US 20250267009A1

(19) **United States**

(12) **Patent Application Publication**

(10) **Pub. No.: US 2025/0267009 A1**

(43) **Pub. Date: Aug. 21, 2025**

Arshanskii et al.

(54) **METHOD FOR PROVIDING CONTENT FOR AUTHENTICATION AND AUTHENTICATING CONTENT**

(71) Applicant: **Terra Quantum AG**, St. Gallen (CH)

(72) Inventors: **Aleksei Arshanskii**, St. Gallen (CH); **Alexander Kolybelnikov**, St. Gallen (CH)

(73) Assignee: **Terra Quantum AG**, St. Gallen (CH)

(21) Appl. No.: **19/052,380**

(22) Filed: **Feb. 13, 2025**

(30) **Foreign Application Priority Data**

Feb. 21, 2024 (EP) 24158852

Publication Classification

(51) **Int. Cl.**

H04L 9/32 (2006.01)

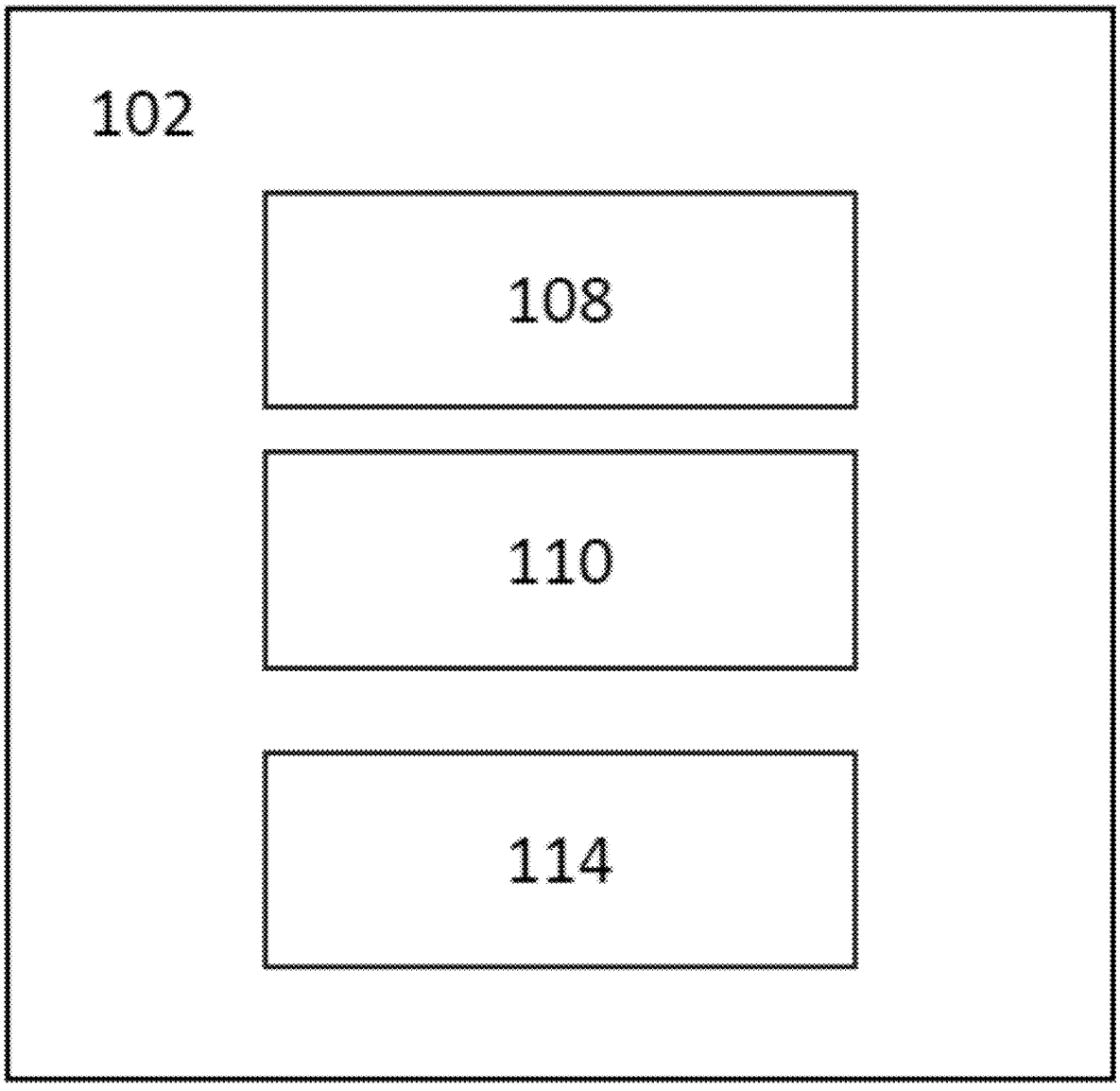
G06F 21/32 (2013.01)

(52) **U.S. Cl.**

CPC ***H04L 9/3247*** (2013.01); ***G06F 21/32*** (2013.01)

(57) **ABSTRACT**

A computer-implemented method for providing content of a content author for authentication includes obtaining, by the content author, a first author fragment of content; generating a first state author vector from the first author fragment of content; and creating a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and a first digital signature.



