



(51) International Patent Classification:

G06F 21/30 (2013.01) H04L 9/32 (2006.01)
G06F 21/60 (2013.01)

(21) International Application Number:

PCT/AU2018/000167

(22) International Filing Date:

06 September 2018 (06.09.2018)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2017903658 08 September 2017 (08.09.2017) AU

(71) Applicant: **FTR LABS PTY LTD** [AU/AU]; c/- HopgoodGanim, Level 8, Waterfront Place, 1 Eagle Street, Brisbane QLD 4000 (AU).

(72) Inventors: **ULDRIDGE, Marc Jonathan**; c/- Level 8, Waterfront Place, 1 Eagle Street, Brisbane QLD 4000 (AU).
DOUGLASS, Anthony; c/- Level 8, Waterfront Place, 1 Eagle Street, Brisbane QLD 4000 (AU).

(74) Agent: **HOPGOODGANIM**; Level 8, Waterfront Place, 1 Eagle Street, Brisbane QLD 4000 (AU).

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

(54) Title: METHOD AND SYSTEM FOR VERIFYING A RECORDING

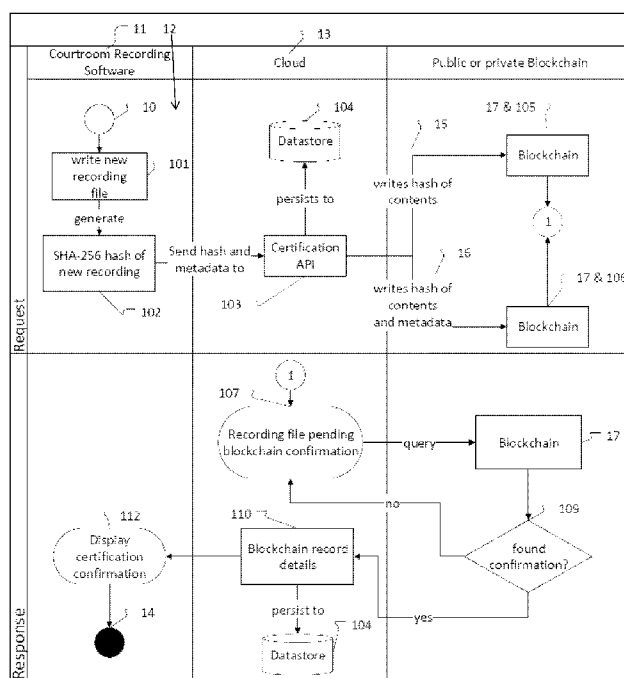


FIG 1

(57) **Abstract:** A method for verifying a recording comprising the steps of a) Creating the recording using a first electronic device; b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording; c) Sending, using the first electronic device, the electronic recording file to a certification server; d) Generating, using the certification server, one or more certification requests based on at least a portion of the information in the electronic recording file, and sending the one or more certification requests to a blockchain; e) Receiving, with the certification server, confirmation of the approval of the one or more certification requests by the blockchain; and f) Generating and/or displaying a verification confirmation on the first electronic device.

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))*

METHOD AND SYSTEM FOR VERIFYING A RECORDING

TECHNICAL FIELD

[0001] The present invention relates to a method and system for verifying a recording. In particular, the present invention relates to a method and system for verifying the authenticity of a recording without disclosing the contents of the recording.

BACKGROUND ART

[0002] In legal and legal-related proceedings, maintaining the integrity of the record is a crucial job. For instance, the testimony of a witness or the statements of an accused, if not properly preserved, can lead a judge or jury to make a wrong decision.

[0003] Typically, audio and/or video recordings are made during court hearings, and the electronic file of these recordings becomes the official record of the proceedings. From time to time, a party in a proceeding before a court may assert that the recording in the electronic file does not align with their recollection of events, and has therefore been altered or tampered with.

[0004] While the likelihood of a successful, undiscovered alteration of an electronic file of this type is relatively low, the making of such an allegation may have serious ramifications both for the custodian of the recording and the proceedings of the court.

[0005] As a result, there would be an advantage if it were possible to provide a reliable way in which to independently verify that the electronic file contains an accurate and unaltered recording of the court proceedings.

[0006] It will be clearly understood that, if a prior art publication is referred to herein, this reference does not constitute an admission that the publication forms part of the common general knowledge in the art in Australia or in any other country.

SUMMARY OF INVENTION

[0007] The present invention is directed to method and system for verifying a recording which may at least partially overcome at least one of the abovementioned disadvantages or provide the consumer with a useful or commercial choice.

[0008] With the foregoing in view, the present invention in one form, resides broadly in a method for verifying a recording comprising the steps of:

- a) Creating the recording using a first electronic device;
- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording;
- c) Sending, using the first electronic device, the electronic recording file to a certification server;
- d) Generating, using the certification server, one or more certification requests based on at least a portion of the information in the electronic recording file, and sending the one or more certification requests to a blockchain;
- e) Receiving, with the certification server, confirmation of the approval of the one or more certification requests by the blockchain; and
- f) Generating and/or displaying a verification confirmation on the first electronic device.

[0009] The first electronic device may be of any suitable form. For instance, the first electronic device may be a computer, mobile telephone, tablet or the like. The recording may be made using any suitable technique. However, in a preferred embodiment of the invention, the recording may be made using a software program provided on the first electronic device, an electronic application downloaded to the first electronic device and so on.

[0010] Any suitable form of recording may be made. For instance, the recording may be an audio recording, a video recording or both an audio and video recording.

[0011] The recording may be a recording of anything capable of being recorded. However, it is envisaged that the method may be more usually used to record an activity where it would be advantageous or desirable to ensure that the recording is an accurate recording of the activity. For instance, the recording may be of a speech or lecture, a political activity (such as a council or parliamentary session or the like), a scientific experiment and so on. More preferably, however, the recording may be a recording of a legal or legal-related proceeding, such as a police interview, court hearing (or a hearing before a similar judicial body), a deposition, a hearing before a disciplinary tribunal or administrative body and the like, or any suitable combination thereof.

[0012] It is envisaged that the recording may comprise a recording of the entire proceeding (speech, lecture, political activity, interview, court hearing, deposition and so on), or the recording may comprise a portion of the overall proceeding (for instance, a session or a day of a court case and the like).

[0013] In other embodiments of the invention, the recording may comprise a relatively short part of the overall proceeding. In this embodiment, it is envisaged that a recording containing a relatively short part of the overall proceeding may be verified while the proceeding is ongoing. This may be particularly advantageous for long proceedings (such as court hearings, police interviews and the like) where, instead of waiting until the completion of the proceeding to verify the recording, portions of the proceeding may be periodically verified while the proceeding continues. This may be beneficial in that it may reduce the period of time between the recording being created and its verification, reducing the likelihood of the recording being tampered with.

[0014] The recording may comprise any suitable portion of the proceeding. For instance, the recording may comprise a portion of the proceeding in which a particular speaker was speaking, or in which a particular topic was being discussed. In other embodiments, the proceeding may be divided into multiple recordings based on time intervals, such that each proceeding comprises a plurality of recordings. In other words, a recording may comprise a period of time shorter than the total length of the proceeding.

