



- (51) **International Patent Classification:**  
*H04L 29/08* (2006.01)      *H04W 4/46* (2018.01)  
*H04L 12/58* (2006.01)      *H04W 4/12* (2009.01)
- (21) **International Application Number:**  
PCT/US2019/068429
- (22) **International Filing Date:**  
23 December 2019 (23.12.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**  
16/237,634      31 December 2018 (31.12.2018) US  
16/237,626      31 December 2018 (31.12.2018) US
- (71) **Applicant: T-MOBILE USA, INC.** [US/US]; 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).
- (72) **Inventor: OBAIDI, Ahmad, Arash;** 12920 SE 38th Street, Bellevue, WA 98006-1350 (US).

(74) **Agent: SMITH, Michael, J.** et al.; PERKINS COIE LLP, P.O. Box 1247, Seattle, WA 98111-1247 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM,

(54) **Title:** USING A BLOCKCHAIN TO DETERMINE TRUSTWORTHINESS OF MESSAGES WITHIN A TELECOMMUNICATIONS NETWORK FOR A SMART CITY

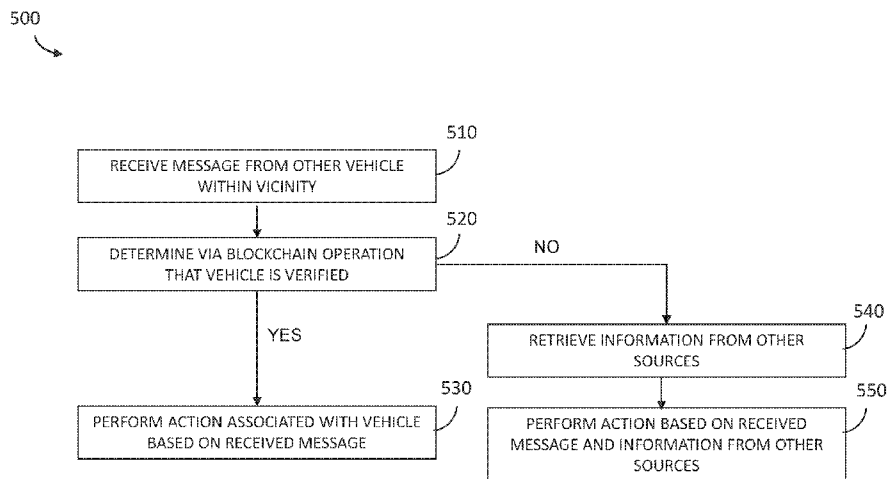


FIG. 5

(57) **Abstract:** Systems and methods are described herein for configuring vehicles and infrastructure (e.g., buildings, smart homes, traffic devices, utilities and associated systems, emergency response systems, and so on) to include blockchain nodes, so a smart city or area of the various devices can be supported by a blockchain network, with some or all devices and systems provisioned with nodes acting as distributed nodes for the blockchain network.



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,  
KM, ML, MR, NE, SN, TD, TG).

**Published:**

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

## USING A BLOCKCHAIN TO DETERMINE TRUSTWORTHINESS OF MESSAGES WITHIN A TELECOMMUNICATIONS NETWORK FOR A SMART CITY

### BACKGROUND

**[0001]** Various types of networks, including wireless networks, cellular networks, and other types of telecommunications networks, provide people across the world with communication services. For example, in most locations around the world, a user of a mobile device can access a network and communicate with other users or systems, either via voice calls, text messages, or data over the Internet. These networks, and their entrenched ubiquity, have connected users to many different users as well as to vast troves of information and services. Telecommunications networks, arguably, have made the world better for people.

**[0002]** However, such networks include various physical and virtual vulnerabilities, and a small minority of people will try and take advantage of these vulnerabilities to profit from fraudulent and other deceitful acts. Therefore, network providers will continue to improve the telecommunications networks, their components, and/or devices and systems that utilize the networks, with technology capable of preventing or deterring nefarious actors from attempting to exploit the network weaknesses.

### BRIEF DESCRIPTION OF THE DRAWINGS

**[0003]** Embodiments of the present technology will be described and explained through the use of the accompanying drawings.

**[0004]** Figure 1 is a block diagram illustrating a suitable network environment of devices and components representing nodes of a blockchain network.

**[0005]** Figure 2A is a block diagram illustrating communications between two separate devices represented as nodes of a blockchain network.

**[0006]** Figure 2B is a block diagram illustrating communications between a device and a network component, where both are represented as nodes of a blockchain network.

**[0007]** Figure 2C is a block diagram illustrating communications between network components represented as nodes of a blockchain network.

**[0008]** Figure 3 is a block diagram illustrating a network of vehicles communicating as nodes on a blockchain network.

**[0009]** Figure 4 is a block diagram illustrating a network of vehicles and infrastructure communicating as nodes on a blockchain network.

**[0010]** Figure 5 is a flow diagram illustrating a method of performing actions for a vehicle based on messages received from other vehicles.

**[0011]** Figure 6 is a flow diagram illustrating a method of performing actions based on information received from an infrastructure system or device.

**[0012]** The drawings have not necessarily been drawn to scale. Similarly, some components or operations can be separated into different blocks or combined into a single block for discussion of some of the embodiments of the present technology. Moreover, while the technology is amenable to various modifications and alternative forms, specific embodiments have been shown by way of example in the drawings and are described in detail below. The intention, however, is not to limit the technology to the particular embodiments described. On the contrary, the technology is intended to cover all modifications, equivalents, and alternatives falling within the scope of the technology as defined by the appended claims.

## DETAILED DESCRIPTION

### Overview

**[0013]** Systems and methods are described herein for providing blockchain functionality to a telecommunications network, its components, and devices and systems that communicate over the telecommunications network. The systems and methods (collectively, “systems”) can implement devices, systems, components, and so on with agents or other modules that transform or establish them as nodes (or sub-nodes) distributed across a network, such as nodes of a blockchain network.

**[0014]** For example, vehicles and infrastructure (e.g., buildings, smart homes, traffic devices, utilities and associated systems, emergency response systems, and so

on) can be configured to include blockchain nodes, such that a smart city or area can be supported by a blockchain network, with any devices and systems provisioned with nodes acting as distributed nodes for the blockchain network.

**[0015]** By utilizing aspects of a blockchain network, the smart city or area can self-regulate or self-manage operations within the network. Thus, the systems and devices can utilize the blockchain to determine when communications between devices are trustworthy (e.g., not compromised and communications are legitimately from the devices), among other benefits.

**[0016]** In some implementations, provisioning vehicles with blockchain nodes can facilitate reliable and trustworthy communications between the vehicles (e.g., V2V communications), and/or communications between vehicles and infrastructure systems to devices (e.g., V2X communications).

**[0017]** For example, the systems receive, at a blockchain node within a computing system of a vehicle, a message from another vehicle within a vicinity of the vehicle, where the message from the other vehicle includes information associated with a route currently traveled by the vehicle. The systems then determine, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain associated with a telecommunications network that facilitates communications between the vehicle and the other vehicle. When the other vehicle is verified by the blockchain operation, the systems perform an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle.

**[0018]** Thus, vehicles, including autonomous vehicles, can include a system within a connected area network of the vehicle that includes a blockchain node. The node determines, based on information maintained by a blockchain for a telecommunications network, whether signals sent to the autonomous vehicle from one or more devices in a vicinity of the autonomous vehicle are trustworthy signals. An action module then causes an action associated with the vehicle to be performed in response to the signals from the one or more devices when the blockchain node determines that the signals are trustworthy.

**[0019]** Provisioning infrastructure devices and systems with blockchain nodes can facilitate reliable and trustworthy communications between various entities

associated with the infrastructure devices and systems (e.g., emergency response systems, security systems, and so on), and recipients of messaging and other communications (e.g., end users or devices).

**[0020]** For example, the systems receive, at a blockchain node of a computing device, an alert from an infrastructure device, where the alert from the infrastructure device includes information identifying an abnormal condition at the infrastructure device. The systems then determine, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified on a blockchain associated with a telecommunications network that facilitates communications between the computing device and the infrastructure device. When the infrastructure device is determined to be verified by the blockchain operation, the systems perform an action to respond to the alert from the infrastructure device.

**[0021]** Thus, a computing device can include a system for monitoring operations of devices within a smart city. The system can include a blockchain node, contained by a device within the smart city, that determines, based on information maintained by a blockchain for a telecommunications network associated with the smart city, whether signals sent to device from other devices within the smart city are trustworthy signals. Further, the system can include an action module that causes certain actions to be performed in response to the signals from the other devices when the blockchain node determines that the signals are trustworthy.

**[0022]** Therefore, the systems can provision some or all devices and systems of an area or city with blockchain nodes, in order to build, manage, and utilize a blockchain or distributed ledger for the area or city when determining whether communications (e.g., messages or data communications) are trustworthy and sent from known and reliable devices or systems, among other benefits.

**[0023]** In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of embodiments of the present technology. It will be apparent, however, that embodiments of the present technology can be practiced without some of these specific details.

### Examples of Telecommunication Networks as Blockchain Networks of Nodes

**[0024]** As described herein, in some embodiments, the systems manage devices, components, and systems of or associated with a telecommunications network as nodes on a blockchain network. Devices, therefore, function as nodes (or sub-nodes) that are distributed across the blockchain network.

**[0025]** Nodes on a blockchain network perform various functions for the network. They process transactions and maintain copies (e.g., replicated databases or ledgers) of the blockchain. Thus, the distributed nodes combine to be the blockchain network. For example, with respect to cryptocurrencies (e.g., Bitcoin), the nodes check new currency transactions against a consensus protocol, which is a uniform system of agreement between all the nodes of the network when validating transactions processed by the nodes. Therefore, a node itself, relying on the consensus protocol, determines whether to validate transactions at the node.

**[0026]** There can be different types of nodes, such as full nodes, sub-nodes, and agents. Full nodes maintain a complete copy of every block (e.g., record) and transaction within the blockchain network, and validate the blocks/transactions against the consensus protocol. Sub-nodes and agents, however, can only validate their own transactions. In some cases, a group of sub-nodes or agents can act, together, as a node or full node. Further, nodes, sub-nodes, and agents can act as endpoint nodes (when communications between nodes in the network end or terminate) or as redistribution nodes (where communications are redistributed to other nodes of the network).

