APPARATUS, SYSTEMS AND METHODS FOR AUTHORIZATION OF ELECTRONIC TRANSACTIONS BASED ON SECURED ZONES

BACKGROUND

[0001] Consumers are conducting electronic transactions with increasing frequency. Because of fraudulent individuals who are able to obtain financial information about the consumer and their financial accounts, the consumer is at risk for having such fraudulent individual access and steal their assets and/or personal information using fraudulent electronic transactions. Accordingly, there is a need in the arts to thwart the fraudulent individual's attempt to obtain such consumer identity and account information.

SUMMARY

[0002] Systems and methods of providing secure electronic-based transactions to a consumer are disclosed. An exemplary embodiment employs a system that compares a distance between a determined location of a personal electronic device of the consumer with the location of an electronic transaction. An example embodiment accesses a predefined distance. This predefined distance may be represented as a radius, or a secured zone, around the personal electronic device of the consumer. Then, if the determined location of the electronic transaction is within the predefined distance from (within the secured zone of) the personal electronic device of the consumer, the electronic transaction is permitted.

[0003] Alternatively, or additionally, a predefined location is associated with the predefined distance. An exemplary embodiment employs a system that compares a distance between the predefined location with the location of the electronic transaction. Then, if the determined location of the electronic transaction is within the predefined distance from (within the secured zone of) the predefined location, the electronic transaction is permitted.

[0004] In some embodiments, the predefined distance is stored securely in blockchain information that is uniquely associated with the particular consumer who is accessing their financial information to conduct an electronic transaction. Since a blockchain is not accessible by a fraudulent individual, the fraudulent individual will never have access to the predefined distance that is necessary for verification of the electronic transaction. Various other information that may be used to verify an electronic transaction may optionally be secured within the consumer's blockchain information.

[0005] The predefined distance is a variable value that can be user-defined. For example, if the consumer is travelling in a foreign country, the consumer may choose to decrease the length of the predefined distance for the duration of their travels. Thus, the consumer can feel that any electronic transactions that they perform, such as accessing an automated teller machine (ATM) for cash in the local country currency, may be performed in a secure and reliable manner. Further, in the event that their ATM card is lost or stolen, they will appreciate that their card will be impossible to use for a fraudulent electronic transaction. Further, in the event of a lost or stolen ATM card, the consumer can immediately modify the predefined distance that has been securely stored in their blockchain information to a different predefined distance, such as a few inches or feet, or even no distance. (Then, if their misplaced ATM card is later found by the consumer or if their lost ATM card is returned to the consumer, the consumer can again change and securely store the predefined distance into their secure blockchain information so that they may continue to user their ATM card.)

BRIEF DESCRIPTION OF THE DRAWINGS

[0006] Preferred and alternative embodiments are described in detail below with reference to the following drawings:

[0007] FIGURE 1 is a block diagram of an embodiment of a transaction authorization system; and

[0008] FIGURE 2 is a block diagram of another embodiment of a transaction authorization system;

[0009] FIGURE 3 is a block diagram of another embodiment of a transaction authorization system;

[0010] FIGURE 4 is an example graphical user interface (GUI) that may be presented to the consumer during the transaction verification and authorization process;

[0011] FIGURE 5 is a map based version of a presented GUI; and

[0012] FIGURE 6 is a block diagram of an example transaction authorization system.

DETAILED DESCRIPTION

[0013] FIGURE 1 is a block diagram of an embodiment of a transaction authorization system 100. The non-limiting illustrated embodiment of the transaction authorization system 100 comprises at least one electronic transaction verification system 102 that is in communication with a electronic mobile device 104 that is presumably in the personal possession of a consumer conducting an electronic transaction and that is in communication with an electronic transaction device 106.

[0014] The electronic transaction verification system 102 manages consumer blockchain information 108 that is uniquely associated with the consumer who is conducting the electronic transaction. The blockchain information 108 is conceptually illustrated as residing in a single block. One skilled in the art understands that in practice, the consumer blockchain information 108 resides in a distributed system of other electronic devices that are

communicatively coupled to the electronic transaction verification system 102 via the communication network 110. When a transaction verification and authorization process is underway, the electronic transaction verification system 102 accesses these distributed locations so that the particular consumer information residing in the consumer blockchain information 108 may be accessed and used for transaction verification and authorization.

