

STORAGE AND COMMUNICATION ENVIRONMENT FOR CRYPTOGRAPHIC TAGS

Technical Field

[0001] The present invention relates to storing data via a blockchain, and more particularly, to a mechanism for securely delivering readable tag data associated with a physical object to a remotely located blockchain.

Background

[0002] A centralized database stores and maintains data in a single database (e.g., a database server) at one location. This location is often a central computer, for example, a desktop central processing unit (CPU), a server CPU, or a mainframe computer. Information stored on a centralized database is typically accessible from multiple different points. Multiple users or client workstations can work simultaneously on the centralized database, for example, based on a client/server configuration. A centralized database is easy to manage, maintain, and control, especially for purposes of security because of its single location. Within a centralized database, data redundancy is minimized as a single storing place of all data also implies that a given set of data only has one primary record.

[0003] Meanwhile, blockchain systems store data on an immutable ledger, provide distributed and decentralized access to the immutable ledger through non-trusting participants, establish consensus requirements for agreement between the non-trusting participants such that no one entity can change the immutable ledger without agreement from others, invoke smart contracts, and the like. A blockchain is formed by a network of participants which agree to add a block (with data stored therein) to the immutable ledger. Before being added, the block is linked to a previous block on the immutable ledger thereby forming a chain. This immutable and incorruptible nature of blockchain makes it safe from falsified information and hacks. The decentralized nature also gives it the unique quality of being trustless, in that parties do not need to establish trust before they can transact safely.

Summary

[0004] Viewed from a first aspect, the present invention provides an apparatus comprising: a network interface configured to receive tag data that is read from a tag associated with a physical object and signed with a key assigned to the tag; a processor configured to determine that the signed tag data is validly signed based on a corresponding key pair of the tag which is accessible to the blockchain peer, and determine, via the blockchain peer, whether the decrypted tag data satisfies one or more predefined conditions of the physical object; and a storage configured to store the determination via a blockchain database.

[0005] Preferably, the present invention provides an apparatus wherein the tag data comprises sensor data that is sensed by one or more sensor devices that are coupled to the tag.

[0006] Preferably, the present invention provides an apparatus wherein the sensor data comprises a value of one or more of temperature, location, fluid flow rate, pH, velocity, acceleration, viscosity, illumination, spectral measurements, image, pressure, vibration, gravitational forces, and rotational speed.

[0007] Preferably, the present invention provides an apparatus wherein the processor is further configured to verify the authenticity of the tag based on a sensor identifier that is included within the tag data.

[0008] Preferably, the present invention provides an apparatus wherein the processor is configured to determine whether the tag data violates one or more predefined conditions embedded within logic of a chaincode that runs on the blockchain peer.

[0009] Preferably, the present invention provides an apparatus wherein the network interface is further configured to transmit, via chaincode that runs on the blockchain peer, an alert to a computer device associated with the physical object.

[0010] Preferably, the present invention provides an apparatus wherein the tag data is further signed by a key assigned to the reader, and the processor is further configured to determine that the signed tag data is validly signed based on a corresponding key pair of the reader which is accessible to the blockchain peer.

[0011] Preferably, the present invention provides an apparatus wherein the processor is configured to store an identifier of the tag and the tag data as a key-value pair in a state database of the blockchain.

[0012] Viewed from another aspect, the present invention provides a method comprising: retrieving sensor data from one or more hardware sensors coupled to a tag and storing the sensor data within a memory of the tag; receiving a read request from a reader associated with a blockchain platform; verifying the authenticity of the blockchain platform based on handshake protocol between the tag and the blockchain via the reader; and in response to a successful verification of the blockchain platform, signing the sensor data based on a private key of the tag, and transmitting the signed sensor data to the reader.

[0013] Preferably, the present invention provides a method further comprising checking, via a bootloader on the tag, the integrity of software running on the tag during a power up of the tag.

[0014] Preferably, the present invention provides a method wherein the verifying the authenticity of the blockchain platform comprises receiving data signed by the blockchain platform, and verifying the signed data based on a corresponding key of the blockchain platform stored by the tag.

[0015] Preferably, the present invention provides a method further comprising verifying, by the tag, the authenticity of the reader based on a handshake protocol with the reader.

[0016] Preferably, the present invention provides a method further comprising performing a key exchange with the blockchain platform to establish a shared key between the tag and the blockchain platform.

[0017] Preferably, the present invention provides a method wherein the signing of the sensor data further comprises encrypting the sensor data based on the shared key with the blockchain platform prior to transmitting the signed sensor data to the reader.

[0018] Preferably, the present invention provides a method further comprising detecting, via the tag, that a data violation has occurred based on values of the sensor data retrieved from the one or more hardware sensors and storing the data violation within the memory.

[0019] Preferably, the present invention provides a method wherein the memory of the tag is read and write protected thereby preventing the private key from being read or modified by an external entity.

[0020] Viewed from another aspect, the present invention provides a method comprising: receiving, via a network, tag data that is read from a tag associated with a physical object and signed with a key assigned to the tag; determining, via a blockchain peer, that the signed tag data is validly signed based on a corresponding key pair of the tag which is accessible to the blockchain peer; determining, via the blockchain peer, whether the tag data satisfies one or more predefined conditions of the physical object; and storing the determination via a blockchain database.

[0021] Preferably, the present invention provides a method further comprising verifying the authenticity of the tag based on a sensor identifier included within the tag data.

[0022] Preferably, the present invention provides a method wherein the determining comprises determining whether the tag data violates one or more predefined conditions embedded within logic of a chaincode running on the blockchain peer.

[0023] Preferably, the present invention provides a method further comprising transmitting, via chaincode running on the blockchain peer, an alert to a computing device associated with the physical object.

Brief Description of the Drawings

[0024] FIG. 1 is a diagram illustrating a storage and communication environment between a tag and a blockchain according to example embodiments.

[0025] FIG. 2A is a diagram illustrating an example blockchain architecture configuration, according to example embodiments.

[0026] FIG. 2B is a diagram illustrating a blockchain transactional flow among nodes, according to example embodiments.

[0027] FIG. 3A is a diagram illustrating a permissioned network, according to example embodiments.

[0028] FIG. 3B is a diagram illustrating another permissioned network, according to example embodiments.

[0029] FIG. 3C is a diagram illustrating a permissionless network, according to example embodiments.

[0030] FIG. 4A is a diagram illustrating a process of tag data being read at different locations of a supply chain according to example embodiments.

[0031] FIG. 4B is a diagram illustrating a process of storing tag data to a blockchain ledger according to example embodiments.

[0032] FIG. 4C is a diagram illustrating a user interface which displays tag data associated with a physical object according to example embodiments.

[0033] FIG. 5A is a diagram illustrating a method of receiving tag data according to example embodiments.

[0034] FIG. 5B is a diagram illustrating a method of transmitting tag data according to example embodiments.

[0035] FIG. 6A is a diagram illustrating an example system configured to perform one or more operations described herein, according to example embodiments.

[0036] FIG. 6B is a diagram illustrating another example system configured to perform one or more operations described herein, according to example embodiments.

[0037] FIG. 6C is a diagram illustrating a further example system configured to utilize a smart contract, according to example embodiments.

[0038] FIG. 6D is a diagram illustrating yet another example system configured to utilize a blockchain, according to example embodiments.

[0039] FIG. 7A is a diagram illustrating a process of a new block being added to a distributed ledger, according to example embodiments.

[0040] FIG. 7B is a diagram illustrating data contents of a new data block, according to example embodiments.

[0041] FIG. 7C is a diagram illustrating a blockchain for digital content, according to example embodiments.

[0042] FIG. 7D is a diagram illustrating a block which may represent the structure of blocks in the blockchain, according to example embodiments.

[0043] FIG. 8A is a diagram illustrating an example blockchain which stores machine learning (artificial intelligence) data, according to example embodiments.

[0044] FIG. 8B is a diagram illustrating an example quantum-secure blockchain, according to example embodiments.

[0045] FIG. 9 is a diagram illustrating an example system that supports one or more of the example embodiments.

Detailed Description

[0046] It will be readily understood that the instant components, as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations. Thus, the following detailed description of the embodiments of at least one of a method, apparatus, non-transitory computer readable medium and system, as represented in the attached figures, is not intended to limit the scope of the application as claimed but is merely representative of selected embodiments.

[0047] The instant features, structures, or characteristics as described throughout this specification may be combined or removed in any suitable manner in one or more embodiments. For example, the usage of the phrases "example embodiments", "some embodiments", or other similar language, throughout this specification refers to the fact that a particular feature, structure, or characteristic described in connection with the embodiment may be included in at least one embodiment. Thus, appearances of the phrases "example embodiments", "in some embodiments", "in other embodiments", or other similar language, throughout this specification do not necessarily all refer to the same group of embodiments, and the described features, structures, or characteristics may be combined or removed in any suitable manner in one or more embodiments. Further, in the diagrams, any connection between elements can permit one-way and/or two-way communication even if the depicted connection is a one-way or two-way arrow. Also, any device depicted in the drawings can be a different device. For example, if a mobile device is shown sending information, a wired device could also be used to send the information.

[0048] In addition, while the term "message" may have been used in the description of embodiments, the application may be applied to many types of networks and data. Furthermore, while certain types of connections, messages, and signaling may be depicted in exemplary embodiments, the application is not limited to a certain type of connection, message, and signaling.

[0049] Example embodiments provide methods, systems, components, non-transitory computer readable media, devices, and/or networks, which extend the trust, security, and immutability of blockchain to the physical world.

[0050] In one embodiment the application utilizes a decentralized database (such as a blockchain) that is a distributed storage system, which includes multiple nodes that communicate with each other. The decentralized database includes an append-only immutable data structure resembling a distributed ledger capable of maintaining records between mutually untrusted parties. The untrusted parties are referred to herein as peers or peer nodes. Each peer maintains a copy of the database records and no single peer can modify the database records without a consensus being reached among the distributed peers. For example, the peers may execute a consensus protocol to validate blockchain storage transactions, group the storage transactions into blocks, and build a hash chain over the blocks. This process forms the ledger by ordering the storage transactions, as is necessary, for consistency. In various embodiments, a permissioned and/or a permissionless blockchain can be used. In a public or permissionless blockchain, anyone can participate without a specific identity. Public blockchains can involve native cryptocurrency and use consensus based on various protocols such as Proof of Work (PoW). On the other hand, a permissioned blockchain database provides secure interactions among a group of entities which share a common goal but which do not fully trust one another, such as businesses that exchange funds, goods, information, and the like.

[0051] This application can utilize a blockchain that operates arbitrary, programmable logic, tailored to a decentralized storage scheme and referred to as "smart contracts" or "chaincodes." In some cases, specialized chaincodes may exist for management functions and parameters which are referred to as system chaincode. The application can further utilize smart contracts that are trusted distributed applications which leverage tamper-proof properties of the blockchain database and an underlying agreement between nodes, which is referred to as an endorsement or endorsement policy. Blockchain transactions associated with this application can be "endorsed" before being committed to the blockchain while transactions which are not endorsed, are disregarded. An endorsement policy allows chaincode to specify endorsers for a transaction in the form of a set of peer nodes that are necessary for endorsement. When a client sends the transaction to the peers specified in the endorsement policy, the transaction is executed to validate the transaction. After validation, the transactions enter an ordering phase in which a consensus protocol is used to produce an ordered sequence of endorsed transactions grouped into blocks.