[0015] The recording may be of any suitable length, and it is envisaged that recordings of the same proceeding may be of different lengths, or may all be of the same length. The length of the recording is not critical, although it is preferable that the recording is relatively short so that the likelihood of the recording being tampered with between being recorded and verified is reduced or minimised. Thus, it is envisaged that the length of the recording may be no more than one hour. More preferably, the length of the recording may be no more than 30 minutes. Yet more preferably, the length of the recording may be no more than 15 minutes. Even more preferably, the length of the recording may be no more than 10 minutes. Most preferably, the length of the recording may be no more than 5 minutes.

[0016] It is envisaged that the length of the recording may be predetermined, such that recordings are created at predetermined time intervals. Thus, in this embodiment, the first electronic device may be adapted to create a recording at every predetermined time interval, even though the proceeding may be continuing. Preferably the verification of the recording occurs immediately upon, or soon after, the creation of the recording, so that the time between the creation of the recording and its verification is minimised.

[0017] In embodiments of the invention in which the recording is of a legal or legal-related proceeding, it is envisaged that the first electronic device may comprise a computer located in the location where the proceeding is being held (such as a courtroom or the like). Preferably, the computer is provided with recording software in order to create the recording. Any suitable recording software may be provided, although in a preferred embodiment of the invention, the software may create a digital recording.

[0018] In a preferred embodiment of the invention, the recording may be stored in the memory of the first electronic device. The recording may be stored in any suitable electronic format. Alternatively, the recording may not be stored in the memory of the first electronic device, and may instead be sent to another electronic device (such as the certification server) for storage. In this embodiment of the invention, the recording may be sent continuously during the creation of the recording, or may be sent at the conclusion of the recording. In another embodiment

of the invention, the recording may be stored on a storage medium, such as a disc, external hard drive, flash drive or the like, or a combination thereof.

[0019] The recording may be stored or saved in any suitable format. More specifically, the recording may be stored or saved in any suitable file format. For instance, the recording may be stored or saved as one or more of the following file types: AVI, ASF, MOV, QT, AVCHD, FLV, SWF, MPG, MP3, MP4, WMV, H.264, DivX, WAV, OGG, GSM, DCT, FLAC, AU, AIFF, VOX, RAW, WMA, AAC, ATRAC, RA, DSS, MSV or DVF. In a specific embodiment of the invention, the recording may be saved or stored as a TRM file.

[0020] As previously stated, an electronic recording file is generated by the first electronic device, the electronic recording file being based on the recording and one or more further pieces of data associated with the recording.

[0021] It is envisaged that, in some embodiments of the invention, the electronic recording file may include the recording. More preferably, however, the electronic recording file may be based on the recording, but may not comprise the recording itself. In this embodiment of the invention, the electronic recording file may be based on any suitable information based on the recording. For instance, the electronic recording file may comprise a hash function based on the recording. More preferably, the electronic recording file may comprise a cryptographic hash function based on the recording.

[0022] In a specific embodiment of the invention, the electronic recording file may comprise a cryptographic hash function from the SHA-2 set of cryptographic hash functions. In particular, the electronic recording file may comprise an SHA-256 hash of the recording.

[0023] The one or more further pieces of data associated with the recording may be of any suitable form. Preferably, however, the one or more further pieces of data may comprise metadata associated with the recording, the first electronic device and so on. It is envisaged that the one or more further pieces of data may include one or more of the file name of the recording, the first electronic device serial number, the serial number of the motherboard of the first electronic device, information regarding

the network card of the first electronic device (such as the MAC address, the IP address and so on), the details of any users of the first electronic device (such as the names of the users, the times and dates that users logged in and/or out of the first electronic device and/or the recording software), the date and time at which the recording was made, the geographic location at which the recording was made, the matter or proceeding to which the recording relates and so on.

[0024] The electronic recording file may be sent to the certification server using any suitable technique. For instance, the electronic recording file may be sent in the form of an email, SMS message, MMS message or the like. More preferably, however, the electronic recording file may be sent to the certification server as a machine-readable electronic message. In another embodiment of the invention, the electronic recording file may be sent to the certification server via one or more application programming interfaces (APIs). The electronic recording file is preferably sent electronically, for instance using a Wi-Fi connection, Bluetooth connection or the like, or a combination thereof.

[0025] It is envisaged that the electronic recording file may be sent to an API running on the certification server, or may be running on a second electronic device (such as a computer, mobile telephone, tablet compute or the like) in electronic communication with the certification server.

[0026] In embodiments of the invention in which the electronic recording file is in machine-readable format, it is envisaged that the certification server and/or the API associated with the certification server may automatically generate the one or more certification requests in response to receiving the electronic recording file. In some embodiments of the invention, the certification server may also save or store the electronic recording file. The electronic recording file may be saved or stored in electronic memory associated with the certification server (such as a hard drive or the like), remote memory (such as Cloud memory), or on a storage medium, such as a disc, external hard drive, flash drive or the like, or a combination thereof.

[0027] As previously stated, the one or more certification requests are based on at least a portion of the information in the electronic recording file. For instance, a certification request may be based on the recording, a hash function based on the

recording, a cryptographic hash function based on the recording, at least one or the one or more further pieces of data associated with the recording, or any suitable combination thereof.

[0028] In a preferred embodiment of the invention, a plurality of certification requests may be generated by the certification server (or, in some embodiments, an API associated with the certification server). In this embodiment of the invention, it is envisaged that, while each of the certification requests may contain some information that is common to other certification requests, no certification request is identical to another certification request. For instance, in a specific embodiment of the invention, a pair of certification requests may be generated. A first certification request may be based on a cryptographic hash function based on the recording, while a second certification request may be based on a cryptographic hash function based on the recording in combination with the one or more further pieces of information associated with the recording.

[0029] The one or more certification requests may be sent to the blockchain in any suitable form. Preferably, however, the one or more certification requests are sent to the blockchain in machine-readable form. The one or more certification requests are preferably sent electronically, for instance using a Wi-Fi connection, Bluetooth connection or the like, or a combination thereof. Preferably, the action of sending the one or more certification requests to the blockchain involves initiating the creation of one or more new records on the blockchain. Preferably, a hash function (or a cryptographic hash function) of the contents of each of the one or more certification requests is written to the blockchain. Preferably, a timestamp provided by the blockchain is also recorded. The one or more certification requests may form a portion of a blockchain (such as one or more blocks within a blockchain, or a portion of a block within a blockchain).

[0030] Any suitable blockchain may be used. However, in a preferred embodiment of the invention, the blockchain may be a public blockchain, or an open source blockchain. In a specific embodiment of the invention, the blockchain may be the Hyperledger blockchain hosted by the Linux Foundation.

[0031] If the one or more certification requests are successfully written to the blockchain, the blockchain may send a confirmation notification confirming this to the confirmation server (or the API associated with the confirmation server).

Alternatively, the confirmation server (or the API associated with the confirmation server) may continuously or periodically query the blockchain to determine whether the one or more certification requests have been successfully written to the blockchain. Confirmation of the writing of the certification requests to the blockchain may be received in any suitable form. However, in a preferred embodiment of the invention, the confirmation of the writing of the certification requests to the blockchain may be in the form of blockchain record information.

[0032] In either event, once the confirmation server (or the API associated with the confirmation server) receives confirmation of the approval of the one or more certification requests (i.e. that the one or more certification requests have been written to the blockchain), the confirmation (for instance, in the form of the blockchain record information) may be saved or stored in electronic memory associated with the certification server (such as a hard drive or the like), remote memory (such as Cloud memory), or on a storage medium, such as a disc, external hard drive, flash drive or the like, or a combination thereof.