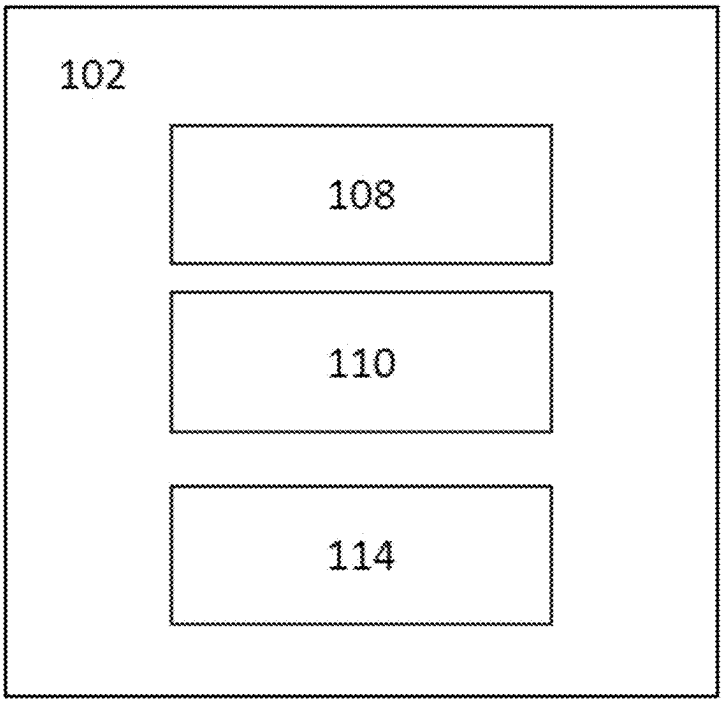


Fig. 1

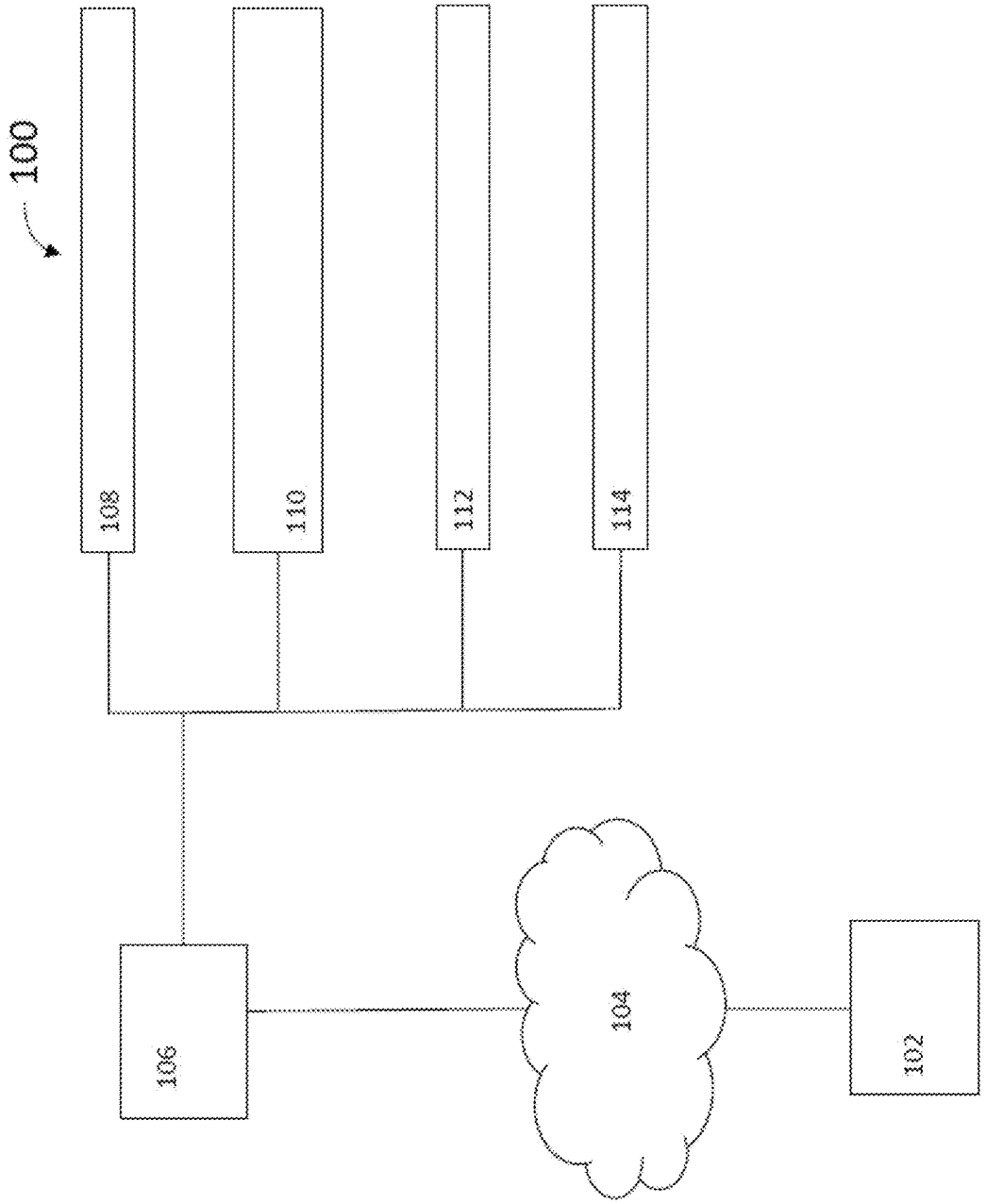


Fig. 1a

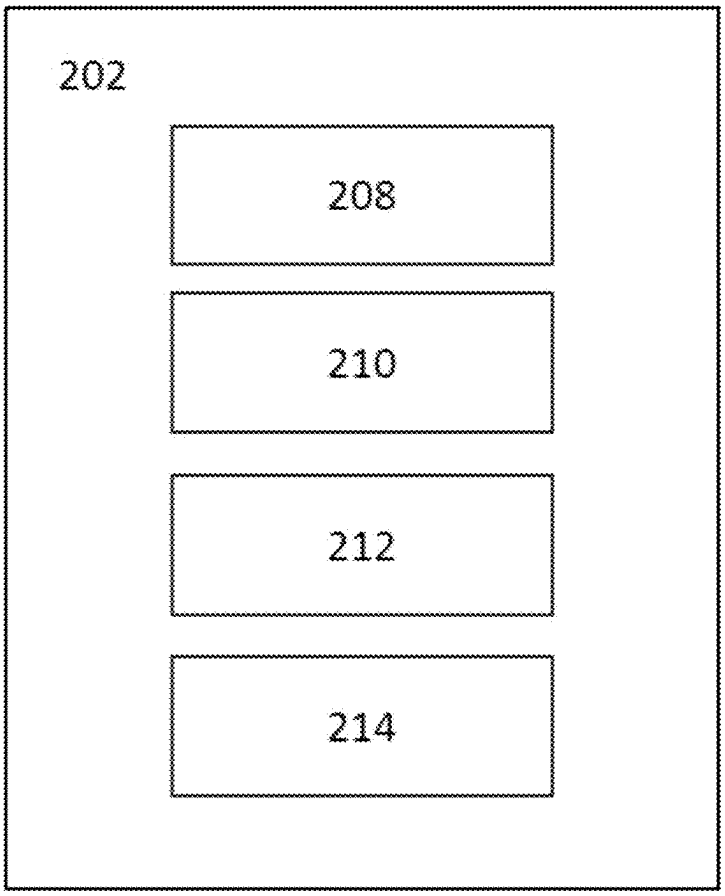


Fig. 2

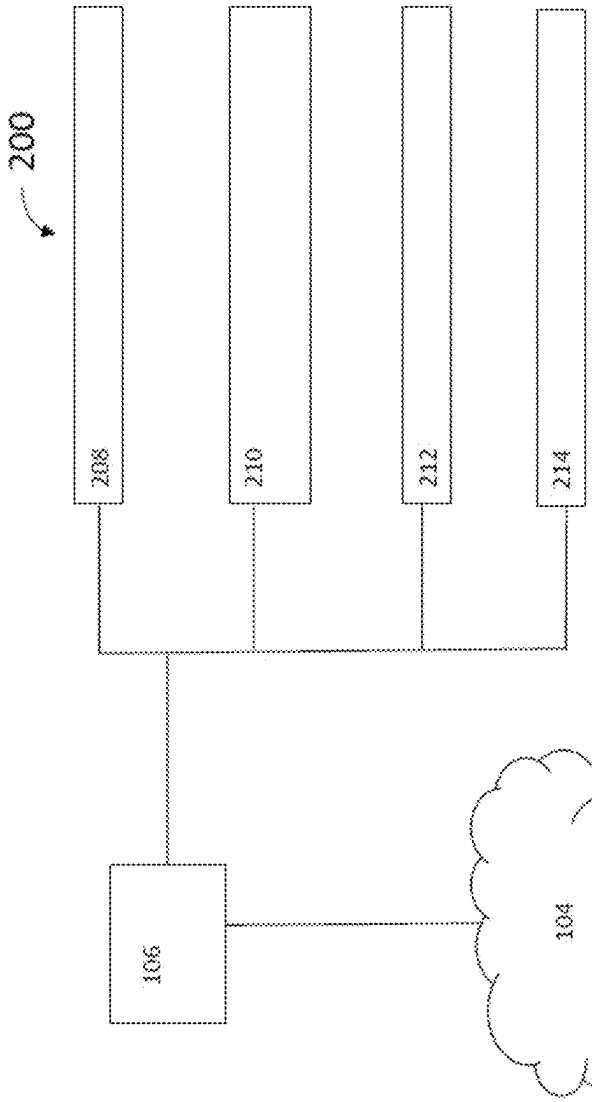


Fig. 2a

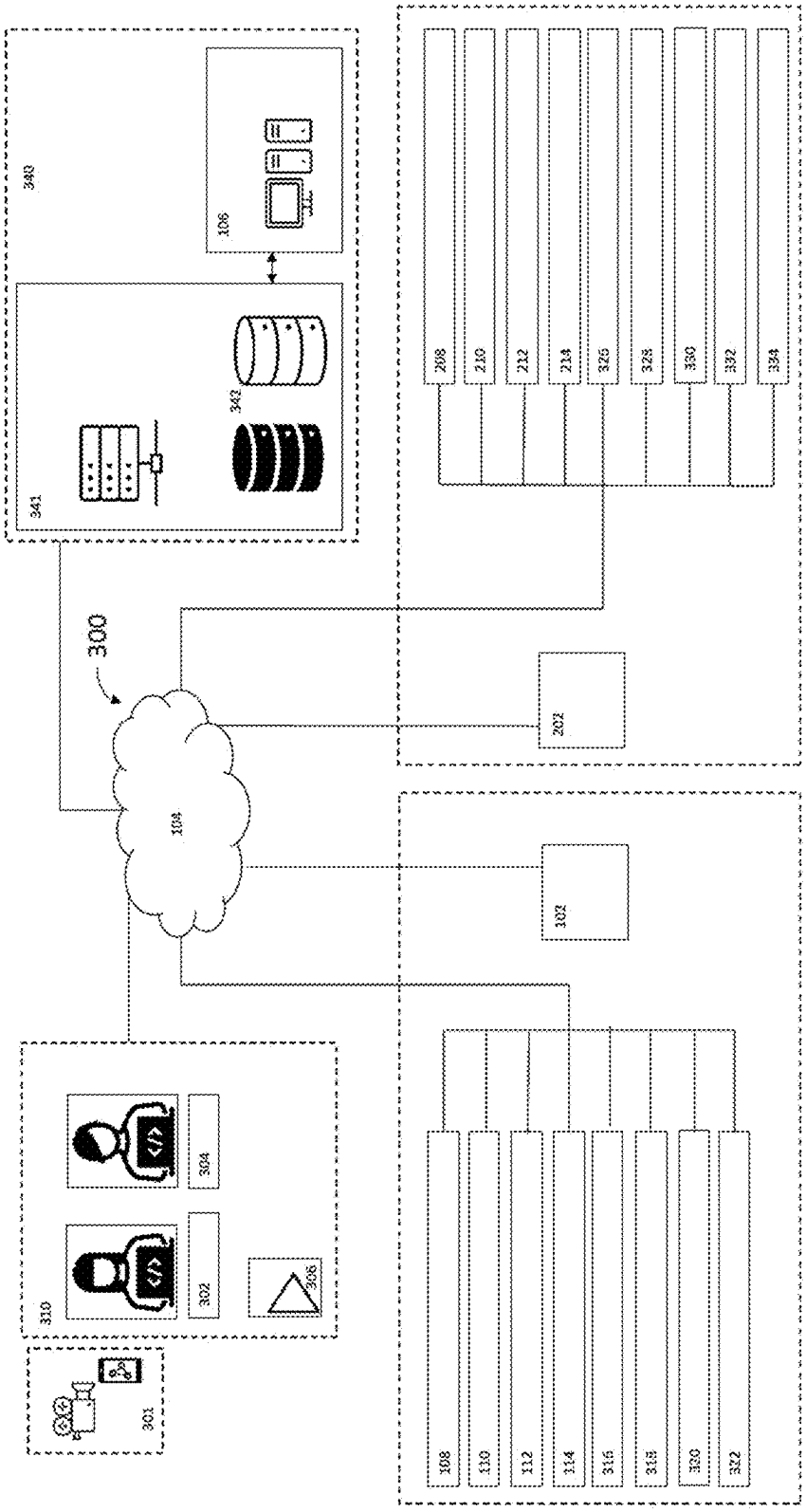

300
340
106
341
342
208
210
212
214
326
328
330
332
334
202
104
102
310
304
302
306
301
108
110
112
114
316
318
320
322

