of digital currency to the certificate authority 108 to verify validity of the received unit(s) of digital currency and/or an identity of the certificate authority 108, the transaction manager 148 may be configured to include a "count" parameter in a message sent to the certificate authority 108 that includes the unit(s) of digital currency to be verified. The count parameter may be set to a value denoting a count of the number of units of digital currency included in the message for verification. The currency verifier 160 may then verify the received unit(s) of digital currency and respond to the merchant apparatus 106 with a message including a count parameter indicating the number of units of digital currency verified as being valid. Accordingly, if the transaction manager 148 receives a response message indicating one or more units of digital currency were counterfeit (e.g., if the count parameter value in the response was less than the value of the count parameter in the message sent to the certificate authority 108), the transaction manager 148 may be configured to determine that one or more units of digital currency were not valid and take appropriate action, such as by notifying the consumer, cancelling the transaction, and/or the like.

If the unit of digital currency and/or the message conveying the unit of digital currency comprises usage step information, the currency verifier 160 may determine whether a correlation exists between the received usage step information and usage step information stored in the memory 152 in association with the serial number for the unit of digital currency. For example, the currency verifier 160 may determine whether the identity of the last recipient/conveyee of the unit of digital currency as indicated in the most recent usage step stored in the usage history for the unit of digital currency in the memory 152 matches the identity of the conveyor (e.g., the consumer and/or consumer device 102) in the current transaction. If the currency verifier 160 determines that a correlation exists between the received usage step information and stored usage step information, the currency verifier 160 may validate the unit of digital currency and may update the stored usage step information to include the most recent usage step information (e.g., a transaction conveying the unit of digital currency from the consumer device 102 to the merchant apparatus 106, a timestamp for the time of the transaction, and/or the like). The currency verifier may then send the validated unit of digital currency to the merchant apparatus 106.

If, on the other hand, the currency verifier 160 determines that a unit of digital currency is not valid, the currency verifier 160 may remove the potential counterfeit digital currency unit from circulation. The currency verifier 160 may further notify the merchant apparatus 106 and/or consumer device 102 that the unit of digital currency was determined to be invalid so that the parties may take appropriate action with respect to the transaction, such as by cancelling the transaction or providing another form of payment. The currency verifier 160 may additionally or

alternatively alert appropriate authorities, such as the police and/or the currency management apparatus 104 of the potential counterfeit unit of digital currency.

Once the transaction manager 148 has received sufficient valid payment (e.g., a sufficient sum of valid units of digital currency) for the transaction, the transaction manager 148 may notify the merchant that the consumer has fulfilled payment terms for the transaction. If a larger sum of digital currency units than the price of the transaction has been conveyed to the merchant apparatus 106, the transaction manager 148 may take steps to refund the consumer the difference, such as by conveying one or more units of digital currency to the consumer device 102 to refund the difference and/or notifying the merchant to refund the consumer the difference. The merchant may then provide the good(s) and/or service(s) transacted for.

When conveying the one or more units of digital currency to the consumer device 102, such as for change or a refund for a transaction between the consumer device 102 and merchant apparatus 106, it will be appreciated that the transaction manager 148 may be configured to implement any one or more of the methods by which the currency wallet manager 128 may be configured to convey digital currency to the merchant apparatus 106. In this regard, for example, the transaction manager 148 may be configured to send the conveyed unit(s) of digital currency to the consumer device 102 and/or may be configured to send a message conveying the unit(s) of digital currency to the certificate authority 108 as an intermediary so that the currency verifier 160 may verify the validity of conveyed unit(s) of digital currency prior to forwarding to the conveyee consumer device 102. When receiving digital currency conveyed to the consumer device 102 by the merchant apparatus 106 from the certificate authority 108, the currency wallet manager 128 and currency verifier 160 may be further configured to implement a PKI enabled handshaking as described above in connection with the transaction manager 148 in order to prevent a party from mimicking the certificate authority 108.

Flow Charts According to Exemplary Embodiments of the Invention

FIG. 7 illustrates a flowchart according to an exemplary method for using digital currency according to an exemplary embodiment of the invention. The method may include the currency wallet manager 128 establishing an identity of the consumer, which may include establishing the identity of the consumer device 102 used by the consumer, to the currency management apparatus 104, at operation 700. The currency wallet manager 128 may establish the identity by sending a message to the currency management apparatus 104 including a digital signature that may be verified by the currency manager 138 to establish the consumer's identity based at least in part upon a public key infrastructure. The currency wallet manager 128 may further request one or more units of digital currency, at operation 710. Operation 720 may comprise the currency wallet manager 128 receiving one or more units of digital currency issued by the currency management apparatus 104. The currency wallet manager 128 may then store the received units of digital currency in a digital currency wallet, such as in memory 122, at operation 730. Operation 740 may comprise the currency wallet manager 128 entering into a transaction agreement with a merchant, such as in response to consumer interaction with the user interface 126 and/or a transaction

agreement received from a merchant apparatus 106. The currency wallet manager 128 may then access unit(s) of digital currency from the digital currency wallet, at operation 750. Operation 760 may comprise the currency wallet manager 128 conveying the accessed unit(s) of digital currency to the merchant (e.g., to the merchant apparatus 106) as at least partial payment for the
5 transaction. When implementing a counterfeit protection scheme, operation 760 may comprise the currency wallet manager 128 sending the accessed unit(s) of digital currency to the certificate authority 108, which may validate the unit(s) of digital currency prior to forwarding to the merchant apparatus 106.

FIG. 8 illustrates a flowchart according to an exemplary method for implementing a
10 counterfeit protection scheme according to an exemplary embodiment of the invention. The method may include the currency verifier 160 registering serial number(s) for generated and/or issued unit(s) of digital currency, at operation 800. In this regard, the currency verifier 160 may register one or more serial numbers allocated to a currency management apparatus 104 and/or may register serial numbers for generated digital currency units sent to the certificate authority 108
15 for registration by the currency management apparatus 104. Operation 810 may comprise the currency verifier 160 storing verification information associated with the serial number(s) in the memory 152. This verification information may comprise, for example, usage step information or a random code. If the verification information comprises a random code, operation 810 may further comprise the currency verifier 160 generating a random code for a serial number and adding the
20 random code to the respective digital currency unit. If the certificate authority had been forwarded unit(s) of digital currency for registration by the currency management apparatus 104, the currency verifier may return the unit(s) of digital currency to the currency management apparatus 104 following registration.

Operation 820 may comprise the currency verifier 160 receiving a unit of digital currency
25 conveyed in a transaction and verification information associated with the unit of digital currency. The currency verifier 160 may then determine the serial number of the received digital currency unit, at operation 830. Operation 840 may then comprise the currency verifier 160 accessing stored verification information associated with the determined serial number from the memory 152. The currency verifier 160 may then determine whether a correlation exists between the received
30 verification information and the stored verification information. If a correlation does exist, the currency verifier 160 may update the stored verification information and/or the verification information of the digital currency unit, at operation 860. In this regard, the currency verifier 160 may store a new usage step reflecting the current transaction to the memory 152 in association with the serial number for the digital currency unit and/or may generate a new random code for use
35 in a subsequent transaction and replace the existing random code. Operation 870 may then comprise the currency verifier 160 validating the unit of digital currency and forwarding the digital currency unit to the conveyee in the transaction (e.g., a merchant apparatus 106). If, on the other hand, a correlation does not exist the currency verifier 160 may invalidate the unit of digital currency and take appropriate action (e.g., notify the consumer device 102 conveying the unit of

digital currency, notify the merchant apparatus 106 designated as conveyee, notify the police, and/or the like).