[0033] As previously stated, once confirmation of the approval of the one or more certification requests is received, a verification confirmation is generated and/or displayed on the first electronic device. In some embodiments of the invention, the confirmation server (or the API associated with the confirmation server) may generate the verification confirmation and send it to the first electronic device. In these embodiments of the invention, the verification confirmation may be sent in any suitable form, such as an email, SMS message, MMS message or the like. More preferably, however, the verification confirmation may be sent to the certification server as a machine-readable electronic message. The verification confirmation is preferably sent electronically, for instance using a Wi-Fi connection, Bluetooth connection or the like, or a combination thereof.

[0034] It is envisaged that, upon receipt of the verification confirmation, the first electronic device (or the recording software associated with the first electronic

device) may record the verification confirmation against the recording and/or the electronic recording file. The verification confirmation may be recorded electronically against the recording and/or the electronic recording file. Alternatively, the verification confirmation may be recorded electronically against the recording and/or the electronic recording file and the verification confirmation (or a notification confirming receipt of the verification confirmation) may be displayed on the first electronic device (or in the recording software associated with the first electronic device). The notification may be of any suitable form, such as a pop-up notification for a user, an audible or visual signal, a certificate or notice displayed on the first electronic device or the like. Alternatively, the notification may be displayed within the recording software, for instance in the form of text, symbols, or through a visual cue such as a change in the colour, size etc. of text within the recording software.

[0035] In an alternative embodiment of the invention, the confirmation server may send the confirmation of the approval of the one or more certification requests (for instance, in the form of the blockchain record information) to the first electronic device. In this embodiment of the invention, it is envisaged that, upon receipt of the confirmation of the approval of the one or more certification requests, the first electronic device (or the recording software associated with the first electronic device) may generate and/or display the verification confirmation.

[0036] Once generated, the verification confirmation may be recorded and/or displayed in the same manner as described previously.

[0037] In some embodiments of the invention, the first electronic device may be adapted to generate both the electronic recording file and the one or more certification requests based on at least a portion of the information in the electronic recording file. In these embodiments of the invention, the first electronic device may be adapted to send the one or more certification requests to a blockchain. Thus, in a further aspect, the invention resides broadly in a method for verifying a recording comprising the steps of:

- a) Creating the recording using a first electronic device;

- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording;
- c) Generating, using the first electronic device, one or more certification requests based on at least a portion of the information in the electronic recording file, and sending the one or more certification requests to a blockchain;
- d) Receiving, with the first electronic device, confirmation of the approval of the one or more certification requests by the blockchain; and
- e) Generating and/or displaying a verification confirmation on the first electronic device.

[0038] In another aspect, the invention resides broadly in a method of confirming a verification of a recording by a blockchain, the method comprising the steps of:

- a) Retrieving a recording from electronic memory associated with a first electronic device;
- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and, optionally, one or more further pieces of data associated with the recording;
- c) Sending, using the first electronic device, the electronic recording file to a certification server;
- d) Retrieving, from electronic memory associated with the certification server, blockchain record details associated with the electronic recording file;
- e) Sending, using the certification server, the blockchain record details to the first electronic device;
- f) Generating and/or displaying a verification confirmation associated with the blockchain record details on the first electronic device; and
- g) Optionally verifying the electronic recording file with a blockchain that generated the blockchain record details.

[0039] In some embodiments of the invention, the electronic recording file comprises information based on the recording and one or more further pieces of data associated with the recording.

[0040] In some embodiments of the invention, the first electronic device may be adapted to generate the electronic recording file and the one or more certification requests based on at least a portion of the information in the electronic recording file. The first electronic device may also be adapted to retrieve, from electronic memory associated with the first electronic device, blockchain record details associated with the electronic recording file. In these embodiments of the invention, the first electronic device may be adapted to send the one or more certification requests to a blockchain. Thus, in yet another aspect, the invention resides broadly in a method of confirming a verification of a recording by a blockchain, the method comprising the steps of:

- a) Retrieving a recording from electronic memory associated with a first electronic device;
- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and, optionally, one or more further pieces of data associated with the recording;
- c) Retrieving, from electronic memory associated with the first electronic device, blockchain record details associated with the electronic recording file;
- d) Generating and/or displaying a verification confirmation associated with the blockchain record details on the first electronic device; and
- e) Optionally verifying the electronic recording file with a blockchain that generated the blockchain record details.

[0041] In a further aspect, the invention resides broadly in a system for verifying a recording, the system comprising:

at least one processor, at least one non-transitory computer readable storage medium storing instructions thereon that, when executed by the at least one processor, cause the system to:

verify an electronic recording file associated with the recording and generated by a first electronic device, wherein verifying the electronic recording file comprises generating one or more certification requests, sending the one or more certification requests to a blockchain, and receiving confirmation of the approval of the one or more certification requests by the blockchain.

[0042] Any of the features described herein can be combined in any combination with any one or more of the other features described herein within the scope of the invention.

[0043] The reference to any prior art in this specification is not, and should not be taken as an acknowledgement or any form of suggestion that the prior art forms part of the common general knowledge.

BRIEF DESCRIPTION OF DRAWINGS

[0044] Preferred features, embodiments and variations of the invention may be discerned from the following Detailed Description which provides sufficient information for those skilled in the art to perform the invention. The Detailed Description is not to be regarded as limiting the scope of the preceding Summary of the Invention in any way. The Detailed Description will make reference to a number of drawings as follows:

[0045] Figure 1 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention.

[0046] Figure 2 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention.

[0047] Figure 3 illustrates a screenshot of a step in a method for verifying a recording according to an embodiment of the present invention.

[0048] Figure 4 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention.

[0049] Figure 5 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention.

DESCRIPTION OF EMBODIMENTS

[0050] Figure 1 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention. In this Figure, a recording 10 is made on recording software 11 running on a first electronic device 12. In this embodiment, the first electronic device 12 is located in a courtroom, and the recording 10 is a video and audio recording of a legal proceeding. The first electronic device 12 in this embodiment is a computer.

[0051] The first electronic device 12 stores the recording 10 in the memory of the first electronic device 12 as an electronic file 101. In the embodiment of the invention shown in Figure 1, the electronic file 101 is a TRM file.

[0052] The first electronic device 12 generates, from the electronic file 101, an electronic recording file 102. The electronic recording file 102 is a cryptographic hash of the contents of the electronic file 101, and in particular an SHA-256 hash of the contents of the electronic file 101. In addition, the electronic recording file 102 includes further pieces of data associated with the recording 10. In this embodiment, the further pieces of data include the name of the electronic file 101, the motherboard serial number of the first electronic device, the network card MAC address of the first electronic device 12 and the details of the user logged into the recording software 11 when the recording 10 was made.

[0053] The electronic recording file 102 is transmitted electronically to a cloud-based certification server 13. The electronic recording file 102 is received by an API 103 associated with the certification server 13. The API 103 both stores or saves the electronic recording file 102 to memory 104 associated with the certification server 13 and also generates a first certification request 15 and a second certification request 16.