Fig. 3

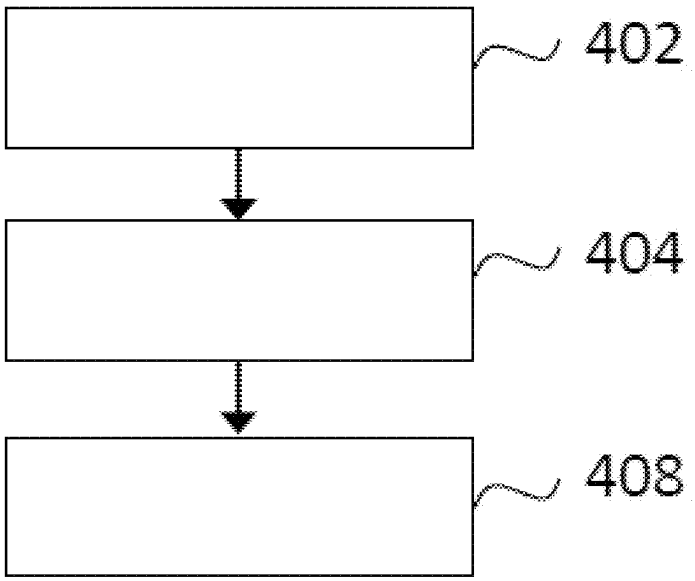


Fig. 4

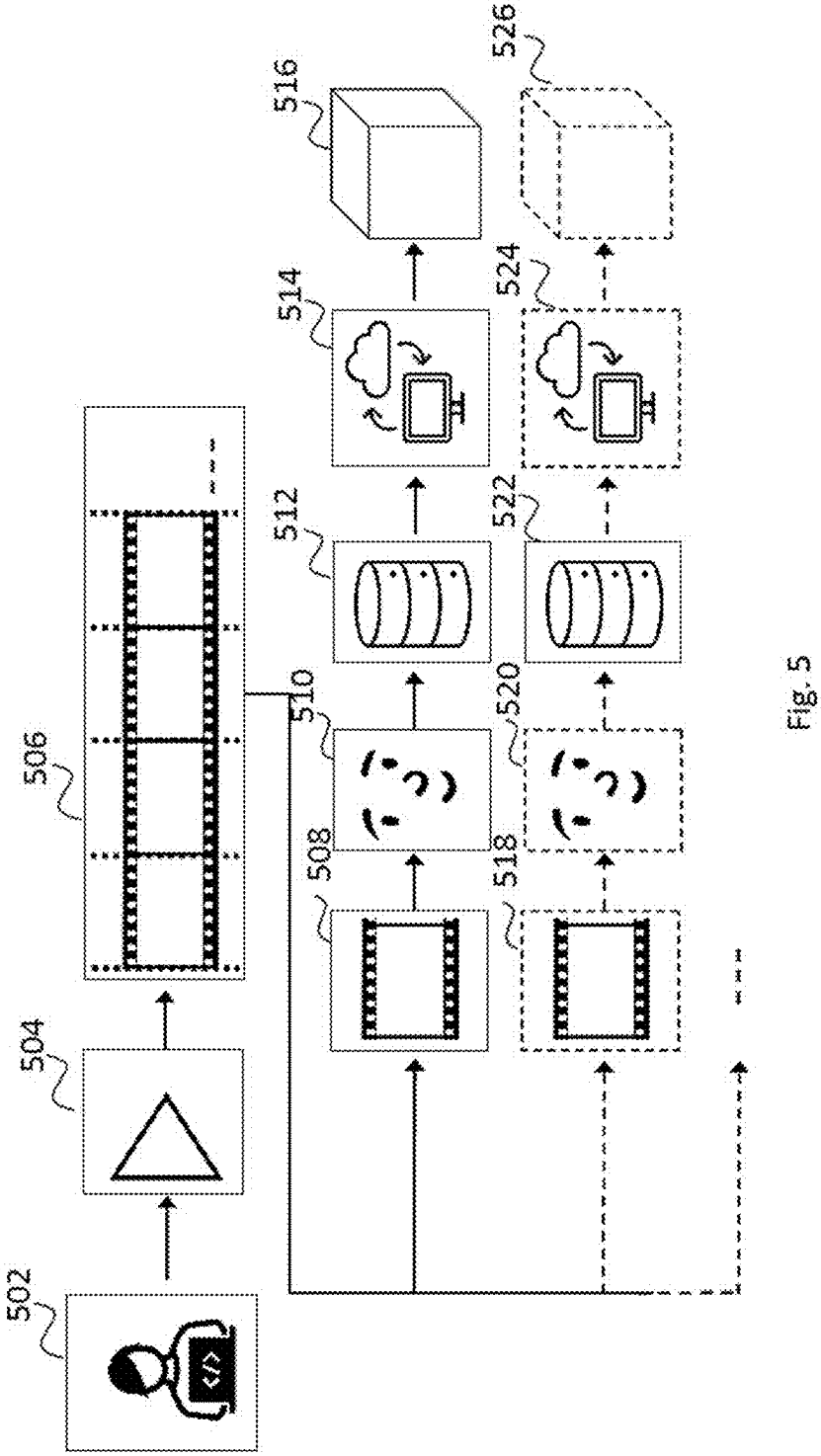


Fig. 5

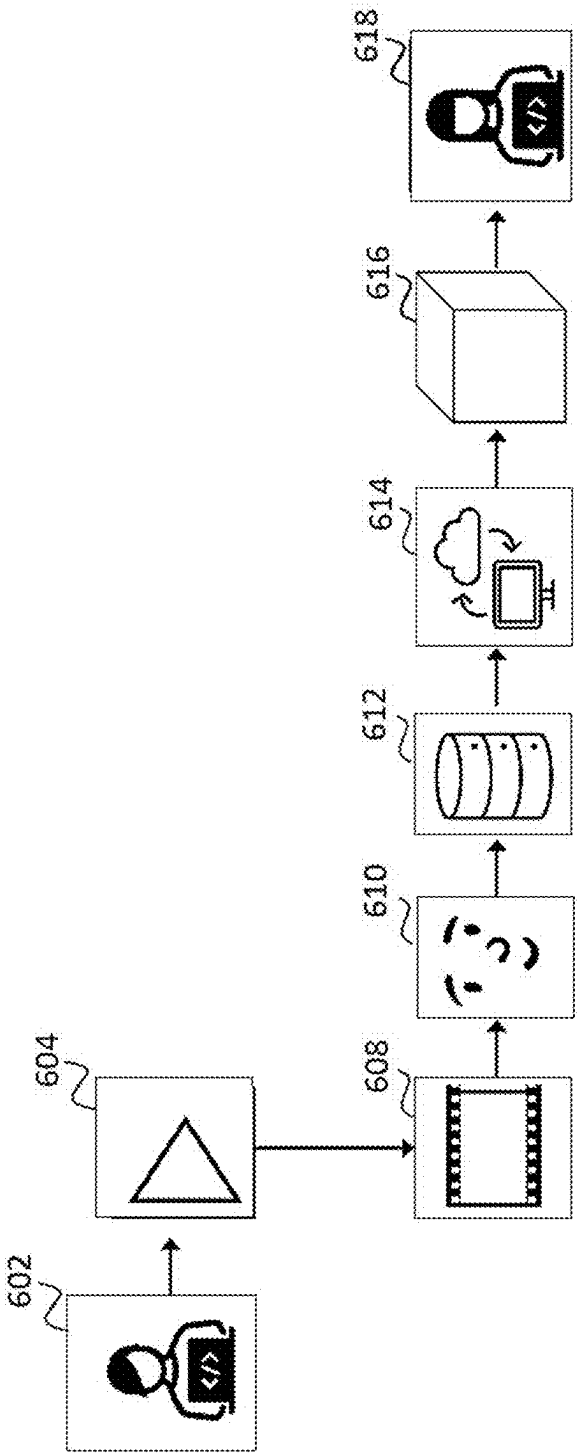


Fig. 6

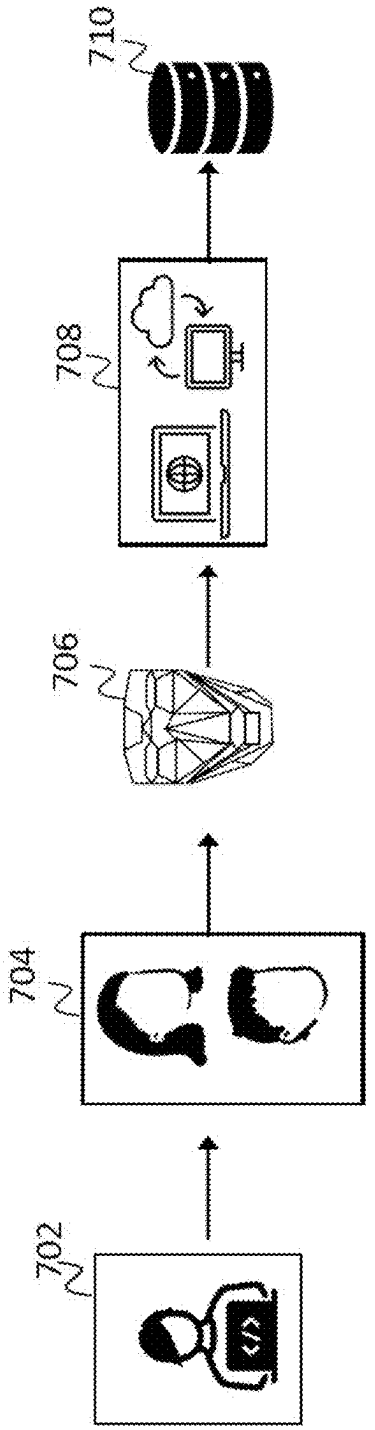


Fig. 7

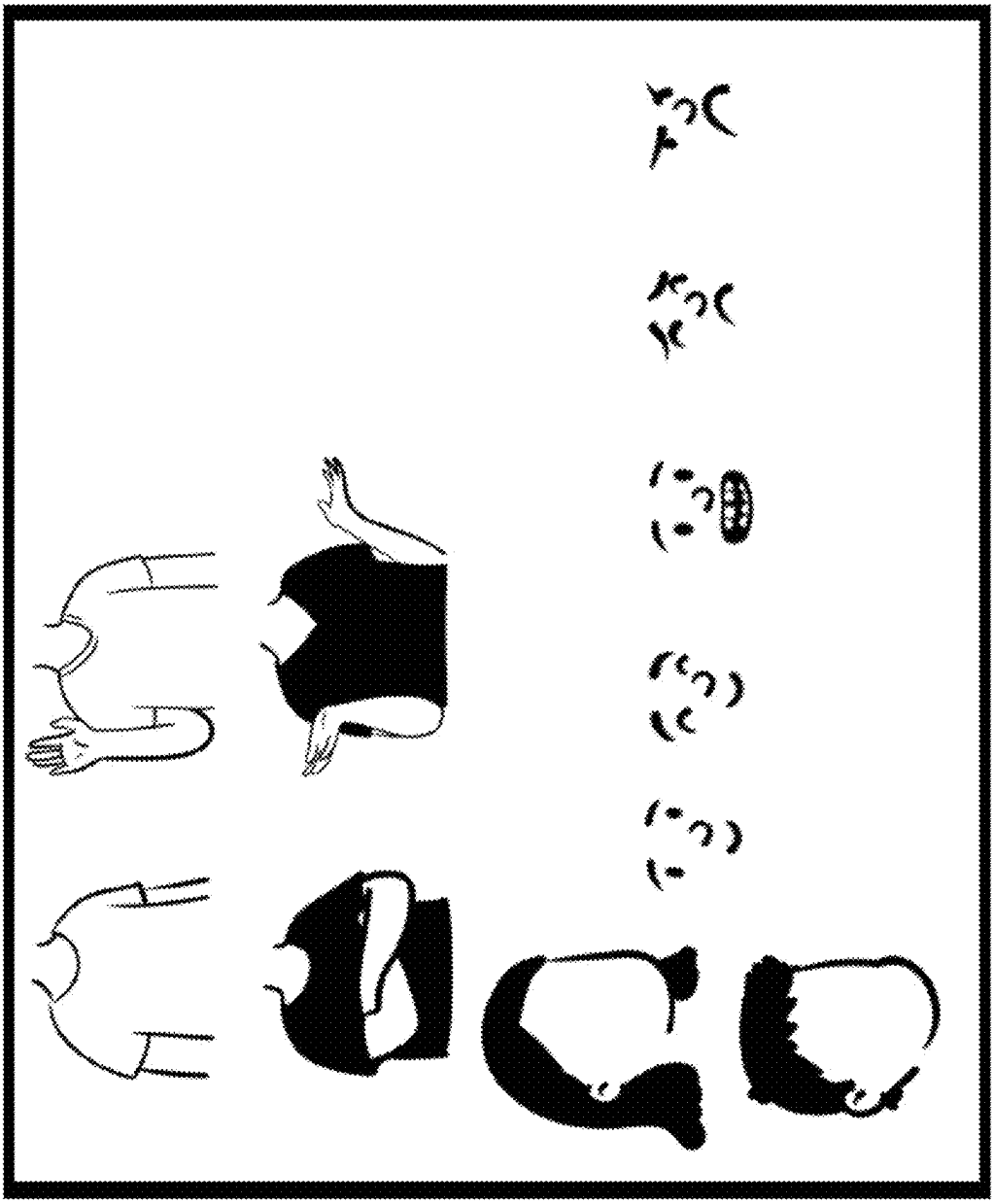


Fig. 8

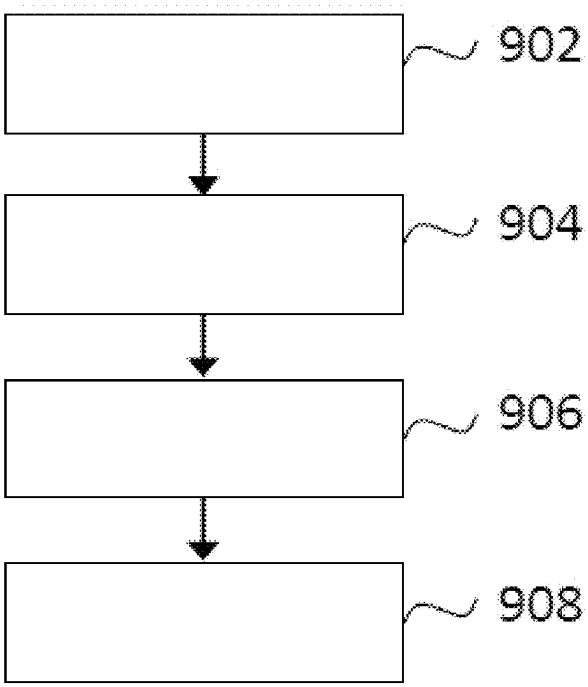


Fig. 9

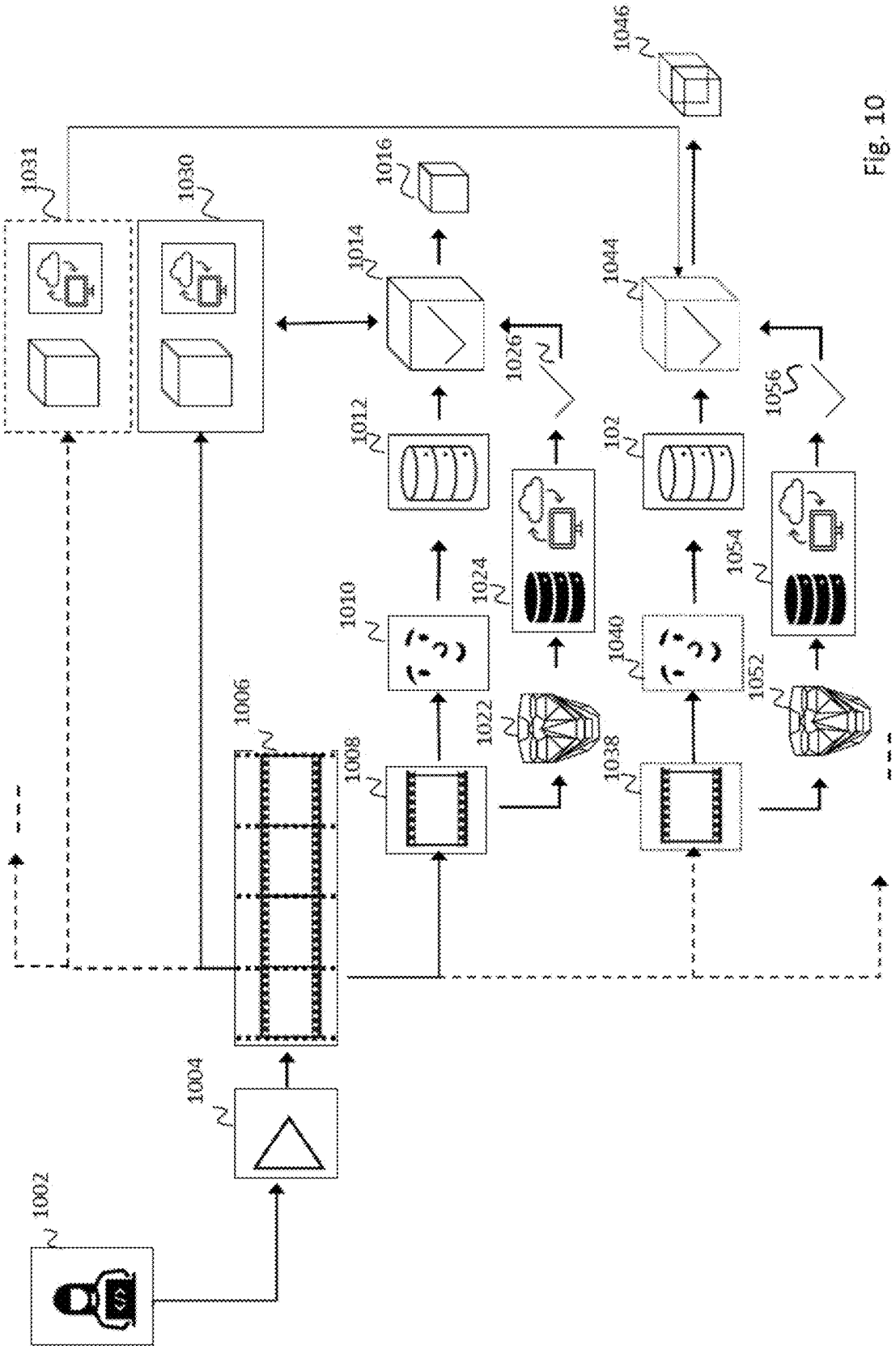

1002
1004
1006
1008
1010
1012
1014
1016
1022
1024
1026
