US 20170053249A1

(19) **United States**

(12) **Patent Application Publication**

Tunnell et al.

(10) **Pub. No.: US 2017/0053249 A1**

(43) **Pub. Date: Feb. 23, 2017**

(54) **ELECTRONIC CRYPTO-CURRENCY MANAGEMENT METHOD AND SYSTEM**

(71) Applicant: **NXT-ID, Inc.**, Shelton, CT (US)

(72) Inventors: **David Tunnell**, Palm Bay, FL (US); **Charles Morgan**, Katy, TX (US)

(21) Appl. No.: **15/225,780**

(22) Filed: **Aug. 1, 2016**

Related U.S. Application Data

(60) Provisional application No. 62/198,817, filed on Jul. 30, 2015.

Publication Classification

(51) **Int. Cl.**

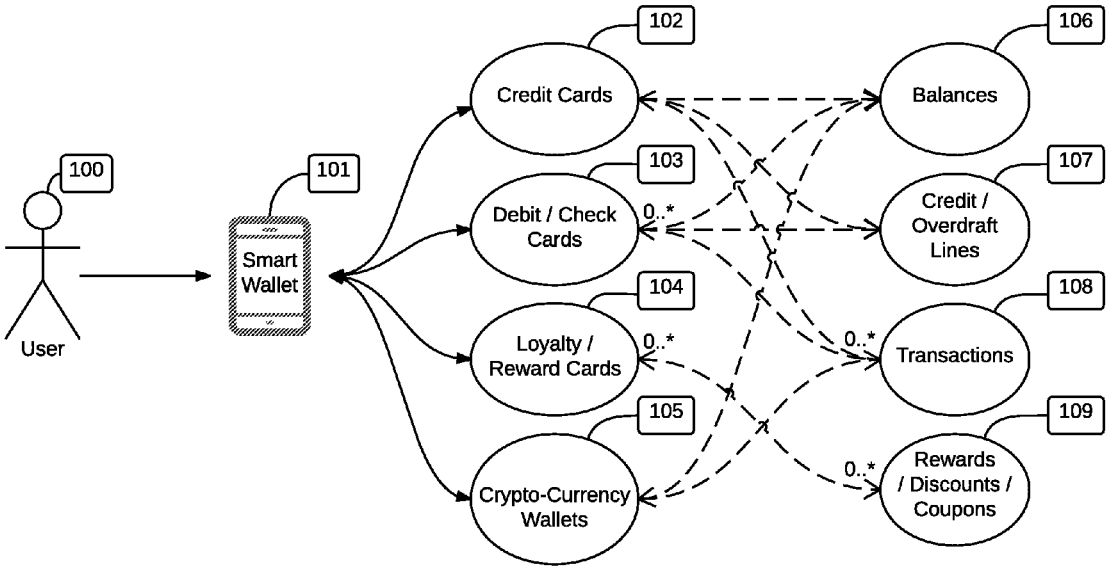
G06Q 20/06	(2006.01)
G06Q 30/02	(2006.01)
G06Q 20/38	(2006.01)

(52) **U.S. Cl.**

CPC ***G06Q 20/065*** (2013.01); ***G06Q 20/382*** (2013.01); ***G06Q 30/0207*** (2013.01)

(57) **ABSTRACT**

Systems, methods and machines related to conducting a crypto-currency transaction. A method comprises creating a full block chain representing a plurality of past crypto-currency transactions, forwarding the full block chain to a first processing component for use in executing a new crypto-currency transaction, the first processing component forwarding an original local block chain to a second processing component, the second processing component executing the transaction and generating an updated local block chain with details related to the transaction, and forwarding the updated local block chain to the first processing component.



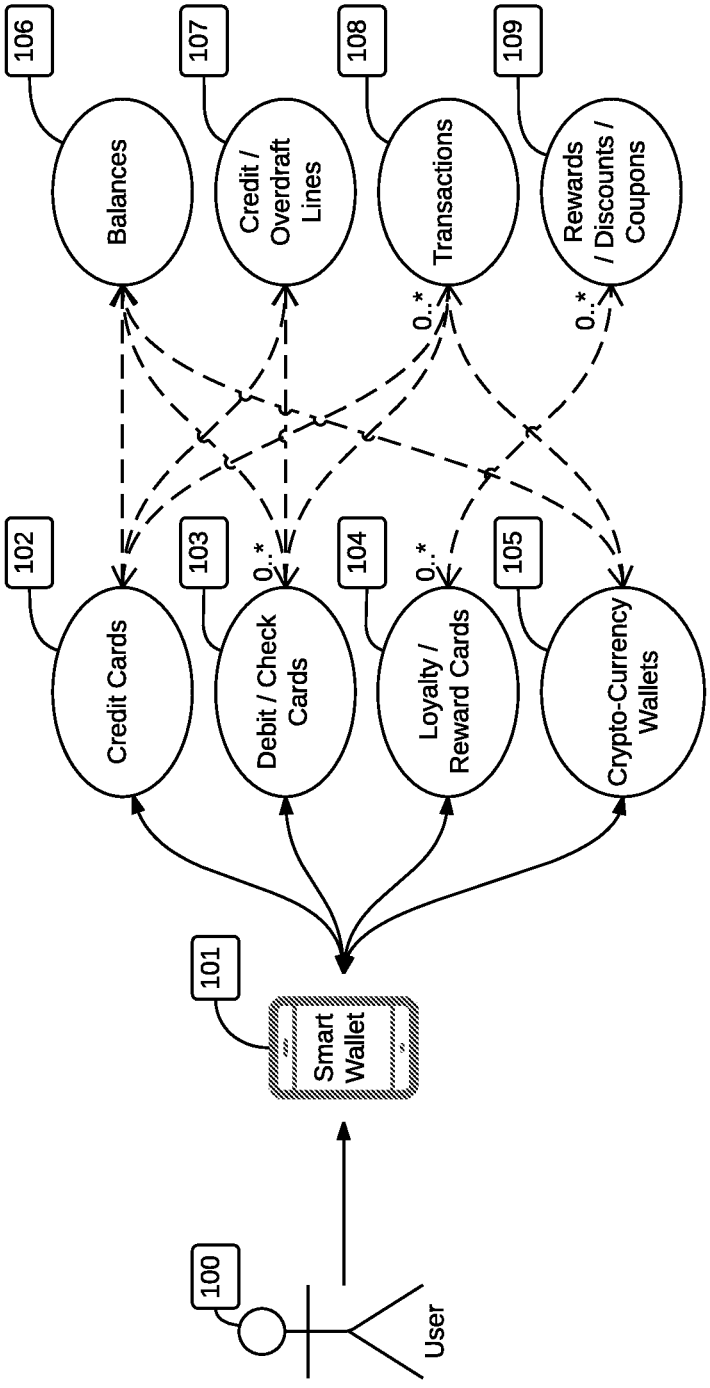

106
107
108
109
Balances
Credit / Overdraft Lines
Transactions
Rewards / Discounts / Coupons
0..*
0..*
102
103
104
105
0..*
0..*
Credit Cards
Debit / Check Cards
Loyalty / Reward Cards
Crypto-Currency Wallets
101
Smart Wallet
100
User