[0052] This application can utilize nodes that are the communication entities of the blockchain system. A "node" may perform a logical function in the sense that multiple nodes of different types can run on the same physical server. Nodes are grouped in trust domains and are associated with logical entities that control them in various ways. Nodes may include different types, such as a client or submitting-client node which submits a transaction-invocation to an endorser (e.g., peer), and broadcasts transaction-proposals to an ordering service (e.g., ordering node). Another type of node is a peer node which can receive client submitted transactions, commit the transactions and maintain a state and a copy of the ledger of blockchain transactions. Peers can also have the role of an endorser, although it is not a requirement. An ordering-service-node or orderer is a node running the

communication service for all nodes, and which implements a delivery guarantee, such as a broadcast to each of the peer nodes in the system when committing transactions and modifying a world state of the blockchain, which is another name for the initial blockchain transaction which normally includes control and setup information.

[0053] This application can utilize a ledger that is a sequenced, tamper-resistant record of all state transitions of a blockchain. State transitions may result from chaincode invocations (i.e., transactions) submitted by participating parties (e.g., client nodes, ordering nodes, endorser nodes, peer nodes, etc.). Each participating party (such as a peer node) can maintain a copy of the ledger. A transaction may result in a set of asset key-value pairs being committed to the ledger as one or more operands, such as creates, updates, deletes, and the like. The ledger includes a blockchain (also referred to as a chain) which is used to store an immutable, sequenced record in blocks. The ledger also includes a state database which maintains a current state of the blockchain.

[0054] This application can utilize a chain that is a transaction log which is structured as hash-linked blocks, and each block contains a sequence of N transactions where N is equal to or greater than one. The block header includes a hash of the block's transactions, as well as a hash of the prior block's header. In this way, all transactions on the ledger may be sequenced and cryptographically linked together. Accordingly, it is not possible to tamper with the ledger data without breaking the hash links. A hash of a most recently added blockchain block represents every transaction on the chain that has come before it, making it possible to ensure that all peer nodes are in a consistent and trusted state. The chain may be stored on a peer node file system (i.e., local, attached storage, cloud, etc.), efficiently supporting the append-only nature of the blockchain workload.

[0055] The current state of the immutable ledger represents the latest values for all keys that are included in the chain transaction log. Since the current state represents the latest key values known to a channel, it is sometimes referred to as a world state. Chaincode invocations execute transactions against the current state data of the ledger. To make these chaincode interactions efficient, the latest values of the keys may be stored in a state database. According to various embodiments, the state database of the blockchain ledger is a key-value store (KVS). The state database may be simply an indexed view into the chain's transaction log, it can therefore be regenerated from the chain at any time. The state database may automatically be recovered (or generated if needed) upon peer node startup, and before transactions are accepted.

[0056] Blockchain technology enables sharing of data among multiple parties through a secure, immutable, distributed ledger with verifiable provenance and attribution. Blockchain systems may be incorporated with existing industries including food safety, maritime shipments, supply chain, Internet of Things (IoT), diamond tracking, and the like. In related blockchain systems, to access the blockchain, a system usually provides input methods that operate through external sources that may include enterprise software, scanning of physical documents, integration within existing devices that lack security, and human input. However, these input methods fail to provide the same

level of trust and security that is implemented by the blockchain network. The most vulnerable input sources are those that rely on human input or insecure devices.

[0057] Therefore, in order for blockchain to be securely extended to the physical world, the security and communication must be as secure as the blockchain itself. Radio frequency identification (RFID) systems provide one such channel to the physical world. RFID tags can be attached to a physical asset or in a surrounding environment of an asset (e.g., a pallet, a car, a truck, a storage area, etc.). However, RFID tags can be cloned fairly easily. Furthermore, the RF channel on which RFID tags communicate can be intercepted easily because such tags tend to rely on simple password based schemes for authentication.

[0058] The example embodiments are directed to a tag-based communication environment which overcomes the drawbacks of the previous tag-based systems by extending a blockchain to a tag that is attached to or about a physical asset. Accordingly, a chain of trust may be established between a tag, a reader, and a blockchain. The tag may include a private key that is embedded (written) within a secure memory of the tag and inaccessible to external entities. Meanwhile, a corresponding public key of the private key may be stored at the blockchain network, for example, on a blockchain ledger, a blockchain storage, or the like. Every tag may be provisioned with a private key and then registered into the blockchain. When the tag sends data to the blockchain, the tag may sign the data with its private key. The blockchain may then use the corresponding public key to verify the tag's signature and likewise verify the authenticity of the tag's data.

[0059] A secure executable program may be loaded into the tag which includes instructions for responding to requests from readers of the tag. The readers that relay information from the tag to the blockchain may be trusted or untrusted. If the readers are trusted, they may include a private key stored therein having a corresponding public key stored by the blockchain. The trusted readers may also sign the tag data thereby creating an additional layer of security. Furthermore, the blockchain may store a corresponding public key of the reader to thereby verify that the reader's signature is valid.

[0060] The tag may be a programmable computer system with a secure hardware root of trust. The tag may include a network interface (e.g., RFID in one embodiment, etc.), a wireless antenna, a battery, etc. The tag may also include one or more communication interfaces (e.g., Bluetooth, etc.), which enable the tag to electrically couple with one or more sensor devices. Thus, it is possible for the tag to wake up and capture sensor data at periodic stages from a sensor that is coupled thereto.

[0061] In some embodiments, the tag may be provisioned with a key from a blockchain certificate authority (CA), however, embodiments are not limited thereto. In some embodiments, the CA may be used to reduce a storage load on tag and/or the blockchain. The private key may be stored within a protectible non-volatile memory

of the tag via an external system using a communications interface such as RFID, Bluetooth (wireless) or a port (wired). In addition, once the tag is provisioned, the external system may protect memory locations where the private key is stored to prevent the private key from being accessed or overwritten. Furthermore, the hardware of the tag can be controlled so that only a program running with special privileges on the hardware can access the private key. An example of such a program is a bootloader that loads when the tag is powered up. The bootloader can also enable hardware protection schemes so that no subsequent code can ever be run on the hardware. The bootloader may also protect access ports and prevent a debugger from read and write access to the memory and CPU of the tag.

[0062] The bootloader may start each time the tag begins to power up. Here, the bootloader may check the integrity of the software application running on the tag. This check may be performed each time the tag is powered on. For example, the bootloader may check a CRC of the application image each time the tag boots up to verify the integrity of the application. The bootloader may also be updated through a device firmware update signed with a secret key. The update may make the application code permanent to the tag.

[0063] The tag may be provisioned with a private key that has a corresponding public key stored by the blockchain. Here, the private key may be used by the tag to sign tag data while the corresponding public key stored on the blockchain may be used to verify the signed tag data. Accordingly, the tag may send tag data and a digital signature which is based on the tag data to the blockchain. The tag may perform key exchange using Elliptic Curve Diffie Hellman (ECDH), or the like. Following the key exchange, the tag can use the generated shared key to encrypt the tag data using an algorithm like AES, or the like, and store the encrypted data on the blockchain where it can be decrypted by the blockchain, for example, automatically or when one or more conditions are met.

[0064] To create the digital signature, the tag may create a one-way hash of the electronic tag data to be signed. The private key may be used to generate the hash using an algorithm like Elliptic Curve Digital Signature Algorithm (ECDSA), or the like. The hash is the digital signature. The hash may be encrypted instead of the entire tag data because the hash can convert an arbitrary-sized input into a fixed length value which is usually much shorter than the original tag data. The value of the hash is unique to the hash data. The blockchain may use a public key (that corresponds to the tag's private key) to verify that the signature is indeed corresponding to the tag data, and that it was indeed generated using the correct private key. For example, the blockchain may use an ECDSA signature verification algorithm. This ensures that the tag data is authenticated and not tampered with.

[0065] The tag may respond to queries from a RFID reader. For example, the tag could be a "smart" tag. When the tag is queried by a RFID reader, the tag may respond with a request for a verifiable signature and identifier of the RFID reader. Here, the tag may store corresponding public keys of associated RFID readers. When the RFID reader responds with its identifier (which may be hashed using the RFID reader's private key), the tag may verify

the private key based on the corresponding public key to verify the integrity of the RFID reader. Furthermore, the tag may provide sensor data, a tag serial number, and the like, which are encrypted by the tag using an encryption key (e.g., after ECDH key exchange, etc.). The RFID reader may relay this data (by decrypting first, and then re-encrypting with a shared key between the RFID reader and the blockchain) tag data to the blockchain via a wireless protocol such as Wi-Fi, Bluetooth (if short range), and the like. The RFID reader may also add additional data from any sensors that the reader is attached to, for example, from a positional sensor that provides its location. An authorized RFID reader will be able to decrypt the tag data. Otherwise, the RFID reader just works as a relay between the tag and the blockchain. When the RFID reader works as a relay, the ECDH key exchange is between the tag and the blockchain server and the encrypted tag data is sent from tag to server without the RFID reader decrypting it in between. In this case, the tag also verifies the integrity of the blockchain server by using the stored public key of the server, in a similar way to what is described for the verification of the RFID reader above.

[0066] One example use case for this system is a supply chain. Each entity (e.g., manufacturer, distributor, transporter, retailer, etc.) may be connected to the blockchain and required to capture tag data at various points in the supply chain. Meanwhile, the tag may be electrically coupled to sensors which the tag causes to sense information periodically (e.g., every 10 minutes, etc.). For example, a tag may be coupled to a thermometer which captures a temperature reading every 10 minutes that is then stored by the tag. When the tag is read by a reader, the tag may sign the sensor data with its private key and provide it to the reader. The tag may also encrypt the data with a shared key generated with ECDH, or the like, between the tag and the reader or the tag and a blockchain server. The sensor data may be fed to the blockchain for further analysis. In some embodiments, the sensor data may also be used to further authenticate the tag. For example, a sensor identifier, geographic location, etc., may be provided by the tag as well to verify that the tag is in communication with a predefined sensor.

[0067] Some of the benefits of the example embodiments include extending the security of a blockchain to a physical environment where the tag is located. The private key embedded within the tag may allow the tag to uniquely sign all data being sent from the tag to the blockchain. Furthermore, additional data may be provided by the tag (e.g., sensor ID, sensor data, geolocation, etc.) which can be used to further verify the authenticity of the tag, and thus the object to which the tag is attached. The blockchain may have the public key for the tag. As another example, secure readers may also have the public key enabling the readers to verify the tag signature as well.

[0068] In the example embodiments, a blockchain may be used as a means of providing back-end storage for the tag data. However, the embodiments are not limited thereto. It should be appreciated that the storage may include any trusted system such as a secure server, a secure database, or the like.

[0069] FIG. 1 illustrates a storage and communication environment 100 between a tag 110 and a blockchain 130 according to example embodiments. Referring to FIG. 1, the blockchain 130 is distributed among a plurality of blockchain peers which each store a copy of the blockchain ledger. The blockchain peers may participate in endorsement of transactions as well. New blocks may be added to the blockchain 130 by an orderer node (not shown) that communicates with the blockchain peers within a secure network (blockchain network).

