



- (51) **International Patent Classification:**
G06Q 10/08 (2012.01) *G06Q 10/06* (2012.01)
- (21) **International Application Number:**
PCT/US2022/012504
- (22) **International Filing Date:**
14 January 2022 (14.01.2022)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
63/134,680 07 January 2021 (07.01.2021) US
- (71) **Applicant:** COVESTRO LLC [US/US]; 1 Covestro Circle, Pittsburgh, Pennsylvania 15205 (US).
- (72) **Inventors:** OWENS, Steven G.; 251 Ritter Road, Sewickley, Pennsylvania 15143 (US). STEPPAN, David D.; 104 Drury Court, Gibsonia, Pennsylvania 15044 (US). GILES, Eric C.; 1638 Farmington Court, Pittsburgh, Pennsylvania 15237 (US). CLOHERTY, Scott M.; 738 Mission Hills Drive, Canonsburg, Pennsylvania 15317 (US). ULAM, Devin W.; 526 North Meadowcroft Avenue, Pittsburgh, Pennsylvania 15216 (US).

(74) **Agent:** BENDER, Richard P.; 1 Covestro Circle, Pittsburgh, 15205 (US).

(81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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, 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).

(54) **Title:** TITLE - BLOCKCHAIN VERIFICATION SYSTEM FOR SPRAY FOAM INSULATION

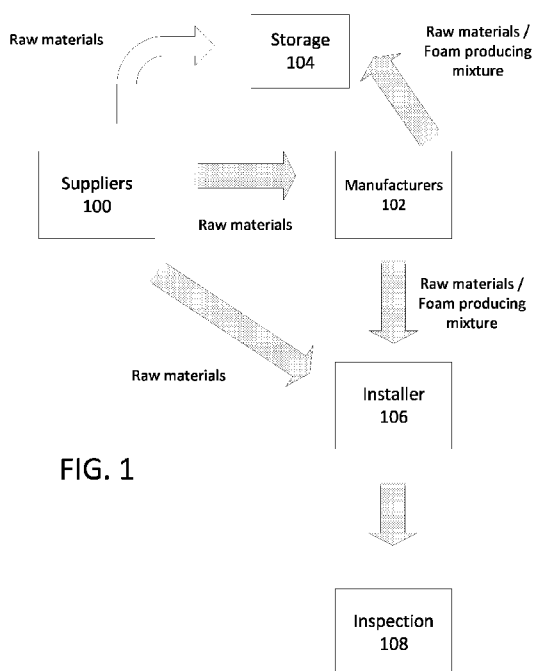


FIG. 1

(57) **Abstract:** A method of securing data associated with a product includes identifying raw materials needed to produce the product where suppliers supply raw materials to installers of the product. The method includes, for each identified raw material, identifying an associated supplier, and, for each identified supplier, receiving, from the identified supplier, a communication comprising quality data corresponding to its associated raw material, generating a supplier block that is associated with the identified supplier, storing the quality data in the supplier block of the identified supplier, adding the supplier block to a blockchain, and identifying one or more installers of the product. For each identified installer, the method includes receiving a communication comprising installation data associated with the product, generating an installation block that is associated with the identified installer, storing the installation data in the installation block of the identified installer, and adding the installation block to the blockchain.

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *with information concerning request for restoration of the right of priority in respect of one or more priority claims (Rules 26bis.3 and 48.2(b)(vii))*

TITLE - BLOCKCHAIN VERIFICATION SYSTEM FOR SPRAY FOAM INSULATION

BACKGROUND

[0001] In spray foam production, product quality is based on a variety of factors such as processing parameters, raw material specifications, and storage conditions. Variability in these factors can cause field failures of spray foam, which can lead to increased costs in warranty claims to manufactures. This is especially true for failures that occur years after manufacturing when manufacture and production records are no longer traceable to the final product.

SUMMARY

[0002] This disclosure is not limited to the particular systems, methodologies or protocols described, as these may vary. The terminology used in this description is for the purpose of describing the particular versions or embodiments, and is not intended to limit the scope.

[0003] As used in this document, the singular forms “a,” “an,” and “the” include plural references unless the context clearly dictates otherwise. Unless defined otherwise, all technical and scientific terms used in this document have the same meanings as commonly understood by one of ordinary skill in the art. As used in this document, the term “comprising” means “including, but not limited to.”

[0004] In an embodiment, a method of securing data associated with a product includes, by an electronic device, identifying a plurality of raw materials needed to produce the product. One or more suppliers supply at least a portion of the plurality of raw materials to one or more installers of the product. The method includes, for each identified raw material, identifying an

associated supplier of the identified raw material, and, for each identified supplier, receiving, from the identified supplier, a communication comprising quality data corresponding to its associated raw material, generating a supplier block that is associated with the identified supplier, storing at least a portion of the quality data in the supplier block of the identified supplier, adding the supplier block to a blockchain, and identifying one or more installers of the product. For each identified installer, the method includes receiving, from the identified installer, a communication comprising installation data associated with the product, generating an installation block that is associated with the identified installer, storing at least a portion of the installation data in the installation block of the identified installer, and adding the installation block to the blockchain. At least a portion of the blockchain is accessible by one or more of the identified suppliers and/or one or more of the identified installers according to an access policy associated with the blockchain. The access policy includes an access control list that defines one or more access rights to the blockchain.

[0005] In various embodiments, a computer program that includes one or more programming instructions, that when executed on an electronic device, cause the electronic device to perform the above-described method is disclosed.

[0006] In various embodiments, a system for securing data associated with a product includes an electronic device and a computer-readable storage medium is disclosed. The computer-readable storage medium includes one or more programming instructions that, when executed, cause the electronic device to perform the above-described method.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 illustrates an example lifecycle of spray foam insulation.

[0008] FIG. 2 illustrates an example spray foam insulation management system.

[0009] FIG. 3 illustrates an example blockchain structure.

[0010] FIG. 4 illustrates a flow chart of an example method of performing tamper-evident logging.

[0011] FIG. 5 illustrates an example of a source log.

[0012] FIG. 6A illustrates a flow chart of an example method of verifying access requests to a target blockchain.

[0013] FIGS. 6B and 6C illustrates example access requests according to various embodiments.

[0014] FIG. 7 illustrates an example delegation process.

[0015] FIG. 8 illustrates an illustration of an example multiple-tier delegation process according to an embodiment.

[0016] FIGS. 9A and 9B illustrate example tokens and data according to various embodiments.

[0017] FIG. 10 illustrates a block diagram of example hardware that may be used to contain or implement program instructions.

DETAILED DESCRIPTION

[0018] The following terms shall have, for purposes of this application, the respective meanings set forth below:

[0019] A “block” or a “node” refers to a data structure that includes a link to one or more other data structures. In certain embodiments, a block may include a grouping of data or data records. A block of a blockchain may include a link to an immediately preceding block in the blockchain, a subsequent block in the blockchain, a different block in the blockchain, or a different block in another blockchain.

[0020] A “blockchain” refers to a distributed data structure that includes a sequence of blocks that are linked together.

[0021] An “electronic device” or a “computing device” refers to a device that includes a processor and memory. Each device may have its own processor and/or memory, or the processor and/or memory may be shared with other devices as in a virtual machine or container arrangement. The memory may contain or receive programming instructions that, when executed by the processor, cause the electronic device to perform one or more operations according to the programming instructions. Examples of electronic devices include personal computers, servers, mainframes, virtual machines, containers, gaming systems, televisions, and mobile electronic devices such as smartphones, personal digital assistants, cameras, tablet computers, laptop computers, media players and the like. In a client-server arrangement, the client device and the server are each electronic devices, in which the server contains instructions and/or data that the client device accesses via one or more communications links in one or more communications networks. In a virtual machine arrangement, a server may be an electronic device, and each virtual machine or container may also be considered to be an electronic device. In the discussion below, a client device, server device, virtual machine or container may be referred to simply as a “device” for brevity.

[0022] The terms “memory,” “memory device,” “computer-readable medium”, “data store,” “data storage facility” and the like each refer to a non-transitory device on which computer-readable data, programming instructions or both are stored. Except where specifically stated otherwise, the terms “memory,” “memory device,” “computer-readable medium”, “data store,” “data storage facility” and the like are intended to include single device embodiments, embodiments in which multiple memory devices together or collectively store a set of data or instructions, as well as individual sectors within such devices.

[0023] The terms “processor” and “processing device” refer to a hardware component of an electronic device that is configured to execute programming instructions. Except where specifically stated otherwise, the singular term “processor” or “processing device” is intended to include both single-processing device embodiments and embodiments in which multiple processing devices together or collectively perform a process.

[0024] A “private key” refers to an asymmetric cryptographic key that is used to encrypt or decrypt messages, data, information, or other content. Messages encrypted using a private key may be decrypted by a recipient who possesses an associated public key. Likewise, messages that are encrypted using an associated public key may be decrypted using a private key.

[0025] A “public key” refers to an asymmetric cryptographic key that are generally obtained and used without restriction to encrypt and/or decrypt messages. Messages encrypted using a public key may be decrypted by a recipient who possesses an associated private key. Likewise, messages that are encrypted using a private key may be decrypted by a recipient who possesses an associated public key.

[0026] A “spray foam product” or “spray foam insulation” refers to a foam producing mixture that, when the active components of the mixture are combined, will create a foam

insulation structure that will harden in place and/or the foam insulation structure itself. The polyol component and the isocyanate component are considered the active components of the mixture, as the foam is produced once these two components come into contact with each other. Spray foam insulation provides insulation and serves as an air-barrier.

[0027] Spray foam insulation is applied in a spray fashion using a spray application apparatus. If spray foam insulation is not produced as expected with the correct combination of materials or under improper processing conditions, the insulation may be created with voids, differences in foam density, adhesion issues, poor mixing and poor foam quality, and/or other concerns. These issues are sometimes identified at the manufacturing level. But often, they are identified further along the supply chain, such as at distribution or end-use. As such, it is important to have traceability and trackability of spray foam insulation through its manufacture, delivery, installation, and use lifecycle in order to more precisely pinpoint the cause or source of any quality problems.

[0028] FIG. 1 illustrates an example lifecycle of spray foam insulation according to various embodiments. A spray foam insulation manufacturing process may involve suppliers of raw materials providing **100** one or more raw materials to a manufacturer. The suppliers may provide the manufacturer with materials and specifications and lot specific data associated with the provided raw materials. Examples of raw materials are discussed in more detail below.

[0029] The manufacturer may combine **102** the raw materials in an appropriate combination or apportionment into a foam producing mixture, which it may provide to one or more contractors. The raw materials and/or the foam producing mixture may be stored **104** before being transported to a contractor, a job site, or other location. The raw materials may be stored in a manufacturing warehouse or other storage location before being transported.

[0030] As illustrated by FIG. 1, one or more suppliers may provide **100** one or more raw materials directly to an installer. An installer refers to a person or entity who is responsible for applying a foam producing mixture to create a foam structure. An example of an installer may be a contractor, a sub-contractor, and/or the like. An installer may receive one or more raw materials from one or more suppliers and/or one or more manufacturers. The installer may combine one or more of the received raw materials to create a foam producing mixture, which may be applied or installed as spray foam insulation as described in more detail below.

[0031] At a job site, an installer (or other party) may apply **106** a foam producing mixture. The foam producing mixture may be sprayed by a person or a robot, onto a surface, such as onto an exterior wall, or the inside surface of a roof, to which the foam producing mixture will adhere and the foam structure will be created and harden in place. Various spray application devices such as, for example, spray guns, can be used to spray the foam producing mixture onto a surface. Spray application devices may include a heater to heat the foam producing mixture or its components, to make the mixture less viscous and more likely to be sprayed evenly. As noted above, polyurethane foam is formed from combining a polyol component that typically comprises one or more polyols and other additives, such as blowing agents and flame retardants, among others, and a polyisocyanate component. In these cases, it is often desirable that the polyol component and polyisocyanate component be metered and mixed in a plural-component spray gun at a 1:1 volume ratio.

[0032] The spray emitted from the spray application device may be in a shape reflective of the nozzle, which is often in the shape of a cone. It is referred to herein as a cone, although the shape may not be mostly circular; the cone may have an oblong or a flat shape. The spray forms a pattern as it hits and attaches to the surface to which it is applied. The person or robot that

applies the spray then moves the spray application device to apply a relatively even amount of the foam onto the intended surface. The speed and movement of the person or robot applying the foam, as well as the locations that are sprayed, may depend upon the quality of the cone and spray pattern. In applying the spray, it is important to maintain uniform or minimum thickness, and monitor the quality of the foam such that it does not contain voids.

[0033] Once installed, the spray foam insulation may be inspected **108** by one or more inspectors. Spray foam insulation may be inspected to confirm that installation complies with one or more rules, regulations, specifications, codes, and/or the like. For example, the spray foam insulation may be inspected **108** by building inspector to confirm compliance with one or more building codes.

[0034] Although the present disclosure discusses the use of spray foam insulation, it is understood that the systems and methods disclosed in this document may also apply to other products or types of products.

[0035] FIG. 2 illustrates an example product management system according to an embodiment. As illustrated in FIG. 2, a system **200** may include one or more host electronic devices **204a-N** and one or more client electronic devices **202a-N**. A host electronic device **204a-N** may be located remotely from a client electronic device **202a-N**. A server is an example of a host electronic device **204a-N** according to an embodiment. A host electronic device **204a-N** may have or be in communication with one or more data stores **206a-N**. In various embodiments, a host electronic device **204a-N** may include or be in communication with a rights management system **220**.

[0036] A host electronic device **204a-N** may be in communication with one or more client electronic devices **202a-N** over one or more communication networks **208a-N**. A

communication network **208a-N** may be a local area network (LAN), a wide area network (WAN), a mobile or cellular communication network, an extranet, an intranet, the Internet and/or the like.

[0037] In various embodiments, a client electronic device **202a-N** may be a portable electronic device such as, for example, a smartphone, a tablet, a laptop, a wearable and/or the like. In other embodiments, a client electronic device **202a-N** may be desktop computer or other electronic device.

[0038] A client electronic device **202a-N** may be associated with a particular participant or representative in the supply chain lifecycle of the product. For example, as illustrated in FIG. 2, one or more client electronic devices **202a-N** may be associated with a manufacturer **212** of spray foam insulation, a supplier **214** of spray foam insulation, an installer **216** of spray foam insulation, an inspector **218** responsible for inspecting spray foam insulation or installation of spray foam insulation, and/or the like.

[0039] As illustrated by FIG. 2, one or more host electronic devices **204a-N** may have access to one or more blockchains **210a-N**. The one or more blockchains may be used to manage the lifecycle of the product, as described throughout this disclosure. The one or more host electronic devices may read, write, query, and/or otherwise access the blockchain. For example, the one or more host electronic devices may create new blocks on the blockchain, access the blockchain, and/or retrieve information from the blockchain in response to receiving requests from one or more client electronic devices.

[0040] As illustrated by FIG. 2, one or more host electronic devices **204a-N** may include or be in communication with a rights management system **220**. A rights management system **220** may include one or more electronic devices and/or one or more data stores. A rights management

system **220** may maintain and/or implement one or more access policies that are applicable to the blockchain as explained in more detail below.

[0041] FIG. 3 illustrates an example blockchain data structure according to an embodiment. A blockchain **300a-N** includes one or more blocks **302a-N**. Optionally, a block may include one or more log records **304a-N**. As new log records are generated, a corresponding data representation of those log records may be added to the blockchain **300a-N** as part of a new block. As such, blocks **302a-N** of a blockchain **300a-N** may be positioned in a linear, sequential order. For example, blocks may be arranged in a chronological order. Blocks **302a-N** in a blockchain **300a-N** are linked to preceding blocks in the chain as illustrated in FIG. 3.

[0042] Optionally, one or more blocks **302a-N** of a blockchain **300a-N** may occupy the same data store or memory space. Alternatively, a blockchain **300a-N** may be implemented as via a distributed data store. For instance, blocks **302a-N** of a blockchain **300a-N** may not occupy the same data store or memory space, but rather two or more blocks in a blockchain may be implemented as distributed data stores. These distributed data stores may exist amongst remote electronic devices. For instance, part of a blockchain **300a-N** may be stored in a data store that is associated with a first electronic device in a first location, while a different part of the blockchain may be stored in a different data store that is associated with a second electronic device in a second location that is different from the first location.

[0043] A block **302a-N** of a blockchain **300a-N** may be located in a data store at a first location, while a second block of the blockchain may be located in a data store at a second location. Despite remote storage proximity to one another, the blocks **302a-N** may still form the blockchain **310a-N** as they are linked to one another such as, for example, by way of their signatures.

[0044] In various embodiments, one or more participants of the system (e.g., manufacturers, suppliers, installers, and/or other authorized users) may have a key pair that each may use to communicate and/or verify or authenticate communications and other information shared throughout the system. The key pair may include a private key and a public key associated with each participant. For example, if Supplier A, Supplier B and Supplier C are participants of the system, each may be associated with its own public/private key pair $\{ K_{pu}, K_{pr} \}$.

[0045] A participant may generate its own public and private keys. For example, a system associated with a participant may include a key generator, such as, for example, a random key generator, which may generate a public/private key pair for the participant. All client electronic devices associated with the participant may utilize the same public/private key pair in its communications with the system in order to uniquely authenticate itself as part of the participant's network. It is understood that client electronic devices associated with a participant may utilize different public/private key pairs in some embodiments, each associated with the participant. In various embodiments, one or more electronic devices associated with a participant (e.g., one or more client electronic devices) may store a generated key pair in a secure data store associated with such device.

[0046] In various embodiments, each participant of the system may provide its public key with the system. The system may store one or more public keys and an indication of the participant to which it belongs in one or more data stores such as, for example, a key store. As explained in more detail below, the system may utilize a key store to authenticate communications via the system.

[0047] FIG. 4 illustrates a flow chart of an example method of securing the integrity of production of a product through tamper-evident logging according to an embodiment. Tamper-evident logging refers to a process that makes changes, modifications or access to log records easily detectable. This is true for modifications or changes made by unauthorized users who have no privileges on the system, as well as authorized users of the system.

[0048] As illustrated by FIG. 4, the system may identify **400** one or more raw materials. The one or more raw materials may be materials needed to produce the product, in whole or in part. For instance, a raw material of a product may be a material from which the product is made. In various embodiments, a listing of one or more raw materials needed to produce the product may be stored in a data store associated with or accessible by a host electronic device.

