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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 July 2020 (23.07.2020)

WIPO | PCT

(10) International Publication Number
WO 2020/149991 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
H04L 9/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:
PCT/US2019/068424

(22) International Filing Date:
23 December 2019 (23.12.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
16/247,344 14 January 2019 (14.01.2019) US

(71) Applicant: **POLYSIGN, INC.** [US/US]; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US).

(72) Inventors: **SCHWARTZ, David**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **BRITTO, Arthur**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **TONG, Anna**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **PAPAHADJOPOULOS, Kimon**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **MORRIS, William**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **KATAKI, Chiranjeeb**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **RODRIGUEZ, Eric**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US). **HANRAHAN, Conor**; 1700 Broadway St., 6th Floor, Oakland, California 94612 (US).

(74) Agent: **MORRIS & KAMLAY LLP** et al.; 1911 Fort Myer Drive, Suite 1050, Arlington, Virginia 22209 (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,

(54) Title: PREVENTING A TRANSMISSION OF AN INCORRECT COPY OF A RECORD OF DATA TO A DISTRIBUTED LEDGER SYSTEM

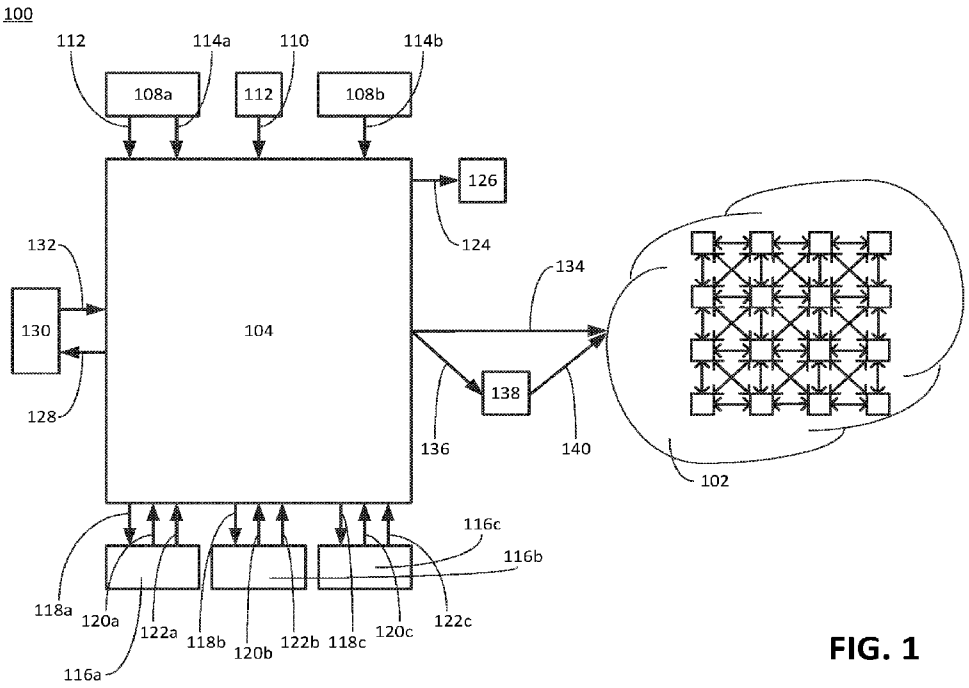

FIG. 1

(57) Abstract: An incorrect copy of a record of data can be prevented from being transmitted to a distributed ledger system. A first file can be received and can include information, in audio or video form, with a description of a subject matter of the record of data and with an authorization to transmit the copy to the distributed ledger system. The first file can be sent to a device. A second file can be received from the device and can include information that confirms that the description of the subject matter, included in the first file, is correct, and that confirms that an entity, which controlled production of the first file, has permission to authorize causing the copy to be transmitted to the distributed ledger system. The correct copy can be caused, based on a receipt of the first and the second files, to be transmitted to the distributed ledger system.

WO 2020/149991 A1

[Continued on next page]

HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

PREVENTING A TRANSMISSION OF AN INCORRECT COPY OF A RECORD OF DATA TO A DISTRIBUTED LEDGER SYSTEM

BACKGROUND

[0001] A blockchain can be a database that can be used to ensure an authenticity of a record of data. The blockchain can be organized as a sequence of blocks. A block can be added to the blockchain after a discrete duration of time has elapsed since a previous block was added to the blockchain. A block can include one or more records of data received by an electronic ledger system within the discrete duration of time since the previous block was added to the blockchain. A current block can include a hash of the previous block, a timestamp, and the one or more records of data that are a subject of the current block. The hash of the previous block can be a cryptographic hash. Another hash can represent the one or more records of data that are the subject of the current block. The other hash can be, for example, a merkle tree root hash. Because a subsequent block can include a hash of the current block, etc., an alteration of a record of data included in the blockchain can be determined by reference to hashes included in subsequent blocks.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The accompanying drawings, which are included to provide a further understanding of the disclosed technologies, are incorporated in and constitute a part of this specification. The drawings also illustrate implementations of the disclosed technologies and together with the detailed description serve to explain the principles of implementation of the disclosed technologies. No attempt is made to show structural details in more detail than may be necessary for a fundamental understanding of the disclosed technologies and the various ways in which it can be practiced.

[0003] FIG. 1 is a diagram illustrating an example of an environment for preventing a transmission of an incorrect copy of a record of data to an electronic network, according to the disclosed technologies.

[0004] FIGS. 2A through 2I are a flow diagram illustrating an example of a method for preventing a transmission of an incorrect copy of a record of data to an electronic network, according to the disclosed technologies.

[0005] FIG. 3 illustrates an example computing device suitable for implementing configurations of the disclosed technologies.

DETAILED DESCRIPTION

[0006] As used herein, a statement that a component can be "configured to" perform an operation can be understood to mean that the component requires no structural alterations, but merely needs to be placed into an operational state (e.g., be provided with electrical power, have an underlying operating system running, etc.) in order to perform the operation.

[0007] A blockchain can be a database that can be used to ensure an authenticity of a record of data. The blockchain can be organized as a sequence of blocks. A block can be added to the blockchain after a discrete duration of time has elapsed since a previous block was added to the blockchain. A block can include one or more records of data received by an electronic ledger system within the discrete duration of time since the previous block was added to the blockchain. A current block can include a hash of the previous block, a timestamp, and the one or more records of data that are a subject of the current block. The hash of the previous block can be a cryptographic hash. Another hash can represent the one or more records of data that are the subject of the current block. The other hash can be, for example, a merkle tree root hash. Because a subsequent block can include a hash of the current block, etc., an alteration of a record of data included in the blockchain can be determined by reference to hashes included in subsequent blocks.

[0008] The electronic ledger system can operate the blockchain. The electronic ledger system can include an electronic device or, alternatively, can include several electronic devices disposed in a peer-to-peer network. An electronic ledger system in which several electronic devices are disposed in a peer-to-peer network can be referred to as a distributed ledger system. Each electronic device in the distributed ledger system can be referred to as a node of the distributed ledger system. Each node can save a copy of the blockchain. In response to a block

being added to the blockchain, each node can update its copy of the blockchain. A consensus algorithm can receive, from the nodes, respective copies of the blockchain. The consensus algorithm can determine a consensus about which of the respective copies of the blockchain is a correct copy of the blockchain. In response to a determination of the consensus, the nodes can update their respective copies of the blockchain to be the correct copy of the blockchain. Because a distributed ledger system can use a consensus algorithm to determine the correct copy of the blockchain, an alteration of a record of data included in a copy of the blockchain stored at a node of the distributed ledger system can be prevented from being deemed to be the correct copy of the record of data. In this manner, a distributed ledger system can be used to ensure an authenticity of a record of data.

[0009] However, the efficacy of a distributed ledger system in ensuring an authenticity of a record of data depends upon a copy of the record of data that is transmitted to the distributed ledger system being a correct copy. Particularly in the case of a record of data associated with a transaction between entities, having an incorrect copy of the record of data transmitted to the distributed ledger system can cause one or more errors in the transaction to the detriment of one or both of the entities associated with the transaction. Significantly, in response to an incorrect copy of a record of data having been transmitted to the distributed ledger system, the nodes of the distributed ledger system can needlessly waste a substantial amount of time and energy updating their respective copies of the blockchain to include the incorrect copy of the record of data. For example, an average Bitcoin transaction on the Bitcoin.org blockchain consumes about 215 kilowatt-hours of energy.

[0010] Conventional techniques for authenticating a record of data before having the record of data transmitted to the distributed ledger system are inadequate. Authentication based upon knowledge or an authenticating item (e.g., a password, a token, etc.) is insufficient because an entity, different from the entities associated with the record of data, can obtain the knowledge (e.g., password) or possession of the authenticating item (e.g., token). Although authentication based upon an inherence factor (e.g., a biometric identifier) can prevent such an entity from authenticating a record of data, such a technique still does not ensure that the entity performing the authentication of the record of data does so with correct knowledge of a subject matter of the record of data.

[0011] The disclosed technologies can prevent an incorrect copy of a record of data from being transmitted to a distributed ledger system. A first file can be received. The first file can include information, in audio form or video form, with: (1) a description of a subject matter of the record of data and (2) an authorization to cause a copy of the record of data to be transmitted to the distributed ledger system. The first file can be sent to a device. A second file can be received from the device. The second file can include information that confirms that: (1) the description of the subject matter, included in the first file, is correct, and (2) an entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the distributed ledger system. The correct copy of the record of data can be caused, based on a receipt of the first file and the second file, to be transmitted to the distributed ledger system.

[0012] FIG. 1 is a diagram illustrating an example of an environment 100 for preventing a transmission of an incorrect copy of a record of data to an electronic network 102, according to the disclosed technologies. The environment 100 can include, for example, the electronic network 102 and a system 104 for preventing transmission of an incorrect copy of a record of data to the electronic network 102. The record of data can be associated with an item for which an authentication of a copy is important. For example, the record of data can be associated with a transaction, a will or testament, a document related to a quality assurance program, a document to be used as evidence in a judicial proceeding, or the like. The electronic network 102 can include a distributed ledger system. If the record of data is associated with a transaction, then, additionally or alternatively, the electronic network 102 can include one or more of an Automated Clearing House network, a payment rail network, another electronic ledger system, or the like. If the electronic network 102 is a distributed ledger system, then the record of data can be included, by the distributed ledger system, in a block to be added, by the distributed ledger system, to a blockchain.