FIG. 9 illustrates a flowchart according to an exemplary method for generating and issuing digital currency according to an exemplary embodiment of the invention. The method may include the currency manager 138 generating a unit of digital currency, at operation 900. The currency manager 138 may then receive a message sent by a consumer device 102 associated with a consumer, at operation 910. The message may comprise a digital signature generated using a private key associated with the consumer (e.g., the private key of the consumer device 102). Operation 920 may comprise the currency manager 138 establishing an identity of one or more of a consumer or a consumer device 102 associated with the consumer based at least in part upon the digital signature in accordance with a public key infrastructure. Operation 910 and/or operation 920 may further comprise the currency manager 138 receiving a request for one or more units of digital currency sent by the consumer device 102. Operation 930 may then comprise the currency manager 138 issuing the unit of digital currency to the consumer. In this regard, the currency manager 138 may either send the unit of digital currency to the consumer device 102 or may send the unit of digital currency to the certificate authority 108 to enable the certificate authority 108 to store verification information to be used for verification of the unit of digital currency when subsequently used in a transaction. The certificate authority 108 may then send the unit of digital currency to the consumer device 102.

FIG. 10 illustrates a flowchart according to an exemplary method for receiving digital currency as payment for a transaction according to an exemplary embodiment of the invention. The method may include the transaction manager 148 entering into a transaction with a consumer device 102, at operation 1000. In this regard, the transaction manager 148 may enter into a transaction with a consumer device 102 at the behest of a consumer associated with the consumer device 102. Operation 1010 may then comprise the transaction manager 148 receiving a unit of digital currency conveyed to the merchant apparatus 106 by the consumer device 102 as at least partial payment for the transaction. In this regard, operation 1010 may comprise the transaction manager 148 receiving a unit of digital currency sent by the consumer device 102. Alternatively, operation 1010 may comprise the transaction manager 148 receiving a unit of digital sent by the certificate authority 108, to which the consumer device 102. In this regard, the consumer device 102 may have sent the unit of digital currency conveyed to the merchant apparatus 106 to the certificate authority 108 to enable the certificate authority 108 to verify validity of the unit of digital currency in accordance with a counterfeit protection scheme prior to forwarding the unit of digital currency to the merchant apparatus 106. In some embodiments, the transaction manager 148 may further implement a public key infrastructure enabled handshaking with the certificate authority 108 to establish validity of the unit of digital currency and/or to verify authenticity of the certificate authority 108.

FIGs. 7-10 are flowcharts of a system, method, and computer program product according to exemplary embodiments of the invention. It will be understood that each block or step of the flowcharts, and combinations of blocks in the flowcharts, may be implemented by various means,

such as hardware and/or a computer program product comprising one or more computer-readable mediums having computer readable program instructions stored thereon. For example, one or more of the procedures described herein may be embodied by computer program instructions of a computer program product. In this regard, the computer program product(s) which embody the
5 procedures described herein may be stored by one or more memory devices of a mobile terminal, server, or other computing device and executed by a processor in the computing device. In some embodiments, the computer program instructions comprising the computer program product(s) which embody the procedures described above may be stored by memory devices of a plurality of computing devices. As will be appreciated, any such computer program product may be loaded
10 onto a computer or other programmable apparatus to produce a machine, such that the computer program product including the instructions which execute on the computer or other programmable apparatus creates means for implementing the functions specified in the flowchart block(s) or step(s). Further, the computer program product may comprise one or more computer-readable memories on which the computer program instructions may be stored such that the one or more
15 computer-readable memories can direct a computer or other programmable apparatus to function in a particular manner, such that the computer program product comprises an article of manufacture which implements the function specified in the flowchart block(s) or step(s). The computer program instructions of one or more computer program products may also be loaded onto a computer or other programmable apparatus to cause a series of operational steps to be
20 performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block(s) or step(s).

Accordingly, blocks or steps of the flowcharts support combinations of means for
25 performing the specified functions and combinations of steps for performing the specified functions. It will also be understood that one or more blocks or steps of the flowcharts, and combinations of blocks or steps in the flowcharts, may be implemented by special purpose hardware-based computer systems which perform the specified functions or steps, or combinations of special purpose hardware and computer program product(s).

The above described functions may be carried out in many ways. For example, any
30 suitable means for carrying out each of the functions described above may be employed to carry out embodiments of the invention. In one embodiment, a suitably configured processor may provide all or a portion of the elements of the invention. In another embodiment, all or a portion of the elements of the invention may be configured by and operate under control of a computer
35 program product. The computer program product for performing the methods of embodiments of the invention includes a computer-readable storage medium, such as the non-volatile storage medium, and computer-readable program code portions, such as a series of computer instructions, embodied in the computer-readable storage medium.

Conclusion

As such, then, some embodiments of the invention provide several advantages to computing devices, computing device users, merchants, and financial service providers. Embodiments of the invention provide for the generation of digital currency that is verifiable using a public key infrastructure. Embodiments of the invention further facilitate transactions using digital currency. Some embodiments provide counterfeit protection schemes. Use of a centralized trust facilitator, such as a certificate authority, by embodiments of the invention further provides for scaling in that multiple currency management apparatuses managed by multiple financial institutions, multiple consumers, multiple consumer devices, multiple merchants, and/or multiple merchant apparatuses can be added to a system for facilitating generation and exchange of digital currency.

Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these inventions pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the embodiments of the invention are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Moreover, although the foregoing descriptions and the associated drawings describe exemplary embodiments in the context of certain exemplary combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative embodiments without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

WHAT IS CLAIMED IS:

1. A method comprising:
entering into a transaction with a merchant;
5 accessing a unit of digital currency from a digital currency wallet, wherein the unit of digital currency is verifiable based at least in part upon a public key infrastructure; and
conveying the unit of digital currency to the merchant as at least partial payment for the transaction.
- 10 2. The method of Claim 1, further comprising:
establishing an identity of a consumer to a currency management apparatus by sending a message to the currency management apparatus, the message comprising a signature generated using a private key associated with the consumer, wherein the identity of the consumer is verifiable based at least in part upon the signature in accordance with the public key infrastructure;
15 receiving the unit of digital currency issued by the currency management apparatus; and
storing the received unit of digital currency in the digital currency wallet prior to entering into the transaction with the merchant.
- 20 3. The method of Claim 2, further comprising verifying validity of the received unit of digital currency based at least in part upon the public key infrastructure.
4. The method of Claim 1, wherein the unit of digital currency is verified for a predefined value through a digital signature generated by a currency management apparatus responsible for issuing digital currency using a private key of the currency management apparatus,
25 and wherein validity of the unit of digital currency is verifiable based at least in part upon the digital signature in accordance with the public key infrastructure.
5. The method of Claim 1, wherein the unit of digital currency comprises a unique serial number assigned by a currency management apparatus responsible for issuing digital
30 currency.
6. The method of Claim 5, wherein conveying the unit of digital currency to the merchant as at least partial payment for the transaction comprises sending the unit of digital currency to a certificate authority along with verification information enabling the certificate
35 authority to verify validity of the unit of digital currency based at least in part upon a determination of whether a correlation exists between the verification information and information stored by the certificate authority in association the unique serial number.
7. The method of Claim 6, wherein the verification information comprises a usage
40 step or a random code assigned to the unit of digital currency for use in a single transaction.