[0054] In the embodiment of the invention shown in Figure 1, the first certification request 15 contains the SHA-256 hash of the contents of the electronic file 101. The second certification request 16 also contains the SHA-256 hash of the contents of the electronic file 101, along with the further pieces of data. Thus, the contents of the second certification request 16 are, in effect, the same as the contents of the

electronic recording file 102. Thus, while some of the information in the first certification request 15 and the second certification request 16 is the same, the first certification request 15 and the second certification request 16 are not identical to one another.

[0055] The first certification request 15 and the second certification request 16 are transmitted electronically to a blockchain 17. The first certification request 15 is written to the blockchain 17 as a new record 105, while the second certification request 16 is written to the blockchain as a new record 106. Along with the contents of the first certification request and the second certification request 16, respectively, the records 105, 106 also include a timestamp (i.e. a date and time at which the records 105, 106 are written to the blockchain 107) provided by the blockchain 107.

[0056] Once the certification requests 15, 16 are written to the blockchain 17, a confirmation service 107 periodically (or continuously, if preferred) queries the blockchain 17 to seek confirmation 109 of whether the records 105, 106 have been successfully written to the blockchain 17. It will be understood that if the records 105, 106 are successfully written to the blockchain 17, then the contents of the records 105, 106 (and therefore the recording 10) are accepted as being correct and unaltered.

[0057] If the confirmation service 107 does not receive confirmation of the records 105, 106 being written to the blockchain 17, a further query is sent to the blockchain 17. On the other hand, if confirmation of the successful writing of records 105, 106 to the blockchain 17 is received by the confirmation service 107, the blockchain record details 110 are electronically transmitted to the certification server 13. The blockchain record details 110 are saved or stored in memory 104 associated with the certification server 13 and are also electronically transmitted to the first electronic device 12.

[0058] Upon receipt of the blockchain record details 110, the first electronic device 12 (or the recording software 11 associated with the first electronic device 12) generates a verification confirmation 112. The verification confirmation 112 is associated with the recording 10 by the recording software 11. In the embodiment of the invention shown in Figure 1, the first electronic device 12 also displays the

verification confirmation 112 on a display 14 of the first electronic device 12. While it is envisaged that the verification confirmation 112 may be generated automatically by the first electronic device 12 on receipt of the blockchain record details 110, the display of the verification confirmation 112 may be in response to a user query, or may occur automatically once the verification confirmation 112 is received.

[0059] Figure 2 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention. More specifically, Figure 2 illustrates a method for confirming the verification of a recording.

[0060] In Figure 2, a recording file 201 that is saved in the memory of a first electronic device 12 is loaded into playback software 202 running on the first electronic device 12. The first electronic device 12 (and the playback software 202) generates an electronic recording file 203 that is a cryptographic hash of the contents of the recording file 201, and in particular an SHA-256 hash of the contents of the recording file 201. In addition, the electronic recording file 203 includes further pieces of data associated with the recording file 201. In this embodiment, the further pieces of data include the name of the recording file 201.

[0061] The electronic recording file 203 is electronically transmitted to a cloud-based certification server 13 and, in particular, a certification API 204 associated with the certification server 13. The certification API 204 retrieves data from memory associated with the certification server 13. In particular, the certification API 204 retrieves the blockchain record details 205 associated with the recording file 201.

[0062] The blockchain record details 205 are then electronically transmitted to the first electronic device 12, and a verification confirmation 206 is displayed to a user. If desired, the electronic recording file 203 may be independently verified on the blockchain 207.

[0063] Figure 3 illustrates a screenshot of a step in a method for verifying a recording according to an embodiment of the present invention. In this Figure, a plurality of recordings 300 are displayed to a user on an interface 301.

[0064] When a verified recording 302 appears in the list, a verification confirmation 303 is displayed on the interface indicating that the recording 302 has

been verified by a blockchain. As previously mentioned, this indicates to a user that the recording 302 is a correct and unaltered recording of the, for instance, legal proceeding recorded therein.

[0065] Figure 4 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention. In this Figure, a recording 10 is made on recording software 11 running on a first electronic device 12. In this embodiment, the first electronic device 12 is located in a courtroom, and the recording 10 is a video and audio recording of a legal proceeding. The first electronic device 12 in this embodiment is a computer.

[0066] The first electronic device 12 stores the recording 10 in the memory of the first electronic device 12 as an electronic file 101. In the embodiment of the invention shown in Figure 1, the electronic file 101 is a TRM file.

[0067] The first electronic device 12 generates, from the electronic file 101, an electronic recording file 102. The electronic recording file 102 is a cryptographic hash of the contents of the electronic file 101, and in particular an SHA-256 hash of the contents of the electronic file 101. In addition, the electronic recording file 102 includes further pieces of data associated with the recording 10. In this embodiment, the further pieces of data include the name of the electronic file 101, the motherboard serial number of the first electronic device, the network card MAC address of the first electronic device 12 and the details of the user logged into the recording software 11 when the recording 10 was made.

[0068] Unlike the embodiment of the invention illustrated in Figure 1, the electronic recording file 102 is not transmitted electronically to a cloud-based certification server. Instead, the first electronic device 12 generates a first certification request 15 and a second certification request 16 and transmits these electronically to a blockchain 17.

[0069] In the embodiment of the invention shown in Figure 4, the first certification request 15 contains the SHA-256 hash of the contents of the electronic file 101. The second certification request 16 also contains the SHA-256 hash of the contents of the electronic file 101, along with the further pieces of data. Thus, the contents of the

second certification request 16 are, in effect, the same as the contents of the electronic recording file 102. Thus, while some of the information in the first certification request 15 and the second certification request 16 is the same, the first certification request 15 and the second certification request 16 are not identical to one another.

[0070] The first certification request 15 is written to the blockchain 17 as a new record 105, while the second certification request 16 is written to the blockchain as a new record 106. Along with the contents of the first certification request and the second certification request 16, respectively, the records 105, 106 also include a timestamp (i.e. a date and time at which the records 105, 106 are written to the blockchain 107) provided by the blockchain 107.

[0071] Once the certification requests 15, 16 are written to the blockchain 17, a confirmation service 107 periodically (or continuously, if preferred) queries the blockchain 17 to seek confirmation 109 of whether the records 105, 106 have been successfully written to the blockchain 17. It will be understood that if the records 105, 106 are successfully written to the blockchain 17, then the contents of the records 105, 106 (and therefore the recording 10) are accepted as being correct and unaltered.

[0072] If the confirmation service 107 does not receive confirmation of the records 105, 106 being written to the blockchain 17, a further query is sent to the blockchain 17. On the other hand, if confirmation of the successful writing of records 105, 106 to the blockchain 17 is received by the confirmation service 107, the blockchain record details 110 are electronically transmitted to the first electronic device 12. The blockchain record details 110 are saved or stored in memory 104 associated with the first electronic device 12.

[0073] Upon receipt of the blockchain record details 110, the first electronic device 12 (or the recording software 11 associated with the first electronic device 12) generates a verification confirmation 112. The verification confirmation 112 is associated with the recording 10 by the recording software 11. In the embodiment of the invention shown in Figure 1, the first electronic device 12 also displays the verification confirmation 112 on a display 14 of the first electronic device 12. While it

is envisaged that the verification confirmation 112 may be generated automatically by the first electronic device 12 on receipt of the blockchain record details 110, the display of the verification confirmation 112 may be in response to a user query, or may occur automatically once the verification confirmation 112 is received.

[0074] Figure 5 illustrates a flowchart of a method and system for verifying a recording according to an embodiment of the present invention. More specifically, Figure 5 illustrates a method for confirming the verification of a recording.