[0015] Further, the electronic transaction verification system 102, during any particular electronic transaction, manages the verification process whereby an ongoing electronic transaction is verified and/or is authorized for the consumer. In practice, the electronic transaction verification system 102 manages consumer blockchain information for thousands of, or more, individual consumer. Embodiments of the transaction authorization system 100 has the capability of concurrently managing the transaction verification and authorization process for thousands of, or more, electronic transactions.

[0016] The electronic transaction verification system 102 and the consumer's electronic mobile device 104 are communicatively coupled together via the communication system 110. The electronic transaction device 106 is also communicatively coupled to the electronic transaction verification system 102. Here, there is no need for the electronic transaction device 106 to be communicatively coupled to the electronic mobile device 104. Further, if the consumer is using an optional transaction device 112, such as an ATM card or the like, to facilitate the electronic transaction, the transaction device 112 does not need to be communicatively coupled to the consumer's electronic mobile device 104 or to the electronic transaction verification system 102 for completion of the transaction verification and authorization process. Such embodiments are inherently less complicated in architecture and/or operation, and may be implemented at a lower cost.

[0017] During a transaction, location information defining the location of the electronic mobile device 104 is determined and is communicated to the electronic transaction verification system 102. Also, location information defining the location of the electronic

transaction device 106 is determined and is communicated to the electronic transaction verification system 102. Alternatively, or additionally, identity information that identifies the electronic transaction device 106 may be used to access a database wherein the location information of the electronic transaction device 106 may be accessed and then provided to the electronic transaction verification system 102.

[0018] Once the locations of the electronic mobile device 104 and the electronic transaction device 106 are determined, the electronic transaction verification system 102 determines a distance between the electronic mobile device 104 and the electronic transaction device 106. The electronic transaction verification system 102 then compares the determined distance between the electronic mobile device 104 and the electronic transaction device 106 with a predefined distance, interchangeably referred to herein as a secured zone. If the determined distance between the electronic mobile device 104 and the electronic transaction device 106 is less than or equal to the predefined distance, then some embodiments of the transaction authorization system 100 determine that the electronic transaction may be verified and/or authorized. In some embodiments, if the transaction authorization system 100 determines that that the determined distance is not less than or equal to the predefined distance, then transaction authorization may be withheld, may be delayed, and/or may be conditional upon an explicit authorization from the consumer.

[0019] The location of the electronic mobile device 104 may be monitored on a real time basis. Accordingly, as the consumer moves from one location to another, the secured zone effectively moves along with the changing location of the consumer, and is thus dynamic.

[0020] The predefined distance, in some embodiments, is securely stored as part of the consumer blockchain information 108. During the transaction verification and authorization process, the electronic transaction verification system 102 accesses this secure predefined distance. In some embodiments, the consumer has to authorize the electronic

transaction verification system 102 to access the predefined distance from their secure consumer blockchain information 108 during the electronic transaction.

[0021] FIGURE 1 illustrates that the electronic mobile device 104 is in communication with (is communicatively coupled to) the communication network 110 via a wireless signal 114. For example, the electronic mobile device 104 may be communicatively coupled to a cell tower of a wireless system. As another non-limiting example, the electronic mobile device 104 may be communicatively coupled to a Wi-fi node that is part of the communication network 110. In other situations, the electronic mobile device 104 may be communicatively coupled to the communication network 110 via a wire-based connector, such as when the electronic mobile device 104 is a personal computer, laptop device, personal assistant or the like where the consumer is using the wire connector to connect their electronic mobile device 104 to the communication network 110.

[0022] FIGURE 1 further illustrates that the electronic transaction device 106 is in communication with (is communicatively coupled to) the communication network 110 via a wireless signal 116. In other situations, the electronic transaction device 106 may be communicatively coupled to the communication network 110 via a wire-based connector, such as when the electronic transaction device 106 is part of a networked system that is managed and controlled by a financial institution or other institution.