**[0027]** Telecommunication networks are well suited to managing communications between components (e.g., devices, cells, access points, registers, databases, gateways, and so on) by representing the components as nodes of blockchain networks. For example, any devices associated with the network, communicating via the network, and/or within or providing the network, can be nodes and function to validate transactions, authenticate other devices, perform actions or operations, or otherwise communicate over the network based on blockchain transactions.

**[0028]** Figure 1 is a block diagram illustrating a suitable network environment 100 of devices and components representing nodes of a blockchain network. As depicted,

a telecommunications network 110 can extend into virtually any area, location, structure, or environment, providing services to devices and systems of all scales - from mobile devices to smart homes and other single structures, to communities, cities, and other groups of structures or devices.

**[0029]** The telecommunications network is provided via a network architecture 120, such as the various components that provide communication services (e.g., voice calls, text and other messaging, data communications, and so on) to mobile devices and other user equipment. As described herein, the network architecture can include access points or networks, gateways, core networks components (e.g., operations components, packet control components, policy control functions, charging components, subscriber databases, and so on), and so on.

**[0030]** Devices, systems, and geographical areas can access the telecommunications network 110 through a variety of different sites, access points, and/or networks. For example, a small cell site (e.g., a femtocell, picocell, or other small cell) 130 can provide access to the network 110 to a small or targeted area, such as a smart home hub 132 and its various connected (internet of things, or IoT) devices 134, 136. The small cell site 130 can provide access to the smart home hub 132 and the devices 134, 136 directly (as well as any mobile devices), or the devices can access the network 110 via the smart home hub 132.

**[0031]** In addition to the small cell site 130, the devices, systems, and/or areas can access the network 110 via base stations or other cell sites, such as base station 140. For example, mobile devices 142, 144 can communicate over the network 110 by accessing the network 110 via the base station 140.

**[0032]** Further, devices, systems, and/or other areas, such as smart cities and their various components and infrastructure can access the network 110 via provisioned access networks 150, such as access networks 150 supported by access points 155 (e.g., wireless access points, hotspots, routers, and so on), or other cell sites 160 (e.g., small cells or base stations positioned to service specific areas or centers).

**[0033]** For example, a smart city 170 can include structures 172 (e.g., houses, buildings, schools, hospitals, and so on) that connect to the network 110 via the access network 150. Vehicles 174 can also access the network 110 via the access network

150. Further, various utilities 176 and their systems or devices (e.g., electric grid components, water systems, gas or other fuel systems, wireless infrastructure systems, emergency response systems, and so on), can communicate over the network 110. Also, devices 178 (e.g., traffic lights and other devices, street lamps, parking meters, and so on), access the network 110 via the access network 150.

**[0034]** Some or all of these systems and devices 172, 174, 176, 178 can communicate with one another via the network 110. For example, vehicles 174 can communicate with other vehicles 174, or with certain devices 178 (e.g., traffic lights), or with services provided by utilities 176 (e.g., emergency response services), or with structures 172 (e.g., smart home devices) over the network 110. As another example, a utility (e.g., the electric grid) can communicate with other utilities (e.g., the emergency response system), with vehicles 174, and so on.

**[0035]** Thus, in some embodiments, the telecommunications network 110 (managed by the network architecture 120) provides communication services to a wide range of all the different devices and systems capable of communications – from single mobile devices 142, 144 to large-scale connected cities 170 of devices, systems, and structures. Further, although Figure 1 depicts examples of how these device and systems access the network 110, other configurations are possible. For example, mobile device 142 can access the network 110 via small cell site 130, and IoT device 132 can access the network 110 via the base station 140, among other configurations.

**[0036]** As described herein, some or all of the devices or systems depicted in Figure 1 or the other Figures can act as or be configured to function as a node or sub-node of a blockchain network. A node or sub-node can be implemented as a module, agent, or another component of a device or system. The agents or modules can be functional modules or engines that are implemented with a combination of software (e.g., executable instructions, or computer code) and hardware (e.g., at least a memory and processor). Accordingly, as used herein, in some examples a module or engine is a processor-implemented module or set of code and represents a computing device having a processor that is at least temporarily configured and/or programmed by executable instructions stored in memory to perform one or more of the particular functions that are described herein.

**[0037]** As nodes (or sub-nodes), the devices or systems function to maintain a distributed ledger (e.g., a blockchain) of transactions. Further, the devices or systems can collaboratively function to validate, verify, certify, or authenticate data and/or transactions communicated between the nodes. Thus, the devices or systems, working as nodes of a blockchain network, operate to provide security, reliability, and/or redundancy between themselves and various portions or segments of the telecommunications network 110.

**[0038]** The blockchain, being associated with the network and various devices or systems, can be configured to track or store information specific to communications over the network. For example, blockchain transactions can include information identifying a location of a user or device (e.g., GPS information, cell tower or base station information, access point information, and so on), device or user identifiers, such as Mobile Station International Subscriber Directory Number (MSISDN) or International Mobile Equipment Identity (IMEI) information, biometric information and other biological or physical user identifiers, and so on.

**[0039]** For example, a device can access a network and run an instance of an Ethereum virtual machine, and utilize various device or network-specific information when authenticating onto the network via various blockchain transactions. The blockchain, tracking and maintaining such information, can then authenticate the device via the information with a high degree of confidence, knowing that the actual device (or the person behind the device) is valid and authorized to access the network.

**[0040]** To that end, the devices or systems, as nodes, can perform specific functions when communicating with other devices or systems, depending on their role within the network 110 or how they are being utilized. For example, a mobile device (e.g., mobile device 142), can act as an endpoint node of a blockchain network, whereas a gateway component of the network architecture 120 can function as a redistribution node.

**[0041]** Following the example, the mobile device, when communicating with other devices, can compare perform blockchain transactions to compare certificates of other devices in communication with the mobile device, whereas the gateway component can maintain a complete ledger of an entire network of blocks or transactions, and allow access to core network components when both requesting

device and core network components are verified by the gateway component. Figures 2A-2C provide examples of such functionality for different devices, components, or systems.

**[0042]** Figure 2A is a block diagram illustrating communications 200 between two separate devices represented as nodes of a blockchain network. For example, a device 210 can send a message to a device 220 over the network 110. The device can also send, via a node component 215 or similar agent associated with the device 210, a certificate or other identifier of the device. The device 220, via its node component or agent, can verify the device 210 based on the transmitted certificate.

**[0043]** For example, the device 220 can compare the credentials of the device 210 with one or more previous transactions performed by the device 210 on the network. When the credentials are associated with authenticated or acceptable transactions (or previous verifications), the device 220 verifies the device 210 to the network 110 (enabling the device 210 to utilize all or certain services provided by the network 210). Upon verification, the device 220 can transmit a verification message back to the device 210 (which can add the message to the blockchain via the node 215). Thus, in some embodiments, one device can verify and/or authenticate another device to the network 110 or other devices or systems associated with the network 110 by utilizing blockchain processes.

**[0044]** Figure 2B is a block diagram illustrating communications 230 between a device and a network component, where both are represented as nodes of a blockchain network. For example, the device 210 can send a message to a network component 240 (e.g., a network component of architecture 120), such as when attempting to access the network 110 via one or more access points. The device 210, via its associated agent 250, transmits information to the network component 240, which compares the information, via its associated blockchain node 245, to records of the blockchain, in order to validate the device 210 to the network 110.

**[0045]** For example, such as process can occur every time the device 210 accesses the network 110, or in response to potential attempts to access the network 110 without permission or knowledge of the various network components 240. Once validated, the node 245 adds a transaction to the blockchain representing activity within the network 110, and the device 210 communicates over the network 110 as

requested. Thus, in some embodiments, network components 240 can, at each or some of the components, perform validation processes for a device that attempts to access services provided by the network 210.

**[0046]** Figure 2C is a block diagram illustrating communications 260 between network components represented as nodes of a blockchain network. At times, one network component 270 can perform various blockchain processes in order to permit another network component (e.g., component 240) to perform its intended functions for the network 110.

**[0047]** For example, the network component 240 can, via its agent 245, send a message to the network component 270 as part of a normal core network function or process. To avoid perpetuating messages from a compromised component, the network component 270 can, via its node 275, compare the message to the blockchain, and give permission for the network component 240 to continue to operate within the network 110. Thus, in some embodiments, the network components themselves can act as nodes of a blockchain in order to maintain the integrity and reliability of operation and processes of the telecommunications network 110.

**[0048]** Thus, in various embodiments, the telecommunications network 110 utilizes the functionality of a distributed ledger to provide various components, devices, or systems with the means to act as authentication, validation, or verification interfaces for the network 110. The following section illustrates details for specific embodiments employing such functionality.

**[0049]** Figure 1 and the discussion herein provide a brief, general description of a suitable computing environment in which devices and network components function as nodes on a blockchain network can be supported and implemented. Although not required, aspects of the various components or systems are described in the general context of computer-executable instructions, such as routines executed by a general-purpose computer, e.g., mobile device, a server computer, or personal computer. The system can be practiced with other communications, data processing, or computer system configurations, including: Internet appliances, hand-held devices (including tablet computers and/or personal digital assistants (PDAs)), all manner of cellular or mobile phones, multi-processor systems, microprocessor-based or programmable consumer electronics, set-top boxes, network PCs, mini-computers, mainframe

computers, and the like. Indeed, the terms "computer," "host," and "host computer," and "mobile device" and "handset" are generally used interchangeably herein, and refer to any of the above devices and systems, as well as any data processor.

**[0050]** Aspects of the system can be embodied in a special purpose computing device or data processor that is specifically programmed, configured, or constructed to perform one or more of the computer-executable instructions explained in detail herein. Aspects of the system can also be practiced in distributed computing environments where tasks or modules are performed by remote processing devices, which are linked through a communications network, such as a Local Area Network (LAN), Wide Area Network (WAN), or the Internet. In a distributed computing environment, program modules can be located in both local and remote memory storage devices.