[0075] In Figure 5, a recording file 201 that is saved in the memory of a first electronic device 12 is loaded into playback software 202 running on the first electronic device 12. The first electronic device 12 (and the playback software 202) generates an electronic recording file 203 that is a cryptographic hash of the contents of the recording file 201, and in particular an SHA-256 hash of the contents of the recording file 201. In addition, the electronic recording file 203 includes further pieces of data associated with the recording file 201. In this embodiment, the further pieces of data include the name of the recording file 201.

[0076] The first electronic device 12 retrieves, from electronic storage 204 associated with the first electronic device 12, the blockchain record details 205 associated with the recording file 201. The blockchain record details 205 and/or the electronic recording file 203 may be electronically transmitted from the first electronic device 12 to the blockchain 207 for verification. Upon verification by the blockchain 207, a verification confirmation 206 is displayed to a user on a display 14 of the first electronic device 12.

[0077] In the present specification and claims (if any), the word 'comprising' and its derivatives including 'comprises' and 'comprise' include each of the stated integers but does not exclude the inclusion of one or more further integers.

[0078] Reference throughout this specification to 'one embodiment' or 'an embodiment' means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearance of the phrases 'in one embodiment' or 'in an embodiment' in various places throughout this specification are not necessarily all

referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more combinations.

[0079] In compliance with the statute, the invention has been described in language more or less specific to structural or methodical features. It is to be understood that the invention is not limited to specific features shown or described since the means herein described comprises preferred forms of putting the invention into effect. The invention is, therefore, claimed in any of its forms or modifications within the proper scope of the appended claims (if any) appropriately interpreted by those skilled in the art.

CLAIMS

1. A method for verifying a recording comprising the steps of:
 - a) Creating the recording using a first electronic device;
 - b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording;
 - c) Sending, using the first electronic device, the electronic recording file to a certification server;
 - d) Generating, using the certification server, one or more certification requests based on at least a portion of the information in the electronic recording file, and sending the one or more certification requests to a blockchain;
 - e) Receiving, with the certification server, confirmation of the approval of the one or more certification requests by the blockchain; and
 - f) Generating and/or displaying a verification confirmation on the first electronic device.
2. A method according to claim 1 wherein the recording is an audio recording, a video recording or both an audio and video recording.
3. A method according to claim 1 or claim 2 wherein the recording is saved or stored as a TRM file.
4. A method according to any one of the preceding claims wherein the electronic recording file comprises a cryptographic hash function based on the recording.
5. A method according to claim 4 wherein the cryptographic hash function comprises an SHA-256 hash of the recording.
6. A method according to any one of the preceding claims wherein the one or more further pieces of data associated with the recording include one or more of the file name of the recording, the first electronic device serial number, the serial number of the motherboard of the first electronic device, information regarding a network card of the first electronic device, details of any users of the first electronic device, date and time at which the recording was made, geographic location at which the recording was made and/or a matter or proceeding to which the recording relates.

7. A method according to any one of the preceding claims wherein the electronic recording file is sent to the certification server as a machine-readable electronic message.
8. A method according to claim 4 or claim 5 wherein the certification server generates a pair of certification requests.
9. A method according to claim 8 wherein a first of the pair of certification requests is based on the cryptographic hash function, and a second of the pair of certification requests is based on the cryptographic hash function in combination with the one or more further pieces of information associated with the recording.
10. A method according to any one of the preceding claims wherein the one or more certification requests are sent to the blockchain in machine-readable form.
11. A method according to any one of the preceding claims wherein a hash function or cryptographic hash function of contents of each of the one or more certification requests is written to the blockchain.
12. A method according to any one of the preceding claims wherein the confirmation of the approval of the one or more certification requests by the blockchain is received in the form of blockchain record information.
13. A method according to any one of the preceding claims wherein the verification confirmation is recorded electronically against the recording and/or the electronic recording file by the first electronic device.
14. A method for verifying a recording comprising the steps of:
 - a) Creating the recording using a first electronic device;
 - b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording;

- c) Generating, using the first electronic device, one or more certification requests based on at least a portion of the information in the electronic recording file, and sending the one or more certification requests to a blockchain;
- d) Receiving, with the first electronic device, confirmation of the approval of the one or more certification requests by the blockchain; and
- e) Generating and/or displaying a verification confirmation on the first electronic device.

15. A method of confirming a verification of a recording by a blockchain, the method comprising the steps of:

- a) Retrieving a recording from electronic memory associated with a first electronic device;
- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and one or more further pieces of data associated with the recording;
- c) Sending, using the first electronic device, the electronic recording file to a certification server;
- d) Retrieving, from electronic memory associated with the certification server, blockchain record details associated with the electronic recording file;
- e) Sending, using the certification server, the blockchain record details to the first electronic device;
- f) Generating and/or displaying a verification confirmation associated with the blockchain record details on the first electronic device; and
- g) Optionally verifying the electronic recording file with a blockchain that generated the blockchain record details.

16. A method according to any one of the preceding claims wherein the recording is a recording of a legal or legal-related proceeding.

17. A method according to any one of the preceding claims wherein the first electronic device comprises a computer provided with recording software in order to create the recording.

18. A method according to claim 17 when dependent on claim 16 wherein the first electronic device is located in the location where the proceeding is being held.

19. A method of confirming a verification of a recording by a blockchain, the method comprising the steps of:

- a) Retrieving a recording from electronic memory associated with a first electronic device;
- b) Generating, using the first electronic device, an electronic recording file, the electronic recording file comprising information based on the recording and, optionally, one or more further pieces of data associated with the recording;
- c) Retrieving, from electronic memory associated with the first electronic device, blockchain record details associated with the electronic recording file;
- d) Generating and/or displaying a verification confirmation associated with the blockchain record details on the first electronic device; and
- e) Optionally verifying the electronic recording file with a blockchain that generated the blockchain record details.

20. A system for verifying a recording, the system comprising:

at least one processor, at least one non-transitory computer readable storage medium storing instructions thereon that, when executed by the at least one processor, cause the system to:

verify an electronic recording file associated with the recording and generated by a first electronic device, wherein verifying the electronic recording file comprises generating one or more certification requests, sending the one or more certification requests to a blockchain, and receiving confirmation of the approval of the one or more certification requests by the blockchain.