[0070] The tag 110 may include an antenna 111 for wireless radio frequency communication with a reader 120 which has a corresponding antenna 121. The tag 110 further includes a communication interface 112 which enables the tag 110 to couple to a sensor 115. Here, the communication interface 112 may include a wired/port, a Bluetooth interface, RFID interface, NFC interface, or the like. Accordingly, the tag 110 and the sensor 115 may be electronically coupled, optically coupled, coupled via radio frequency, and the like. The sensor 115 may include a thermometer, a speedometer, a global-positioning system, an accelerometer, a flow meter, a hygrometer, a pressure sensor, and/or the like. The sensor 115 may include multiple different types of sensors (e.g., two or more types of sensors). Also, it should be appreciated that the type of sensors may be of a different type than those specifically listed.

[0071] For example, the tag 110 may wake up periodically (e.g., every 5 minutes) and request a reading from the sensor 115 via the communication interface 112. The sensor reading may be stored in a memory of the tag 110 that includes a list of sensor readings. Furthermore, when the tag 110 is read by the reader 120, the tag 110 may transmit the list of readings from the sensor 115 that have been collected since a most recent reading by the reader 120. The tag may also send processed information on the sensor data, for example, min and max temperature readings and corresponding time stamps, or the number of people in a room after image processing on a camera image. The tag 110 may sign the sensor data with its private key. The tag may also encrypt the sensor data. Also, the tag may send a serial number (ID) of the tag, a geographic location, a timestamp, and the like.

[0072] Prior to transmitting data to the reader 120, the tag 110 may first verify that the reader 120 is a valid reader using a handshake protocol. For example, the tag 110 may store a list of public keys corresponding to one or more readers. The tag 110 may query the reader 120 for its private key (or data signed by the reader 120 with the reader's private key). The reader 120 may provide the signed data to the tag 110. If the signature verification is successful, the tag 110 may determine that the reader 120 is a valid reader.

[0073] In some embodiments, ECDH may be used to calculate a secret key (session key) for encryption and hashing. The shared secret may be the key used for hashing or may be used to derive the key. For example, the tag 110 may establish an AES encryption key with the blockchain network hosting the blockchain 130. The encrypted tag data may be stored on the blockchain 130 and decrypted by a smart contract or blockchain application and made available to other applications such as analytics, etc.

[0074] The tag 110 may support various security algorithms such as AES, SHA256, and ECDSA. An external system may program a private key in a section of memory within the tag 110 that can be finalized permanently, ensuring that the private key cannot be changed once it has been stored on the tag 110. Further, an initial code running in a processor of the tag 110 can be configured so that the private key written into the tag 110 cannot be read by any unprivileged code that is running on the processor. These features ensure that the tag 110 cannot be cloned. The tag 110 may also support different communication protocols such as NFC, RFID, and Bluetooth Low Energy Profile (BLE), wired interfaces such as I2C, SPI, or other standard or proprietary interfaces, thereby providing flexibility for coupling sensors and readers to the tag 110.

[0075] In the example embodiments, the blockchain 130 stores the corresponding public key of the tag's private key, and the tag 110 is protected from being cloned and/or overwritten. Accordingly, a chain of trust is created between the tag 110 to the blockchain 130. It is not necessary that the reader 120 also be a trusted reader. However, the example embodiments may include both situations. In one example, the reader 120 may include its own private key for signing the tag data read from the tag 110. Accordingly, the reader 120 may separately sign the tag data thereby verifying the authenticity of the reader 120. If the reader 120 is not trusted, the reader 120 may simply act as a pass through device and relay the tag data to the blockchain 130 or other intermediate node.

[0076] The blockchain 130 stores the tag data received from the tag 110. The data can be made available by a blockchain peer 132 which includes smart contracts (deployed as chaincode on the blockchain peer 132), blockchain applications, and the like. For example, the tag data may be provided to analytic applications, smart contracts, payment processes, and other business process software.

[0077] In some embodiments, a certificate authority 140 may be used to reduce a storage load on the tag 110 and also generate keys that are assigned to the tag 110, the reader 120, and the blockchain 130. In this example, the certificate authority 140 may store blockchain public keys which the tag 110 can retrieve when needed, and then delete after use. Likewise, the blockchain 130 can retrieve public keys of tags (including the tag 110) from the certificate authority 140, when needed. In this alternative arrangement, there may also be one or more intermediate certificate authorities (not shown) between the tag 110 and the certificate authority 140, and the blockchain 130 and the certificate authority 140. In this example, the intermediate certificate authority can respond to requests from the tag 110 as well as the certificate authority 140 therefore requests do not bottleneck at the certificate authority 140. Furthermore, the intermediate certificate authority may sign the responses to the requests with its own signature.

[0078] In this alternative example, the reader 120 may query the tag 110. The tag 110 may identify itself (ID) and generate a random message that requests a signed message from a source it can trust. In this example, the reader 120 may be an untrusted reader, so it then forwards the request to the blockchain 130. If the blockchain node / server has a master private key (the corresponding public key of the tag 110), the blockchain server may

sign the message and also create a challenge for the tag 110 to authenticate itself. However, if the blockchain server does not have the private key, it can request the certificate authority 140 to sign the message. The certificate authority 140 is assumed to be trusted by the blockchain 130 in this example.

[0079] In this example, the blockchain server may have access to the public key of the tag via a consensus mechanism with the rest of the blockchain 130. The signed message may be sent to the tag 110 which can verify the authenticity of the server because the tag has access to the public key of the certificate authority 140. The tag 110 may also sign the challenge sent by the blockchain server and send it to the server which can verify the signature because it has the public key of the tag 110. The blockchain server can also send its own public key (signed by the certificate authority 140) to the tag 110. In this example, the blockchain server (authenticated by the certificate authority 140 and verified by the tag 110) and the tag 110 (verified by the blockchain server) can communicate with messages signed by their respective private keys. The blockchain server and tag 110 can also perform ECDH and generate a symmetric session key for encryption of the data. At the end of the session (or a timeout, or a specified number of uses), the tag 110 can delete the symmetric session key and / or the public key of the server.

[0080] An alternate mechanism may include that the tag 110 stores the public keys of some of the blockchain servers (e.g., a small subset that is determined via consensus between the servers). In this case, when the tag 110 requests authentication of the blockchain server, the server can request one of its peers to provide a signature. In this example, there is no need for a "certificate authority" since it is now distributed within the network. This differentiation is potentially that of a permissioned blockchain versus a public blockchain. Additionally, the protocol may include a mechanism to update the set of public keys that are trusted. In both the CA and consensus approaches above, the protocol to update trusted keys can be done. For example, the tag 110 may request authentication from two or more of the trusted sources to initiate key updates in order to make it harder to break, and so that a single bad actor cannot break it.

[0081] FIG. 2A illustrates a blockchain architecture configuration 200, according to example embodiments. Referring to FIG. 2A, the blockchain architecture 200 may include certain blockchain elements, for example, a group of blockchain nodes 202. The blockchain nodes 202 may include one or more nodes 204-210 (these four nodes are depicted by example only). These nodes participate in a number of activities, such as blockchain transaction addition and validation process (consensus). One or more of the blockchain nodes 204-210 may endorse transactions based on endorsement policy and may provide an ordering service for all blockchain nodes in the architecture 200. A blockchain node may initiate a blockchain authentication and seek to write to a blockchain immutable ledger stored in blockchain layer 216, a copy of which may also be stored on the underpinning physical infrastructure 214. The blockchain configuration may include one or more applications 224 which are linked to application programming interfaces (APIs) 222 to access and execute stored program/application code 220 (e.g.,

chaincode, smart contracts, etc.) which can be created according to a customized configuration sought by participants and can maintain their own state, control their own assets, and receive external information. This can be deployed as a transaction and installed, via appending to the distributed ledger, on all blockchain nodes 204-210.

[0082] The blockchain base or platform 212 may include various layers of blockchain data, services (e.g., cryptographic trust services, virtual execution environment, etc.), and underpinning physical computer infrastructure that may be used to receive and store new transactions and provide access to auditors which are seeking to access data entries. The blockchain layer 216 may expose an interface that provides access to the virtual execution environment necessary to process the program code and engage the physical infrastructure 214. Cryptographic trust services 218 may be used to verify transactions such as asset exchange transactions and keep information private.

[0083] The blockchain architecture configuration of FIG. 2A may process and execute program/application code 220 via one or more interfaces exposed, and services provided, by blockchain platform 212. The code 220 may control blockchain assets. For example, the code 220 can store and transfer data, and may be executed by nodes 204-210 in the form of a smart contract and associated chaincode with conditions or other code elements subject to its execution. As a non-limiting example, smart contracts may be created to execute reminders, updates, and/or other notifications subject to the changes, updates, etc. The smart contracts can themselves be used to identify rules associated with authorization and access requirements and usage of the ledger. For example, the smart contract (or chaincode executing the logic of the smart contract) may read blockchain data 226 which may be processed by one or more processing entities (e.g., virtual machines) included in the blockchain layer 216 to generate results 228 including alerts, determining liability, and the like, within a complex service scenario. The physical infrastructure 214 may be utilized to retrieve any of the data or information described herein.

[0084] A smart contract may be created via a high-level application and programming language, and then written to a block in the blockchain. The smart contract may include executable code which is registered, stored, and/or replicated with a blockchain (e.g., distributed network of blockchain peers). A transaction is an execution of the smart contract code which can be performed in response to conditions associated with the smart contract being satisfied. The executing of the smart contract may trigger a trusted modification(s) to a state of a digital blockchain ledger. The modification(s) to the blockchain ledger caused by the smart contract execution may be automatically replicated throughout the distributed network of blockchain peers through one or more consensus protocols.

[0085] The smart contract may write data to the blockchain in the format of key-value pairs. Furthermore, the smart contract code can read the values stored in a blockchain and use them in application operations. The smart contract code can write the output of various logic operations into one or more blocks within the blockchain. The

code may be used to create a temporary data structure in a virtual machine or other computing platform. Data written to the blockchain can be public and/or can be encrypted and maintained as private. The temporary data that is used/generated by the smart contract is held in memory by the supplied execution environment, then deleted once the data needed for the blockchain is identified.

[0086] A chaincode may include the code interpretation (e.g., the logic) of a smart contract. For example, the chaincode may include a packaged and deployable version of the logic within the smart contract. As described herein, the chaincode may be program code deployed on a computing network, where it is executed and validated by chain validators together during a consensus process. The chaincode may receive a hash and retrieve from the blockchain a hash associated with the data template created by use of a previously stored feature extractor. If the hashes of the hash identifier and the hash created from the stored identifier template data match, then the chaincode sends an authorization key to the requested service. The chaincode may write to the blockchain data associated with the cryptographic details.

[0087] FIG. 2B illustrates an example of a blockchain transactional flow 250 between nodes of the blockchain in accordance with an example embodiment. Referring to FIG. 2B, the transaction flow may include a client node 260 transmitting a transaction proposal 291 to an endorsing peer node 281. The endorsing peer 281 may verify the client signature within the transaction proposal 291 and execute a chaincode function to initiate the transaction. The output may include the chaincode results, a set of key/value versions that were read in the chaincode (read set), and the set of keys/values that were written in chaincode (write set). Here, the endorsing peer 281 may determine whether or not to endorse the transaction proposal. The proposal response 292 is sent back to the client 260 along with an endorsement signature, if approved. The client 260 assembles the endorsements into a transaction payload 293 and broadcasts it to an ordering service node 284. The ordering service node 284 then delivers ordered transactions as blocks to all peers 281-283 on a channel. Before committal to the blockchain, each peer 281-283 may validate the transaction. For example, the peers may check the endorsement policy to ensure that the correct allotment of the specified peers have signed the results and authenticated the signatures against the transaction payload 293.