[0013] Optionally, the system 104 can be configured to receive 106a a copy of the record of data from a device 108a associated with a second entity. Alternatively and optionally, the system 104 can be configured to receive 110 the copy of the record of data from a device 112. The device 112 can be different from the device 108a associated with the second entity. For

example, if the record of data is associated with a transaction, the device 112 can be associated with one of the entities associated with the transaction.

[0014] The system 104 can be configured to receive 114a a first file. For example, the system 104 can be configured to receive 114a the first file from the device 108a associated with the second entity. The first file can include a first information. The first information can be in audio form or video form. The first information can include a description of a subject matter of the record of data. The first information can include an authorization to cause the copy of the record of data to be transmitted to the electronic network 102. The second entity can be an individual or an organization. For example, the first information can be a video or audio recording, produced under a control of the second entity, that states, "This is Bob Smith, chief financial officer of Bigco. I hereby authorize the transfer of $7 million from the Bigco account with Empire State Bank to the account that Upstart has with First National Bank."

[0015] In a first optional implementation of the disclosed technologies, the description of the subject matter can be required to include one or more specific words or phrases. For example, if this first optional implementation requires the use of the word "authorize," then a video or audio recording that states, "This is Bob Smith, chief financial officer of Bigco. I hereby approve the transfer of $7 million from the Bigco account with Empire State Bank to the account that Upstart has with First National Bank." can be a reason to treat the first information as not including an authorization to cause the copy of the record of data to be transmitted to the electronic network 102. For example, it is possible that Bob Smith misspoke his statement. Alternatively, it is possible that Bob Smith deliberately spoke the word "approve" so that the first information would be treated as not including an authorization to cause the copy of the record of data to be transmitted to the electronic network 102. For example, Bob Smith may have been under duress because he was compelled to make the video or audio recording.

[0016] Optionally, the system 104 can be configured to determine a type of the subject matter of the record of data. For example, the system 104 can be configured to determine that the type of the subject matter of the record of data is "a withdrawal of funds from the Bigco account with Empire State Bank."

[0017] Optionally, the system 104 can be configured to determine an identity of the second entity. For example, the system 104 can be configured to determine that Bob Smith is the identity of the second entity. For example, the system 104 can be configured to determine the identity of the second entity from an identity of the device 108a associated with the second entity. Additionally or alternatively, the system 104 can be configured to determine the identity of the second entity by analyzing the first information to determine the identity of the second entity. For example, the system 104 can be configured to use image data processing techniques, face recognition techniques, audio data processing techniques, voice recognition techniques, the like, or some combination of the foregoing to determine the identity of the second entity.

[0018] Optionally, the system 104 can be configured to determine, based on the identity and the type of the subject matter, that the second entity has permission to cause the copy of the record of data to be transmitted to the electronic network 102. For example, the system 104 can be configured to determine, based on: (1) the identity of the second entity being Bob Smith and (2) the type of the subject matter of the file of software being "a withdrawal of funds from the Bigco account with Empire State Bank," that Bob Smith has permission to cause the copy of the record of data (in which the type of the subject matter is "a withdrawal of funds from the Bigco account with Empire State Bank") to be transmitted to the electronic network 102. For example, if the type of the subject matter was "a withdrawal of funds from the Bigco account with Pension Management Corporation" (the company that manages the pension funds of the employees of Bigco), then the system 104 can be configured to determine, based on the identity and the type of the subject matter, that the second entity does not have permission to cause the copy of the record of data to be transmitted to the electronic network 102.

[0019] Optionally, the system 104 can be configured to determine, based on the type of the subject matter, a device 116a associated with a first entity. The first entity can be an individual or an organization. For example, the system 104 can be configured to determine, based on the type of the subject matter of the file of software being "a withdrawal of funds from the Bigco account with Empire State Bank," that the device 116a associated with the first entity should be a device associated with Alice Jones, comptroller of Bigco.

[0020] The system 104 can be configured to send 118a the first file to the device 116a associated with the first entity.

[0021] The system 104 can be configured to receive 120a, from the device 116a associated with the first entity, a second file. The second file can include a second information. The second information can confirm that the description of the subject matter, included in the first file, is correct. For example, the second information can confirm that the description of the subject matter of the record of data ("the transfer of $7 million from the Bigco account with Empire State Bank to the account that Upstart has with First National Bank"), included in the first file, is correct. Optionally, the second information can be in audio form or video form.

[0022] The system 104 can be configured to receive 122a, from the device 116a associated with the first entity, a third file. The third file can include a third information. The third information can confirm that the second entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the electronic network 102. For example, the third information can confirm that the second entity (Bob Smith), which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the electronic network 102. Optionally, the third information can be in audio form or video form.

[0023] In a second optional implementation of the disclosed technologies, both the second file and the third file can be included in a combined file. The system 104 can be configured to receive the combined file.

[0024] Optionally, the system 104 can be configured to receive, from the device 116a associated with the first entity, a digital signature. The digital signature can identity the first entity. In a third optional implementation of the disclosed technologies, the digital signature can include a hash of the first file. For example, including the hash of the first file in the digital signature can provide confirmation that the first file, and not another file, was reviewed by the first entity.

[0025] Optionally, the system 104 can be configured to reference a digital certificate to confirm the digital signature. The digital certificate can provide an indication that the first entity is authorized to review the first file.

[0026] Optionally, in a fourth optional implementation of the disclosed technologies, the device 116a associated with the first entity can be a plurality of devices. A count of the plurality of devices can be a first number. The first entity can be a plurality of first entities. A count of the plurality of first entities can be a second number. The first number can be equal to the second number. Alternatively, the first number can be different from the second number. That is, more than one entity can be associated with the same device, or more than one device can be associated with the same entity. The second file can be a plurality of second files. A count of the plurality of second files can be a third number. The third file can be a plurality of third files. A count of the plurality of third files can be a fourth number. The third number can be equal to the fourth number. Alternatively, the third number can be different from the fourth number. That is, the system 104 may receive more second files than third files, or more third files than second files.

[0027] For example, the plurality of devices can include the device 116a, a device 116b, and a device 116c. For example, the device 116a can be associated with Alice Jones, comptroller of Bigco; the device 116b can be associated with Charlie Sanders, an accounts payable accountant at Bigco; and the device 116c can be associated with Dave Porter, a staff accountant at Bigco. The system 104 can be configured to send 118a the first file to the device 116a, to send 118b the first file to the device 116b, and to send 118c the first file to the device 116c. The system 104 can be configured to receive 120a, from the device 116a, a first second file, to receive 120b, from the device 116b, a second second file, and to receive 120c, from the device 116c, a third second file. The system 104 can be configured to receive 122a, from the device 116a, a first third file, to receive 122b, from the device 116b, a second third file, and to receive 122c, from the device 116c, a third third file.

[0028] Optionally, in the fourth optional implementation, the system 104 can be configured to determine that the third number is greater than a threshold. That is, the number of second files that the system 104 receives is greater than a threshold. For example, if the threshold is two and

the system 104 receives second files from the device 104a, the device 104b, and the device 104c, then the system 104 can determine that the number of second files received is greater than the threshold.

[0029] Optionally, in the fourth optional implementation, the system 104 can be further configured to determine that the fourth number is greater than the threshold. That is, the number of third files that the system 104 receives is also greater than the threshold. For example, if the threshold is two and the system 104 receives third files from the device 104a, the device 104b, and the device 104c, then the system 104 can determine that the number of third files received is greater than the threshold.

[0030] Optionally, in a fifth optional implementation of the disclosed technologies, the first file can be a plurality of first files. A count of the plurality of first files can be a first number. That is, in one or more situations more than one first file may need to be received by the system 104 and reviewed by the second entity in order to authorize causing the copy of the record of data to be transmitted to the electronic network 102. The second file can be a plurality of second files. A count of the plurality of second files can be a second number. The third file can be a plurality of third files. A count of the plurality of third files can be a third number. The second number can be equal to the third number. Alternatively, the second number can be different from the third number. That is, the system 104 may receive more second files than third files, or more third files than second files.

[0031] The plurality of first files can be received from a plurality of devices associated with one or more second entities. For example, the plurality of devices associated with the one or more second entities can include the device 108a and a device 108b. For example, the device 108a can be associated with Bob Smith, chief financial officer of Bigco; and the device 108b can be associated with Ellen Johnson, account manager for the Upstart account at Bigco. For example, the system 104 can be configured to receive 114a a first first file from the device 108a and to receive 114b a second first file from the device 108b.

[0032] Optionally, in the fifth optional implementation, the system 104 can be configured to determine that the second number is greater than a threshold and that the third number is greater than the threshold. That is, the number of second files and the number of third files that the

system 104 receives is greater than the threshold. For example, if the threshold is one and the system 104 receives, from the device 116a: (1) a second file and a third file for the first file produced under the control of Bob Smith and (2) a second file and a third file for the first file produced under the control of Ellen Johnson, then the system 104 can determine that the number of second files received is greater than the threshold and that the number of third files received is greater than the threshold.

[0033] Optionally, in a sixth optional implementation of the disclosed technologies, the system 104 can be configured to cause, based on a receipt of the first file, the second file, and the third file, a digital signature to be associated with the copy of the record of data. For example, the digital signature can provide confirmation that: (1) the copy of the record of data has been authorized to be transmitted to the electronic network 102 and (2) the entity that authorized the copy of the record of data to be transmitted to the electronic network 102 has permission for such an authorization.

[0034] Optionally, in a seventh optional implementation of the disclosed technologies, the system 104 can be configured to cause one or more of the first file, the second file, or the third file to be stored 124 in a retrieval system 126. In this manner, these files can be available for future review.

[0035] Optionally, in the seventh optional implementation, the system 104 can be configured to cause a digital certificate to be associated with the first file. The digital certificate can provide an indication that the first file has been stored 124 in the retrieval system 126.