Figure 1

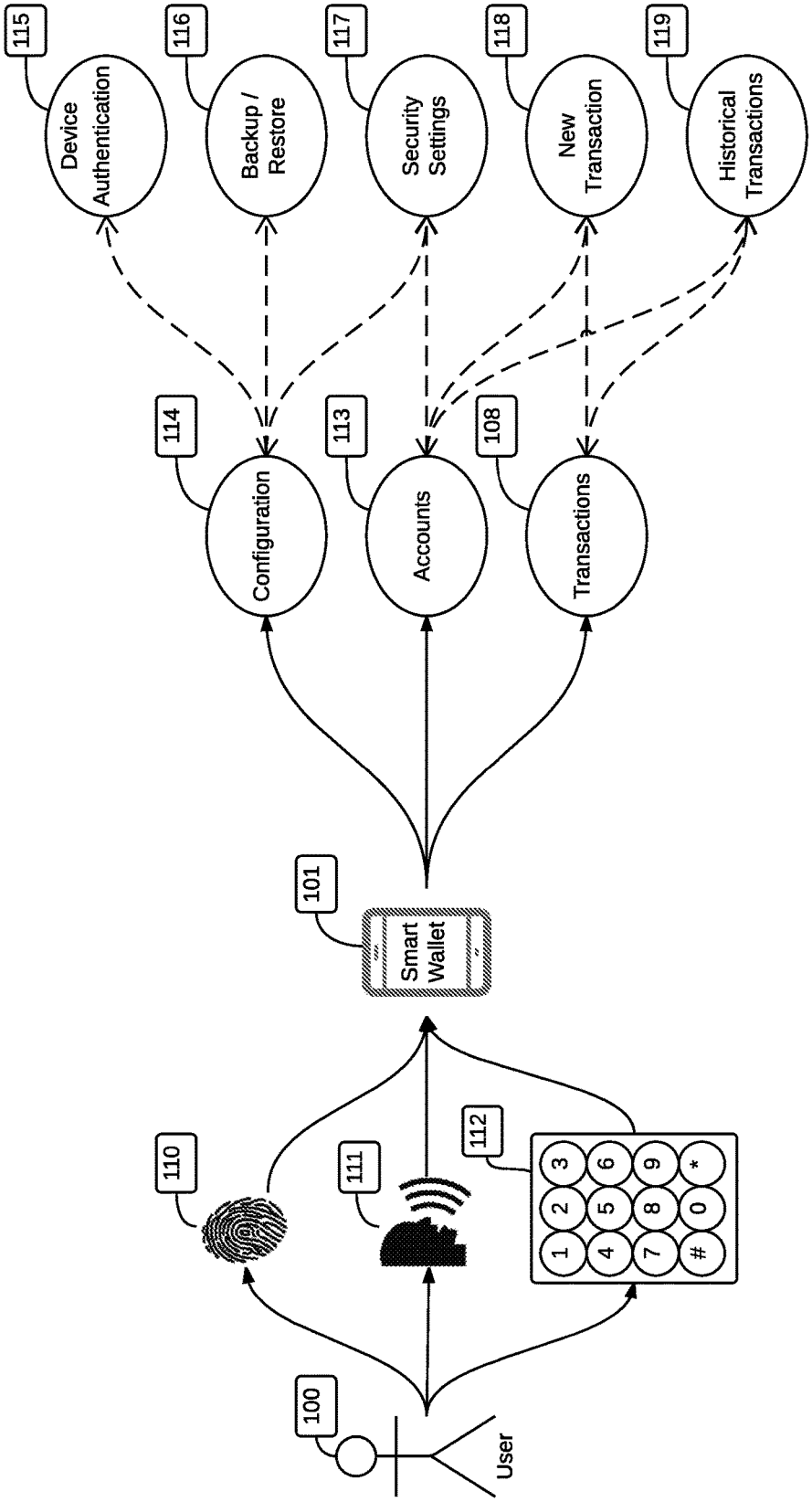

115
Device Authentication
116
Backup / Restore
117
Security Settings
118
New Transaction
119
Historical Transactions
114
Configuration
113
Accounts
108
Transactions
101
Smart Wallet
110
111
112
1 2 3
4 5 6
7 8 9
0 *
100
User

Figure 2

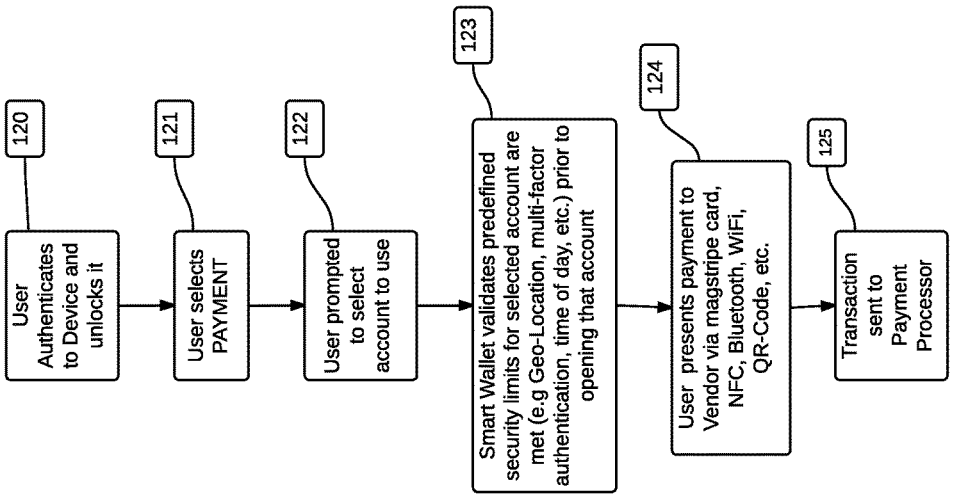

120
User Authenticates to Device and unlocks it
121
User selects PAYMENT
122
User prompted to select account to use
123
Smart Wallet validates predefined security limits for selected account are met (e.g Geo-Location, multi-factor authentication, time of day, etc.) prior to opening that account
124
User presents payment to Vendor via magstripe card, NFC, Bluetooth, WiFi, QR-Code, etc.
125
Transaction sent to Payment Processor

