(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 November 2022 (17.11.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/240361 A1

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04L 9/32* (2006.01)
G06Q 50/28 (2012.01) *G06Q 10/08* (2012.01)

(21) International Application Number:
PCT/SG2022/050309

(22) International Filing Date:
11 May 2022 (11.05.2022)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10202104979S 12 May 2021 (12.05.2021) SG

(71) Applicant: **BUNKERCHAIN PTE LTD** [SG/SG]; 7 Temasek Boulevard #12-02B, Suntec Tower One, Singapore 038987 (SG).

(72) Inventors: **LOH, Yeda Vance**; 28 Fourth Avenue, Singapore 268670 (SG). **LING, Yen Wei**; 10 Sallim Road, Singapore 387640 (SG). **CHEN, Hui**; 17 Hazel Park Terrace #05-03, Singapore 678944 (SG).

(74) Agent: **SPRUSON & FERGUSON (ASIA) PTE LTD**; P.O. Box 1531, Robinson Road Post Office, Singapore 903031 (SG).

(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, IQ, IR, IS, IT, JM, 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, ST, SV, SY, TH, TJ, TM,

WO 2022/240361 A1

(54) Title: METHOD AND SYSTEM FOR FACILITATING A TRANSACTION AT ONE OR MORE NODES OF A BLOCKCHAIN NETWORK

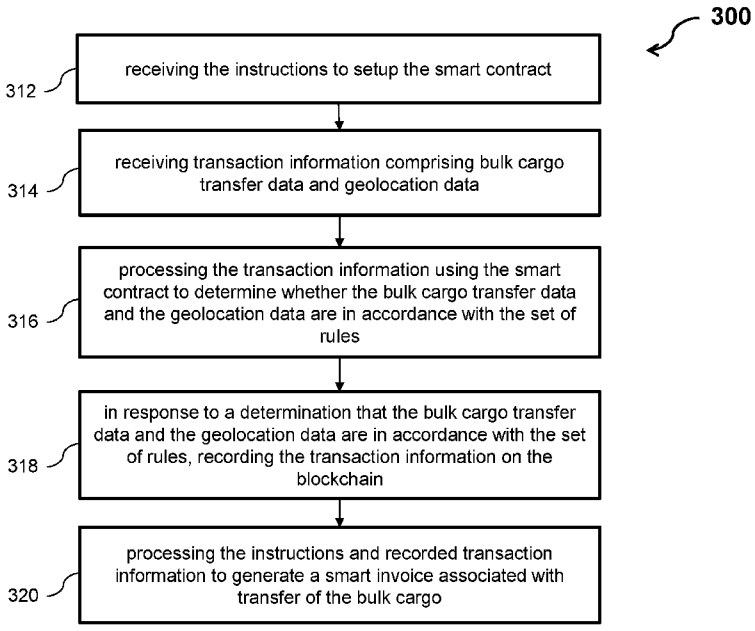

FIG. 3B

(57) Abstract: A method and a system for facilitating a transaction at one or more nodes of a blockchain network are provided. The one or more nodes are configured to manage a blockchain. The method includes receiving instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, receiving transaction information including bulk cargo transfer data and geolocation data, processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, and in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, recording the transaction information on the blockchain.

[Continued on next page]

TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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

— *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*

Method and System for Facilitating a Transaction at One or More Nodes of a Blockchain Network

Technical Field

[0001] The present disclosure generally relates to a method and a system for facilitating a transaction at one or more nodes of a blockchain network.

Background Art

[0002] Commercial documents such as invoice, manifest, bill of lading etc. are typically used between transacting parties (e.g. sellers, buyers, consignees, consignors and carriers) to show that a particular transaction has been carried out and/or to request payment. These commercial documents can be in hard copy or electronic format. Issuance and handling of these commercial documents are traditionally performed manually or semi-automatically using software. However, while software may be an effective and useful tool for generating the documents, the output can only be as accurate as the information entered into it. Further, the issuance and handling processes can be vulnerable to fraudulent activities. For example, an external malicious actor may masquerade as an entity party to the transaction and use the entity's identification and authentication information, e.g. identifier, password etc. without the entity's permission to gain access to the processes, commit fraud or other crimes. A malicious insider may also falsify information used to generate commercial documents for financial gain.

[0003] Maritime trade and transportation can be vulnerable to commercial fraud as a maritime trade transaction typically involves several parties – e.g. buyer, seller, ship-owner, charterer, ship's master or crew, insurer, banker, broker or agent. Maritime fraud can occur when one of these parties succeeds in deceiving another as to some fact or circumstance in connection with maritime activities which enables the party to obtain money or goods unjustly. Maritime fraud can involve misuse, falsification and/or tampering of commercial contracts and documents, such as bills of lading. In some cases, several parties can act in collusion to defraud another. Bulk cargo trade, and in particular liquid bulk cargo trade (e.g. bunkering – the supply of marine fuel for use in ships) can be especially vulnerable, as the cargo is typically transported unpackaged in large quantities.

[0004] A need therefore exists to improve the manner in which transactions are facilitated, to prevent and minimise commercial fraud.

Summary

[0005] In an embodiment, there is provided a method for facilitating a transaction at one or more nodes of a blockchain network. The one or more nodes are configured to manage a blockchain. The method includes receiving instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, receiving transaction information including bulk cargo transfer data and geolocation data, processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, and in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, recording the transaction information on the blockchain.

[0006] In another embodiment, there is provided a system for facilitating a transaction at one or more nodes of a blockchain network. The one or more nodes are configured to manage a blockchain. The system includes a processing device configured to receive instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, receive transaction information comprising bulk cargo transfer data and geolocation data, process the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules and in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, record the transaction information on the blockchain.

[0007] Details of one or more embodiments of the subject matter of this specification are set forth in the accompanying drawings and the description below. Other desirable features and characteristics will become apparent from the subsequent description and the appended claims, taken in conjunction with the accompanying drawings and the background of the disclosure.

Brief Description of Drawings

[0008] Embodiments will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only, and in conjunction with the drawings, in which:

Fig. 1

[0009] Fig. 1 shows a schematic diagram of a blockchain network, in accordance with embodiments of the disclosure.

Fig. 2

[0010] Fig. 2 shows a schematic diagram of a computing device configured to implement a node in a blockchain network, in accordance with embodiments of the disclosure.

Figs. 3A and 3B

[0011] Figs. 3A and 3B show a flowchart illustrating an example of a method for facilitating a transaction at one or more nodes of a blockchain network, in accordance with embodiments of the disclosure.

Fig. 4

[0012] Fig. 4 shows a schematic diagram of a blockchain network, in accordance with embodiments of the disclosure.

Fig. 5

[0013] Fig. 5 shows a flowchart illustrating an exchange of information in a blockchain network, in accordance with embodiments of the disclosure.

Figs. 6A, 6B and 6C

[0014] Figs. 6A, 6B and 6C show schematic diagrams of the blockchain network of Fig. 4, in accordance with embodiments of the disclosure.

Fig. 7

[0015] Fig. 7 shows a schematic diagram illustrating an exchange of information in a blockchain network, in accordance with embodiments of the disclosure.

Fig. 8

[0016] Fig. 8 shows another schematic diagram illustrating an exchange of information in a blockchain network, in accordance with embodiments of the disclosure.

Fig. 9

[0017] Fig. 9 shows another schematic diagram illustrating an exchange of information in a blockchain network, in accordance with embodiments of the disclosure.

Fig. 10

[0018] Fig. 10 shows another schematic diagram illustrating an exchange of information with a blockchain network, in accordance with embodiments of the disclosure.

Fig. 11

[0019] Fig. 11 shows a schematic diagram of an example of a computing device used to implement a node in a blockchain system, in accordance with embodiments of the disclosure.

[0020] Skilled artisans will appreciate that elements in the figures are illustrated for simplicity and clarity and have not necessarily been depicted to scale. For example, the dimensions of some of the elements in the illustrations, block diagrams or flowcharts may be exaggerated in respect to other elements to help to improve understanding of the present embodiments.

Description of Embodiments

[0021] Embodiments of the disclosure seek to provide methods and systems for facilitating a transaction at one or more nodes of a blockchain network, the one or more nodes configured to manage a blockchain. In various embodiments, the methods and devices can receive information associated with the transaction, use the blockchain to record the information, and use smart contracts (i.e. computer protocols implemented in the form of computer code that are incorporated into the blockchain) to facilitate, verify, or enforce the negotiation and/or performance of the transaction. In this manner, the methods and devices can ensure that information is immutable and tamperproof, and can eliminate the need for human interaction in processes associated with the transaction. In embodiments, the transactions can relate to bulk cargo trade, and in particular, liquid bulk cargo trade (e.g. bunkering – the supply of marine fuel for use in ships).

[0022] Embodiments of the disclosure can produce one or more technical effects. In various embodiments, the methods and devices can set up a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, and can process transaction information including bulk cargo transfer data and geolocation data using the smart contract to verify that a bulk cargo has been transferred according to the set of rules. The methods and devices can, in response to a determination that the bulk cargo has been transferred according to the set of rules, record the transaction information on the blockchain and generate a smart invoice associated with transfer of the bulk cargo. Further, in various embodiments, the methods and devices can facilitate the negotiation leading to the transfer of bulk cargo between a seller and a buyer through a trade smart contract. The trade smart contract, once

invoked by both the seller and the buyer, can be used to generate the smart contract for determining whether a bulk cargo has been transferred according to a set of rules. Accordingly, through use of a blockchain network and one or more smart documents (e.g. the smart contract, the smart invoice and the trade smart contract), the methods and devices in accordance with embodiments of the disclosure can store and process information with a data structure that eliminates the need for human interaction and prevent tampering and/or manipulation by malicious actors.

[0023] In embodiments of the disclosure, the smart document (e.g. the smart contract, the smart invoice and the trade smart contract) can include a plurality of subroutines or functions, each of which can be a sequence of program instructions that performs a specific task. The smart documents can be operational code that can be fully or partially executed without human interaction. In various embodiments, a preceding smart document can include instructions to generate a subsequent smart document, based on instructions of the preceding smart document and as a result of a positive determination that conditions defined in the preceding smart document are met. Digitally signed information received from trusted hardware can include, but is not limited to, a copy of the smart document that is signed by a private key of the user indicative of agreement to the terms and/or rules of the smart document, and digitally signed information from data acquisition devices (e.g. sensors and measuring instruments such as mass flow meters etc.). Digitally signed information can also include mass flow data calculated with sounding methods (e.g. sounding or measuring tapes), which can determine the volume of bulk cargo transferred. In embodiments, the subsequent smart document can include a cryptographic hash of one or more preceding smart documents.

[0024] Thus, a smart document in accordance with embodiments of the disclosure can be generated responsive to the fulfilment of conditions defined in a preceding smart document. Information associated with the fulfilment of the defined conditions can be sent by trusted equipment or data acquisition devices (e.g. processing devices, sensors and/or measuring instruments) and can be verified by one or more nodes of the blockchain network. The use of multiple smart documents that can execute operational code based on machine data from trusted hardware or data acquisition devices, and tied to, for example, movement and storage of bulk cargo, can advantageously eliminate human interaction, reduce attack surface and improve security of the blockchain network.

[0025] For example, a first smart contract associated with a bulk cargo transaction can be configured to execute only when machine-derived data trigger and complete the first smart contract. The first smart contract can, in turn, generate a key that can activate the second smart contract which can rely on machine-generated data to trigger and complete the smart

contract. The second smart contract can lead to a subsequent third smart contract, and this can be carried out n-times depending on transaction requirements. In embodiments of the disclosure, a smart contract executing on the blockchain can receive information from trusted device(s) along a supply chain and can verify an action in a transaction without human participation, the smart contract can in turn generate subsequent smart contracts which can lead to eventual generation of smart documents (e.g. transfer receipts, invoice, and other trade documentation).

[0026] Embodiments of the present disclosure will be described, by way of example only, with reference to the drawings. Like reference numerals and characters in the drawings refer to like elements or equivalents.

[0027] Some portions of the description which follows are explicitly or implicitly presented in terms of algorithms and functional or symbolic representations of operations on data within a computer memory. These algorithmic descriptions and functional or symbolic representations are the means used by those skilled in the data processing arts to convey most effectively the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities, such as electrical, magnetic or optical signals capable of being stored, transferred, combined, compared, and otherwise manipulated.

[0028] Unless specifically stated otherwise, and as apparent from the following, it will be appreciated that throughout the present specification, discussions utilizing terms such as “associating”, “calculating”, “comparing”, “determining”, “extracting”, “forwarding”, “generating”, “identifying”, “including”, “inserting”, “modifying”, “receiving”, “recording”, “replacing”, “scanning”, “transmitting”, “updating” or the like, refer to the action and processes of a computer system, or similar electronic device, that manipulates and transforms data represented as physical quantities within the computer system into other data similarly represented as physical quantities within the computer system or other information storage, transmission or display devices.

[0029] The present specification also discloses apparatus for performing the operations of the methods. Such apparatus may be specially constructed for the required purposes or may include a computer or other computing device selectively activated or reconfigured by a computer program stored therein. The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various machines may be used with programs in accordance with the teachings herein. Alternatively, the construction of

more specialized apparatus to perform the required method steps may be appropriate. The structure of a computer will appear from the description below.

[0030] In addition, the present specification also implicitly discloses a computer program, in that it would be apparent to the person skilled in the art that the individual steps of the method described herein may be put into effect by computer code. The computer program is not intended to be limited to any particular programming language and implementation thereof. It will be appreciated that a variety of programming languages and coding thereof may be used to implement the teachings of the disclosure contained herein. Moreover, the computer program is not intended to be limited to any particular control flow. There are many other variants of the computer program, which can use different control flows without departing from the spirit or scope of the disclosure.

[0031] Furthermore, one or more of the steps of the computer program may be performed in parallel rather than sequentially. Such a computer program may be stored on any computer readable medium. The computer readable medium may include storage devices such as magnetic or optical disks, memory chips, or other storage devices suitable for interfacing with a computer. The computer readable medium may also include a hard-wired medium such as exemplified in the Internet system, or wireless medium such as exemplified in the mobile telephone system. The computer program when loaded and executed on a computer effectively results in an apparatus that implements the steps of the preferred method.