[0036] Optionally, in an eighth optional implementation of the disclosed technologies, the system 104 can be configured to send 128 one or more of the second file or the third file to a device 130 associated with a third entity. The third entity can be an individual or an organization. For example, the device 130 can be associated with Fran Dunlop, a quality assurance specialist at Bigco.

[0037] Optionally, in the eighth optional implementation, the system 104 can be configured to receive 132, from the device 130 associated with the third entity, a fourth file. The fourth file can include a fourth information. The fourth information can confirm that the first entity, which

controlled production of the one or more of the second file or the third file, has permission to approve an authenticity of the first file, Optionally, the fourth information can be in audio form or video form.

[0038] The system 104 can be configured to cause, based on a receipt of the first file, the second file, and the third file, the copy of the record of data to be transmitted 134 to the electronic network 102. Optionally, the system 104 can be configured to cause the copy of the record of data to be transmitted 134 to the electronic network 102 by sending 136 the copy of the record of data to a remote device 138. The copy of the record of data can be transmitted 140 to the electronic network 102 by the remote device 138.

[0039] The system 104 can be configured to prevent, based on a lack of the receipt of one or more of the first file, the second file, or the third file, the transmission of the copy of the record of data to the electronic network 102.

[0040] If the system 104 is in the fourth optional implementation, then: (1) the system 104 can be configured to cause the copy of the record of data to be transmitted to the electronic network 102 further based on the third number being greater than the threshold and (2) the system 104 can be configured to prevent the transmission of the copy of the record of data based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, or the third number being less than or equal to the threshold.

[0041] If, in the fourth optional implementation, the system 104 is further configured to determine that the fourth number is greater than the threshold, then: (1) the system 104 can be further configured to cause the copy of the record of data to be transmitted to the electronic network 102 further based on the fourth number being greater than the threshold and (2) the system 104 can be configured to prevent the transmission of the copy of the record of data based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

[0042] If the system 104 is in the fifth optional implementation, then: (1) the system 104 can be configured to cause the copy of the record of data to be transmitted to the electronic network

102 further based on the third number being greater than the threshold and the fourth number being greater than the threshold and (2) the system 104 can be configured to prevent the transmission of the copy of the record of data based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

[0043] If the system 104 is in the sixth optional implementation, then: (1) the system 104 can be configured to cause the copy of the record of data to be transmitted to the electronic network 102 further based on the digital signature being associated with the copy of the record of data and (2) the system 104 can be configured to prevent the transmission of the copy of the record of data based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, or a lack of the digital signature being associated with the copy of the record of data.

[0044] If the system 104 is in the eighth optional implementation, then: (1) the system 104 can be configured to cause the copy of the record of data to be transmitted to the electronic network 102 further based on a receipt of the fourth file and (2) the system 104 can be configured to prevent the transmission of the copy of the record of data based on one or more of the lack of the receipt of one or more of the first file, the second file, the third file, or the fourth file.

[0045] FIGS. 2A through 2I are a flow diagram illustrating an example of a method 200 for preventing a transmission of an incorrect copy of a record of data to an electronic network, according to the disclosed technologies. For example, the record of data can be associated with a transaction, a will or testament, a document related to a quality assurance program, a document to be used as evidence in a judicial proceeding, or the like. The electronic network can include a distributed ledger system. If the record of data is associated with a transaction, then, additionally or alternatively, the electronic network can include one or more of an Automated Clearing House network, a payment rail network, another electronic ledger system, or the like. If the electronic network is a distributed ledger system, then the record of data can be included, by the distributed ledger system, in a block to be added, by the distributed ledger system, to a blockchain.

[0046] With reference to FIG. 2A, in the method 200, at an optional operation 202, a copy of the record of data can be received from a device associated with a second entity. Alternatively, at an optional operation 204, the copy of the record of data can be received from a device other than a device associated with the second entity.

[0047] At an operation 206, a first file can be received. The first file can include a first information. The first information can be in audio form or video form. The first information can include a description of a subject matter of the record of data. The first information can include an authorization to cause the copy of the record of data to be transmitted to the electronic network. In a first optional implementation of the disclosed technologies, the description of the subject matter can be required to include one or more specific words or phrases.

[0048] At an optional operation 208, a type of the subject matter of the record of data can be determined.

[0049] At an optional operation 210, an identity of the second entity can be determined. For example, the identity of the second entity can be determined from an identity of the device associated with the second entity. Additionally or alternatively, the identity of the second entity can be determined by analyzing the first information to determine the identity of the second entity. For example, the identity of the second entity can be determined using image data processing techniques, face recognition techniques, audio data processing techniques, voice recognition techniques, the like, or some combination of the foregoing.

[0050] At an optional operation 212, a state that the second entity has permission to cause the copy of the record of data to be transmitted to the electronic network can be determined based on the identity of the second entity and the type of the subject matter of the record of data.

[0051] At an optional operation 214, a device associated with a first entity can be determined based on the type of the subject matter of the record of data.

[0052] With reference to FIG. 2B, at an operation 216, the first file can be sent to the device associated with the first entity.

[0053] At an operation 218, a second file can be received from the device associated with the first entity. The second file can include a second information. The second information can confirm that the description of the subject matter, included in the first file, is correct. Optionally, the second information can be in audio form or video form.

[0054] At an operation 220, a third file can be received from the device associated with the first entity. The third file can include a third information. The third information can confirm that the second entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the electronic network. Optionally, the third information can be in audio form or video form.

[0055] In a second optional implementation of the disclosed technologies, both the second file and the third file can be included in a combined file so that operation 218 and operation 220 can be combined.

[0056] With reference to FIG. 2C, at an optional operation 222, a digital signature can be received from the device associated with the first entity. The digital signature can identity the first entity. In a third optional implementation of the disclosed technologies, the digital signature can include a hash of the first file. For example, including the hash of the first file in the digital signature can provide confirmation that the first file, and not another file, was reviewed by the first entity.

[0057] At an optional operation 224, a digital certificate can be referenced to confirm the digital signature. The digital certificate can provide an indication that the first entity is authorized to review the first file.

[0058] Optionally, in a fourth optional implementation of the disclosed technologies, the device associated with the first entity can be a plurality of devices. A count of the plurality of devices can be a first number. The first entity can be a plurality of first entities. A count of the plurality of first entities can be a second number. The first number can be equal to the second number. Alternatively, the first number can be different from the second number. That is, more than one entity can be associated with the same device, or more than one device can be associated with the same entity. The second file can be a plurality of second files. A count of

the plurality of second files can be a third number. The third file can be a plurality of third files. A count of the plurality of third files can be a fourth number. The third number can be equal to the fourth number. Alternatively, the third number can be different from the fourth number. That is, more second files than third files can be received, or more third files than second files can be received.

[0059] With reference to FIG. 2D, in the fourth optional implementation, at an optional operation 226, the third number can be determined to be greater than a threshold. That is, the number of second files received is greater than a threshold.

[0060] In the fourth optional implementation, at an optional operation 228, the fourth number can be determined to be greater than the threshold. That is, the number of third files received is greater than the threshold.

[0061] Optionally, in a fifth optional implementation of the disclosed technologies, the first file can be a plurality of first files. A count of the plurality of first files can be a first number. The plurality of first files can be received from a plurality of devices associated with the second entity. That is, in one or more situations more than one first file may need to be received and reviewed by the second entity in order to authorize causing the copy of the record of data to be transmitted to the electronic network. The second file can be a plurality of second files. A count of the plurality of second files can be a second number. The third file can be a plurality of third files. A count of the plurality of third files can be a third number. The second number can be equal to the third number. Alternatively, the second number can be different from the third number. That is, more second files than third files can be received, or more third files than second files can be received.

[0062] With reference to FIG. 2E, in the fifth optional implementation, at an optional operation 230, the second number can be determined to be greater than a threshold. That is, the number of second files received is greater than a threshold.

[0063] In the fifth optional implementation, at an optional operation 232, the third number can be determined to be greater than the threshold. That is, the number of third files received is greater than the threshold.

[0064] With reference to FIG. 2F, in a sixth optional implementation of the disclosed technologies, at an optional operation 234, a digital signature can be caused, based on a receipt of the first file, the second file, and the third file, to be associated with the copy of the record of data. For example, the digital signature can provide confirmation that: (1) the copy of the record of data has been authorized to be transmitted to the electronic network and (2) the entity that authorized the copy of the record of data to be transmitted to the electronic network has permission for such an authorization.

[0065] With reference to FIG. 2G, in a seventh optional implementation of the disclosed technologies, at an optional operation 236, one or more of the first file, the second file, or the third file can be caused to be stored in a retrieval system. In this manner, these files can be available for future review.

[0066] In the seventh optional implementation, at an optional operation 238, a digital certificate can be caused to be associated with the first file. The digital certificate can provide an indication that the first file has been stored in the retrieval system.

[0067] With reference to FIG. 2H, in an eighth optional implementation of the disclosed technologies, at an optional operation 240, one or more of the second file or the third file can be sent to a device associated with a third entity.

[0068] In the eighth optional implementation, at an optional operation 242, a fourth file can be received from the device associated with the third entity. The fourth file can include a fourth information. The fourth information can confirm that the first entity, which controlled production of the one or more of the second file or the third file, has permission to approve an authenticity of the first file, Optionally, the fourth information can be in audio form or video form.

[0069] With reference to FIG. 2I, at an operation 244, the copy of the record of data can be caused, based on a receipt of the first file, the second file, and the third file, to be transmitted to the electronic network. Optionally, the copy of the record of data can be transmitted to the electronic network by sending the copy of the record of data to a remote device. The copy of the record of data can be transmitted to the electronic network by the remote device.

[0070] At an operation 246, the transmission of the copy of the record of data to the electronic network can be prevented based on a lack of the receipt of one or more of the first file, the second file, or the third file.

[0071] If operations in the method 200 are performed according to the fourth optional implementation, then: (1) the copy of the record of data can be caused to be transmitted to the electronic network further based on the third number being greater than the threshold and (2) the transmission of the copy of the record of data to the electronic network can be prevented based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, or the third number being less than or equal to the threshold.