8. A computer program product comprising at least one computer-readable storage medium having computer-readable program instructions stored therein, the computer-readable program instructions comprising:

- 5 a program instruction for entering into a transaction with a merchant;
a program instruction for accessing a unit of digital currency from a digital currency wallet, wherein the unit of digital currency is verifiable based at least in part upon a public key infrastructure; and
a program instruction for conveying the unit of digital currency to the merchant as at least
10 partial payment for the transaction.

9. The computer program product of Claim 8, further comprising:

- a program instruction for establishing an identity of a consumer to a currency management apparatus by causing a message to be sent to the currency management apparatus, the message
15 comprising a signature generated using a private key associated with the consumer, wherein the identity of the consumer is verifiable based at least in part upon the signature in accordance with the public key infrastructure;
a program instruction for causing the unit of digital currency issued by the currency management apparatus to be received; and
20 a program instruction for storing the received unit of digital currency in the digital currency wallet prior to entering into the transaction with the merchant..

10. The computer program product of Claim 9, further comprising verifying validity of the received unit of digital currency based at least in part upon the public key infrastructure.

25

11. The computer program product of Claim 8, wherein the unit of digital currency is verified for a predefined value through a digital signature generated by a currency management apparatus responsible for issuing digital currency using a private key of the currency management apparatus, and wherein validity of the unit of digital currency is verifiable based at least in part
30 upon the digital signature in accordance with the public key infrastructure.

12. The computer program product of Claim 8, wherein the unit of digital currency comprises a unique serial number assigned by a currency management apparatus responsible for issuing digital currency.

35

13. The computer program product of Claim 12, wherein conveying the unit of digital currency to the merchant as at least partial payment for the transaction comprises causing the unit of digital currency to be sent to a certificate authority along with verification information enabling the certificate authority to verify validity of the unit of digital currency based at least in part upon a

determination of whether a correlation exists between the verification information and information stored by the certificate authority in association the unique serial number.

14. The computer program product of Claim 13, wherein the verification information
5 comprises a usage step or a random code assigned to the unit of digital currency for use in a single transaction.

15. An apparatus comprising a processor and a memory storing instructions that when
executed by the processor cause the apparatus to at least:
10 enter into a transaction with a merchant;
access a unit of digital currency from a digital currency wallet, wherein the unit of digital
currency is verifiable based at least in part upon a public key infrastructure; and
convey the unit of digital currency to the merchant as at least partial payment for the
transaction.

16. The apparatus of Claim 15, wherein the instructions when executed by the processor
further cause the apparatus to:
establish an identity of a consumer to a currency management apparatus by sending a
message to the currency management apparatus, the message comprising a signature generated
20 using a private key associated with the consumer, wherein the identity of the consumer is verifiable
based at least in part upon the signature in accordance with the public key infrastructure;
receive the unit of digital currency issued by the currency management apparatus; and
store the received unit of digital currency in the digital currency wallet prior to entering into
the transaction with the merchant.

17. The apparatus of Claim 16, wherein the instructions when executed by the
processor further cause the apparatus to verify validity of the received unit of digital currency
based at least in part upon the public key infrastructure.

18. The apparatus of Claim 15, wherein the unit of digital currency is verified for a
predefined value through a digital signature generated by a currency management apparatus
responsible for issuing digital currency using a private key of the currency management apparatus,
and wherein validity of the unit of digital currency is verifiable based at least in part upon the digital
signature in accordance with the public key infrastructure.

19. The apparatus of Claim 15, wherein the unit of digital currency comprises a unique
serial number assigned by a currency management apparatus responsible for issuing digital
currency.

20. The apparatus of Claim 19, wherein the instructions when executed cause the apparatus to convey the unit of digital currency to the merchant as at least partial payment for the transaction by sending the unit of digital currency to a certificate authority along with verification information enabling the certificate authority to verify validity of the unit of digital currency based at least in part upon a determination of whether a correlation exists between the verification
5 information and information stored by the certificate authority in association the unique serial number.

21. The apparatus of Claim 20, wherein the verification information comprises a usage
10 step or a random code assigned to the unit of digital currency for use in a single transaction.

22. An apparatus comprising:
means for entering into a transaction with a merchant;
means for accessing a unit of digital currency from a digital currency wallet, wherein the
15 unit of digital currency is verifiable based at least in part upon a public key infrastructure; and
means for conveying the unit of digital currency to the merchant as at least partial payment for the transaction.

23. An apparatus comprising a processor and a memory storing instructions that when
20 executed by the processor cause the apparatus to at least:
receive a unit of digital currency conveyed in a transaction and associated verification information, wherein the received unit of digital currency includes a serial number, and wherein the unit of digital currency is verifiable based at least in part upon a public key infrastructure;
determine whether a correlation exists between the received verification information and
25 stored verification information associated with the serial number; and
verify validity of the unit of digital currency based at least in part upon the determination of whether a correlation exists.

24. The apparatus of Claim 23, wherein the instructions when executed by the
30 processor cause the apparatus to verify that the unit of digital currency is valid and send the received unit of digital currency to a merchant apparatus to which the unit of digital currency is conveyed in the transaction when a correlation is determined to exist between the received verification information and the stored verification information.

25. The apparatus of Claim 24, wherein the received verification information
35 comprises a random code and the instructions when executed by the processor cause the apparatus to determine whether a correlation exists by determining whether the received random code matches a stored random code associated with the serial number.

26. The apparatus of Claim 25, wherein the instructions when executed by the processor further cause the apparatus to implement a public key infrastructure enabled handshaking with the merchant apparatus to establish validity of the unit of digital currency to the merchant apparatus.

5

27. The apparatus of Claim 25, wherein when the received random code matches the stored random code, the instructions when executed by the processor further cause the apparatus to:

generate a new random code;

10

replace the received random code with the new random code prior to sending the unit of digital currency to the merchant apparatus such that the unit of digital currency sent to the merchant apparatus includes the new random code; and

store the new random code in association with the serial number for use in a future validation of the unit of digital currency.

15

28. An apparatus comprising a processor and a memory storing instructions that when executed by the processor cause the apparatus to at least:

generate a unit of digital currency, wherein the unit of digital currency is verifiable based at least in part upon a public key infrastructure;

20

receive a message sent by a consumer device associated with a consumer, wherein the message comprises a digital signature generated by the consumer device;

establish an identity of one or more of the consumer or the consumer device based at least in part upon the digital signature in accordance with the public key infrastructure; and issue the unit of digital currency to the consumer.