[0032] In embodiments of the present disclosure, the term ‘server’ may mean a single computing device or a computer network of a plurality of interconnected computing devices which operate together to perform one or more functions. In other words, the server may be contained within a single hardware unit or be distributed among several or many different hardware units.

[0033] The term “configured to” is used in the specification in connection with systems, apparatus, and computer program components. For a system of one or more computers to be configured to perform particular operations or actions means that the system has installed on it software, firmware, hardware, or a combination of them that in operation cause the system to perform the operations or actions. For one or more computer programs to be configured to perform particular operations or actions means that the one or more programs include instructions that, when executed by data processing apparatus, cause the apparatus to perform the operations or actions. For special-purpose logic circuitry to be configured to perform particular operations or actions means that the circuitry has electronic logic that performs the operations or actions.

[0034] A blockchain is a data structure that can store information, e.g., transactions, in a manner that can prevent tampering and manipulation of the data by malicious actors. The transactions stored in this manner can be immutable and subsequently verified. A blockchain typically includes one or more blocks. Each block is linked to a preceding block before it in the blockchain by including a cryptographic hash of the preceding block. Each block also may include a timestamp, its own cryptographic hash, and one or more transactions. As each block contains a hash of the preceding block, the linked blocks forms a chain, and the iterative process of generating a block with the preceding hash value confirms integrity of preceding blocks. The transactions, which generally have already been verified by the nodes of the blockchain system, may be hashed and encoded into a data structure, such as a Merkle tree. In a Merkle tree, data at leaf nodes of the tree is hashed, and all hashes in each branch of the tree may be concatenated at a root of the branch. This process continues up the tree to the root of the entire tree, which stores a hash that is representative of all data in the tree. A hash purporting to be of a transaction stored in the tree can be quickly verified by determining whether it is consistent with the structure of the tree.

[0035] A blockchain network includes a network of computing nodes that manage, update, and maintain one or more blockchains. The network may be a public blockchain network, a private blockchain network, or a consortium blockchain network (also known as a federated blockchain). Numerous entities can operate in a public blockchain network, and each of the entities can operate one or more nodes in the public blockchain network. Accordingly, the public blockchain network can be considered a public network with respect to the participating entities. Typically, a majority of entities (nodes) must sign every block for the block to be valid and added to the blockchain of the blockchain network. Examples of public blockchain networks include particular peer-to-peer payment networks that leverage a distributed ledger, referred to as blockchain.

[0036] A public blockchain network typically supports public transactions. A public transaction is announced to all nodes in the public blockchain network, and is stored in a global blockchain. A global blockchain is a blockchain replicated across all nodes, with all nodes in consensus with respect to the global blockchain. To achieve consensus (e.g., agreement to the addition of a block to a blockchain), a consensus protocol is implemented in the public blockchain network. Examples of consensus protocols include proof-of-work (POW) (e.g., implemented in the some crypto-currency networks), proof-of-stake (POS), and proof-of-authority (POA).

[0037] A private blockchain network is typically provided for a particular entity that centrally controls read and write permissions. The entity controls nodes that are able to participate in

the blockchain network. Consequently, private blockchain networks are generally referred to as permissioned networks that place restrictions on who is allowed to participate in the network, and on their level of participation (e.g., only in certain transactions). Various types of access control mechanisms can be used (e.g., a central authority can control admission).

[0038] A consortium blockchain network (also known as a federated blockchain network) is private among the participating entities. In a consortium blockchain network, the consensus process is controlled by an authorised set of nodes, with one or more nodes being operated by a respective entity. For example, a consortium of four entities can operate a consortium blockchain network, each of which operates at least one node in the consortium blockchain network. Accordingly, the consortium blockchain network can be considered a private network with respect to the participating entities. In some examples, each entity (node) must sign every block in order for the block to be valid, and added to the blockchain. In some examples, at least a sub-set of entities (nodes) (e.g., at least two entities) must sign every block in order for the block to be valid, and added to the blockchain.

[0039] Fig. 1 shows a schematic diagram of a blockchain network, in accordance with embodiments of the disclosure. The blockchain network 100 can include a plurality of nodes, e.g., nodes 102, 104, 106, 108, configured to manage a blockchain 110. The nodes 102, 104, 106, 108 can form the network 100, such as a peer-to-peer (P2P) network. Each of the nodes 102, 104, 106, 108 can be a computing device, such as a server configured to store a copy of the blockchain 110, or can be software running on the computing device, such as a process or an application. Each of the nodes 102, 104, 106, 108 can have a unique identifier (e.g. a digital signature employing asymmetric cryptography).

[0040] The blockchain 110 can include a list of records in the form of data blocks, such as blocks B1-B4 in Fig. 1. Each of the blocks B1-B4 can include metadata such as a timestamp, a cryptographic hash of a previous block, and data of the present block, which can be transactions or information associated with verification programs such as smart contracts. For example, as illustrated in Fig. 1, block B4 may include metadata, a cryptographic hash of block B3, transaction data of block B3 and a cryptographic hash of the transaction data. A hashing operation may be performed on the previous block to generate the cryptographic hash of the previous block. For example, the hashing operation can convert inputs of various lengths into cryptographic outputs of a fixed length through a hash algorithm, such as SHA-256.

[0041] The nodes 102, 104, 106, 108 can be configured to perform an operation on the blockchain 110. For example, when a node, e.g., the node 102, wants to store new data onto the blockchain 110, the node 102 may generate a new block to be added to the blockchain 120 and broadcast the new block to other nodes, e.g., the nodes 104, 106, 108, in the network

100. Based on legitimacy of the new block, provided through for an endorsement policy, e.g., validity of its signature and transactions, the other nodes may determine to accept the new block, such that the node 102 and the other nodes may add the new block to their respective copies of the blockchain 110. As this process repeats, more and more blocks of data may be added to the blockchain 110.

[0042] Fig. 2 illustrates a schematic diagram of a computing device 200 for implementing a node, e.g., the node 102 shown in Fig. 1, in a blockchain system, according to an embodiment. Referring to Fig. 2, the computing device 200 can include a communication interface 202, a processor 204, and a memory 206. The communication interface 202 can facilitate communications between the computing device 200 and devices implementing other nodes in the network e.g., nodes 102, 104, 106, 108 shown in Fig. 1. In some embodiments, the communication interface 202 is configured to support one or more communication standards, such as an Internet standard or protocol, e.g. Message Queuing Telemetry Transport (MQTT), Internet Protocol Version 4 (IPv4) and/or Internet Protocol Version 6 (IPv6) etc., and an Integrated Services Digital Network (ISDN) standard etc. In embodiments, the communication interface 202 can include one or more of a Local Area Network (LAN) card, a cable modem, a satellite modem, a data bus, a cable, a wireless communication channel, a radio-based communication channel, a cellular communication channel, an Internet Protocol (IP) based communication device, or other communication devices for wired and/or wireless communications. In embodiments, the communication interface 202 can be based on public cloud infrastructure, private cloud infrastructure, hybrid public/private cloud infrastructure.

[0043] The processor 204 can include one or more dedicated processing units, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), or various other types of processors or processing units. The processor 204 is coupled with the memory 206 and is configured to execute instructions stored in the memory 206. The memory 206 may store processor-executable instructions and data, such as a copy of the blockchain 110 in Fig. 1. The memory 206 may include any type of volatile or non-volatile memory devices, or a combination thereof, such as a static random-access memory (SRAM), an electrically erasable programmable read-only memory (EEPROM), an erasable programmable read-only memory (EPROM), a programmable read-only memory (PROM), a read-only memory (ROM), a magnetic memory, a flash memory, or a magnetic or optical disk. When the instructions in the memory 206 are executed by the processor 204, the computing device 200 may perform an operation on the blockchain 110.

[0044] Users of a blockchain network, e.g., the blockchain network 100, can use the blockchain network to record various types of information. For instance, one or more users

can use the blockchain network 100 to record and process information, to facilitate transactions associated with transfer of bulk cargo, e.g. for supply of marine fuel for use in ships (also known as bunkering). In embodiments, the one or more users can agree to record the contractual agreement on the blockchain 110 so that the blockchain network 110 can process and verify whether the one or more users adhere to the rules that they have agreed to. In some embodiments, the blockchain 110 can use one or more smart contracts executing on the blockchain 110 to provide the verification. Smart contracts are computer protocols implemented in the form of computer code that are incorporated into the blockchain 110, to facilitate, verify, or enforce the negotiation and/or performance of contracts. For example, the users of the blockchain 110 can program agreed terms (e.g., rules associated with transfer of bulk cargo, such as quantity, price and terms of delivery) into a smart contract using a programming language, such as C++, Java, Solidity, Python, etc., and use the smart contract to verify whether the bulk cargo has been transferred according to the agreed terms. Also for example, the smart contract can include a plurality of subroutines or functions, each of which can be a sequence of program instructions that performs a specific task. The smart contract can be operational code that can be fully or partially executed without human interaction. In embodiments, a preceding smart contract can include instructions to generate a subsequent smart contract, based on instructions of the preceding smart contract and as a result of fulfilment of conditions defined in the preceding smart contract. Information indicative of the fulfilment of conditions can include digitally signed information (e.g. data sets) received from trusted hardware or data acquisition devices (e.g. sensors, measuring instruments such as mass flow meters, automatic identification system (AIS) transponders etc.). Digitally signed information can also include mass flow data calculated with sounding methods (e.g. sounding or measuring tapes), which can determine the volume of bulk cargo transferred. The automatic identification system (AIS) is an automatic tracking system that uses transceivers on ships and is used by vessel traffic services (VTS). An AIS transponder can provide information such as identification, position, course, and speed of a ship to other ships and coastal authorities.

[0045] In some embodiments, the blockchain 110 can accept a smart contract defining the agreed terms if all users who are parties to the transaction indicate that they agree with the terms expressed in the smart contract. For example, the users can indicate that they agree with the terms expressed in the smart contract by signing the smart contract using their private key. In another example, the users can indicate that they agree with the terms expressed in the smart contract by submitting a copy of the smart contract for recordation on the blockchain 110. In yet another example, the users can indicate that they agree with the terms expressed in the smart contract to an administrator (or a trusted authority), and the administrator can submit the smart contract to the blockchain 110 after having determined all users who are

parties to the transaction have indicate to the administrator that they agree with the terms expressed in the smart contract.

[0046] Figs. 3A and 3B show a flowchart illustrating an example of a method 300 for facilitating a transaction at one or more nodes of a blockchain network, in accordance with embodiments of the disclosure. The method 300 can be implemented with the computing device 200 shown in Fig. 2. Figs. 3A and 3B are described in detail with reference to Figs. 4 and 5, which show a schematic diagram of a blockchain network 400 and a flowchart illustrating an exchange of information in the blockchain network 400 respectively. As shown in Fig. 4, the blockchain network 400 in an embodiment of the disclosure can be managed by four entities comprising Trader A, Trader B, Supplier and Auditor, each operating one or more nodes 402, 404, 406, 408 in the network 400. The blockchain managed by the network 400 can be configured to include three smart contracts, i.e. a trade smart contract 410, a delivery note contract 412 and a smart invoice 414. The trade smart contract 410 and the delivery note contract 412 are also referred to as a request 410 and a smart contract 412 in the following paragraphs. In an embodiment, the node 406 can be configured to receive bulk cargo transfer data 416, 418 (e.g. mass flow data, storage tank data, pump data, temperature gauge data etc.) and geolocation data 420 (e.g. automatic identification system (AIS) data, global positioning system (GPS) data etc.). In an embodiment, the mass flow data can be obtained from one or more mass flow meters. In another embodiment, the mass flow data can be calculated with sounding methods (e.g. with sounding or measuring tapes), which can determine the volume of bulk cargo transferred. Fig. 5 shows the relationship of each smart contract (i.e. the trade smart contract 410, the delivery note contract 412 and the smart invoice 414) in an embodiment of the disclosure. Input parameters for the trade smart contract 410 can include a purchase order 502 from Trader A and a sales order 504 from Trader B. Input parameters for the delivery note contract 412 can include trade information 506 associated with the trade smart contract 410, bulk cargo transfer data 416, 418 (e.g. mass flow data, storage tank data, pump data, temperature gauge data etc.) and geolocation data 420 (e.g. automatic identification system (AIS) data, global positioning system (GPS) data etc.). Input parameters for the smart invoice 414 can include the trade information 506 associated with the trade smart contract 410 and bunker delivery note (BDN) 508 associated with the delivery note contract 412. In embodiments, the input parameters for the delivery note contract 412 can also include a cryptographic hash of the trade smart contract 410, and the input parameters for the smart invoice 414 can include the cryptographic hash of the trade smart contract 410 and/or the cryptographic hash of the delivery note contract 412.

[0047] In embodiments of the disclosure, the method 300 for facilitating a transaction at one or more nodes of the blockchain network 400 can include step 302 of receiving a request 410

to generate instructions to setup a smart contract 412 for determining whether a bulk cargo has been transferred according to a set of rules. The transaction can relate to a bulk cargo transfer (e.g. bunkering – a supply of fuel to a ship, for use by the ship). The method 300 can also include step 304 of processing the request 410 to verify whether the request 410 is in accordance with an endorsement policy. The step 304 of processing the request 410 to verify whether the request 410 is in accordance with the endorsement policy can include receiving an authorisation from each of the one or more nodes associated with the request 410, the authorisation generated in response to a determination that the request is digitally signed by one of the one or more nodes. For example, the traders A and B may be associated with the request 410, the endorsement policy may require that the request 410 to be digitally signed with a private key of originator of request 410. The step of receiving an authorisation from each of the one or more nodes associated with the request 410 can include receiving an authorisation from the nodes 402 and 404, in response to a determination that the request is digitally signed with the private key of the originator. In an embodiment, the authorisation, being an approval of the request 410 (i.e. the trade smart contract 410), can be a copy of the request 410 digitally signed by each of the nodes 402 and 404.