Figure 3

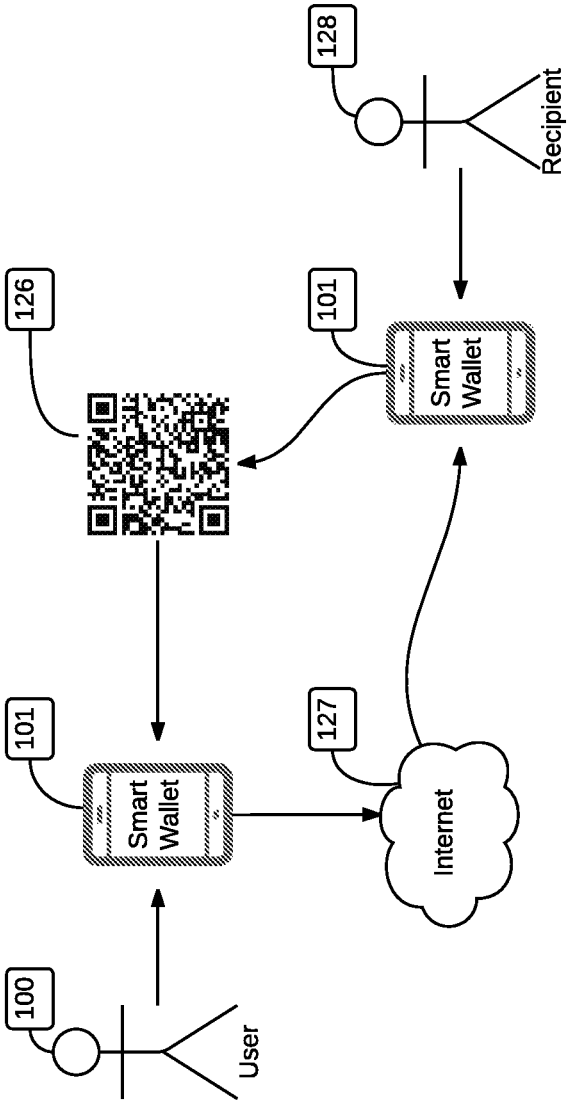

128
Recipient
126
101
Smart Wallet
101
Smart Wallet
127
Internet
100
User

Figure 4

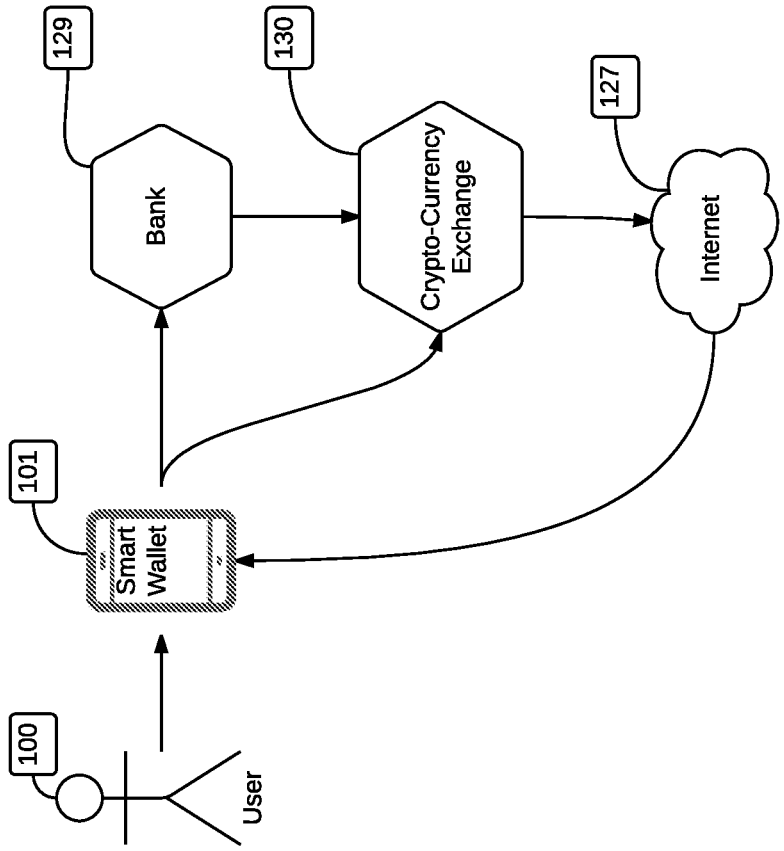

129
130
127
Bank
Crypto-Currency Exchange
Internet
101
Smart Wallet
100
User

Figure 5

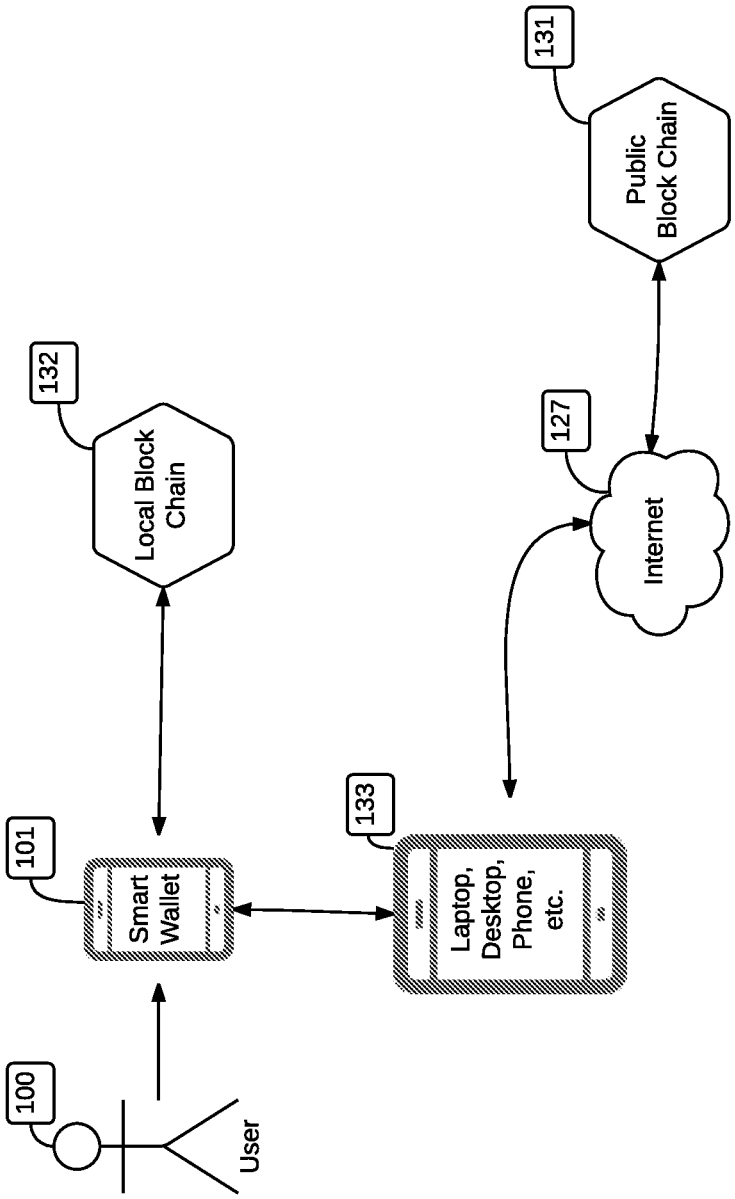

131
Public Block Chain
132
Local Block Chain
127
Internet
101
Smart Wallet
133
Laptop, Desktop, Phone, etc.
100
User

Figure 6

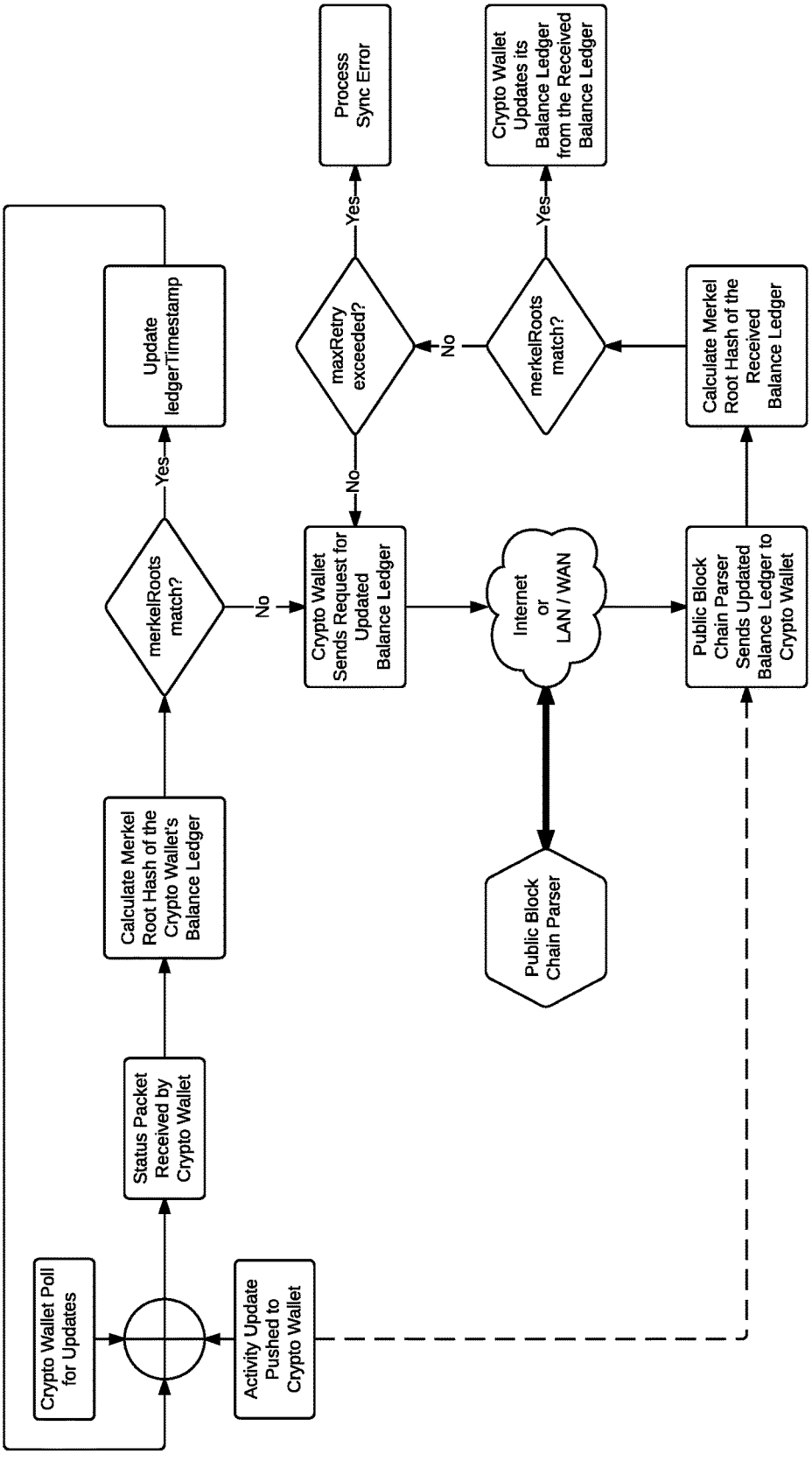

Crypto Wallet Poll for Updates
Activity Update Pushed to Crypto Wallet
Status Packet Received by Crypto Wallet
Calculate Merkel Root Hash of the Crypto Wallet's Balance Ledger
merkelRoots match?
Yes
Update ledgerTimestamp
No
Crypto Wallet Sends Request for Updated Balance Ledger
maxRetry exceeded?
Yes
Process Sync Error
No
merkelRoots match?
Yes
Crypto Wallet Updates its Balance Ledger from the Received Balance Ledger
Calculate Merkel Root Hash of the Received Balance Ledger
Internet or LAN / WAN
Public Block Chain Parser
Public Block Chain Parser Sends Updated Balance Ledger to Crypto Wallet

Figure 7

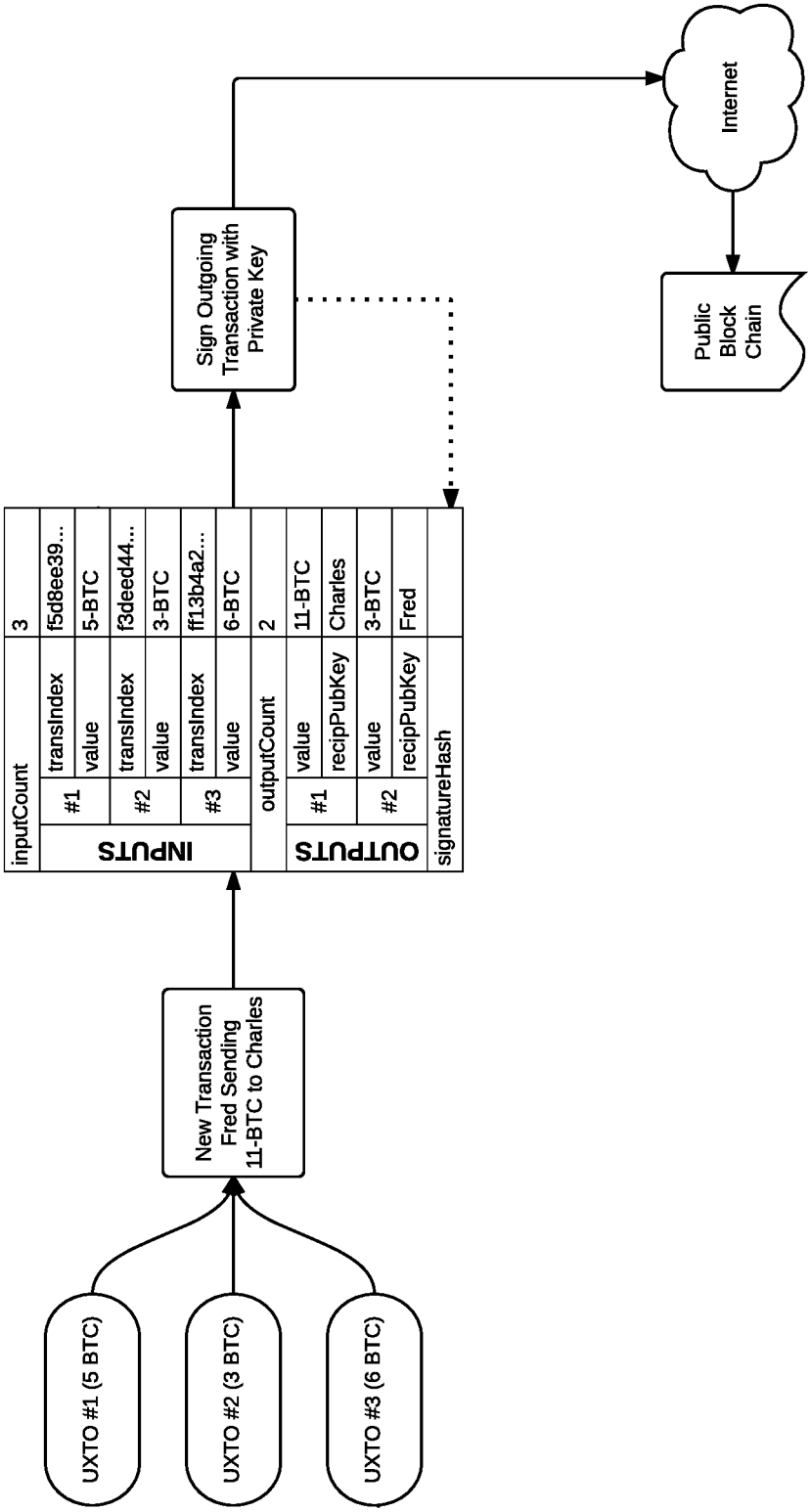

UXTO #1 (5 BTC)
UXTO #2 (3 BTC)
UXTO #3 (6 BTC)
New Transaction Fred Sending 11-BTC to Charles
inputCount 3
INPUTS
#1 transIndex f5d8ee39...
value 5-BTC
#2 transIndex f3deed44...
value 3-BTC
#3 transIndex ff13b4a2...
value 6-BTC
outputCount 2
OUTPUTS
#1 value 11-BTC
recipPubKey Charles
#2 value 3-BTC
recipPubKey Fred
signatureHash
Sign Outgoing Transaction with Private Key
Internet
Public Block Chain