[0049] Example raw materials used in producing spray foam insulation may include liquids or gases that are sprayed into atmospheric pressure and temperature conditions, where the materials react with each other to produce foam. Such foam producing mixtures are typically prepared such that components of the mixture typically are mixed together just before it is sprayed and applied on a surface, where it will harden. The foam producing mixture typically comprises an organic polyisocyanate, a polymeric polyol, and a blowing agent.

[0050] Any of the known organic polyisocyanates may be used to produce spray foam insulation within the scope of this disclosure. Examples of suitable polyisocyanates include, without limitation, substituted or unsubstituted aromatic, aliphatic, and cycloaliphatic polyisocyanates having at least two isocyanate groups. Polyfunctional aromatic isocyanates are often used. Specific examples of suitable aromatic isocyanates include, but are not limited to, 4,4'- diphenylmethane diisocyanate (MDI), polymeric MDI (pMDI), toluene diisocyanate, allophanate-modified isocyanates, isocyanate-terminated prepolymers and carbodiimide-

modified isocyanates. The organic polyisocyanate may comprise pMDI having an average NCO functionality of from 2.2 to 3.3 and a viscosity of from 25 to 2000 mPas and prepolymers thereof prepared with polyols or other oligomers or polymers such as polyether or polyester polyols that contain active hydrogen atoms. The pMDI may have a functionality of from 2.2 to 3.0 and a viscosity less than about 800 mPas at 25°C. Any mixtures of organic polyisocyanates may be used.

[0051] The organic polyisocyanate(s) is/are included in the foam producing mixture, in an amount of at least 50%, such as from 55% to 75%, or, in some cases, from 59% to 69% by weight, based on total weight of the foam producing mixture.

[0052] The polymeric polyol may be any material having at least two reactive groups capable of reacting with an isocyanate group. The polymeric polyol may be an aromatic polyester polyol and/or a polyether polyol, such as those having an average hydroxyl functionality of from 2 to 8, such as 2 to 6, or, in some cases, 2.0 to 2.5, and/or a hydroxyl number of 100 mg KOH/gm to 1000 mgKOH/gm or, in some cases, 200 mgKOH/gm to 500 mgKOH/gm. In certain embodiments, a blend of an aromatic polyester polyol and a polyester and/or polyether polyol that contains renewable content derived from incorporation of regenerable materials, such as fatty acid triglycerides, sugar, or natural glycerin, is used. The polymeric polyol(s) is/are present in an amount of 10% to 40%, such as 20% to 40%, or, in some cases, 25% to 35% by weight, based on total weight of the foam producing mixture.

[0053] The relative amounts of organic polyisocyanate and polymeric polyol(s) used in the foam producing mixture are selected so as to provide the composition with a NCO:OH index of at least 1.8, such as at least 2.0, or, in some cases, 2.0 to 3.0.

[0054] As indicated, the mixture may include a blowing agent composition having one or more hydrocarbon blowing agents with an atmospheric pressure boiling point of at least 20°C (68°F). In certain embodiments, the blowing agent composition may include a hydrocarbon with an atmospheric pressure boiling point of at least 20°C (68°F) and water. As used in this disclosure, “hydrocarbon” refers to chemical compounds composed primarily of carbon and hydrogen that may contain heteroatoms such as oxygen, nitrogen, sulfur, or other elements. In certain embodiments, halogenated blowing agents with a global warming potential (“GWP”) $\geq$ 25 (100 year) and ozone depletion potential (“ODP”) > 0 are not used.

[0055] Specific examples of suitable hydrocarbons with an atmospheric pressure boiling point of at least 20°C (68°F) include, but are not limited to, n-pentane (atmospheric pressure boiling point of 36.1°C (96.9°F)), isopentane (atmospheric pressure boiling point of 27.7°C (81.9°F)), cyclopentane (atmospheric pressure boiling point of 49°C (120.2°F)), hexane (atmospheric pressure boiling point of 68°C (154.4°F)), 2,2-dimethylbutane (atmospheric pressure boiling point of 50°C (122°F)), 2-methylpentane (atmospheric pressure boiling point of 60°C (140°F)), 1-hexene (atmospheric pressure boiling point of 63°C (145.4°F)), 1-pentene (atmospheric pressure boiling point of 30°C (86°F)), acetone (atmospheric pressure boiling point of 56°C (132.8°F)), acetaldehyde (atmospheric pressure boiling point of 20.2°C (68.4°F)), dimethyl carbonate (atmospheric pressure boiling point of 90°C (194°F)), methylal (atmospheric pressure boiling point of 42.3°C (108.1°F)), ethyl formate (atmospheric pressure boiling point of 54.3°C (129.7°F)), methyl acetate (atmospheric pressure boiling point of 56.9°C (134.4°F)), and methyl formate (atmospheric pressure boiling point of 31.8°C (89.2°F)). As will be appreciated, mixtures of two or more of any of the foregoing or unlisted suitable hydrocarbons may be used.

In certain embodiments, the hydrocarbons with an atmospheric pressure boiling point of at least 20°C (68°F) is n-pentane, isopentane, cyclopentane, methyl formate, and/or methylal.

[0056] In certain embodiments, the hydrocarbon with an atmospheric pressure boiling point of at least 20°C (68°F) is present in an amount of at least 1% by weight, such as at least 2% by weight, or, in some cases, at least 3% by weight and up to 10% by weight, such as up to 8% by weight, or, in some cases, up to 6% by weight, based on total weight of the foam producing mixture.

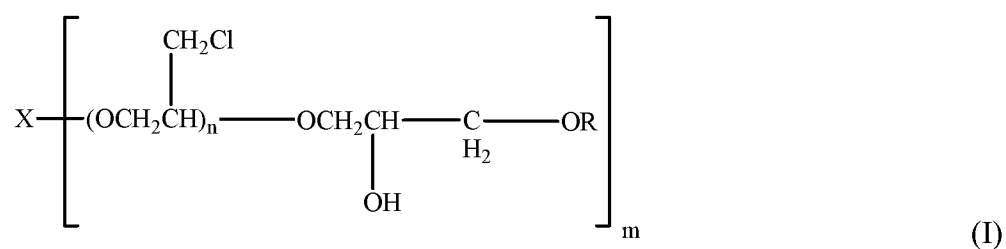
[0057] In addition to the hydrocarbon blowing agent, some water may be included in the blowing agent composition. As will be appreciated, water reacts with isocyanates to produce carbon dioxide gas as an auxiliary blowing agent. The amount of water included in the foam-forming composition will often range from 0.05% to 1.0% by weight, such as 0.1% to 0.8% by weight, based on total weight of the foam producing mixture.

[0058] If desired, it is also possible that the blowing agent composition may include a hydrocarbon, such as a hydrofluoroolefin, having an atmospheric pressure boiling point of less than 20°C (68°F), specific examples of which include, but are not limited to, butane (atmospheric pressure boiling point of -1°C (30.2°F)), isobutane (atmospheric pressure boiling point of -11.7°C (10.9°F)), butylene (atmospheric pressure boiling point of -6.6°C (20.1°F)), isobutylene (atmospheric pressure boiling point of -6.9°C (19.6°F)), trans-1-chloro-3,3,3-trifluoropropene (atmospheric pressure boiling point of 19°C (66.2°F)), and dimethyl ether (atmospheric pressure boiling point of -24°C (-11.2°F)).

[0059] In addition, the foam producing mixture may include any of a variety of optional ingredients.

[0060] The foam producing mixture may include a flame retardant composition. Suitable flame retardants for use in the foam-forming composition include, without limitation, halogenated, such as brominated flame retardants, such as brominated polyols, and phosphonated flame retardants, such as a halogenated, such as chlorinated, phosphates.

[0061] In certain embodiments, the brominated flame retardant comprises a brominated polyether polyol of the general formula (I):



[0062] in which n is a number of 0 to 7, m is a number of 2 to 3; X is a saturated or unsaturated brominated polyol residue; and R is hydrogen or an alkyl group having 1 to 5 carbon atoms. Specific examples of suitable brominated polyether polyols are commercially available as Ixol® B-251 and Ixol® M-125 from Solvay Fluorides LLC.

[0063] Other suitable brominated flame retardants include, but are not limited to, 3,4,5,6-tetrabromophthalic acid, tribromoneopentyl alcohol, 1,3-propanediol, 2,2-bis(bromomethyl), and pentabromophenyl ether, among others, including mixtures of two or more thereof. Suitable commercially available brominated flame retardants also include those available from ICL Industrial Products as the SaFRon® (6000 Series) brominated flame retardants. Mixtures of two or more of such brominated flame retardants can be used. In certain embodiments, the brominated flame retardant does not contain phosphorous.

[0064] Specific examples of suitable phosphorous compounds, such as halogenated phosphates, include, without limitation, tris-(2-chloroethyl)phosphate, tris-(2-chloroisopropyl)phosphate (TCPP), tris(1,3-dichloroisopropyl)phosphate, tris-(2,3-

dibromopropyl)phosphate and tetrakis-(2-chloroethyl) ethylene diphosphate, Diethyl Bis-(2-hydroxyethyl)-aminomethylphosphonate, phosphoric acid, triethyl ester, polymer with oxirane and phosphorus oxide (P_2O_5), triethyl phosphate, including mixtures of two or more thereof. Isocyanate-reactive and/or non-reactive non-halogenated phosphorous compounds are often used.

[0065] In certain embodiments, the total amount of flame retardant in the foam producing mixture is at least 1% by weight, such as at least 2% by weight and no more than 10% by weight, such as no more than 5% by weight, based on the total weight of the foam producing mixture.

[0066] In certain embodiments, the foam producing mixture includes a surfactant to, for example, stabilize the foaming reaction mixture until it obtains rigidity. Such surfactants may include a liquid or solid organosilicon compound, a polyethylene glycol ether of a long chain alcohol, a tertiary amine, an alkanolamine salt of a long chain alkyl acid sulfate ester, an alkylsulfonic ester, or an alkylarylsulfonic acid, or a mixture thereof. Such surfactants are employed in amounts sufficient to stabilize the foaming reaction mixture against collapse and the formation of large and uneven cells. Often, 0.1 to 10 % by weight of the surfactant is used, based on the total weight of the foam producing mixture.

[0067] In certain embodiments, one or more catalysts are used in the foam producing mixture. Any suitable catalyst may be used including tertiary amines, such as, without limitation, triethylenediamine, N-methylmorpholine, pentamethyl diethylenetriamine, dimethylcyclohexylamine, tetra-methylethylenediamine, 1-methyl-4-dimethylaminoethyl-piperazine, 3-methoxy-N-dimethyl-propylamine, N-ethylmorpholine, diethylethanol-amine, N-cocomorpholine, N,N-dimethyl-N',N'-dimethylisopropyl-propylene diamine, N,N-diethyl-3-diethyl aminopropylamine and dimethyl-benzyl amine. A catalyst for the trimerization of

polyisocyanates, such as an alkali metal alkoxide or carboxylate, or certain tertiary amines, are often employed. Such catalysts are used in an amount which measurably increases the rate of reaction of the polyisocyanate. Typical amounts are 0.1 to 10.0 % by weight, based on the total weight of the foam producing mixture.

[0068] For each identified raw material, the system may identify **402** an associated supplier of the raw material. In various embodiments, the system may access a list of raw materials and associated suppliers of each from one or more data stores associated with or accessible by a host electronic device.

[0069] In various embodiments, the system may receive **404** a communication from one or more of the identified suppliers. For instance, a host electronic device may receive **404** an electronic communication from one or more client electronic devices associated with a supplier. The communication may include quality data corresponding to the raw material that it provides for the product. Quality data may refer to material specifications or lot specific data corresponding to the raw materials. For example, information pertaining to storage conditions of the raw materials, transportation conditions of the raw materials, and/or the like may be included in quality data. For example, information pertaining to transportation conditions of raw materials may include for example, a carrier used to transport the raw materials, a temperature associated with a transportation method (e.g., of a truck, railcar, or other mode of transportation) in which the raw materials were transported, a length of transport, and/or the like.

[0070] In various embodiments, the received communication may include message content and a digital signature. The message content may be quality data corresponding to one or more raw materials that the supplier supplies. The system may use the digital signature to confirm that the communication actually came from the supplier.

[0071] A supplier may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, a supplier may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, a supplier that is sending quality data for a raw material may generate a hashed value corresponding to the quality data by applying one or more hashing algorithms to the quality data. The supplier may encrypt the hashed value with the supplier's private key to generate a digital signature corresponding to the message content.

[0072] The supplier may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **406** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified supplier (or an otherwise authorized supplier). In this way, only authorized suppliers may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content was not altered, modified or otherwise changed after it was sent.

[0073] The system may decrypt the received digital signature using the supplier's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the supplier. If the decryption is not successful, the system may disregard the communication.

[0074] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the supplier to the received message content to

generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[0075] The system may create **408** a log file that includes at least a portion of the received quality data. The system may generate **410** a new block for a blockchain. The system may store the created log file in the new block.

[0076] In various embodiments, if a target blockchain already exists, the system may generate **410** a block to append to the end of the target blockchain. The target blockchain may store information about the product through its lifecycle. For example, the target blockchain may store information about spray foam insulation or a batch of spray foam insulation throughout its lifecycle. In other embodiments, a target blockchain may store information pertaining to a foam producing mixture manufactured by a particular manufacturer. Additional and/or other target blockchains may be used within the scope of this disclosure.

[0077] Referring back to FIG. 4, the system may add **412** the new block to a target blockchain. If the target blockchain already exists, the system may identify the last block of the target blockchain. The last block may be associated with a signature. The signature may be derived or based on a signature of a block that precedes the last block in the target blockchain. The preceding block may immediately precede the last block in the target blockchain, or it may not immediately precede the last block but be separated from the target block by one or more other blocks.

[0078] For instance, the signature of the last block may be a result of one or more cryptographic operations, such as, for example, a hash function, performed on at least a portion

of the contents of a block that precedes the last block in the target blockchain. As such, the blocks of the blockchain may be inextricably linked together, and modification of one block will require modification of the previous blocks in the chain.

[0079] The system may add the new block to the target blockchain by performing one or more cryptographic operations on at least a portion of the content of the last block in the target blockchain to generate a signature. The system may add the signature to the new block and append it the end of the target blockchain. For instance, the system may link the new block to the last block of the target blockchain.

[0080] If a target blockchain does not already exist, the system may generate a first block of a blockchain. If the generated block is also the only block in the target blockchain, then the signature of the block may not be based on a preceding block because there is no preceding block in the chain. In this situation, the signature of the block may be a result of one or more cryptographic operations performed on at least part of the block, such as, for example, a portion of the block's log records.

[0081] In various embodiments, the system may maintain a source log that tracks which blocks are associated with which participant in the lifecycles. For instance, if the system receives quality data from Supplier 1 to add to the target block chain for a raw material, the system may assign a unique identifier to Supplier 1. The system may update a source log to associate one or more generated blocks with the source of the information stored within the block. For instance, the system may assign Supplier 1 the unique identifier "02d3" and may store in the source log an indication of the newly created block associated with Supplier 1. This indication may be the signature of or other unique identifier associated with the newly created block. FIG. 5 illustrates an example of a source log according to an embodiment.

[0082] Referring back to FIG. 4, the system may identify **414** one or more manufacturers of the product. The system may access a list of manufacturers from one or more data stores associated with or accessible by a host electronic device.

[0083] In various embodiments, the system may receive **416** a communication from one or more of the identified manufacturers. For instance, a host electronic device may receive **416** an electronic communication from one or more client electronic devices associated with a manufacturer. The communication may include manufacturing data corresponding to the product. Manufacturing data may include production specifications, storage data, testing results, certifications, storage and/or transportation conditions, and/or the like. For example, transportation conditions associated with a foam producing mixture may include, without limitation, a carrier used to transport the mixture, a temperature associated with a transportation method (e.g., of a truck, railcar, or other mode of transportation) in which the mixture was transported, a length of transport, and/or the like. A manufacturer may provide additional transport-related data.

[0084] Manufacturing data may include information pertaining to one or more conditions under which a product is produced. For a foam producing mixture, manufacturing data may include, without limitation, chemical flow rates and temperatures, pressures, line speed, formulation, product identifier, lot numbers of raw materials and final product, applied foam temperature and temperature profile, presence and size and location of voids, ambient temperature, and ambient humidity.

[0085] Storage data may include information pertaining to one or more conditions under which a product is stored such as, for example, a storage location, a time spend in storage, a storage temperature, a storage humidity, other environmental conditions, and/or the like.

[0086] Testing results may include information pertaining to one or more tests performed on a product including, without limitation, the results of any tests that have been performed. For spray foam insulation, testing results may include, for example, density and tests required by ASTM C-1289 including, without limitation, compressive strength, dimensional stability, and thermal resistance tests.

[0087] In various embodiments, the received communication may include message content and a digital signature. The message content may be manufacturing data, production data, storage data, and/or testing results corresponding to one or more products that the manufacturer produces. The system may use the digital signature to confirm that the communication actually came from the manufacturer.

[0088] A manufacturer may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, a manufacturer may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, a manufacturer that is sending manufacturing data may generate a hashed value corresponding to the data by applying one or more hashing algorithms to the data. The manufacturer may encrypt the hashed value with the manufacturer's private key to generate a digital signature corresponding to the message content.

[0089] The manufacturer may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate **418** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified manufacturer (or an otherwise authorized manufacturer). In this way, only authorized

manufacturers may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content wasn't altered, modified or otherwise changed after it was sent.

[0090] The system may decrypt the received digital signature using the manufacturer's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the manufacturer. If the decryption is not successful, the system may disregard the communication.

[0091] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the manufacturer to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[0092] The system may create **420** a log file that includes at least a portion of the received manufacturing data. The system may generate **422** a new block for the target blockchain. The system may store the created log file in the new block. In various embodiments, the system may add **424** the new block to the target blockchain. For example, the system may add **424** the new block to the target blockchain in a manner similar to that described above.

[0093] The system may update the source log to associate with generated manufacturer block with the manufacturer that provided the corresponding manufacturing data. For instance, the system may assign Manufacturer 1 the unique identifier "u9ra" and may store in the source

log an indication of the newly created block associated with Manufacturer 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[0094] In various embodiments, the system may identify **426** one or more installers of the product. The system may access a list of installers from one or more data stores associated with or accessible by a host electronic device.