[0072] If operations in the method 200 performed according to the fourth optional implementation include determining that the fourth number is greater than the threshold, then: (1) the copy of the record of data can be caused to be transmitted to the electronic network further based on the fourth number being greater than the threshold and (2) the transmission of the copy of the record of data to the electronic network can be prevented based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

[0073] If operations in the method 200 are performed according to the fifth optional implementation, then: (1) the copy of the record of data can be caused to be transmitted to the electronic network further based on the third number being greater than the threshold and the fourth number being greater than the threshold and (2) the transmission of the copy of the record of data to the electronic network can be prevented based on one or more of the lack of the receipt of one or more of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

[0074] If operations in the method 200 are performed according to the sixth optional implementation, then: (1) the copy of the record of data can be caused to be transmitted to the electronic network further based on the digital signature being associated with the copy of the record of data and (2) the transmission of the copy of the record of data to the electronic network can be prevented based on one or more of the lack of the receipt of one or more of the first file,

the second file, or the third file, or a lack of the digital signature being associated with the copy of the record of data.

[0075] If operations in the method 200 are performed according to the eighth optional implementation, then: (1) the copy of the record of data can be caused to be transmitted to the electronic network further based on a receipt of the fourth file and (2) the transmission of the copy of the record of data to the electronic network can be prevented based on the lack of the receipt of one or more of the first file, the second file, the third file, or the fourth file.

[0076] In general, in light of the technologies described above, one of skill in the art understands that technologies to prevent transmission of an incorrect copy of a record of data to an electronic network can include any combination of some or all of the foregoing configurations.

[0077] Configurations of the disclosed technologies may be implemented in and used with a variety of component and network architectures. FIG. 3 illustrates an example computing device 20 suitable for implementing configurations of the disclosed technologies. The device 20 can be, for example, a desktop or laptop computer, or a mobile computing device such as a smart phone, tablet, or the like. The device 20 can include a bus 21 (which can interconnect major components of the computer 20, such as a central processor 24), a memory 27 (such as random-access memory (RAM), read-only memory (ROM), flash RAM, or the like), a user display 22 (such as a display screen), a user input interface 26 (which can include one or more controllers and associated user input devices such as a keyboard, mouse, touch screen, and the like), a fixed storage 23 (such as a hard drive, flash storage, and the like), a removable media component 25 (operative to control and receive an optical disk, flash drive, and the like), and a network interface 29 operable to communicate with one or more remote devices via a suitable network connection.

[0078] The bus 21 can allow data communication between the central processor 24 and one or more memory components, which can include RAM, ROM, and other memory, as previously noted. Typically RAM can be the main memory into which an operating system and application programs are loaded. A ROM or flash memory component can contain, among other code, the basic input-output system (BIOS) which can control basic hardware operation such as the

interaction with peripheral components. Applications resident with the computer 20 can generally be stored on and accessed via a computer readable medium, such as a hard disk drive (e.g., fixed storage 23), an optical drive, floppy disk, or other storage medium.

[0079] The fixed storage 23 can be integral with the computer 20 or can be separate and accessed through other interfaces. The network interface 29 can provide a direct connection to a remote server via a wired or wireless connection. The network interface 29 can provide such connection using any suitable technique and protocol as is readily understood by one of skill in the art, including digital cellular telephone, WiFi™, Bluetooth®, near-field, and the like. For example, the network interface 29 can allow the computer to communicate with other computers via one or more local, wide-area, or other communication networks, as described in further detail below.

[0080] Many other devices or components (not shown) can be connected in a similar manner (e.g., document scanners, digital cameras and so on). Conversely, all of the components illustrated in FIG. 3 need not be present to practice the disclosed technologies. The components can be interconnected in different ways from that illustrated. The operation of a computer such as that illustrated in FIG. 3 is readily known in the art and is not discussed in detail in this application. Code to implement the disclosed technologies can be stored in computer-readable storage media such as one or more of the memory 27, fixed storage 23, removable media 25, or on a remote storage location.

[0081] More generally, various configurations of the presently disclosed technologies can include or be realized in the form of computer-implemented processes and apparatuses for practicing those processes. Configurations also can be realized in the form of a computer program product having computer program code containing instructions embodied in non-transitory and/or tangible media, such as floppy diskettes, CD-ROMs, hard drives, universal serial bus (USB) drives, or any other machine readable storage medium, such that when the computer program code is loaded into and executed by a computer, the computer becomes an apparatus for practicing configurations of the disclosed technologies. Configurations also can be realized in the form of computer program code, for example, whether stored in a storage medium, loaded into and/or executed by a computer, or transmitted over some transmission

medium, such as over electrical wiring or cabling, through fiber optics, or via electromagnetic radiation, such that when the computer program code is loaded into and executed by a computer, the computer becomes an apparatus for practicing configurations of the disclosed technologies. When implemented on a general-purpose microprocessor, the computer program code segments configure the microprocessor to create specific logic circuits.

[0082] In some configurations, a set of computer-readable instructions stored on a computer-readable storage medium can be implemented by a general-purpose processor, which can transform the general-purpose processor or a device containing the general-purpose processor into a special-purpose device configured to implement or carry out the instructions. Configurations can be implemented using hardware that can include a processor, such as a general purpose microprocessor and/or an application-specific integrated circuit (ASIC) that embodies all or part of the techniques according to configurations of the disclosed technologies in hardware and/or firmware. The processor can be coupled to memory, such as RAM, ROM, flash memory, a hard disk or any other device capable of storing electronic information. The memory can store instructions adapted to be executed by the processor to perform the techniques according to configurations of the disclosed technologies.

[0083] The foregoing description, for purpose of explanation, has been described with reference to specific configurations. However, the illustrative discussions above are not intended to be exhaustive or to limit configurations of the disclosed technologies to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The configurations were chosen and described in order to explain the principles of configurations of the disclosed technologies and their practical applications, to thereby enable others skilled in the art to utilize those configurations as well as various configurations with various modifications as may be suited to the particular use contemplated.

CLAIMS

1. A method for preventing a transmission of an incorrect copy of a record of data to a distributed ledger system, the method comprising:

receiving, by a processor, a first file, the first file including a first information, wherein the first information:

is in at least one of audio form or video form,

includes a description of a subject matter of the record of data, and

includes an authorization to cause a copy of the record of data to be transmitted to the distributed ledger system;

sending, by the processor, the first file to a device associated with a first entity;

receiving, by the processor and from the device associated with the first entity, a second file, the second file including a second information, wherein the second information confirms that the description of the subject matter, included in the first file, is correct;

receiving, by the processor and from the device associated with the first entity, a third file, the third file including a third information, wherein the third information confirms that a second entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the distributed ledger system;

causing, by the processor and based on a receipt of the first file, the second file, and the third file, the copy of the record of data to be transmitted to the distributed ledger system; and

preventing, by the processor and based on a lack of the receipt of at least one of the first file, the second file, or the third file, the transmission of the copy of the record of data to the distributed ledger system.

2. The method of claim 1, wherein the record of data is associated with a transaction.

3. The method of claim 1, wherein the record of data is to be included, by the distributed ledger system, in a block to be added, by the distributed ledger system, to a blockchain.

4. The method of claim 1, wherein the receiving the second file and the receiving the third file comprise receiving a combined file, the combined file including the second file and the third file.

5. The method of claim 1, further comprising receiving, by the processor, the copy of the record of data from a device associated with the second entity.

6. The method of claim 1, further comprising receiving, by the processor, the copy of the record of data from a device other than a device associated with the second entity.

7. The method of claim 1, wherein at least one of the second information or the third information is in the at least one of audio form or video form.

8. The method of claim 1, further comprising:

determining, by the processor, a type of the subject matter of the record of data;

determining, by the processor, an identity of the second entity; and

determining, by the processor and based on the identity and the type of the subject matter, that the second entity has permission to cause the copy of the record of data to be transmitted to the distributed ledger system.

9. The method of claim 8, wherein the determining the identity of the second entity comprises analyzing the first information to determine the identity of the second entity.

10. The method of claim 1, further comprising:

determining, by the processor, a type of the subject matter of the record of data; and

determining, by the processor and based on the type of the subject matter, the device associated with the first entity.

11. The method of claim 1, further comprising:

receiving, by the processor and from the device associated with the first entity, a digital signature; and

referencing, by the processor, a digital certificate to confirm the digital signature.

12. The method of claim 11, wherein the digital signature includes a hash of the first file.

13. The method of claim 1, wherein:

the device associated with the first entity comprises a plurality of devices, a count of the plurality of devices being a first number;

the first entity comprises a plurality of first entities, a count of the plurality of first entities being a second number;

the second file comprises a plurality of second files, a count of the plurality of second files being a third number; and

the third file comprises a plurality of third files, a count of the plurality of third files being a fourth number.

14. The method of claim 13, further comprising determining, by the processor, that the third number is greater than a threshold, wherein:

the causing the copy of the record of data to be transmitted to the distributed ledger system is further based on the third number being greater than the threshold; and

the preventing the transmission of the copy of the record of data is based on at least one of the lack of the receipt of at least one of the first file, the second file, or the third file, or the third number being less than or equal to the threshold.

15. The method of claim 14, further comprising determining, by the processor, that the fourth number is greater than the threshold, wherein:

the causing the copy of the record of data to be transmitted to the distributed ledger system is further based on the fourth number being greater than the threshold; and

the preventing the transmission of the copy of the record of data is based on at least one of the lack of the receipt of at least one of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

16. The method of claim 1, wherein:

the first file comprises a plurality of first files, a count of the plurality of first files being a first number;

the second file comprises a plurality of second files, a count of the plurality of second files being a second number; and

the third file comprises a plurality of third files, a count of the plurality of third files being a third number.

17. The method of claim 16, further comprising:

determining, by the processor, that the second number is greater than a threshold; and

determining, by the processor, that the third number is greater than the threshold, wherein:

the causing the copy of the record of data to be transmitted to the distributed ledger system is further based on the third number being greater than the threshold and the fourth number being greater than the threshold; and

the preventing the transmission of the copy of the record of data is based on at least one of the lack of the receipt of at least one of the first file, the second file, or the third file, the third number being less than or equal to the threshold, or the fourth number being less than or equal to the threshold.