1/5

DRAWINGS

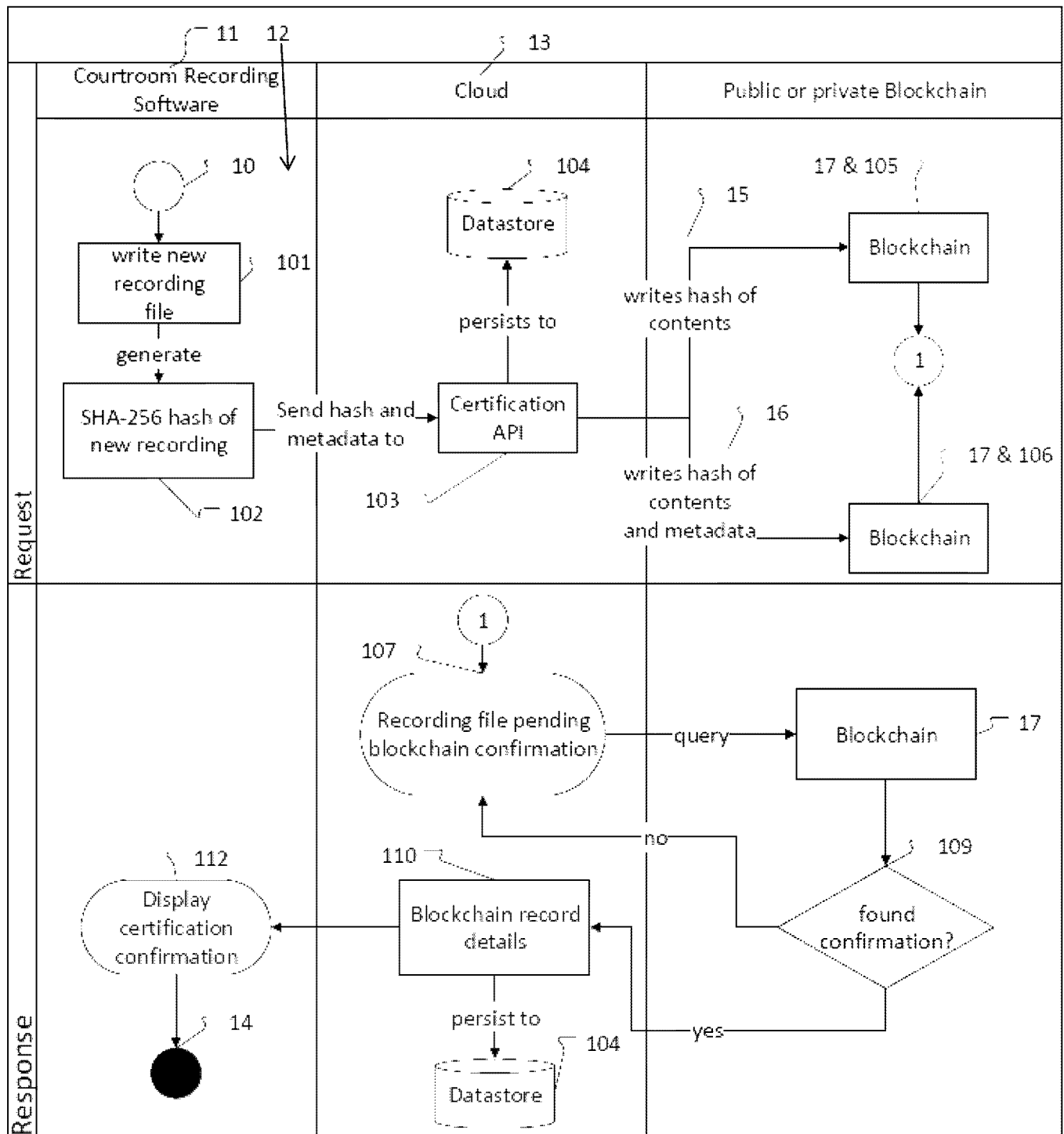


FIG 1

2/5

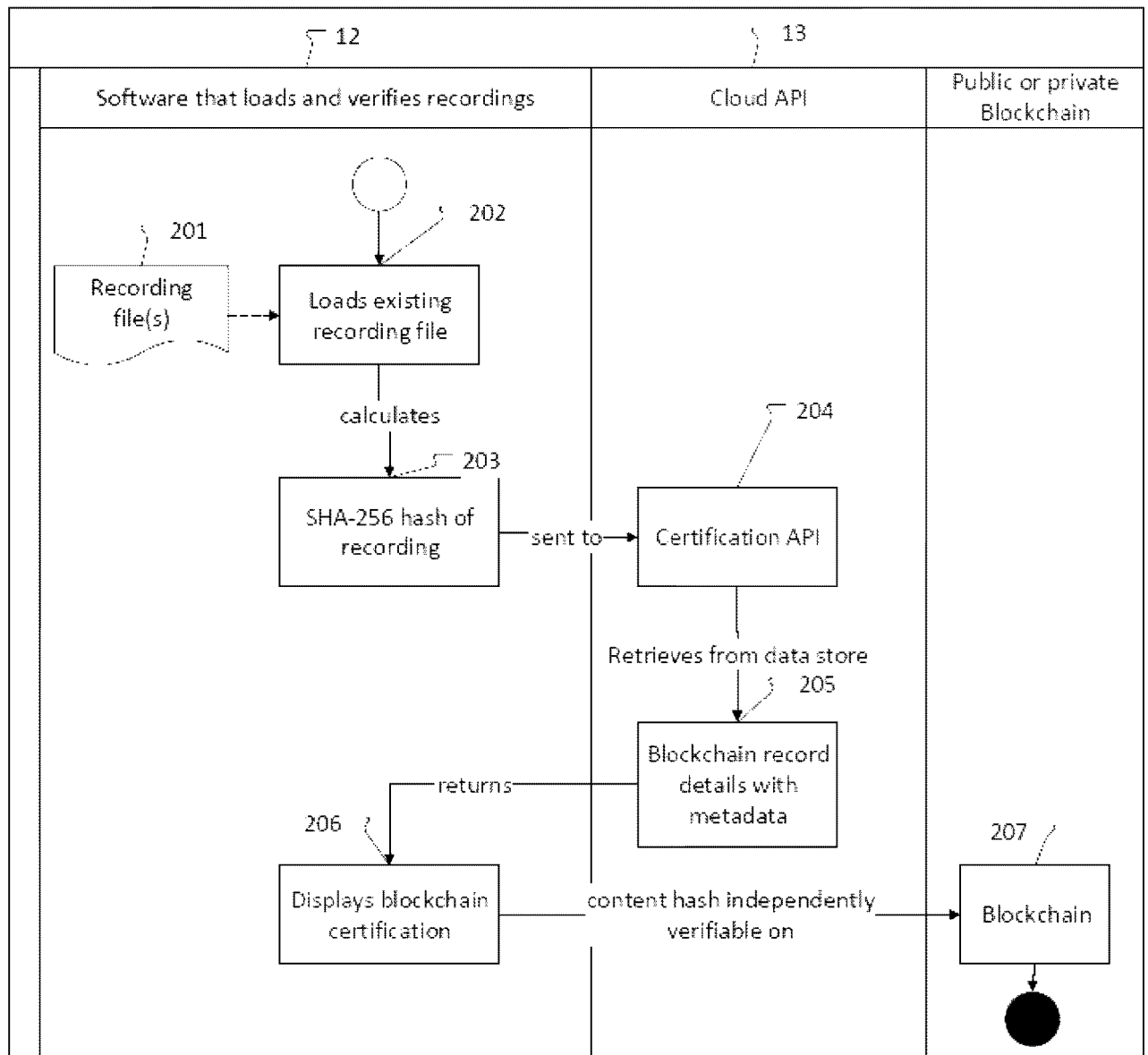


FIG 2

3/5

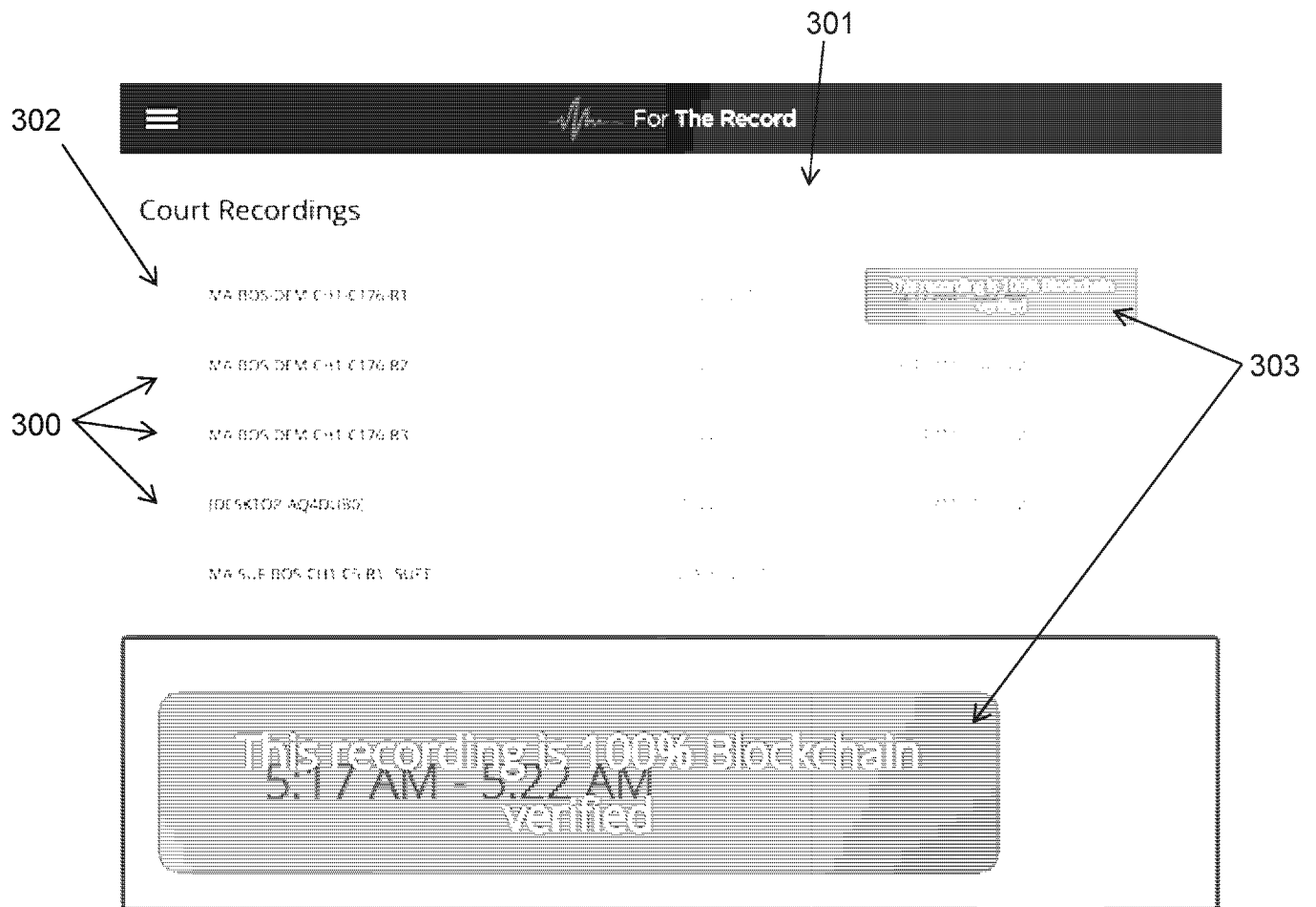


FIG 3

4/5

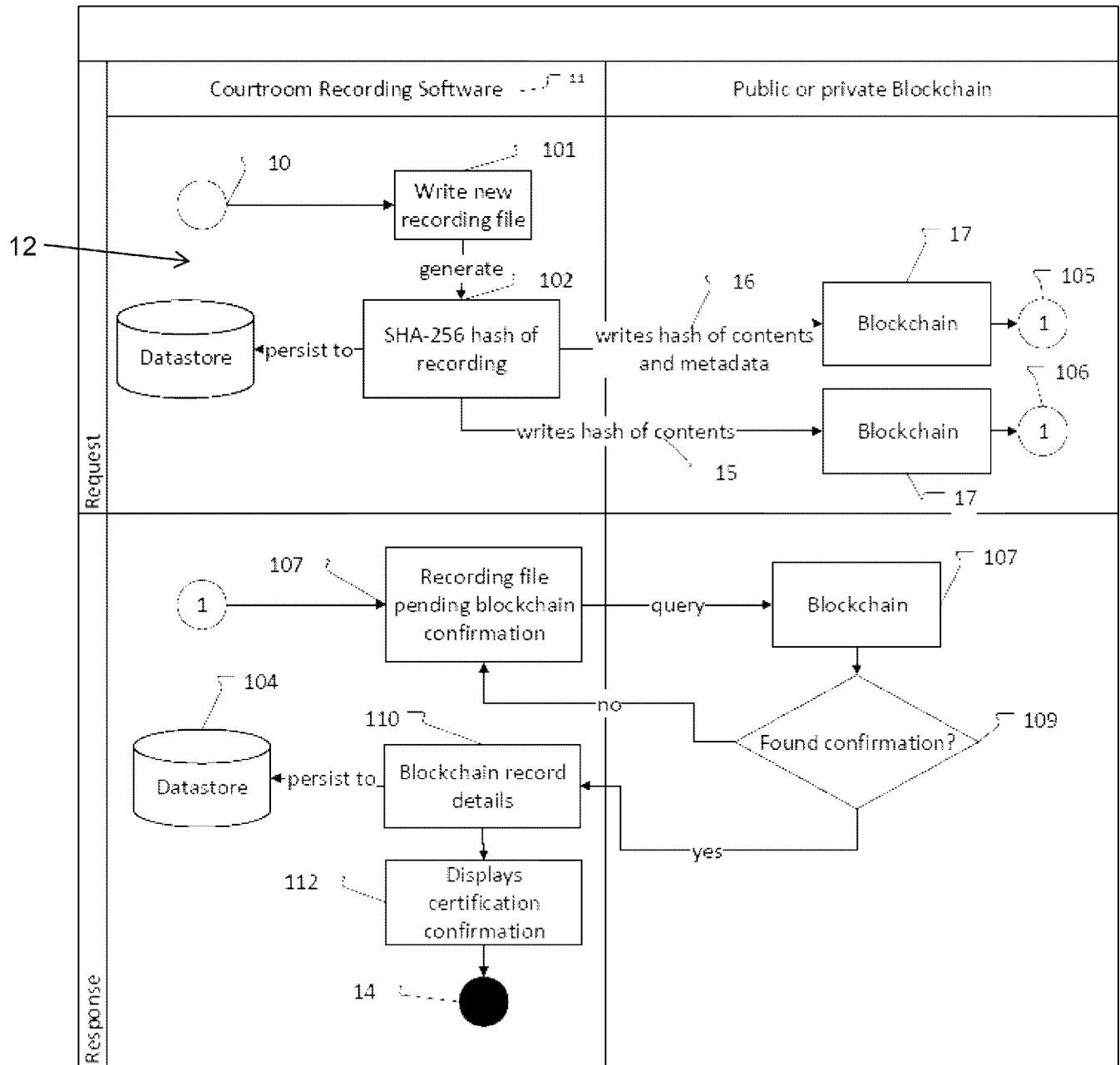


FIG 4

5/5

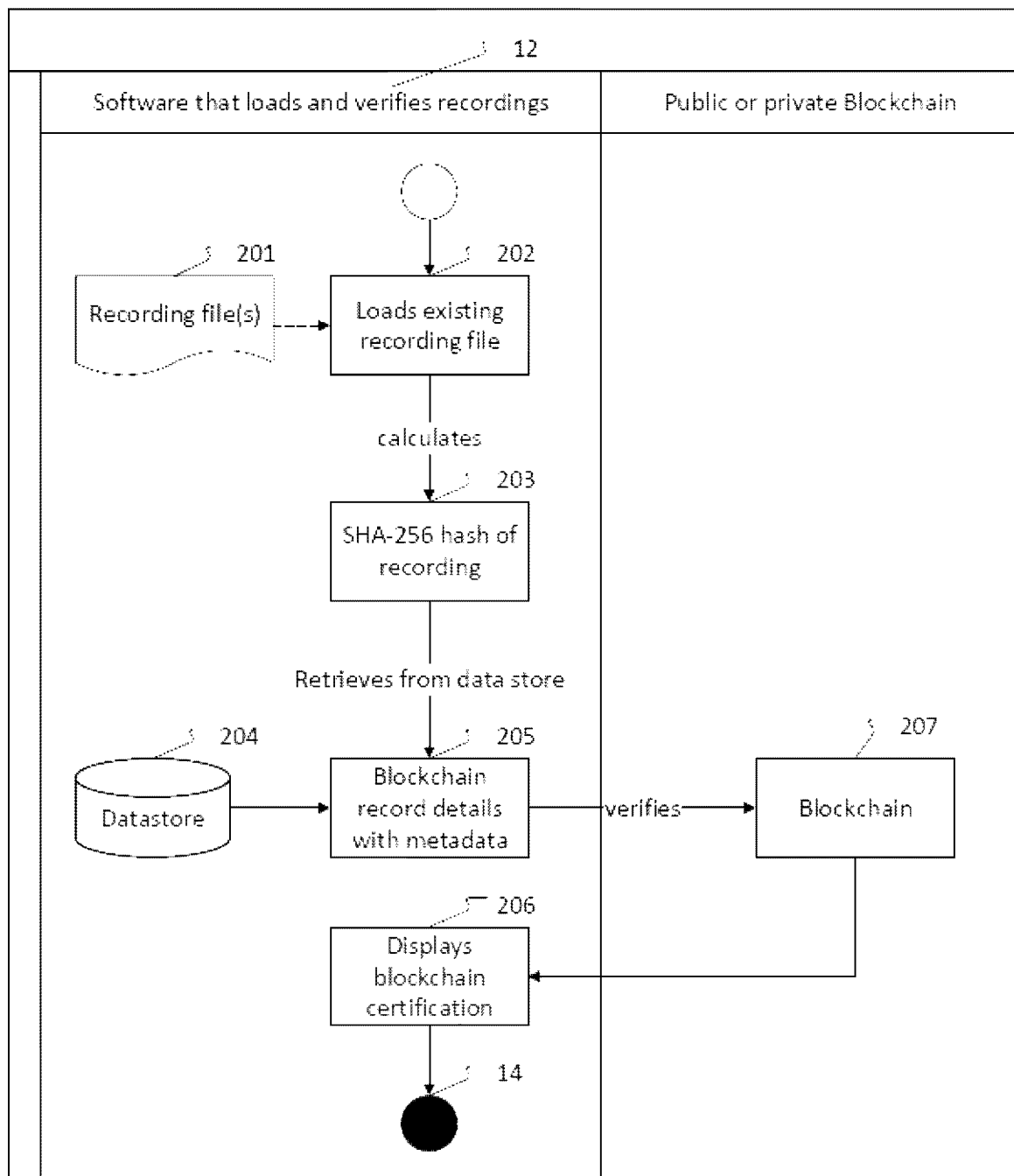


FIG 5

INTERNATIONAL SEARCH REPORT

 International application No.
PCT/AU2018/000167

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30 (2013.01) G06F 21/60 (2013.01) H04L 9/32 (2006.01)

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)

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)

EPOQUE PATENW: Keywords - "blockchain, authenticate, audio, video, recording, footage, clips, music" & similar terms.

Google Patents & Scholar: Keywords - "blockchain, verify, video, audio, server"; date limited upto and including 8 Sep 2017.

Applicant & Inventor Name searches: performed in Espacenet, Google Patents & IP Australia internal databases.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	Documents are listed in the continuation of Box C	



Further documents are listed in the continuation of Box C



See patent family annex

* "A"	Special categories of cited documents: document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent but published on or after the international filing date	"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