**[0051]** Aspects of the system can be stored or distributed on computer-readable media (e.g., physical and/or tangible non-transitory computer-readable storage media), including magnetically or optically readable computer discs, hard-wired or preprogrammed chips (e.g., EEPROM semiconductor chips), nanotechnology memory, or other data storage media. Indeed, computer implemented instructions, data structures, screen displays, and other data under aspects of the system can be distributed over the Internet or over other networks (including wireless networks), on a propagated signal on a propagation medium (e.g., an electromagnetic wave(s), a sound wave, etc.) over a period of time, or they can be provided on any analog or digital network (packet switched, circuit switched, or another scheme). Portions of the system can reside on a server computer, while corresponding portions can reside on a client computer such as a mobile or portable device, and thus, while certain hardware platforms are described herein, aspects of the system are equally applicable to nodes on a network. In an alternative embodiment, the mobile device or portable device can represent the server portion, while the server can represent the client portion.

**[0052]** In some embodiments, the devices can include network communication components that enable the devices to communicate with remote servers or other portable electronic devices by transmitting and receiving wireless signals using a licensed, semi-licensed, or unlicensed spectrum over communications networks. In some cases, the telecommunication network can be comprised of multiple networks, even multiple heterogeneous networks, such as one or more border networks, voice

networks, broadband networks, service provider networks, Internet Service Provider (ISP) networks, and/or Public Switched Telephone Networks (PSTNs), interconnected via gateways operable to facilitate communications between and among the various networks. The communications network can also include third-party communications networks such as a Global System for Mobile (GSM) mobile communications network, a code/time division multiple access (CDMA/TDMA) mobile communications network, a 3rd or 4th generation (3G/4G) mobile communications network (e.g., General Packet Radio Service (GPRS/EGPRS)), Enhanced Data rates for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS), or Long Term Evolution (LTE) network), 5G mobile communications network, IEEE 802.11 (WiFi), or other 3GPP or non-3GPP communications networks.

#### Examples of Determining Communications Over a Network are Trustworthy

**[0053]** As described herein, in some embodiments, the systems and methods configure devices and systems (such as devices and systems that are part of the smart city 170) to themselves determine whether the communications (e.g., messages, data, voice, and so on), originate or come from trustworthy sources, such as other devices and systems.

**[0054]** In some cases, the systems and devices interacting with one another can be vehicles, such as autonomous vehicles, electric vehicles, or any other vehicles that contain a controller area network (CAN) or other computer system or network that manages sensors and controls some or all aspects of the operation of the vehicle. Figure 3 is a block diagram illustrating a network of vehicles 300 communicating as nodes on a blockchain network.

**[0055]** Vehicles 174A-C can communicate over the telecommunications network 110, provided as a wireless, LTE, IMS, or other type of network by the network architecture 120. The vehicles 174A-C can include computing devices or systems that facilitate connections between the network 110 and the vehicles 174A-C. Thus, in some cases, a vehicle as described herein is a connected vehicle.

**[0056]** As an example, a connected vehicle can connect to the network 110 via one or more network devices attached or provided to the vehicle, such as the T-Mobile® Sync Up Drive™, which connects to an on board diagnostic (OBD) reader,

such as via an OBD-II port of a dashboard of the vehicle, or other controller area network (CAN) bus components or devices of the connected vehicle. The attached devices can, for example, collect information and/or diagnose various events, issues, or changing statuses of the vehicle and its components, monitor and track the operation of the vehicle, and so on. The devices and/or internal computing systems, therefore, establish the connected vehicle as a device on the communications network 110.

**[0057]** Of course, other devices can provide similar information associated with the connected vehicle, such as a mobile device associated with drivers of the vehicles (e.g., who can be subscribers of the network 110), subscriber identity modules (SIM), such as eSIMs (or other dynamically reprogrammable modules), integrated with the vehicles, and/or other communication components that are part of the vehicles and/or devices within the vehicles and configured to communicate over the communications network 110.

**[0058]** In some cases, the vehicles 174A-C can include various sensors that facilitate the capturing of information associated with the vehicles and their surroundings. The vehicles 174A-C can include ultrasonic sensors, radar sensors, imaging sensors, GPS or accelerometers, and so on.

**[0059]** The vehicles can also include vehicle-to-vehicle communication (V2V) components, which enable vehicles to communicate with one another (in real-time), such as relay information from one vehicle to another. For example, the vehicle 174C can be further ahead on a route of travel, and relay information 174A back to the vehicle 174C that identifies potential issues encountered along the route - traffic, environmental conditions, vehicle movements (e.g., lane changes), vehicle problems (e.g., notification of a flat tire), and so on. Some example V2V applications include Intersection Movement Assist (IMA) applications, Left Turn Assist (LTA) applications, and so on.

**[0060]** Autonomous vehicles, in some cases, can be specifically reliant, and therefore vulnerable, to communications between vehicles that are untrustworthy, or unreliable, such as communications sent by compromised vehicles (or compromised systems within the vehicles).

**[0061]** Therefore, as described herein, the systems may provision or equip the vehicles 174A-C with nodes 310, 320, and 330, which perform blockchain operations to determine whether communications received from other vehicles are reliable and come from trustworthy sources.

**[0062]** As depicted, some or all of the vehicles 174A-C that communicate over the network 110 can be configured or provisioned to include a blockchain node, such as a node that includes a blockchain agent configured to perform blockchain transactions, operations, or other processes associated with a blockchain or ledger, which tracks and maintains a history of all transactions performed within the telecommunications network 110 by the vehicles 174A-C.

**[0063]** In some embodiments, the nodes are implemented as JavaScript modules (e.g., "Node.js"), or other similar modules (e.g., Solidity modules) and the ledger or blockchain is configured as JavaScript array. Thus, each vehicle 174A-C can include a blockchain node. A vehicle, having a blockchain node, is capable of accessing a full copy of the blockchain representing the network 110, performing operations associated with the blockchain, and adding transaction data (e.g., blocks) to the blockchain associated with activities and actions performed by the vehicle and/or other vehicles of the network 110.

**[0064]** In addition to vehicles 174A-C, the smart city 170 can include various infrastructure entities. Figure 4 is a block diagram illustrating a network of vehicles and infrastructure 400 communicating as nodes on a blockchain network.

**[0065]** The network 400 includes the structures 172, utilities 176, and devices 178 described herein. For example, pole stations, traffic signals, and other smart road or smart city devices 178 (e.g., such as 5G micro base stations placed in buildings, on utility poles, and so on) can be connected to the network 110, and facilitate exchanges of information between the vehicles 174A-C and the network 110. Similarly, one or more networked devices can communicate with a vehicle when it is parked at home, in a parking garage, or in a parking space. Therefore, in some cases, a vehicle can encounter and exchange information with various networked devices when travelling, and the devices provide the access to the communications network 110.

**[0066]** Further, the infrastructure entities can communicate, over the network 110, with a user device 440, such as a mobile device, laptop, tablet, and so on,

associated with a user and configured to monitor, track, analyze, and/or provide a status about operations at the entities and/or other information associated with the structures 172, vehicles 174, utilities 176, devices 178, and so on, of the smart city 170.

**[0067]** For example, one or more devices 178, such as utility meters (e.g., automatic meter reading (AMR) devices) can send information over the network 110 to the user device 440 that indicates consumption of a utility, status of operation of a utility at a structure 172, and so on. Other devices 178 can send status information, alerts, or other signals, such as alerts that indicate an emergency at a location or area, signals that provide information to other devices 178, vehicles, and so on, or other information or data.

**[0068]** For example, with respect to vehicles, the network 110 can facilitate vehicle-to-everything (V2X) communications, such as communications between the vehicles 174A-C and pedestrians (e.g., at user device 440), roadway or traffic devices (e.g., traffic signals such as smart signals, stoplights, digital signs, lighting, parking meters, charging systems, and other smart devices or systems along a route of travel), and so on.

**[0069]** In addition, the infrastructure entities can include smart grid components (e.g., power stations, transformers, and so on, network infrastructure components, light poles), retail environments, emergency response devices, systems, or entities, cameras, smart home or building sensors (e.g. temperature sensors, gas or fire alarms, and so on), campus or area grid systems, and so on.

**[0070]** As described herein, the systems may provision or equip the infrastructure entities with nodes 410, 420, and 430, as well as the user device with node 445. The nodes 410, 420, 430, 445 can perform blockchain operations to determine whether communications between entities are trustworthy and not originating from compromised entities (e.g., poison pill entities) that can harm the network 110 or the infrastructure entities.

**[0071]** The nodes 410, 420, 430, 445 include a blockchain agent configured to perform blockchain transactions, operations, or other processes associated with a blockchain or ledger, which tracks and maintains a history of some or all transactions performed within the telecommunications network 110 within the smart city 170.

**[0072]** As described herein, in some embodiments, the nodes are implemented as JavaScript modules (e.g., “Node.js”), or other similar modules (e.g., Solidity modules) and the ledger or blockchain is configured as JavaScript array. Thus, each vehicle 174A-C can include a blockchain node. A system or device, having a blockchain node, is capable of accessing a full copy of the blockchain representing the network 110, performing operations associated with the blockchain, and adding transaction data (e.g., blocks) to the blockchain associated with activities and actions performed by the systems and devices of the network 110.

**[0073]** Thus, as depicted in Figures 3 and/or 4, the systems facilitate the managing and verifying of communications between vehicles and/or infrastructure over the communications network 110 by utilizing the vehicles 174A-C and infrastructure systems and devices 172, 174, 176, 178 as distributed nodes of a blockchain.

**[0074]** Figure 5 is a flow diagram illustrating a method of performing actions for a vehicle based on messages received from other vehicles. The method 500 can be performed by a blockchain node of a vehicle 174A-C (e.g., nodes 310, 320, 330), and, accordingly, is described herein merely by way of reference thereto. It will be appreciated that the method 500 can be performed on any suitable hardware or network component.