18. The method of claim 1, wherein the causing the copy of the record of data to be transmitted to the distributed ledger system comprises sending the copy of the record of data to a remote device, the copy of the record of data to be transmitted to the distributed ledger system by the remote device.

19. The method of claim 1, further comprising causing, by the processor and based on a receipt of the first file, the second file, and the third file, a digital signature to be associated with the copy of the record of data, wherein:

the causing the copy of the record of data to be transmitted to the distributed ledger system is further based on the digital signature being associated with the copy of the record of data; and

the preventing the transmission of the copy of the record of data is based on at least one of the lack of the receipt of at least one of the first file, the second file, or the third file, or a lack of the digital signature being associated with the copy of the record of data.

20. The method of claim 1, further comprising causing, by the processor, at least one of the first file, the second file, or the third file to be stored in a retrieval system.

21. The method of claim 20, further comprising causing, by the processor, a digital certificate to be associated with the first file, the digital certificate providing an indication that the first file has been stored in the retrieval system.

22. The method of claim 1, further comprising:

sending, by the processor, at least one of the second file or the third file to a device associated with a third entity; and

receiving, by the processor and from the device associated with the third entity, a fourth file, the fourth file including a fourth information, wherein the fourth information confirms that the first entity, which controlled production of the at least one of the second file or the third file, has permission to approve an authenticity of the first file,

wherein the causing the copy of the record of data to be transmitted to the distributed ledger system is further based on a receipt of the fourth file; and

the preventing the transmission of the copy of the record of data is based on the lack of the receipt of at least one of the first file, the second file, the third file, or the fourth file.

23. A non-transitory computer-readable medium storing computer code for controlling a processor to cause the processor to prevent a transmission of an incorrect copy of a record of data to a distributed ledger system, the computer code including instructions to cause the processor to:

receive a first file, the first file including a first information, wherein the first information:

is in at least one of audio form or video form,

includes a description of a subject matter of the record of data, and

includes an authorization to cause a copy of the record of data to be transmitted to the distributed ledger system;

send the first file to a device associated with a first entity;

receive, from the device associated with the first entity, a second file, the second file including a second information, wherein the second information confirms that the description of the subject matter, included in the first file, is correct;

receive, from the device associated with the first entity, a third file, the third file including a third information, wherein the third information confirms that a second entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the distributed ledger system;

cause, based on a receipt of the first file, the second file, and the third file, the copy of the record of data to be transmitted to the distributed ledger system; and

prevent, based on a lack of the receipt of at least one of the first file, the second file, or the third file, the transmission of the copy of the record of data to the distributed ledger system.

24. A system for preventing a transmission of an incorrect copy of a record of data to a distributed ledger system, the system comprising:

a memory configured to store a first file, a second file, and a third file; and

a processor configured to:

receive the first file, the first file including a first information, wherein the first information:

is in at least one of audio form or video form,

includes a description of a subject matter of the record of data, and

includes an authorization to cause a copy of the record of data to be transmitted to the distributed ledger system;

send the first file to a device associated with a first entity;

receive, from the device associated with the first entity, the second file, the second file including a second information, wherein the second information confirms that the description of the subject matter, included in the first file, is correct;

receive, from the device associated with the first entity, the third file, the third file including a third information, wherein the third information confirms that a second entity, which

controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the distributed ledger system;

cause, based on a receipt of the first file, the second file, and the third file, the copy of the record of data to be transmitted to the distributed ledger system; and

prevent, based on a lack of the receipt of at least one of the first file, the second file, or the third file, the transmission of the copy of the record of data to the distributed ledger system.

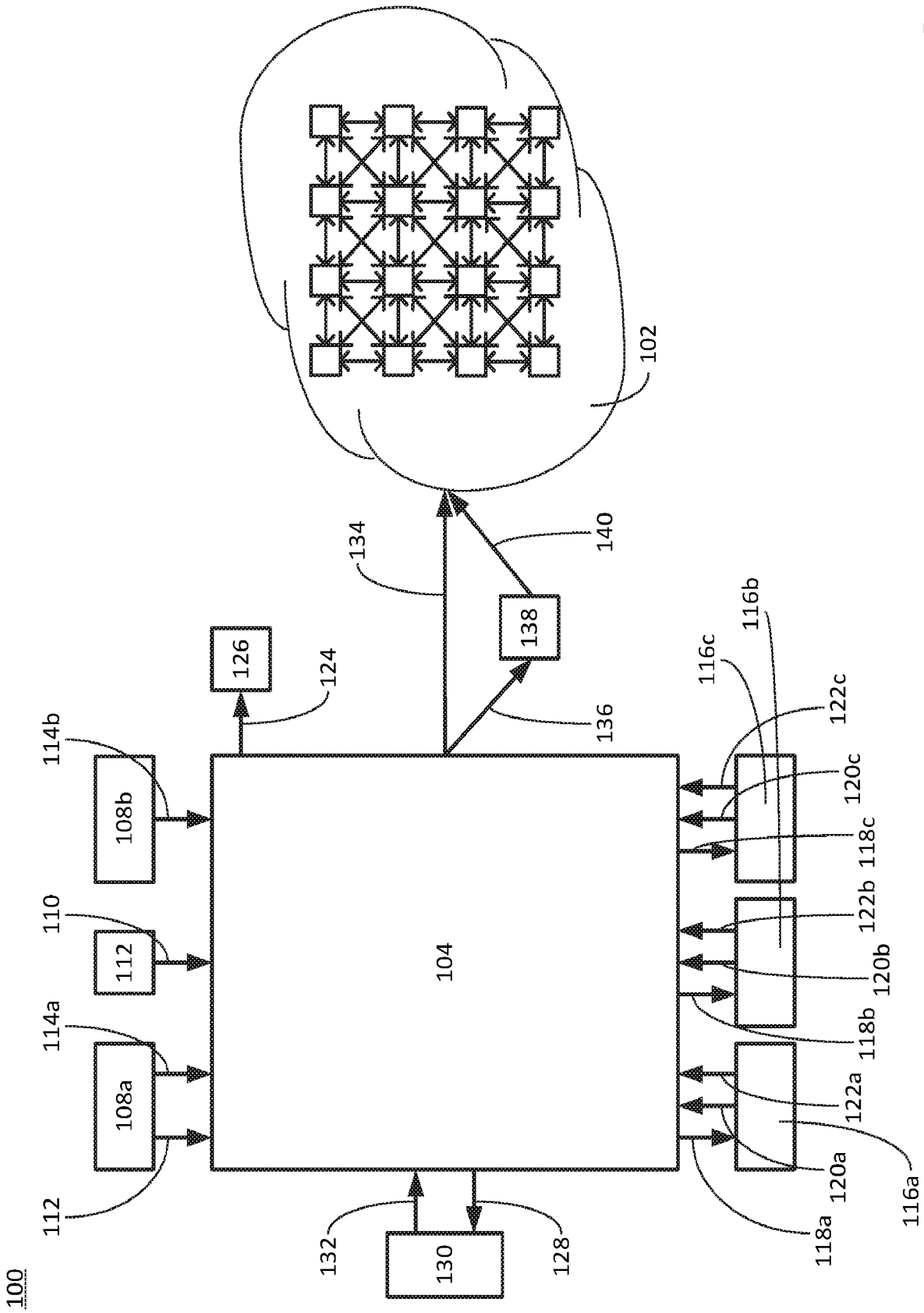
100
102
104
108a
108b
110
112
114a
114b
116a
116b
116c
118a
118b
118c
120a
120b
120c
122a
122b
122c
124
126
128
130
132
134
136
138
140

FIG. 1

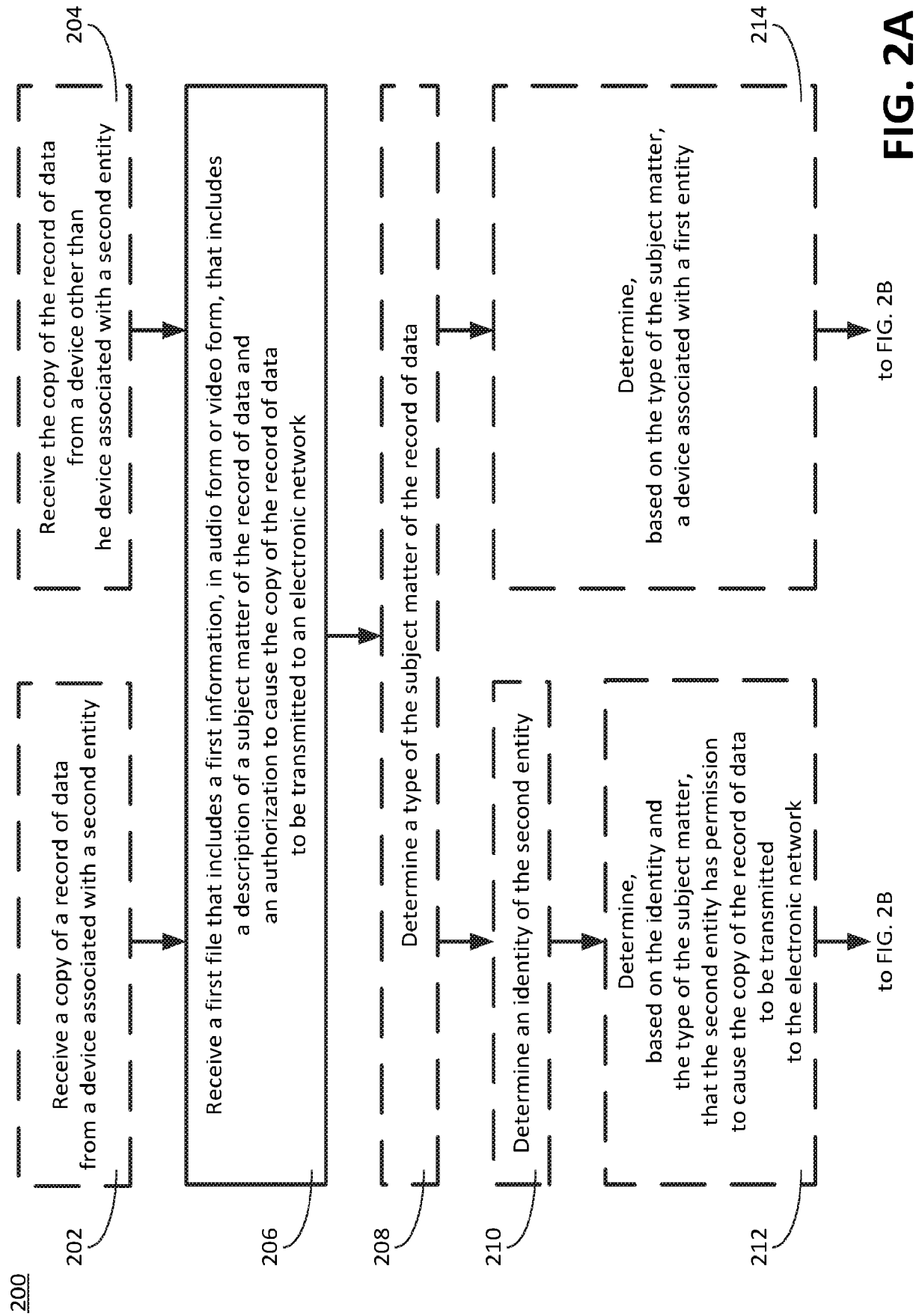
200
202
Receive a copy of a record of data from a device associated with a second entity
204
Receive the copy of the record of data from a device other than he device associated with a second entity
206
Receive a first file that includes a first information, in audio form or video form, that includes a description of a subject matter of the record of data and an authorization to cause the copy of the record of data to be transmitted to an electronic network
208
Determine a type of the subject matter of the record of data
210
Determine an identity of the second entity
212
Determine, based on the identity and the type of the subject matter, that the second entity has permission to cause the copy of the record of data to be transmitted to the electronic network
214
Determine, based on the type of the subject matter, a device associated with a first entity
to FIG. 2B
to FIG. 2B