1030
1031
1038
1040
1042
1044
1046
1052
1054
1056
102

Fig. 10

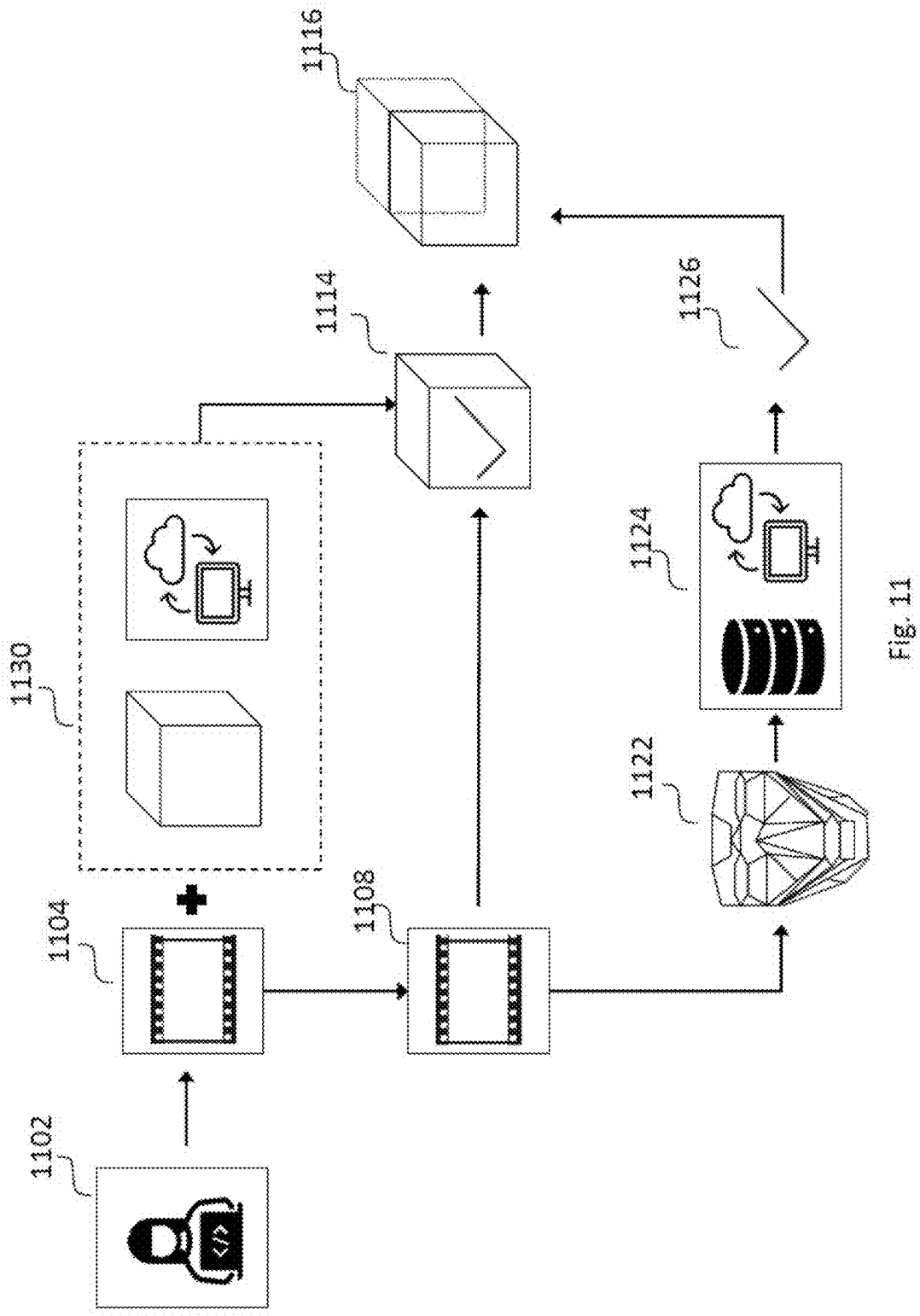


Fig. 11

METHOD FOR PROVIDING CONTENT FOR AUTHENTICATION AND AUTHENTICATING CONTENT

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The instant application claims priority to European Patent Application No. 24158852.4, filed Feb. 21, 2024, which is incorporated herein in its entirety by reference.