**[0075]** In operation 510, the blockchain node of a vehicle (e.g., a node contained by a CAN of a vehicle) receives a message from another vehicle within a vicinity of the vehicle. For example, the node can receive a message from another vehicle that includes information associated with a route currently traveled by the vehicle, or other vehicle-to-vehicle communications, as described herein.

**[0076]** Example messages, contents, or information that can be transmitted between vehicles includes information identifying a current traffic condition on the route of travel, a current weather condition on the route of travel, vehicle movement information, and so on.

**[0077]** For example, when the vehicles are autonomous vehicles, the information can include lane assist information, intersection movement assist information, left turn assist information, or other information or data for the other vehicle that identifies, to the vehicle, the movements of the other vehicle along the route of travel.

**[0078]** In operation 520, the blockchain node determines, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain associated with a telecommunications network that facilitates communications between the vehicle and the other vehicle. For example, the node can perform an operation associated with a blockchain for the network 110 to compare or otherwise identify blocks or transactions associated with the other vehicle that can be able to provide information that verifies the other vehicle as being legitimate, trustworthy, and/or non-compromised (e.g., operating as intended).

**[0079]** In some embodiments, the node can determine or place certain vehicles on a white list, gray list, or black list, depending upon the information contained on the blockchain for the vehicle. For example, when a blockchain operation indicates a vehicle has been stolen, the vehicle is placed on a blacklist, when a blockchain operation indicates a vehicle has not certified (via the blockchain or via one or more motor vehicle entities) within a certain time period, the vehicle is placed on a gray list, and when a vehicle has provided a root certificate or other verifiable information, the vehicle is on a white list.

**[0080]** Thus, in some cases, the blockchain operation can compare contents of the message received from the other vehicle with contents of previous messages transmitted from the other vehicle and contained by the blockchain, compare identification information for the other vehicle within contents of the message received from the another vehicle with identification information within contents of previous messages transmitted from the other vehicle and contained by the blockchain, determine that the other vehicle is verified when information within the message matches information contained by transactions of the blockchain that are associated with the other vehicle, and so on.

**[0081]** In operation 530, when the other vehicle is determined to be verified by the blockchain operation, the computing system of the vehicle performs an action (or, causes an action to be performed), associated with the vehicle based on the information associated with the route currently traveled by the vehicle. For example, the vehicle can change lanes, slow down or decelerate, speed up or accelerate, adjust or modify a planned route of travel, and so on.

**[0082]** In operation 540, when the other vehicle is determined not to be verified by the blockchain operation, the node retrieves route information from other sources (e.g., other devices connected to the vehicle via the network 110). For example, the node can request information from the other sources (e.g., traffic devices, other vehicles, and so on), in order to confirm or supplement information received from the unverified other vehicle.

**[0083]** In some cases, the node can pause or prevent performance of an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle until the information is confirmed by an additional source of information.

**[0084]** In operation 550, the computing system of the vehicle performs (or causes to be performed) the action associated with the vehicle based on the information associated with the route currently traveled by the vehicle and retrieved from the other sources. For example, similar to operation 530, the vehicle can change lanes, slow down or decelerate, speed up or accelerate, adjust or modify a planned route of travel, and so on.

**[0085]** Once or during performance of the action, the node, in some cases, can perform a transaction to the blockchain that includes a hash of a previous block in the blockchain, a timestamp for the transaction, and transaction data that identifies the action performed by the vehicle and information identifying the other vehicle that sent the message.

**[0086]** Thus, in some embodiments, the systems utilize blockchain nodes to verify V2V communications, V2X communications, and so on. As described herein, any vehicle can operate a distributed node of a blockchain, configured as a system within a computer area network of a vehicle (e.g., an autonomous vehicle) that includes a blockchain node that determines, based on information maintained by a blockchain for a telecommunications network, whether signals or information sent to the autonomous vehicle from one or more devices in a vicinity of the autonomous vehicle are trustworthy signals or information, and an action module that causes performance of an action associated with the vehicle in response to the signals or information from the one or more devices when the blockchain node determines that the signals are trustworthy.

**[0087]** As described herein, in addition to communications between vehicles and other vehicles, systems or devices (V2V and V2X communications), the systems described herein can configure infrastructure entities as distributed nodes of a blockchain associated with the network 110, in order to verify that communications originating from the entities are trustworthy and not compromised, among other benefits.

**[0088]** Figure 6 is a flow diagram illustrating a method 600 of performing actions based on information received from an infrastructure system or device. The method 600 can be performed by a blockchain node of the infrastructure entities (e.g., nodes 410, 420, 430, 445), and, accordingly, is described herein merely by way of reference thereto. It will be appreciated that the method 600 can be performed on any suitable hardware or network component.

**[0089]** In operation 610, a blockchain node of a computing device receives a message alert from an infrastructure device, where the message from the infrastructure device includes information identifying a current condition at the infrastructure device. For example, the node 445 of the user device 440 can receive an alert from one or more of the structures 172, utilities 176, or other devices 178, where the alert identifies an abnormal condition at the entity.

**[0090]** The alert or other message can indicate, for example, an emergency at a location that includes the infrastructure device, such as a power failure at the area at which power is provided via an electric grid, the triggering of a security alarm, smoke alarm, and so on at a location or within a structure, and so on.

**[0091]** As one example, when the infrastructure device 178 is a utility meter associated with a utility, the information identifying an abnormal condition at the infrastructure device can include information that indicates a failure of one or more components providing the utility (e.g., transmitting such information to an automated meter reading (AMR) device that automatically collects data from the utility meter). As another example, the infrastructure device is an emergency alert device for a location, and the computing device is a mobile device configured to alert an emergency responder of an emergency at the location.

**[0092]** In operation 620, the blockchain node of the computing device determines via a blockchain operation performed by the blockchain node, whether the

infrastructure device is verified on a blockchain associated with a telecommunications network that facilitates communications between the computing device and the infrastructure device. For example, the node can perform an operation associated with a blockchain for the network 110 to compare or otherwise identify blocks or transactions associated with the infrastructure device that can be able to provide information that verifies the device as being legitimate, trustworthy, and/or non-compromised (e.g., operating as intended).

**[0093]** Thus, in some cases, the blockchain operation can compare contents of a received message with contents of previous messages transmitted from the device and contained by the blockchain. The operation then compares identification information for the device within contents of the message received from the device with identification information within contents of previous messages transmitted from the device and contained by the blockchain. The operation can then determine that the device is verified when information within the message matches information contained by transactions of the blockchain that are associated with the device, and so on.

**[0094]** When the infrastructure device is determined to be verified by the blockchain operation, the user device, in operation 630, performs (or causes to be performed) an action to respond to the message from the infrastructure device. For example, the user device 445 can automatically respond to the message to mitigate an abnormal condition at the infrastructure device, to alert users (e.g., emergency responders) or send notifications of certain conditions or statuses at a location, and so on.

**[0095]** When the infrastructure device is determined not to be verified by the blockchain operation, the blockchain node of the user device performs an action to prevent or otherwise mitigate the infrastructure device from transmitting additional messages to other computing devices. For example, the node can send messages to other devices to ignore messages from the device, determined to be compromised. The node can also alert a user associated with the user device that the compromised device is transmitting erroneous or nefarious messages to devices over the network 110.

**[0096]** In some cases, the blockchain node of the computing device can perform a transaction to the blockchain that includes a hash of a previous block in the blockchain, a timestamp for the transaction, and transaction data that identifies the action performed to respond to the message from the infrastructure device.

**[0097]** Thus, the systems can configure infrastructure entities as distributed nodes of a blockchain. Each of the structure 172, utilities 176, or devices 178 can include a system for monitoring operations of devices within a smart city, including a blockchain node, contained by a device within the smart city. The system determines, based on information maintained by a blockchain for a telecommunications network associated with the smart city, whether signals sent to device from other devices within the smart city are trustworthy signals. An action module of the system then causes performance of actions associated in response to the signals from the other devices when the blockchain node determines that the signals are trustworthy.

**[0098]** Thus, in some embodiments, the systems enable a smart city to monitor itself by utilizing vehicles and entities within the city (or other location) as distributed nodes of a blockchain. The city can then utilize any node when checking the validity or trustworthiness of communications over a network, and perform actions, when appropriate, to mitigate compromised devices or systems, among other benefits.

#### Conclusion

**[0099]** Unless the context clearly requires otherwise, throughout the description and the claims, the words "comprise," "comprising," and the like are to be construed in an inclusive sense, as opposed to an exclusive or exhaustive sense; that is to say, in the sense of "including, but not limited to." As used herein, the terms "connected," "coupled," or any variant thereof means any connection or coupling, either direct or indirect, between two or more elements; the coupling or connection between the elements can be physical, logical, or a combination thereof. Additionally, the words "herein," "above," "below," and words of similar import, when used in this application, refer to this application as a whole and not to any particular portions of this application. Where the context permits, words in the above Detailed Description using the singular or plural number can also include the plural or singular number respectively. The word "or," in reference to a list of two or more items, covers all of the following interpretations

of the word: any of the items in the list, all of the items in the list, and any combination of the items in the list.

**[00100]** As used herein, being above a threshold means that a value for an item under comparison is above a specified other value, that an item under comparison is among a certain specified number of items with the largest value, or that an item under comparison has a value within a specified top percentage value. As used herein, being below a threshold means that a value for an item under comparison is below a specified other value, that an item under comparison is among a certain specified number of items with the smallest value, or that an item under comparison has a value within a specified bottom percentage value. As used herein, being within a threshold means that a value for an item under comparison is between two specified other values, that an item under comparison is among a middle specified number of items, or that an item under comparison has a value within a middle specified percentage range.

**[00101]** The above Detailed Description of examples of the technology is not intended to be exhaustive or to limit the technology to the precise form disclosed above. While specific examples for the technology are described above for illustrative purposes, various equivalent modifications are possible within the scope of the technology. For example, while processes or blocks are presented in a given order, alternative implementations can perform routines having steps, or employ systems having blocks, in a different order, and some processes or blocks can be deleted, moved, added, subdivided, combined, and/or modified to provide alternative or subcombinations. Each of these processes or blocks can be implemented in a variety of different ways. Also, while processes or blocks are at times shown as being performed in series, these processes or blocks can instead be performed or implemented in parallel, or can be performed at different times. Further any specific numbers noted herein are only examples: alternative implementations can employ differing values or ranges.