[0048] The method 300 can also include step 306 of recording the request 410 on the blockchain 110 in response to a determination that the request 410 is in accordance with the endorsement policy. Step 308 includes receiving order information comprising the set of rules. In embodiments of the disclosure, the order information can include a purchase order and a sales order. As shown in Fig. 5, the sales order may be transmitted by a node associated with Trader B and the purchase order may be transmitted by a node associated with Trader A. The set of rules may include contractual terms for a bunker fuel trade transaction. For example, the set of rules can identify the seller, the buyer and include product specification (e.g. type of fuel, associated specification such as quality, brand etc.), product quantity, price and terms of delivery (e.g. receiving ship identifier such as ship name, international maritime organisation (IMO) number, location, date and time range for delivery of the bulk cargo etc.). In other words, the set of rules can include bulk cargo transfer requirements and temporal geolocation requirements associated with the bunker fuel trade transaction. The set of rules can also include variability thresholds associated with the bulk cargo transfer requirements and the temporal geolocation requirements. Step 310 can include processing the set of rules and the recorded request 410 to generate the instructions to setup the smart contract 412. In embodiments, the step 310 can include generating a cryptographic hash of the set of rules and the recorded request 410, and including the cryptographic hash in the smart contract 412.

[0049] With reference to Fig. 3B, step 312 can include receiving the instructions to setup the smart contract 412 for determining whether the bulk cargo has been transferred according to

the set of rules. The nodes 402, 404, 406, 408 can process the instructions and deploy the smart contract 412 on the blockchain 110. Step 314 can include receiving transaction information comprising bulk cargo transfer data 416, 418 and geolocation data 420. In an embodiment associated with bunkering (i.e. the supply of fuel to ships), the transaction information can be transmitted by both bunkering tanker (i.e. supply ship) and receiving vessel. In another embodiment, the transaction information can be transmitted by a terminal (e.g. an onshore supplier) and a vessel (e.g. a bunkering tanker receiving and storing the fuel supply). The bulk cargo transfer data 416, 418 can include, for example temporal mass flow data (i.e. mass flow data relating to specific time instances, e.g. at start and end of delivery, and at predetermined intervals at predetermined intervals before, after and or during delivery). In an embodiment, the mass flow data can be obtained from one or more mass flow meters. In another embodiment, the mass flow data can be calculated with sounding methods (e.g. with sounding or measuring tapes), which can determine the volume of bulk cargo transferred. The bulk cargo transfer data 416, 418 can also include data from other sensors and/or meters, and can include, for example, storage tank data, pump data and temperature gauge data etc. relating to specific time instances, e.g. at start and end of delivery, and at predetermined intervals before, after and or during delivery. The geolocation data 420 can include, for example, automatic identification system (AIS) data, global positioning system (GPS) data etc. relating to specific time instances, e.g. at start and end of delivery, and at predetermined intervals before, after and or during delivery.

[0050] Step 316 can include processing the transaction information using the smart contract 412 to determine whether the bulk cargo transfer data 416, 418 and the geolocation data 420 are in accordance with the set of rules. Processing of the transaction information can include, for example, verifying whether the bulk cargo transfer data and the geolocation data fall within the respective variability thresholds associated with the bulk cargo transfer requirements and temporal geolocation requirements. This can include, for example, determining, using the geolocation data 420 whether both the bunkering tanker (i.e. supply ship) and the receiving vessel are in proximity to each other and at the location in time specified in the set of rules. In response to a determination that the bulk cargo transfer data 416, 418 and the geolocation data 420 are in accordance with the set of rules, step 318 can include recording the transaction information including the bulk cargo transfer data 416, 418 and the geolocation data 420 on the blockchain 110. In embodiments, the method 300 can further include step 320 of processing the instructions and recorded transaction information to generate a smart invoice associated with transfer of the bulk cargo. In embodiments, the step 320 can include generating a cryptographic hash of the instructions and recorded transaction, and including

the cryptographic hash in the smart invoice. In some embodiments, the smart invoice can further include the cryptographic hash of the set of rules and the recorded request 410.

[0051] Fig. 6A shows a schematic diagram of the blockchain network 400 of Fig. 4, in accordance with embodiments of the disclosure. In an embodiment, each entity (i.e. Trader A, Trade B, Supplier and Auditor) can generate a respective root certificate 600, 602, 604, 606 (i.e. a public key certificate that identifies a root certificate authority) self-signed with a corresponding private key of the entity. The root certificate is stored in respective peer nodes 402, 404, 406, 408 and order server 608 of the blockchain network 400. Organisation administrators of each entity can use the root certificate of the entity to register one or more users, and the one or more users can access the peer node of the entity. Each transaction will be signed by a trust chain and verified with the organisation public key. Moreover, through the alliance chain method, the transaction process adopts the certificate authority (CA) signature to authenticate the participants. Each entity can have a unique MSP (membership service provider) identifier (MSPID). In an embodiment, the MSPID of an entity can be associated with a domain name system (DNS) address of the entity. The root certificate is issued through the CA centre, and each enterprise can establish its own intermedia certificate for internal users through the root certificate. Blockchain can verify transactions with the CA certificates and ensure that the participants on the blockchain are verified.

[0052] Fig. 6B shows an implementation of a public key infrastructure (PKI) of the blockchain network 400. In an embodiment, an administrator of an entity (e.g. Trader A, currently shown as organisation A “OrgA” in Fig. 6B) can initiate a CA server 610, and create the root certificate 600 and a private key associated with the entity OrgA. The root certificate 600 can be transmitted to a peer node 402 associated with the entity OrgA and order server 608 of the blockchain network 400. In embodiments, when a user (userA) is to be registered with the blockchain network 400, identification and authentication information (e.g. username and password) associated with the user can be transmitted to the CA server 610. The CA server 610 can generate an intermediate certificate 612 and a private key associated with the user. In embodiments, a wallet associated with the user can be generated based on MSPID of the user, the intermediate certificate 612 and the private key associated with the user. The user can access the entity’s peer node 402 and the order server 608 with the wallet. Transactions submitted by the user can be signed using the wallet. The peer node 402 and the order server 608 can verify the signature of the transactions submitted by the user with the root certificate 600 of OrgA. Thus, user certificates (also known as intermediate certificates) within blockchain network 400 can be generated with root certificate of the entity that is associated with the users. A user within the blockchain network 400 can create a wallet with the user certificate and private key associated with the user.

[0053] Fig. 7 shows a schematic diagram illustrating an exchange of information in the blockchain network 400, in accordance with embodiments of the disclosure. With reference to Fig. 7, audit node 408 can be configured to scan for begin and end transaction data in step 1 (i.e. subscribe the begin and end transaction data), so that when there is begin or end transaction invoke, the audit node will listen the event and get the begin or end transaction data. The trade smart contract can be deployed in blockchain with endorsement policy, and both traders can approve the trade smart contract. In step 2, Trader A can create a purchase order, invoke the trade smart contract and push purchase order to the blockchain, which can be recorded on the blockchain. In step 3, the blockchain 110 can then emitted contract event, system can listen the contract event and create sales orders. In step 4, Trader B can invoke trade smart contract and push sales order to blockchain to store. The process of trade smart contract is completed. In step 5, delivery note contract can auto-create according to the trade smart contract. In step 6, delivery information such as delivery quantity, IOT & MFM data and vessel and bunker tanker AIS location, can be auto pushed to the blockchain. AIS location data captured by GPS and can be logged when the transaction begin or end. In step 7, when delivery note contract completed, blockchain will auto complete invoice smart contract.

[0054] Fig. 8 shows a schematic diagram illustrating an exchange of information in the blockchain network 400, in accordance with embodiments of the disclosure. The trade smart contract 410 can be deployed on the blockchain 110 with endorsement policy, with the smart contract being effective (i.e. initiated) once the endorsement policy is verified. A buyer (e.g. Trader A) can invoke the trade smart contract 410, and push the purchase order 502. The blockchain 110 can store the purchase order 502 in the blockchain and invoke the contract event. A seller (e.g. Trader B) can push a sale order 504. The blockchain network 400 can verify the seller. If the verification is successful, the trade smart contract 410 can be completed and can in turn generate a delivery note contract 412. In other words, Traders A and B can initiate a transaction by invoking the trade smart contract 410. The trade smart contract 410 can include key fields required in a complete bunker fuel trade transaction. The key fields include, but is not limited to, a buyer, a seller, product information (e.g. specification, quality, name etc.), quantity, price and terms of delivery (e.g. receiving ship identifier such as ship name, international maritime organisation (IMO) number, location, date and time range for delivery of the bulk cargo etc.). A successful submission occurs when both purchase and sale orders are submitted (regardless of sequence). The purchase and sale orders 502, 504 are stored on the smart contract which in turn can generate a new block that can be used to activate the delivery note contract 412. The new block can be identified as “smart contract 1 unique identifier”.

[0055] Fig. 9 shows a schematic diagram illustrating an exchange of information in the blockchain network 400, in accordance with embodiments of the disclosure. The audit node 408 can be configured to scan for begin and end transaction data and can, in embodiments, and monitor the entire delivery process. Once a bunker tanker starts to deliver fuel to a receiving vessel, the client application can obtain the location via GPS or AIS transponder, and store the bulk cargo transfer data and the geolocation data (package IOT data, MFM datalog, AIS location) in the blockchain. Once the deliver completed, the receiving vessel can transmit the bulk cargo transfer data and the geolocation data. The blockchain will then generate a smart invoice. In embodiments, the smart invoice can generate a further smart contract associated with payment and settlement. In embodiments, payment and settlement can occur either via fiat method (via link up with banks) or via utility token payment via crypt-currency settlement.

[0056] In embodiments, the bulk cargo transfer data can include physical transfer start data and physical transfer end data. The physical transfer start data (which can be recorded as physical transfer start block on the blockchain) can include transaction start time, mass flow data from mass flow meter installed on ship/terminal (e.g. time at start of fuel transfer, mass in air, begin forward inversion in air, totaliser loading and delivery at operation start etc.), AIS data such as longitude and latitude from the bunker tanker and other equipment data (e.g. storage tank data, pump data, temperature gauge data etc.). The physical transfer end data (which can be recorded as physical transfer end block on the blockchain) can include transaction end time, mass flow data from mass flow meter installed on ship/terminal (e.g. time at end of fuel transfer, end forward inversion in air, totaliser loading and delivery at operation end etc.), AIS data such as longitude and latitude from the bunker tanker and other equipment data (e.g. storage tank data, pump data, temperature gauge data etc.). In some embodiments, the mass flow data can be calculated with sounding methods (e.g. with sounding or measuring tapes), which can determine the volume of bulk cargo transferred.

[0057] In an embodiment, a complete delivery smart contract can include physical transfer start data, physical transfer end data, smart contract 1 unique identifier, geolocation data from both the ships proving that the bunker vessel and receiving vessel match the geolocation requirements in the trade smart contract and delivery location, the date and time specified in the trade smart contract (the date and time when the transaction is carried out must be within the date range specified in trade smart contract) and geolocation data from both the ships proving that the bunker vessel and receiving vessel are side by side during the physical transfer start time and physical transfer end time.

[0058] Upon completion of the 3 required blocks based on pre-set parameters (i.e. physical transfer start block, physical transfer end block and smart contract 1 unique identifier, the delivery note smart contract can generate a new block called “smart contract 2 unique identifier” that can be used to generate smart invoice. Information from the complete delivery note contract can be used to generate a bunker delivery note 508. In embodiments, the smart invoice can include “smart contract 1 unique identifier”, “smart contract 2 unique identifier”, information from the bunker delivery note 508 and information from the trade smart contract 410 and delivery note contract 412 which can be used to generate a final price for the transaction. In embodiments, the smart invoice can generate a further smart contract associated with payment and settlement. In embodiments, payment and settlement can occur either via fiat method (via link up with banks) or via utility token payment via crypt-currency settlement. In embodiments, a new block can be generated based on the smart invoice, and can be used to activate the further smart contract. The new block can be identified as “smart invoice unique identifier”.

[0059] Fig. 10 shows a schematic diagram illustrating an exchange of information with a blockchain network, in accordance with embodiments of the disclosure. Digitally signed information (e.g. data sets) received from trusted hardware (e.g. sensors, measuring instruments such as mass flow meters etc.) can use Message Queuing Telemetry Transport (MQTT) (a lightweight, publish-subscribe network protocol) for exchange of information with a blockchain network. For example, a MQTT broker can deploy in the cloud. The vessel can push the digitally signed information (e.g. data sets) received from trusted hardware (e.g. sensors, measuring instruments such as mass flow meters etc.) in real time. The physical supplier can subscribe to the information as a MQTT client. When the transaction begins, the physical MQTT client will get the digitally signed information (e.g. data sets) received from trusted hardware, retrieve the vessel’s AIS location, package the data and transmit to blockchain. The data package can contain the bulk cargo transfer data and geolocation data. The transfer of the bulk cargo transfer data and geolocation data for end transaction will be the same.

[0060] Embodiments of the disclosure provide a method and system that can automate set up multiple smart contracts in the bunker supply chain once a trade is entered. Embodiments of the disclosure can advantageously provide a distributed system. Particularly, different task such as trade, bunker loading, and bunker distributing are executed on the same network through blockchain network. Each participants visits own independent node on the blockchain to ensure that the trade data in the trade chain is transparent and auditable, and trade records are tamper-proof when their ERP is independent.

[0061] Moreover, through the alliance chain method, the transaction process adopts the certificate authority (CA) signature to authenticate the participants. Each enterprise has a unique MSP (membership service provider). The root certificate is issued through the CA centre, and each enterprise can establish its own intermedia certificate for internal users through the root certificate. Blockchain can verify transactions with the CA certificates and ensure that the participants on the blockchain are verified.

[0062] Use of multiple smart contracts (or a multi-layer smart contract), through the trade smart contract, delivery note contract, smart invoice and settlement contract can allow the entire process of bulk cargo trade management to be established on the blockchain. As the entire transaction process is completed on the blockchain, embodiments of the invention can provide a controllable process and a tamper-proof operation record.