Figure 8

ELECTRONIC CRYPTO-CURRENCY MANAGEMENT METHOD AND SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims the benefit of U.S. provisional patent application filed Jul. 30, 2015 and assigned Application No. 62/198,989, which is incorporated herein in its entirety.

FIELD OF THE INVENTION

[0002] The present invention relates generally to crypto-currencies. More particularly, the present invention relates to a secure mobile device capable of managing crypto-currency accounts, balances and transactions in addition to normal electronic smart wallet functions.

BACKGROUND OF THE INVENTION

[0003] The following background information may present examples of specific aspects of the prior art (e.g., without limitation, approaches, facts, or common wisdom) that, while expected to be helpful to further educate the reader as to additional aspects of the prior art, is not to be construed as limiting the present invention, or any embodiments thereof, to anything stated or implied therein or inferred thereupon.

[0004] A crypto-currency is a virtual currency that uses cryptography for security, making it difficult to counterfeit while allowing for nearly anonymous financial transactions between two parties using private and public keys. Crypto-currencies are not issued by a central authority, theoretically rendering it immune to interference or manipulation. The primary drawbacks are theft of the private key thereby allowing the attacker to assume control of the associated crypto-currency "wallet", and the loss of the private key due to a software or hardware failure thereby rendering the crypto-currency "wallet" orphaned and its contents irretrievable, even by the owner.

[0005] Here are examples of relevant prior art.

[0006] US published patent application 20150026072 entitled "Global World Universal Digital Mobile and Wearable Currency Image Token and Ledger," outlines the basic transfer of value from a sender account to a recipient account using a universal digital currency as a way to circumvent currency exchange costs and banking fees when conducting global commerce.

[0007] Published US Patent application 20150066748 entitled "Systems and Methods for Transferring Value to and Managing User Selected Accounts," allows the general transfer of value between accounts using a consumer device and based on input from the user resulting in various financial systems interacting in such a way as to create an escrow account and effectuating the transfer of value from the funding account, through the escrow account to the receiving account.

[0008] US published patent application number 20140244506 entitled "Dynamic Payment Authorization System and Method" allows a user to locally authenticate their identity to a mobile device and then authorize a financial transaction against their physical account. The mobile device then receives either an approval or disapproved code, which will be compared to the transaction code received by the vendor's POS (point of sale) terminal prior to actually committing the payment transaction.

[0009] Published US patent application 20140244500 entitled "Intermodal money transport system and method related to real-time cash or cash equivalent transfers on electronic devices with an intermodal money application interface that functions as an automated teller machine over one or more open loop financial networks by utilizing a virtual account management system and an intermodal money transport protocol" allows for conducting financial transactions from an electronic device using escrow accounts in conjunction with a specifically defined data transport protocol which includes an encrypted PIN as a means of security.

[0010] US published patent application 20150120569 entitled "Virtual Currency Address Security" allows for the creation of a digital currency address based on public keys to be used in a web-based crypto-currency wallet.

[0011] Published patent application US 20150088721 entitled "Digital Transactional Procedures & Implements" outlines the basic procedure to transfer value between different crypto-currencies and is intended for a domain-wide approach to the acceptance of new crypto-currencies by giving them an exchange rate with an existing crypto-currency.

[0012] Published patent application US 20140258121 entitled "Method and Apparatus for Providing Secured Anonymized Payment" allows for users to conduct financial transactions utilizing a mobile device without a physical trusted service manager by leveraging an anonymous settlement service platform which in turn uses a database lookup to validate the user's identity and accounts that can be used in the transaction.

[0013] US published patent application 20130117185 entitled "Method for conducting a transaction between a merchant site and a customer's electronic device without exposing payment information to a server-side application of the merchant site" allows use of a mobile device to send electronic payment information stored on the device to a payment processor which then creates a token based on the information it received from the mobile device; the token is then delivered to the server-side application to be used in actually conducting the financial transaction.

[0014] US published patent application 20140279551 entitled "Minting and Use of Digital Money" discusses the overall creation of crypto-currency coins and how transactions can be limited, completed and verified.

[0015] Published US patent application 20120123924 entitled "Virtual Currency Configuration Apparatuses, Methods and Systems" discusses a system for flexible monetization of goods and services and how such a service could interact with a smart wallet device.

[0016] U.S. Pat. No. 8,712,918 entitled "Electronic Currency, Electronic Wallet Therefor and Electronic Payment Systems Employing Them" allows for a user to use a mobile device, into which they have already transferred funds electronically from physical financial accounts, to purchase goods or services from a vendor without having to contact the original financial institution to authorize the transaction as the actual electronic currency is held within the mobile device.

[0017] US published patent application 20130166455 entitled "Creating and Using Digital Currency" allows for creation of a physical device or medium that carries a value

that can be transferred to a digital domain and is protected by a physical, state-changing tamper device that indicates the device's security state.

[0018] U.S. Pat. No. 8,041,338 entitled "Mobile Wallet and Digital Payment" allows for use of a mobile device to act as one or more mobile payment cards by establishing a link between each mobile payment card and form of currency. The payments from this mobile device may employ public-key cryptography to securely transmit payment information wirelessly.

[0019] US published patent application 20080195499 entitled "Method of Providing Cash and Cash Equivalent For Electronic Transactions" outlines a system for peer-to-peer commerce using electronic wallets that store electronic token files. Those token files can be passed from wallet to wallet without oversight from a third party and are only validated by the owner of the token for a small fee. In this system token validation is not required prior to conducting a transaction.

[0020] US published patent application 20060165060 entitled "Method and Apparatus for Managing Credentials Through a Wireless Network" generally outlines the use of a mobile device as a digital wallet that holds cryptographic credentials issued from a financial institution, directly to the device, which in turn can be used to authorize financial transactions at Point of Sales terminals via wireless or other means.

[0021] U.S. Pat. No. 7,640,432 entitled "Electronic Cash Controlled by Non-Homomorphic Signatures" describes how digital coins can be managed, verified and digitally signed within a mobile device.

[0022] U.S. Pat. No. 6,157,920 entitled "Executable Digital Cash for Electronic Commerce" allows for a very simplified version of crypto-currency that is protected only by a digital certificate. This digital cash is generated by the first user as a type of offer and accepted by a second user using either a computer or mobile device running specific software capable of accepting the offered digital cash from the first user.

SUMMARY OF THE INVENTION

[0023] Although numerous patents exist, including those listed above, that presently appear relevant, the present embodiment of the system and method is novel and substantially different in a plurality of elements and methods, thus rendering the embodiments nonobvious to a person skilled in the art. However, it is recognized that there is a significant body of prior art in the fields of electronic money transfers, electronic payments and financial accounts, including but not limited to cards, virtual accounts, computer systems, automated teller machines, and other computing devices that utilize or access financial networks.

[0024] The present invention describes a system and method, that is superior to the prior art, for a new and novel way to effect real-time value transfers using a mobile device and any other device (e.g. automated teller machine, point of sale system, self-service kiosk, personal computer, mobile phone, etc.) over one or more financial networks during a single financial transaction, thereby enabling users to convert a plurality of financial instruments (e.g. cash, check, payment card, crypto-currency, money order, cash voucher, E-coupon, virtual currency, etc.) into a 'virtual cash token' which is readily convertible into cash or a cash equivalent that is more universally accepted by merchants and other parties.

[0025] Embodiments of the present invention disclosed herein describe methods and systems whereby an electronic smart-wallet device or application can be used by an individual to manage not only all of their conventional financial instruments (e.g. debit cards, check cards, credit cards, etc.), loyalty cards, and membership cards, but also provides secure management for a plurality of crypto-currency accounts. These attributes facilitate the real-time use of one or more crypto-currencies for making a payment, receiving crypto-currency payments, and crypto-currency exchange (e.g. cash to crypto-currency, crypto-currency to cash, crypto-currency to a different crypto-currency, etc.).

[0026] It is important to note that the novel techniques and devices employed by the present invention seamlessly integrate accounts, assets and credentials, further facilitate their use as well as their security. By applying a standard set of security features and configurable rules across all of a user's accounts, assets, and credentials, the user has a uniform experience that is easy to learn without sacrificing security, while protecting the user from loss, theft, and fraud.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] The skilled artisan will understand that the drawings, described below, are for illustration purposes only. The drawings are not intended to limit the scope of the present invention in any way.