FIG. 2A

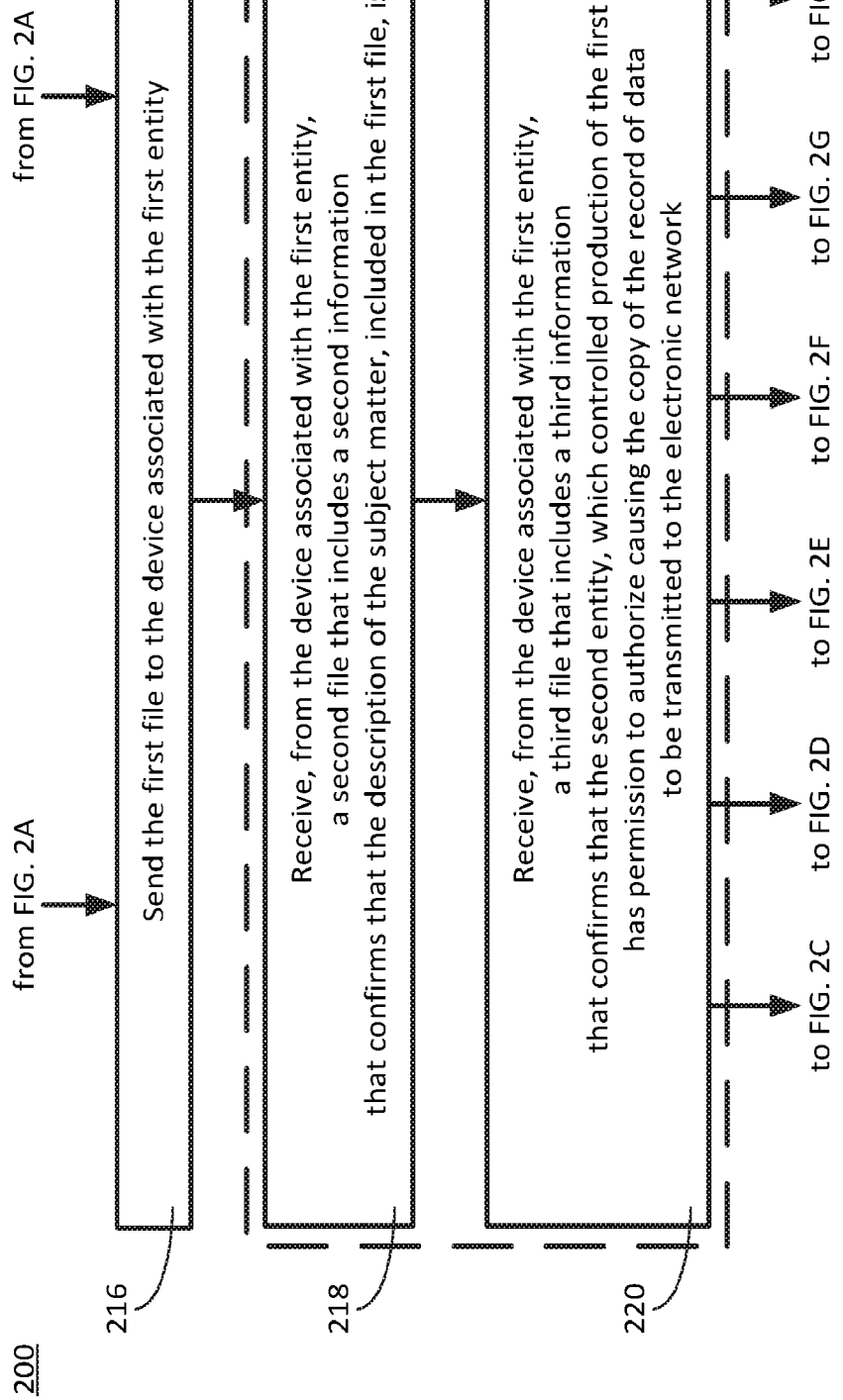
200
from FIG. 2A
from FIG. 2A
Send the first file to the device associated with the first entity
Receive, from the device associated with the first entity, a second file that includes a second information that confirms that the description of the subject matter, included in the first file, is correct
Receive, from the device associated with the first entity, a third file that includes a third information that confirms that the second entity, which controlled production of the first file, has permission to authorize causing the copy of the record of data to be transmitted to the electronic network
216
218
220
to FIG. 2C
to FIG. 2D
to FIG. 2E
to FIG. 2F
to FIG. 2G
to FIG. 2H

FIG. 2B

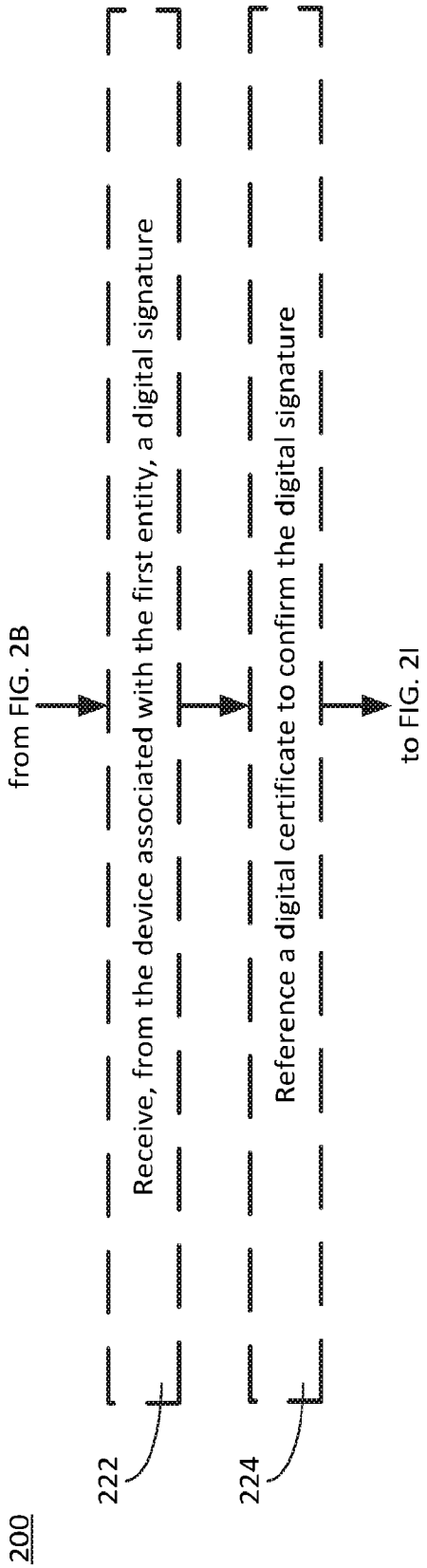
200
222
224
from FIG. 2B
Receive, from the device associated with the first entity, a digital signature
Reference a digital certificate to confirm the digital signature
to FIG. 2I