[0063] Through automatic acquisition of bulk transfer data (e.g. mass flow meter data log) automatic acquisition of vessel and bunker tanker geolocation data, smart contracts can be automatically executed without human intervention, as the initiation and completion of smart contract transactions rely on machine-generated data. Terms of engagement can be recorded in the smart contract which automatically perform verification of the machine-generated data. For example, the quantity and deviation threshold of bunker loading and bunker distributing in the trade order are set in the delivery note contract. An alarm can be sounded if the threshold is exceeded. The distance threshold between the receiving vessel and bunker tanker is set in the Deliver note contract. If the threshold exceeds, the deliver note contract cannot be created. In embodiments, the blockchain network can be configured to compare field details from the trade smart contract to respective field details in the delivery note contract. Field details can include, but is not limited to bunker tanker information (e.g. IMO number of the bunker tanker), vessel information (e.g. IMO number of the vessel), quantity of bulk cargo delivered, transaction start time and date, as well as transaction end time and date. In embodiments, a smart invoice is generated if the field details from the trade smart contract correspond with the respective field details in the delivery note contract (e.g. the bunker tanker and vessel IMO numbers in delivery smart contract are the same as the bunker tanker and vessel IMO numbers in the trade smart contract, and the start and end time of the transaction fall within the time period defined in the trade smart contract).

[0064] Embodiments of the disclosure can advantageously ensure that all smart documents generated from the invention is unique to the transaction as it can include machine generated data from the physical transfer/storage of the bulk cargo rather than from traditional human generated forms (hard copy or electronic). For example, a purchase and sale is automated and linked to a master contract for supply of fuel. The information on the fuel required will be

automatically calculated and sent to the invention based on the forward-looking journey to the next port. Information is then sent to the supplier of the fuel for the supply which is automatically included into the first smart contract which will be executed only when a machine generated data verifies that the conditions have been met before leading to the second smart contract and so on. All of which relies on independently verified data. Thus, the process can be fully automated with one smart contract completed before the next one begins and only when the completion of the first smart contract is done will the next contract begins.

[0065] Through a trade specific infrastructure design, implemented via a blockchain network, embodiments of the disclosure can advantageously provide interoperability between different systems of participants in a distributed ledger environment. More advantageously, multiple smart contracts “layering” can ensure that a preceding (e.g. parent) smart contract will be completed by only if predetermined conditions and/or actions or specific information (e.g. bulk cargo transfer data, geolocation data) are received and validated before a subsequent (child) contract can be executed. This can go on n times. These documents generated are stored on the blockchain and can provide an an audit trail of the entire life cycle of the documents.

[0066] Embodiments of the disclosure can advantageously reduce the possibility of fraud due to human interaction in activities (e.g. transportation, storage, purchase, sale and consumption) carried out in logistics associated with bulk commodities (e.g. bulk cargo, liquid bulk communities). Embodiments of the disclosure can also advantageously reduce internal theft or misuse of technology. Entities implementing embodiments of the disclosure can include

[0067] Fig. 11 depicts an example of a computing device 1100, hereinafter interchangeably referred to as a computer system 1100, where one or more such computing devices 1100 may be used to execute the method 300 of Figs. 3A and 3B. One or more components of the exemplary computing device 1100 can also be used to implement the systems 100, 400 as well as the nodes 402, 404, 406 and 408 of blockchain network 400. The following description of the computing device 1100 is provided by way of example only and is not intended to be limiting.

[0068] As shown in Fig. 11, the example computing device 1100 includes a processor 1107 for executing software routines. Although a single processor is shown for the sake of clarity, the computing device 1100 may also include a multi-processor system. The processor 1107 is connected to a communication infrastructure 1106 for communication with other components of the computing device 1100. The communication infrastructure 1106 may include, for example, a communications bus, cross-bar, or network.

[0069] The computing device 1100 further includes a main memory 1108, such as a random access memory (RAM), and a secondary memory 1110. The secondary memory 1110 may include, for example, a storage drive 1112, which may be a hard disk drive, a solid state drive or a hybrid drive and/or a removable storage drive 1117, which may include a magnetic tape drive, an optical disk drive, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), or the like. The removable storage drive 1117 reads from and/or writes to a removable storage medium 1177 in a well-known manner. The removable storage medium 1177 may include magnetic tape, optical disk, non-volatile memory storage medium, or the like, which is read by and written to by removable storage drive 1117. As will be appreciated by persons skilled in the relevant art(s), the removable storage medium 1177 includes a computer readable storage medium having stored therein computer executable program code instructions and/or data.

[0070] In an alternative implementation, the secondary memory 1110 may additionally or alternatively include other similar means for allowing computer programs or other instructions to be loaded into the computing device 1100. Such means can include, for example, a removable storage unit 1122 and an interface 1150. Examples of a removable storage unit 1122 and interface 1150 include a program cartridge and cartridge interface (such as that found in video game console devices), a removable memory chip (such as an EPROM or PROM) and associated socket, a removable solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), and other removable storage units 1122 and interfaces 1150 which allow software and data to be transferred from the removable storage unit 1122 to the computer system 1100.

[0071] The computing device 1100 also includes at least one communication interface 1127. The communication interface 1127 allows software and data to be transferred between computing device 1100 and external devices via a communication path 1126. In embodiments of the disclosure, the communication interface 1127 permits data to be transferred between the computing device 1100 and a data communication network, such as a public data or private data communication network. The communication interface 1127 may be used to exchange data between different computing devices 1100 which such computing devices 1100 form part an interconnected computer network. Examples of a communication interface 1127 can include a modem, a network interface (such as an Ethernet card), a communication port (such as a serial, parallel, printer, GPIB, IEEE 1394, RJ45, USB), an antenna with associated circuitry and the like. The communication interface 1127 may be wired or may be wireless. Software and data transferred via the communication interface 1127 are in the form of signals which can be electronic, electromagnetic, optical or other signals capable of being

received by communication interface 1127. These signals are provided to the communication interface via the communication path 1126.

[0072] As shown in Fig. 11, the computing device 1100 further includes a display interface 1102 which performs operations for rendering images to an associated display 1155 and an audio interface 1152 for performing operations for playing audio content via associated speaker(s) 1157.

[0073] As used herein, the term "computer program product" may refer, in part, to removable storage medium 1177, removable storage unit 1122, a hard disk installed in storage drive 1112, or a carrier wave carrying software over communication path 1126 (wireless link or cable) to communication interface 1127. Computer readable storage media refers to any non-transitory, non-volatile tangible storage medium that provides recorded instructions and/or data to the computing device 1100 for execution and/or processing. Examples of such storage media include magnetic tape, CD-ROM, DVD, Blu-ray™ Disc, a hard disk drive, a ROM or integrated circuit, a solid state storage drive (such as a USB flash drive, a flash memory device, a solid state drive or a memory card), a hybrid drive, a magneto-optical disk, or a computer readable card such as a PCMCIA card and the like, whether or not such devices are internal or external of the computing device 1100. Examples of transitory or non-tangible computer readable transmission media that may also participate in the provision of software, application programs, instructions and/or data to the computing device 1100 include radio or infra-red transmission channels as well as a network connection to another computer or networked device, and the Internet or Intranets including e-mail transmissions and information recorded on Websites and the like.

[0074] The computer programs (also called computer program code) are stored in main memory 1108 and/or secondary memory 1110. Computer programs can also be received via the communication interface 1127. Such computer programs, when executed, enable the computing device 1100 to perform one or more features of embodiments discussed herein. In embodiments, the computer programs, when executed, enable the processor 1107 to perform features of the above-described embodiments. Accordingly, such computer programs represent controllers of the computer system 1100.

[0075] Software may be stored in a computer program product and loaded into the computing device 1100 using the removable storage drive 1117, the storage drive 1112, or the interface 1150. The computer program product may be a non-transitory computer readable medium. Alternatively, the computer program product may be downloaded to the computer system 1100 over the communication path 1126. The software, when executed by the processor 1107,

causes the computing device 1100 to perform the necessary operations to execute the method 300 of Figs. 3A and 3B.

[0076] It is to be understood that the embodiment of Fig. 11 is presented merely by way of example to explain the operation and structure of the system 1100. Therefore, in some embodiments one or more features of the computing device 1100 may be omitted. Also, in some embodiments, one or more features of the computing device 1100 may be combined together. Additionally, in some embodiments, one or more features of the computing device 1100 may be split into one or more component parts.

[0077] It will be appreciated that the elements illustrated in Fig. 11 function to provide means for performing the various functions and operations of the system as described in the above embodiments.

[0078] When the computing device 1100 is configured to realise the system 400 to for facilitate a transaction at one or more nodes of a blockchain network, the one or more nodes configured to manage a blockchain, the system 400 will have a non-transitory computer readable medium 1112 having stored thereon an application which when executed causes the system 400 to perform steps comprising: receiving instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, receiving transaction information comprising bulk cargo transfer data and geolocation data, processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules and in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, recording the transaction information on the blockchain.

[0079] In embodiments, the computing device 1100 can include at least one processor 1107 and a non-transitory computer-readable storage medium 1112 coupled to the at least one processor 1107 and storing programming instructions for execution by the at least one processor 1107. The programming instructions can instruct the at least one processor 1107 to receive instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules, receive transaction information comprising bulk cargo transfer data and geolocation data, process the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules and in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, record the transaction information on the blockchain.

[0080] In some embodiments, the programming instructions can instruct the at least one processor 1107 to process the instructions and recorded transaction information to generate a smart invoice associated with transfer of the bulk cargo.

[0081] In some embodiments, the programming instructions can instruct the at least one processor 1107 to record a cryptographic hash of the smart invoice on the blockchain.

[0082] In some embodiments, the programming instructions can instruct the at least one processor 1107 to receive a request to generate the instructions to setup the smart contract, process the request to verify whether the request is in accordance with an endorsement policy, in response to a determination that the request is in accordance with the endorsement policy, record the request on the blockchain, receive order information comprising the set of rules and process the set of rules and recorded request to generate the instructions to setup the smart contract.

[0083] In some embodiments, the programming instructions can instruct the at least one processor 1107 to record a cryptographic hash of the instructions to setup the smart contract on the blockchain.

[0084] In some embodiments, the programming instructions can instruct the at least one processor 1107 to receive an authorisation from each of the one or more nodes associated with the request, the authorisation generated in response to a determination that the request is digitally signed by one of the one or more nodes.

[0085] In some embodiments, the bulk cargo transfer data comprises temporal mass flow meter data and wherein the geolocation data comprises temporal automatic identification system (AIS) data. In some embodiments, the set of rules comprises bulk cargo transfer requirements, temporal geolocation requirements and respective variability thresholds associated with the bulk cargo transfer requirements and temporal geolocation requirements. In some embodiments, the programming instructions can instruct the at least one processor 1107 to verify whether the bulk cargo transfer data and the geolocation data fall within the respective variability thresholds associated with the bulk cargo transfer requirements and temporal geolocation requirements.

[0086] It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present disclosure as shown in the specific embodiments without departing from the spirit or scope of the disclosure as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

Claims

1. A method for facilitating a transaction at one or more nodes of a blockchain network, the one or more nodes configured to manage a blockchain, the method comprising:

receiving instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules;

receiving transaction information comprising bulk cargo transfer data and geolocation data;

processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules; and

in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, recording the transaction information on the blockchain;

wherein the bulk cargo transfer data comprises temporal mass flow data;

wherein the set of rules comprises bulk cargo transfer requirements and variability thresholds associated with the bulk cargo transfer requirements; and

wherein processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules comprises verifying whether the bulk cargo transfer data fall within the variability thresholds associated with the bulk cargo transfer requirements.

2. The method as claimed in claim 1, further comprising processing the instructions and recorded transaction information to generate a smart invoice associated with transfer of the bulk cargo.

3. The method as claimed in claim 2, further comprising recording a cryptographic hash of the smart invoice on the blockchain.

4. The method as claimed in any one of claims 1 to 3, further comprising:

receiving a request to generate the instructions to setup the smart contract;

processing the request to verify whether the request is in accordance with an endorsement policy;

in response to a determination that the request is in accordance with the endorsement policy, recording the request on the blockchain;

receiving order information comprising the set of rules; and

processing the set of rules and recorded request to generate the instructions to setup the smart contract.

5. The method as claimed in claim 4, further comprising recording a cryptographic hash of the instructions to setup the smart contract on the blockchain.

6. The method as claimed in claim 4 or 5, wherein processing the request to verify whether the request is in accordance with the endorsement policy comprises receiving an authorisation from each of the one or more nodes associated with the request, the authorisation generated in response to a determination that the request is digitally signed by one of the one or more nodes.

7. The method as claimed in any one of claims 1 to 6, wherein the geolocation data comprises temporal automatic identification system (AIS) data.

8. The method as claimed in claim 7, wherein the set of rules comprises temporal geolocation requirements and variability thresholds associated with the temporal geolocation requirements.

9. The method as claimed in claim 8, wherein processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules comprises verifying whether the geolocation data fall within the variability thresholds associated with the temporal geolocation requirements.

10. A system for facilitating a transaction at one or more nodes of a blockchain network, the one or more nodes configured to manage a blockchain, the system comprising:

a processing device configured to:

receive instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules;

receive transaction information comprising bulk cargo transfer data and geolocation data;

process the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules; and

in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, record the transaction information on the blockchain

wherein the bulk cargo transfer data comprises temporal mass flow data;

wherein the set of rules comprises bulk cargo transfer requirements and variability thresholds associated with the bulk cargo transfer requirements; and

wherein processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules comprises verifying whether the bulk cargo transfer data fall within the variability thresholds associated with the bulk cargo transfer requirements.

11. The system as claimed in claim 10, wherein the processing device is further configured to process the instructions and recorded transaction information to generate a smart invoice associated with transfer of the bulk cargo.

12. The system as claimed in claim 11, wherein the processing device is further configured to record a cryptographic hash of the smart invoice on the blockchain.

13. The system as claimed in any one of claims 10 to 12, wherein the processing device is further configured to:

receive a request to generate the instructions to setup the smart contract;

process the request to verify whether the request is in accordance with an endorsement policy;

in response to a determination that the request is in accordance with the endorsement policy, record the request on the blockchain;

receive order information comprising the set of rules; and

process the set of rules and recorded request to generate the instructions to setup the smart contract.