FIELD OF THE DISCLOSURE

[0002] The present disclosure generally relates to the field of content authentication linked to a specific content author and, more particularly, to distribution ledger-based methods and systems for providing authenticated content and/or verifying provided content of a content author.

BACKGROUND OF THE INVENTION

[0003] In recent years, due to existing technologies for creating realistic impersonations of people, numerous threats associated with forgery of identity or identity theft have been created in media content. As deepfake technology has evolved to be increasingly convincing and available to the public, media content can easily be manipulated to replace one person's likeness convincingly with that of another using artificial intelligence. In many cases, it is very difficult to differentiate between the truthful original content and the manipulated content. Hence, there is a need for methods to authenticate content, in particular, the truthfulness of the people's identity, actions, and/or behavior presented in media content.

[0004] Current methods are available for authenticating media content. In the prior art, authentication methods of content, such as the method described in U.S. Pat. No. 11,075,744 B2, involve distribution ledger-based methods for creating blocks of information associated with media recordings. In U.S. Pat. No. 10,176,309 B2 watermarked content segments are sent for authentication. For authentication, the content is checked, whether the received content segments correspond to the cryptographic representation of the sent water marked content segments. In WO 2022/049053 A1 content segments, specifically signed by a registered content owner, that are sent for authentication, are checked regarding whether the indicated content owner of the received content segments corresponds to the truthful identity of the content owner.

[0005] However, all these use cases do not aim specifically at the authentication of the identity of a person perceived or represented in the content. They do not confirm that the person represented in the content is indeed the indicated person and not a digitally manipulated counterfeit. As a result, misleading information can be disseminated to the public. In addition, identity theft and fraud can have a detrimental effect on cybersecurity.

BRIEF SUMMARY OF THE INVENTION

[0006] Given the known prior art, what is needed is a method that is able to authenticate and confirm a person perceived in media content as not manipulated or forged, in particular, resistant to deepfake technology.

[0007] The present disclosure describes a method to authenticate and/or verify content of a content author to be authentic, truthful, and not manipulated nor forged by means of distribution ledger-based methods and systems. Embodiments described herein include a computer-implemented method and device for providing content of a content author for authentication, and a computer-implemented method and device for authenticating a provided content of a content author.

[0008] In a first aspect of the disclosure, a computer-implemented method for providing content of a content author for authentication comprises: obtaining, by the content author, a first author fragment of content; generating a first state author vector from the first author fragment of content; and creating a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature.

[0009] Creating a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature enhances the security of authentication. By incorporating the first digital signature into the first block of key information, the content being exchanged cannot be altered or tampered with without the signature becoming invalid. It may verify the identity of the content author involved, ensuring that only the content author who is verified in the account can access and transact on the network. It may also provide non-repudiation, meaning parties cannot deny their involvement in the transaction. Thus, it increases transparency and trust in the system.

[0010] Authentication, in the context of the present disclosure, may generally refer to an ongoing or continuous verification process of the content author in the content. The first aspect of the disclosure aims at providing content of a content author for authentication.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S)

[0011] FIG. **1** is a schematic diagram of a device for providing content of a content author for authentication according to an embodiment of the present disclosure.

[0012] FIG. **1***a* is a schematic diagram of a device for providing content of a content author for authentication according to an embodiment of the present disclosure.

[0013] FIG. **2** is a schematic illustration of a device for authenticating a provided content of a content author according to an embodiment of the present disclosure.

[0014] FIG. **2***a* is a schematic illustration of a device for authenticating a provided content of a content author according to an embodiment of the present disclosure.

[0015] FIG. **3** is a schematic overview of a digital distribution ledger-based environment in which the method and system according to the present disclosure may be employed.

[0016] FIG. **4** is a flowchart for a method for providing content of a content author for authentication in accordance with an embodiment of the present disclosure.

[0017] FIG. **5** is a flowchart for a method for providing content of a content author for authentication in accordance with an embodiment of the present disclosure.

[0018] FIG. **6** is a flow diagram for a method for providing content of a content author for authentication in accordance with an embodiment of the present disclosure.

[0019] FIG. **7** is a flow diagram illustrating a method for providing content of a content author for authentication in accordance with an embodiment of the present disclosure.

[0020] FIG. **8** shows examples of state vectors in accordance with the disclosure.

[0021] FIG. **9** is a flow diagram illustrating a method for authenticating a provided content of a content author in accordance with an embodiment of the present disclosure.

[0022] FIG. **10** is a flow diagram illustrating a method for authenticating a provided content of a content author in accordance with an embodiment of the present disclosure.

[0023] FIG. **11** is a flow diagram illustrating a method for authenticating a provided content of a content author in accordance with an embodiment of the present disclosure.

DETAILED DESCRIPTION OF THE INVENTION

[0024] The methods of the present disclosure are useful in proving the identity of the content author as the rightful identity. In particular, the methods aim at proving that the behavior, actions, gestures, and/or acoustic phonetics or sounds conducted by the content author perceived in the content by the content user have not been modified. In the context of the disclosure, authentication may intend at a first level to prove that the person perceived in the content is indeed the content author or one of the content authors. Authentication may further intend at a second level to prove that the actions and/or the behavior and/or the voice of the person perceived in the content by the content user as rightful, original, authentic, and unmodified.

[0025] Methods and systems for providing content for authentication and authenticating content will now be described with reference to FIGS. **1** to **11** for the example of a device for providing content for authentication and authenticating provided content.

[0026] FIG. **1** shows a device for providing content of a content author for authentication **102** that comprises a content fragment unit **108**, an author state recognition unit **110**, an author communication unit **112** and a first output unit **114**, wherein each of the mentioned units may be also connected to a server system **106** via a communication network **104**, as shown in FIG. **1***a* and FIG. **3**. The device for providing content of a content author for authentication **102** may be a communication device, such as a computer, tablet computer or mobile phone, or part of an application on a mobile device. The device for providing content of a content author for authentication **102** may be employed by the content author.

[0027] The content fragment unit **108** is configured to obtain a first author fragment of content. The content fragment unit may further be configured to obtain a second author fragment of content.

[0028] The author state recognition unit **110** is adapted to generate a first state author vector from the first author fragment of content. The author state recognition unit **110** may be further configured to generate a second state author vector from the second author fragment of content.

[0029] The first output unit **114** is configured to create a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature.

[0030] The first output unit **114** may be further configured to create a second block of key information based on the second author fragment of content, wherein the second block of key information comprises information of the second state author vector and the second digital signature, wherein the second author fragment is a subsequent fragment of the first author fragment of content, wherein the first author fragment of content and the second author fragment of content are connected sequentially.

[0031] With reference to FIG. **1***a*, device **102** may be embedded in a content providing environment **100** which may be part of a digital media platform or an application on a mobile device.

[0032] As can be further taken from FIG. **1***a*, the content providing environment **100** comprises device **102** for providing content of a content author for authentication that is connected to the server system **106** via the communication network **104**. The device **102** may communicate via the communication network **104** and the server system **106** with the units **108** to **114**.

[0033] The author communication unit **112** may be configured to request a first certificate to create a first digital signature for the first author fragment of content from a key center. The author communication unit **112** may be further configured to request from the key center a second certificate to create a second digital signature for the second author fragment of content.

[0034] The communication network **104** may be a wired, wireless, or mixed network. In some examples, the communication network **104** may be the internet.

[0035] A schematic illustration that shows an embodiment of the device **102** with additional units is given in FIG. **3**.

[0036] FIG. **2** shows a device **202** for authenticating a provided content of a content author that comprises a content receiving unit **208**, a user communication unit **210**, an input unit **212** and an authentication unit **214**, wherein each of the mentioned units may be also connected to the server system **106** via the communication network **104**, as shown in FIG. **2***a* and FIG. **3**.

[0037] The device for authenticating a provided content of a content author **302** may be a communication device, such as a computer, tablet computer or mobile phone, or part of an application on a mobile device. The device for authenticating a provided content of a content author **302** may be employed by the content user **102** who wishes to authenticate the content provided by the content author for truthfulness of the content.

[0038] The content receiving unit **208** is configured to receive content from the content author.

[0039] The user communication unit **210** is configured to request from a key center information of a first block of key information based on a first author fragment of content, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature. The user communication unit **210** may be further configured to request from a key center information of a second block of key information based on a second author fragment of content, wherein the second author fragment of content is associated with the content author and wherein the second block of key information comprises information of a second state author vector and a second digital signature.

[0040] The input unit **212** is configured to obtain a first user fragment of content, wherein the first user fragment of content corresponds to the first author fragment of content. The input unit **212** may be further configured to obtain a

second user fragment of content, wherein the second user fragment of content corresponds to the second author fragment of content.

[0041] The authentication unit **214** is configured to verify and authenticate the content by checking the correctness of the first digital signature. The authentication unit **214** may be further configured to verify the content by checking the correctness of the second digital signature, wherein the authentication unit **214** may be further configured to send instructions to add the second block of key information to the first block of key information connecting the first block of key information and the second block of key information sequentially. In an example, the authentication unit **214** may be further configured to verify the content by comparing information from the second state user vector with information from the second block of key information.

[0042] A schematic illustration that shows an embodiment of the device **202** with additional units is given in FIG. **2***a* and FIG. **3**.

[0043] With reference to FIG. **2***a*, device **202** may be embedded in an authenticating content environment **200** which may be part of a digital media platform or an application on a mobile device.

[0044] As can be further taken from FIG. **2***a*, the device **202** for authenticating a provided content of a content author **302** may be connected to the server system **106** via the communication network **104** and may communicate via the communication network **104** and the server system **106** with the units **208** to **214**.

[0045] A schematic illustration that shows a digital distribution ledger-based environment **300** to which the method and system according to the present disclosure may be applied to is given in FIG. **3**.

[0046] As can be taken from FIG. **3**, the digital distribution ledger-based environment **300** may comprise a media platform environment **310**, a distributed ledger network **340**, the device for providing content of a content author for authentication **102**, the device for authenticating a provided content of a content author **202**, wherein each of them is connected to the communication network **104**. The communication network **104** may be a cloud environment.