**[00102]** The teachings of the technology provided herein can be applied to other systems, not necessarily the system described above. The elements and acts of the various examples described above can be combined to provide further implementations of the technology. Some alternative implementations of the

technology can include not only additional elements to those implementations noted above, but also can include fewer elements.

**[00103]** These and other changes can be made to the technology in light of the above Detailed Description. While the above description describes certain examples of the technology, and describes the best mode contemplated, no matter how detailed the above appears in text, the technology can be practiced in many ways. Details of the system can vary considerably in its specific implementation, while still being encompassed by the technology disclosed herein. As noted above, particular terminology used when describing certain features or aspects of the technology should not be taken to imply that the terminology is being redefined herein to be restricted to any specific characteristics, features, or aspects of the technology with which that terminology is associated. In general, the terms used in the following claims should not be construed to limit the technology to the specific examples disclosed in the specification, unless the above Detailed Description section explicitly defines such terms. Accordingly, the actual scope of the technology encompasses not only the disclosed examples, but also all equivalent ways of practicing or implementing the technology under the claims.

**[00104]** Certain aspects of the technology are presented below in certain claim forms reduce the number of claims, but the applicant contemplates the various aspects of the technology in any number of claim forms. For example, while only one aspect of the technology is recited as a computer-readable medium claim, other aspects can likewise be embodied as a computer-readable medium claim, or in other forms, such as being embodied in a means-plus-function claim. Any claims intended to be treated under 35 U.S.C. § 112(f) will begin with the words "means for", but use of the term "for" in any other context is not intended to invoke treatment under 35 U.S.C. § 112(f). Accordingly, the applicant reserves the right to pursue additional claims after filing this application to pursue such additional claim forms, in either this application or in a continuing application.

## CLAIMS

What is claimed is:

1. A non-transitory computer-readable medium whose contents, when executed by a computing system of a vehicle, cause the computing system to perform a method, the method comprising:

receiving, at a blockchain node within the computing system of the vehicle, a message from another vehicle within a vicinity of the vehicle, wherein the message from the other vehicle includes information associated with a route currently traveled by the vehicle;

determining, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain associated with a telecommunications network that facilitates communications between the vehicle and the other vehicle; and

when the other vehicle is determined to be verified by the blockchain operation, performing an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle.

2. The non-transitory computer-readable medium of claim 1, further comprising:

when the other vehicle is determined not to be verified by the blockchain operation:

retrieving route information from other sources; and

performing the action associated with the vehicle based on the information associated with the route currently traveled by the vehicle and retrieved from the other sources.

3. The non-transitory computer-readable medium of claim 1, further comprising:

when the other vehicle is determined to not be a trustworthy source of information by the blockchain operation, pausing performance of an action associated with the vehicle based on the information associated

with the route currently traveled by the vehicle until the information is confirmed by an additional source of information.

4. The non-transitory computer-readable medium of claim 1, wherein the blockchain node within the computing system of the vehicle includes a Javascript script that acts as a blockchain agent for the computing system that is configured to operate as a distributed node for the blockchain associated with the telecommunications network.

5. The non-transitory computer-readable medium of claim 1, further comprising:

performing, by the blockchain node within the computing system of the vehicle, a transaction to the blockchain that includes a hash of a previous block in the blockchain, a timestamp for the transaction, and transaction data that identifies the action performed by the vehicle and information identifying the other vehicle that sent the message.

6. The non-transitory computer-readable medium of claim 1, wherein determining, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain includes comparing contents of the message received from the other vehicle with contents of previous messages transmitted from the other vehicle and contained by the blockchain.

7. The non-transitory computer-readable medium of claim 1, wherein determining, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain includes comparing identification information for the other vehicle within contents of the message received from the other vehicle with identification information within contents of previous messages transmitted from the other vehicle and contained by the blockchain.

8. The non-transitory computer-readable medium of claim 1, wherein determining, via a blockchain operation performed by the blockchain node, whether the other vehicle is verified on a blockchain includes determining that the other vehicle

is verified when information within the message matches information contained by transactions of the blockchain that are associated with the other vehicle.

9. The non-transitory computer-readable medium of claim 1, wherein the information associated with a route currently traveled by the vehicle includes information identifying a current traffic condition along the route currently traveled by the vehicle.

10. The non-transitory computer-readable medium of claim 1, wherein the vehicle and the other vehicle are autonomous vehicles, and wherein the information associated with a route currently traveled by the vehicle includes lane assist information.

11. The non-transitory computer-readable medium of claim 1, wherein the vehicle and the other vehicle are autonomous vehicles, and wherein the information associated with a route currently traveled by the vehicle includes intersection movement assist information.

12. The non-transitory computer-readable medium of claim 1, wherein the vehicle and the other vehicle are autonomous vehicles, and wherein the information associated with a route currently traveled by the vehicle includes left turn assist information.

13. The non-transitory computer-readable medium of claim 1, wherein performing an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle includes causing the vehicle to decelerate.

14. The non-transitory computer-readable medium of claim 1, wherein performing an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle includes causing the vehicle to accelerate.

15. The non-transitory computer-readable medium of claim 1, wherein performing an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle includes causing the vehicle to change lanes.

16. The non-transitory computer-readable medium of claim 1, wherein performing an action associated with the vehicle based on the information associated with the route currently traveled by the vehicle includes modifying a GPS planned route of travel for the vehicle.

17. A method performed by a telecommunications network, the method comprising:

receiving, at a blockchain node within a computing system of a vehicle, a message from a device within a vicinity of the vehicle,  
determining, via a blockchain operation performed by the blockchain node, whether the device is verified on a blockchain associated with the telecommunications network,  
wherein the telecommunications network facilitates communications between the vehicle and the device; and  
when the device is determined to be verified by the blockchain operation, performing an action associated with the vehicle based on the information received from the device.

18. The method of claim 17, further comprising:

when the device is determined not to be verified by the blockchain operation:  
retrieving information from other devices within the vicinity of the vehicle;  
and  
performing the action associated with the vehicle based on the information retrieved from the other sources.

19. The method of claim 17, wherein the device is a device operating to control travel of vehicles within the vicinity of the vehicle.

20. A system within a connected area network of an autonomous vehicle, the system comprising:

- a blockchain node that determines, based on information maintained by a blockchain for a telecommunications network, whether signals sent to the autonomous vehicle from one or more devices in a vicinity of the autonomous vehicle are trustworthy signals; and
- an action module that causes performance of an action associated with the vehicle in response to the signals from the one or more devices when the blockchain node determines that the signals are trustworthy.

21. A non-transitory computer-readable medium whose contents, when executed by a computing system, cause the computing system to perform a method, the method comprising:

- receiving, at a blockchain node of a computing device, an alert from an infrastructure device within a smart city of infrastructure devices, wherein the infrastructure device is a device that monitors conditions at a structure, location, or utility within the smart city of infrastructure devices;
- wherein the alert from the infrastructure device includes information identifying an abnormal condition at the infrastructure device;
- determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified on a blockchain associated with a telecommunications network that facilitates communications between the computing device and the infrastructure device within the smart city; and
- when the infrastructure device is determined to be verified by the blockchain operation, performing an action to respond to the alert from the infrastructure device.

22. The non-transitory computer-readable medium of claim 21, wherein the infrastructure device transmits alert associated with emergency conditions at a structure, location, or utility within the smart city, the method further comprising:

when the infrastructure device is determined not to be verified by the blockchain operation:

performing an action to prevent the infrastructure device from transmitting additional alerts associated with emergency conditions at the structure, location, or utility within the smart city to other computing devices.

23. The non-transitory computer-readable medium of claim 21, wherein the blockchain node of the computing device includes a Javascript script that acts as a blockchain agent for the computing device and is configured to operate as a distributed node for the blockchain associated with the telecommunications network.

24. The non-transitory computer-readable medium of claim 21, further comprising:

performing, by the blockchain node of the computing device, a transaction to the blockchain that includes a hash of a previous block in the blockchain, a timestamp for the transaction, and transaction data that identifies the action performed to respond to the alert from the infrastructure device.

25. The non-transitory computer-readable medium of claim 21, wherein determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified includes comparing contents of the alert received from the infrastructure device with contents of previous alerts transmitted from the infrastructure device.

26. The non-transitory computer-readable medium of claim 21, wherein determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified includes comparing credential information within the alert received from the infrastructure device with credential information of previous alerts transmitted from the infrastructure device.

27. The non-transitory computer-readable medium of claim 21, wherein the information identifying an abnormal condition at the infrastructure device includes

information that indicates an emergency at a location that includes the infrastructure device.

28. The non-transitory computer-readable medium of claim 21, wherein the infrastructure device is part of an electric grid providing power to an area, and wherein the information identifying an abnormal condition at the infrastructure device includes information that indicates a power failure at the area at which power is provided via the electric grid.

29. The non-transitory computer-readable medium of claim 21, wherein the infrastructure device is a utility meter associated with a utility, and wherein the information identifying an abnormal condition at the infrastructure device includes information that indicates a failure of one or more components providing the utility.

30. The non-transitory computer-readable medium of claim 21, wherein performing an action to respond to the alert from the infrastructure device includes automatically responding to the alert to mitigate the abnormal condition at the infrastructure device.

31. The non-transitory computer-readable medium of claim 21, wherein performing an action to respond to the alert from the infrastructure device includes sending a notification to one or more users that identifies the abnormal condition at the infrastructure device.

32. A method performed by a telecommunications network, the method comprising:

receiving, at a blockchain node of a computing device, a message from an infrastructure device;

wherein the message identifies a current condition at the infrastructure device

determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified on a blockchain associated

with a telecommunications network that facilitates communications between the computing device and the infrastructure device; and when the infrastructure device is determined to be verified by the blockchain operation, performing an action to respond to the current condition at the infrastructure device.

33. The method of claim 32, further comprising:  
when the infrastructure device is determined not to be verified by the blockchain operation:  
performing an action to prevent the infrastructure device from transmitting additional messages to other computing devices.