14. The system as claimed in claim 13, wherein the processing device is further configured to record a cryptographic hash of the instructions to setup the smart contract on the blockchain.

15. The system as claimed in claim 14, wherein the processing device is configured to receive an authorisation from each of the one or more nodes associated with the

request, the authorisation generated in response to a determination that the request is digitally signed by one of the one or more nodes.

16. The system as claimed in any one of claims 10 to 15, wherein the geolocation data comprises temporal automatic identification system (AIS) data.

17. The system as claimed in claim 16, wherein the set of rules comprises temporal geolocation requirements and variability thresholds associated with the temporal geolocation requirements.

18. The system as claimed in claim 17, wherein the processing device is configured to verify whether the geolocation data fall within the variability thresholds associated with the temporal geolocation requirements.

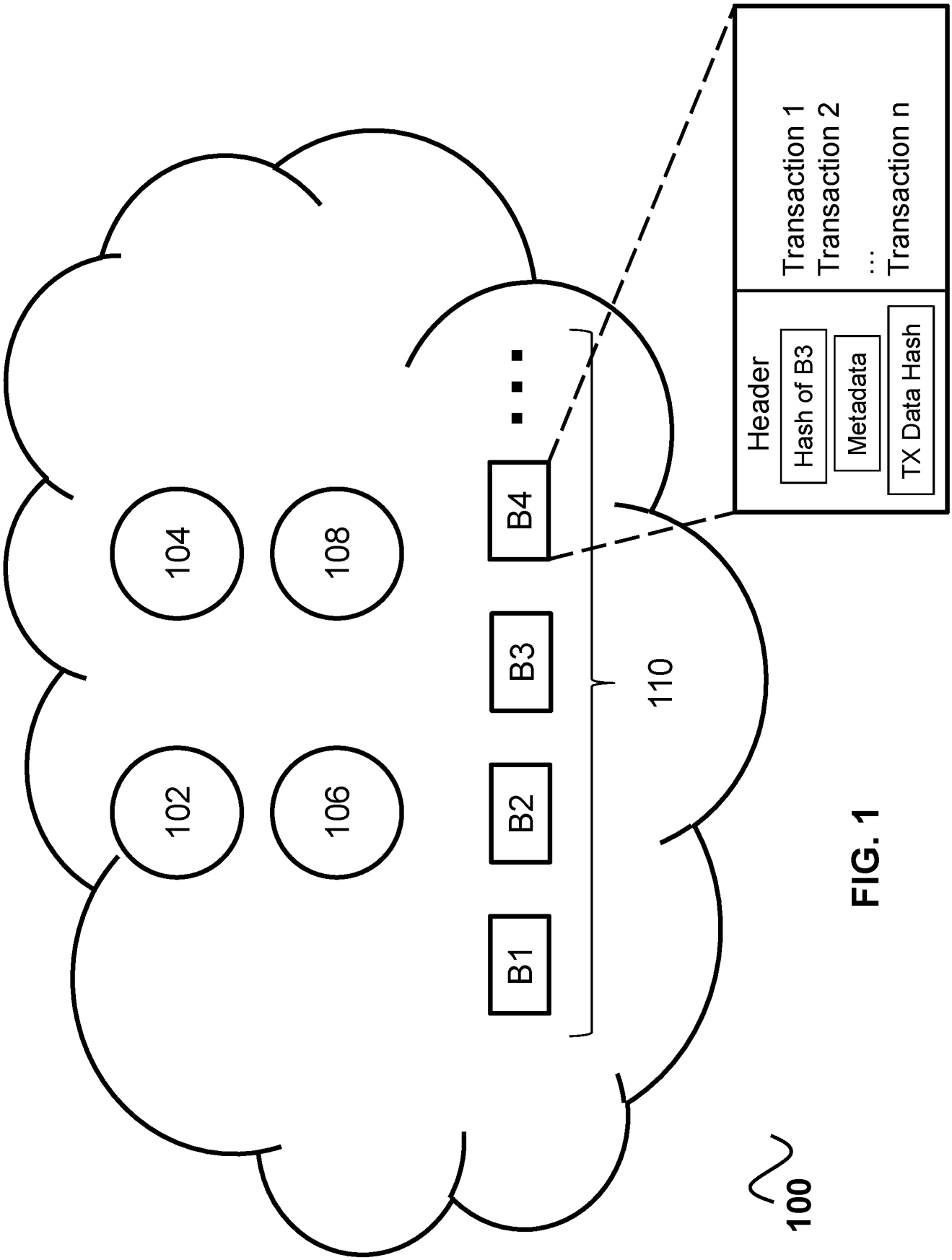
100
102
104
106
108
110
B1
B2
B3
B4
Header
Hash of B3
Metadata
TX Data Hash
Transaction 1
Transaction 2
...
Transaction n

FIG. 1

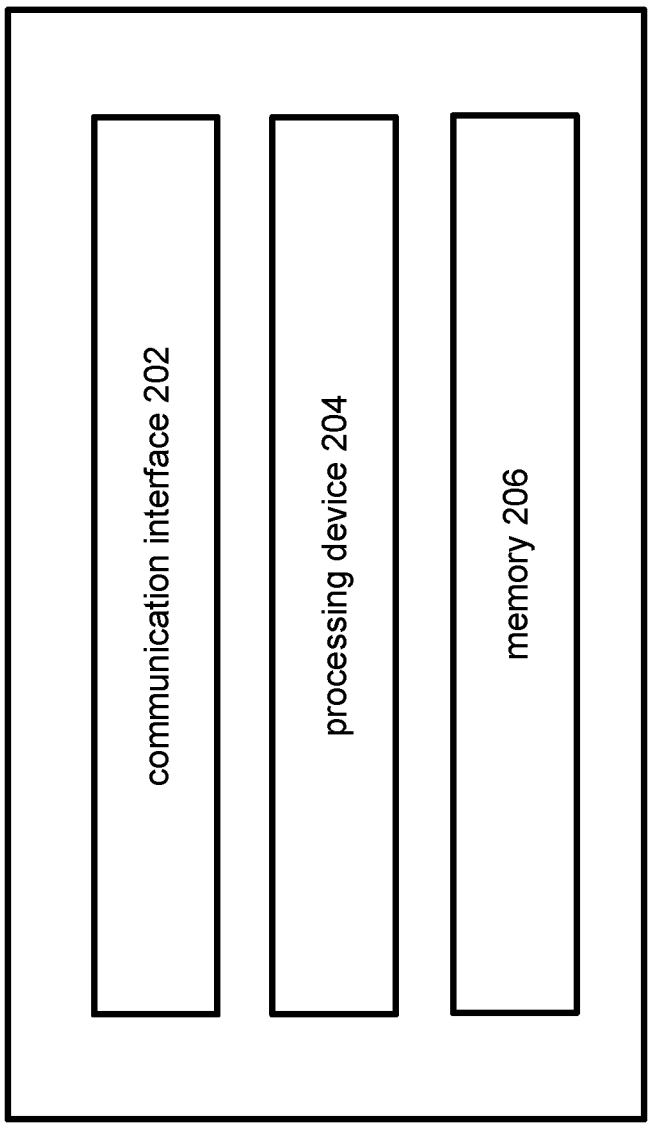
communication interface 202
processing device 204
memory 206
200

FIG. 2

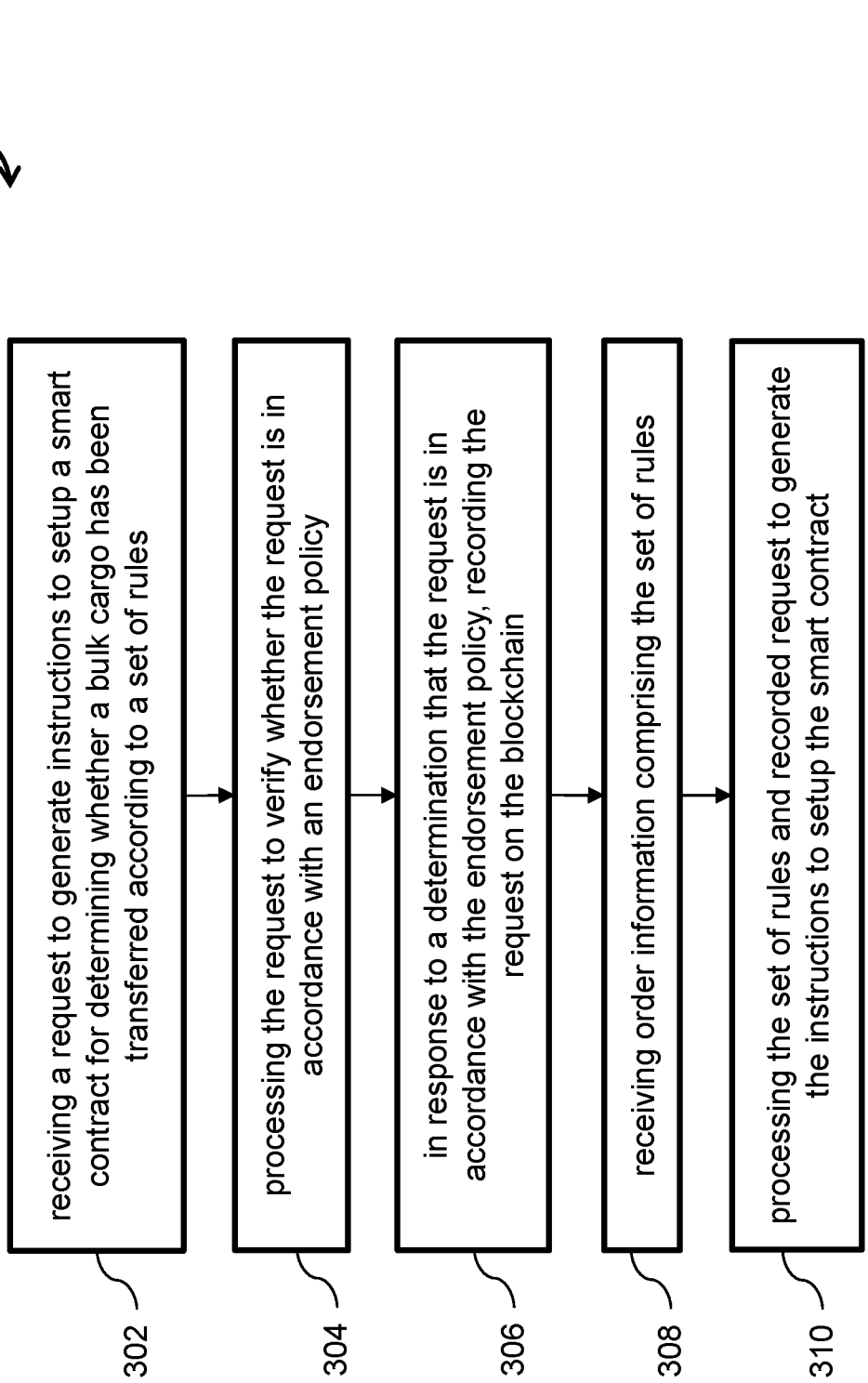
300
receiving a request to generate instructions to setup a smart contract for determining whether a bulk cargo has been transferred according to a set of rules
302
processing the request to verify whether the request is in accordance with an endorsement policy
304
in response to a determination that the request is in accordance with the endorsement policy, recording the request on the blockchain
306
receiving order information comprising the set of rules
308
processing the set of rules and recorded request to generate the instructions to setup the smart contract
310

FIG. 3A

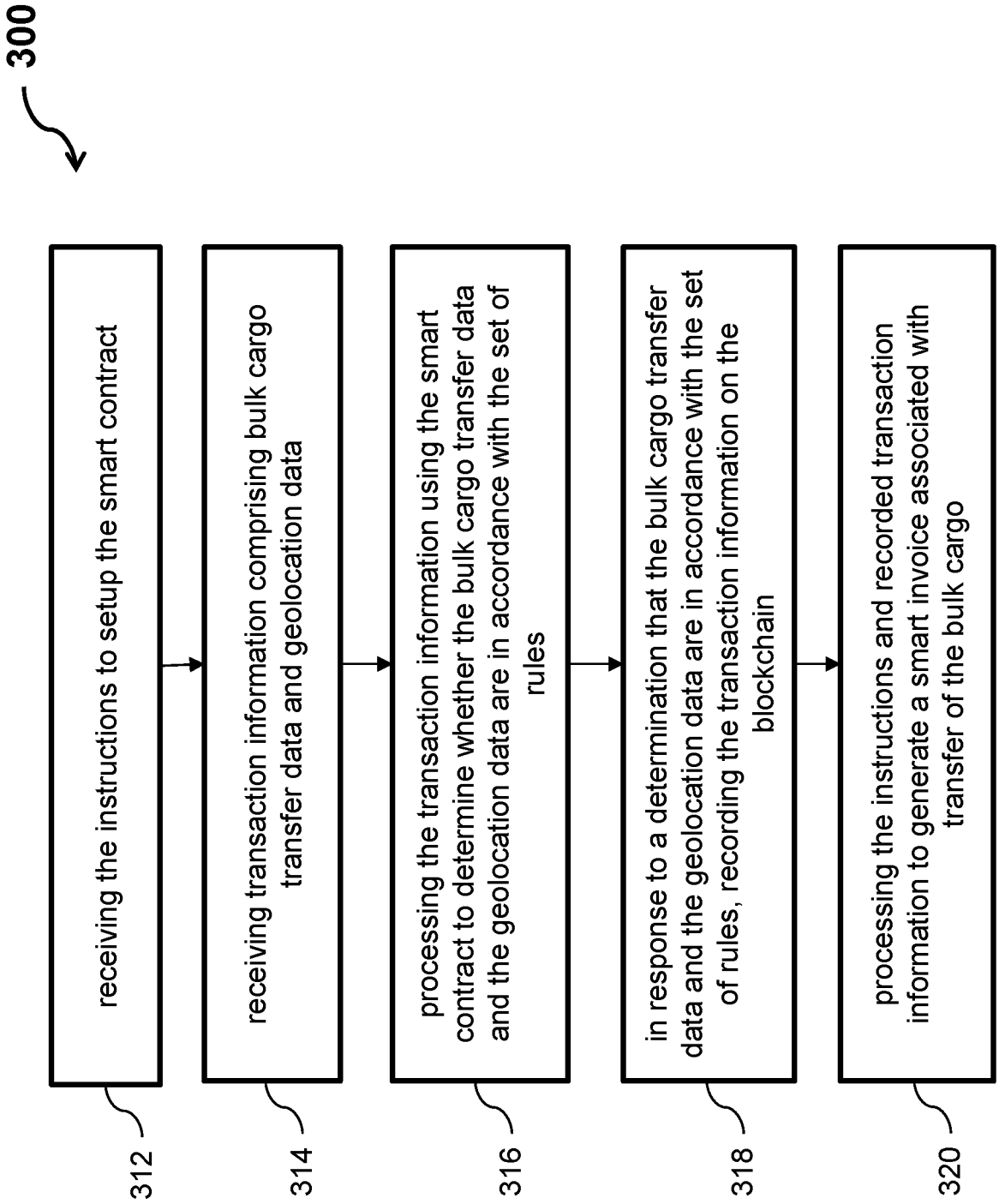
300
receiving the instructions to setup the smart contract
312
receiving transaction information comprising bulk cargo transfer data and geolocation data
314
processing the transaction information using the smart contract to determine whether the bulk cargo transfer data and the geolocation data are in accordance with the set of rules
316
in response to a determination that the bulk cargo transfer data and the geolocation data are in accordance with the set of rules, recording the transaction information on the blockchain
318
processing the instructions and recorded transaction information to generate a smart invoice associated with transfer of the bulk cargo
320