[0088] Referring again to FIG. 2B, the client node initiates the transaction 291 by constructing and sending a request to the peer node 281, which is an endorser. The client 260 may include an application leveraging a supported software development kit (SDK), which utilizes an available API to generate a transaction proposal. The proposal is a request to invoke a chaincode function so that data can be read and/or written to the ledger (i.e., write new key value pairs for the assets). The SDK may serve as a shim to package the transaction proposal into a properly architected format (e.g., protocol buffer over a remote procedure call (RPC)) and take the client's cryptographic credentials to produce a unique signature for the transaction proposal.

[0089] In response, the endorsing peer node 281 may verify (a) that the transaction proposal is well formed, (b) the transaction has not been submitted already in the past (replay-attack protection), (c) the signature is valid, and (d) that the submitter (client 260, in the example) is properly authorized to perform the proposed operation on that channel. The endorsing peer node 281 may take the transaction proposal inputs as arguments to the invoked chaincode function. The chaincode is then executed against a current state database to produce transaction results including a response value, read set, and write set. However, no updates are made to the ledger at this point. In 292, the set of values, along with the endorsing peer node's 281 signature is passed back as a proposal response to the SDK of the client 260 which parses the payload for the application to consume.

[0090] In response, the application of the client 260 inspects/verifies the endorsing peers signatures and compares the proposal responses to determine if the proposal response is the same. If the chaincode only queried the ledger, the application would inspect the query response and would typically not submit the transaction to the ordering node service 284. If the client application intends to submit the transaction to the ordering node service 284 to update the ledger, the application determines if the specified endorsement policy has been fulfilled before submitting (i.e., did all peer nodes necessary for the transaction endorse the transaction). Here, the client may include only one of multiple parties to the transaction. In this case, each client may have their own endorsing node, and each endorsing node will need to endorse the transaction. The architecture is such that even if an application selects not to inspect responses or otherwise forwards an unendorsed transaction, the endorsement policy will still be enforced by peers and upheld at the commit validation phase.

[0091] After successful inspection, in step 293 the client 260 assembles endorsements into a transaction proposal and broadcasts the transaction proposal and response within a transaction message to the ordering node 284. The transaction may contain the read/write sets, the endorsing peers' signatures and a channel ID. The ordering node 284 does not need to inspect the entire content of a transaction in order to perform its operation, instead the ordering node 284 may simply receive transactions from all channels in the network, order them chronologically by channel, and create blocks of transactions per channel.

[0092] The blocks are delivered from the ordering node 284 to all peer nodes 281-283 on the channel. The data section within the block may be validated to ensure an endorsement policy is fulfilled and to ensure that there have been no changes to ledger state for read set variables since the read set was generated by the transaction execution. Furthermore, in step 295 each peer node 281-283 appends the block to the channel's chain, and for each valid transaction the write sets are committed to the current state database. An event may be emitted, to notify the client application that the transaction (invocation) has been immutably appended to the chain, as well as to notify whether the transaction was validated or invalidated.

[0093] FIG. 3A illustrates an example of a permissioned blockchain network 300, which features a distributed, decentralized peer-to-peer architecture. In this example, a blockchain user 302 may initiate a transaction to the permissioned blockchain 304. In this example, the transaction can be a deploy, invoke, or query, and may be issued through a client-side application leveraging an SDK, directly through an API, etc. Networks may provide access to a regulator 306, such as an auditor. A blockchain network operator 308 manages member permissions, such as enrolling the regulator 306 as an "auditor" and the blockchain user 302 as a "client". An auditor could be restricted only to querying the ledger whereas a client could be authorized to deploy, invoke, and query certain types of chaincode.

[0094] A blockchain developer 310 can write chaincode and client-side applications. The blockchain developer 310 can deploy chaincode directly to the network through an interface. To include credentials from a traditional data source 312 in chaincode, the developer 310 could use an out-of-band connection to access the data. In this example, the blockchain user 302 connects to the permissioned blockchain 304 through a peer node 314. Before proceeding with any transactions, the peer node 314 retrieves the user's enrollment and transaction certificates from a certificate authority 316, which manages user roles and permissions. In some cases, blockchain users must possess these digital certificates in order to transact on the permissioned blockchain 304. Meanwhile, a user attempting to utilize chaincode may be required to verify their credentials on the traditional data source 312. To confirm the user's authorization, chaincode can use an out-of-band connection to this data through a traditional processing platform 318.

[0095] FIG. 3B illustrates another example of a permissioned blockchain network 320, which features a distributed, decentralized peer-to-peer architecture. In this example, a blockchain user 322 may submit a transaction to the permissioned blockchain 324. In this example, the transaction can be a deploy, invoke, or query, and may be issued through a client-side application leveraging an SDK, directly through an API, etc. Networks may provide access to a regulator 326, such as an auditor. A blockchain network operator 328 manages member permissions, such as enrolling the regulator 326 as an "auditor" and the blockchain user 322 as a "client". An auditor could be restricted only to querying the ledger whereas a client could be authorized to deploy, invoke, and query certain types of chaincode.

[0096] A blockchain developer 330 writes chaincode and client-side applications. The blockchain developer 330 can deploy chaincode directly to the network through an interface. To include credentials from a traditional data source 332 in chaincode, the developer 330 could use an out-of-band connection to access the data. In this example, the blockchain user 322 connects to the network through a peer node 334. Before proceeding with any transactions, the peer node 334 retrieves the user's enrollment and transaction certificates from the certificate authority 336. In some cases, blockchain users must possess these digital certificates in order to transact on the permissioned blockchain 324. Meanwhile, a user attempting to utilize chaincode may be required to verify their

credentials on the traditional data source 332. To confirm the user's authorization, chaincode can use an out-of-band connection to this data through a traditional processing platform 338.

[0097] In some embodiments, the blockchain herein may be a permissionless blockchain. In contrast with permissioned blockchains which require permission to join, anyone can join a permissionless blockchain. For example, to join a permissionless blockchain a user may create a personal address and begin interacting with the network, by submitting transactions, and hence adding entries to the ledger. Additionally, all parties have the choice of running a node on the system and employing the mining protocols to help verify transactions.

[0098] FIG. 3C illustrates a process 350 of a transaction being processed by a permissionless blockchain 352 including a plurality of nodes 354. A sender 356 desires to send payment or some other form of value (e.g., a deed, medical records, a contract, a good, a service, or any other asset that can be encapsulated in a digital record) to a recipient 358 via the permissionless blockchain 352. In one embodiment, each of the sender device 356 and the recipient device 358 may have digital wallets (associated with the blockchain 352) that provide user interface controls and a display of transaction parameters. In response, the transaction is broadcast throughout the blockchain 352 to the nodes 354. Depending on the blockchain's 352 network parameters the nodes verify 360 the transaction based on rules (which may be pre-defined or dynamically allocated) established by the permissionless blockchain 352 creators. For example, this may include verifying identities of the parties involved, etc. The transaction may be verified immediately or it may be placed in a queue with other transactions and the nodes 354 determine if the transactions are valid based on a set of network rules.

[0099] In structure 362, valid transactions are formed into a block and sealed with a lock (hash). This process may be performed by mining nodes among the nodes 354. Mining nodes may utilize additional software specifically for mining and creating blocks for the permissionless blockchain 352. Each block may be identified by a hash (e.g., 256 bit number, etc.) created using an algorithm agreed upon by the network. Each block may include a header, a pointer or reference to a hash of a previous block's header in the chain, and a group of valid transactions. The reference to the previous block's hash is associated with the creation of the secure independent chain of blocks.

[00100] Before blocks can be added to the blockchain, the blocks must be validated. Validation for the permissionless blockchain 352 may include a proof-of-work (PoW) which is a solution to a puzzle derived from the block's header. Although not shown in the example of FIG. 3C, another process for validating a block is proof-of-stake. Unlike the proof-of-work, where the algorithm rewards miners who solve mathematical problems, with the proof of stake, a creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as "stake." Then, a similar proof is performed by the selected/chosen node.

[00101] With mining 364, nodes try to solve the block by making incremental changes to one variable until the solution satisfies a network-wide target. This creates the PoW thereby ensuring correct answers. In other words, a potential solution must prove that computing resources were drained in solving the problem. In some types of permissionless blockchains, miners may be rewarded with value (e.g., coins, etc.) for correctly mining a block.

[00102] Here, the PoW process, alongside the chaining of blocks, makes modifications of the blockchain extremely difficult, as an attacker must modify all subsequent blocks in order for the modifications of one block to be accepted. Furthermore, as new blocks are mined, the difficulty of modifying a block increases, and the number of subsequent blocks increases. With distribution 366, the successfully validated block is distributed through the permissionless blockchain 352 and all nodes 354 add the block to a majority chain which is the permissionless blockchain's 352 auditable ledger. Furthermore, the value in the transaction submitted by the sender 356 is deposited or otherwise transferred to the digital wallet of the recipient device 358.

[00103] FIG. 4A illustrates a process 400A of tag data being read at different locations of a supply chain according to example embodiments. Referring to FIG. 4A, a security protocol between a tag (not shown) at different locations of a supply chain and a blockchain network 410 is shown. In this example, the tag is electrically coupled to a temperature sensor. Here, the tag may wake up every 2 minutes, 5 minutes, 20 minutes, etc.) and take a temperature reading which is stored on the tag. The temperature reading may be encrypted and added to a list of readings that the tag maintains in its local storage. Readers are positioned at different locations on the supply chain including a manufacturer 402, a transporter 404, and a retailer 406. The blockchain network 410 may include a network of blockchain peers that are distributed at different geographical locations. Therefore, each of the manufacturer 402, the transporter 404, and the retailer 406 may interact with different blockchain peers of the blockchain network 410.

[00104] When the tag is read, the tag may verify the reader through a handshake protocol. For example, the tag may be a smart tag which stores a public key of each of the respective readers. The tag may request the reader to provide a signature using the reader's private key. The tag may then verify the reader's private key is valid using the corresponding public key of the reader (e.g., by hashing/encrypting the same data, etc.) and determining the two hashes match and therefore the signature is valid. If the reader is verified, a session may be started. Alternatively the verification may happen between the blockchain server and the tag, with the RFID reader acting as a pass-through. For example, ECDH may be used by the tag to establish a session key for encryption and hashing with the blockchain. The tag then sends the tag data (including any temperature measurements captured and stored in the list, or postprocessed tag data) to the reader. The tag signs the tag data using the tag's private key. Also, the tag may encrypt the data using the session key established using ECDH. Therefore, the reader will be unable to decrypt the tag data.