FIG. 2C

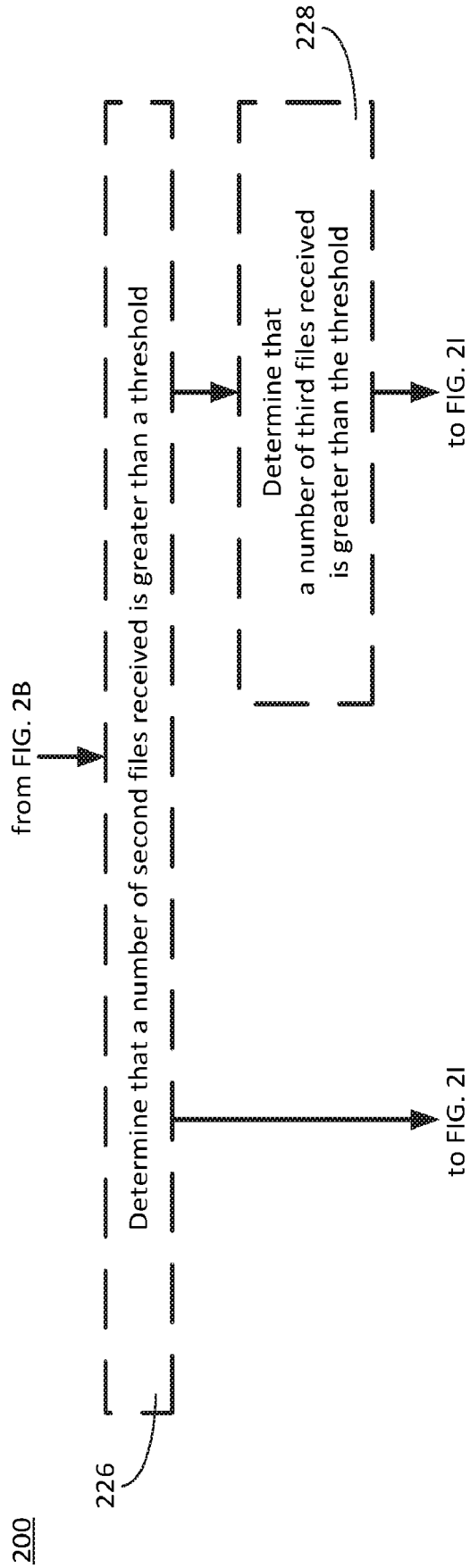
200
226
Determine that a number of second files received is greater than a threshold
228
Determine that a number of third files received is greater than the threshold
from FIG. 2B
to FIG. 2I
to FIG. 2I

FIG. 2D

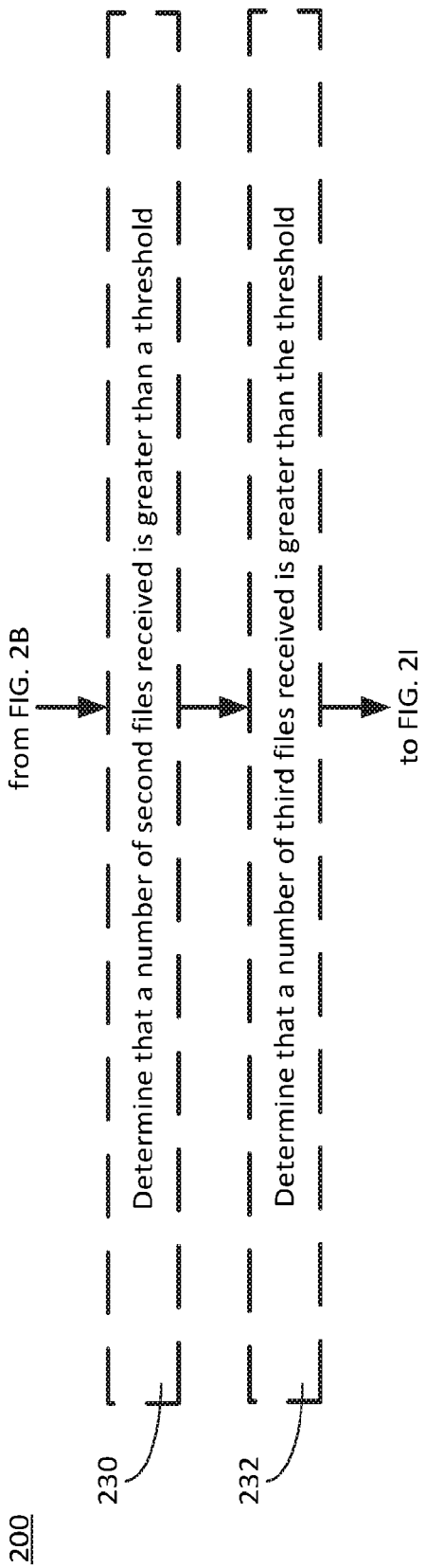
200
230
232
from FIG. 2B
Determine that a number of second files received is greater than a threshold
Determine that a number of third files received is greater than the threshold
to FIG. 2I

FIG. 2E

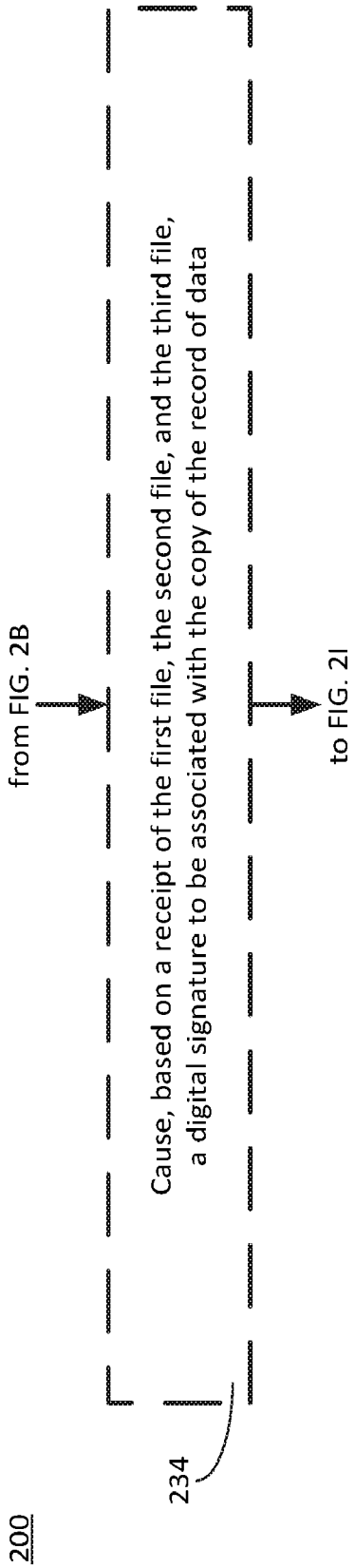
200
234
Cause, based on a receipt of the first file, the second file, and the third file, a digital signature to be associated with the copy of the record of data
from FIG. 2B
to FIG. 2I

FIG. 2F

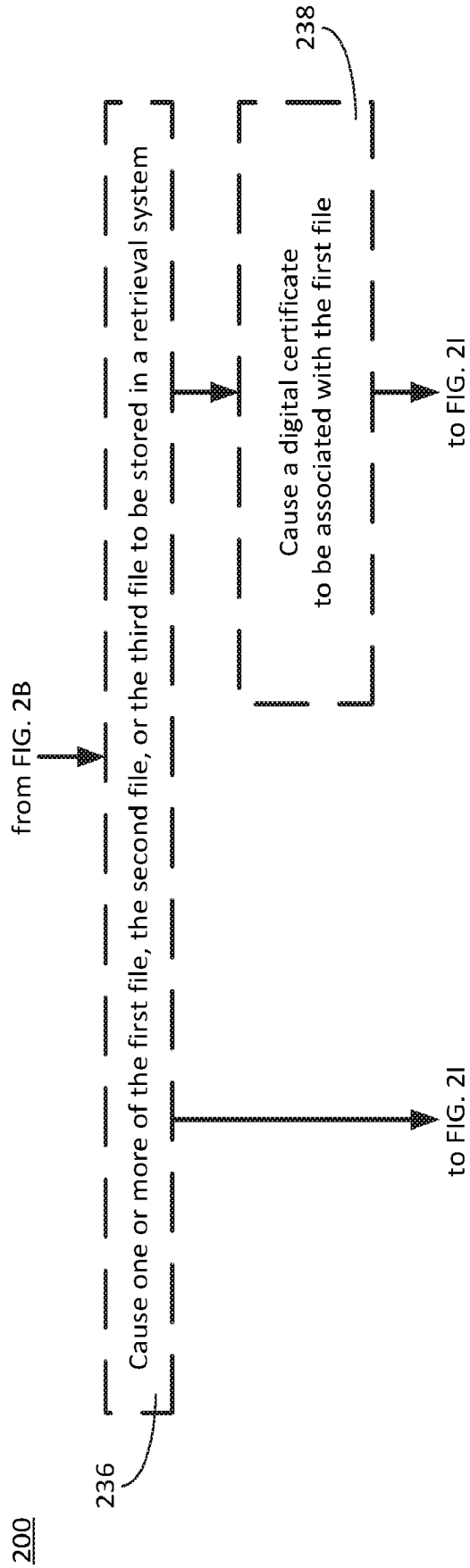
200
from FIG. 2B
236
Cause one or more of the first file, the second file, or the third file to be stored in a retrieval system
238
Cause a digital certificate to be associated with the first file
to FIG. 2I
to FIG. 2I

FIG. 2G

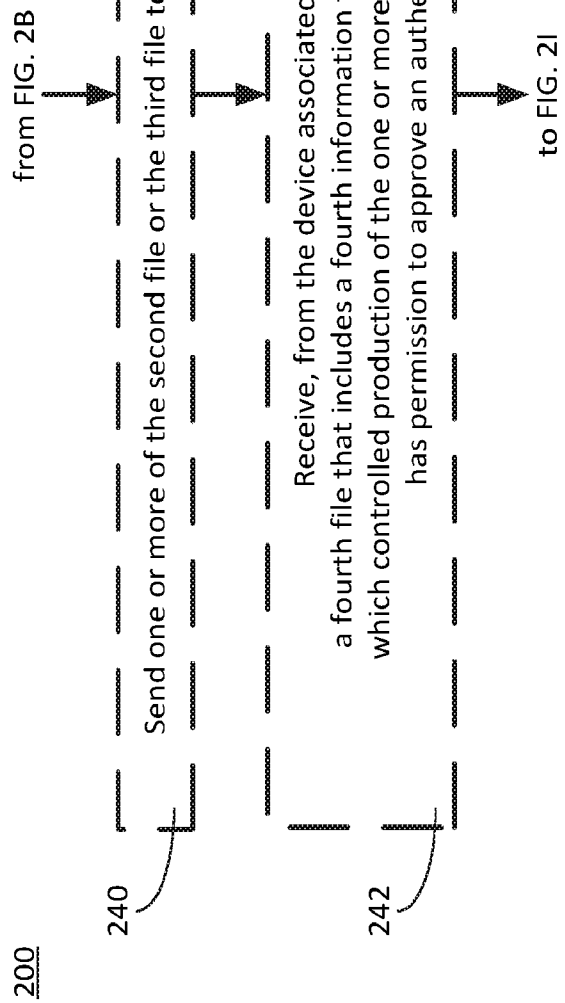
200
240
242
from FIG. 2B
Send one or more of the second file or the third file to a device associated with a third entity
Receive, from the device associated with the third entity, a fourth file that includes a fourth information that confirms that the first entity, which controlled production of the one or more of the second file or the third file, has permission to approve an authenticity of the first file
to FIG. 2I