25

29. The apparatus of Claim 28, wherein the instructions when executed by the processor cause the apparatus to generate the unit of digital currency by generating a unit of digital currency verified for a predefined value and signed with a digital signature, wherein validity of the unit of digital currency is verifiable based at least in part upon the digital signature in accordance with the public key infrastructure.

30

30. The apparatus of Claim 28, wherein the instructions when executed by the processor further cause the apparatus to assign a unique serial number to the unit of digital currency.

35

31. The apparatus of Claim 30, wherein the instructions when executed by the processor further cause the apparatus to send the unit of digital currency to a certificate authority to enable the certificate authority to store verification information to be used for verification of the unit of digital currency when the unit of digital currency is subsequently used in a transaction.

40

32. An apparatus comprising a processor and a memory storing instructions that when executed by the processor cause the apparatus to at least:

enter into a transaction with a consumer device; and

5 receive a unit of digital currency conveyed by the consumer device as at least partial payment for the transaction, wherein the unit of digital currency is verifiable based at least in part upon a public key infrastructure.

33. The apparatus of Claim 32, wherein the unit of digital currency is verified for a predefined value through a digital signature generated by a currency management apparatus
10 responsible for issuing digital currency using a private key of the currency management apparatus, and wherein validity of the unit of digital currency is verifiable based at least in part upon the digital signature in accordance with the public key infrastructure.

34. The apparatus of Claim 33, wherein the unit of digital currency comprises a unique
15 serial number, and wherein the instructions when executed by the processor cause the apparatus to receive the unit of digital currency by receiving the unit of digital currency from a certificate authority after the certificate authority has verified validity of the unit of digital currency based at least in part upon a determination of whether a correlation exists between verification information provided to the certificate authority along with the unit of digital currency by the consumer device
20 and information stored by the certificate authority in association the unique serial number.

35. The apparatus of Claim 34, wherein the instructions when executed by the processor further cause the apparatus to implement a public key infrastructure enabled
handshaking with the certificate authority to establish validity of the unit of digital currency and
25 verify authenticity of the certificate authority.

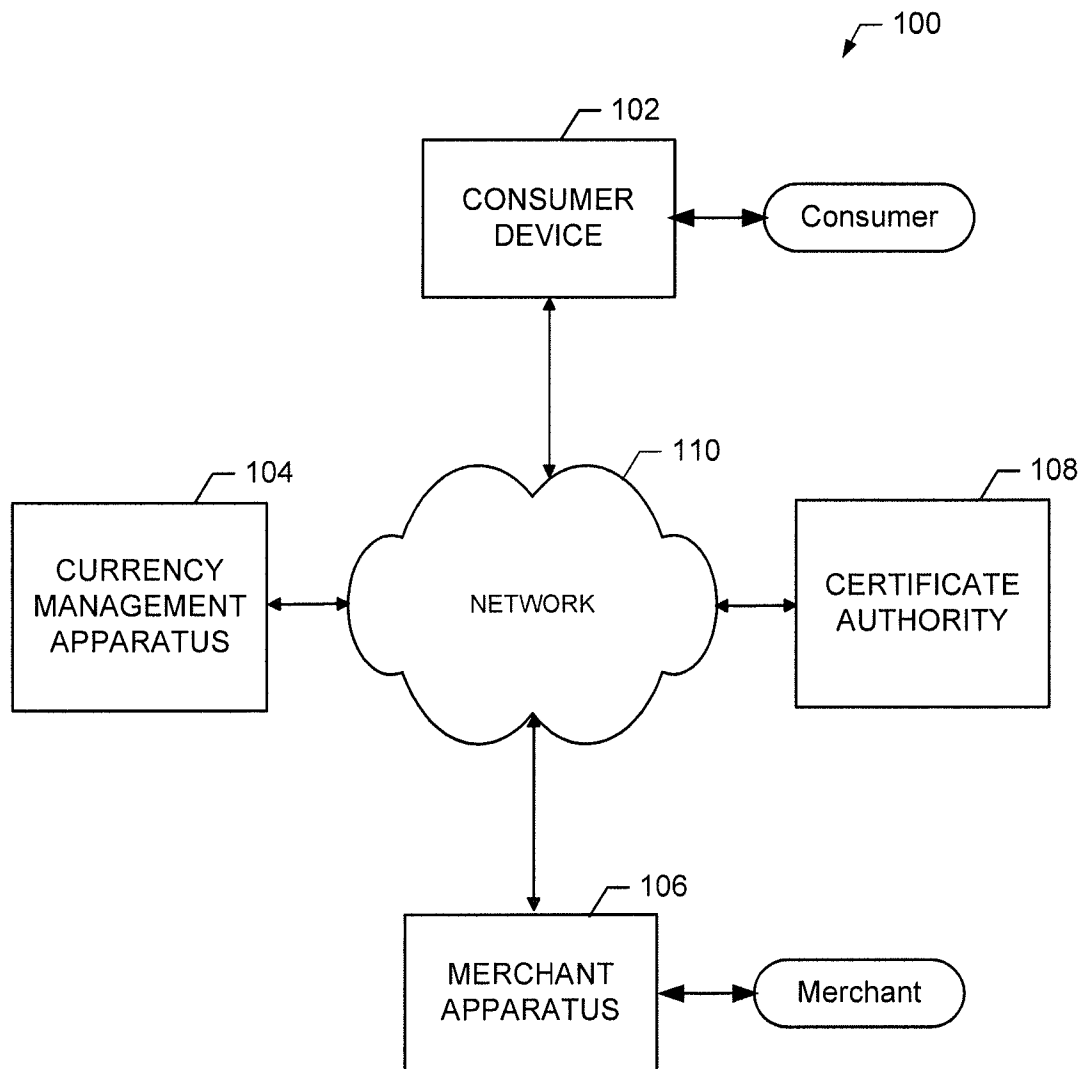
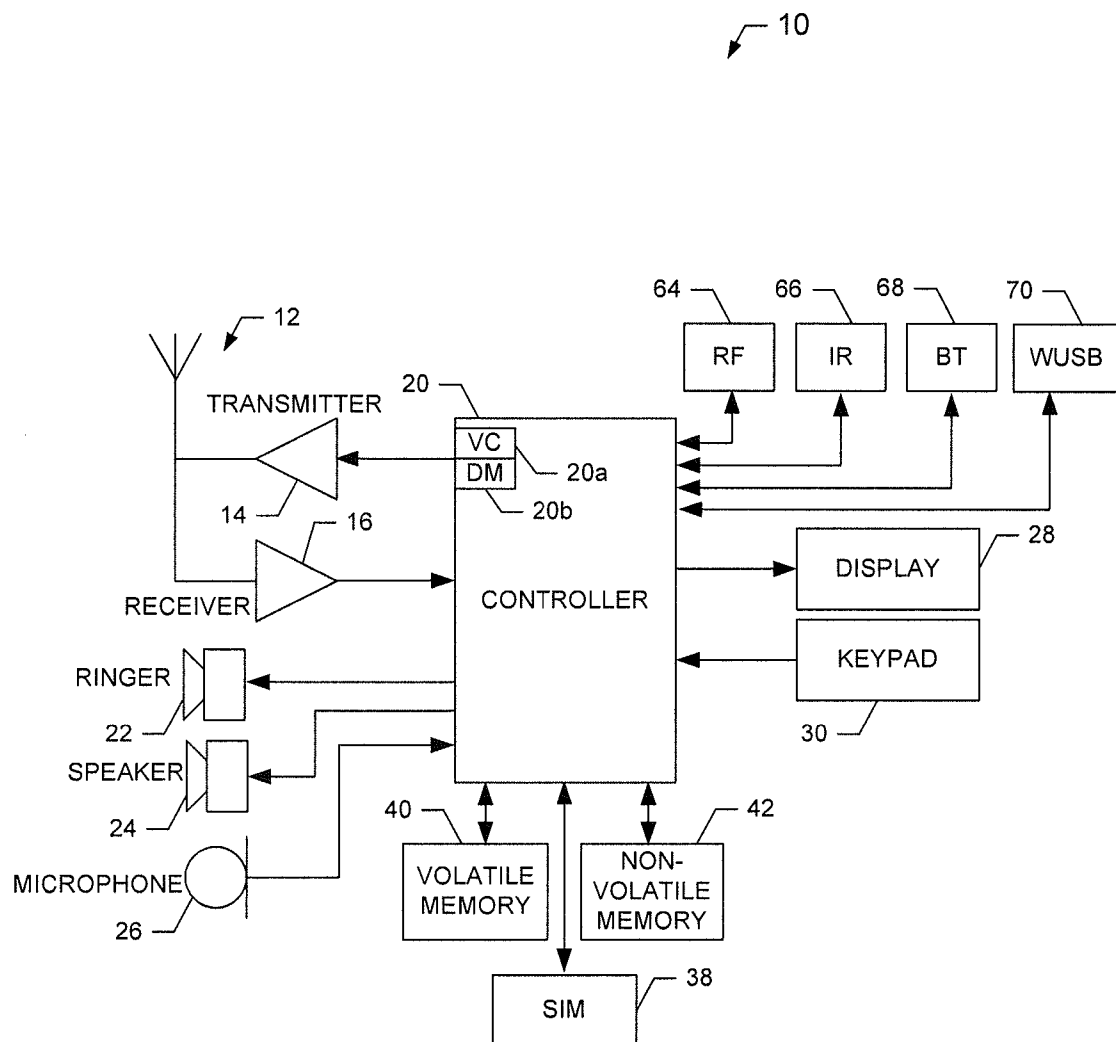