[00105] In this example, the readers at the manufacturer 402, the transporter 404, and the retailer 406 may be connected to the blockchain network 410 via a hypertext transfer protocol (HTTP) connection. The blockchain network 410 may receive the tag data and unpack the encrypted tag data to decrypt the tag data and verify the tag's signature using a corresponding public key of the tag. If the reader is a trusted reader, the blockchain network 410 may further unpack the reader's signature to determine that the reader is a valid reader based on a corresponding public key of the reader stored by the blockchain network 410. If the validation of the tag and the reader are successful, the blockchain 410 stores the tag data (e.g., as shown in FIG. 4B) to the blockchain ledger. If the tag or the reader is not successfully validated, the blockchain may record an attempt by the unregistered tag or reader on the blockchain. Also, any additional information about the tag such as date, time, geolocation, and the like, may also be recorded by the blockchain network 410 on the blockchain ledger in either scenario.

[00106] If the readers are untrusted, the tag may refuse to communicate with the reader. As another example, the tag may check if the reader is semi-trusted meaning that the reader can reach the correct blockchain network 410 and confirm some secret that is shared by the blockchain network 410 and the tag, such as a shared secret. Here, the tag may send a challenge to the blockchain network 410 via the untrusted reader. If the response returned from the blockchain network 410 is correct, the tag knows that the reader is communicating with the correct blockchain network 410 and will send the tag data. Even if the reader is intercepting data from the tag, the data will not be of much use since it is also encrypted using a session key shared between the tag and the blockchain network 410.

[00107] In some embodiments, the blockchain network 410 may include peer nodes that are controlled by the respective parties to the supply chain including the manufacturer 402, the transporter 404, and the retailer 406, however, embodiments are not limited thereto. In this example, each party may write data to the blockchain through traditional endorsement/consensus protocols and each party maintains their own copy of the blockchain ledger.

[00108] The blockchain network 410 may also include one or more smart contracts 412 which can analyze the tag data provided from the supply chain. For example, the smart contract 412 may query all tags scanned by a given reader, query all the tracking history for a given tag, query all the enrolled tags, verify that the sensor readings (e.g., temperature readings, etc.) from a given tag are within safe limits that are pre-defined in the logic of the smart contract 412, cross-verify time-stamps from tag with other data in blockchain (GPS logs, reader logs) to further verify the authenticity of the tag data, and the like. In some embodiments, the smart contract 412 may also make data available to other applications such as a notification application 414 which can send out an alert to one or more interested parties (e.g., computing devices thereof) indicating that the sensor data has indicated an issue such as predefined condition is not met. In the example of FIG. 4A, the notification service 414 sends alerts or other notifications to a user interface that is displayed on user device 420.

[00109] The smart contract 412 may store various monitoring conditions of a physical object that is being tracked by the tags. For example, goods, materials, parts, or the like, may be transported through the supply chain and have various requirements such as temperature requirements (e.g., cold chain, etc.), humidity requirements, pressure requirements, timing requirements, and the like. The tag data relayed back from the readers at each of the positions on the supply chain may be monitored by the smart contract 412 to determine whether any conditions have been violated. The conditions may be embedded within the logic of the smart contract 412. Furthermore, although referred to herein as a smart contract, when packaged into executable code and deployed on a blockchain peer, the smart contract may be referred to as chaincode which includes the logic of the smart contract.

[00110] FIG. 4B illustrates a process 400B of storing tag data to a blockchain ledger according to example embodiments. Referring to FIG. 4B, each blockchain peer included within the blockchain network 410 shown in FIG. 4A may include a blockchain 432 and a state database 434 which are included within the blockchain ledger. The blockchain peer may also include a peer application 431 for blockchain communications and a smart contract 430 which may be the same or different from the smart contract 412 shown in FIG. 4A.

[00111] Each time a tag sends back tag data, the blockchain 432 may be updated with a new block 433. Also, the state database 434 may be updated to reflect the most current values of the tag. Here, the state database 434 may store key-value pairs where the key corresponds to the device ID of the tag and the value is actually multiple values 436 including various data read by the reader from the tag, for example, a logging ID of a reader that called the tag, a logging signature of the caller, an operation code, a device ID of the tag, a device signature of the tag, device metadata of the tag, a terminal ID, a terminal signature, terminal metadata, and the like. This data may also be stored as a unique transaction on the blockchain 432 (e.g., within the new block 433). In this example, the smart contract 430 may analyze the tag data stored on the blockchain 432 and the state database 434 and perform various operations and communicate with other applications/services.

[00112] FIG. 4C illustrates a user interface 450 which displays tag data associated with a physical object according to example embodiments. For example, the user interface 450 may be output by a service or application that is running or in communication with the blockchain or a blockchain peer. Referring to FIG. 4C, the user interface includes data of a tag at different reading times and at different positions on the supply chain. In this example, the user interface 450 includes attributes such as a status value 451, a data value 452, a tag ID value 453, a reader ID value 454, and sensor values 455. The user interface may also display other or additional data attributes such as geolocation, whether verification of the tag signature is successful, and the like. In this example the user interface outputs a warning 456 indicating that one of the tag readings indicates a failure of a condition included within the logic of a smart contract.

[00113] FIG. 5A illustrates a method 510 of receiving tag data according to example embodiments. As a non-limiting example, the method 500 may be performed by a blockchain peer node, a server, a database node, or the like. Referring to FIG. 5, in 512, the method may include receiving, via a network, tag data that is read from a tag associated with a physical object and signed using a private key assigned to the tag, and the data may be encrypted by the tag. For example, the receiving may include receiving a message or other communication from a reader of the tag. The tag, in some embodiments, may be an RFID tag. However, embodiments are not limited thereto.

[00114] The tag data may include an identifier of the tag as well as additional data that is being fed back and that is capable of verifying the tag. For example, the additional data may include sensor data from one or more sensors that are electrically coupled to the tag. Here, the tag may periodically or randomly trigger or otherwise request a sensor to capture a reading. The sensor data may include any kinds of sensor values of any kinds of sensors, including fluid flow rate, temperature, velocity, acceleration, humidity, pressure, and the like. The sensor data may be used to verify that the physical object associated with the tag is being properly cared for. In other words, the sensor data may be used to verify that the physical object is being kept in specified conditions or the like. As another example, the sensor data may be used to further verify the authenticity of the tag. For example, a geolocation value, a sensor ID, or the like, may be included within the tag data and used to further verify that the tag is coupled to the correct sensor. In some embodiments, in addition to signing the tag data, the tag may encrypt the tag data using a AES encryption, or the like, which is established with the blockchain.

[00115] In 514, the method may include determining, via a blockchain peer, that the signed tag data is validly signed based on a corresponding key pair of the tag which is accessible to the blockchain peer. For example, the tag may be signed with a private key that is uniquely assigned and embedded within a secure storage of the tag. Meanwhile, the blockchain peer may access and use a public key of the tag which is stored in a blockchain peer memory to verify that the private key of the tag is valid. In some embodiments, the method may further include verifying the authenticity of the tag based on a sensor identifier included within the tag data.

[00116] In 516, the method may include determining, via the blockchain peer, whether the tag data satisfies of one or more predefined conditions of the physical object. In 518, the method may include storing the determination via a blockchain database. In some embodiments, the determining may include determining whether the tag data violates one or more predefined conditions embedded within logic of a chaincode running on the blockchain peer. Here, the conditions may include environmental conditions for the physical object such as storage conditions, temperature conditions, timing conditions, and the like.

[00117] In some embodiments, the method may further include transmitting, via chaincode running on the blockchain peer, an alert to a computing device associated with the physical object. In some embodiments, the tag

data is further signed by a key assigned to the reader, and the method further comprises determining that the signed tag data is validly signed based on a corresponding key pair of the reader which is accessible to the blockchain peer. In some embodiments, the storing may include storing an identifier of the tag and the tag data as a key-value pair in a state database of the blockchain. In one non-limiting example use case, the determining may include determining whether temperature data within the tag data violates one or more temperature requirements for the physical object that are embedded within logic of a chaincode running on the blockchain peer.

[00118] FIG. 5B illustrates a method 520 of transmitting tag data according to example embodiments. Referring to FIG. 5B, in 522 the method may include retrieving sensor data from one or more hardware sensors coupled to a tag and storing the sensor data within a memory of the tag. In 524, the method may include receiving a read request from a reader associated with a blockchain platform. In 526, the method may include verifying the authenticity of the blockchain platform based on handshake protocol between the tag and the blockchain via the reader. In 528, the method may include, in response to a successful verification of the blockchain platform, signing the sensor data based on a private key of the tag, and transmitting the signed sensor data to the reader.

[00119] In some embodiments, the method may further include checking, via a bootloader on the tag, the integrity of software running on the tag during a power up of the tag. In some embodiments, the method may further include verifying the authenticity of the blockchain platform comprises receiving data signed by the blockchain platform, and verifying the signed data based on a corresponding key of the blockchain platform stored by the tag. In some embodiments, the method may further include verifying, by the tag, the authenticity of the reader based on a handshake protocol with the reader. In some embodiments, the method may include performing a key exchange with the blockchain platform to establish a shared key between the tag and the blockchain platform.

[00120] In some embodiments, the signing the sensor data may further include encrypting the sensor data based on the shared key with the blockchain platform prior to transmitting the signed sensor data to the reader. In some embodiments, the method may further include detecting, via the tag, that a data violation has occurred based on values of the sensor data retrieved from the one or more hardware sensors and storing the data violation within the memory. In some embodiments, the memory of the tag is read and write protected thereby preventing the private key from being read or modified by an external entity.

[00121] FIG. 6A illustrates an example system 600 that includes a physical infrastructure 610 configured to perform various operations according to example embodiments. Referring to FIG. 6A, the physical infrastructure 610 includes a module 612 and a module 614. The module 614 includes a blockchain 620 and a smart contract 630 (which may reside on the blockchain 620), that may execute any of the operational steps 608 (in module 612) included in any of the example embodiments. The steps/operations 608 may include one or more of the embodiments described or depicted and may represent output or written information that is written or read from one

or more smart contracts 630 and/or blockchains 620. The physical infrastructure 610, the module 612, and the module 614 may include one or more computers, servers, processors, memories, and/or wireless communication devices. Further, the module 612 and the module 614 may be a same module.

[00122] FIG. 6B illustrates another example system 640 configured to perform various operations according to example embodiments. Referring to FIG. 6B, the system 640 includes a module 612 and a module 614. The module 614 includes a blockchain 620 and a smart contract 630 (which may reside on the blockchain 620), that may execute any of the operational steps 608 (in module 612) included in any of the example embodiments. The steps/operations 608 may include one or more of the embodiments described or depicted and may represent output or written information that is written or read from one or more smart contracts 630 and/or blockchains 620. The physical infrastructure 610, the module 612, and the module 614 may include one or more computers, servers, processors, memories, and/or wireless communication devices. Further, the module 612 and the module 614 may be a same module.

[00123] FIG. 6C illustrates an example system configured to utilize a smart contract configuration among contracting parties and a mediating server configured to enforce the smart contract terms on the blockchain according to example embodiments. Referring to FIG. 6C, the configuration 650 may represent a communication session, an asset transfer session or a process or procedure that is driven by a smart contract 630 which explicitly identifies one or more user devices 652 and/or 656. The execution, operations and results of the smart contract execution may be managed by a server 654. Content of the smart contract 630 may require digital signatures by one or more of the entities 652 and 656 which are parties to the smart contract transaction. The results of the smart contract execution may be written to a blockchain 620 as a blockchain transaction. The smart contract 630 resides on the blockchain 620 which may reside on one or more computers, servers, processors, memories, and/or wireless communication devices.