[0095] The system may receive **428** a communication from one or more of the identified installers. For instance, a host electronic device may receive **428** an electronic communication from one or more client electronic devices associated with an installer. The communication may include installation data and/or manufacturing associated with the product. For example, in certain situations, an installer may receive raw materials from one or more suppliers and/or manufacturers, and may create a foam producing mixture. As such, an installer may provide one or more communications that include manufacturing data.

[0096] Installation data may include information such as, for example, installation specifications, an installation location, a date of installation, a name of one or more individuals who installed the product, one or more images of the installed product, one or more images of different parts of the installation process showing that installation specifications were followed, weather conditions at the time of installation, type and thickness of installed insulation, installation materials used (e.g., membrane fasteners, glue, etc.), a report or other proof of inspector approval, and/or the like. An image capture device such as, for example, a camera, a video recorder, an infrared imaging device, and/or the like may be used to capture one or more images or videos within the scope of this disclosure.

[0097] In various embodiments, the received communication may include message content and a digital signature. The message content may be installation data. The system may use the digital signature to confirm that the communication actually came from the installer.

[0098] An installer may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, an installer may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, an installer that is sending installation data may generate a hashed value corresponding to the data by applying one or more hashing algorithms to the data. The installer may encrypt the hashed value with the installer's private key to generate a digital signature corresponding to the message content.

[0099] The installer may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified installer (or an otherwise authorized installer). In this way, only authorized installers may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data. Authenticating the received communication may also involve confirming that the message content was not altered, modified or otherwise changed after it was sent.

[00100] The system may decrypt the received digital signature using the installer's public key to yield a decrypted value. The decrypted value may be the received hashed value. If

the decryption is successful, the system will know that the communication originated with the installer. If the decryption is not successful, the system may disregard the communication.

[00101] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the installer to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[00102] In various embodiments, the system may authenticate **430** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified installer (or an otherwise authorized installer). In this way, only authorized installers may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data.

[00103] The system may authenticate **430** a received communication using cryptography. For example, the system may verify that a received communication was sent by a known or authorized installer by confirming that the communication was encrypted using the installer's private key. For example, in response to receiving a communication from an installer, the system may retrieve that installer's public key from the key store. The system may attempt to decrypt the received communication using the retrieved public key. If the retrieved public key is successful in decrypting the communication, the system can be confident that the communication originated from the authorized installer. If the retrieved public key is not successful in decrypting the communication, the system may discard the communication since it was not sent

from the purported installer. Additional and/or alternate authentication protocols may be used within the scope of this disclosure.

[00104] The system may create **432** a log file that includes at least a portion of the received installation data. The system may generate **434** a new block for the target blockchain. The system may store the created log file in the new block. In various embodiments, the system may add **436** the new block to the target blockchain. For example, the system may add **436** the new block to the target blockchain in a manner similar to that described above.

[00105] The system may update the source log to associate with generated installer block with the installer that provided the corresponding installation data. For instance, the system may assign Installer 1 the unique identifier “1x2h” and may store in the source log an indication of the newly created block associated with Installer 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[00106] In various embodiments, at least a portion of the target blockchain may be accessible by one or more of the identified suppliers, the identified manufacturers, and/or the identified installers. For example, as discussed above, one or more of the suppliers, manufacturers, and/or installers may add data to the target blockchain pertaining to the raw materials for spray foam insulation, the manufacture of spray foam insulation, and/or the installation of spray foam insulation. As described in more detail below, one or more suppliers, manufacturers, and/or installers may query or request information that is stored in the target blockchain.

[00107] In various embodiments, the system may identify **438** one or more inspectors of the product. The system may access a list of inspectors from one or more data stores associated with or accessible by a host electronic device.

[00108] The system may receive **440** a communication from one or more of the identified inspectors. For instance, a host electronic device may receive **440** an electronic communication from one or more client electronic devices associated with an inspector. The communication may include inspection data associated with the product. Inspection data may include information such as, for example, inspection specifications, an inspection location, a date of inspection, a name of one or more individuals who inspected the product, one or more images of the inspected product, one or more images of different parts of the inspection process, a report or other proof of inspector approval or comments, and/or the like. An image capture device such as, for example, a camera, a video recorder, an infrared imaging device, and/or the like may be used to capture one or more images or videos within the scope of this disclosure.

[00109] In various embodiments, the received communication may include message content and a digital signature. The message content may be inspection data. The system may use the digital signature to confirm that the communication actually came from the inspector.

[00110] An inspector may generate a digital signature for a communication by performing one or more cryptographic operations on at least a portion of the message content. For example, an inspector may generate a digital signature for a communication by generating, by an electronic device, a hash of at least a portion of the message content to generate a hashed value. For instance, an inspector that is sending inspection data may generate a hashed value corresponding to the data by applying one or more hashing algorithms to the data. The inspector may encrypt the hashed value with the inspector's private key to generate a digital signature corresponding to the message content.

[00111] The inspector may send the communication and corresponding digital signature to the system. In various embodiments, the system may authenticate the received

communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified inspector (or an otherwise authorized inspector). In this way, only authorized inspectors may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data.

Authenticating the received communication may also involve confirming that the message content wasn't altered, modified or otherwise changed after it was sent.

[00112] The system may decrypt the received digital signature using the inspector's public key to yield a decrypted value. The decrypted value may be the received hashed value. If the decryption is successful, the system will know that the communication originated with the inspector. If the decryption is not successful, the system may disregard the communication.

[00113] The system may also verify the integrity of the message content. The system may apply the same hashing algorithm(s) used by the inspector to the received message content to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the message content has not changed since it was sent. If the values do not match, the system may disregard the communication as the message content has been changed after it was sent.

[00114] In various embodiments, the system may authenticate **442** the received communication. Authenticating the communication may involve verifying that the communication originated from an authorized source such as, for example, an identified inspector (or an otherwise authorized inspector). In this way, only authorized inspectors may request that information be added to a target blockchain, and users or those who access the target blockchain can be confident that the target blockchain only includes relevant data.

[00115] The system may authenticate **442** a received communication using cryptography. For example, the system may verify that a received communication was sent by a known or authorized inspector by confirming that the communication was encrypted using the inspector's private key. For example, in response to receiving a communication from an inspector, the system may retrieve that inspector's public key from the key store. The system may attempt to decrypt the received communication using the retrieved public key. If the retrieved public key is successful in decrypting the communication, the system can be confident that the communication originated from the authorized inspector. If the retrieved public key is not successful in decrypting the communication, the system may discard the communication since it was not sent from the purported inspector. Additional and/or alternate authentication protocols may be used within the scope of this disclosure.

[00116] The system may create **444** a log file that includes at least a portion of the received inspection data. The system may generate **446** a new block for the target blockchain. The system may store the created log file in the new block. In various embodiments, the system may add **448** the new block to the target blockchain. For example, the system may add **448** the new block to the target blockchain in a manner similar to that described above.

[00117] The system may update the source log to associate with generated inspection block with the inspector that provided the corresponding inspection data. For instance, the system may assign Inspector 1 the unique identifier "td8h" and may store in the source log an indication of the newly created block associated with Inspector 1. This indication may be the signature of or other unique identifier associated with the newly created block.

[00118] In various embodiments, at least a portion of the target blockchain may be accessible by one or more of the identified suppliers, the identified manufacturers, the identified

installers, and/or the identified inspectors. For example, as discussed above, one or more of the suppliers, manufacturers, installers, and/or inspectors may add data to the target blockchain pertaining to the raw materials for spray foam insulation, the manufacture of spray foam insulation, the installation of spray foam insulation, and/or the inspection of spray foam insulation. As described in more detail below, one or more suppliers, manufacturers, installers, and/or inspectors may query or request information that is stored in the target blockchain.

[00119] One or more host electronic devices may receive one or more access requests. An access request may include a request to access certain information that is stored on the target blockchain. For instance, an access request may be a request to access storage information associated with a particular lot of spray foam insulation. As another example, an access request may be a request to access information about the raw materials used to manufacture a certain lot of spray foam insulation. Additional and/or alternate access requests may be made within the scope of this disclosure.

[00120] An access request may originate from a participant (e.g., a supplier, a manufacturer, an installer, an inspector and/or the like) and/or one or more authorized business partners of one or more participants. However, the system may only grant access to requested information if it is permitted by an access policy associated with the target blockchain. An access policy is a list, table, or other data structure that identifies privileges or permissions that apply to a particular resource or set of resources.

[00121] An access control list (ACL) is an example of an access policy according to an embodiment. A blockchain is another example of an access policy according to an embodiment. For example, one or more permissions and associated requestors may be stored on an access control blockchain. The access control blockchain may be separate from the target blockchain. A

host electronic device may access an access control blockchain in order to determine whether a requestor has the requisite permissions to access the requested resources from the target blockchain. For example, an access control blockchain may include one or more blocks with one or more access rights associated with one or more of the resources and/or one or more authorized users of the target blockchain.

[00122] An access policy may define one or more permissions associated with one or more authorized users of the target blockchain. In various embodiments, the access policy may define one or more permissions based on type of authorized users, for example, suppliers, manufacturers, and installers. Alternatively, an access policy may define one or more permissions to one or more users on a case-by-case basis. Example permissions may include, without limitation, read access, write access, copy permission, download permission, and/or the like.

[00123] A rights management system may restrict access to one or more blockchains and/or information stored by one or more blockchains in accordance with one or more applicable access policies. For example, a rights management system may control who can access what information on a blockchain and for what purposes this information may be accessed or further utilized. For instance, a supplier may access product data of its manufacturer that is stored on the blockchain. However, the supplier may not access product data of a different manufacturer.

[00124] As another example, a manufacturer may access quality data for its supplier(s), but the manufacturer may not have access to quality data for other suppliers. Similarly, an inspector may access manufacturing information of a particular manufacturer, but not others. As another example, an installer may share installation information with a particular inspector but not others. Similarly, an installer may share installation information with a particular

manufacturer, but not others. For instance, an installer may be required to share certain installation information with a manufacturer for the manufacturer to use to verify that its warranty has not been voided by improper installation.

[00125] FIG. 6A illustrates a flow chart of an example method of verifying access requests to a target blockchain according to an embodiment. As illustrated by FIG. 6A, a host electronic device may receive **600** an access request from a requestor. In various embodiments, a requestor may be a supplier, a manufacturer, an installer, an inspector, and/or the like. The access request may include an indicator of one or more resources stored on the blockchain for which access is sought. A resource refers to information pertaining to the supply, manufacturer, installation, inspection, or other processing or use of a product having information that is stored on a target blockchain. A resource may be information itself or one or more log records that includes such information. The resources may be identified based on the source of the access request.

[00126] For example, information associated with a raw material may be stored and/or indexed according to a lot number provided by a supplier for the raw material. Information stored on the blockchain pertaining to the raw material may be stored in association with its lot number. Similarly, information associated with a foam producing mixture and/or spray foam insulation may be stored and/or indexed according to a unique identifier provided by a manufacturer of the foam producing mixture and/or spray foam. Information stored on the blockchain pertaining to the manufactured product may be stored in association with its lot manufacturing number.

[00127] Similarly, information associated with an installed product (e.g., applied spray foam insulation) may be stored and/or indexed according to installation details. The installation details may include a date of installation, a time of installation and/or a location of installation.

[00128] The host electronic device may identify **602** one or more blocks of the target blockchain that include at least a portion of the resources. For example, if a manufacturer would like to know if the characteristics of a lot of raw materials affected the compressive strength of the product (e.g., if a recent lot was defective) made by the manufacturer, the manufacturer may query the blockchain for all manufacturing lots generated using at least a portion of the raw material lot.

[00129] The host electronic device may identify **604** the access policy that corresponds to the target blockchain, and may determine **606**, based on the access policy whether the requestor is permitted to access the requested resources. For instance, the host electronic device may search the access policy for the requestor's identity, and may obtain the permissions granted to the requestor. If the request being made by the requestor is permitted by the policy, the host electronic device may grant **608** access to the requested resources to the requestor. Otherwise, the host electronic device may deny **610** access.

[00130] As an example, Supplier A may make an access request to obtain quality data associated with a lot of raw materials that it provided to a manufacturer and that is stored on a target blockchain. The access policy for the target blockchain may indicate that Supplier A is permitted to access its own information (e.g., information that it provided to the target blockchain), and therefore may grant access to the requesting supplier. However, if Supplier A attempts to access quality data associated with raw materials provided to the manufacturer by Supplier B, the system may deny the request.

[00131] In various embodiments, the system may determine a unique identifier associated with a requestor. If the unique identifier of the requestor does not match a unique identifier associated with the creator of block for which access is being sought (as specified, for example, by the source log), the system may deny the request. If the unique identifier of the requestor matches a unique identifier associated with the creator of the block for which access is being sought, the system may grant the request.

[00132] The types of queries of a target blockchain that may be made may vary based on the user or type of user requesting the query. For example, a supplier of a raw material may submit a query to a host electronic device for access to a specification report for one or more raw materials of the supplier used to make a certain product or batch of product. As another example, a manufacturer of product may query for raw material specifications, raw material transportation conditions, quality reports associated with raw materials, storage conditions of foam producing mixtures, and/or the like. As yet another example of querying, an installer of product may query regarding storage conditions of the product, installation conditions, and/or the like.

[00133] FIGS. 6B and 6C show a visual depiction of example access requests according to various embodiments. As shown in FIG. 6B, blockchain **612** includes two supplier blocks **614**, **616**, two manufacturer blocks **618**, **620**, and two installation blocks **622**, **624**. It is understood that different numbers of one or more such blocks may be used within the scope of this disclosure. In this example, Supplier A has posted quality data pertaining to Lot A of raw materials to the blockchain. As such, the system may grant a request by Supplier A to access this quality data because the access rights may permit Supplier A to access information that it has supplied to the blockchain **612**.

[00134] In this example, Supplier B has posted quality data pertaining to Lot B of raw materials to the blockchain **612**. As such, the system may deny a request by Supplier A to access this quality data because the access rights may prohibit any supplier other than Supplier B from accessing this information.

[00135] FIG. 6C illustrates an example where Supplier A and Supplier B have supplied raw materials for product that is being manufactured by Manufacturer C as part of M Lot 1 and M Lot 2. The system may grant a request from Manufacturer C to access quality information pertaining to Lot A and/or Lot B of the raw materials. The system may also grant a request from Manufacturer C to access manufacturing data pertaining to M Lot 1 and/or M Lot 2. However, if Manufacturer D, who is not involved in the manufacture of M Lot 2, tries to access information pertaining to the product of this lot, the system may deny the request. Similarly, the system may deny Manufacturer D access to information pertaining to supplier blocks that are not associated with the manufacture of Manufacturer D's products.

[00136] It is understood that additional and/or alternate access examples, access rights, participants, and/or the like may be used within the scope of this disclosure.

[00137] In various embodiments, an authorized blockchain participant may delegate one or more of its access rights to the blockchain to one or more business partners. A business partner refers to an entity, organization, or individual with whom a participant has a business or other relationship. Examples of business partners include, without limitation, customers, clients, partners, manufacturers, installers, inspectors, suppliers, distributors, vendors, agents, affiliates, subsidiaries, contractors, and/or the like.

[00138] For example, an authorized supplier may delegate one or more of its blockchain access rights to one or more of its customers. Similarly, an authorized manufacturer may

delegate one or more of its blockchain access rights to one or more of its customers, installers, distributors, agents, and/or other partners.

[00139] FIG. 7 illustrates an example delegation process according to an embodiment. As illustrated by FIG. 7, the system may generate **700** a token for one or more authorized participants. For example, when an authorized user registers with, enrolls with, and/or accesses the system, the system may generate **700** one or more tokens for the user. A token refers to an object that includes an identifier associated with the user and one or more blockchain access rights granted to that user. In various embodiments, a token may include an indication of the information or resources on a blockchain to which one or more of the access rights apply or correspond. For instance, a participant may have a first set of access rights to a first set of information that is on a blockchain, but a second set of access rights to a second set of information that is stored on the blockchain. A token that is generated for the participant may include a listing of such access rights and information or resources to which each of the access rights apply. Alternatively, the system may generate **700** multiple tokens for a participant, each token corresponding to particular information from the blockchain and one or more applicable access rights.

[00140] For example, FIGS. 9A and 9B illustrate two sets of quality data that a supplier may store on a blockchain. The system may generate a token **902** that corresponds to both sets of quality data (or at least a portion of both sets) as illustrated in FIG. 9A. As illustrated in FIG. 9A, the token may identify a particular subset of the quality data and one or more access rights associated with the subset. In various embodiments, one or more access rights may apply to the quality data as a whole rather than on a subset-by-subset basis.

[00141] In other embodiments, the system may generate multiple tokens **904a**, **904b** as illustrated in FIG. 9B. As shown in FIG. 9B, one token **904a** corresponds to the access rights associated with one set of information (Quality Data 1), while another token **904b** corresponds to access rights associated with another set of information (Quality Data 2). It is understood that additional and/or alternate tokens, information, access rights and/or the like may be used within the scope of this disclosure.

[00142] The access rights and information to which they correspond may be determined based on those reflected in one or more access policies associated with the blockchain, as described above. In various embodiments, the access rights may include an indication as to whether a user may delegate one or more access rights may be delegated. The indication may also indicate which access the rights the user may delegate, which information stored on the blockchain such rights may be delegated, how many tiers of delegation are permitted, and/or the like. For example, FIG. 7 illustrates a single tier of delegation (from a participant to one or more business partners). But, in certain embodiments, a participant may be able to delegate one or more rights through multiple tiers of business partners. FIG. 8 illustrates an illustration of an example multiple-tier delegation process according to an embodiment. As illustrated in FIG. 8, a system **800** may issue a token to a participant **802**. The participant **802** may delegate one or more of its access rights to access certain information Business Partner 1 **804** and Business Partner 2 **806**. For example, as illustrated in FIG. 8, participant **802** may delegate access rights A and B to Info A Business Partner 1 **804**, and access rights C and D to Info A Business Partner 2 **806**. It is understood that additional or alternate right delegations or combinations of delegations may be made within the scope of this disclosure. As illustrated in FIG. 8, this may be considered a single tier of delegation.

[00143] Business Partner 1 **804** in turn may delegate at least a portion of its access rights for Info A to Business Partner 3 **808**, while Business Partner 2 **806** may delegate at least a portion of its access rights for Info A to Business Partner 4 **810** and Business Partner 5 **812**. As illustrated in FIG. 8, this may be considered a second tier of delegation. Although FIG. 8 illustrates two delegation tiers, it is understood that additional or fewer tiers of delegation may be used within the scope of this disclosure.