[0023] The communication network 110 is illustrated as a generic communication system. In one embodiment, the communication network 110 comprises a cellular telephone system, such as a radio frequency (RF) wireless system. Accordingly, the electronic mobile device 104 and/or the electronic transaction device 106 includes a suitable transceiver. Alternatively, the communication network 110 may be a telephony system, the Internet, a Wi-fi system, a microwave communication system, a fiber optics system, an intranet system, a local access network (LAN) system, an Ethernet system, a cable system, a radio frequency system, a cellular system, an infrared system, a satellite system, or a hybrid system

comprised of multiple types of communication media. Additionally, embodiments of the transaction authorization system 100 may be implemented using other types of communication technologies, such as but not limited to, digital subscriber loop (DSL), X.25, Internet Protocol (IP), Ethernet, Integrated Services Digital Network (ISDN) and asynchronous transfer mode (ATM). Also, embodiments of the transaction authorization system 100 may be configured to communicate over combination systems having a plurality of segments which employ different formats for each segment that employ different technologies on each segment.

[0024] In operation, the consumer initiates an electronic transaction at the electronic transaction device 106. The electronic transaction device 106 communicates with the electronic transaction verification system 102 to initiate the transaction verification and authorization process. Alternatively, or additionally, the transaction verification and authorization process may be initiated by the consumer who uses their electronic mobile device 104 to start the electronic transaction.

[0025] Then, in an example embodiment, the electronic transaction verification system 102 is provided and/or obtains location information that defines the location of the electronic transaction device 106, and therefore that defines the location of the ongoing electronic transaction. Then, the electronic transaction verification system 102 accesses or obtains current location information (in real time or near-real time) for the consumer's electronic mobile device 104. Presumably, the consumer is in the immediate vicinity of and/or is in possession of their electronic mobile device 104. If the determined distance between the electronic mobile device 104 and the electronic transaction device 106 is within the predefined distance, then embodiments of the transaction authorization system 100 may infer that the consumer is the authorized person who is conducting the ongoing electronic transaction. Therefore, the electronic transaction may then be permitted to go to completion by the transaction authorization system 100.

[0026] On the other hand, if the determined distance between the electronic mobile device 104 and the electronic transaction device 106 is greater than the predefined distance, then embodiments of the transaction authorization system 100 may infer that the consumer is not the person who is conducting the ongoing electronic transaction. That is, embodiments may infer that a fraudulent individual is attempting to conduct the electronic transaction. Therefore, the electronic transaction may then be prevented from going to completion by the transaction authorization system 100.

[0027] In the various embodiments, the consumer has the ability to control the value of the predefined distance that is used during the transaction verification and authorization process. The user may specify this value, in any suitable metric, prior to the initiation of the electronic transaction. The user-defined predefined distance may be expressed as a radius distance. Here, the distance between a determinable location of the electronic transaction device 106 and the electronic mobile device 104 is readily comparable to a radius distance value.

[0028] In some embodiments, the consumer is permitted to enable or disable operation of the transaction authorization system 100. Alternatively, or additionally, the consumer may be allowed to activate or deactivate the security zone. Here, the transaction verification and authorization process may be based on other or additional information, such as the secure information residing in the consumer blockchain information 108.

[0029] Alternatively, or additionally, the predefined distance may be specified by any authorized third party. For example, a particular predefined distance may be specified by a credit card company for credit card-based electronic transactions. Here, if the consumer is using their credit card for an electronic transaction, the predefined distance specified by the credit card company is used during the transaction verification and authorization process. If another type of financial instrument is used by the consumer, a different predefined distance is used for the transaction verification and authorization process.