FIG. 3B

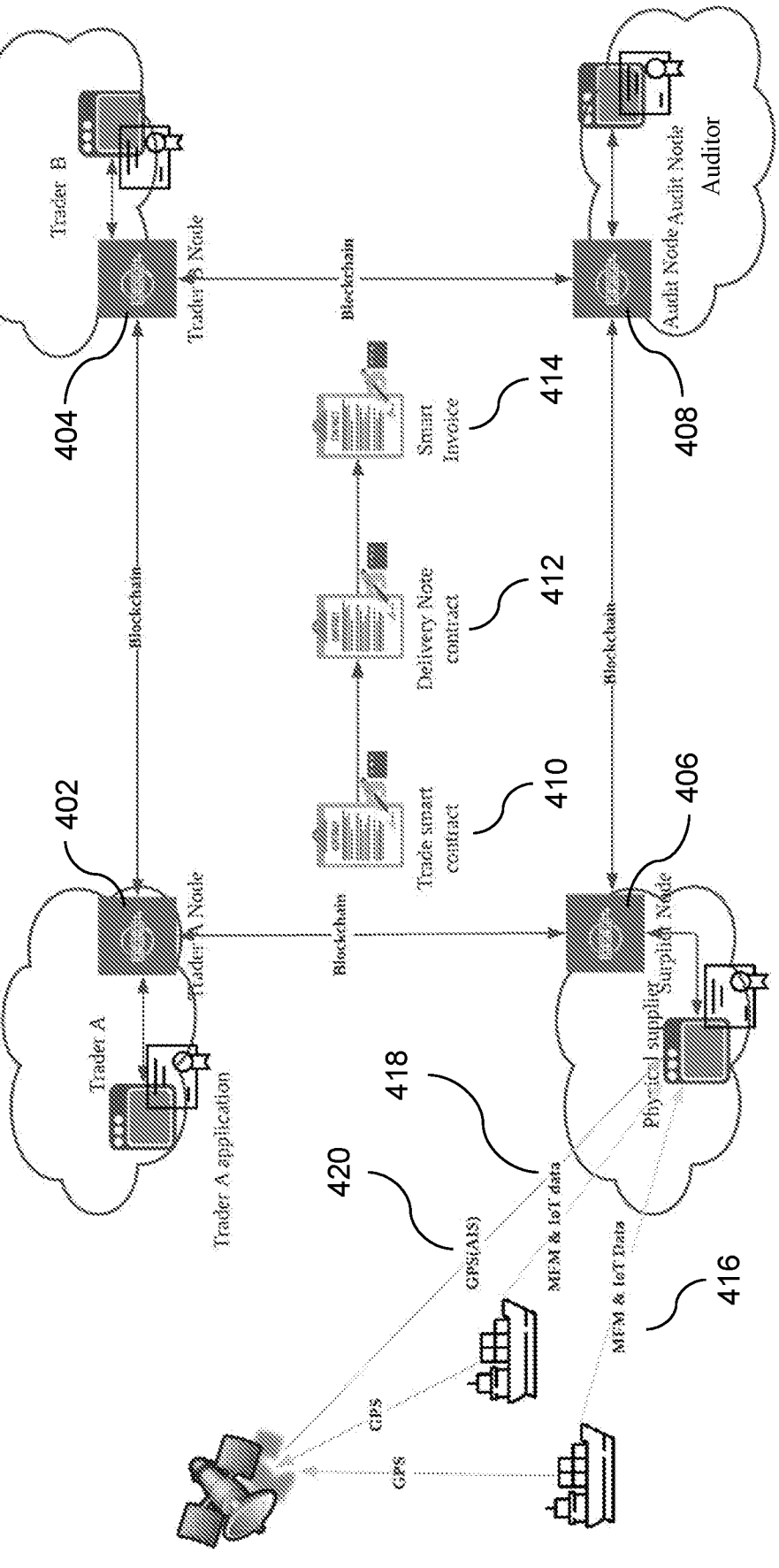
Trader B
Trader B Node
Blockchain
Audit Node
Auditor
404
408
Smart Invoice
414
Delivery Note contract
412
Trade smart contract
410
402
406
Trader A
Trader A application
Trader A Node
Blockchain
Physical supplier
Supplier Node
418
420
GPS(AIS)
MEM & IoT data
GPS
GPS
MEM & IoT Data
416
400

FIG. 4

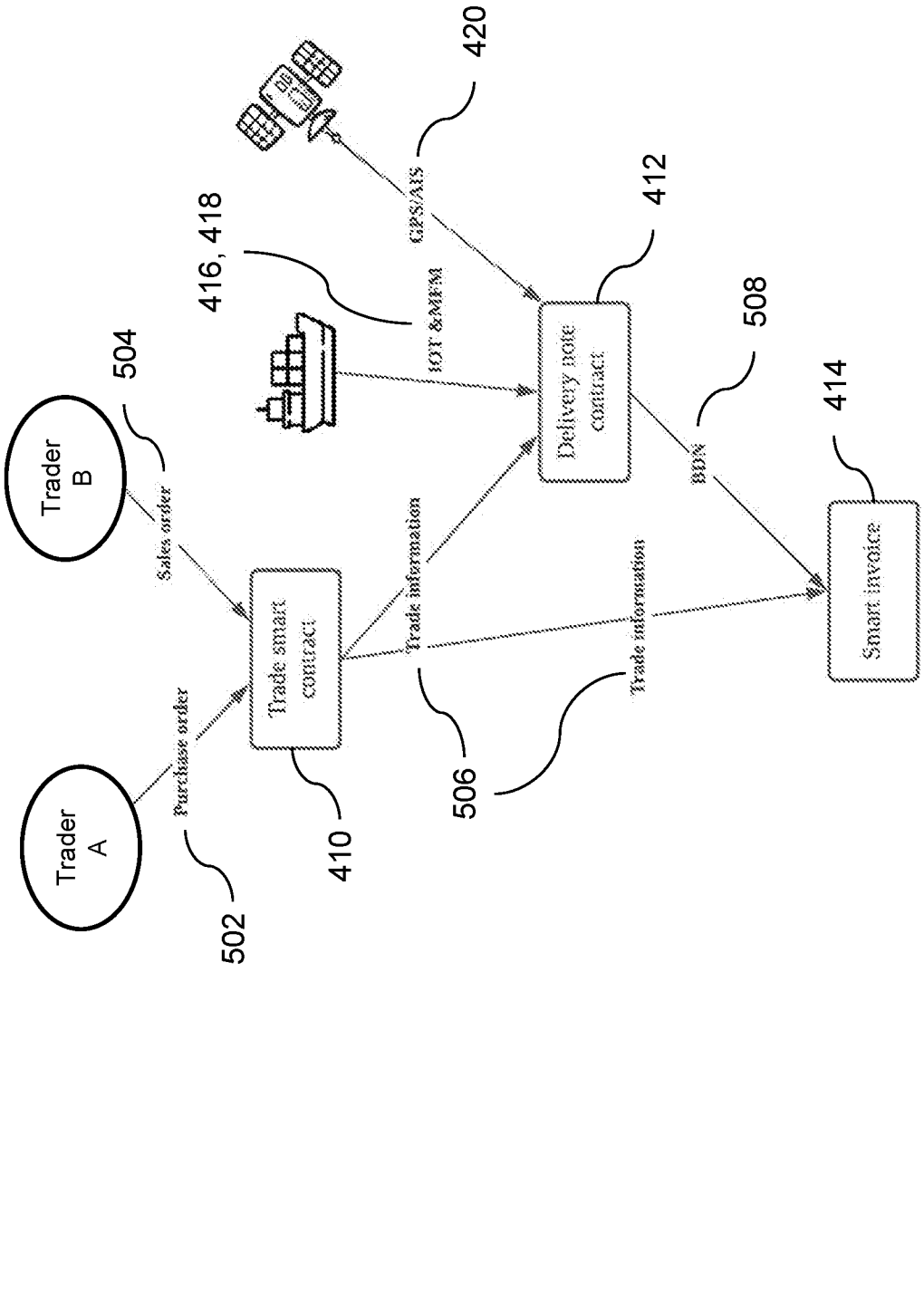
500
Trader A
Trader B
Purchase order
Sales order
Trade smart contract
Trade information
Trade information
Delivery note contract
BDN
Smart invoice
IOT &MFM
GPS/AIS
502
504
410
506
416, 418
420
412
508
414

FIG. 5

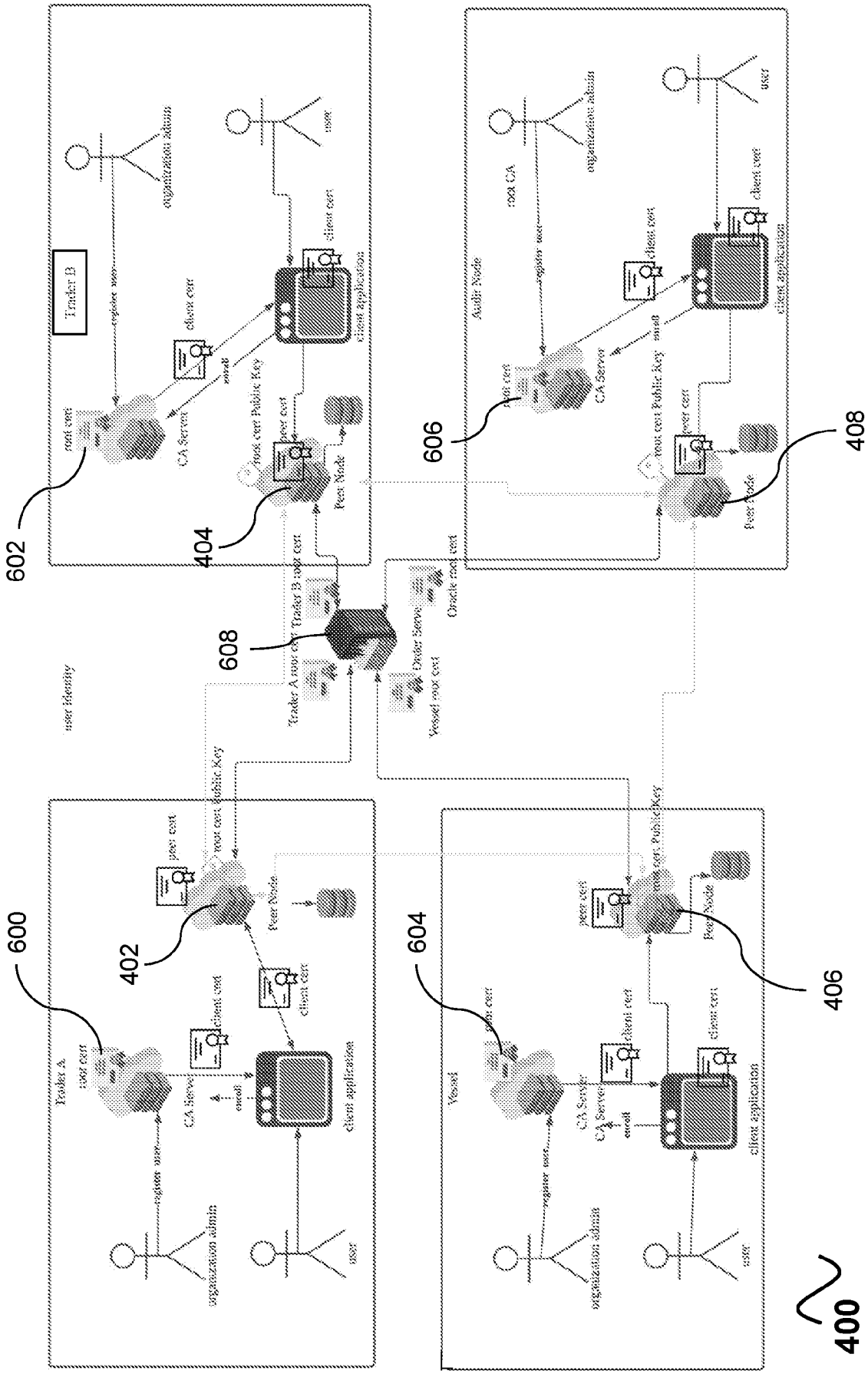
Trader B
organization admin
user
register user
client cert
enroll
CA Server
root cert
client application
root cert Public Key
peer cert
Peer Node
602
404
608
606
408
Audit Node
root CA
Trader A root cert
Trader B root cert
Oracle root cert
Vessel root cert
user identity
Oracle Server
600
402
Trader A
Vessel
604
406
400