[0047] The media platform environment **310** may provide a digital platform for the content author **102** and the content user **202** to interact with one another. The content author **302** may employ a communication device **301**, such as a computer, tablet computer, or mobile phone, or any device that is capable to provide content **306** for authentication. The content **306** may comprise multimedia elements. As an example, the content may comprise different digital media content forms of text, audio, images, animations, and/or video or a combination thereof. The content may be uploaded to the media platform. The content user **304** may employ a communication device, such as a computer, tablet computer, or mobile phone to authenticate the provided content **306** of the content author. The media platform may be an application installed on the communication device of the content author **302**. The media platform environment **310** may include a computer program comprising computer-readable instructions (not shown) that when the program is executed by a computer, cause the computer to carry out the method shown in FIG. **4** or FIG. **9**.

[0048] The distributed ledger network **340** may comprise a key center **341**, databases **342**, and a server system **106**. The distributed ledger network **340** may record all structural information that has been transmitted and received, such as transactions and updates, between the devices **102** and **202**, the media platform environment **310**, the network **104** and the server system **106**. The distributed ledger network may be linked to the media platform environment **310**, devices **102** and **202**, the key center **341**, the databases **342**, and the server system **106** via the communication network **104**. Some or all of these entities **310**, **102**, **202**, **341**, **342**, **106** may be operated or controlled by the distributed ledger network **340**. For example, the devices **102** and **202** may include a software client capable of communicating with the distributed ledger network **340**.

[0049] The distributed ledger network **340** may interact with devices **102** and **202**, in particular with the author communication unit **112**, the first output unit **114**, the user communication unit **210** and the authentication unit **214**, to manage cryptographic transaction data related to the state vector of the fragments of content within the digital distribution ledger-based environment **300**. It may verify and validate the transactions before adding them to the distributed ledger network. It may use cryptographic principles like hashing and digital signatures to encrypt data and ensure its integrity and confidentiality of the blocks of key information and content.

[0050] The distributed ledger **340** may further interact with the content fragment unit **108** and the content receiving unit to handle upload, storage, and access control for the content **306** on the media platform environment **310**. The plurality of fragments of content may be hashed, and the hash may be stored in the distributed ledger network **240**, which may ensure its immutability and authenticate its origin.

[0051] The distributed ledger **340** may further interact with the devices **102** and **202** to enable streaming the media content **306** of the content author **302** to the content user **304**.

[0052] The key center may comprise modules (not shown) that are configured to handle the registration of the content author **302** and the content user **304** and the authentication of the content author through registered biometrics vector data of the content author **302**. The key center may further keep track of who has permission to access the content **306**.

[0053] The key center **341** may comprise the databases **342**. The databases **342** may comprise the biometrics vector database and the state vector database.

[0054] The server system **106** may be a physical or a virtual server. The server system **106** may function as a distributed storage that may store the structural information about the blocks of key information. The server system **106** may use decentralized storage solutions based on blockchain technology that may increase security and reduce reliance of the digital distribution ledger-based environment **300**.

[0055] The device for providing content of a content author for authentication **102** may further comprise an author vector replacing unit **316**, a second output unit **318**, a biometrics data providing unit **320**, and a sending unit **322**.

[0056] The author vector replacing unit **316** may be configured to replace the first state author vector by a first database state author vector, wherein the first database state author vector is a vector of a state vectors database wherein a metric between the first state author vector and the first database state author vector lies below a pre-defined threshold value.

[0057] The second output unit **318** may be configured to generate the first author fragment after a pre-defined time of content has passed prior to obtaining the first author fragment of content.

[0058] The biometrics data providing unit **320** may be configured to provide biometrics vector data of the content author.

[0059] The sending unit **322** may be configured to send the biometrics vector data for verification and confirmation of the identity of the content author to the key center and further configured to send instructions to store verified biometrics vector data of the content author in a biometrics vector database.

[0060] The device for authenticating a provided content of a content author **202** may further comprise a user state recognition unit **326**, a user vector replacing unit **328**, a biometrics vector obtaining unit **330**, a first control unit **332**, and a second control unit **334**.

[0061] The user state recognition unit **326** may be configured to generate a first state user vector from the first user fragment of content. The user state recognition unit **326** may be further configured to generate a second state user vector from the second user fragment of content.

[0062] The user vector replacing unit **328** may be configured to replace the first state user vector by a first database state user vector, wherein the first database state user vector is a vector of a state vectors database wherein a metric between the first state user vector and the first database state user vector lies below a pre-defined threshold value.

[0063] The biometrics vector obtaining unit **330** may be configured to obtain a first biometrics vector from the first author fragment of content.

[0064] The first control unit **332** may be configured to compare the first biometrics vector with biometrics vector data of the content author stored in a biometrics vectors database. The first control unit **332** may be further configured to verify the biometrics vector.

[0065] The second control unit **334** may be configured to check the content for connectivity of a plurality of blocks and/or the presence of missing and/or excess blocks of the plurality of blocks.

[0066] FIG. **4** shows a flow diagram illustrating a method for providing content of a content author for authentication in accordance with an embodiment of the present disclosure. This method may be initiated by the content user.

[0067] In a first step **402**, a first author fragment of content is obtained by the content author.

[0068] In a second step **404**, a first state author vector from the first author fragment of content is generated.

[0069] In a third step **408**, a first block of key information based on the first author fragment of content is created, wherein the first block of key information comprises information of the first state author vector and the first digital signature.

[0070] FIGS. **4** and **5** show the method from the perspective of the device for providing content of a content author for authentication. A more in-depth example of the method for providing content of a content author for authentication is given in FIG. **5**.

[0071] FIG. **5** shows the method for providing content of a content author for authentication applied to pre-recorded content.

[0072] In a first step **502**, content may be created by a content author. The content author may represent a plurality of persons registered in an account of the content author. The content author may be perceived audibly, visually, or in both manner in the content.

[0073] In a second step **504**, the content may be obtained. The content provided for authentication may be pre-recorded. The content may be any multimedia element. The content may be recorded by a camera or smartphone or any tool that can record multimedia.

[0074] In a third step **506**, the content may be fragmentized in a plurality of fragments, wherein the content may be fragmentized according to a pre-defined rule, and, optionally, wherein the pre-defined rule comprises the fragmentation of content in a pre-defined number of equal fragments.

[0075] In a step **508**, a first author fragment of content is obtained by the content author. The first author fragment of content may be one of the plurality of fragments, wherein a block of key information may be created for each of the fragments of the plurality of fragments. Step **508** may correspond to step **402** of FIG. **4**.

[0076] In a step **510**, a first state author vector from the first author fragment of content is generated. The first state author vector may not be confined to the states of the content author but may also pertain to the actions of the content author. Further examples of the state author vector are given in FIG. **8**. Step **510** may correspond to step **404** of FIG. **4**.

[0077] In a step **512**, the first state author vector may be replaced by a first database state author vector, wherein the first database state author vector is a vector of a state vectors database, wherein a metric between the first state author vector and the first database state author vector lies below a pre-defined threshold value.

[0078] The state vectors database may refer to a database that stores vector data of the outward appearance, the face comprising the structural composition of the face and/or expressions of the face, the body comprising the structural composition of the body and/or movements of the body, the voice, or similar aspects of different persons who may not be the content author. Each vector may consist of a set of numerical values or features that describe the characteristics of an object. The object may be related to the outward appearance, the face comprising the structural composition of the face and/or expressions of the face, the body comprising the structural composition of the body and/or movements of the body, the voice, or similar aspects. The state vectors database may employ similarity search, where the goal is to retrieve vectors that are similar to the first state author vector. By using appropriate distance metrics, such as Euclidean distance or cosine similarity, the state vectors database may quickly identify similar vectors within the database. The most similar vector may be chosen as the first database state author vector replacing the first state author vector.

[0079] As an advantage of replacing the first state author vector by a first database state author vector, stability of the system may be increased, as bringing all vectors to a common standard, the system as well as all comparison operations may be simplified. As a further advantage, the computational power as well as the memory requirements can be decreased, since the identifier of the first state author vector can be replaced by the number of the first database state author vector in the state vectors database, instead of saving the entire data information of the first state vector itself. Hence, the storage space of the first block of key information may be saved.

[0080] In a step **514**, a first certificate to create a first digital signature for the first author fragment of content may be requested from a key center.

[0081] The first digital signature may be used for verification of authenticity. It may help in affirming that the sender of the key information, which may be the content author, is legitimate and not an impostor. It further may confirm that the block of key information sent has not been altered in transit. It may help in validating that the signer that may be the content author or the key center is authorized to carry out certain transactions or may have permission to access data. The digital signature may guarantee security, trust, and consent. It may ensure the secure conduct of the transactions of the blocks of key information and may enable a system to which the methods and devices of the present disclosure are applied to be tamper evident.

[0082] The key center may contain all information related to the content author or may access all information about the content author. The information of the content author may relate to the registered biometrics data of the content author and the content. Further information regarding biometrics data is given in FIG. **7**.

[0083] In a step **516**, a first block of key information based on the first author fragment of content is created, wherein the first block of key information comprises information of the first state author vector and the first digital signature. Step **516** may correspond to step **408** of FIG. **4**.

[0084] The first block of key information may further comprise information about the numbering of the first block of key information, and/or a preceding state author vector, wherein the preceding state author vector is obtained from a fragment of content preceding the first author fragment, and/or the first certificate for verification of the first digital signature. Said information may pertain to structural information about the first block of key information.

[0085] In a further step (not shown), the structural information about the first block of key information may be transmitted by the content author to the key center.

[0086] In an additional step (not shown), instructions for storing the information in a distributed ledger linked to an account of the content author may be sent.

[0087] Steps **508** to **516** may be repeated for a second author fragment of content by steps **518** to **526**. The second author fragment of content may be one of the plurality of fragments, wherein the first author fragment precedes the second author fragment of content.

[0088] In step **518**, a second author fragment of content is obtained.

[0089] In step **520**, a second state author vector from the second author fragment of content is generated.

[0090] In step **522**, the second state author vector may be replaced by a second database state author vector, wherein the second database state author vector may be a vector of a state vectors database, wherein a metric between the second state author vector and the second database state author vector may lie below a pre-defined threshold value.

[0091] In step **524**, a second certificate to create a second digital signature for the second author fragment of content may be requested from the key center.

[0092] In step **526**, a second block of key information based on the second author fragment of content may be created, wherein the second block of key information comprises information of the second state author vector and the second digital signature, wherein the second author fragment may be a subsequent fragment of the first author fragment of content, wherein the first author fragment of content and the second author fragment of content may be connected sequentially. The second block of key information may be a subsequent block of key information of the first block of key information. The first block of key information may be a previous or a preceding block of key information in relation to a second block of key information. The second block of key information may be a next block of key information succeeding the first block of key information. This may be the case in any embodiment comprising a first and a second block of key information, a pair of blocks of key information or a chain of blocks of key information. The first and/or second block of key information may be part of a plurality of (any number of) blocks of key information, such as a blockchain.