[0030] Alternatively, or additionally, other geometry forms may be used define the predefined distance. For example, a square, an oval, or other geometric shape, or polygon may be used. An outline of a known structure, such as a shopping mall or other location where an electronic transaction is likely to occur, may be used. In some embodiments, a plurality of different predefined distances may be used, wherein one of a plurality of predefined distances is selected depending upon the particular situation of the electronic transaction. For example, but not limited to, a radius value may be used when the consumer is conducting the electronic transaction at an ATM device. In a situation where the consumer is at a shopping mall, the predefined distance defined by the extents of the shopping mall may be used to verify and authorize point of purchase transaction occurring within the shopping mall. Any suitable geometry that defines the predefined distance are contemplated by the various embodiments.

[0031] FIGURE 2 is a block diagram of another embodiment of a transaction authorization system. One skilled in the art appreciates that the actual location of the consumer's electronic mobile device 104 may not be determinable or may not be determinable with any reliable degree of accuracy. However, the electronic mobile device 104 may be in communication with another intermediate device 202 wherein the location of that device is known and/or is determinable. For example, the electronic mobile device 104 may be wirelessly communicating with a cell phone tower, a Wi-fi node, or the like (the intermediate device 202) via wireless signal 204. The intermediate device 202 may then use a wireless signal 206 (or a wire-based connector) to communicatively couple the electronic mobile device 104 to the communication network 110.

[0032] Here, since the electronic mobile device 104 is communicatively coupled to the electronic transaction verification system 102 via the intermediate device 202, and since the location of the intermediate device 202 is known and/or may be determinable, the location of the intermediate device 202 may be used as a proxy location for the consumer

and/or for the consumer's electronic mobile device 104 for the transaction verification and authorization process.

[0033] Further, in some embodiments, once the nature or characteristic of the intermediate device 202 is determined, a different predefined distance may be used to perform the transaction verification and authorization process. For example, the electronic mobile device 104 may be provisioned with a global positioning system (GPS) that can be used to precisely determine the location of the electronic mobile device 104. However, at times, the GPS system may be turned off, may be inactive, or may be inoperable. In such a situation, since the exact location of the electronic mobile device 104 cannot be obtained from the onboard GPS, then a proxy location can be determined from the location of the intermediate device 202. To illustrate, the consumer may be travelling in an automobile, an aircraft or other vehicle where determination of a location of the electronic mobile device 104 is not practical. The transaction may be occurring at an electronic transaction device 106 that is part of the vehicle. When then transaction authorization system 100 determines that the ongoing transaction is occurring, and that the location of the consumer is being approximated by the determined proxy location of the intermediate device 202, then a different predefined distance may be used for the transaction verification and authorization process. For example, if the intermediate device 202 is a cell tower, the predefined distance may need to be adjusted and enlarged as compared to situations where the location of the transaction authorization system 100 can be accurately determined. In the case of an aircraft, a relatively small predefined distance may be used as compared to the predefined distance that is used to verify and authenticate an ATM or point of purchase transaction since a reasonable inference may be made that the consumer is on board the aircraft. Conversely, if the consumer's electronic mobile device 104 does not have an operable GPS, a relatively large predefined distance may be used as compared to the predefined distance that is used to verify and authenticate an ATM or point of purchase transaction.

[0034] In some situations, the electronic transaction verification system 102 may be in communication with the electronic mobile device 104. The consumer may use a suitable secure interface to specify their current location as the proxy location for their electronic mobile device 104. Preferably, in such situations, additional levels of security and/or authorization (such as personal identification numbers, pins, passwords, and other forms for identity verification) are used to ensure that the user-specified proxy location is not being provided by a fraudulent individual.

[0035] FIGURE 3 is a block diagram of another embodiment of a transaction authorization system. In this example non-limiting embodiment, a known location is used as the proxy location for the transaction verification and authorization process. Here, the known location is compared with the determined location of the electronic transaction device 106. For example, the consumer may be at a shopping mall or other location, area, geographic region, or the like. To illustrate, the user may be attempting to obtain cash at an ATM, may be attempting to make a payment or obtain cash at a bank, and/or may be attempting to purchase a product or service at a store (interchangeably referred to herein in as a point of purchase transaction). As another example, the consumer may be at an event (such as a stadium, a farmer's market, or other venue) where a vendor is using a portable electronic transaction device 106 to conduct the electronic transaction.