34. The method of claim 32, wherein the blockchain node of the computing device includes a Javascript script that acts as a blockchain agent for the computing device and is configured to operate as a distributed node for the blockchain associated with the telecommunications network.

35. The method of claim 32, further comprising:  
performing, by the blockchain node of the computing device, a transaction to the blockchain that includes a hash of a previous block in the blockchain, a timestamp for the transaction, and transaction data that identifies the action performed to respond to the message from the infrastructure device.

36. The method of claim 32, wherein determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified includes comparing contents of the message received from the infrastructure device with contents of previous messages transmitted from the infrastructure device.

37. The method of claim 32, wherein determining, via a blockchain operation performed by the blockchain node, whether the infrastructure device is verified includes comparing credential information within the message received from the

infrastructure device with credential information maintained for the infrastructure device by the blockchain.

38. The method of claim 32, wherein the infrastructure device is a utility meter that monitors use of a utility at a location, and wherein the computing device is an automated meter reading (AMR) device that automatically collects data from the utility meter.

39. The method of claim 32, wherein the infrastructure device is an emergency alert device for a location, and wherein the computing device is a mobile device configured to alert an emergency responder of an emergency at the location.

40. A system for monitoring operations of devices within a smart city, the system comprising:

a blockchain node, contained by a device within the smart city, that determines, based on information maintained by a blockchain for a telecommunications network associated with the smart city, whether signals sent to the device from other devices within the smart city are trustworthy signals; and

an action module that causes performance of actions associated in response to the signals from the other devices when the blockchain node determines that the signals are trustworthy.