[0093] The first state author vector and the second state author vector each may be linked to a timestamp of the content.

[0094] Steps **508** to **516** may be repeated until a block of key information for all author fragments of content of the plurality of fragments has been created.

[0095] FIG. **6** shows the method for providing content of a content author for authentication applied to real-time content. Therefore, the example of the method shown in FIG. **6** differs from the example shown in FIG. **5** in that the content is transmitted in real-time.

[0096] In a first step **602**, content may be created by a content author. The content author may represent a plurality of persons registered in an account of the content author. The content author may be perceived audibly, visually, or in both manner in the content.

[0097] In a second step **604**, the content provided for authentication may be transmitted in real-time. Hence, the first author fragment may be generated after a pre-defined time of content has passed prior to obtaining the first author fragment of content. The content may be any multimedia element. The content may be recorded by a camera or smartphone or any tool that can record multimedia.

[0098] In step **608**, a first author fragment of content is obtained by the content author. Step **608** may correspond to step **402** of FIG. **4**.

[0099] In step **610**, a first state author vector from the first author fragment of content is generated. Step **610** may correspond to step **404** of FIG. **4**.

[0100] In step **612**, the first state author vector may be replaced by a first database state author vector, wherein the first database state author vector may be a vector of a state vectors database, wherein a metric between the first state author vector and the first database state author vector may lie below a pre-defined threshold value.

[0101] In step **614**, a first certificate to create a first digital signature for the first author fragment of content is requested from a key center.

[0102] In step **616**, a first block of key information is created based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature. The first block of key information may further comprise information about the biometrics of the content author, the timestamp of the first state author vector, and/or the first certificate for verification of the first digital signature. Step **616** may correspond to step **408** of FIG. **4**.

[0103] In step **618**, the first block of key information may be sent to a content user, who intends to verify the truthfulness of the content provided by the content author and the identity of the person perceived in the content.

[0104] Steps **608** to **618** may be repeated for every author fragment that has been generated after passing a pre-defined time of content transmitted in real-time until the real-time transmission of content has ceased.

[0105] FIG. **7** shows a further example of the method from the perspective of the biometrics data providing unit **320**.

[0106] In step **702**, biometrics vector data of the content author may be provided by the content author.

[0107] Because the content author may represent one or more persons to be verified in the content, biometrics vector data for one or multiple persons may be provided, as can be taken from step **704**. The biometrics vector data for one or multiple persons may be linked to an account of the content author, wherein the account of the content author in the key center is linked to the biometrics vector database.

[0108] In step **708**, the biometrics vector data may be sent for verification and confirmation of the identity of the content author to the key center.

[0109] In step **710**, instructions for storing verified biometrics vector data of the content author in a biometrics vector database may be sent.

[0110] FIG. **8** shows examples of state vectors. This list is not exhaustive. The state author vector may not only refer to the state of the content author at said specific time in the content, but also generally to the state of being or physical condition of the content author at said specific time in the content. For example, the state author vector may comprise parameters of the content author's state or physical condition. The parameters of the content author's state or condition may relate to personal characteristics of the content author. They may pertain to the outward appearance, the face comprising the structural composition of the face and/or expressions of the face, the body comprising the structural composition of the body and/or movements of the body, the voice, or similar aspects of the content author.

[0111] FIG. **9** shows a flow diagram illustrating an example of a method for authenticating a provided content of a content author from the complementary perspective of a content user.

[0112] In a first step **902**, the content of the content author is received by the content user.

[0113] In a second step **904**, information of a first block of key information based on a first author fragment of content is requested from a key center, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature.

[0114] In a third step **906**, a first user fragment of content is obtained, wherein the first user fragment of content corresponds to the first author fragment of content.

[0115] In a fourth step **908**, the content is authenticated checking the correctness of the first digital signature.

[0116] A more in-depth example of the method for authenticating the provided content of a content author from the complementary perspective of a content user is given in FIG. **10**.

[0117] In step **1002**, a content user may be a person who intends to authenticate the identity of the content author. The content user may be a person who consumes the content provided by the content author.

[0118] In a step **1004**, the content of the content author is received by the content user. Step **1004** may correspond to step **902** of FIG. **9**. The received content may be pre-recorded.

[0119] In a step **1006**, the received content may be fragmentized in a plurality of fragments, wherein the first author fragment of content is one of the plurality of fragments. The content may be fragmentized according to a pre-defined rule, and, optionally, wherein the pre-defined rule may comprise the fragmentation of content in a pre-defined number of equal fragments.

[0120] In a step **1030**, information of a first block of key information based on a first author fragment of content is requested from a key center, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature. Step **1030** may correspond to step **904** of FIG. **9**.

[0121] Step **1030** may comprise requesting biometrics vector data of the content author perceived in the content from the key center.

[0122] In a step **1008**, a first user fragment of content is obtained, wherein the first user fragment of content corresponds to the first author fragment of content. Step **1008** may correspond to step **906** of FIG. **9**.

[0123] In the case of untampered content, when the user fragment of content corresponds to the author fragment of content, the user fragment of content and the author fragment of content may be identical.

[0124] In a step **1010**, a first state user vector from the first user fragment of content may be generated.

[0125] In a step **1012**, the first state user vector may be replaced by a first database state user vector, wherein the first database state user vector may be a vector of a state vectors database wherein a metric between the first state user vector and the first database state user vector may lie below a pre-defined threshold value.

[0126] In a step **1014**, the content is authenticated by comparing information of the first state user vector with information of the first block of key information and checking the correctness of the first digital signature. Step **1014** may correspond to step **908** of FIG. **9**.

[0127] In an additional step (not shown), the content may be authenticated by comparing information of the first state user vector with information of the first block of key information.

[0128] In a step **1016**, the authenticated first block of key information may be created.

[0129] Steps **1030** and **1008** to **1016** may be repeated for a second author fragment of content until every author fragment of content of the plurality of author fragments of content has been authenticated.

[0130] In a step **1031**, information of a second block of key information based on a second author fragment of content may be requested from the key center, wherein the second author fragment of content may be associated with the content author and wherein the second block of key information may comprise information of a second state author vector and a second digital signature.

[0131] In a step **1038**, a second user fragment of content may be obtained, wherein the second user fragment of content may correspond to the second author fragment of content.

[0132] In a step **1040**, a second state user vector from the second user fragment of content may be generated.

[0133] In a step **1042**, the second state user vector may be replaced by a second database state user vector, wherein the second database state user vector is a vector of a state vectors database wherein a metric between the second state user vector and the second database state user vector lies below a pre-defined threshold value.

[0134] In a step **1044**, the content is authenticated by checking the correctness of the second digital signature.

[0135] In an additional step (not shown), the content may be verified by comparing information of the second state user vector with information of the second block of key information.

[0136] In a further step (not shown), the content may be checked for connectivity of a plurality of blocks and/or the presence of missing and/or excess blocks of the plurality of blocks.

[0137] In a step **1046**, instructions to add the second block of key information to the first block of key information may be sent connecting the first block of key information and the second block of key information sequentially. The second block of key information may be connected to the first block of key information through a hash value of the first block of key information.

[0138] In addition to authenticating the content by checking the correctness of the first digital signature and by comparing information of the first state user vector with information of the first block of key information, biometrics data of the content author perceived in the content is verified.

[0139] Therefore, the method illustrated in FIG. **10** may further comprise steps related to the verification of biometrics data.

[0140] In a step **1022**, a first biometrics vector from the first user fragment of content may be obtained by the content user.

[0141] In a step **1024**, the first biometrics vector may be compared with the biometrics vector data of the content author stored in a biometrics vectors database.

[0142] In a step **1026**, the first biometrics vector may be verified. Verified biometrics information of the first biometrics vector may be stored in the first block of key information. The verifying of the first state user vector and the first biometrics vector may be conducted independently of each other.

[0143] Steps **1022** to **1026** may be repeated for an additional user fragment of content, such as the second user fragment of content until every author fragment of content of the plurality of fragments regarding the biometrics data of the content author has been verified.

[0144] In a step **1052**, a second biometrics vector from the second user fragment of content may be obtained by the content user.

[0145] In a step **1054**, the second biometrics vector may be compared with the biometrics vector data of the content author stored in a biometrics vectors database.

[0146] In a step **1056**, the second biometrics vector may be verified. Verified biometrics information of the second biometrics vector may be in the first block of key information. The verifying of the second state user vector and the second biometrics vector may be conducted independent of each other.

[0147] FIG. **11** shows the method for authenticating a provided content of a content author applied to real-time content. Therefore, the example of the method shown in FIG. **11** differs from the example shown in FIG. **10** in that the content is received in real-time.

[0148] In a step **1102**, a content user may be a person who intends to authenticate the identity of the content author. The content user may be a person who consumes the content provided by the content author.

[0149] In a step **1104**, the content of the content author is received by the content user. The content may be received in real-time. Step **1104** may correspond to step **902** of FIG. **9**.

[0150] In a step **1130**, information of a first block of key information based on a first author fragment of content is requested from a key center, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature. Step **1130** may correspond to step **904** of FIG. **9**.

[0151] Step **1030** may comprise requesting biometrics vector data of the content author perceived in the content from the key center.

[0152] In a step **1108**, a first user fragment of content is obtained, wherein the first user fragment of content corresponds to the first author fragment of content. Step **1108** may correspond to step **906** of FIG. **9**.

[0153] In a step **1114**, the content is authenticated by comparing information of the first state user vector with information of the first block of key information and checking the correctness of the first digital signature. Step **1114** may correspond to step **908** of FIG. **9**.

[0154] In a step **1116**, the authenticated first block of key information may be created.

[0155] Steps **1130** and **1108** to **1116** may be repeated for an additional author fragment of content, such as second author fragment of content, until the real-time transmission of content has ceased.

[0156] In a further step, information of a second block of key information based on a second author fragment of content is requested from the key center, wherein the second author fragment of content is associated with the content author and wherein the second block of key information comprises information of a second state author vector and a second digital signature.

[0157] In addition to authenticating the content by checking the correctness of the first digital signature, biometrics data of the content author perceived in the content may be also verified.

[0158] Therefore, the method illustrated in FIG. **11** may further comprise steps related to the verification of biometrics data.