[0036] Embodiments of the transaction authorization system 100 determine a location proximate to the ongoing electronic transaction that is associated with a known location 302. The known location 302 is associated with a predefined distance. The transaction verification and authorization process may then be performed based on the known location, the associated predefined distance, and the determined location of the electronic transaction device 106.

[0037] In an example embodiment, the consumer may initiate a communication with the electronic transaction verification system 102 and specify their current location

and/or specify the known location. For example, the consumer may indicate that they are in a particular venue such as a stadium. As another non-limiting example, the consumer may specify that they are currently in a particular city, town, or other identifiable region. The user-specified location may then be used for any occurring electronic transactions while the consumer is at or is nearby the user-specified location. Preferably, in such situations, additional levels of security and/or authorization (such as personal identification numbers, pins, passwords, or answers to particular questions) are used to ensure that the user-specified proxy location is not being provided by a fraudulent individual.

[0038] Alternatively, or additionally, information pertaining to past electronic transactions that have been previously verified and authorized is stored within the secure blockchain information 108. After some duration, embodiments of the transaction authorization system 100 may learn that the consumer is frequently located at a particular known location. One skilled in the art appreciates that there are likely to be a plurality of such known locations that the consumer frequents. Once the location of the electronic transaction device 106 is determined, the determined location of the electronic transaction device 106 can be compared with the plurality of known locations that the consumer is frequently at. Since the consumer blockchain information 108 is secure, it is not possible for a fraudulent individual access the secure consumer blockchain information 108 to learn about these known locations that are associated with the consumer.

[0039] As noted herein, the predefined distance may be represented using any suitable geometry. For example, if the known location 302 is associated with a building or other predefined region, the predefined distance may be represented using the geometry of the known location. For example, but not limited to, if the known location is a building that has one or more stores or is a field where a farmer's market in typically held, the predefined distance may be represented using a rectangle 304. Any suitable geometry may be used for the predefined distance that is associated with a known location.

[0040] FIGURE 4 is an example graphical user interface (GUI) 402 that may be presented to the consumer during the transaction verification and authorization process. In this non-limiting example of an ongoing transaction verification and authorization process, the consumer receives a message from the electronic transaction verification system 102 that is presented on a display 404 of their electronic mobile device 104, here conceptually illustrated as the well known cell phone or smart phone. The GUI 402 indicates that an electronic transaction is occurring, presents information about the transaction, and a provides a query requesting that the user authenticate the transaction and/or to take immediate security measures in the event that they are not conducting the electronic transaction. Any suitable GUI 402 that communicates information to the consumer during an ongoing electronic transaction is contemplated by the various embodiments.

[0041] In some embodiments, if a particular electronic transaction is denied by the transaction authorization system 100, an alarm or other suitable notification is sent to the consumer's electronic mobile device 104 or another device that is being used by or that is accessible to the consumer. Accordingly, the consumer may be informed that a potentially fraudulent electronic transaction has been denied, and that they should take corrective and/or precautionary actions to safeguard their property. Any suitable visual, haptic, and/or auditory warning or alarm may be generated and communicated to the consumer's electronic mobile device 104 or another suitable device. Further, the warning or alarm can be communicated to other entities, such as a bank or other financial intuitions, or even the consumer's spouse, friend or other close personal contact.

[0042] The GUI 402 is configured to permit the consumer to input any information back to the electronic transaction verification system 102 via actuation of one or more of the controllers 406 residing on the surface of the electronic mobile device 104. Any suitable GUI 402 that enables the consumer to input information during an ongoing electronic transaction is contemplated by the various embodiments. Some embodiments may require the consumer

to input confidential and secret information that is known only to the consumer. Information corresponding to or matching with the input provided by the consumer may be securely stored in the consumer blockchain information 108. In response to receiving the information from the consumer, the electronic transaction may then be verified and/or authenticated, thereby permitting the electronic transaction to move to completion.