FIG. 6A

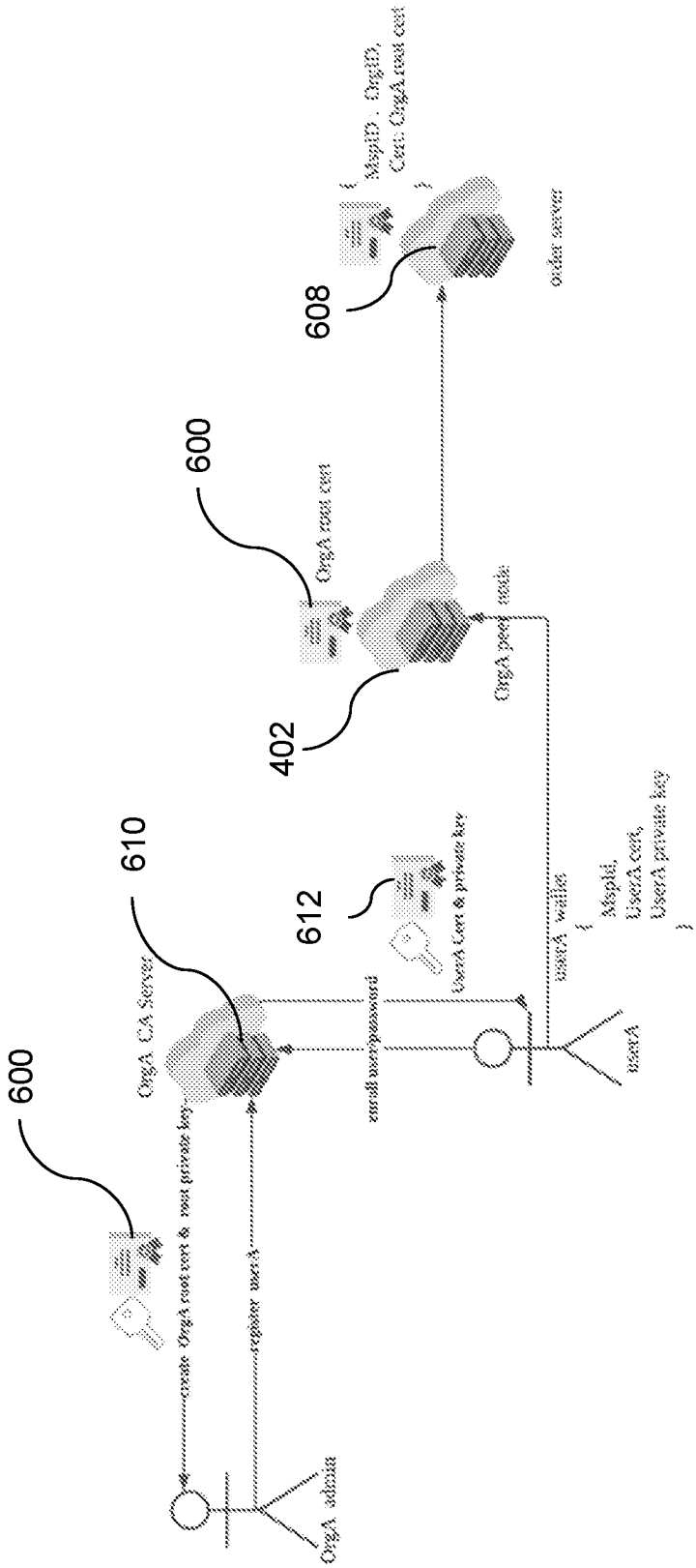
600
OrgA admin
create OrgA root cert & root private key
register user1
OrgA CA Server
610
enroll user/password
612
User1 Cert & private key
600
OrgA root cert
402
OrgA peer node
608
order server
MspID , OrgID,
Cert: OrgA root cert
}
user1 wallet
{
MspId,
User1 cert,
User1 private key
}
user1

FIG. 6B

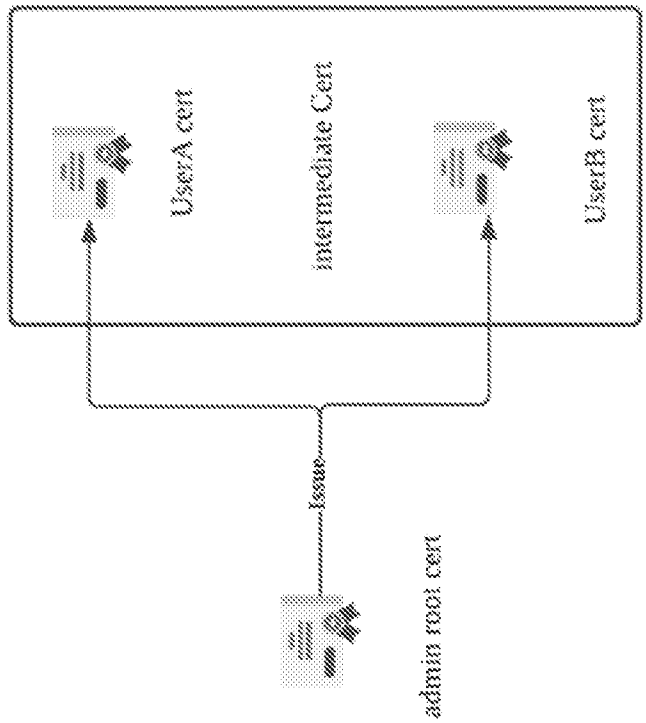
UserA cert
Intermediate Cert
UserB cert
Issue
admin root cert

FIG. 6C

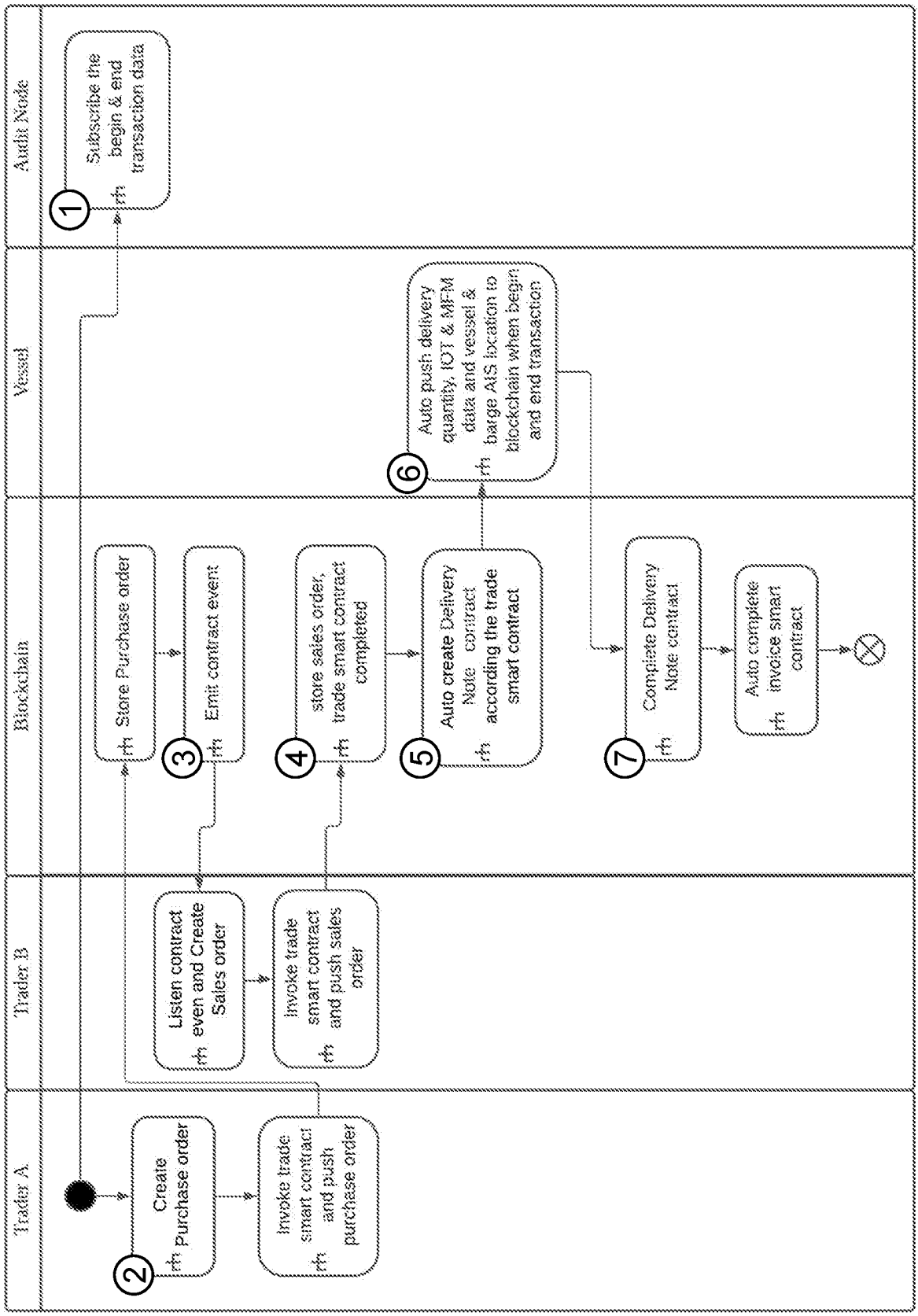
Trader A
Trader B
Blockchain
Vessel
Audit Node
1
Subscribe the begin & end transaction data
2
Create Purchase order
Invoke trade smart contract and push purchase order
Listen contract even and Create Sales order
Invoke trade smart contract and push sales order
Store Purchase order
3
Emit contract event
4
store sales order, trade smart contract completed
5
Auto create Delivery Note contract according the trade smart contract
6
Auto push delivery quantity, IOT & MFM data and vessel & barge AIS location to blockchain when begin and end transaction
7
Complete Delivery Note contract
Auto complete invoice smart contract

FIG. 7

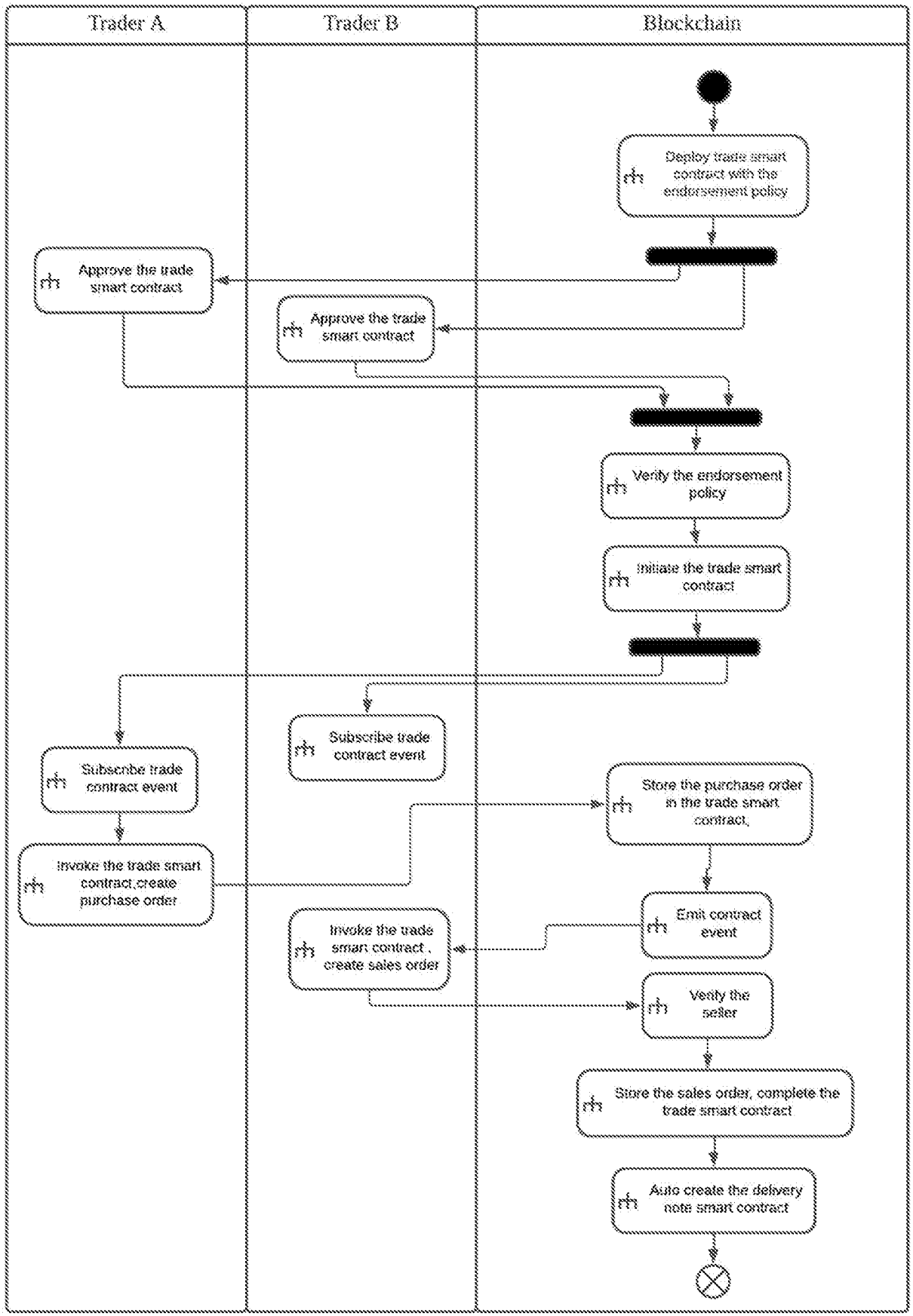
Trader A
Trader B
Blockchain
Deploy trade smart contract with the endorsement policy
Approve the trade smart contract
Approve the trade smart contract
Verify the endorsement policy
Initiate the trade smart contract
Subscribe trade contract event
Subscribe trade contract event
Store the purchase order in the trade smart contract,
Invoke the trade smart contract,create purchase order
Emit contract event
Invoke the trade smart contract , create sales order
Verify the seller
Store the sales order, complete the trade smart contract
Auto create the delivery note smart contract