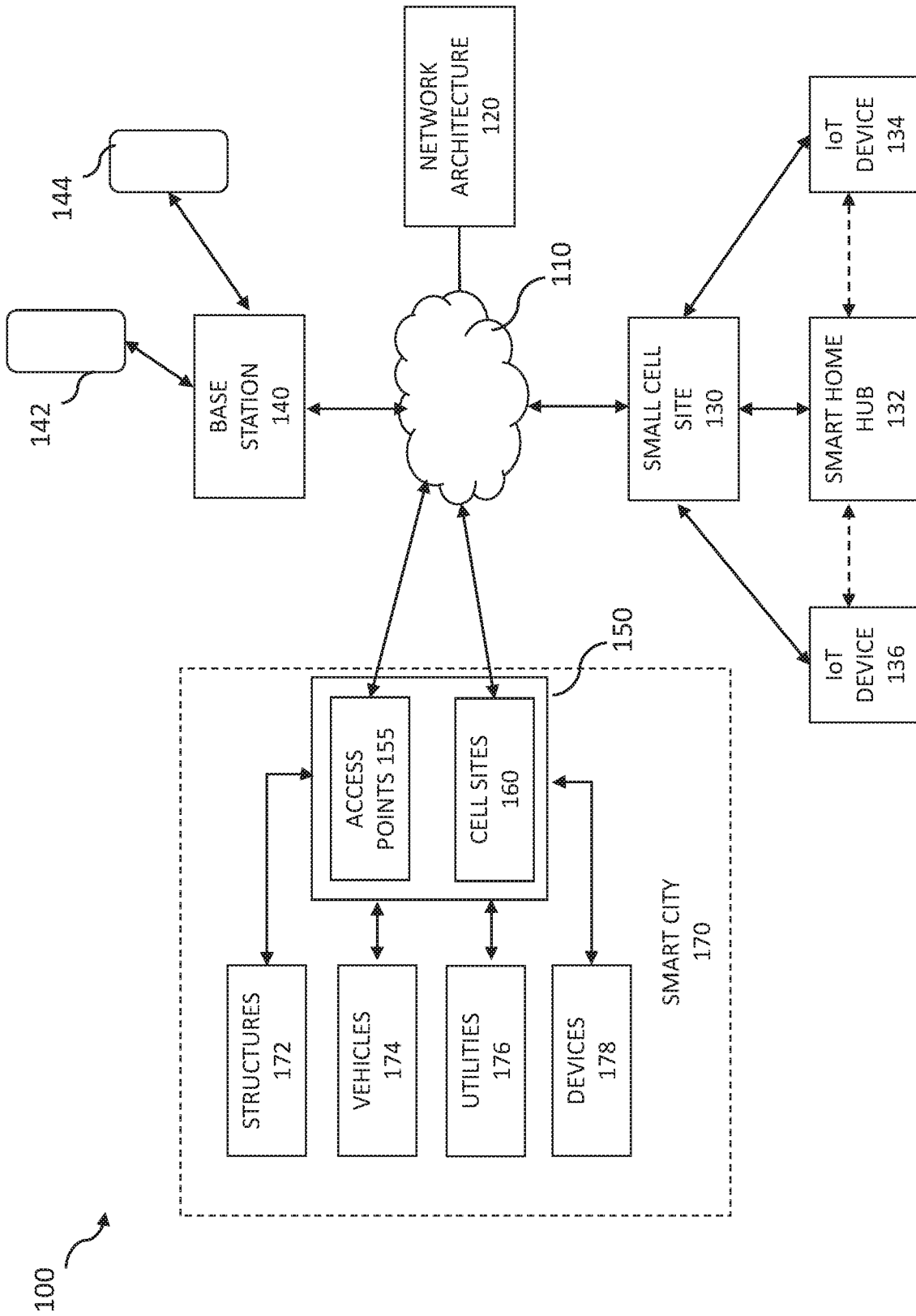


FIG. 1

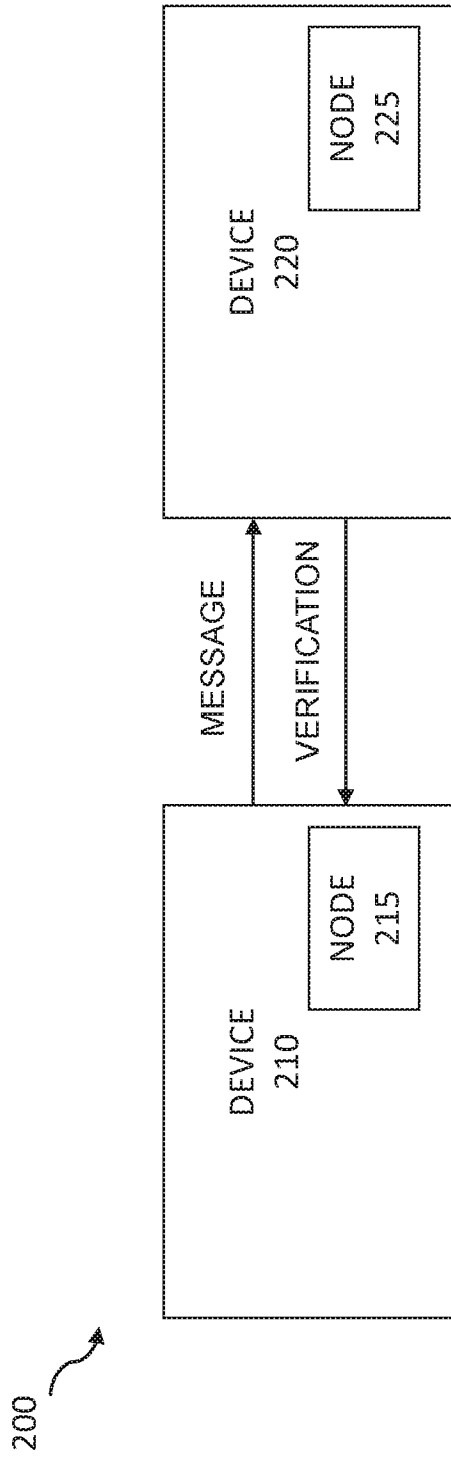


FIG. 2A

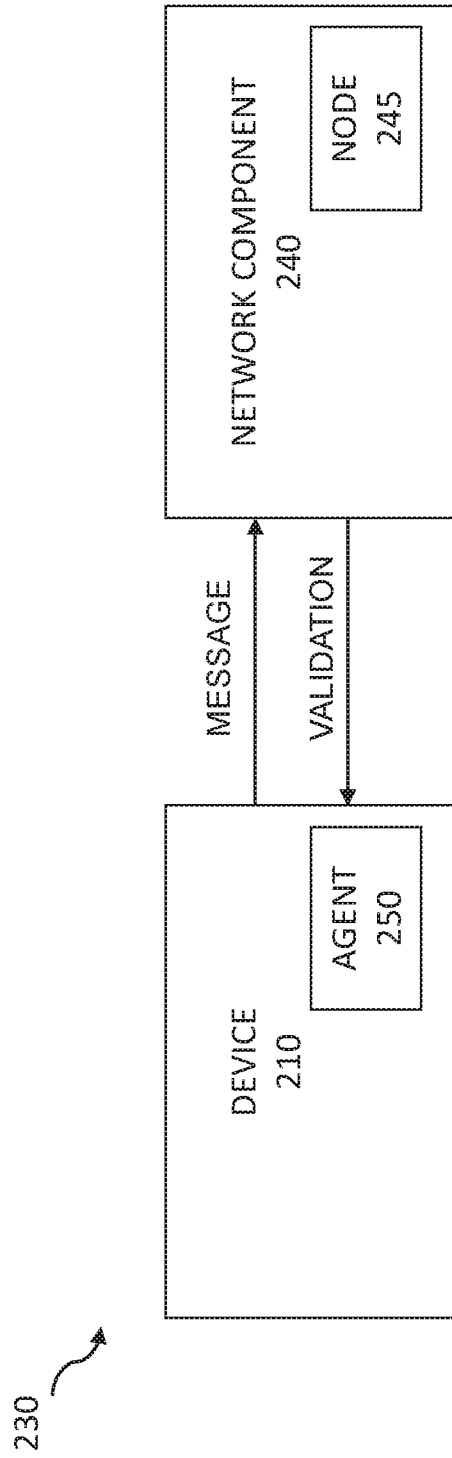


FIG. 2B

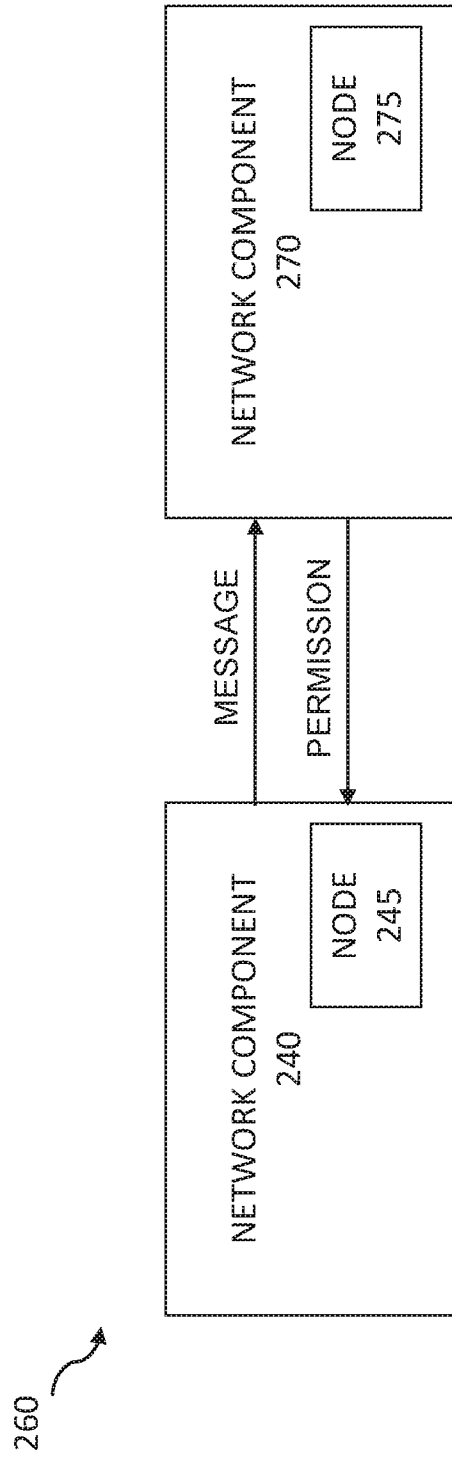


FIG. 2C

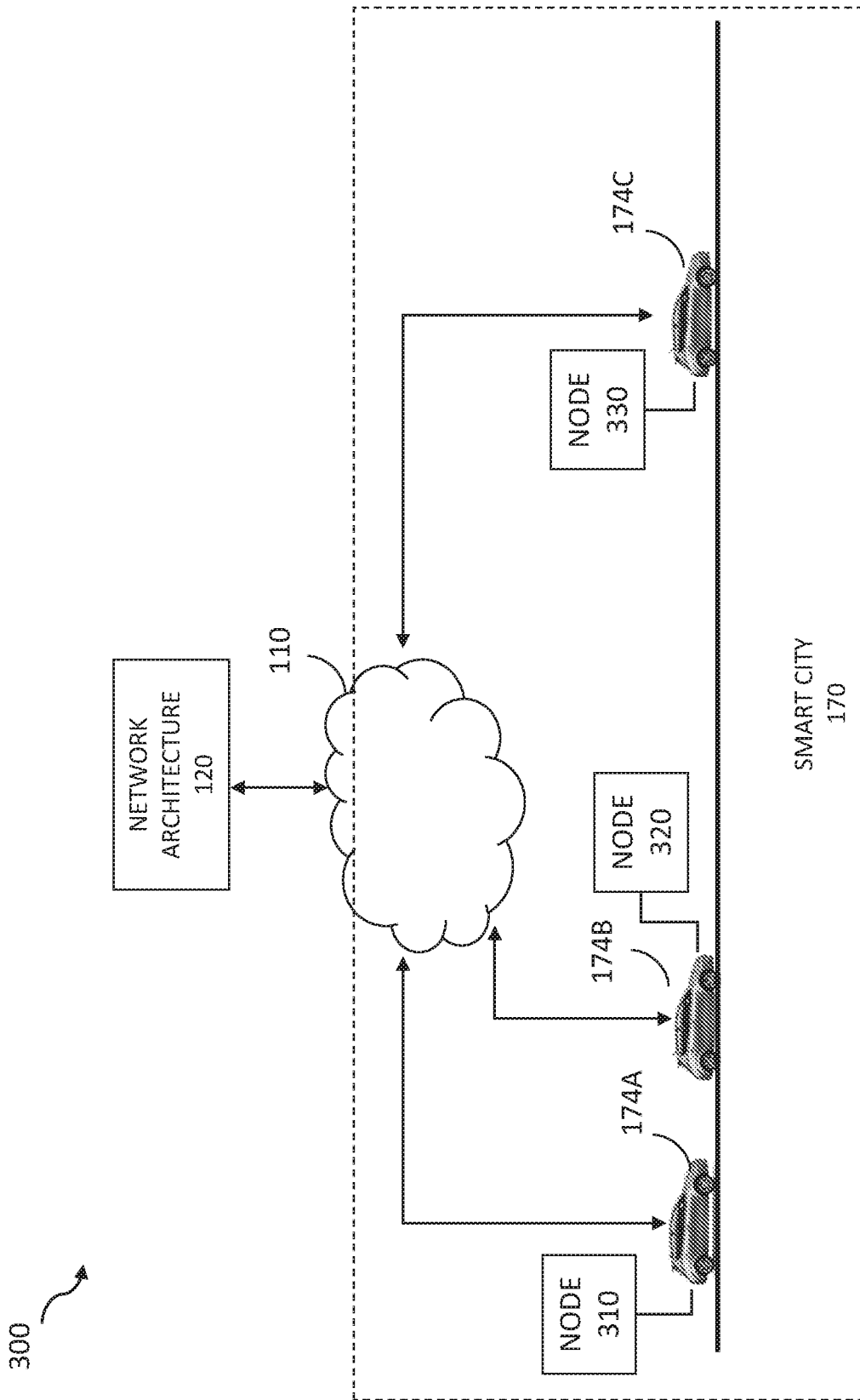


FIG. 3

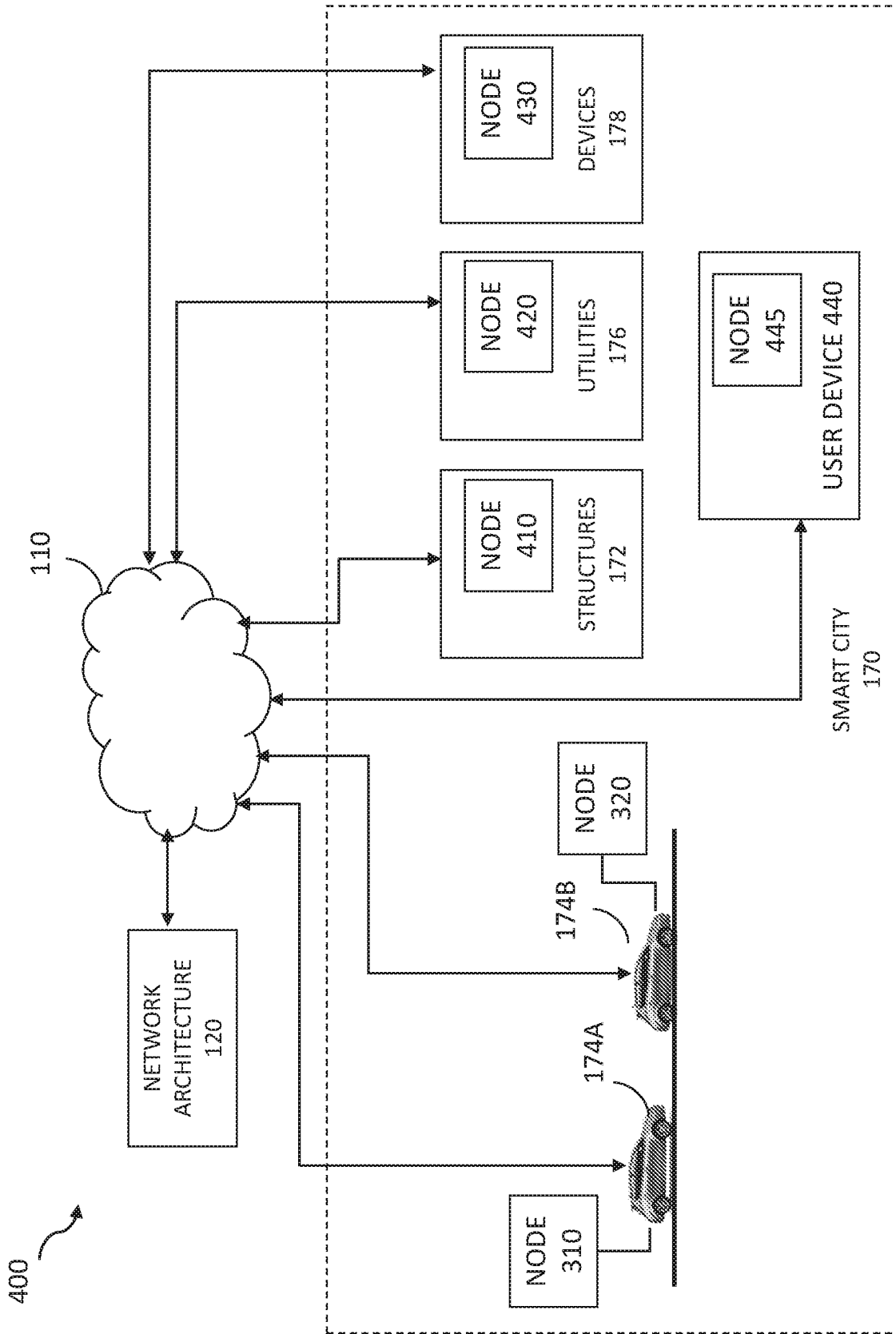


FIG. 4

500 ↗

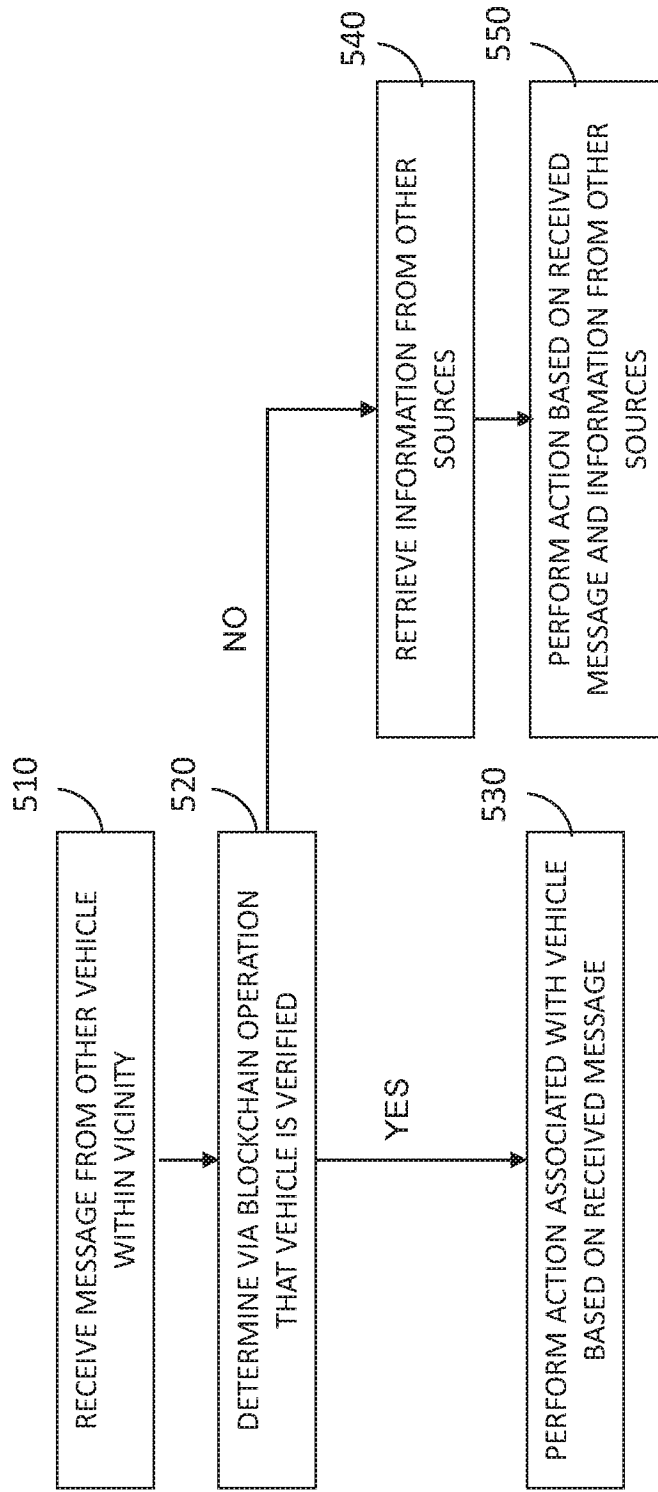


FIG. 5

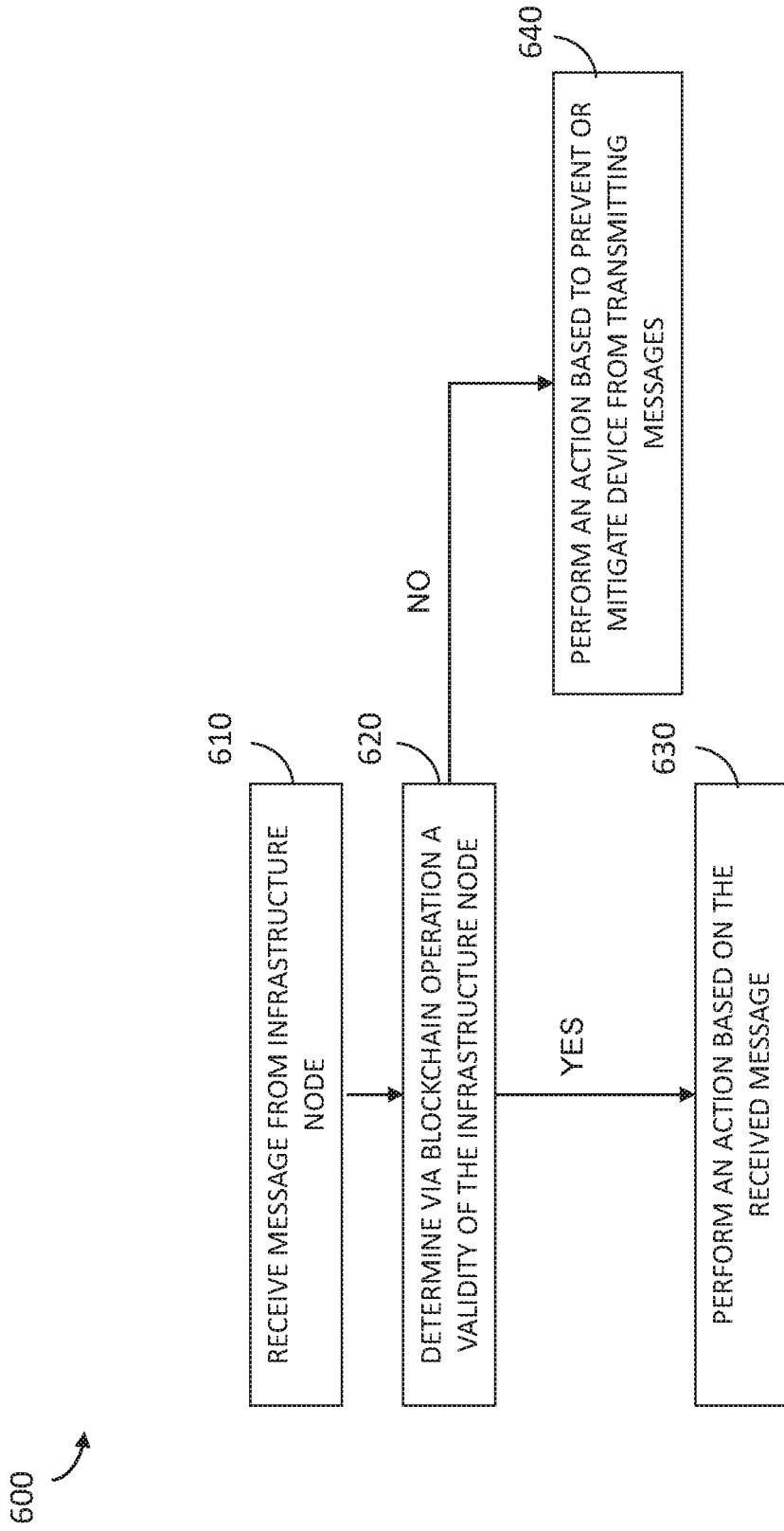


FIG. 6

**A. CLASSIFICATION OF SUBJECT MATTER****H04L 29/08(2006.01)i, H04L 12/58(2006.01)i, H04W 4/46(2018.01)i, H04W 4/12(2009.01)i**

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

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

H04L 29/08; G06Q 10/00; G06Q 20/06; G06Q 30/00; H04L 29/06; H04L 9/08; H04L 9/30; H04L 12/58; H04W 4/46; H04W 4/12

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

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) &amp; keywords: blockchain, vehicle, message, verify, action, trustworthy, infrastructure device, smart city, alert

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018-0091596 A1 (INTEL CORPORATION) 29 March 2018 paragraphs [0042]-[0050]; claims 1, 5; and figures 4-5	1-40
A	CN 107508859 A (BEIJING JIAOTONG UNIVERSITY) 22 December 2017 claims 1-6	1-40
A	WO 2018-126029 A2 (INTEL CORPORATION) 05 July 2018 paragraphs [0065]-[0068]; and figure 3	1-40
A	WO 2018-014123 A1 (ROYAL BANK OF CANADA) 25 January 2018 claims 1-14	1-40
A	US 2016-0283920 A1 (JUSTIN FISHER et al.) 29 September 2016 paragraphs [0015]-[0016]; and figure 1	1-40

 Further documents are listed in the continuation of Box C. See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"D" document cited by the applicant in the international application