[0043] In the various embodiments, the electronic transaction device 106 was generically and conceptually described as a device that the consumer is interacting with or is using to conduct an electronic transaction. Embodiments of the transaction authorization system 100 are configured to facilitate electronic transactions with any electronic transaction device now known or later developed. Non-limiting example of electronic transaction devices 106 include automatic payment systems such as toll road collection points, an Internet of things (IoT) device, a credit card reader, a robot device, an artificial intelligence (AI) device, or even a web site. The various electronic transaction devices 106 may be stationary in a fixed location or may be mobile.

[0044] For example, the consumer may wish to make an electronic transaction for payment of a house mortgage or automobile payment to their local bank. In one instance, the consumer may go to the local bank and use one of their automated devices to conduct the electronic transaction payment. Since the consumer is in physical proximity of the bank's electronic transaction device 106, a relatively short first predefined distance may be used during the transaction verification and authorization process. On the other hand, the consumer may log onto a website of the local bank. Here, a proxy location of the bank website may be used, and a location of the consumer's personal computer (such as their home) may be used to determine the distance between the consumer and the bank's web site. Here, a greater second predefined distance, selected based on the known characteristics of the bank's electronic transaction device 106, here the internet web site, to conduct the transaction verification and authorization process. Enhanced security for such example electronic

transactions is provided when various information used during the transaction verification and authorization process is securely stored in the consumer blockchain information 108 associated with that particular consumer.

[0045] In the various embodiments, any suitable currency type and/or currency denomination now known or later developed may be used. In some embodiments, the consumer may select which particular currency from a plurality of different currencies are to be used for all of, or a part of, the electronic transaction. For example, but not limited to, the transaction authorization system 100 may permit payment using bank funds available at a local or remote financial institution, foreign currency funds available at an overseas institution, an electronic payment system (such a PayPal or Google money), credit available from a financial organization (such as a credit card, home or personal equity line of credit, etc.) credits available from the vendor who is a participant in the electronic transaction, an electronic wallet or the like, or a form of crypto-currency, digital tokens, or the like.

[0046] FIGURE 5 is a map based version of a presented GUI 502. In such embodiments, the GUI 502 may be presented as a map or other geographic based graphic. The map may show current location 504 of the electronic mobile device 104, a location of the electronic transaction device 106 being used for the electronic transaction (shown as a red dot in the center of the circular secure zone), locations of other potential electronic transaction device that are within the secure zone that might be used by the consumer to conduct an electronic transaction (shown as a red dot), and the predefined secure zone 504. Here, the consumer will intuitively understand the nature of the predefined distance relative to their electronic mobile device 104 and the electronic transaction device 106. In some situations, the map information may prompt the consumer to change the value of the predefined distance.

[0047] FIGURE 6 is an example block diagram of an example computing system that may be used to practice embodiments of a electronic transaction verification system 102

described herein. Note that one or more general purpose virtual or physical computing systems suitably instructed or a special purpose computing system may be used to implement an electronic transaction verification system 102. Further, the electronic transaction verification system 102 may be implemented in software, hardware, firmware, or in some combination to achieve the capabilities described herein.

[0048] Note that one or more general purpose or special purpose computing systems/devices may be used to implement the described techniques. However, just because it is possible to implement the electronic transaction verification system 102 on a general purpose computing system does not mean that the techniques themselves or the operations required to implement the techniques are conventional or well known.

[0049] The computing system 600 may comprise one or more server and/or client computing systems and may span distributed locations. In addition, each block shown may represent one or more such blocks as appropriate to a specific embodiment or may be combined with other blocks. Moreover, the various blocks of the transaction authorization system 100 may physically reside on one or more machines, which use standard (*e.g.*, TCP/IP) or proprietary interprocess communication mechanisms to communicate with each other.

[0050] In the embodiment shown, computer system 600 comprises a computer memory ("memory") 601, a display 602, one or more Central Processing Units ("CPU") 603, Input/Output devices 604 (*e.g.*, keyboard, mouse, CRT or LCD display, etc.), other computer-readable media 605, and one or more network connections 606. The consumer blockchain information 108 is shown residing in memory 601. In other embodiments, some portion of the contents, some of, or all of the components of the electronic transaction verification system 102 may be stored on and/or transmitted over the other computer-readable media 607. The components of the electronic transaction verification system 102 preferably execute on one or more CPUs 603 and manage the transaction verification and

authorization process, as described herein. Other code or programs 607 and potentially other data repositories, such as data repository 608, also optionally reside in the memory 601, and preferably execute on one or more CPUs 603 (and/or processors 603a). Of note, one or more of the components in FIGURE 6 may not be present in any specific implementation. For example, some embodiments embedded in other software may not provide means for user input or display.