[00144] Referring back to FIG. 7, the system may send **702** the generated token to the authorized participant. The authorized participant may receive the token and store **704** the token. In some embodiments, the participant may send the token as part of a communication to the system. For example, a participant may send its token to the system along with an access request. In some embodiments, the system may determine what access rights the participant has based on the received token. In other embodiments, the system may confirm that the access rights denoted in the received token align with the access rights maintained by the system (e.g., those of one or more access policies).

[00145] A participant may generate **706** a digital signature for a token by generating, by an electronic device, a hash of at least a portion of the token to generate a hashed value. The participant may encrypt the hashed value with the participant's private key to generate a digital signature corresponding to the message content.

[00146] A participant may delegate one or more of its access rights to a business partner by providing **708** the business partner with a delegated token and the digital signature corresponding to the delegated token. The delegated token may be the participant's token (or a portion thereof), a reference to the participant's token, a new token based on the participant's

token, and/or the like. A participant may only delegate the access rights that it has for certain information. In this way, a participant cannot grant more rights to a delegate that it itself has.

[00147] For example, a supplier may have read access for a first set of quality data that includes storage conditions and transportation of a raw material it provides for spray foam insulation. The supplier may have read and modify access for a second set of quality data that includes quantity and volume information associated with a raw material that it provides for the spray foam insulation. The supplier may delegate its read access to the first set of quality data and/or its read/modify access to the second set of quality data to one of its manufacturers. However, the supplier may not delegate modify access to the second set of quality data to the manufacturer because the supplier does not have this right. The delegated token may include an indication of the participant who delegated one or more access rights, and an indication of the one or more delegated access rights.

[00148] The participant may send the token and corresponding digital signature to a business partner. When the business partner makes an access request **710** to the system, it may include the delegated token and the received digital signature with the request. The system may attempt to decrypt **712** the received digital signature using the participant's public key to yield a received hashed value. If the decryption is successful, the system will know that the token provided by the business partner was issued by the participant. If the decryption is not successful, the system may disregard the communication.

[00149] The system may also verify **714** the integrity of the token. The system may apply the same hashing algorithm(s) used by the participant to generate a hashed value. The system may compare the hashed value it generated to the received hashed value. If the two values are the same, the system has verified that the token has not changed since it was sent. If

the values do not match, the system may disregard the communication as the token has been changed after it was sent.

[00150] The system may determine **716** whether the delegating participant has the right to delegate the access rights to the information being requested. For instance, the system may identify the delegating participant from the received token, and may confirm its delegation rights with one or more of the system access policies. If the system determines that the delegating participant does not have the necessary delegation rights for the information being requested, the system may deny the access request.

[00151] Referring back to FIG. 4, in various embodiments, the system may perform **450** one or more verification checks on of the target blockchain. The system may perform **450** one or more verification checks in response to one or more triggering events. A triggering event refers to an action performed on the target blockchain or a request made to the target blockchain. For example, if a request for a particular type of information is made to the target blockchain, the system may perform a verification check to determine whether the requested information is consistent with other information logged at the target blockchain. Additional and/or alternate triggering events may be used within the scope of this disclosure.

[00152] In other embodiments, the system may perform **450** one or more verification checks at one or more regular intervals, or in response to a user requesting a verification check.

[00153] For example, in response to receiving installation data for spray foam insulation, the system may perform **450** a verification check to determine whether the received installation data is consistent with the production data. For instance, whether the production specification for the spray foam insulation is consistent with the installation specifications. For example, the production specification may be compared to the installation specifications to determine whether

the proper insulation type and thickness was installed. Additional and/or alternate types of comparisons may be performed within the scope of this disclosure.

[00154] In response to the verification check failing, the system may perform **452** one or more remedial actions. For example, in the above example, the system may automatically send one or more notifications if an inconsistency between the production specifications and the installation specifications is detected. The notification may be an email or other electronic notification, and the system may send it to one or more applicable parties such as, for example, the manufacturer of the spray foam insulation at issue, the installer of the spray foam insulation at issue, and/or the like.

[00155] Alternative remedial actions may include opening a case that includes a root cause analysis, making corrective action assignments, and/or identifying one or more proposed preventive measures. In various embodiments, one or more participants of the system may be able to contribute to identifying the root cause and/or proposed one or more corrective or remedial actions.

[00156] As another example of a verification check, the system may identify building code information associated with a location where product is to be installed. In various embodiments, building code information may be published to the blockchain. For instance, building information may be published to the same block as other installation information pertaining to a particular product. In various embodiments, building code information may be provided by an installer or a building inspector. In other embodiments, building code information may be retrieved from a data store (e.g., a third party data store accessible by the system) that includes building classifications and/or other relevant building code information.

[00157] The system may determine whether the installation data provided by the installer of the product is consistent with the building code information, such as, for example, appropriate R-value of insulation and that the insulation was used in a system that meets building code. In response to the installation data not being consistent with the building code information, the system may determine that the verification check has failed, and take one or more remedial actions. For example, the system may automatically generate a notification of the inconsistency, and send the notification to one or more applicable parties such as, for example, the installer.

[00158] FIG. 10 depicts a block diagram of hardware that may be used to contain or implement program instructions, such as those of a cloud-based server, electronic device, virtual machine, or container. A bus **1000** serves as an information highway interconnecting the other illustrated components of the hardware. The bus may be a physical connection between elements of the system, or a wired or wireless communication system via which various elements of the system share data. Processor **1005** is a processing device that performs calculations and logic operations required to execute a program. Processor **1005**, alone or in conjunction with one or more of the other elements disclosed in FIG. 10, is an example of a processing device, computing device or processor as such terms are used within this disclosure. The processing device may be a physical processing device, a virtual device contained within another processing device, or a container included within a processing device.

[00159] A memory device **1020** is a hardware element or segment of a hardware element on which programming instructions, data, or both may be stored. Read only memory (ROM) and random access memory (RAM) constitute examples of memory devices, along with cloud storage services.

[00160] An optional display interface **1030** may permit information to be displayed on the display **1035** in audio, visual, graphic or alphanumeric format. Communication with external devices, such as a computing device, may occur using various communication devices **1040**, such as a communication port or antenna. A communication device **1040** may be communicatively connected to a communication network, such as the Internet or an intranet.

[00161] The hardware may also include a user input interface **1045** which allows for receipt of data from input devices such as a keyboard or keypad **1050**, or other input device **1055** such as a mouse, a touch pad, a touch screen, a remote control, a pointing device, a video input device and/or a microphone. Data also may be received from an image capturing device **1010** such as a digital camera or video camera. A positional sensor **1015** and/or motion sensor **1065** may be included to detect position and movement of the device. Examples of motion sensors **1065** include gyroscopes or accelerometers. An example of a positional sensor **1015** is a global positioning system (GPS) sensor device that receives positional data from an external GPS network.

[00162] Various embodiments may include a computer-readable medium containing programming instructions that are configured to cause one or more processors to perform the functions described in the context of the previous figures.

[00163] The features and functions described above, as well as alternatives, may be combined into many other different systems or applications. Various alternatives, modifications, variations or improvements may be made by those skilled in the art, each of which is also intended to be encompassed by the disclosed embodiments.

CLAIMS

What Is Claimed Is:

1. A method of securing data associated with a product, the method comprising:
by an electronic device:
 identifying a plurality of raw materials needed to produce the product, wherein
 one or more suppliers supply at least a portion of the plurality of raw materials to one or
 more installers of the product,
 for each identified raw material, identifying an associated supplier of the
 identified raw material,
 for each identified supplier:
 receiving, from the identified supplier, a communication comprising
 quality data corresponding to its associated raw material,
 generating a supplier block that is associated with the identified supplier,
 storing at least a portion of the quality data in the supplier block of the
 identified supplier,
 adding the supplier block to a blockchain, and
 identifying one or more installers of the product, and
 for each identified installer:
 receiving, from the identified installer, a communication comprising
 installation data associated with the product,

generating an installation block that is associated with the identified installer,

storing at least a portion of the installation data in the installation block of the identified installer, and

adding the installation block to the blockchain,

wherein at least a portion of the blockchain is accessible by one or more of the identified suppliers and/or one or more of the identified installers according to an access policy associated with the blockchain, wherein the access policy includes an access control list that defines one or more access rights to the blockchain.

2. The method of claim 1, further comprising performing one or more of the following:
authenticating the communication from the identified supplier before adding the supplier block to the blockchain; or

authenticating the communication from the identified installer before adding the installation block to the blockchain.

3. The method of claim 2, wherein authenticating the communication from the identified supplier comprises:

receiving a digital signature in connection with the communication from the identified supplier;

retrieving a public key associated with the identified supplier from a key store; and
using the public key to decrypt the digital signature to yield a decrypted value.

4. The method of claim 3, further comprising:

applying a hashing algorithm to the communication from the identified supplier to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the supplier block to the blockchain.

5. The method of claim 2, wherein authenticating the communication from the identified installer comprises:

receiving a digital signature in connection with the communication from the identified installer;

retrieving a public key associated with the identified installer from a key store; and

using the public key to decrypt the digital signature to yield a decrypted value.

6. The method of claim 5, further comprising:

applying a hashing algorithm to the communication from the identified installer to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the installer block to the blockchain.

7. The method of claim 1, further comprising:

identifying one or more inspectors of the product; and

for each identified inspector:

receiving, from the identified inspector, a communication comprising inspection data associated with the product,

generating an inspection block that is associated with the identified inspection,

storing at least a portion of the inspection data in the inspection block of the identified inspector,

adding the inspection block to the blockchain, and

wherein at least a portion of the blockchain is accessible by the identified inspectors according to the one or more access rights.

8. The method of claim 7, further comprising:

for a first identified inspector from the one or more identified inspector, generating a token for the first identified inspector, wherein the token comprises:

an identifier associated with the first identified inspector,

one or more of the one or more access rights that correspond to the first identified inspector, and

for each of the access rights that correspond to the first identified inspector, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and

sending the token to the first identified inspector.

9. The method of claim 8, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified inspector the first identified inspector can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

10. The method of claim 8, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

11. The method of claim 8, further comprising:

by an electronic device associated with the first identified inspector:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights that correspond to the first identified inspector, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

12. The method of claim 11, further comprising:

by the electronic device associated with the first identified inspector:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the first identified inspector.

13. The method of claim 12, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the first identified inspector.

14. The method of claim 1, further comprising:

receiving an access request from a first identified supplier, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the first identified supplier is permitted to access the one or more resources; and

in response to determining that the first identified supplier is permitted to access the one or more resources, providing access to the one or more resources to the first identified supplier.

15. The method of claim 14, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

16. The method of claim 14, wherein:

the one or more resources correspond to the first identified supplier,
determining whether the first identified supplier is permitted to access the one or more resources comprises determining that the first identified supplier is permitted to access the one or more resources.

17. The method of claim 14, wherein:

the one or more resources correspond to one or more other suppliers,
determining whether the first identified supplier is permitted to access the one or more resources comprises determining that the first identified supplier is not permitted to access the one or more resources.

18. The method of claim 1, further comprising:

receiving an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources; and

determining, based on the access policy, whether the first identified installer is permitted to access the one or more resources;

in response to determining that the first identified installer is permitted to access the one or more resources, providing access to the one or more resources to the first identified installer.

19. The method of claim 18, further comprising accessing a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

20. The method of claim 1, wherein the production data comprises one or more images of the product after it is produced, wherein the one or more images are captured by an infrared imaging device.

21. The method of claim 1, further comprising:

accessing building code information associated with a location where the product is to be installed;

determining whether the installation data is consistent with the building code information by comparing at least a portion of the installation data to at least a portion of the building code information;

in response to the determining that the installation data is not consistent with the installation specification:

automatically generating a notification of the inconsistency, and

sending the notification to one or more of the identified installers.

22. The method of claim 1, further comprising:

for a first identified supplier from the one or more identified suppliers, generating a token for the first identified supplier, wherein the token comprises:

an identifier associated with the first identified supplier,
one or more of the one or more access rights that correspond to the first identified supplier, and

for each of the one or more access rights that correspond to the first identified supplier, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
sending the token to the first identified supplier.

23. The method of claim 22, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified supplier the first identified supplier can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

24. The method of claim 23, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

25. The method of claim 22, further comprising:

by an electronic device associated with the first identified supplier:
generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights corresponding to the first identified supplier, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

26. The method of claim 25, further comprising:

by the electronic device associated with the first identified supplier:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the first identified supplier.

27. The method of claim 26, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the first identified supplier.

28. The method of claim 1, further comprising:

for a first identified installer from the one or more identified installers, generating a token for the first identified installer, wherein the token comprises:

an identifier associated with the first identified installer,
one or more of the one or more access rights that correspond to the first identified installer, and
for each of the one or more access rights that correspond to the first identified installer, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
sending the token to the first identified installer.

29. The method of claim 28, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified installer the first identified installer can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

30. The method of claim 29, wherein the token further comprises an indication of how many tiers of delegation the first identified installer is permitted to make.

31. The method of claim 28, further comprising:

by an electronic device associated with the first identified installer:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

32. The method of claim 31, further comprising:

by the electronic device associated with the first identified installer:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the first identified installer.

33. The method of claim 32, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the first identified installer.

34. The method of claim 1, further comprising:

receiving an access request from a business partner, wherein the access request comprises:

a token,

a digital signature corresponding to the token, and

an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determining whether the participant is an identified supplier or an identified installer, in response to determining that the participant is an identified supplier or an identified installer, retrieving a public key associated with the participant from a key store,

decrypting the digital signature using the retrieved public key to generate a decrypted value.

35. The method of claim 34, further comprising:

applying a hashing algorithm to the token to generate a hashed value;

determining whether the decrypted value matches the hashed value.

36. The method of claim 34, further comprising:

identifying one or more of the one or more access rights that are associated with the participant;

determining whether the access rights associated with the participant permit the participant to access the one or more resources stored on the blockchain for which access is sought; and

in response to determining that the access rights associated with the participant permit the participant access, granting access to the one or more resources to the business partner.

37. The method of claim 34, further comprising:

identifying one or more of the one or more access rights that are associated with the participant; and

determining whether the one or more access rights associated with the participant permits the participant to delegate access rights.

38. The method of claim 34, wherein the participant is one of the identified suppliers, wherein the business partner is a customer of the identified supplier.

39. The method of claim 1, further comprising:

receiving an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the first identified installer is permitted to access the one or more resources; and

in response to determining that the first identified installer is permitted to access the one or more resources, providing access to the one or more resources to the first identified installer.

40. The method of claim 1, further comprising:

identifying one or more manufacturers of the product,

for each identified manufacturer:

receiving, from the identified manufacturer, a communication comprising manufacturing data associated with the product, wherein the manufacturing data comprises one or more of the following:

production data,

storage data, or

testing results,

generating a manufacturer block that is associated with the identified manufacturer,

storing at least a portion of the manufacturing data in the manufacturer block of the identified manufacturer, and

adding the manufacturer block to the blockchain,

wherein at least a portion of the blockchain is accessible by one or more of the identified manufacturers according to the access policy.

41. The method of claim 40, wherein the quality data comprises information pertaining to one or more transportation conditions of the associated raw material during transportation from the supplier to a manufacturer.

42. The method of claim 40, wherein the manufacturing data comprises information pertaining to one or more transportation conditions of the product or one or more components of the product during transportation from the manufacturer to the installer.

43. The method of claim 40, further comprising authenticating the communication from the identified manufacturer before adding the manufacturer block to the blockchain.

44. The method of claim 43, wherein authenticating the communication from the identified manufacturer comprises:

receiving a digital signature in connection with the communication from the identified manufacturer;

retrieving a public key associated with the identified manufacturer from a key store; and
using the public key to decrypt the digital signature to yield a decrypted value.

45. The method of claim 44, further comprising:

applying a hashing algorithm to the communication from the identified manufacturer to yield a hashed value;

determining whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, adding the manufacturer block to the blockchain.

46. The method of claim 40, further comprising:

receiving an access request from a first identified manufacturer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determining one or more blocks of the blockchain that include at least a portion of the resources;

determining, based on the access policy, whether the first identified manufacturer is permitted to access the one or more resources; and

in response to determining that the first identified manufacturer is permitted to access the one or more resources, providing access to the one or more resources to the first identified manufacturer.

47. The method of claim 46, wherein:

the one or more resources correspond to a second manufacturer,

determining whether the first identified manufacturer is permitted to access the one or more resources comprises determining that the first manufacturer is not permitted to access the one or more resources.

48. The method of claim 46, wherein:

the one or more resources correspond to one or more suppliers who provided raw materials to the first identified manufacturer;

determining whether the first identified manufacturer is permitted to access the one or more resources comprises determining that the first manufacturer is permitted to access the one or more resources.

49. The method of claim 45, wherein:

the one or more resources correspond to one or more suppliers who did not provided raw materials to the first identified manufacturer;

determining whether the first identified manufacturer is permitted to access the one or more resources comprises determining that the first manufacturer is not permitted to access the one or more resources.

50. The method of claim 40, wherein:

the manufacturing data comprises one or more production specifications associated with the product that is produced,

the installation data comprises one or more installation specifications associated with the product that is installed,

the method further comprises determining whether the production specifications are consistent with the installation specifications by comparing at least a portion of the production specification to at least a portion of the installation specifications,

in response to determining that the production specifications are not consistent with the installation specifications:

automatically generating a notification of the inconsistency, and

sending the notification to one or more of the identified manufacturers or the identified installers.

51. The method of claim 40, further comprising:

for a first identified manufacturer from the one or more identified manufacturers, generating a token for the first identified manufacturer, wherein the token comprises:

an identifier associated with the first identified manufacturer,
one or more of the one or more access rights that correspond to the first identified manufacturer, and
for each of the one or more access rights corresponding to the first identified manufacturer, an indication of a subset of information that is stored on the blockchain to which the corresponding access right corresponds; and
sending the token to the first identified manufacturer.

52. The method of claim 51, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified manufacturer the first identified manufacturer can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

53. The method of claim 52, wherein the token further comprises an indication of how many tiers of delegation the first identified manufacturer is permitted to make.