FIG. 2H

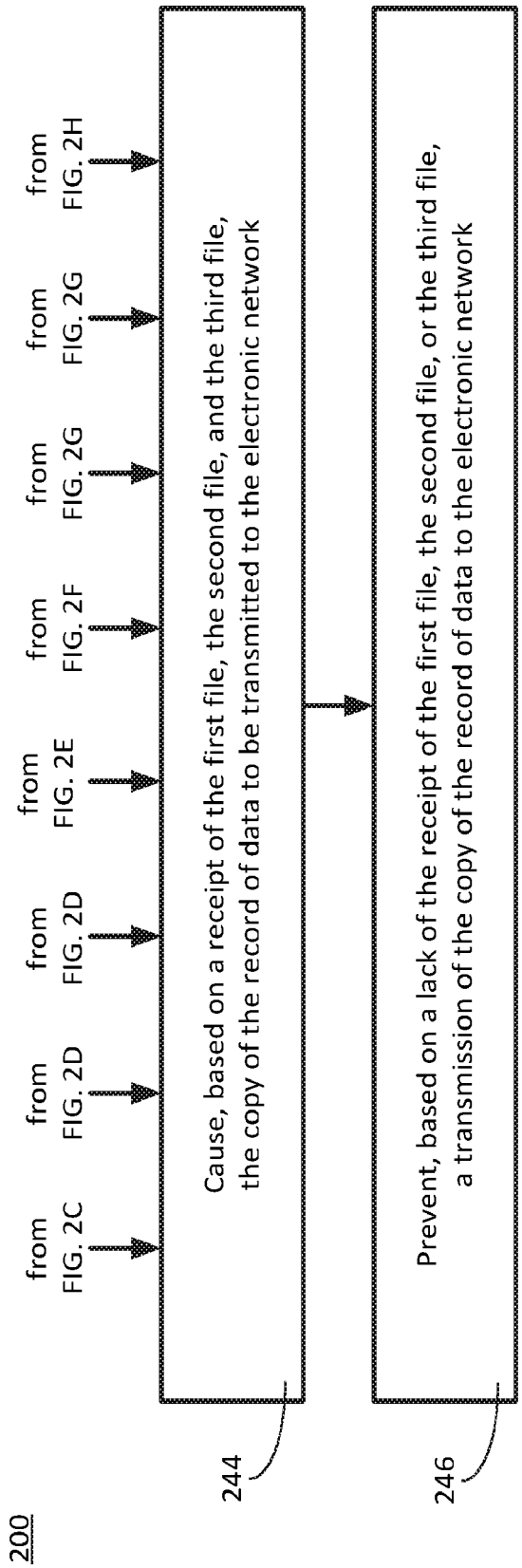
200
from FIG. 2C
from FIG. 2D
from FIG. 2D
from FIG. 2E
from FIG. 2F
from FIG. 2G
from FIG. 2G
from FIG. 2H
Cause, based on a receipt of the first file, the second file, and the third file, the copy of the record of data to be transmitted to the electronic network
244
Prevent, based on a lack of the receipt of the first file, the second file, or the third file, a transmission of the copy of the record of data to the electronic network
246

FIG. 2I

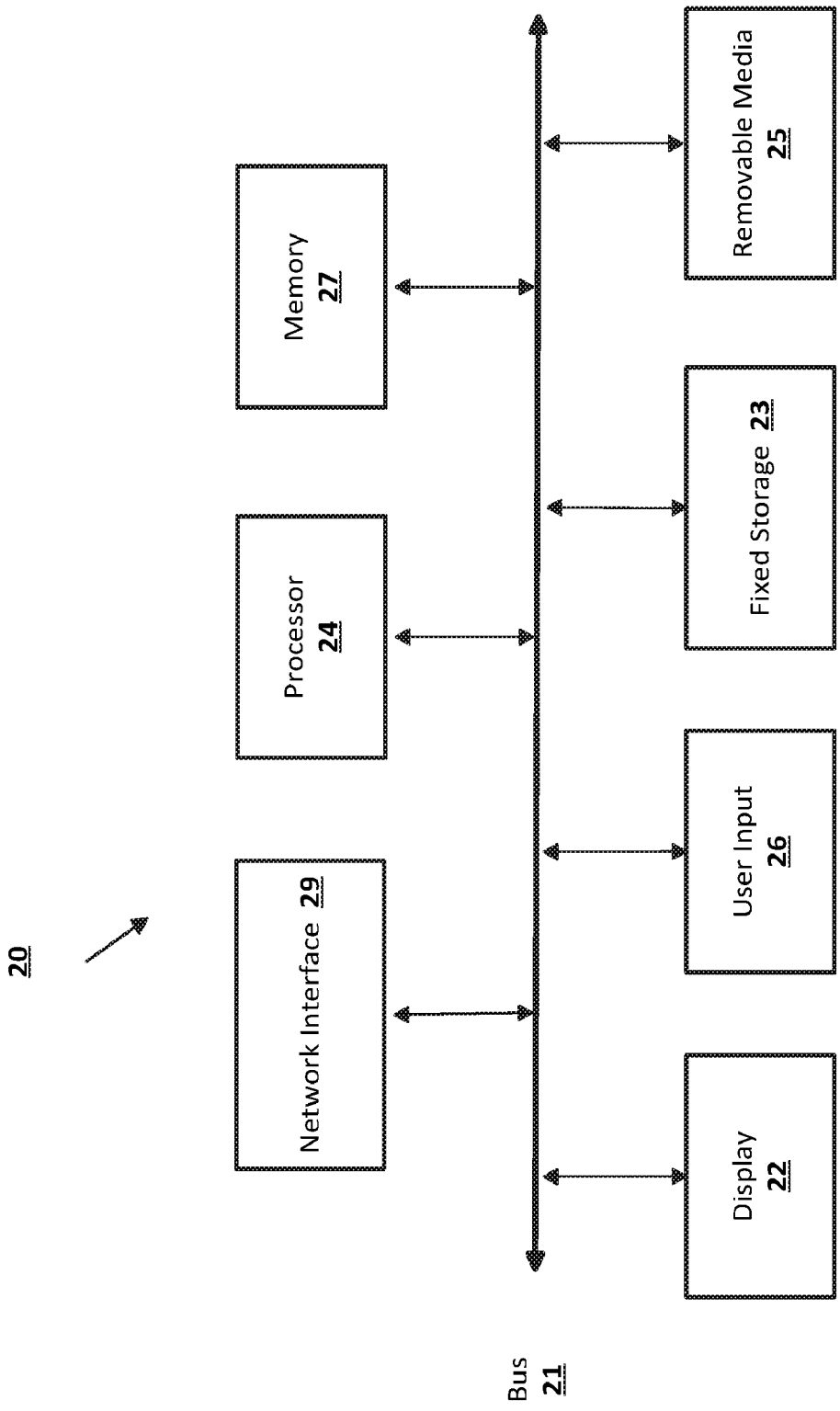
20
Network Interface 29
Processor 24
Memory 27
Display 22
User Input 26
Fixed Storage 23
Removable Media 25
Bus 21

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2019/068424

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i, H04L 9/06(2006.01)i, H04L 9/32(2006.01)i, H04L 29/08(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 9/08; G06F 17/30; G06Q 20/06; G06Q 20/08; G06Q 20/40; G06Q 40/02; H04L 13/18; H04L 29/06; H04N 21/6334; H04L 9/06; H04L 9/32; H04L 29/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: blockchain, distributed ledger, copy, transaction, audio, authorization, description

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017-0132625 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 11 May 2017 paragraphs [0019]-[0032] and claims 1, 11	1-24
A	US 2018-0315046 A1 (RAYMOND ANTHONY JOAO) 01 November 2018 claims 1, 3, 5	1-24
A	US 7769997 B2 (KEVIN STEWART DICK et al.) 03 August 2010 claims 1-16	1-24
A	KR 10-1880935 B1 (UBIVELOX INC.) 23 July 2018 paragraphs [0014]-[0039]	1-24
A	KR 10-1891734 B1 (ILCHE CO., LTD.) 24 August 2018 paragraphs [0025]-[0050] and claim 5	1-24

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 April 2020 (28.04.2020)	**28 April 2020 (28.04.2020)**

Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
BYUN, Sung Cheal
Telephone No. +82-42-481-8262

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2019/068424

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2017-0132625 A1	11/05/2017	CA 3004423 A1	11/05/2017
		CN 108292397 A	17/07/2018
		EP 3371759 A1	12/09/2018
		JP 2019-500675 A	10/01/2019
		MX 2018005594 A	01/08/2018
		SG 11201803751 A	28/06/2018
		WO 2017-079214 A1	11/05/2017
US 2018-0315046 A1	01/11/2018	US 2014-0372306 A1	18/12/2014
		US 2014-0372307 A1	18/12/2014
		US 2014-0372311 A1	18/12/2014
		US 2014-0372312 A1	18/12/2014
		US 2016-0086187 A1	24/03/2016
US 7769997 B2	03/08/2010	CA 2494948 A1	19/02/2004
		EP 1543648 A2	22/06/2005
		EP 1543648 B1	25/04/2012
		US 2003-0163704 A1	28/08/2003
		US 2005-0091540 A1	28/04/2005
		US 2005-0160095 A1	21/07/2005
		US 6874089 B2	29/03/2005
		US 7853795 B2	14/12/2010
		WO 2004-015524 A2	19/02/2004
		WO 2004-015524 A3	07/10/2004
KR 10-1880935 B1	23/07/2018	KR 10-2018-0030971 A	27/03/2018
KR 10-1891734 B1	24/08/2018	KR 10-2018-0005527 A	16/01/2018
		KR 10-2018-0048512 A	10/05/2018