[0051] In a typical embodiment, the electronic transaction verification system 102 includes one or more engines or components 609-612 that concurrently manage a plurality of ongoing electronic transactions for a plurality of different consumers. In some embodiments, multiple engines are available to manage various functions during a transaction verification and authorization process. An example engine is a location determination engine 609 that receives location information for the electronic mobile device 104 and/or the electronic transaction device 106 for the determination of the respective locations. A distance comparison engine 610 manages the comparison of the distance between the electronic mobile device 104 and the electronic transaction device 106 with the predefined distance. A user identity information engine 611 manages confirmation of a consumer's identification during the transaction verification and authorization process. An authorization and notice engine 612 manages the authorization process one a valid electronic transaction has been identified, and/or generation of notifications to the consumer, such as if the electronic transaction has been authorized or denied. Embodiments may include other engines not described herein that manage other operations pertaining to the transaction verification and authorization process and/or that pertain to other functions occurring at the electronic transaction verification system 102.

[0052] In at least some embodiments, the electronic transaction devices 106 are external to the electronic transaction verification system 102 and are available, potentially, over one or more networks 110. Other and/or different modules may be implemented. In

addition, the electronic transaction verification system 102 may interact via the network 110 one or more third-party information provider systems 613, such as purveyors of information used in consumer blockchain information 108. Also, of note, the consumer blockchain information 108 may be provided external to the electronic transaction verification system 102 as well, for example in a distributed architecture at a plurality of devices or the like accessible over one or more networks 110.

[0053] In an example embodiment, components/modules of the electronic transaction verification system 102 are implemented using standard programming techniques. For example, the electronic transaction verification system 102 may be implemented as a "native" executable running on the CPU 603 (and/or the processor 603a), along with one or more static or dynamic libraries. In other embodiments, the electronic transaction verification system 102 may be implemented as instructions processed by a virtual machine. A range of programming languages known in the art may be employed for implementing such example embodiments, including representative implementations of various programming language paradigms, including but not limited to, object-oriented (*e.g.*, Java, C++, C#, Visual Basic.NET, Smalltalk, and the like), functional (*e.g.*, ML, Lisp, Scheme, and the like), procedural (*e.g.*, C, Pascal, Ada, Modula, and the like), scripting (*e.g.*, Perl, Ruby, Python, JavaScript, VBScript, and the like), and declarative (*e.g.*, SQL, Prolog, and the like).

[0054] The embodiments described above may also use well-known or proprietary, synchronous or asynchronous client-server computing techniques. Also, the various components may be implemented using more monolithic programming techniques, for example, as an executable running on a single CPU computer system, or alternatively decomposed using a variety of structuring techniques known in the art, including but not limited to, multiprogramming, multithreading, client-server, or peer-to-peer, running on one or more computer systems each having one or more CPUs. Some embodiments may execute concurrently and asynchronously and communicate using message passing techniques.

Equivalent synchronous embodiments are also supported. Also, other functions could be implemented and/or performed by each component/module, and in different orders, and in different components/modules, yet still achieve the described functions.

[0055] In addition, programming interfaces to the data stored as part of the electronic transaction verification system 102 (*e.g.*, in the data repositories 108) can be available by standard mechanisms such as through C, C++, C#, and Java APIs; libraries for accessing files, databases, or other data repositories; through scripting languages such as XML; or through Web servers, FTP servers, or other types of servers providing access to stored data. The electronic transaction verification system 102 may be implemented as one or more database systems, file systems, or any other technique for storing such information, or any combination of the above, including implementations using distributed computing techniques.