[0028] FIG. **1** illustrates devices and their associated interconnects as associated with the present invention.

[0029] FIG. **2** illustrates a user (**100**) unlocking a smart wallet (**101**) using multifactor authentication.

[0030] FIG. **3** describes the general flow of events and actions when a user unlocks a device (**120**), selects that they wish to create a new payment transaction (**121**) and selects which account they wish to use for the transaction (**122**).

[0031] FIG. **4** generally describes how a user (**100**) can select a crypto-currency, such as but not limited to bitcoin, directly to a recipient (**128**).

[0032] FIG. **5** shows the general process of the user (**100**) using their smart wallet (**101**) to purchase more crypto-currency from a crypto-currency exchange (**130**) with one of the user's (**100**) bank (**129**) accounts configured on the smart wallet (**101**).

[0033] FIG. **6** illustrates generally how a user's (**100**) smart wallet (**101**) synchronizes its local block chain (**132**) with the full public block chain (**131**) by utilizing the User's (**100**) smart phone, laptop, desktop, or other computer platform (**133**) connected to the Internet (**127**).

[0034] FIG. **7** illustrates a transaction ledger synchronization process.

[0035] FIG. **8** illustrates an overview of an outgoing payment transaction.

DETAILED DESCRIPTION OF THE INVENTION

[0036] Embodiments of the present invention are best understood by reference to the detailed figures and description set forth herein. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

For example, it should be appreciated that those skilled in the art will, in light of the teachings of the present invention, recognize a multiplicity of alternate and suitable approaches, depending upon the needs of the particular application, to implement the functionality of any given detail described herein, beyond the particular implementation choices in the following embodiments described and shown. That is, there are numerous modifications and variations of the invention that are too numerous to be listed but that all fit within the scope of the invention. Also, singular words should be read as plural and vice versa and masculine as feminine and vice versa, where appropriate, and alternative embodiments do not necessarily imply that the two are mutually exclusive.

[0037] It is to be further understood that the present invention is not limited to the particular methodology, compounds, materials, manufacturing techniques, uses, and applications, described herein, as these may vary. It is also to be understood that the terminology used herein is used for the purpose of describing particular embodiments only, and is not intended to limit the scope of the present invention. It must be noted that as used herein and in the appended claims, the singular forms "a," "an," and "the" include the plural reference unless the context clearly dictates otherwise. Thus, for example, a reference to "an element" is a reference to one or more elements and includes equivalents thereof known to those skilled in the art. Similarly, for another example, a reference to "a step" or "a means" is a reference to one or more steps or means and may include sub-steps and subservient means.

[0038] All conjunctions used are to be understood in the most inclusive sense possible. Thus, the word "or" should be understood as having the definition of a logical "or" rather than that of a logical "exclusive or" unless the context clearly necessitates otherwise. Structures described herein are to be understood also to refer to functional equivalents of such structures. Language that may be construed to express approximation should be so understood unless the context clearly dictates otherwise.

[0039] Unless defined otherwise, all technical and scientific terms used herein have the same meanings as commonly understood by one of ordinary skill in the art to which this invention belongs. Preferred methods, techniques, devices, and materials are described, although any methods, techniques, devices, or materials similar or equivalent to those described herein may be used in the practice or testing of the present invention. Structures described herein are to be understood also to refer to functional equivalents of such structures. The present invention will now be described in detail with reference to embodiments thereof as illustrated in the accompanying drawings.

[0040] From reading the present disclosure, other variations and modifications will be apparent to persons skilled in the art. Such variations and modifications may involve equivalent and other features which are already known in the art, and which may be used instead of or in addition to features already described herein.

[0041] It should be understood that the scope of the disclosure of the present invention also includes any novel feature or any novel combination of features disclosed herein either explicitly or implicitly or any generalization thereof, whether or not it mitigates any or all of the same technical problems as does the present invention.

[0042] Features, which are described in the context of separate embodiments, may also be provided in combination in a single embodiment. Conversely, various features, which are for brevity, described in the context of a single embodiment, may also be provided separately or in any suitable sub-combination.

[0043] References to "one embodiment," "an embodiment," "example embodiment," "various embodiments," etc., may indicate that the embodiment(s) of the invention so described may include a particular feature, structure, or characteristic, but not every embodiment necessarily includes the particular feature, structure, or characteristic. Further, repeated use of the phrase "in one embodiment," or "in an exemplary embodiment," do not necessarily refer to the same embodiment, however, in some instances they may.

[0044] As is well known to those skilled in the art many careful considerations and compromises typically must be made when designing for the optimal manufacture of a commercial implementation of any system, and in particular, the embodiments of the present invention. A commercial implementation in accordance with the spirit and teachings of the present invention may be configured according to the needs of the particular application, whereby any aspect(s), feature(s), function(s), result(s), component(s), approach (es), or step(s) of the teachings related to any described embodiment of the present invention may be suitably omitted, included, adapted, mixed and matched, or improved and/or optimized by those skilled in the art, using their average skills and known techniques, to achieve the desired implementation that addresses the needs of the particular application.

[0045] A "computer" may refer to one or more apparatus and/or one or more systems that are capable of accepting a structured input, processing the structured input according to prescribed rules, and producing results of the processing as output. Examples of a computer may include non-limiting examples such as: a computer; a stationary and/or portable computer; a computer having a single processor, multiple processors, or multi-core processors, which may operate in parallel and/or not in parallel; a general purpose computer; a supercomputer; a mainframe; a super mini-computer; a mini-computer; a workstation; a micro-computer; a server; a client; an interactive television; a web appliance; a telecommunications device with internet access; a hybrid combination of a computer and an interactive television; a portable computer; a tablet personal computer (PC); a personal digital assistant (PDA); a portable telephone; application-specific hardware to emulate a computer and/or software, such as, for example, a digital signal processor (DSP), a field-programmable gate array (FPGA), an application specific integrated circuit (ASIC), an application specific instruction-set processor (ASIP), a chip, chips, a system on a chip, or a chip set; a data acquisition device; an optical computer; a quantum computer; a biological computer; and generally, an apparatus that may accept data, process data according to one or more stored software programs, generate results, and typically include input, output, storage, arithmetic, logic, and control units.

[0046] "Software" may refer to prescribed rules to operate a computer. Examples of software may include: code segments in one or more computer-readable languages; graphical and or/textual instructions; applets; pre-compiled code; interpreted code; compiled code; and computer programs.

[0047] A "computer-readable medium" may refer to any storage device used for storing data accessible by a computer. Non-limiting examples of a computer-readable

medium may include: a magnetic hard disk; a floppy disk; an optical disk, such as a CD-ROM and a DVD; a magnetic tape; a flash memory; a memory chip; and/or other types of media that can store machine-readable instructions thereon.

[0048] A "computer system" may refer to a system having one or more computers, where each computer may include a computer-readable medium embodying software to operate the computer or one or more of its components. Non-limiting examples of a computer system may include: a distributed computer system for processing information via computer systems linked by a network; two or more computer systems connected together via a network for transmitting and/or receiving information between the computer systems; a computer system including two or more processors within a single computer; and one or more apparatuses and/or one or more systems that may accept data, may process data in accordance with one or more stored software programs, may generate results, and typically may include input, output, storage, arithmetic, logic, and control units.

[0049] A "network" may refer to a number of computers and associated devices that may be connected by communication facilities. A network may involve permanent connections such as cables or temporary connections such as those made through telephone or other communication links. A network may further include hard-wired connections (e.g., coaxial cable, twisted pair, optical fiber, waveguides, etc.) and/or wireless connections (e.g., radio frequency waveforms, free-space optical waveforms, acoustic waveforms, etc.). Examples of a network may include: an internet, such as the Internet; an intranet; a local area network (LAN); a wide area network (WAN); and a combination of networks, such as an internet and an intranet.

[0050] Exemplary networks may operate with any of a number of protocols, such as Internet protocol (IP), asynchronous transfer mode (ATM), and/or synchronous optical network (SONET), user datagram protocol (UDP), IEEE 802.x, near field communication (NFC), Bluetooth™, WiFi™, etc.

[0051] Embodiments of the present invention may include apparatuses for performing the operations disclosed herein. An apparatus may be specially constructed for the desired purposes, or it may comprise a general-purpose device selectively activated or reconfigured by a program stored in the device.

[0052] Embodiments of the invention may also be implemented in one or a combination of hardware, firmware, and software. They may be implemented as instructions stored on a machine-readable medium, which may be read and executed by a computing platform to perform the operations described herein.

[0053] In the following description the terms "computer program medium" and "computer readable medium" may be used to generally refer to media such as, but not limited to, removable storage drives, a hard disk installed in hard disk drive, and the like. These computer program products may provide software to a computer system. Embodiments of the invention may be directed to such computer program products.

[0054] An algorithm as referred to herein is generally considered to be a self-consistent sequence of acts or operations leading to a desired result. These include physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like. It should be understood, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities.

[0055] Unless specifically stated otherwise, and as may be apparent from the following description and claims, it should be appreciated that throughout the specification descriptions utilizing terms such as "processing," "computing," "calculating," "determining," or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulate and/or transform data represented as physical, such as electronic, quantities within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or display devices.

[0056] In a similar manner, the term "processor" may refer to any device or portion of a device that processes electronic data from registers and/or memory to transform that electronic data into other electronic data that may be stored in registers and/or memory. A "computing platform" may comprise one or more processors.