54. The method of claim 51, further comprising:

by an electronic device associated with the first identified manufacturer:

generating a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the corresponding access rights,
and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

55. The method of claim 54, further comprising:

by the electronic device associated with the first identified manufacturer:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the first identified manufacturer.

56. The method of claim 55, wherein generating a digital signature associated with the delegated token comprises:

applying a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypting the hashed value with a private key associated with the first identified manufacturer.

57. The method of claim 40, further comprising:

receiving an access request from a business partner, wherein the access request comprises:

a token,

a digital signature corresponding to the token, and

an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determining whether the participant is an identified manufacturer,

in response to determining that the participant is an identified manufacturer, retrieving a public key associated with the participant from a key store,

decrypting the digital signature using the retrieved public key to generate a decrypted value.

58. The method of claim 57, wherein the participant is of the identified manufacturers, wherein the business partner is a customer of the identified manufacturer.

59. The method of claim 1, wherein the product comprises spray foam insulation.

60. A computer program comprising one or more programming instructions that, when executed by an electronic device, causes the electronic device to perform a method of securing data associated with a product, the method comprising:

identifying a plurality of raw materials needed to produce the product, wherein one or more suppliers supply at least a portion of the plurality of raw materials to one or more installers of the product;

for each identified raw material, identifying an associated supplier of the identified raw material;

for each identified supplier:

receiving, from the identified supplier, a communication comprising quality data corresponding to its associated raw material,

generating a supplier block that is associated with the identified supplier,

storing at least a portion of the quality data in the supplier block of the identified supplier,

adding the supplier block to a blockchain, and

identifying one or more installers of the product, and

for each identified installer:

receiving, from the identified installer, a communication comprising installation data associated with the product,

generating an installation block that is associated with the identified installer,

storing at least a portion of the installation data in the installation block of the identified installer, and

adding the installation block to the blockchain,

wherein at least a portion of the blockchain is accessible by one or more of the identified suppliers and/or one or more of the identified installers according to an access policy associated with the blockchain, wherein the access policy includes an access control list that defines one or more access rights to the blockchain.

61. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to perform one or more of the following:

authenticate the communication from the identified supplier before adding the supplier block to the blockchain;

authenticate the communication from the identified manufacturer before adding the manufacturer block to the blockchain; or

authenticate the communication from the identified installer before adding the installation block to the blockchain.

62. The computer program of claim 61, wherein the one or more programming instructions that, when executed by the electronic device, causes the electronic device to authenticate the communication from the identified supplier comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive a digital signature in connection with the communication from the identified supplier;

retrieve a public key associated with the identified supplier from a key store; and

use the public key to decrypt the digital signature to yield a decrypted value.

63. The computer program of claim 62, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

apply a hashing algorithm to the communication from the identified supplier to yield a hashed value;

determine whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, add the supplier block to the blockchain.

64. The computer program of claim 61, wherein the one or more programming instructions that, when executed by the electronic device, cause the electronic device to authenticate the communication from the identified installer comprise one or more programming instructions that, when executed by the electronic device, cause the electronic device to:

receive a digital signature in connection with the communication from the identified installer;

retrieve a public key associated with the identified installer from a key store; and
use the public key to decrypt the digital signature to yield a decrypted value.

65. The computer program of claim 64, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

apply a hashing algorithm to the communication from the identified installer to yield a hashed value;

determine whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, add the installer block to the blockchain.

66. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

identify one or more inspectors of the product; and

for each identified inspector:

receive, from the identified inspector, a communication comprising inspection data associated with the product,

generate an inspection block that is associated with the identified inspection,

store at least a portion of the inspection data in the inspection block of the identified inspector,

add the inspection block to the blockchain, and

wherein at least a portion of the blockchain is accessible by the identified inspectors according to the one or more access rights.

67. The computer program of claim 66, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

for a first identified inspector from the one or more identified inspector, generate a token for the first identified inspector, wherein the token comprises:

an identifier associated with the first identified inspector,

one or more of the one or more access rights that correspond to the first identified inspector, and

for each of the access rights that correspond to the first identified inspector, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and

send the token to the first identified inspector.

68. The computer program of claim 67, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified inspector the first identified inspector can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

69. The computer program of claim 67, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

70. The computer program of claim 67, further comprising one or more programming instructions that, when executed by a second electronic device, causes the second electronic device to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights that correspond to the first identified inspector, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

71. The computer program of claim 70, further comprising one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

generating a digital signature associated with the delegated token, and

sending the delegated token and the digital signature to the first identified inspector.

72. The computer program of claim 70, wherein the one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypt the hashed value with a private key associated with the first identified inspector.

73. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive an access request from a first identified supplier, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determine one or more blocks of the blockchain that include at least a portion of the resources;

determine, based on the access policy, whether the first identified supplier is permitted to access the one or more resources; and

in response to determining that the first identified supplier is permitted to access the one or more resources, provide access to the one or more resources to the first identified supplier.

74. The computer program of claim 73, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

75. The computer program of claim 73, wherein:
the one or more resources correspond to the first identified supplier,
the one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine whether the first identified supplier is permitted to access the one or more resources comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine that the first identified supplier is permitted to access the one or more resources.

76. The computer program of claim 73, wherein:
the one or more resources correspond to one or more other suppliers,
the one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine whether the first identified supplier is permitted to access the one or more resources comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine that the first identified supplier is not permitted to access the one or more resources.

77. The computer program of claim 76, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

78. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determine one or more blocks of the blockchain that include at least a portion of the resources; and

determine, based on the access policy, whether the first identified installer is permitted to access the one or more resources;

in response to determining that the first identified installer is permitted to access the one or more resources, provide access to the one or more resources to the first identified installer.

79. The computer program of claim 78, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

80. The computer program of claim 60, wherein the production data comprises one or more images of the product after it is produced, wherein the one or more images are captured by an infrared imaging device.

81. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

- access building code information associated with a location where the product is to be installed;

- determine whether the installation data is consistent with the building code information by comparing at least a portion of the installation data to at least a portion of the building code information;

- in response to the determining that the installation data is not consistent with the installation specification:

- automatically generate a notification of the inconsistency, and

- send the notification to one or more of the identified installers.

82. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

- for a first identified supplier from the one or more identified suppliers, generate a token for the first identified supplier, wherein the token comprises:

- an identifier associated with the first identified supplier,

one or more of the one or more access rights that correspond to the first identified supplier, and

for each of the one or more access rights that correspond to the first identified supplier, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
send the token to the first identified supplier.

83. The computer program of claim 82, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified supplier the first identified supplier can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

84. The computer program of claim 83, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

85. The computer program of claim 82, further comprising one or more programming instructions that, when executed by a second electronic device associated with the first identified supplier, causes the second electronic device to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights corresponding to the first identified supplier, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

86. The computer program of claim 85, further comprising the one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

generate a digital signature associated with the delegated token, and
send the delegated token and the digital signature to the first identified supplier.

87. The computer program of claim 86, wherein the one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypt the hashed value with a private key associated with the first identified supplier.

88. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

for a first identified installer from the one or more identified installers, generate a token for the first identified installer, wherein the token comprises:

an identifier associated with the first identified installer,
one or more of the one or more access rights that correspond to the first identified installer, and
for each of the one or more access rights that correspond to the first identified installer, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
send the token to the first identified installer.

89. The computer program of claim 88, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified installer the first identified installer can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

90. The computer program of claim 89, wherein the token further comprises an indication of how many tiers of delegation the first identified installer is permitted to make.

91. The computer program of claim 88, further comprising one or more programming instructions that, when executed by a second electronic device associated with the first identified installer, causes the second electronic device to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

92. The computer program of claim 91, further comprising one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

generate a digital signature associated with the delegated token, and
send the delegated token and the digital signature to the first identified installer.

93. The computer program of claim 92, wherein the one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypt the hashed value with a private key associated with the first identified installer.

94. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive an access request from a business partner, wherein the access request comprises:
a token,

a digital signature corresponding to the token, and

an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determine whether the participant is an identified supplier or an identified installer,

in response to determining that the participant is an identified supplier or an identified installer, retrieve a public key associated with the participant from a key store,

decrypt the digital signature using the retrieved public key to generate a decrypted value.

95. The computer program of claim 94, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

apply a hashing algorithm to the token to generate a hashed value;

determine whether the decrypted value matches the hashed value.

96. The computer program of claim 94, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

identify one or more of the one or more access rights that are associated with the participant;

determine whether the access rights associated with the participant permit the participant to access the one or more resources stored on the blockchain for which access is sought; and

in response to determining that the access rights associated with the participant permit the participant access, grant access to the one or more resources to the business partner.

97. The computer program of claim 94, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

identify one or more of the one or more access rights that are associated with the participant; and

determine whether the one or more access rights associated with the participant permits the participant to delegate access rights.

98. The computer program of claim 94, wherein the participant is one of the identified suppliers, wherein the business partner is a customer of the identified supplier.

99. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determine one or more blocks of the blockchain that include at least a portion of the resources;

determine, based on the access policy, whether the first identified installer is permitted to access the one or more resources; and

in response to determining that the first identified installer is permitted to access the one or more resources, provide access to the one or more resources to the first identified installer.

100. The computer program of claim 60, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

identify one or more manufacturers of the product,

for each identified manufacturer:

receive, from the identified manufacturer, a communication comprising manufacturing data associated with the product, wherein the manufacturing data comprises one or more of the following:

production data,

storage data, or

testing results,

generate a manufacturer block that is associated with the identified manufacturer, store at least a portion of the manufacturing data in the manufacturer block of the identified manufacturer, and

add the manufacturer block to the blockchain,

wherein at least a portion of the blockchain is accessible by one or more of the identified manufacturers according to the access policy associated with the blockchain.

101. The computer program of claim 100, wherein the quality data comprises information pertaining to one or more transportation conditions of the associated raw material during transportation from the supplier to a manufacturer.

102. The computer program of claim 100, wherein the manufacturing data comprises information pertaining to one or more transportation conditions of the product during transportation from the manufacturer to the installer.

103. The computer program of claim 100, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to authenticate the communication from the identified manufacturer before adding the manufacturer block to the blockchain.

104. The computer program of claim 103, wherein the one or more programming instructions that, when executed by the electronic device, cause the electronic device to authenticate the communication from the identified manufacturer comprise one or more programming instructions that, when executed by the electronic device, cause the electronic device to:

- receive a digital signature in connection with the communication from the identified manufacturer;

- retrieve a public key associated with the identified manufacturer from a key store; and
- use the public key to decrypt the digital signature to yield a decrypted value.

105. The computer program of claim 104, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

- apply a hashing algorithm to the communication from the identified manufacturer to yield a hashed value;

determine whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, add the manufacturer block to the blockchain.

106. The computer program of claim 100, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive an access request from a first identified manufacturer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determine one or more blocks of the blockchain that include at least a portion of the resources;

determine, based on the access policy, whether the first identified manufacturer is permitted to access the one or more resources; and

in response to determining that the first identified manufacturer is permitted to access the one or more resources, provide access to the one or more resources to the first identified manufacturer.

107. The computer program of claim 106, wherein:

the one or more resources correspond to a second manufacturer,

the one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when

executed by the electronic device, causes the electronic device to determine that the first manufacturer is not permitted to access the one or more resources.

108. The computer program of claim 106, wherein:

the one or more resources correspond to one or more suppliers who provided raw materials to the first identified manufacturer;

the one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine that the first manufacturer is permitted to access the one or more resources.

109. The computer program of claim 106, wherein:

the one or more resources correspond to one or more suppliers who did not provided raw materials to the first identified manufacturer;

the one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to determine that the first manufacturer is not permitted to access the one or more resources.

110. The computer program of claim 100, wherein:

the manufacturing data comprises one or more production specifications associated with the product that is produced,

the installation data comprises one or more installation specifications associated with the product that is installed,

further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

determine whether the production specifications are consistent with the installation specifications by comparing at least a portion of the production specification to at least a portion of the installation specifications,

in response to determining that the production specifications are not consistent with the installation specifications:

automatically generate a notification of the inconsistency, and

send the notification to one or more of the identified manufacturers or the identified installers.

111. The computer program of claim 100, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

for a first identified manufacturer from the one or more identified manufacturers, generate a token for the first identified manufacturer, wherein the token comprises:

an identifier associated with the first identified manufacturer,

one or more of the one or more access rights that correspond to the first identified manufacturer, and

for each of the one or more access rights corresponding to the first identified manufacturer, an indication of a subset of information that is stored on the blockchain to which the corresponding access right corresponds; and
send the token to the first identified manufacturer.

112. The computer program of claim 111, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified manufacturer the first identified manufacturer can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

113. The computer program of claim 112, wherein the token further comprises an indication of how many tiers of delegation the first identified manufacturer is permitted to make.

114. The computer program of claim 111, further comprising one or more programming instructions that, when executed by a second electronic device associated with the first identified manufacturer, causes the second electronic device to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the corresponding access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

115. The computer program of claim 114, further comprising one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

- generate a digital signature associated with the delegated token, and
- send the delegated token and the digital signature to the first identified manufacturer.

116. The computer program of claim 115, wherein the one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed by the second electronic device, causes the second electronic device to:

- apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

- encrypt the hashed value with a private key associated with the first identified manufacturer.

117. The computer program of claim 100, further comprising one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

- receive an access request from a business partner, wherein the access request comprises:
 - a token,
 - a digital signature corresponding to the token, and
 - an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determine whether the participant is an identified manufacturer,

in response to determining that the participant is an identified manufacturer, retrieve a public key associated with the participant from a key store,

decrypt the digital signature using the retrieved public key to generate a decrypted value.

118. The computer program of claim 117, wherein the participant is of the identified manufacturers, wherein the business partner is a customer of the identified manufacturer.

119. The computer program of claim 60, wherein the product comprises spray foam insulation.

120. A system of securing data associated with a product, the system comprising:

an electronic device; and

a computer-readable storage medium comprising one or more programming instructions that, when executed, cause the electronic device to:

identify a plurality of raw materials needed to produce the product, wherein one or more suppliers supply at least a portion of the plurality of raw materials to one or more installers of the product,

for each identified raw material, identifying an associated supplier of the identified raw material,

for each identified supplier:

receiving, from the identified supplier, a communication comprising quality data corresponding to its associated raw material,
generating a supplier block that is associated with the identified supplier,
storing at least a portion of the quality data in the supplier block of the identified supplier,
adding the supplier block to a blockchain, and
identifying one or more installers of the product, and
for each identified installer:

receiving, from the identified installer, a communication comprising installation data associated with the product,
generating an installation block that is associated with the identified installer,
storing at least a portion of the installation data in the installation block of the identified installer, and

adding the installation block to the blockchain,

wherein at least a portion of the blockchain is accessible by one or more of the identified suppliers and/or one or more of the identified installers according to an access policy associated with the blockchain, wherein the access policy includes an access control list that defines one or more access rights to the blockchain.

121. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, causes the electronic device to perform one or more of the following:

authenticate the communication from the identified supplier before adding the supplier block to the blockchain; or

authenticate the communication from the identified installer before adding the installation block to the blockchain.

122. The system of claim 121, wherein the one or more programming instructions that, when executed, cause the electronic device to authenticate the communication from the identified supplier comprise one or more programming instructions that, when executed by the electronic device, causes the electronic device to:

receive a digital signature in connection with the communication from the identified supplier;

retrieve a public key associated with the identified supplier from a key store; and

use the public key to decrypt the digital signature to yield a decrypted value.

123. The system of claim 122, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

apply a hashing algorithm to the communication from the identified supplier to yield a hashed value;

determine whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, add the supplier block to the blockchain.

124. The system of claim 121, wherein the one or more programming instructions that, when executed, cause the electronic device to authenticate the communication from the identified installer comprise one or more programming instructions that, when executed, cause the electronic device to:

receive a digital signature in connection with the communication from the identified installer;

retrieve a public key associated with the identified installer from a key store; and

use the public key to decrypt the digital signature to yield a decrypted value.

125. The system of claim 124, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

apply a hashing algorithm to the communication from the identified installer to yield a hashed value;

determine whether the hashed value matches the decrypted value; and

in response to determining that the hashed value matches the decrypted value, add the installer block to the blockchain.

126. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

- identify one or more inspectors of the product; and

- for each identified inspector:

- receive, from the identified inspector, a communication comprising inspection data associated with the product,

- generate an inspection block that is associated with the identified inspection,

- store at least a portion of the inspection data in the inspection block of the identified inspector,

- add the inspection block to the blockchain, and

wherein at least a portion of the blockchain is accessible by the identified inspectors according to the one or more access rights.

127. The system of claim 126, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

- for a first identified inspector from the one or more identified inspector, generate a token for the first identified inspector, wherein the token comprises:

- an identifier associated with the first identified inspector,

- one or more of the one or more access rights that correspond to the first identified inspector, and

for each of the access rights that correspond to the first identified inspector, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
send the token to the first identified inspector.

128. The system of claim 127, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified inspector the first identified inspector can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

129. The system of claim 127, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

130. The system of claim 127, further comprising a second computer-readable storage medium comprising one or more programming instructions that, when executed by a second electronic device, cause the second electronic device to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights that correspond to the first identified inspector, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

131. The system of claim 130, wherein the second computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the second electronic device to:

- generating a digital signature associated with the delegated token, and
- sending the delegated token and the digital signature to the first identified inspector.

132. The system of claim 131, wherein the one or more programming instructions that, when executed, cause the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed, cause the second electronic device to:

- apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and
- encrypt the hashed value with a private key associated with the first identified inspector.

133. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

- receive an access request from a first identified supplier, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;
- determine one or more blocks of the blockchain that include at least a portion of the resources;

determine, based on the access policy, whether the first identified supplier is permitted to access the one or more resources; and

in response to determining that the first identified supplier is permitted to access the one or more resources, provide access to the one or more resources to the first identified supplier.

134. The system of claim 133, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

135. The system of claim 133, wherein:

the one or more resources correspond to the first identified supplier,

the one or more programming instructions that, when executed, cause the electronic device to determine whether the first identified supplier is permitted to access the one or more resources comprise one or more programming instructions that, when executed, cause the electronic device to determine that the first identified supplier is permitted to access the one or more resources.

136. The system of claim 133, wherein:

the one or more resources correspond to one or more other suppliers,

the one or more programming instructions that, when executed, cause the electronic device to determine whether the first identified supplier is permitted to access the one or more

resources comprise one or more programming instructions that, when executed, cause the electronic device to determine that the first identified supplier is not permitted to access the one or more resources.