FIG. 1.

**FIG. 2.**

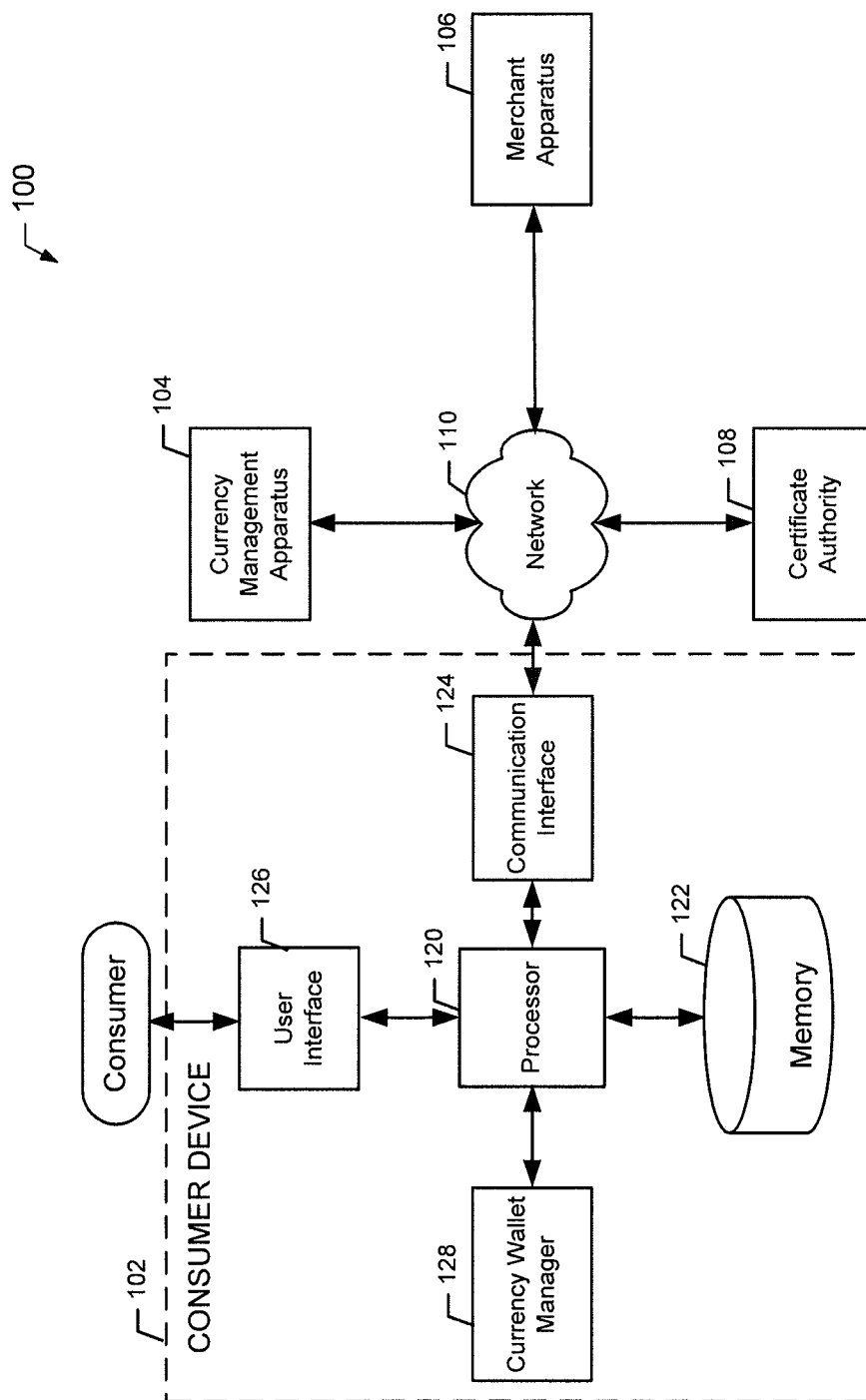


FIG. 3.