[0057] A non-transitory computer readable medium includes, but is not limited to, a hard drive, compact disc, flash memory, volatile memory, random access memory, magnetic memory, optical memory, semiconductor based memory, phase change memory, optical memory, periodically refreshed memory, and the like; however, the non-transitory computer readable medium does not include a pure transitory signal per se.

[0058] The invention described herein consists of a system and method to manage a plurality of traditional financial accounts and crypto-currency accounts including initiating transfers, currency exchanges, submitting payments, and receiving payments. Under this method and the attendant systems and apparatuses, a local, abbreviated block chain is synchronized for crypto-currency transactions and balance validation to enable online shopping and retail store crypto-currency transactions from a local smart wallet device (e.g., a smart walled, a smart phone), just as transactions with other traditional financial accounts such as but not limited to credit, debit, bank, and other financial accounts.

[0059] In one embodiment, a local block chain is synchronized for crypto-currency transactions and balance validation to enable online and retail crypto transactions, for example, along with access to traditional financial accounts such as but not limited to credit, debit, bank, and other financial accounts. This novel approach enables users to authorize the transfer of crypto-currency while offline, while also controlling how and when that data transfer is completed via innovative synchronization of data from the block chain of a crypto-currency device.

[0060] A smart wallet may be protected by a variety of means including one or more private keys, PINs (personal identification numbers), dynamic pairing passwords, symmetric and asymmetric authentication codes, and/or pattern, behavior, or biometric recognition, etc. Under this invention, local authentication may not only be used to secure the private information such as account or crypto-currencies, but also personalize the transaction by utilizing the same

local authentication to perform remote authentication to approve a transaction, in some embodiments.

[0061] Security is also improved under this invention as the smart wallet maintains only enough of the block chain on the device to enable a transaction and the verifications that follow those transactions. The present invention does not store the block chain per se or a direct copy of it. Instead, the present invention stores an account specific transaction ledger (also referred to as an account specific differential transaction ledger) that is derived from information available in the public block chain. Storing only the "differential" updates to the smart device from the user's computer greatly reduces the CPU and storage requirements of the smart device. This method prevents theft, such as the historic crypto-currency theft at Mt GOX, when an owner has a single internet-based wallet that only provides a payment/account address and performs all of the transaction matching in the background. Centralization of all crypto-currency in one purse puts coin at risk, where coin can only be recognized apart from each other by looking at the address to which they were sent.

[0062] Under this invention, the unique manner that a local, abbreviated block chain (in effect, a account specific differential transaction ledger) is synchronized for crypto-currency transactions and balance validation enables online shopping and retail store crypto-currency transactions from a local smart wallet device (typically having limited processing power and memory), just as transactions with other traditional financial accounts, such as but not limited to credit, debit, bank, and other financial accounts.

[0063] This invention not only supports storage and selection of multiple accounts and currencies, but also combining multiple currencies to execute a single transaction or transfer. Such examples might include combining an amount of Bitcoin plus an amount of Litecoin to equal a full transaction amount. A non-transitory computing device such as a server may be used in conjunction with said transaction to in turn, relegate how each currency is converted and combined. This unique ability leads to further decentralizing crypto-currency transactions by spreading the source of the funds between different exchanges, countries, and wallet IDs, etc.

[0064] FIG. **1** illustrates the general, non-limiting scope of the invention. A user (**100**) is able to use the smart wallet (**101**) to manage a plurality of credit cards (**102**), debit/check cards (**103**), loyalty & rewards cards (**104**), and crypto-currency wallets (**105**). Management functions include, but are not limited to, viewing balances (**106**), credit & overdraft line limits (**107**), reviewing historical transactions (**108**) or creating new transactions (**108**), and viewing rewards/discounts/coupons (**109**).

[0065] The "flow" of this transaction from a single device done with minimal user input is novel to the invention, as illustrated, Conventionally, to accomplish this transaction according to the prior art, a user must:

[0066] log into a crypto-currency exchange

[0067] register the bank account they wish to use with their crypto-currency brokerage account request to purchase X-Amount of crypto-currency for X-Amount of dollars (Actually the user is placing a bid to see if someone will "sell you the coins" for the amount specified by the user.)

[0068] once the bid is accepted, the owner of the coins sends them to the user's exchange brokerage account

[0069] once the transaction above has been validated by the block chain processing nodes, the user's brokerage account balance is updated. Now the user can either send the crypto-currency directly to the VPN provider (which requires registering their information with the CC-Exchange) or the user can transfer it to their local crypto-currency wallet and then to the VPN provider.

[0070] In one non-limiting embodiment of the present invention, a user may unlock their mobile device and then select to transfer funds from a checking account into a crypto-currency wallet, while subsequently selecting to pay an online vendor for VPN service using crypto-currency such as but not limited to Bitcoin. This transaction flow protects the user's normal financial accounts from disclosure to the VPN vendor as well as providing a level of anonymity for the user.

[0071] Under one embodiment, the smart wallet device and the configured accounts, a granular security model (where granular security refers to the number of different log-in credentials that are required) protects assets, and sensitive information it contains. Security may be configured based on one or more of a plurality of physical conditions including, but not limited to, graphical location, time of day, and smart wallet device serial number. Security may be configured on a plurality of user supplied authentication mechanisms including, but not limited to fingerprints, PIN codes, voice, sounds, face, iris, heartbeat, scent, challenge response questions, and pass phrases. Security may be additionally controlled by the usage of white-lists and black-lists for a variety of parameters including, but not limited to vendor/payment-recipient, time of day, geo-location, account balances, and transaction value/amount. See for example, co-owned patent applications: Methods and Systems Related to Multi-Factor, Multidimensional, Mathematical, Hidden and Motion Security PINS, filed on Aug. 1, 2016 and assigned application Ser. No. 15/224,998 (Attorney Docket Number 12188-022); Sound-Directed or Behavior-Directed Method and System for Authenticating a User Executing a Transaction, filed Feb. 10, 2016 and assigned application Ser. No. 15/040,984 (Attorney Docket Number 12188-015); Sound-Directed or Behavior-Directed Method and System for Authenticating a User Executing a Transaction, filed on Feb. 10, 2016 and assigned application Ser. No. 15/040,984 (Attorney Docket Number 12188-015); Biometric, Behavioral-Metric, Knowledge-Metric, and Electronics-Metric Directed Authentication and Transaction Method and System, filed on Jul. 5, 2016 and assigned application Ser. No. 15/202,515 (Attorney Docket Number 12188-019); and Multi-Instance Shared Authentication (MISA) Method and System Prior to Data Access, filed on Jun. 23, 2016 and assigned application Ser. No. 15/191,456 (Attorney Docket Number 12188-018), all of which are incorporated by reference herein.

[0072] For a non-limiting example, FIG. **2** shows a user (**100**) unlocking a smart wallet (**101**) by using multifactor authentication, which in this case, includes a fingerprint (**110**), voice recognition (**111**), and a manually entered PIN code (**112**). Once the smart wallet (**101**) is unlocked, the user (**100**) has access to menu items such as transactions (**108**), accounts (**113**), and configuration (**114**). Some of the configuration (**114**) settings may include device authentication settings (**115**), non-centralized backup & restore (**116**), and security settings (**117**). Some of the options available from the accounts (**113**) could be security settings (**117**), new transactions (**118**), and historical transactions (**119**). Options

available from the transactions (**108**) include new transactions (**118**) and historical transactions (**119**).

[0073] Authentication methods may include local authentication and/or remote authentication to validate user ownership of the smart wallet (**101**) as well as implement a method to cryptographically secure wipe user data and de-activate the device in the event the device has been reported lost or stolen or if multiple invalid log-in attempts have been made. The system may also implement a master code capable of re-activating the device to a factory default state in which no user information is available within the device.

[0074] It is important to note that security settings for the device (the smart wallet (**101**)) and account security settings (**117**) can be configured independently allowing for greater granularity in securing the device itself and the information contained within the device. As a non-limiting example, the user can configure the device where it could be unlocked using only a PIN code, while access to debit/checking accounts require a PIN code and a fingerprint, and access to credit cards requires a PIN Code, a fingerprint, and can only be accessed between 5 AM and 11 PM.

[0075] FIG. **3** describes the general flow of events and actions when a user unlocks a device (**120**), such as but not limited to a mobile or wearable device, selects that she wishes to create a new payment transaction (**121**), and selects which account she wishes to use for the transaction (**122**). The account access information is then checked by the smart wallet to ensure the predefined security requirements for access have been met (**123**). If the requirements have not been met the user is prompted to select a different account or to provide additional authentication factors to match or override the security rules.

[0076] If access is granted to the account, the user can then present payment to the vendor by using any of the available methods accepted by the vendor (e.g. Magnetic Stripe, Wireless Magnetic Strip, NFC, Bluetooth, GSM/2G/3G/4G/LTE modem, sound, light, WiFi, Bluetooth, Antenna, WiFi, QR Code, and the like.) (**124**). Payment methods can be selected on the present device or the payment information is sent to another "payment" device to conduct the transaction. The transaction information is then transmitted to a payment processor for approval (**125**).

[0077] FIG. **4** generally describes how a user (**100**) can select and send a crypto-currency, such as but not limited to Bitcoin, directly to a recipient (**128**). In this non-limiting example, the recipient (**128**) sends the user (**100**) the crypto-currency wallet address via any available method, including but not limited to Magnetic Stripe, Wireless Magnetic Strip, NFC, Bluetooth, GSM/2G/3G/4G/LTE modem, sound, light, WiFi, Bluetooth, Antenna, WiFi, QR Code, and the like.