[0056] Also, the example electronic transaction verification system 102 may be implemented in a distributed environment comprising multiple, even heterogeneous, computer systems and networks. Different configurations and locations of programs and data are contemplated for use with techniques of described herein. In addition, the electronic transaction verification system 102 may be physical or virtual computing systems and may reside on the same physical system. Also, one or more of the modules may themselves be distributed, pooled or otherwise grouped, such as for load balancing, reliability or security reasons (such as the blockchain information 108). A variety of distributed computing techniques are appropriate for implementing the components of the illustrated embodiments in a distributed manner including but not limited to TCP/IP sockets, RPC, RMI, HTTP, Web Services (XML-RPC, JAX-RPC, SOAP, etc.) and the like. Other variations are possible. Also, other functionality could be provided by each component/module, or existing functionality could be distributed amongst the components/modules in different ways, yet still achieve the functions of the transaction verification system 102.

[0057] Furthermore, in some embodiments, some or all of the components of the electronic transaction verification system 102 may be implemented or provided in other manners, such as at least partially in firmware and/or hardware, including, but not limited to one or more application-specific integrated circuits (ASICs), standard integrated circuits, controllers executing appropriate instructions, and including microcontrollers and/or embedded controllers, field-programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), and the like. Some or all of the system components and/or data structures may also be stored as contents (*e.g.*, as executable or other machine-readable software instructions or structured data) on a computer-readable medium (*e.g.*, a hard disk; memory; network; other computer-readable medium; or other portable media article to be read by an appropriate drive or via an appropriate connection, such as a DVD or flash memory device) to enable the computer-readable medium to execute or otherwise use or provide the contents to perform at least some of the described techniques. Some or all of the components and/or data structures may be stored on tangible, non-transitory storage mediums. Some or all of the system components and data structures may also be stored as data signals (e.g., by being encoded as part of a carrier wave or included as part of an analog or digital propagated signal) on a variety of computer-readable transmission mediums, which are then transmitted, including across wireless-based and wired/cable-based mediums, and may take a variety of forms (e.g., as part of a single or multiplexed analog signal, or as multiple discrete digital packets or frames). Such computer program products may also take other forms in other embodiments. Accordingly, embodiments of this disclosure may be practiced with other computer system configurations.

[0058] Exhibit I is an example business environment that utilizes one or more of the embodiments of the transaction authorization system 100. Embodiments of the transaction authorization system 100 are envisioned to be used by a limitless number of different types of transactional systems now known or later developed.

[0059] Exhibit II is a conceptual operational scenario of a non-limiting embodiment of the transaction authorization system 100. An image of a map-based GUI is conceptually illustrated in Exhibit II.

[0060] It should be emphasized that the above-described embodiments of the transaction authorization system 100 are merely possible examples of implementations of the invention. Many variations and modifications may be made to the above-described embodiments. All such modifications and variations are intended to be included herein within the scope of this disclosure and protected by the following claims.

Claims:

1. A method for electronic transaction verification and authorization, the method comprising:

determining location of a personal electronic device of a consumer during an electronic transaction;

determining location of an electronic transaction device that the consumer is using to conduct the electronic transaction;

determining a distance between the personal electronic device of the consumer and the electronic transaction device;

comparing the determined distance with a predefined distance; and

verifying and authorizing the electronic transaction when the determined distance less than or equal to the predefined distance.

2. The method of Claim 1, wherein the predefined distance is accessed from consumer blockchain information that is uniquely associated with the consumer.

APPARATUS, SYSTEMS AND METHODS FOR AUTHORIZATION OF ELECTRONIC TRANSACTIONS BASED ON SECURED ZONES

ABSTRACT OF THE DISCLOSURE

Electronic transaction systems and methods are operable to conduct transaction verification and authorization process for an electronic transaction. An exemplary embodiment determines location of a personal electronic device of a consumer during an electronic transaction; determines location of an electronic transaction device that the consumer is using to conduct the electronic transaction; determines a distance between the personal electronic device of the consumer and the electronic transaction device; compares the determined distance with a predefined distance; and verifies and authorizes the electronic transaction when the determined distance less than or equal to the predefined distance.