[00124] FIG. 6D illustrates a system 660 including a blockchain, according to example embodiments. Referring to the example of FIG. 6D, an application programming interface (API) gateway 662 provides a common interface for accessing blockchain logic (e.g., smart contract 630 or other chaincode) and data (e.g., distributed ledger, etc.). In this example, the API gateway 662 is a common interface for performing transactions (invoke, queries, etc.) on the blockchain by connecting one or more entities 652 and 656 to a blockchain peer (i.e., server 654). Here, the server 654 is a blockchain network peer component that holds a copy of the world state and a distributed ledger allowing clients 652 and 656 to query data on the world state as well as submit transactions into the blockchain network where, depending on the smart contract 630 and endorsement policy, endorsing peers will run the smart contracts 630.

[00125] The above embodiments may be implemented in hardware, in a computer program executed by a processor, in firmware, or in a combination of the above. A computer program may be embodied on a computer readable medium, such as a storage medium. For example, a computer program may reside in random access memory ("RAM"), flash memory, read-only memory ("ROM"), erasable programmable read-only memory ("EPROM"), electrically erasable programmable read-only memory ("EEPROM"), registers, hard disk, a removable disk, a compact disk read-only memory ("CD-ROM"), or any other form of storage medium known in the art.

[00126] An exemplary storage medium may be coupled to the processor such that the processor may read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an application specific integrated circuit ("ASIC"). In the alternative, the processor and the storage medium may reside as discrete components.

[00127] FIG. 7A illustrates a process 700 of a new block being added to a distributed ledger 720, according to example embodiments, and FIG. 7B illustrates contents of a new data block structure 730 for blockchain, according to example embodiments. Referring to FIG. 7A, clients (not shown) may submit transactions to blockchain nodes 711, 712, and/or 713. Clients may be instructions received from any source to enact activity on the blockchain 720. As an example, clients may be applications that act on behalf of a requester, such as a device, person or entity to propose transactions for the blockchain. The plurality of blockchain peers (e.g., blockchain nodes 711, 712, and 713) may maintain a state of the blockchain network and a copy of the distributed ledger 720. Different types of blockchain nodes/peers may be present in the blockchain network including endorsing peers which simulate and endorse transactions proposed by clients and committing peers which verify endorsements, validate transactions, and commit transactions to the distributed ledger 720. In this example, the blockchain nodes 711, 712, and 713 may perform the role of endorser node, committer node, or both.

[00128] The distributed ledger 720 includes a blockchain which stores immutable, sequenced records in blocks, and a state database 724 (current world state) maintaining a current state of the blockchain 722. One distributed ledger 720 may exist per channel and each peer maintains its own copy of the distributed ledger 720 for each channel of which they are a member. The blockchain 722 is a transaction log, structured as hash-linked blocks where each block contains a sequence of N transactions. Blocks may include various components such as shown in FIG. 7B. The linking of the blocks (shown by arrows in FIG. 7A) may be generated by adding a hash of a prior block's header within a block header of a current block. In this way, all transactions on the blockchain 722 are sequenced and cryptographically linked together preventing tampering with blockchain data without breaking the hash links. Furthermore, because of the links, the latest block in the blockchain 722 represents every transaction that has come before it. The blockchain 722 may be stored on a peer file system (local or attached storage), which supports an append-only blockchain workload.

[00129] The current state of the blockchain 722 and the distributed ledger 722 may be stored in the state database 724. Here, the current state data represents the latest values for all keys ever included in the chain transaction log of the blockchain 722. Chaincode invocations execute transactions against the current state in the state database 724. To make these chaincode interactions extremely efficient, the latest values of all keys are stored in the state database 724. The state database 724 may include an indexed view into the transaction log of the blockchain 722, it can therefore be regenerated from the chain at any time. The state database 724 may automatically get recovered (or generated if needed) upon peer startup, before transactions are accepted.

[00130] Endorsing nodes receive transactions from clients and endorse the transaction based on simulated results. Endorsing nodes hold smart contracts which simulate the transaction proposals. When an endorsing node endorses a transaction, the endorsing nodes creates a transaction endorsement which is a signed response from the endorsing node to the client application indicating the endorsement of the simulated transaction. The method of endorsing a transaction depends on an endorsement policy which may be specified within chaincode. An example of an endorsement policy is "the majority of endorsing peers must endorse the transaction". Different channels may have different endorsement policies. Endorsed transactions are forward by the client application to ordering service 710.

[00131] The ordering service 710 accepts endorsed transactions, orders them into a block, and delivers the blocks to the committing peers. For example, the ordering service 710 may initiate a new block when a threshold of transactions has been reached, a timer times out, or another condition. In the example of FIG. 7A, blockchain node 712 is a committing peer that has received a new data new data block 730 for storage on blockchain 720. The first block in the blockchain may be referred to as a genesis block which includes information about the blockchain, its members, the data stored therein, etc.

[00132] The ordering service 710 may be made up of a cluster of orderers. The ordering service 710 does not process transactions, smart contracts, or maintain the shared ledger. Rather, the ordering service 710 may accept the endorsed transactions and specifies the order in which those transactions are committed to the distributed ledger 720. The architecture of the blockchain network may be designed such that the specific implementation of 'ordering' (e.g., Solo, Kafka, BFT, etc.) becomes a pluggable component.

[00133] Transactions are written to the distributed ledger 720 in a consistent order. The order of transactions is established to ensure that the updates to the state database 724 are valid when they are committed to the network. Unlike a cryptocurrency blockchain system (e.g., Bitcoin, etc.) where ordering occurs through the solving of a cryptographic puzzle, or *mining*, in this example the parties of the distributed ledger 720 may choose the ordering mechanism that best suits that network.

[00134] When the ordering service 710 initializes a new data block 730, the new data block 730 may be broadcast to committing peers (e.g., blockchain nodes 711, 712, and 713). In response, each committing peer validates the transaction within the new data block 730 by checking to make sure that the read set and the write set still match the current world state in the state database 724. Specifically, the committing peer can determine whether the read data that existed when the endorsers simulated the transaction is identical to the current world state in the state database 724. When the committing peer validates the transaction, the transaction is written to the blockchain 722 on the distributed ledger 720, and the state database 724 is updated with the write data from the read-write set. If a transaction fails, that is, if the committing peer finds that the read-write set does not match the current world state in the state database 724, the transaction ordered into a block will still be included in that block, but it will be marked as invalid, and the state database 724 will not be updated.

[00135] Referring to FIG. 7B, a new data block 730 (also referred to as a data block) that is stored on the blockchain 722 of the distributed ledger 720 may include multiple data segments such as a block header 740, block data 750 (block data section), and block metadata 760. It should be appreciated that the various depicted blocks and their contents, such as new data block 730 and its contents, shown in FIG. 7B are merely examples and are not meant to limit the scope of the example embodiments. In a conventional block, the data section may store transactional information of N transaction(s) (e.g., 1, 10, 100, 500, 1000, 2000, 3000, etc.) within the block data 750.

[00136] The new data block 730 may include a link to a previous block (e.g., on the blockchain 722 in FIG. 7A) within the block header 740. In particular, the block header 740 may include a hash of a previous block's header. The block header 740 may also include a unique block number, a hash of the block data 750 of the new data block 730, and the like. The block number of the new data block 730 may be unique and assigned in various orders, such as an incremental/sequential order starting from zero.

[00137] According to various embodiments, the block data 750 may store tag data 752 received from an electronic tag such as a RFID tag, etc. The tag data 752 may include sensor data, tag identifiers, reader data, reader identifiers, and the like. The tag data 752 includes one or more of the steps, features, processes and/or actions described or depicted herein. Accordingly, the tag data 752 can be stored in an immutable log of blocks on the distributed ledger 720. Some of the benefits of storing the tag data 752 on the blockchain are reflected in the various embodiments disclosed and depicted herein. Although in FIG. 7B, the tag data 752 is depicted in the block data 750, in other embodiments, it may be located in the block header 740 or the block metadata 760. Also, the tag data 752 may be stored as a key-value pair within the state database 724.

[00138] The block metadata 760 may store multiple fields of metadata (e.g., as a byte array, etc.). Metadata fields may include signature on block creation, a reference to a last configuration block, a transaction filter

identifying valid and invalid transactions within the block, last offset persisted of an ordering service that ordered the block, and the like. The signature, the last configuration block, and the orderer metadata may be added by the ordering service 710. Meanwhile, a committer of the block (such as blockchain node 712) may add validity/invalidity information based on an endorsement policy, verification of read/write sets, and the like. The transaction filter may include a byte array of a size equal to the number of transactions that are included in the block data 750 and a validation code identifying whether a transaction was valid/invalid.

[00139] FIG. 7C illustrates an embodiment of a blockchain 770 for digital content in accordance with the embodiments described herein. The digital content may include one or more files and associated information. The files may include media, images, video, audio, text, links, graphics, animations, web pages, documents, or other forms of digital content. The immutable, append-only aspects of the blockchain serve as a safeguard to protect the integrity, validity, and authenticity of the digital content, making it suitable use in legal proceedings where admissibility rules apply or other settings where evidence is taken in to consideration or where the presentation and use of digital information is otherwise of interest. In this case, the digital content may be referred to as digital evidence.

[00140] The blockchain may be formed in various ways. In one embodiment, the digital content may be included in and accessed from the blockchain itself. For example, each block of the blockchain may store a hash value of reference information (e.g., header, value, etc.) along the associated digital content. The hash value and associated digital content may then be encrypted together. Thus, the digital content of each block may be accessed by decrypting each block in the blockchain, and the hash value of each block may be used as a basis to reference a previous block. This may be illustrated as follows:

<u>Block 1</u>	<u>Block 2</u>		<u>Block N</u>
Hash Value 1	Hash Value 2		Hash Value N
Digital Content 1	Digital Content 2		Digital Content N

[00141] In one embodiment, the digital content may be not included in the blockchain. For example, the blockchain may store the encrypted hashes of the content of each block without any of the digital content. The digital content may be stored in another storage area or memory address in association with the hash value of the original file. The other storage area may be the same storage device used to store the blockchain or may be a different storage area or even a separate relational database. The digital content of each block may be referenced or accessed by obtaining or querying the hash value of a block of interest and then looking up that has value in the storage area, which is stored in correspondence with the actual digital content. This operation may be performed, for example, a database gatekeeper. This may be illustrated as follows:

<u>Blockchain</u>	<u>Storage Area</u>
Block 1 Hash Value	Block 1 Hash Value ... Content
.	.
.	.
.	.
Block N Hash Value	Block N Hash Value ... Content

[00142] In the example embodiment of FIG. 7C, the blockchain 770 includes a number of blocks 778₁, 778₂, ... 778_N cryptographically linked in an ordered sequence, where $N \geq 1$. The encryption used to link the blocks 778₁, 778₂, ... 778_N may be any of a number of keyed or un-keyed Hash functions. In one embodiment, the blocks 778₁, 778₂, ... 778_N are subject to a hash function which produces n-bit alphanumeric outputs (where n is 256 or another number) from inputs that are based on information in the blocks. Examples of such a hash function include, but are not limited to, a SHA-type (SHA stands for Secure Hash Algorithm) algorithm, Merkle-Damgard algorithm, HAIFA algorithm, Merkle-tree algorithm, nonce-based algorithm, and a non-collision-resistant PRF algorithm. In another embodiment, the blocks 778₁, 778₂, ..., 778_N may be cryptographically linked by a function that is different from a hash function. For purposes of illustration, the following description is made with reference to a hash function, e.g., SHA-2.