[0078] The user (**100**) then selects an account on their smart wallet (**101**) to use to send the funds via the Internet (**127**) so that the transaction can be validated via the crypto-currency block chain.

[0079] According to the present invention, the validation of the transaction sending crypto-currency to the another user is still accomplished through the public block chain, but the "reception" of that payment on the recipient's or user's device is validated using the "account specific differential transaction ledger" as referred to above.

[0080] Outgoing payments with crypto-currency occur conventionally as the transaction is directly sent to the crypt-currency block chain network.

[0081] But incoming payments to a user's account are detected on the public block chain and then an intermediate server prepares a cryptographically secure differential update that is then sent to the user's smart wallet where it is processed and integrated into their account ledger. Thus the smart wallet does not have to continuously receive the public block chain and process it for potential incoming transactions, thereby reducing the "horsepower" (i.e., the processor capabilities and speed with which it can process data) required on the recipient's device.

[0082] This validation process, according to the present invention, occurs on the smart wallet (**101**). This feature is unlike the prior art, wherein validation of the transaction via the block chain is executed on a computer/server/processor having sufficient processor "horsepower" to carry out the validation in a relatively short time. Generally smart phones lack such processor "horsepower" and validating the block chain before executing the transaction may require several days. Once the transaction is validated as described above, the crypto-currency is deposited in the recipient's (**128**) crypto-currency wallet and a notification is issued by the recipient's (**128**) smart wallet (**101**) once it detects the change in the balance of the crypto-currency wallet.

[0083] FIG. **5** shows the general process of the user (**100**) using their smart wallet (**101**) to purchase more crypto-currency from a crypto-currency exchange (**130**) with one of the user's (**100**) bank (**129**) accounts configured on the smart wallet (**101**). The user (**100**) initiates the transaction by selecting the appropriate financial institution to fund the crypto-currency purchase, then executes the purchase with one of the many crypto-currency exchanges. The purchase is then sent through the Internet (**127**) for validation prior to being deposited into the user's (**100**) crypto-currency wallet, which then appears as a new balance on the user's (**100**) smart wallet (**101**). The new value of the crypto-currency wallet is then immediately available to fund other transactions.

[0084] FIG. **6** shows a very general method of how a user's (**100**) smart wallet (**101**) synchronizes its local block chain (**132**) with the full public block chain (**131**) by utilizing the user's (**100**) smart phone, laptop, desktop, or other computer platform (**133**) connected to the Internet (**127**). When the smart wallet (**101**) connects to the computing platform (**133**), it verifies the state of its latest transactions and determines if the local block chain (**132**) needs synchronization. It is important to note that without updating the local block chain (**132**) on the smart wallet (**101**) there is no other way of securely verifying transactions and balances of crypto-currency wallets. Further details of synchronization processes are described in co-owned patent application entitled Low Bandwidth Crypto-Currency Transaction Execution and Synchronization Method and System, filed on Sep. 7, 2015 and assigned application No. 62/215,066 (Attorney Docket Number 12188-026).

[0085] In another non-limiting example, a user may accept direct payment for an item or service from an individual or entity by using the mobile device's display to show the QR-Code (or another known code format) of the crypto-currency wallet address into which they wish to receive the

payment. The payor, using another device, then scans the visual code from the user's device in order to transfer funds to the payee.

[0086] As a different approach to this embodiment, the user could also wirelessly transmit their wallet address to the payor (via a magnetic stripe, wireless magnetic strip, NFC, Bluetooth, GSM/2G/3G/4G/LTE modem, sound, light, WiFi, Bluetooth, antenna, WiFi, QR Code, and/or magnetic loop as non-limiting examples), or record their wallet address to a magnetic stripe that could then be received or read by the payor.

[0087] In another non-limiting embodiment, a user may unlock a device and decide to transfer all or some of their LiteCoins and DodgeCoins (or other crypto-currencies) into their BitCoin wallet at the current exchange rate, thereby consolidating funds and possibly taking advantage of favorable exchange rates or funding their account prior to conducting a financial transaction.

[0088] In another non-limiting embodiment, an individual, using their smart wallet device, could send Bitcoin or other crypto-currencies to their child, spouse, or friend living in a foreign country that the receiving individual, using their electronic smart wallet, could then use to pay bills either directly with the crypto-currency or by exchanging the crypto-currency into locally accepted currency via a financial institution configured in their smart wallet. Such a scenario securely bypasses international banking fees and exchange rates while providing almost instantly available funds to the receiving party and proof of delivery to the sender.

[0089] In a security related, non-limiting embodiment, the electronic smart wallet's security and usage features can be applied to the crypto-currency wallets contained therein such that wallets can only be opened and utilized in transactions when one or more criteria are met. As a non-limiting example, the user must provide at least three factors of authentication before the wallet can be opened (e.g. fingerprint, voice, PIN, password, NFC/RFID token, etc.) and then transactions can only be performed if they meet certain criteria such as the amount is below a preset limit, the recipient is on a white-list of recipients, the recipient is not on a black-list of recipients, the user is within a certain area (geo-fencing), the transaction is being conducted between certain hours, or the balance of the drawing account is above a predefined limit, etc.

[0090] An additional non-limiting embodiment of the disclosed invention is it's novel handling of the crypto-currency block-chain (the underlying technology that makes crypto-currencies secure and validates transactions) which reduces the storage space requirements and minimizes the impact on battery life for the mobile device.

[0091] In one sense, the block chain may be considered a "rolling" hash. If one does not have the very first transaction (the start of the block chain) then you cannot validate the last transaction (the end of the block chain). If one retained only the tail end of the block chain, one could only validate transactions up to but not including, the first transaction in the retained segment of the chain. Thus someone could in theory tamper with the short/abbreviated retained block chain segment and thereby lead you to believe certain transactions have occurred. The real power of the block chain is derived from its unwieldy size, making it relatively impossible for anyone to tamper with the transaction history due to the requirement of re-calculating the hash of every transaction that has occurred since the time of their "modified" transaction. The more transaction history in the chain, the harder it is to fake it!

[0092] As an example, if the block chain size for Bitcoin exceeds 30 GB (Gigabytes), typically during initial configuration of the device the user would be required to download the entire block-chain, which could take from many hours to several weeks, while the smart device is plugged into an electrical outlet or charger to ensure adequate power is available during the entire block chain download. Only after the entire block chain has been downloaded to the smart device, can crypto-currency transactions be validated and therefore executed using the smart phone.

[0093] As an example, given the current magnitude of crypto-currency transactions, this initial synchronization of the block chain, using a dual-core desktop computer with a dedicated, high-speed Internet connection (50 Mbps) takes approximately 1-CPU-Day to process one (1) weeks worth of block chain transactions.

[0094] Processing requirements will only increase as the transaction volume grows by the broader acceptance of Bitcoin (or other crypto-currencies), and the processing load outlined above is only for one of many crypto-currency block chains.

[0095] According to the present invention, the user can complete the device setup in a matter of minutes and requires only minimal synchronization of the block code thereafter. The synchronization requires that only those crypto-currency transactions that affect the presently-contemplated transaction using the smart device need to be downloaded to the smart device. A software application on the user's desktop, laptop, or mobile device that manages a NXT-ID (assignee of the present application) proprietary synchronization process between the mobile device's condensed, wallet specific, version of the block chain and the complete, public block chain for the crypto-currency involved.

[0096] This capability of having a local, cached, frequently-updated version of the block chain adds significantly to the overall transaction security of the smart device. Until now, this capability has been prevented by mainstream methods of keeping the block chain up to date, with its attendant battery-crushing power requirements and excessive bandwidth data transfers.

[0097] The following example illustrates certain features of the invention and a crypto-currency transaction. Assume a sender wants to send seven Bitcoin to a recipient. But a recipient (the sender was previously a recipient of the Bitcoin he is now sending) can spend only the full-amount of transactions received. Thus the software must gather enough incoming transaction that are greater than or equal to the amount the sender wants to send.

[0098] Assume the sender has incoming transactions that total 12.25 Bitcoin.

[0099] When a transaction request to send seven Bitcoin is generated, two recipients are listed in it. The recipient to receive seven Bitcoin and the sender to receive (back) 5.25 Bitcoin, for a total of 12.25 Bitcoin spent. This technique allows each coin/unit of crypto-currency to be traced all the way back to its origin, even fractional parts of a coin.

[0100] To conduct a transaction, if the sender is sure he has ownership of the "coins", he does not need to have access to the full block chain, only to the last transaction index and

transaction value for each of the "coins" in his wallet. But the sender does need access to the full block chain to ensure he owns those coins.

[0101] Another example transaction is described below. A transaction request is generated and cryptographically signed by a second processing component (for example a component of a mobile phone). The second processing component uses the last transaction index for each unit of crypto-currency to be transferred, the recipient's wallet address, and the senders wallet address in the request. The request is signed by a sender's private cryptographic key associated with the crypto-currency wallet that he is sending the funds from. Note that access to the full block chain of all crypto-currency transactions is not required at this point.

[0102] The signed transaction request is forwarded to the crypto-currency network via the Internet for transaction validation and execution.

[0103] When a new transaction (for the mobile phone user's crypto-currency account) is detected in the public block chain by a first processing component (for example a component of a desktop computer), prepares a cryptographically secure status-update-packet which is then forwarded to the second processing component. The second processing component upon receipt of this status-update-packet determines if a local ledger update is required and if so, it requests the required information from the first processing component. Once the updated ledger entries are received, the data integrity is verified and the new transactions are added to the local ledger. If they are not verified the update is discarded and requested again from the server until either the maximum number of retries is exceeded or the update passes validation.