"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)	"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
"O"	document referring to an oral disclosure, use, exhibition or other means	"&"	document member of the same patent family
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 15 October 2018	Date of mailing of the international search report 15 October 2018
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA Email address: pct@ipaustalia.gov.au	Authorised officer Ravi McCosker AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +612 6283 2933

INTERNATIONAL SEARCH REPORT		International application No.
C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		PCT/AU2018/000167
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/0283920 A1 (FISHER et al.) 29 September 2016 Entire document, especially: Abstract & Para. 3, 16, 18-27 & Claim 1.	1-20
X	US 2016/0371509 A1 (NEWVOICEMEDIA LTD) 22 December 2016 Abstract & Para. 6, 7, 10-13, 54-66, 68-72, 84, 87.	1-20
X	HILLSTROM, A. H. et al., "Video Integrity through Blockchain Technology", Masters Thesis, KTH, School of Information and Communication Technology (ICT), Communication Systems, CoS, 2 August 2017 [retrieved from the Internet 25 May 2018] < URL: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1129877&dswid=-908 > Entire document, especially: Fig. 1.1, 1.3, 3.1 & Pages 9-16, 21, 25, 32, 39, 57, 58.	1-20
A	US 7861088 B1 (BROTHERS) 28 December 2010 Entire document.	1-20
A	US 2017/0221029 A1 (CABLE TELEVISION LABORATORIES INC) 03 August 2017 Entire document.	1-20
A	US 2013/0142330 A1 (SCHULTZ) 06 June 2013 Entire document.	1-20
Form PCT/ISA/210 (fifth sheet) (January 2015)		

INTERNATIONAL SEARCH REPORT		International application No.	
Information on patent family members		PCT/AU2018/000167	
This Annex lists known patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.			
Patent Document/s Cited in Search Report		Patent Family Member/s	
Publication Number	Publication Date	Publication Number	Publication Date
US 2016/0283920 A1	29 September 2016	US 2016283920 A1	29 Sep 2016
US 2016/0371509 A1	22 December 2016	US 2016371509 A1	22 Dec 2016
		US 9553982 B2	24 Jan 2017
		US 2017132421 A1	11 May 2017
		US 9842216 B2	12 Dec 2017
		US 2015012974 A1	08 Jan 2015
		US 2018165461 A1	14 Jun 2018
		WO 2017106792 A1	22 Jun 2017
US 7861088 B1	28 December 2010	US 7861088 B1	28 Dec 2010
US 2017/0221029 A1	03 August 2017	US 2017221029 A1	03 Aug 2017
		US 2017134161 A1	11 May 2017
		US 2017206523 A1	20 Jul 2017
		US 2017337534 A1	23 Nov 2017
US 2013/0142330 A1	06 June 2013	US 2013142330 A1	06 Jun 2013
		US 8879731 B2	04 Nov 2014
End of Annex			