[00143] Each of the blocks 778₁, 778₂, ..., 778_N in the blockchain includes a header, a version of the file, and a value. The header and the value are different for each block as a result of hashing in the blockchain. In one embodiment, the value may be included in the header. As described in greater detail below, the version of the file may be the original file or a different version of the original file.

[00144] The first block 778₁ in the blockchain is referred to as the genesis block and includes the header 772₁, original file 774₁, and an initial value 776₁. The hashing scheme used for the genesis block, and indeed in all subsequent blocks, may vary. For example, all the information in the first block 778₁ may be hashed together and at one time, or each or a portion of the information in the first block 778₁ may be separately hashed and then a hash of the separately hashed portions may be performed.

[00145] The header 772₁ may include one or more initial parameters, which, for example, may include a version number, timestamp, nonce, root information, difficulty level, consensus protocol, duration, media format, source, descriptive keywords, and/or other information associated with original file 774₁ and/or the blockchain. The header 772₁ may be generated automatically (e.g., by blockchain network managing software) or manually by a blockchain participant. Unlike the header in other blocks 778₂ to 778_N in the blockchain, the header 772₁ in the genesis block does not reference a previous block, simply because there is no previous block.

[00146] The original file 774₁ in the genesis block may be, for example, data as captured by a device with or without processing prior to its inclusion in the blockchain. The original file 774₁ is received through the interface of the system from the device, media source, or node. The original file 774₁ is associated with metadata, which, for example, may be generated by a user, the device, and/or the system processor, either manually or automatically. The metadata may be included in the first block 778₁ in association with the original file 774₁.

[00147] The value 776₁ in the genesis block is an initial value generated based on one or more unique attributes of the original file 774₁. In one embodiment, the one or more unique attributes may include the hash value for the original file 774₁, metadata for the original file 774₁, and other information associated with the file. In one implementation, the initial value 776₁ may be based on the following unique attributes:

- 1) SHA-2 computed hash value for the original file
- 2) originating device ID
- 3) starting timestamp for the original file
- 4) initial storage location of the original file
- 5) blockchain network member ID for software to currently control the original file and associated

metadata

[00148] The other blocks 778₂ to 778_N in the blockchain also have headers, files, and values. However, unlike the first block 772₁, each of the headers 772₂ to 772_N in the other blocks includes the hash value of an immediately preceding block. The hash value of the immediately preceding block may be just the hash of the header of the previous block or may be the hash value of the entire previous block. By including the hash value of a preceding block in each of the remaining blocks, a trace can be performed from the Nth block back to the genesis block (and the associated original file) on a block-by-block basis, as indicated by arrows 780, to establish an auditable and immutable chain-of-custody.

[00149] Each of the header 772₂ to 772_N in the other blocks may also include other information, e.g., version number, timestamp, nonce, root information, difficulty level, consensus protocol, and/or other parameters or information associated with the corresponding files and/or the blockchain in general.

[00150] The files 774₂ to 774_N in the other blocks may be equal to the original file or may be a modified version of the original file in the genesis block depending, for example, on the type of processing performed. The type of processing performed may vary from block to block. The processing may involve, for example, any modification of a file in a preceding block, such as redacting information or otherwise changing the content of, taking information away from, or adding or appending information to the files.

[00151] Additionally, or alternatively, the processing may involve merely copying the file from a preceding block, changing a storage location of the file, analyzing the file from one or more preceding blocks, moving the file from one storage or memory location to another, or performing action relative to the file of the blockchain and/or its associated metadata. Processing which involves analyzing a file may include, for example, appending, including, or otherwise associating various analytics, statistics, or other information associated with the file.

[00152] The values in each of the other blocks 776_2 to 776_N in the other blocks are unique values and are all different as a result of the processing performed. For example, the value in any one block corresponds to an updated version of the value in the previous block. The update is reflected in the hash of the block to which the value is assigned. The values of the blocks therefore provide an indication of what processing was performed in the blocks and also permit a tracing through the blockchain back to the original file. This tracking confirms the chain-of-custody of the file throughout the entire blockchain.

[00153] For example, consider the case where portions of the file in a previous block are redacted, blocked out, or pixelated in order to protect the identity of a person shown in the file. In this case, the block including the redacted file will include metadata associated with the redacted file, e.g., how the redaction was performed, who performed the redaction, timestamps where the redaction(s) occurred, etc. The metadata may be hashed to form the value. Because the metadata for the block is different from the information that was hashed to form the value in the previous block, the values are different from one another and may be recovered when decrypted.

[00154] In one embodiment, the value of a previous block may be updated (e.g., a new hash value computed) to form the value of a current block when any one or more of the following occurs. The new hash value may be computed by hashing all or a portion of the information noted below, in this example embodiment.

- a) new SHA-2 computed hash value if the file has been processed in any way (e.g., if the file was redacted, copied, altered, accessed, or some other action was taken)
- b) new storage location for the file
- c) new metadata identified associated with the file
- d) transfer of access or control of the file from one blockchain participant to another blockchain participant

[00155] FIG. 7D illustrates an embodiment of a block which may represent the structure of the blocks in the blockchain 790 in accordance with one embodiment. The block, Block_i , includes a header 772_i , a file 774_i , and a value 776_i .

[00156] The header 772_i includes a hash value of a previous block Block_{i-1} and additional reference information, which, for example, may be any of the types of information (e.g., header information including references, characteristics, parameters, etc.) discussed herein. All blocks reference the hash of a previous block except, of

course, the genesis block. The hash value of the previous block may be just a hash of the header in the previous block or a hash of all or a portion of the information in the previous block, including the file and metadata.

[00157] The file 774_i includes a plurality of data, such as Data 1, Data 2, ..., Data N in sequence. The data are tagged with metadata 1, Metadata 2, ..., Metadata N which describe the content and/or characteristics associated with the data. For example, the metadata for each data may include information to indicate a timestamp for the data, process the data, keywords indicating the persons or other content depicted in the data, and/or other features that may be helpful to establish the validity and content of the file as a whole, and particularly its use a digital evidence, for example, as described in connection with an embodiment discussed below. In addition to the metadata, each data may be tagged with reference REF₁, REF₂, ..., REF_N to a previous data to prevent tampering, gaps in the file, and sequential reference through the file.

[00158] Once the metadata is assigned to the data (e.g., through a smart contract), the metadata cannot be altered without the hash changing, which can easily be identified for invalidation. The metadata, thus, creates a data log of information that may be accessed for use by participants in the blockchain.

[00159] The value 776_i is a hash value or other value computed based on any of the types of information previously discussed. For example, for any given block Block_i, the value for that block may be updated to reflect the processing that was performed for that block, e.g., new hash value, new storage location, new metadata for the associated file, transfer of control or access, identifier, or other action or information to be added. Although the value in each block is shown to be separate from the metadata for the data of the file and header, the value may be based, in part or whole, on this metadata in another embodiment.

[00160] Once the blockchain 770 is formed, at any point in time, the immutable chain-of-custody for the file may be obtained by querying the blockchain for the transaction history of the values across the blocks. This query, or tracking procedure, may begin with decrypting the value of the block that is most currently included (e.g., the last (Nth) block), and then continuing to decrypt the value of the other blocks until the genesis block is reached and the original file is recovered. The decryption may involve decrypting the headers and files and associated metadata at each block, as well.

[00161] Decryption is performed based on the type of encryption that took place in each block. This may involve the use of private keys, public keys, or a public key-private key pair. For example, when asymmetric encryption is used, blockchain participants or a processor in the network may generate a public key and private key pair using a predetermined algorithm. The public key and private key are associated with each other through some mathematical relationship. The public key may be distributed publicly to serve as an address to receive messages from other users, e.g., an IP address or home address. The private key is kept secret and used to digitally sign

messages sent to other blockchain participants. The signature is included in the message so that the recipient can verify using the public key of the sender. This way, the recipient can be sure that only the sender could have sent this message.

[00162] Generating a key pair may be analogous to creating an account on the blockchain, but without having to actually register anywhere. Also, every transaction that is executed on the blockchain is digitally signed by the sender using their private key. This signature ensures that only the owner of the account can track and process (if within the scope of permission determined by a smart contract) the file of the blockchain.

[00163] FIGS. 8A and 8B illustrate additional examples of use cases for blockchain which may be incorporated and used herein. In particular, FIG. 8A illustrates an example 800 of a blockchain 810 which stores machine learning (artificial intelligence) data. Machine learning relies on vast quantities of historical data (or training data) to build predictive models for accurate prediction on new data. Machine learning software (e.g., neural networks, etc.) can often sift through millions of records to unearth non-intuitive patterns.

[00164] In the example of FIG. 8A, a host platform 820 builds and deploys a machine learning model for predictive monitoring of assets 830. Here, the host platform 820 may be a cloud platform, an industrial server, a web server, a personal computer, a user device, and the like. Assets 830 can be any type of asset (e.g., machine or equipment, etc.) such as an aircraft, locomotive, turbine, medical machinery and equipment, oil and gas equipment, boats, ships, vehicles, and the like. As another example, assets 830 may be non-tangible assets such as stocks, currency, digital coins, insurance, or the like.

[00165] The blockchain 810 can be used to significantly improve both a training process 802 of the machine learning model and a predictive process 804 based on a trained machine learning model. For example, in 802, rather than requiring a data scientist / engineer or other user to collect the data, historical data may be stored by the assets 830 themselves (or through an intermediary, not shown) on the blockchain 810. This can significantly reduce the collection time needed by the host platform 820 when performing predictive model training. For example, using smart contracts, data can be directly and reliably transferred straight from its place of origin to the blockchain 810. By using the blockchain 810 to ensure the security and ownership of the collected data, smart contracts may directly send the data from the assets to the individuals that use the data for building a machine learning model. This allows for sharing of data among the assets 830.

[00166] The collected data may be stored in the blockchain 810 based on a consensus mechanism. The consensus mechanism pulls in (permissioned nodes) to ensure that the data being recorded is verified and accurate. The data recorded is time-stamped, cryptographically signed, and immutable. It is therefore auditable,

transparent, and secure. Adding IoT devices which write directly to the blockchain can, in certain cases (i.e. supply chain, healthcare, logistics, etc.), increase both the frequency and accuracy of the data being recorded.

[00167] Furthermore, training of the machine learning model on the collected data may take rounds of refinement and testing by the host platform 820. Each round may be based on additional data or data that was not previously considered to help expand the knowledge of the machine learning model. In 802, the different training and testing steps (and the data associated therewith) may be stored on the blockchain 810 by the host platform 820. Each refinement of the machine learning model (e.g., changes in variables, weights, etc.) may be stored on the blockchain 810. This provides verifiable proof of how the model was trained and what data was used to train the model. Furthermore, when the host platform 820 has achieved a finally trained model, the resulting model may be stored on the blockchain 810.