[0104] The local ledger (also referred to as the "differential transaction ledger") total balance is calculated at the second processing component, and the user interface is updated with the new balance.

[0105] In the description above, the first processing component comprises a server or desktop computer that monitors the full block chain. When a transaction pertaining to the user's wallet is validated by the block chain processing nodes/network (there must be at least two independent validations and usually not more than six validations), the server or desktop computer creates a message to the first processing component advising that the second processing component may need a balance update, and then review that update packet and decide how to proceed. The update packet is either ignored if it is another validation on a previous transaction, updates its outgoing payments ledger, or updates its balance ledger.

[0106] FIG. **7** illustrates a step-by-step flow chart for the transaction ledger synchronization process.

[0107] FIG. **8** illustrates an example of an outgoing payment transaction.

[0108] An exemplary system for implementing the various software aspects of the invention includes a computing device or a network of computing devices. In a basic configuration, computing device may include any type of stationary computing device or a mobile computing device. Computing device typically includes at least one processing unit and system memory. Depending on the exact configuration and type of computing device, system memory may be volatile (such as RAM), non-volatile (such as ROM, flash memory, and the like) or some combination of the two. System memory typically includes operating system, one or more applications, and may include program data. Computing device may also have additional features or functionality. For example, computing device may also include additional data storage devices (removable and/or non-removable) such as, for example, magnetic disks, optical disks, or tape. Computer storage media may include volatile and non-volatile, removable and non-removable media implemented in any method or technology for storage of information, such as computer readable instructions, data structures, program modules or other data. System memory, removable storage and non-removable storage are all examples of computer storage media. Non-transitory computer storage media includes, but is not limited to, RAM, ROM, EEPROM, flash memory or other memory technology, CD-ROM, digital versatile disks (DVD) or other optical storage, magnetic cassettes, magnetic tape, magnetic disk storage or other magnetic storage devices, or any other physical medium which can be used to store the desired information and which can be accessed by computing device. Any such computer storage media may be part of device. A computing device may also have input device(s) such as a keyboard, mouse, pen, voice input device, touch input device, etc. Output device(s) such as a display, speakers, printer, etc. may also be included. Computing device also contains communication connection(s) that allow the device to communicate with other computing devices, such as over a network or a wireless network. By way of example, and not limitation, communication connection(s) may include wired media such as a wired network or direct-wired connection, and wireless media such as acoustic, RF, infrared and other wireless media.

[0109] Computer program code for carrying out operations of the invention described above may be written in a high-level programming language, such as C or C++, for development convenience. In addition, computer program code for carrying out operations of embodiments of the present invention may also be written in other programming languages, such as, but not limited to, interpreted languages. Some modules or routines may be written in assembly language or even micro-code to enhance performance and/or memory usage. It will be further appreciated that the functionality of any or all of the program modules may also be implemented using discrete hardware components, one or more application specific integrated circuits (ASICs), or a programmed digital signal processor or microcontroller. A code in which a program of the present invention is described can be included as a firmware in a RAM, a ROM and a flash memory. Otherwise, the code can be stored in a tangible computer-readable storage medium such as a magnetic tape, a flexible disc, a hard disc, a compact disc, a photo-magnetic disc, a digital versatile disc (DVD). The present invention can be configured for use in a computer or an information processing apparatus which includes a memory, such as a central processing unit (CPU), a RAM and a ROM as well as a storage medium such as a hard disc.

[0110] The "step-by-step process" for performing the claimed functions herein is a specific algorithm, and may be shown as a mathematical formula, in the text of the specification as prose, and/or in a flow chart. The instructions of the software program create a special purpose machine for carrying out the particular algorithm. Thus, in any means-plus-function claim herein in which the disclosed structure is a computer, or microprocessor, programmed to carry out an algorithm, the disclosed structure is not the general

purpose computer, but rather the special purpose computer programmed to perform the disclosed algorithm.

[0111] A general purpose computer, or microprocessor, may be programmed to carry out the algorithm/steps of the present invention creating a new machine. The general purpose computer becomes a special purpose computer once it is programmed to perform particular functions pursuant to instructions from program software of the present invention. The instructions of the software program that carry out the algorithm/steps electrically change the general purpose computer by creating electrical paths within the device. These electrical paths create a special purpose machine for carrying out the particular algorithm/steps.

[0112] Unless specifically stated otherwise as apparent from the discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0113] While the invention has been described with reference to preferred embodiments, it will be understood by those skilled in the art that various changes may be made and equivalent elements may be substituted for elements thereof without departing from the scope of the present invention. The scope of the present invention further includes any combination of the elements from the various embodiments set forth. In addition, modifications may be made to adapt a particular situation to the teachings of the present invention without departing from its essential scope. Therefore, it is intended that the invention not be limited to the particular embodiment disclosed as the best mode contemplated for carrying out this invention, but that the invention will include all embodiments falling within the scope of the appended claims.

What is claimed is:

1. A method for conducting a transaction using crypto-currency by a user having a crypto-currency account, the method comprising:

generating and cryptographically signing a new transaction request at a second processing component responsive to a new transaction desired by the user;

forwarding the new transaction request to a crypto-currency network;

at a first processing component, detecting former transactions related to the user's crypto-currency account in a public block chain of the crypto-currency network and preparing a cryptographically secure status-update message responsive thereto;

the first processing component sending the status-update message to the second processing component; and

at the second processing component receiving the status-update message and determining whether an update to a local ledger is required based on the former transactions detected by the first processing device, if a status update is required, the second processing component requesting update information from the first processing component, receiving the update information, and updating the local ledger.

2. The method of claim **1** wherein the new transaction request uses a last transaction index for each unit of crypto-currency to be transferred, uses a recipient's address, and uses a sender's address.

3. The method of claim **1** wherein the transaction relates to a sender sending funds and wherein the step of generating and cryptographically signing comprises using a private cryptographic key associated with a crypto-currency account of the sender.

4. The method of claim **1** wherein the step of forwarding comprising forwarding the transaction request via the Internet for validation and execution of the transaction.

5. The method of claim **1** upon receiving the update information at the second processing component, the second processing component verifying integrity of data received before executing the updating step.

6. The method of claim **5** wherein if integrity is not verified, the second processing component discarding the update information and requesting the first processing component to resend the update information.

7. The method of claim **1** the local ledger comprising an account-specific differential transaction ledger.

8. The method of claim **1** the second processing component associated with a mobile or wearable device, the method further comprising the second processing component calculating a new crypto-currency account balance and displaying the new crypto-currency account balance on a display of the mobile or wearable device.

9. The method of claim **1** wherein the first processing component exhibits faster processing capabilities than the second processing component.

10. The method of claim **1** wherein the second processing component is an element of a smart phone, a smart wallet, or a wearable device.

11. The method of claim **10** wherein the smart wallet manages personal financial accounts comprising any one or more of credit cards, debit/check cards, loyalty and rewards cards, and crypto-currency wallets for reviewing balances, reviewing credit and overdraft line limits, reviewing historical transactions, reviewing rewards, discounts, and coupons, and for creating new transactions.

12. The method of claim **11** the smart phone or the smart wallet requiring different authentication factors than required to access the personal financial accounts.

13. The method of claim **1** the first processing component an element of an automated teller machine, a point of sale system, a self-service kiosk, a personal computer, or a mobile phone.

14. The method of claim **1** the transaction comprising a financial transaction further comprising one or more of a crypto-currency transfer, a crypto-currency payment, a crypto-currency exchange, a crypto-currency purchase, and receiving crypto-currency.

15. The method of claim **1** wherein a user of a device incorporating the second processing component can execute the transaction without a connection to the first processing component.

16. The method of claim **1** further comprising authenticating the user of a device incorporating the second processing component prior to executing the transaction.

17. A method for conducting a transaction using crypto-currency by a user having a crypto-currency account, the method comprising

a first processing component having access to a full block chain representing a plurality of past crypto-currency transactions;

a second processing component, an element of a device operated by the user, generating and cryptographically signing a new transaction request responsive to a user's request for the new transaction;

the second processing component forwarding the new transaction request to a crypto-currency network;

at the first processing component, detecting former transactions related to the user's crypto-currency account in a public block chain of the crypto-currency network and preparing a cryptographically secure status-update message responsive thereto;

the first processing component sending the status-update message to the second processing component; and

at the second processing component receiving the status-update message and updating a local ledger responsive thereto.

18. The method of claim **17** the local ledger comprising an account-specific differential transaction ledger.

19. The method of claim **17** the second processing component operative with a mobile or wearable device.

20. A mobile or wearable device for conducting a transaction using crypto-currency by a user having a crypto-currency account, the mobile or wearable device comprising:

a second processing component for generating and cryptographically signing a new transaction request responsive to a new transaction desired by the user;

the second processing component forwarding the new transaction request to a crypto-currency network;

a first processing component not an element of the mobile or wearable device detecting former transactions related to the user's crypto-currency account in a public block chain of the crypto-currency network and preparing a cryptographically secure status-update message responsive thereto;

the first processing component sending the status-update message to the second processing component; and

the second processing component receiving the status-update message and determining whether an update to a local ledger is required based on the former transactions detected by the first processing component, if a status update is required, the second processing component requesting update information from the first processing component, receiving the update information, updating the local ledger, calculating a new crypto-currency account balance, and displaying the new crypto-currency account balance on a display of the mobile or wearable device.

* * * * *