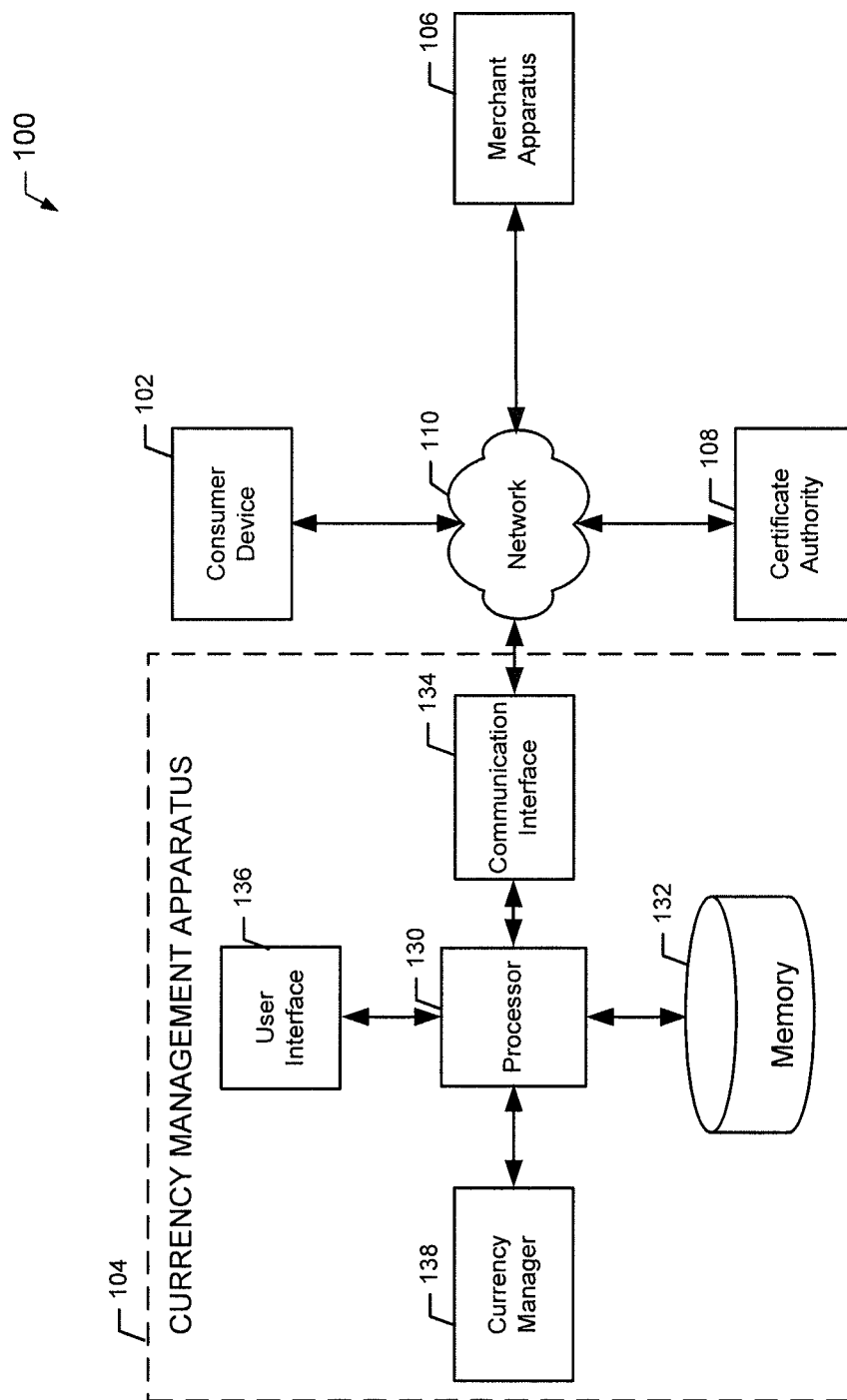


FIG. 4.

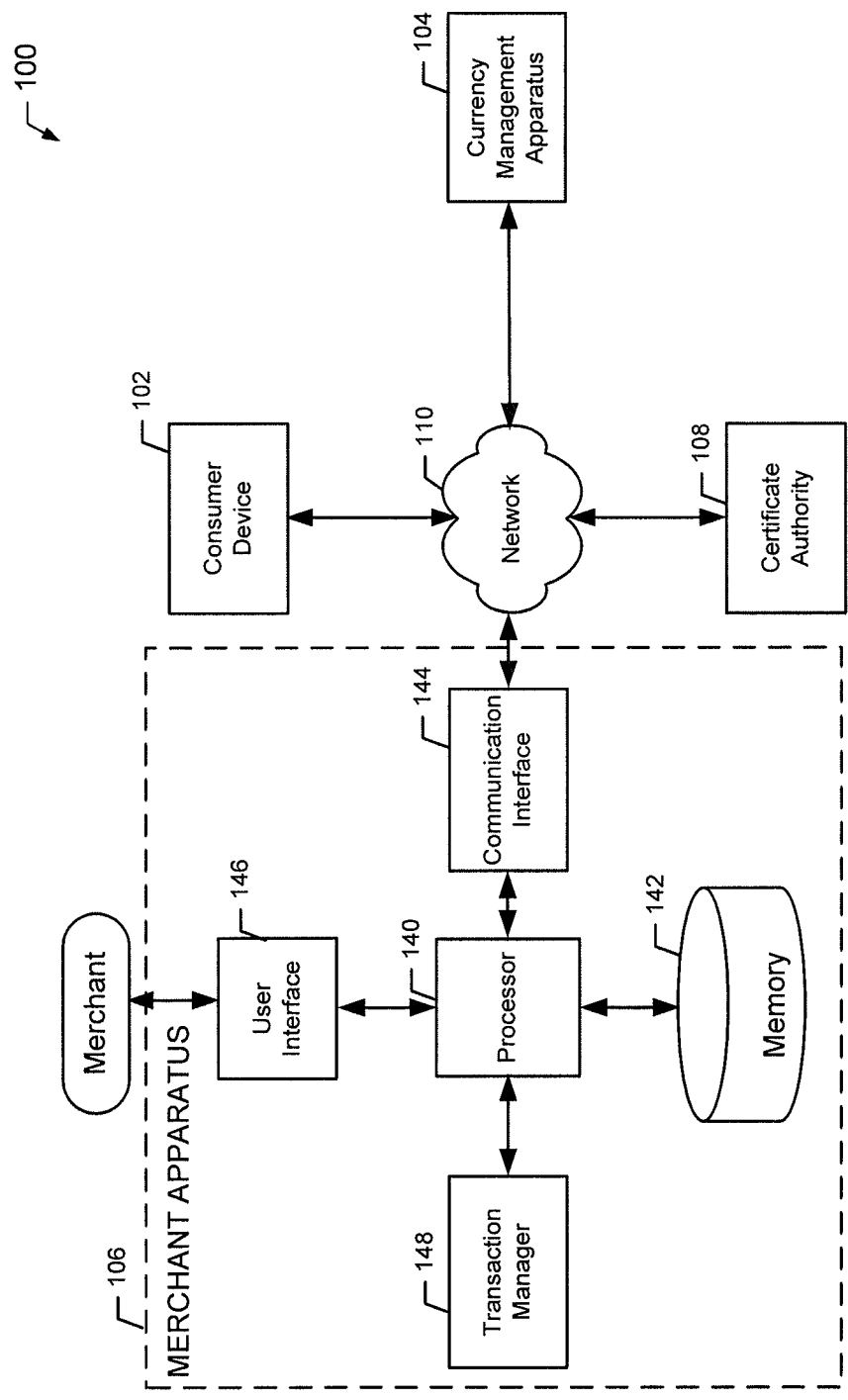


FIG. 5.