137. The system of claim 120, further comprising one or more programming instructions that, when executed, cause the electronic device to:

- receive an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

- determine one or more blocks of the blockchain that include at least a portion of the resources;

- determine, based on the access policy, whether the first identified installer is permitted to access the one or more resources; and

- in response to determining that the first identified installer is permitted to access the one or more resources, provide access to the one or more resources to the first identified installer.

138. The system of claim 137, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, causes the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

139. The system of claim 120, wherein the production data comprises one or more images of the product after it is produced, wherein the one or more images are captured by an infrared imaging device.

140. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

- access building code information associated with a location where the product is to be installed;

- determine whether the installation data is consistent with the building code information by comparing at least a portion of the installation data to at least a portion of the building code information;

- in response to the determining that the installation data is not consistent with the building code information:

- automatically generate a notification of the inconsistency, and

- send the notification to one or more of the identified installers.

141. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

- for a first identified supplier from the one or more identified suppliers, generate a token for the first identified supplier, wherein the token comprises:

- an identifier associated with the first identified supplier,

one or more of the one or more access rights that correspond to the first identified supplier, and

for each of the one or more access rights that correspond to the first identified supplier, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
send the token to the first identified supplier.

142. The system of claim 141, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified supplier the first identified supplier can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

143. The system of claim 142, wherein the token further comprises an indication of how many tiers of delegation the first identified supplier is permitted to make.

144. The system of claim 141, further comprising a second computer-readable storage medium comprising one or more programming instructions that, when executed, cause a second electronic device associated with the first identified supplier to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights corresponding to the first identified supplier, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

145. The system of claim 144, wherein the second computer-readable storage medium further comprises the one or more programming instructions that, when executed, cause the second electronic device to:

generate a digital signature associated with the delegated token, and
send the delegated token and the digital signature to the first identified supplier.

146. The system of claim 145, wherein the one or more programming instructions that, when executed, cause the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed, cause the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and
encrypt the hashed value with a private key associated with the first identified supplier.

147. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

for a first identified installer from the one or more identified installers, generate a token for the first identified installer, wherein the token comprises:

an identifier associated with the first identified installer,
one or more of the one or more access rights that correspond to the first identified installer, and
for each of the one or more access rights that correspond to the first identified installer, an indication of a subset of information that is stored on the blockchain to which the access right corresponds; and
send the token to the first identified installer.

148. The system of claim 147, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified installer the first identified installer can delegate to one or more business partners for each of the subsets of information that to which the access rights corresponds.

149. The system of claim 148, wherein the token further comprises an indication of how many tiers of delegation the first identified installer is permitted to make.

150. The system of claim 147, further comprising a second computer-readable storage medium comprising one or more programming instructions that, when executed, cause a second electronic device associated with the first identified installer to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

151. The system of claim 150, further comprising one or more programming instructions that, when executed by the second electronic device, cause the second electronic device to:

generate a digital signature associated with the delegated token, and
send the delegated token and the digital signature to the first identified installer.

152. The system of claim 151, wherein the one or more programming instructions that, when executed, cause the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed by the second electronic device, cause the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypt the hashed value with a private key associated with the first identified installer.

153. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

receive an access request from a business partner, wherein the access request comprises:

a token,
a digital signature corresponding to the token, and

an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determine whether the participant is an identified supplier or an identified installer, in response to determining that the participant is an identified supplier or an identified installer, retrieve a public key associated with the participant from a key store, decrypt the digital signature using the retrieved public key to generate a decrypted value.

154. The system of claim 153, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

apply a hashing algorithm to the token to generate a hashed value;
determine whether the decrypted value matches the hashed value.

155. The system of claim 153, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

identify one or more of the one or more access rights that are associated with the participant;
determine whether the access rights associated with the participant permit the participant to access the one or more resources stored on the blockchain for which access is sought; and

in response to determining that the access rights associated with the participant permit the participant access, grant access to the one or more resources to the business partner.

156. The system of claim 153, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

identify one or more of the one or more access rights that are associated with the participant; and

determine whether the one or more access rights associated with the participant permits the participant to delegate access rights.

157. The system of claim 153, wherein the participant is one of the identified suppliers, wherein the business partner is a customer of the identified supplier.

158. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

receive an access request from a first identified installer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

determine one or more blocks of the blockchain that include at least a portion of the resources;

determine, based on the access policy, whether the first identified installer is permitted to access the one or more resources; and

in response to determining that the first identified installer is permitted to access the one or more resources, provide access to the one or more resources to the first identified installer.

159. The system of claim 120, wherein the computer-readable storage medium further comprises one or more programming instructions, that when executed, cause the electronic device to:

identify one or more manufacturers of the product,

for each identified manufacturer:

receive, from the identified manufacturer, a communication comprising manufacturing data associated with the product, wherein the manufacturing data comprises one or more of the following:

production data,

storage data, or

testing results,

generate a manufacturer block that is associated with the identified manufacturer,

store at least a portion of the manufacturing data in the manufacturer block of the identified manufacturer,

add the manufacturer block to the blockchain.

160. The system of claim 159, wherein the quality data comprises information pertaining to one or more transportation conditions of the associated raw material during transportation from the supplier to a manufacturer.

161. The system of claim 159, wherein the manufacturing data comprises information pertaining to one or more transportation conditions of the product during transportation from the manufacturer to the installer.

162. The system of claim 159, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, causes the electronic device to authenticate the communication from the identified manufacturer before adding the manufacturer block to the blockchain.

163. The system of claim 162, wherein the one or more programming instructions that, when executed, cause the electronic device to authenticate the communication from the identified manufacturer comprise one or more programming instructions that, when executed, cause the electronic device to:

receive a digital signature in connection with the communication from the identified manufacturer;

retrieve a public key associated with the identified manufacturer from a key store; and

use the public key to decrypt the digital signature to yield a decrypted value.

164. The system of claim 163, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

 apply a hashing algorithm to the communication from the identified manufacturer to yield a hashed value;

 determine whether the hashed value matches the decrypted value; and

 in response to determining that the hashed value matches the decrypted value, add the manufacturer block to the blockchain.

165. The system of claim 164, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

 receive an access request from a first identified manufacturer, wherein the access request comprises an indication of one or more resources stored on the blockchain for which access is sought;

 determine one or more blocks of the blockchain that include at least a portion of the resources;

 determine, based on the access policy, whether the first identified manufacturer is permitted to access the one or more resources; and

 in response to determining that the first identified manufacturer is permitted to access the one or more resources, provide access to the one or more resources to the first identified manufacturer.

166. The system of claim 165, wherein:

the one or more resources correspond to a second manufacturer,

the one or more programming instructions that, when executed, cause the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when executed, cause the electronic device to determine that the first manufacturer is not permitted to access the one or more resources.

167. The system of claim 165, wherein:

the one or more resources correspond to one or more suppliers who provided raw materials to the first identified manufacturer;

the one or more programming instructions that, when executed, cause the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when executed, cause the electronic device to determine that the first manufacturer is permitted to access the one or more resources.

168. The system of claim 165, wherein:

the one or more resources correspond to one or more suppliers who did not provided raw materials to the first identified manufacturer;

the one or more programming instructions that, when executed, cause the electronic device to determine whether the first identified manufacturer is permitted to access the one or more resources comprise one or more programming instructions that, when executed, cause the

electronic device to determine that the first manufacturer is not permitted to access the one or more resources.

169. The system of claim 165, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to access a second blockchain that comprises one or more second blocks, wherein each of the one or more second blocks comprises one or more access rights associated with one or more of the resources and/or one or more authorized users of the blockchain.

170. The system of claim 159, wherein:

the manufacturing data comprises one or more production specifications associated with the product that is produced,

the installation data comprises one or more installation specifications associated with the product that is installed,

the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

determine whether the production specifications are consistent with the installation specifications by comparing at least a portion of the production specification to at least a portion of the installation specifications,

in response to determining that the production specifications are not consistent with the installation specifications:

automatically generate a notification of the inconsistency, and

send the notification to one or more of the identified manufacturers or the identified installers.

171. The system of claim 159, wherein:

the manufacturing data comprises one or more production specifications associated with the product that is produced,

the installation data comprises one or more installation specifications associated with the product that is installed,

the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

determine whether the production specifications are consistent with the installation specifications by comparing at least a portion of the production specification to at least a portion of the installation specifications,

in response to determining that the production specifications are not consistent with the installation specifications:

automatically generate a notification of the inconsistency, and

send the notification to one or more of the identified manufacturers or the identified installers.

172. The system of claim 159, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, causes the electronic device to:

for a first identified manufacturer from the one or more identified manufacturers,
generate a token for the first identified manufacturer, wherein the token comprises:
an identifier associated with the first identified manufacturer,
one or more of the one or more access rights that correspond to the first identified
manufacturer, and
for each of the one or more access rights corresponding to the first identified
manufacturer, an indication of a subset of information that is stored on the blockchain to
which the corresponding access right corresponds; and
send the token to the first identified manufacturer.

173. The system of claim 172, wherein the token further comprises:

an indication of which of the access rights that correspond to the first identified
manufacturer the first identified manufacturer can delegate to one or more business partners for
each of the subsets of information that to which the access rights corresponds.

174. The system of claim 173, wherein the token further comprises an indication of how many
tiers of delegation the first identified manufacturer is permitted to make.

175. The system of claim 172, further comprising a second computer-readable storage medium
comprising one or more programming instructions that, when executed, cause a second
electronic device associated with the first identified manufacturer to:

generate a delegated token for a business partner that comprises:

an indication of one or more delegated access rights, wherein the delegated access rights comprise one or more of the corresponding access rights, and

for each of the delegated access rights, an indication of at least a portion of the subset of information that is stored on the blockchain to which the delegated access rights correspond.

176. The system of claim 175, wherein the second computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the second electronic device to:

generate a digital signature associated with the delegated token, and

send the delegated token and the digital signature to the first identified manufacturer.

177. The system of claim 176, wherein the one or more programming instructions that, when executed, cause the second electronic device to generate a digital signature associated with the delegated token comprise one or more programming instructions that, when executed, cause the second electronic device to:

apply a hashing algorithm to at least a portion of the delegated token to yield a hashed value; and

encrypt the hashed value with a private key associated with the first identified manufacturer.

178. The system of claim 159, wherein the computer-readable storage medium further comprises one or more programming instructions that, when executed, cause the electronic device to:

receive an access request from a business partner, wherein the access request comprises:

a token,

a digital signature corresponding to the token, and

an indication of one or more resources stored on the blockchain for which access is sought,

wherein the token comprises an indication of a participant from whom the token was received, and an indication of one or more access rights delegated to the business partner by the participant,

determine whether the participant is an identified manufacturer,

in response to determining that the participant is an identified manufacturer, retrieve a public key associated with the participant from a key store,

decrypt the digital signature using the retrieved public key to generate a decrypted value.

179. The system of claim 159, wherein the participant is of the identified manufacturers, wherein the business partner is a customer of the identified manufacturer.