FIG. 8

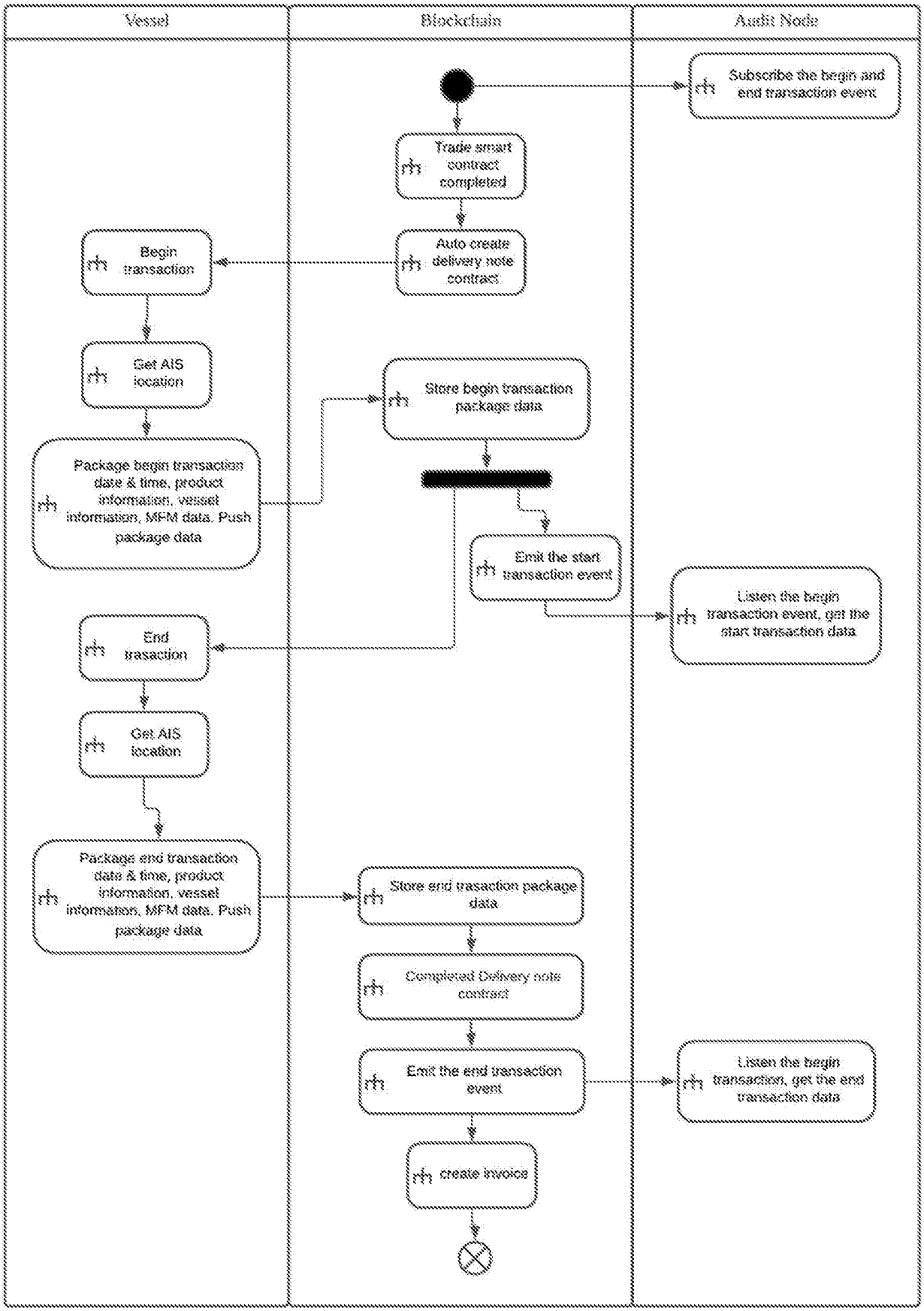
Vessel
Blockchain
Audit Node
Subscribe the begin and end transaction event
Trade smart contract completed
Auto create delivery note contract
Begin transaction
Get AIS location
Store begin transaction package data
Package begin transaction date & time, product information, vessel information, MFM data. Push package data
Emit the start transaction event
Listen the begin transaction event, get the start transaction data
End trasaction
Get AIS location
Package end transaction date & time, product information, vessel information, MFM data. Push package data
Store end trasaction package data
Completed Delivery note contract
Emit the end transaction event
Listen the begin transaction, get the end transaction data
create invoice

FIG. 9

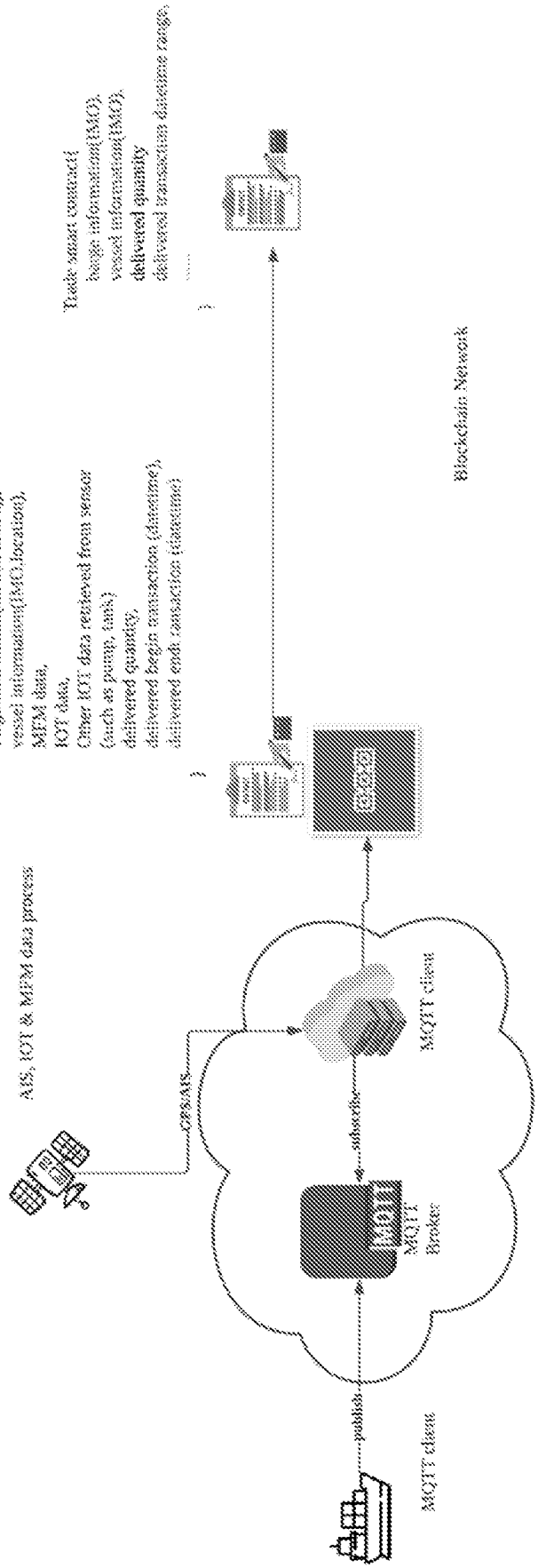
Delivery Note contract{
barge information{IMO,location,},
vessel information{IMO,location},
MFM data,
IOT data,
Other IOT data retrieved from sensor
(such as pump, tank)
delivered quantity,
delivered begin transaction (datetime),
delivered end transaction (datetime)
}
Trade smart contract{
barge information{IMO},
vessel information{IMO},
delivered quantity
delivered transaction datetime range,
.....
}
Blockchain Network
AIS, IOT & MFM data process
GPS/AIS
subscribe
MQTT client
MQTT
Broker
publish
MQTT client

FIG. 10

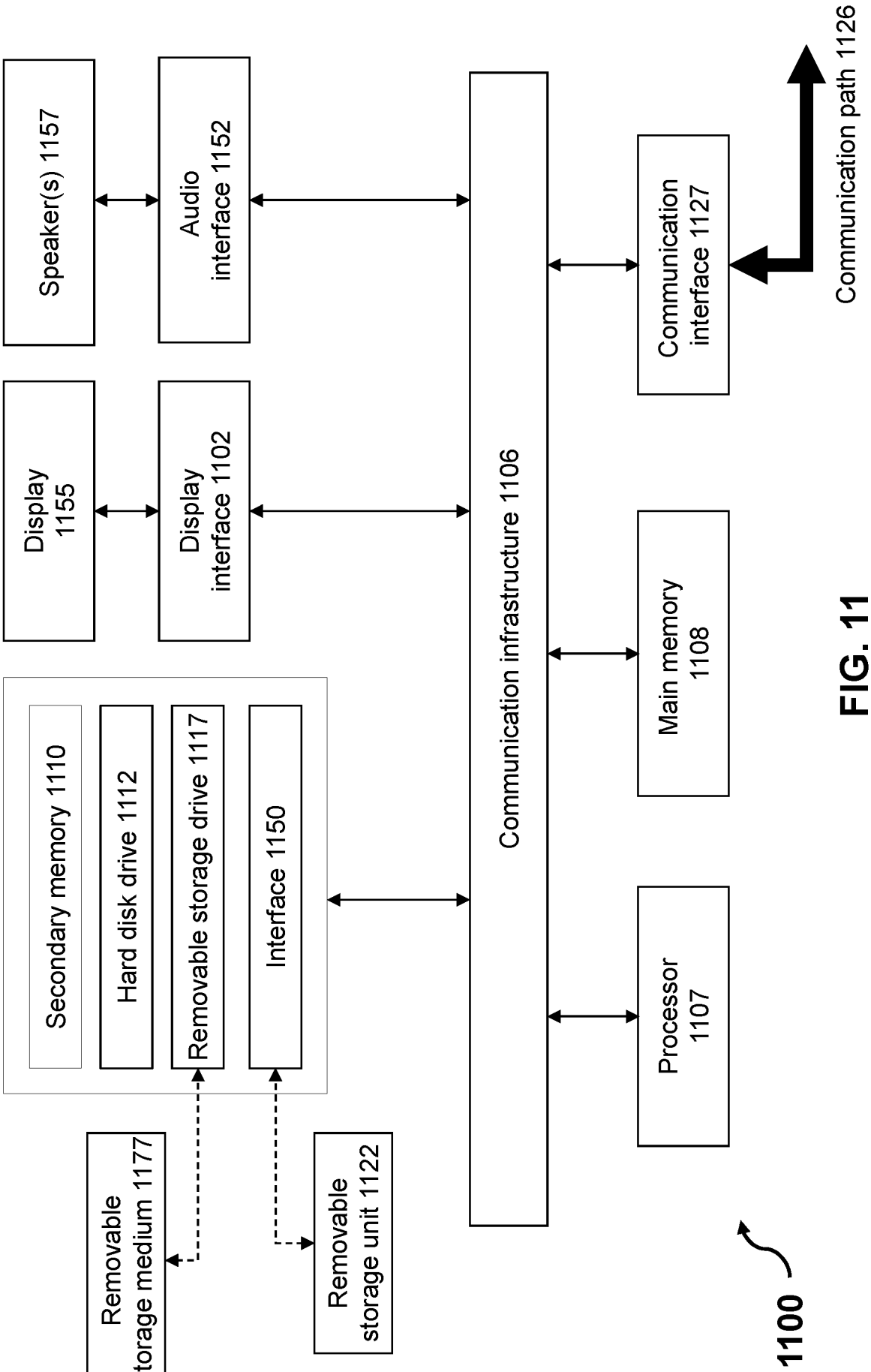
1100
Processor 1107
Main memory 1108
Communication infrastructure 1106
Communication interface 1127
Communication path 1126
Audio interface 1152
Speaker(s) 1157
Display interface 1102
Display 1155
Interface 1150
Removable storage drive 1117
Hard disk drive 1112
Secondary memory 1110
Removable storage unit 1122
Removable storage medium 1177

FIG. 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG2022/050309

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00(2006.01)i; **G06Q 50/28**(2012.01)i; **H04L 9/32**(2006.01)i; **G06Q 10/08**(2012.01)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 9/00(2006.01); B65G 1/137(2006.01); G06F 17/30(2006.01); G06Q 10/06(2012.01); G06Q 20/40(2012.01); G06Q 30/00(2006.01)

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) & Keywords: transaction, blockchain, bulk cargo transfer data, geolocation, verifying

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CRISTHIAN MARTINEZ-RENDON et al. On the continuous contract verification using blockchain and real-time data. Springer. 23 February 2021, pages 1-28, ISSN 1386-7857. Pages 8, 11-12, 14, 17, 21; and figures 1-2, 9	1-18
Y	PETRI HELO et al. Real-time supply chain—A blockchain architecture for project deliveries. Robotics and Computer-Integrated Manufacturing. 18 November 2019, Vol. 63, pages 1-14. Pages 6-9; and figures 6-7	1-18
A	US 2016-0098723 A1 (THE FILING CABINET, LLC) 07 April 2016 (2016-04-07) Paragraphs [0037]-[0050]; claim 1; and figure 2	1-18
A	US 2016-0217399 A1 (ELEMENTUM SCM (CAYMAN) LTD.) 28 July 2016 (2016-07-28) Paragraphs [0063]-[0078]; claim 1; and figure 1	1-18
A	US 2020-0311644 A1 (AMERICA'S COLLECTIBLES NETWORK, INC.) 01 October 2020 (2020-10-01) Paragraphs [0035]-[0045]; claim 1; and figure 1	1-18

☐ 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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 August 2022	**10 August 2022**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea**	**YANG, JEONG ROK**
Facsimile No. **+82-42-481-8578**	Telephone No. **+82-42-481-5709**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG2022/050309

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2016-0098723 A1	07 April 2016	US 2016-0098730 A1	07 April 2016
US 2016-0217399 A1	28 July 2016	None	
US 2020-0311644 A1	01 October 2020	US 11113648 B2	07 September 2021
		US 11195129 B2	07 December 2021
		US 2020-0265381 A1	20 August 2020
		US 2020-0272970 A1	27 August 2020