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&amp;" document member of the same patent family

Date of the actual completion of the international search

01 May 2020 (01.05.2020)

Date of mailing of the international search report

**01 May 2020 (01.05.2020)**

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KIM, Sung Hee

Telephone No. +82-42-481-3516



## INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

**PCT/US2019/068429**

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2018-0091596 A1	29/03/2018	CN 109644136 A DE 112017004838 T5 JP 2019-531544 A US 10284654 B2 WO 2018-063605 A1	16/04/2019 06/06/2019 31/10/2019 07/05/2019 05/04/2018
CN 107508859 A	22/12/2017	CN 107508859 B	21/02/2020
WO 2018-126029 A2	05/07/2018	CN 110024330 A CN 110024352 A CN 110024422 A CN 110050474 A DE 112017006701 T5 EP 3563521 A1 EP 3563545 A2 EP 3563546 A1 EP 3563596 A1 JP 2020-503784 A KR 10-2019-0100177 A TW 201835784 A US 2019-0349190 A1 US 2019-0349254 A1 US 2019-0349261 A1 US 2019-0349426 A1 US 2019-0349433 A1 US 2019-0349733 A1 WO 2018-125989 A2 WO 2018-125989 A3 WO 2018-126029 A3 WO 2018-126065 A1 WO 2018-126075 A1 WO 2018-126076 A1 WO 2018-126077 A1	16/07/2019 16/07/2019 16/07/2019 23/07/2019 19/09/2019 06/11/2019 06/11/2019 06/11/2019 06/11/2019 30/01/2020 28/08/2019 01/10/2018 14/11/2019 14/11/2019 14/11/2019 14/11/2019 14/11/2019 14/11/2019 05/07/2018 23/08/2018 09/08/2018 05/07/2018 05/07/2018 05/07/2018 05/07/2018
WO 2018-014123 A1	25/01/2018	CA 3031133 A1 EP 3485437 A1 US 2018-0018723 A1	25/01/2018 22/05/2019 18/01/2018
US 2016-0283920 A1	29/09/2016	None	