180. The system of claim 120, wherein the product comprises spray foam insulation.

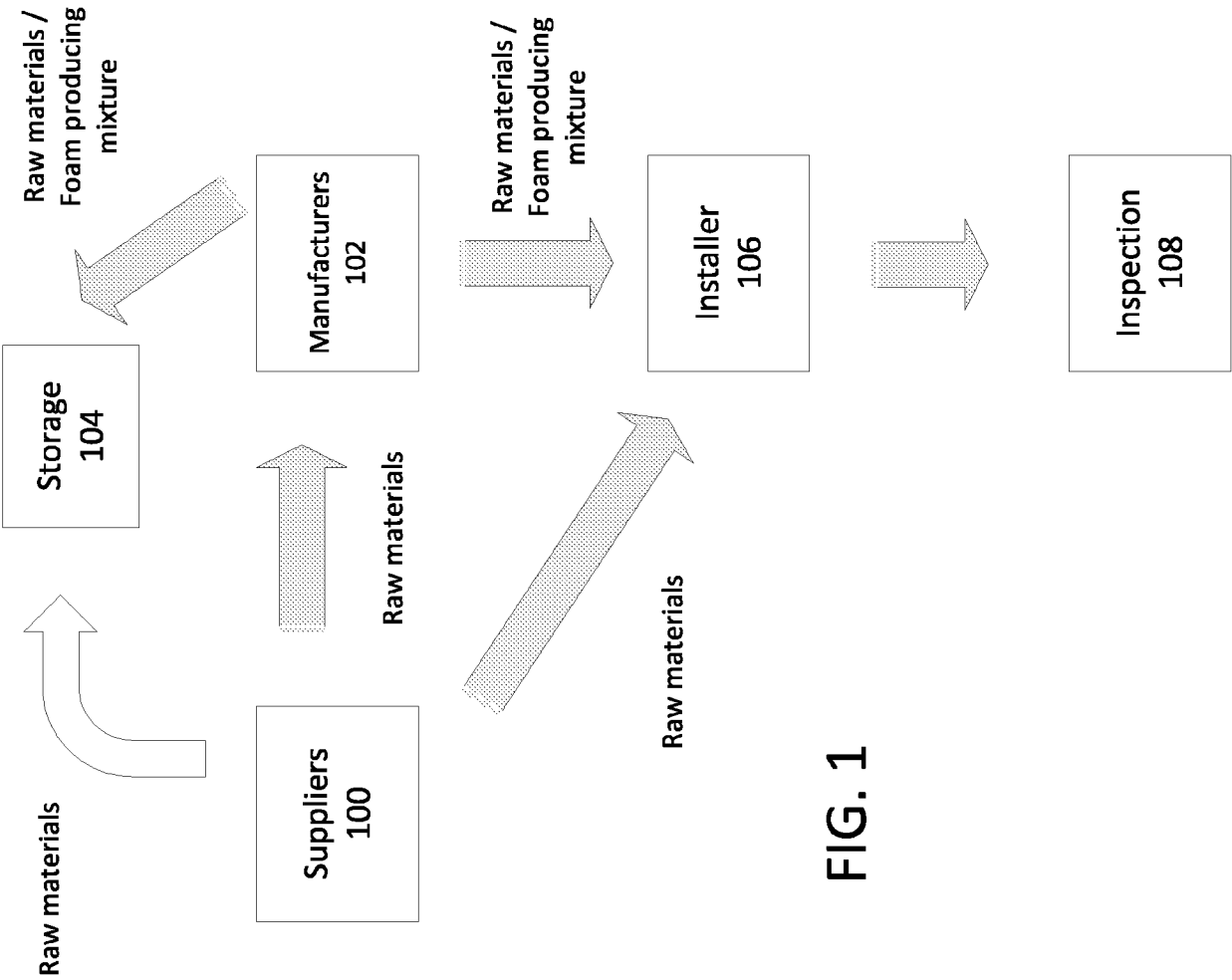


FIG. 1

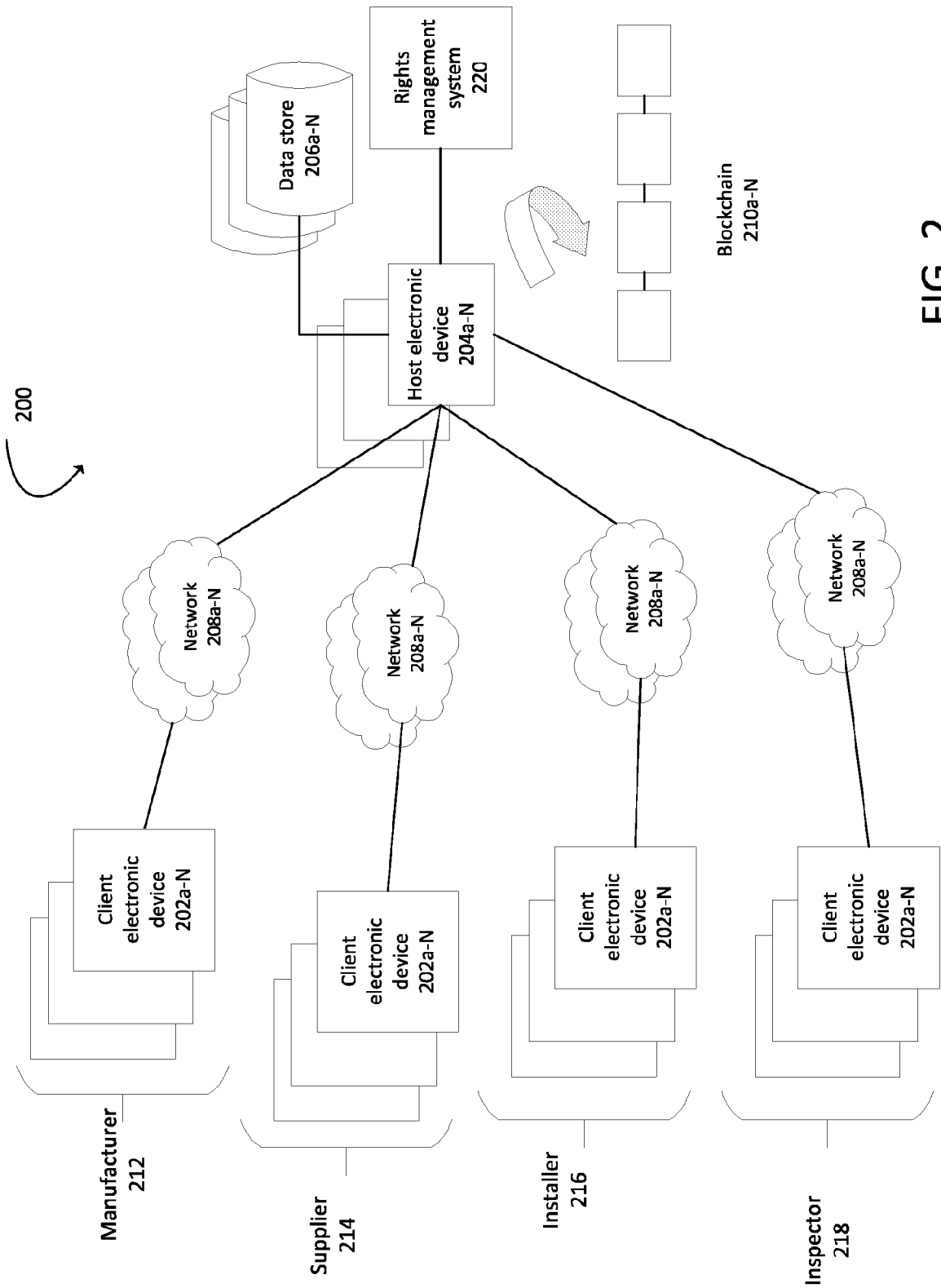


FIG. 2

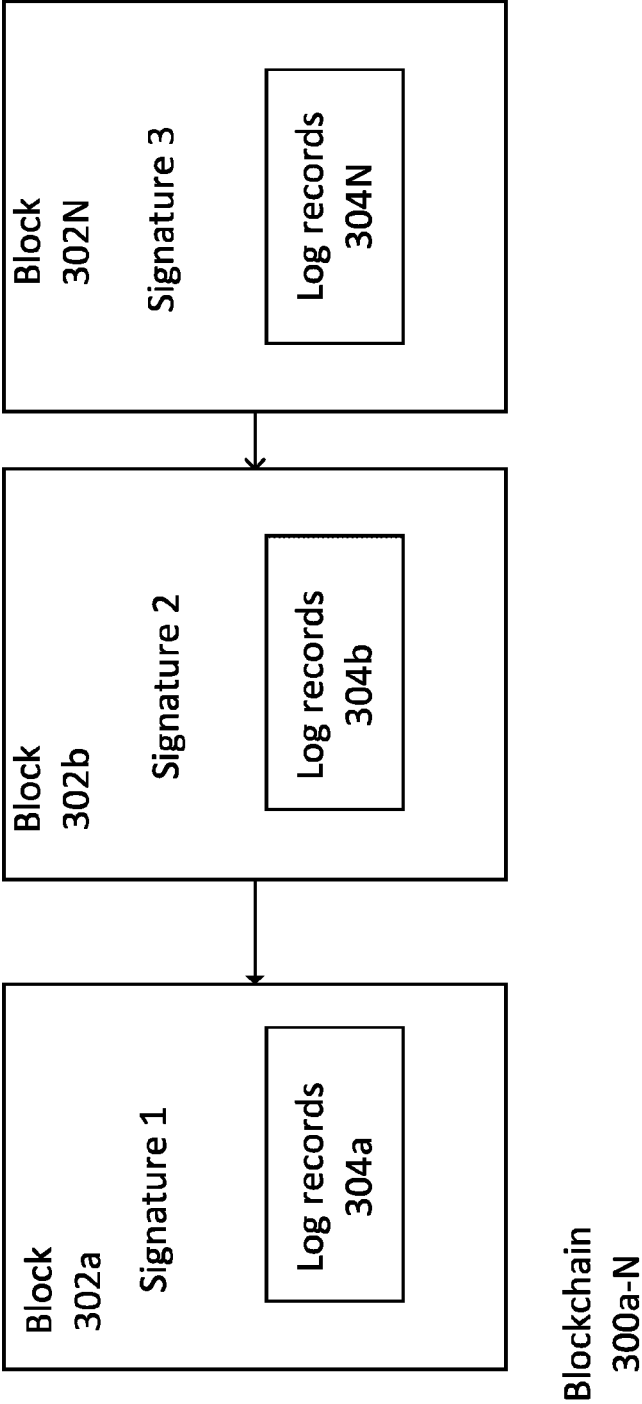


FIG. 3

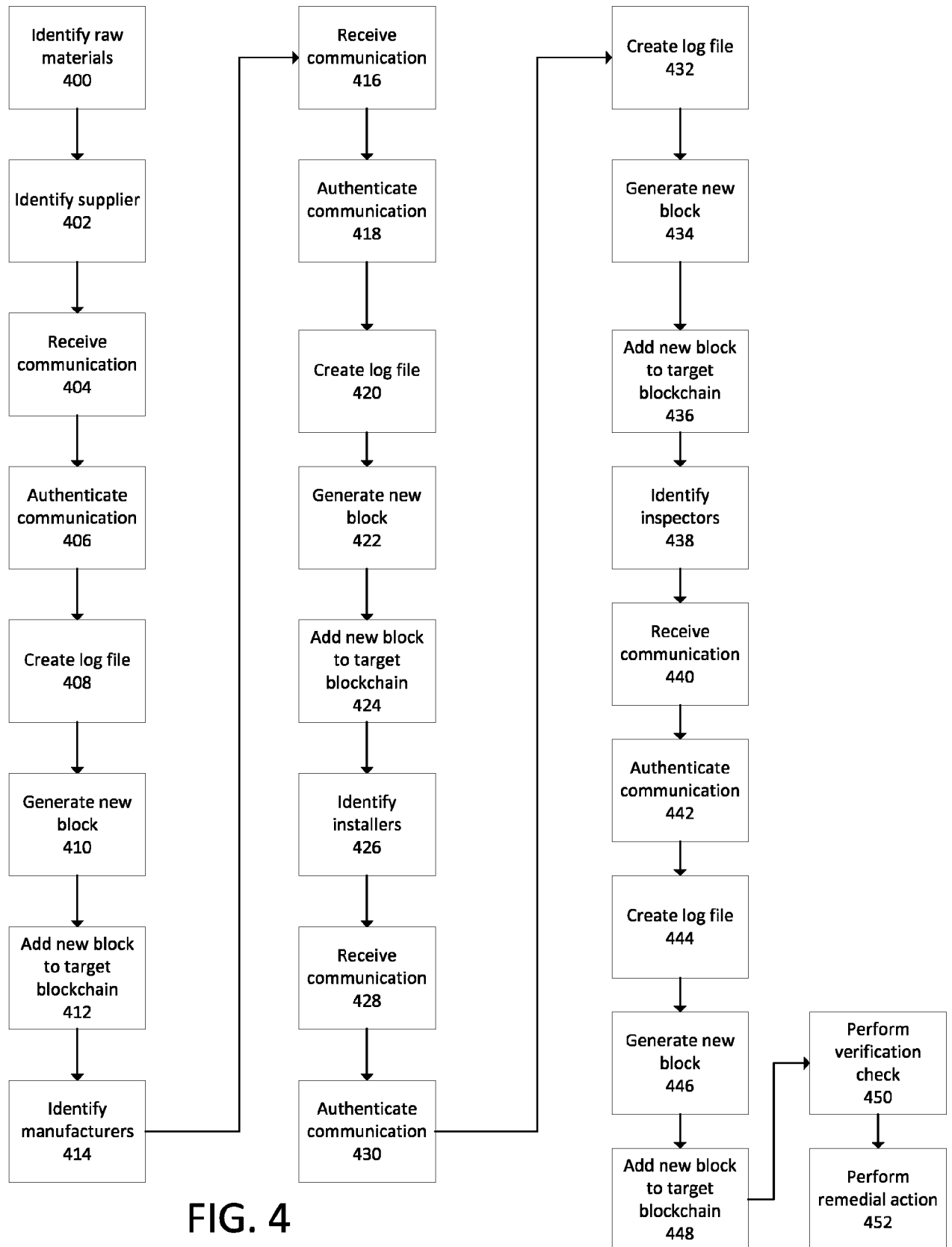


FIG. 4

Source identifier	Block identifier
02d3	Signature 1
G629	Signature 2
02d3	Signature 3
Ab63	Signature 4
02d3	Signature 5
G629	Signature 6
Ab63	Signature 7