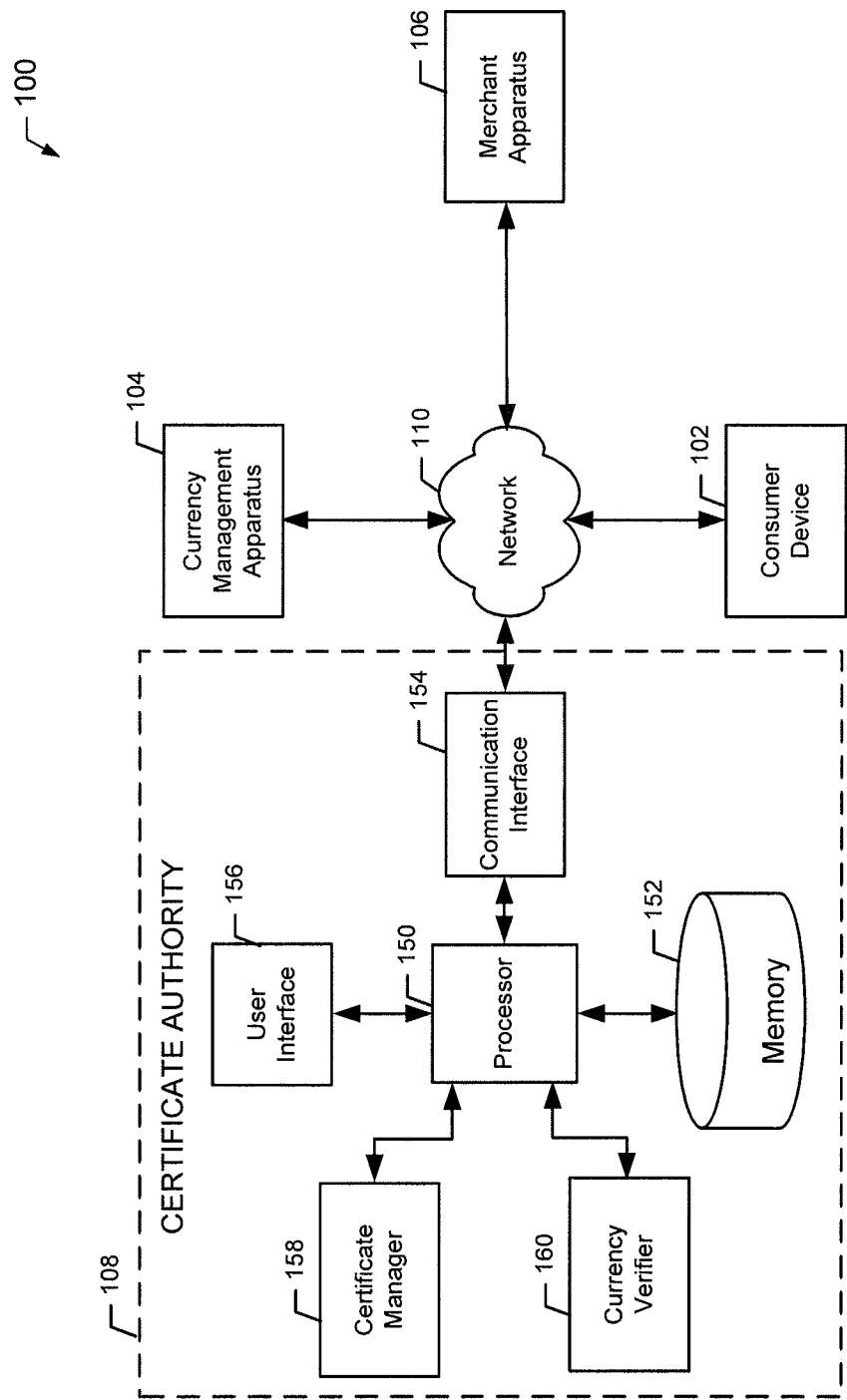


FIG. 6.

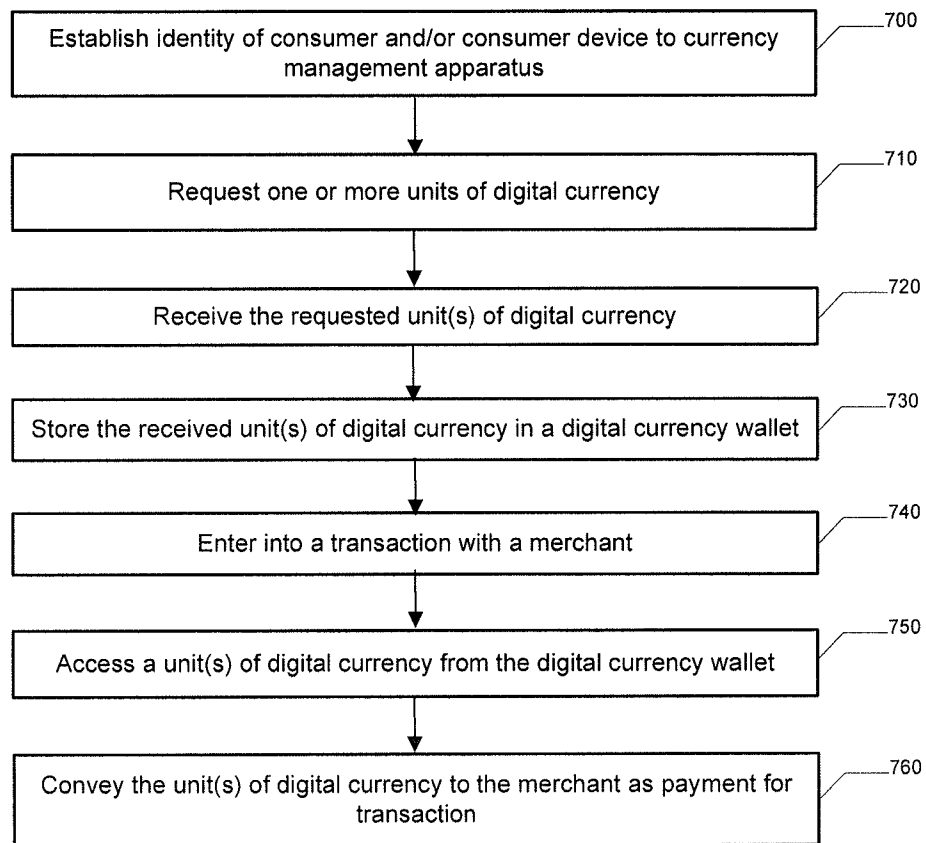
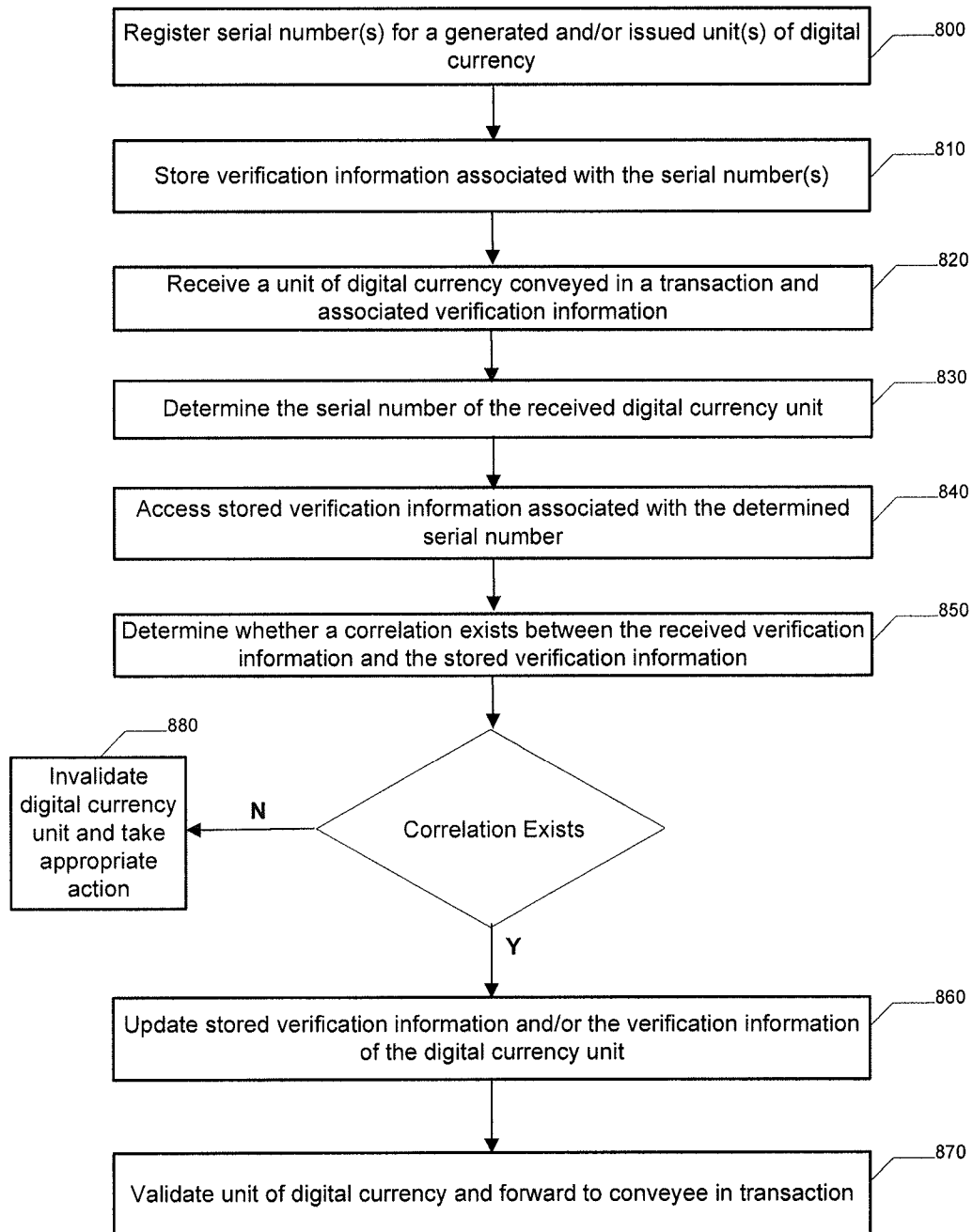