[00168] After the model has been trained, it may be deployed to a live environment where it can make predictions / decisions based on the execution of the final trained machine learning model. For example, in 804, the machine learning model may be used for condition-based maintenance (CBM) for an asset such as an aircraft, a wind turbine, a healthcare machine, and the like. In this example, data fed back from the asset 830 may be input the machine learning model and used to make event predictions such as failure events, error codes, and the like. Determinations made by the execution of the machine learning model at the host platform 820 may be stored on the blockchain 810 to provide auditable / verifiable proof. As one non-limiting example, the machine learning model may predict a future breakdown/failure to a part of the asset 830 and create alert or a notification to replace the part. The data behind this decision may be stored by the host platform 820 on the blockchain 810. In one embodiment the features and/or the actions described and/or depicted herein can occur on or with respect to the blockchain 810.

[00169] New transactions for a blockchain can be gathered together into a new block and added to an existing hash value. This is then encrypted to create a new hash for the new block. This is added to the next list of transactions when they are encrypted, and so on. The result is a chain of blocks that each contain the hash values of all preceding blocks. Computers that store these blocks regularly compare their hash values to ensure that they are all in agreement. Any computer that does not agree discards the records that are causing the problem. This approach is good for ensuring tamper-resistance of the blockchain, but it is not perfect.

[00170] One way to game this system is for a dishonest user to change the list of transactions in their favor, but in a way that leaves the hash unchanged. This can be done by brute force, in other words by changing a record, encrypting the result, and seeing whether the hash value is the same. And if not, trying again and again and again until it finds a hash that matches. The security of blockchains is based on the belief that ordinary computers can only perform this kind of brute force attack over time scales that are entirely impractical, such as the age of the

universe. By contrast, quantum computers are much faster (1000s of times faster) and consequently pose a much greater threat.

[00171] FIG. 8B illustrates an example 850 of a quantum-secure blockchain 852 which implements quantum key distribution (QKD) to protect against a quantum computing attack. In this example, blockchain users can verify each other's identities using QKD. This sends information using quantum particles such as photons, which cannot be copied by an eavesdropper without destroying them. In this way, a sender and a receiver through the blockchain can be sure of each other's identity.

[00172] In the example of FIG. 8B, four users are present 854, 856, 858, and 860. Each of pair of users may share a secret key 862 (*i.e.*, a QKD) between themselves. Since there are four nodes in this example, six pairs of nodes exists, and therefore six different secret keys 862 are used including QKD_{AB}, QKD_{AC}, QKD_{AD}, QKD_{BC}, QKD_{BD}, and QKD_{CD}. Each pair can create a QKD by sending information using quantum particles such as photons, which cannot be copied by an eavesdropper without destroying them. In this way, a pair of users can be sure of each other's identity.

[00173] The operation of the blockchain 852 is based on two procedures (i) creation of transactions, and (ii) construction of blocks that aggregate the new transactions. New transactions may be created similar to a traditional blockchain network. Each transaction may contain information about a sender, a receiver, a time of creation, an amount (or value) to be transferred, a list of reference transactions that justifies the sender has funds for the operation, and the like. This transaction record is then sent to all other nodes where it is entered into a pool of unconfirmed transactions. Here, two parties (*i.e.*, a pair of users from among 854-860) authenticate the transaction by providing their shared secret key 862 (QKD). This quantum signature can be attached to every transaction making it exceedingly difficult to tamper with. Each node checks their entries with respect to a local copy of the blockchain 852 to verify that each transaction has sufficient funds. However, the transactions are not yet confirmed.

[00174] Rather than perform a traditional mining process on the blocks, the blocks may be created in a decentralized manner using a broadcast protocol. At a predetermined period of time (*e.g.*, seconds, minutes, hours, etc.) the network may apply the broadcast protocol to any unconfirmed transaction thereby to achieve a Byzantine agreement (consensus) regarding a correct version of the transaction. For example, each node may possess a private value (transaction data of that particular node). In a first round, nodes transmit their private values to each other. In subsequent rounds, nodes communicate the information they received in the previous round from other nodes. Here, honest nodes are able to create a complete set of transactions within a new block. This new block can be added to the blockchain 852. In one embodiment the features and/or the actions described and/or depicted herein can occur on or with respect to the blockchain 852.

[00175] FIG. 9 illustrates an example system 900 that supports one or more of the example embodiments described and/or depicted herein. The system 900 comprises a computer system/server 902, which is operational with numerous other general purpose or special purpose computing system environments or configurations. Examples of well-known computing systems, environments, and/or configurations that may be suitable for use with computer system/server 902 include, but are not limited to, personal computer systems, server computer systems, thin clients, thick clients, hand-held or laptop devices, multiprocessor systems, microprocessor-based systems, set top boxes, programmable consumer electronics, network PCs, minicomputer systems, mainframe computer systems, and distributed cloud computing environments that include any of the above systems or devices, and the like.

[00176] Computer system/server 902 may be described in the general context of computer system-executable instructions, such as program modules, being executed by a computer system. Generally, program modules may include routines, programs, objects, components, logic, data structures, and so on that perform particular tasks or implement particular abstract data types. Computer system/server 902 may be practiced in distributed cloud computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed cloud computing environment, program modules may be located in both local and remote computer system storage media including memory storage devices.

[00177] As shown in FIG. 9, computer system/server 902 in cloud computing node 900 is shown in the form of a general-purpose computing device. The components of computer system/server 902 may include, but are not limited to, one or more processors or processing units 904, a system memory 906, and a bus that couples various system components including system memory 906 to processor 904.

[00178] The bus represents one or more of any of several types of bus structures, including a memory bus or memory controller, a peripheral bus, an accelerated graphics port, and a processor or local bus using any of a variety of bus architectures. By way of example, and not limitation, such architectures include Industry Standard Architecture (ISA) bus, Micro Channel Architecture (MCA) bus, Enhanced ISA (EISA) bus, Video Electronics Standards Association (VESA) local bus, and Peripheral Component Interconnects (PCI) bus.

[00179] Computer system/server 902 typically includes a variety of computer system readable media. Such media may be any available media that is accessible by computer system/server 902, and it includes both volatile and non-volatile media, removable and non-removable media. System memory 906, in one embodiment, implements the flow diagrams of the other figures. The system memory 906 can include computer system readable media in the form of volatile memory, such as random-access memory (RAM) 910 and/or cache memory 912. Computer system/server 902 may further include other removable/non-removable, volatile/non-volatile computer system storage media. By way of example only, storage system 914 can be provided for reading from and writing to

a non-removable, non-volatile magnetic media (not shown and typically called a "hard drive"). Although not shown, a magnetic disk drive for reading from and writing to a removable, non-volatile magnetic disk (e.g., a "floppy disk"), and an optical disk drive for reading from or writing to a removable, non-volatile optical disk such as a CD-ROM, DVD-ROM or other optical media can be provided. In such instances, each can be connected to the bus by one or more data media interfaces. As will be further depicted and described below, memory 906 may include at least one program product having a set (e.g., at least one) of program modules that are configured to carry out the functions of various embodiments of the application.

[00180] Program/utility 916, having a set (at least one) of program modules 918, may be stored in memory 906 by way of example, and not limitation, as well as an operating system, one or more application programs, other program modules, and program data. Each of the operating system, one or more application programs, other program modules, and program data or some combination thereof, may include an implementation of a networking environment. Program modules 918 generally carry out the functions and/or methodologies of various embodiments of the application as described herein.

[00181] As will be appreciated by one skilled in the art, aspects of the present application may be embodied as a system, method, or computer program product. Accordingly, aspects of the present application may take the form of an entirely hardware embodiment, an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, aspects of the present application may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.

[00182] Computer system/server 902 may also communicate with one or more external devices 920 such as a keyboard, a pointing device, a display 922, etc.; one or more devices that enable a user to interact with computer system/server 902; and/or any devices (e.g., network card, modem, etc.) that enable computer system/server 902 to communicate with one or more other computing devices. Such communication can occur via I/O interfaces 924. Still yet, computer system/server 902 can communicate with one or more networks such as a local area network (LAN), a general wide area network (WAN), and/or a public network (e.g., the Internet) via network adapter 926. As depicted, network adapter 926 communicates with the other components of computer system/server 902 via a bus. It should be understood that although not shown, other hardware and/or software components could be used in conjunction with computer system/server 902. Examples, include, but are not limited to: microcode, device drivers, redundant processing units, external disk drive arrays, RAID systems, tape drives, and data archival storage systems, etc.

[00183] Although an exemplary embodiment of at least one of a system, method, and non-transitory computer readable medium has been illustrated in the accompanied drawings and described in the foregoing detailed description, it will be understood that the application is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications, and substitutions as set forth and defined by the following claims. For example, the capabilities of the system of the various figures can be performed by one or more of the modules or components described herein or in a distributed architecture and may include a transmitter, receiver or pair of both. For example, all or part of the functionality performed by the individual modules, may be performed by one or more of these modules. Further, the functionality described herein may be performed at various times and in relation to various events, internal or external to the modules or components. Also, the information sent between various modules can be sent between the modules via at least one of: a data network, the Internet, a voice network, an Internet Protocol network, a wireless device, a wired device and/or via plurality of protocols. Also, the messages sent or received by any of the modules may be sent or received directly and/or via one or more of the other modules.

[00184] One skilled in the art will appreciate that a "system" could be embodied as a personal computer, a server, a console, a personal digital assistant (PDA), a cell phone, a tablet computing device, a smartphone or any other suitable computing device, or combination of devices. Presenting the above-described functions as being performed by a "system" is not intended to limit the scope of the present application in any way but is intended to provide one example of many embodiments. Indeed, methods, systems and apparatuses disclosed herein may be implemented in localized and distributed forms consistent with computing technology.

[00185] It should be noted that some of the system features described in this specification have been presented as modules, in order to more particularly emphasize their implementation independence. For example, a module may be implemented as a hardware circuit comprising custom very large-scale integration (VLSI) circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices, graphics processing units, or the like.

[00186] A module may also be at least partially implemented in software for execution by various types of processors. An identified unit of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions that may, for instance, be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together but may comprise disparate instructions stored in different locations which, when joined logically together, comprise the module and achieve the stated purpose for the module. Further, modules may be stored on a computer-readable medium, which may be, for instance, a hard disk drive, flash device, random access memory (RAM), tape, or any other such medium used to store data.

[00187] Indeed, a module of executable code could be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and across several memory devices. Similarly, operational data may be identified and illustrated herein within modules and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set or may be distributed over different locations including over different storage devices, and may exist, at least partially, merely as electronic signals on a system or network.

[00188] It will be readily understood that the components of the application, as generally described and illustrated in the figures herein, may be arranged and designed in a wide variety of different configurations. Thus, the detailed description of the embodiments is not intended to limit the scope of the application as claimed but is merely representative of selected embodiments of the application.

[00189] One having ordinary skill in the art will readily understand that the above may be practiced with steps in a different order, and/or with hardware elements in configurations that are different than those which are disclosed. Therefore, although the application has been described based upon these preferred embodiments, it would be apparent to those of skill in the art that certain modifications, variations, and alternative constructions would be apparent.

[00190] While preferred embodiments of the present application have been described, it is to be understood that the embodiments described are illustrative only and the scope of the application is to be defined solely by the appended claims when considered with a full range of equivalents and modifications (e.g., protocols, hardware devices, software platforms etc.) thereto.