FIG. 5

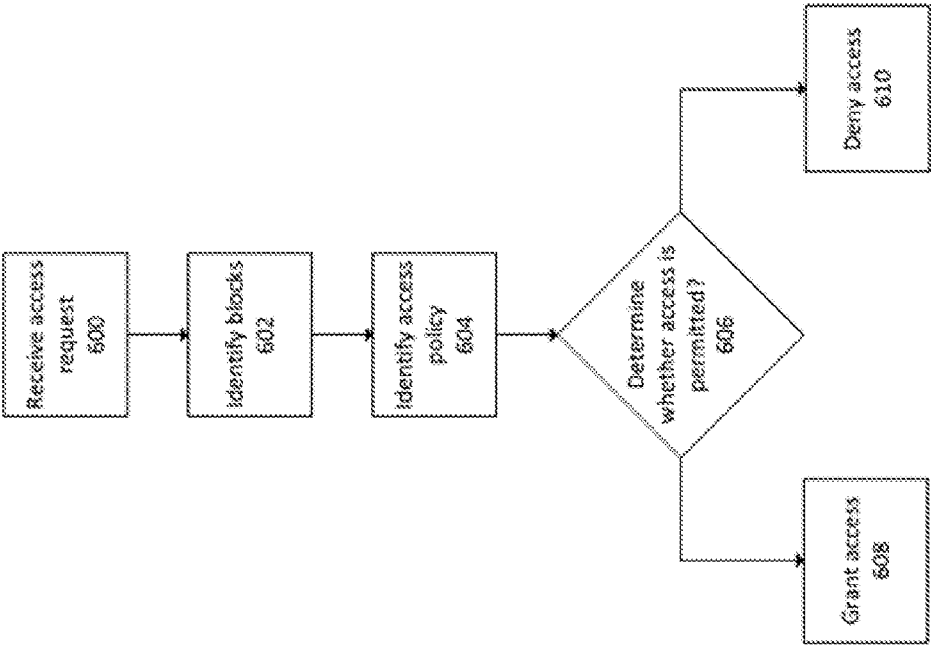


FIG. 6A

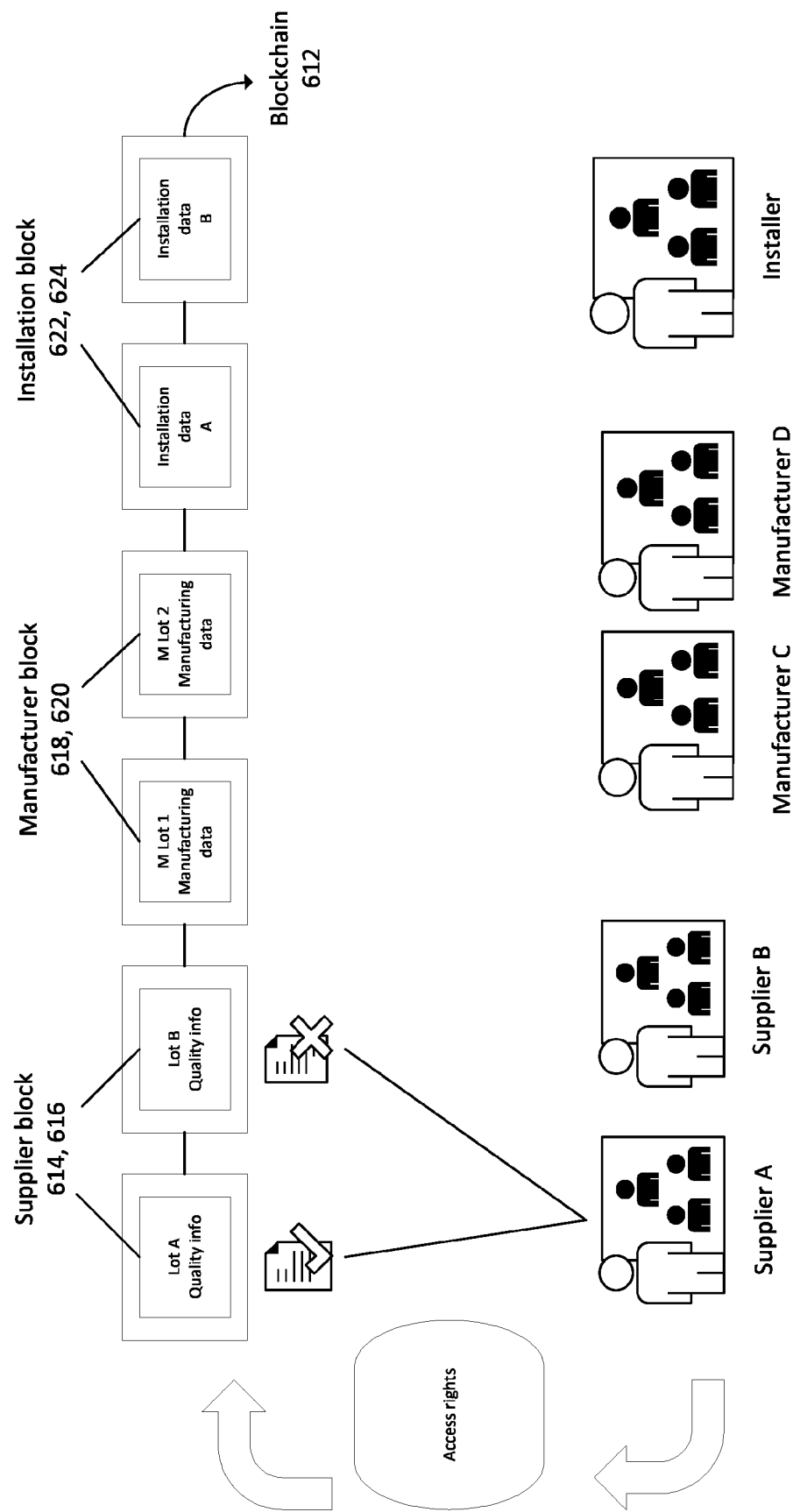


FIG. 6B

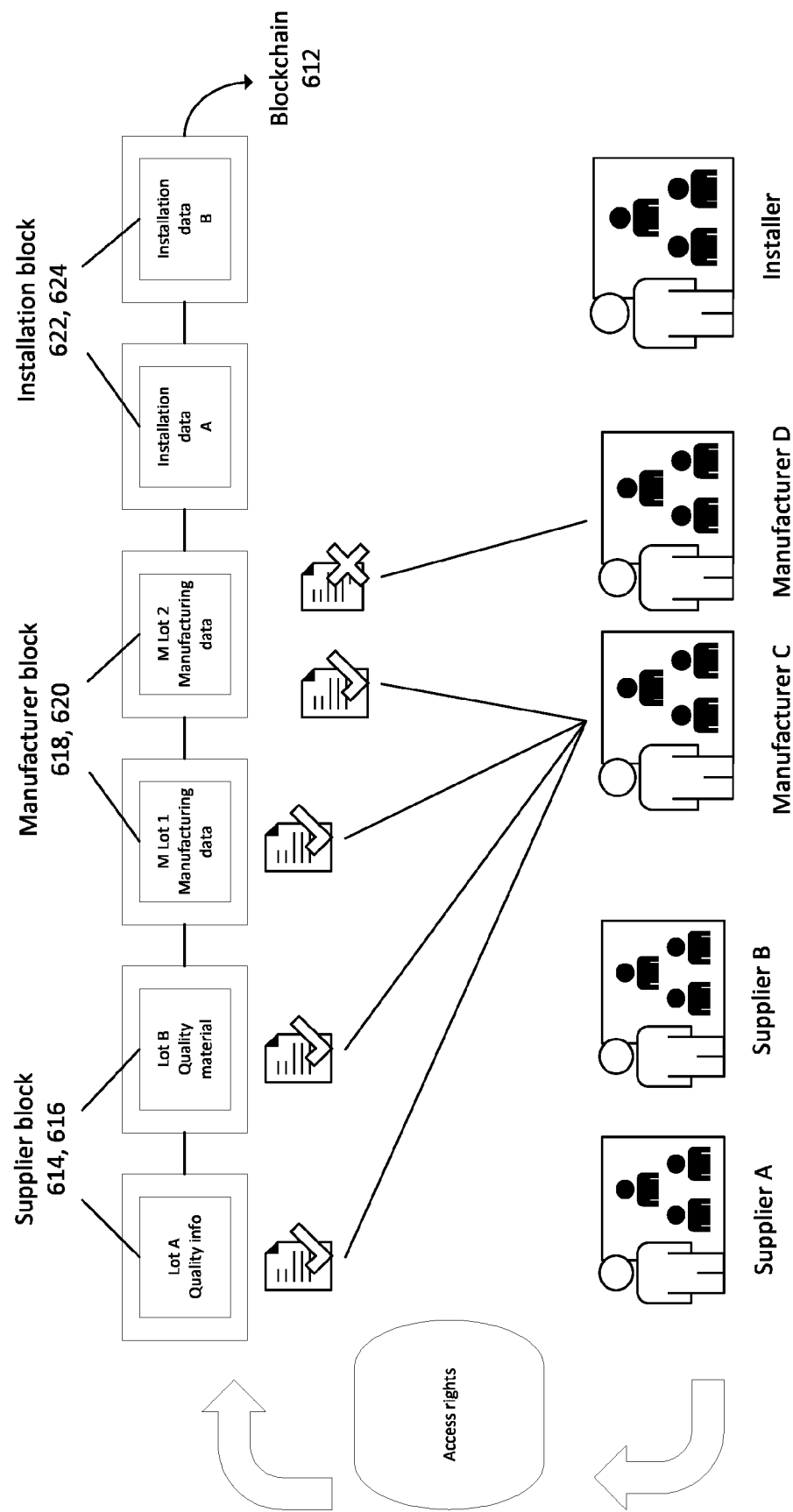


FIG. 6C

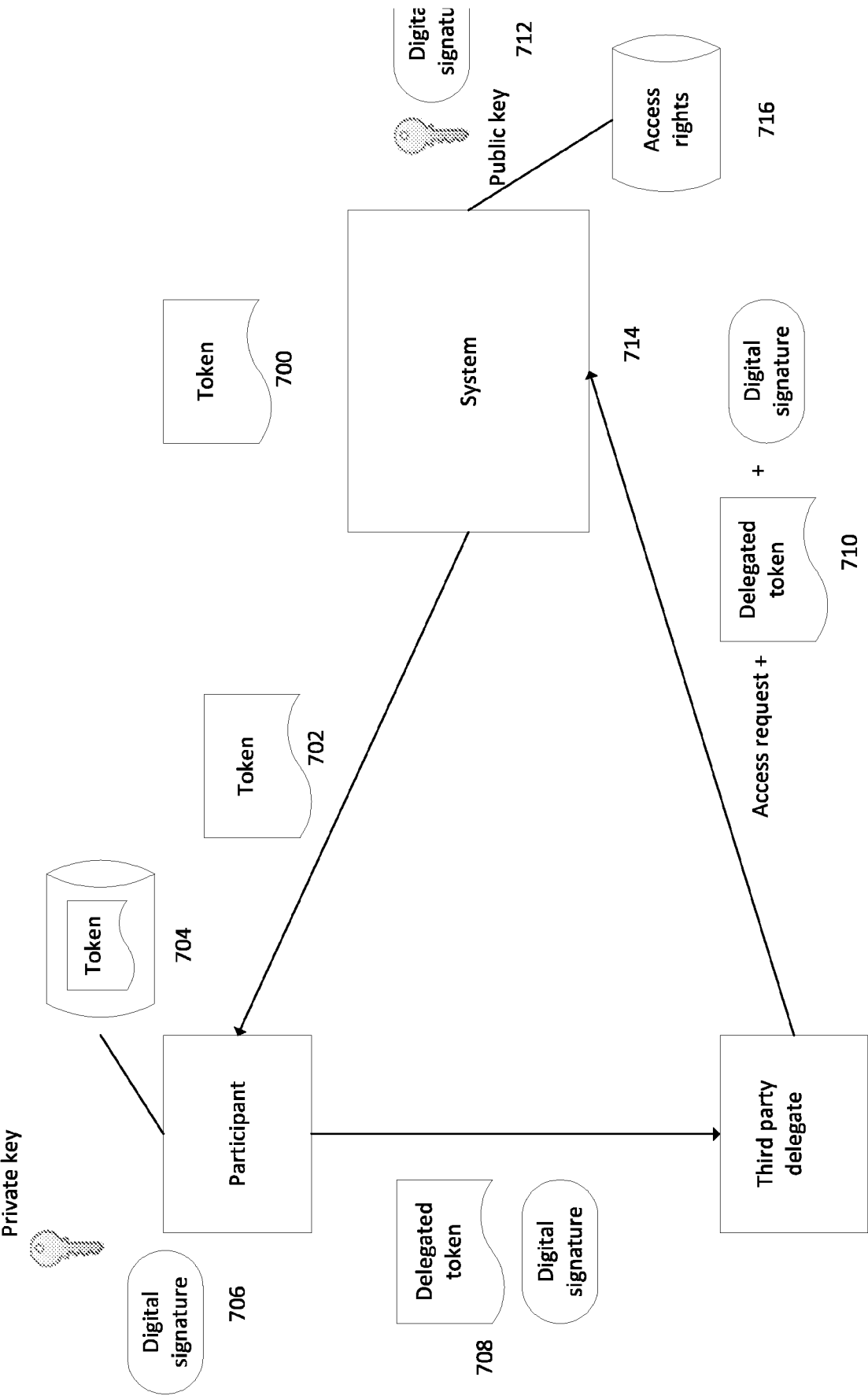


FIG. 7

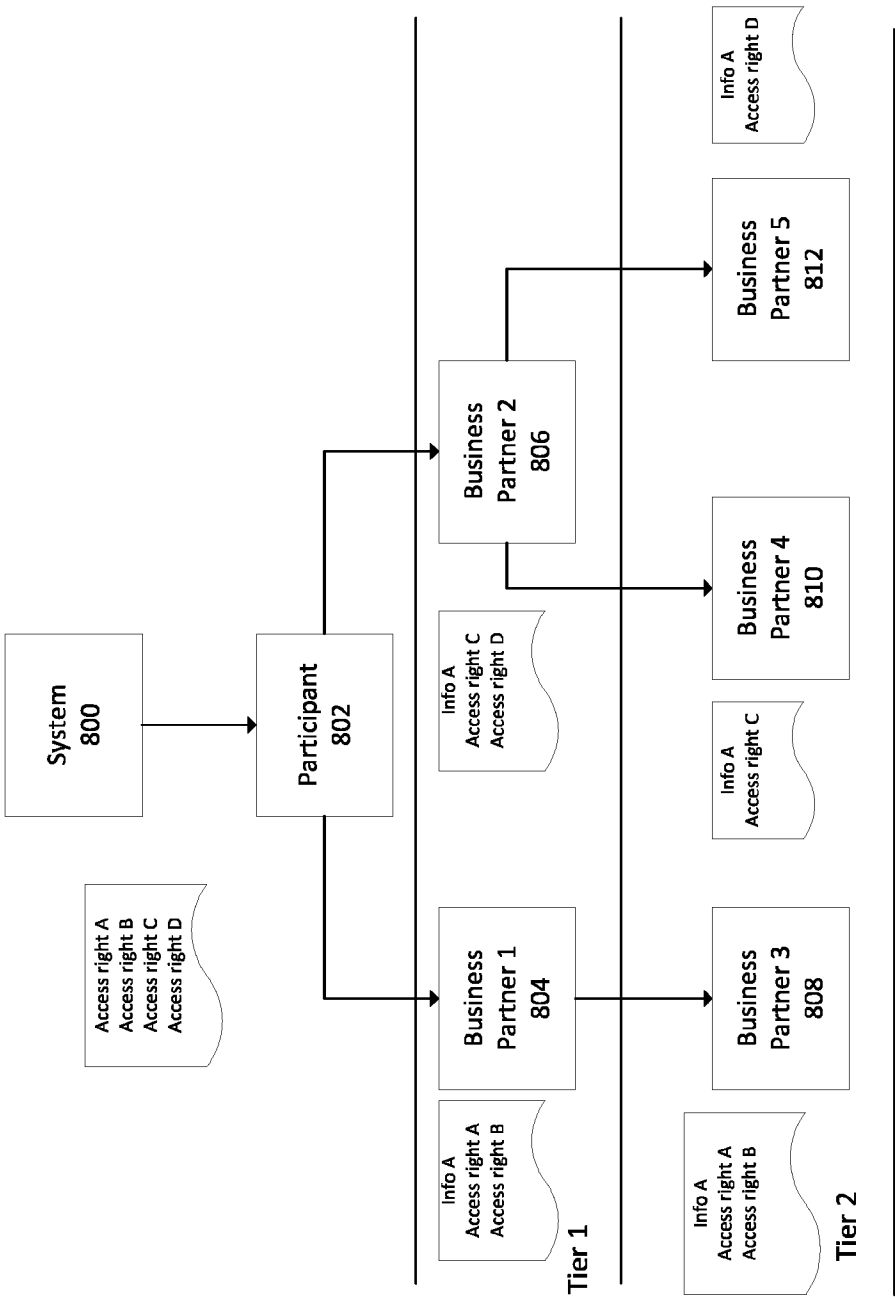


FIG. 8

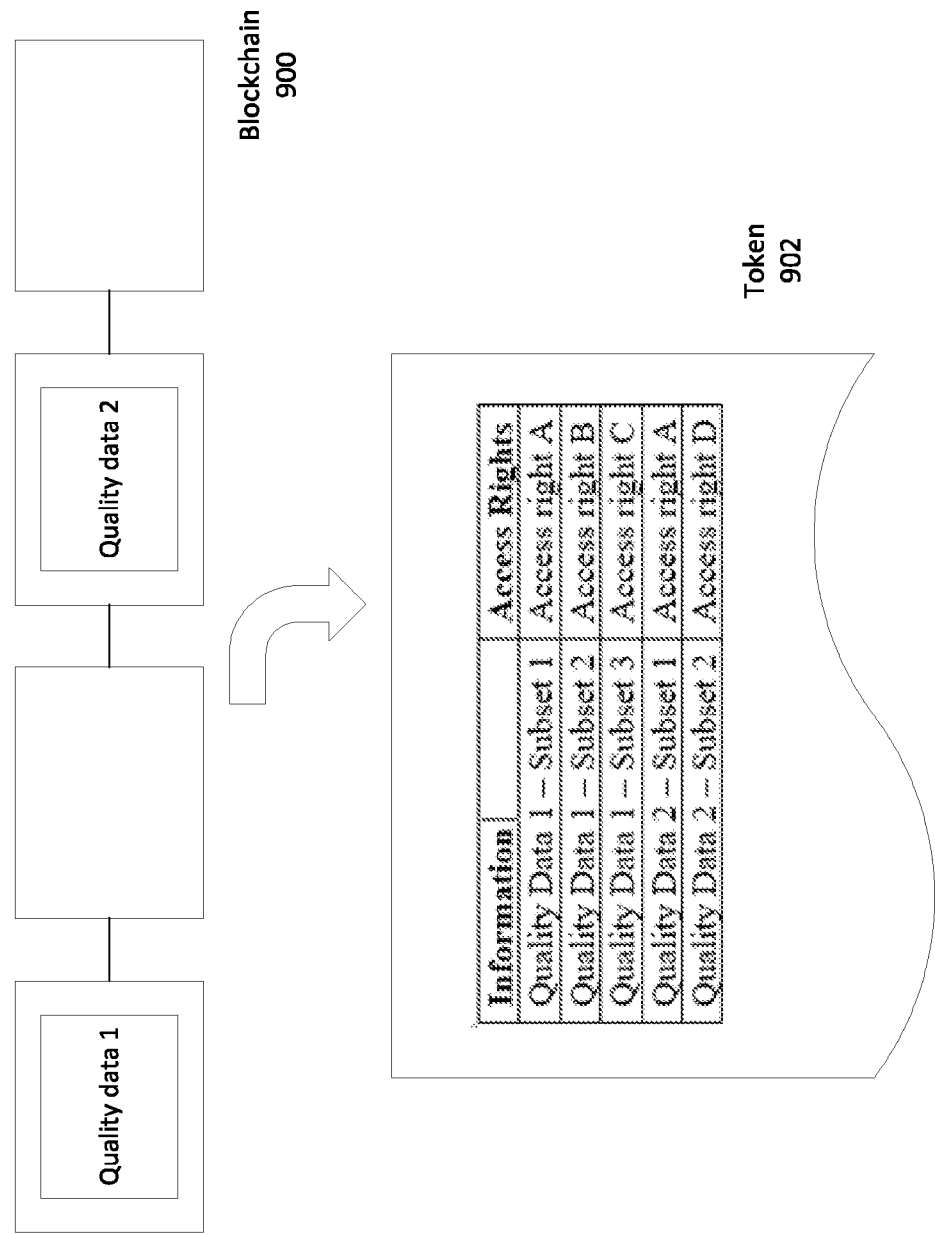


FIG. 9A

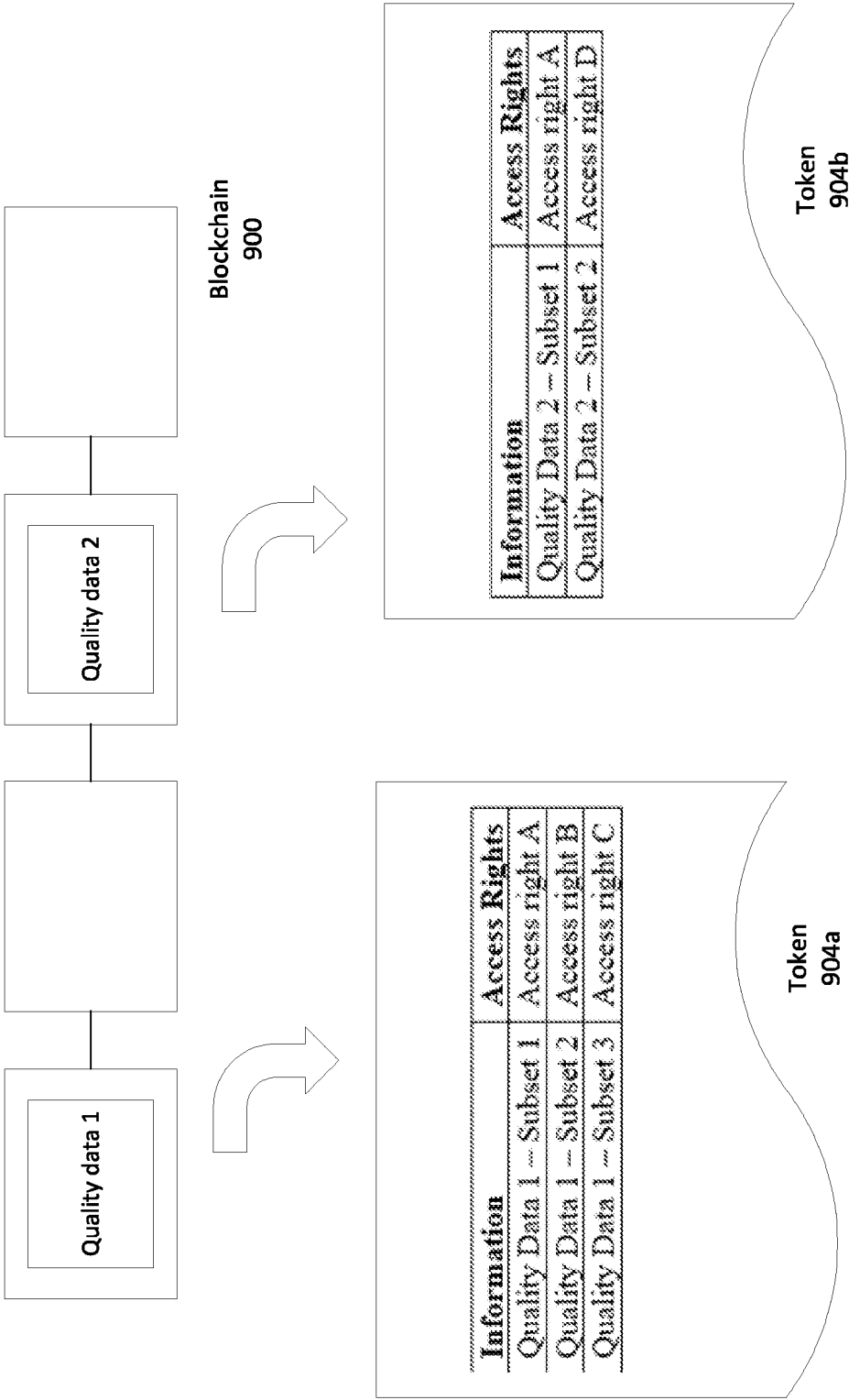


FIG. 9B

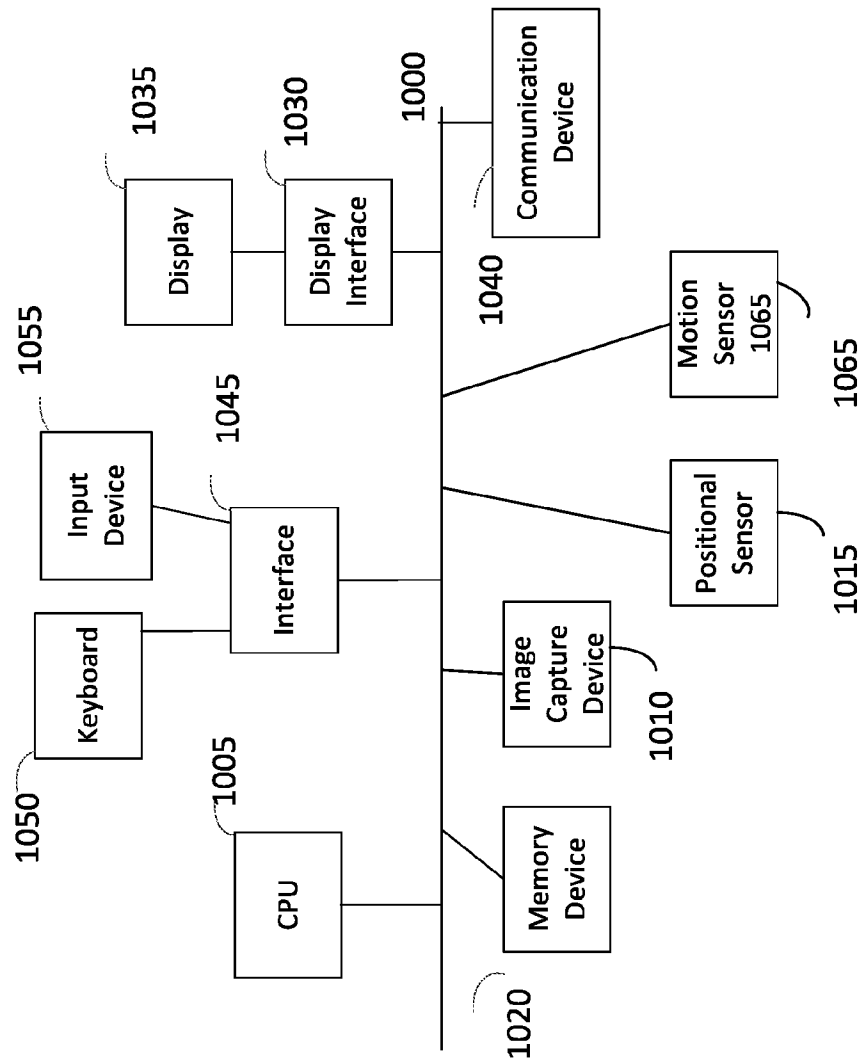


FIG. 10

INTERNATIONAL SEARCH REPORT

International application No

PCT/US2022/012504

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06010/08 G06010/06

ADD .

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)

G060

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MALIK SIDRA ET AL: "ProductChain: Scalable Blockchain Framework to Support Provenance in Supply Chains", 2018 IEEE 17TH INTERNATIONAL SYMPOSIUM ON NETWORK COMPUTING AND APPLICATIONS (NCA), IEEE, 1 November 2018 (2018-11-01), pages 1-10, XP033459589, DOI: 10.1109/NCA.2018.8548322 [retrieved on 2018-11-26] abstract page 1, left-hand column - page 2, right-hand column page 3, left-hand column - page 7, right-hand column page 10, left-hand column figures 1-5; table I ----- -----	1-180

☒ 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

"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

25 April 2022

Date of mailing of the international search report

04/05/2022

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer _____

Nicoli, Félix

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2022/012504

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2019/342085 A1 (KUBE NATHAN JOHN WALTER [CA] ET AL) 7 November 2019 (2019-11-07) abstract page 3 - page 15 page 26 - page 99 figures 1-4, 7 -----	1-180
X	DARA SINCLAIR ET AL: "Security requirement prototyping with hyperledger composer for drug supply chain", CRYPTOGRAPHY, SECURITY AND PRIVACY, ACM, 2 PENN PLAZA, SUITE 701NEW YORKNY10121-0701USA, 19 January 2019 (2019-01-19), pages 158-163, XP058434572, DOI: 10.1145/3309074.3309104 ISBN: 978-1-4503-6618-2 abstract page 158 - page 159 page 162 figures 1-9 -----	1-180
X,P	WO 2021/236762 A1 (COVESTRO LLC [US]) 25 November 2021 (2021-11-25) the whole document -----	1-180

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2022/012504

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2019342085 A1	07-11-2019	NONE	

WO 2021236762 A1	25-11-2021	NONE	