FIG. 7.

**FIG. 8.**

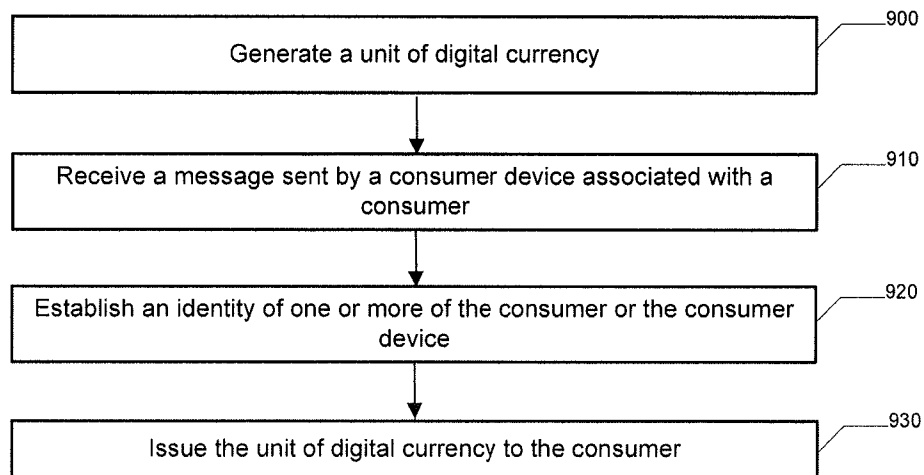


FIG. 9.

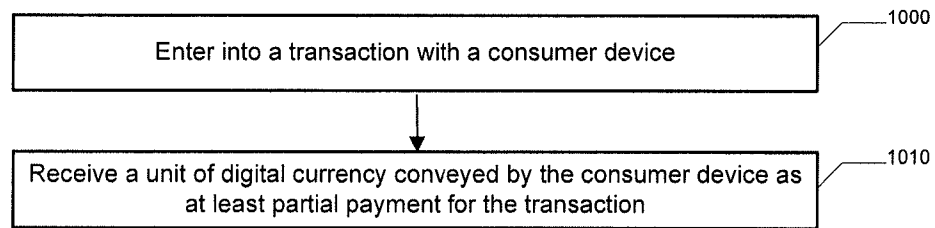


FIG. 10.

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/051252

A. CLASSIFICATION OF SUBJECT MATTER

INV. G07F7/08 G06Q30/00 G06Q20/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G07F G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/15100 A1 (ELUV HOLDINGS LTD [IL]; LUZZATTO KFIR [IL]; LUZZATTO ESTHER [IL]) 1 March 2001 (2001-03-01)	1,5-8, 12-15, 19-24,32
Y	abstract page 4, line 6 - page 8, last line figures 1-4	2-4, 9-11, 16-18, 25-31, 33-35
Y	US 2009/048979 A1 (AL-HERZ AHMED IBRAHIM [US] ET AL) 19 February 2009 (2009-02-19) abstract paragraph [0016] - paragraph [0030] claims 23,24,32	2-4, 9-11, 16-18, 25-31, 33-35



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

16 November 2009

Date of mailing of the international search report

27/11/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Mandato, Davide

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2009/051252

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GRIGG I: "The Ricardian contract" ELECTRONIC CONTRACTING, 2004. PROCEEDINGS. FIRST IEEE INTERNATIONAL WORKSHOP ON SAN DIEGO, CA, USA 6 JULY 2004, PISCATAWAY, NJ, USA, IEEE, 1 January 2004 (2004-01-01), pages 25-31, XP010714504 ISBN: 978-0-7695-2184-8 paragraphs [01.3], [02.1], [02.2] paragraph [03.1] - paragraph [03.2] -----	1-35

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2009/051252

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0115100	A1	01-03-2001	AT 333682 T 15-08-2006
		AU 6466800 A 19-03-2001	
		DE 60029455 T2 19-07-2007	
		EP 1212734 A1 12-06-2002	
		US 7590602 B1 15-09-2009	
US 2009048979	A1	19-02-2009	NONE