[0159] In a step **1122**, a first biometrics vector from the first user fragment of content may be obtained by the content user.

[0160] In a step **1124**, the first biometrics vector may be compared with biometrics vector data of the content author stored in a biometrics vectors database.

[0161] In a step **1126**, the first biometrics vector may be verified. Verified biometrics information of the first biometrics vector may be stored in the first block of key informa-

tion. The verifying of the first state user vector and the first biometrics vector may be conducted independently of each other.

[0162] Steps **1022** to **1026** may be repeated for an additional user fragment of content, such as the second user fragment of content, until the real-time transmission of content has ceased.

[0163] In the context of the disclosure, authentication may refer to the process of determining whether an entity, in particular a content author, is what it declares to be. In the context of the disclosure, this may be achieved through the use of passwords, digital certificates, and/or biometrics data. Embodiments of the present disclosure authenticate that the content is truthful to the information associated with the content author.

[0164] According to an embodiment, after generating the first state author vector from the first author fragment of content, the method may further comprise: requesting from a key center a first certificate to create a first digital signature for the first author fragment of content. Requesting from a key center a first certificate to create a first digital signature for the first author fragment of content may enhance the security of authentication.

[0165] The certificate requested from the key center may comprise a public key and identification information of the content author.

[0166] The content, in the context of the present disclosure, may generally refer to media content consumed or produced by the content author. In particular, the content may comprise multimedia elements. As an example, the content may comprise different digital media content forms of text, audio, images, animations, and/or video or a combination thereof. The content may be uploaded to a digital platform.

[0167] In some examples, the content may be pre-recorded.

[0168] In the context of the present disclosure, the content may be produced by the content author.

[0169] The content author, in the context of the present disclosure, may be part of the content and/or recognized in the content as the content author. The content author may be perceived audibly or visually in the content. As an example, the content author may be perceived by the outward appearance, the face comprising the structural composition of the face and/or expressions of the face, the body comprising the structural composition of the body and/or movements of the body, the voice, or similar aspects related to personal characteristics of the content author.

[0170] The content author may be linked or registered to an account of a digital platform. The content author may be verified in the account of the digital platform. The content author may represent one or more persons who wish to be authenticated in the content, wherein the one or more persons to be authenticated in the content may be linked to an account of the content author.

[0171] In some examples, the content may be fragmentized in a plurality of fragments of content, wherein the first author fragment of content may be one of the plurality of fragments of content, wherein a block of key information may be created for each of the plurality of fragments of content.

[0172] In some examples, the content may be fragmentized according to a pre-defined rule, and, optionally, wherein the pre-defined rule may comprise the fragmentation of content in a pre-defined number of equal fragments of content.

[0173] The state author vector, in the context of the present disclosure, may refer to a mathematical vector that contains data about the state of being or physical condition of the content author at a specific time in the content. The state author vector may not only refer to the state of the content author at said specific time in the content, but also generally to the state of being or physical condition of the content author at said specific time in the content. For example, the state author vector may comprise parameters of the content author's state or physical condition. The parameters of the content author's state or condition may relate to personal characteristics of the content author. They may pertain to the outward appearance, the face comprising the structural composition of the face and/or expressions of the face, the body comprising the structural composition of the body and/or movements of the body, the voice, or similar aspects of the content author. For instance, in some examples, the first state author vector may be linked to a timestamp of the first author fragment of content.

[0174] Another state author vector may be generated for each of the plurality of fragments of content.

[0175] As an advantage, the method according to the present disclosure may enable the actions of the content author to be recorded, captured, registered and/or grasped independently, for instance, from biometrics data in the method.

[0176] The key center, in the context of the present disclosure, may be an independent trusted party, for instance, a software-based online infrastructure that facilitates interactions and transactions between users such as a digital platform. The key center may comprise the account of the content author. The key center may store information about the content author that might be necessary for the authentication, for instance, biometrics data, a password and/or a cryptographic key. The key center may have access, and/or control over the information of the content author.

[0177] The first block of key information, in the context of the disclosure, may be cryptographic transaction data related to the first state author vector of the first author fragment of content.

[0178] The first block of key information may be an intermittent block of a blockchain.

[0179] In some examples, the first block of key information may further comprise information about numbering of the first block of key information, and/or a preceding state author vector, wherein the preceding state author vector may be obtained from a fragment of content preceding the first author fragment, and/or the first certificate for verification of the first digital signature.

[0180] The first digital signature for the first block of key information may be created using a private key of the content author. The first digital signature may be created by the key center.

[0181] According to an example, the method may further comprise: transmitting, by the content author, structural information of the first block of key information to the key center; and sending instructions for storing the structural information in a distributed ledger linked to an account of the content author.

[0182] The structural information of the first block of key information, in the context of this disclosure, may comprise

a unique identifier, a timestamp, and/or a cryptographic hash from a preceding block. The structural information of the first block of key information may be stored in any format, such as a file or a QR-code. The file or the QR-code may be directly linked to the content.

[0183] The unique identifier may be the numbering of the first block of key information, in particular, the unique identifier may be a block number regarding the position of the first block of key information in the blockchain.

[0184] The timestamp may be linked to a timestamp of the first author fragment of content.

[0185] The cryptographic hash from the preceding block may relate to the preceding state author vector of the fragment of content preceding the first author fragment of content.

[0186] If the structural information inside the block was tampered with, the cryptographic hash of the block of key information will change as well. These pieces of structural information may ensure the integrity, security, and continuity of the content of the content author for the content user.

[0187] According to an example, the method may further comprise, prior to creating the first block of key information based on the first author fragment of content: replacing the first state author vector by a first database state author vector, wherein the first database state author vector is a vector of a state vectors database wherein a metric between the first state author vector and the first database state author vector lies below a pre-defined threshold value.

[0188] The state vectors database may refer to a database that stores mathematical vector data that contains data about a state of being or physical condition of different persons who may not be the content author. Each mathematical vector may consist of a set of numerical values or features that describe the characteristics of the state of being or physical condition. The state of being or physical condition may be related to an outward appearance, a face comprising the structural composition of the face and/or expressions of the face, a body comprising the structural composition of the body and/or movements of the body, a voice, or similar aspects of a person. By using appropriate distance metrics, such as Euclidean distance or cosine similarity, a database state author vector most similar to the first state author vector within the state vectors database may be identified.

[0189] The state author vector may be different from the database state author vector. The first database state author vector that may be closest in similarity to the state author vector may replace the first state author vector.

[0190] As an advantage of replacing the first state author vector by a first database state author vector, stability of the system may be increased, as bringing all vectors to a common standard, the system as well as all comparison operations may be simplified. As a further advantage, the computational power as well as the memory requirements can be decreased, since the identifier of the first state author vector can be replaced by the number of the first database state author vector in the state vectors database, instead of saving the entire data information of the first state vector itself. Hence, the storage space of the first block of key information may be saved.

[0191] According to an embodiment, the method may further comprise: prior to obtaining the first author fragment of content, passing a pre-defined time of content that is transmitted continuously.

[0192] According to an embodiment, the method may further comprise: generating the first author fragment after passing a pre-defined time of content.

[0193] In the embodiment mentioned above, the content may be transmitted in real-time. In particular, the content may be delivered and consumed in a continuous manner by a content user. For instance, the content may be a real-time streaming of multimedia elements.

[0194] The predefined time may refer to a specific point or duration that has been predetermined or established in advance.

[0195] As an advantage of the method, creating a first block of key information after passing the pre-defined time of content, wherein the content may be transmitted in real-time, may enable the authentication of real-time content, and therefore, the direct communication that the content author is truthful, trustful, and authentic as perceived in the content transmitted in real-time is possible.

[0196] According to an example, subsequent to creating the first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature, the method may further comprise: sending the first block of key information to the content user.

[0197] In particular, the first block of key information may further comprise information about the biometrics of the content author, the timestamp of the first state author vector, and/or the first certificate for verification of the first digital signature.

[0198] As an advantage of the method, sending the first block of key information to the content user enables the authentication of real-time content. The content may be verified simultaneously to consuming the content, therefore, the direct communication that the content author is truthful, trustful, and authentic as perceived in the content transmitted in real-time is possible.

[0199] According to an example, the method may further comprise: providing, by the content author, biometrics vector data of the content author; sending the biometrics vector data for verification and confirmation of the identity of the content author to the key center; sending instructions for storing verified biometrics vector data of the content author in a biometrics vector database.

[0200] The biometrics vector data, in the context of the disclosure, may refer to mathematical vectors of biometric characteristics or attributes of the content author. The biometrics vector data may comprise facial features, voice patterns, and/or gait patterns of the content author. The biometrics vector data may be registered biometrics vector data of the content author.

[0201] The biometrics vector data may be used as identity verification of the content author. The biometrics vector data may further be used for access control to the account of the content author. The biometrics vector data may be used to authenticate the identity of the content author in each fragment of content.

[0202] In some examples, the content author may represent one or more persons to be verified in the content, wherein one or more persons to be verified in the content are linked to an account of the content author, wherein the biometrics vector data for the one or more persons is provided in the account of the content author.

[0203] In some examples, the account of the content author in the key center may be linked to the biometrics vector database.

[0204] The biometrics vector obtained at any given time may refer to the same verified biometrics vector data in the biometrics vector database. As an advantage, the use of biometrics vector data of the content author may add an additional authentication level for the content author. The state author vector primarily may refer to the authentication of the actions conducted by the content author in the content. The biometrics vector data may refer to the authentication of the identity of the content author. This implementation may further increase the confidentiality, integrity, and authentication of the content. It may increase the efficiency, transparency, security, and trust in the authentication method. It may further help protect against fraud, unauthorized access, and tampering of content.

[0205] According to an example, the method further comprises obtaining a second author fragment of content; generating a second state author vector from the second author fragment of content; creating a second block of key information based on the second author fragment of content, wherein the second block of key information comprises information of the second state author vector and the second digital signature, wherein the second author fragment is a subsequent fragment of the first author fragment of content, wherein the first author fragment of content and the second author fragment of content are connected sequentially.

[0206] According to an example, after generating the second state author vector from the second author fragment of content, the method may further comprise: requesting from a key center a second certificate to create a second digital signature for the second author fragment of content.

[0207] In some examples, the content may be fragmentized in a plurality of fragments, wherein the first author fragment of content and the second author fragment of content each may be one of the plurality of fragments, wherein a block of key information may be created for each of the fragments of the plurality of fragments, wherein the first author fragment may precede the second author fragment of content.

[0208] In some examples, the second block of key information may be a subsequent block of key information of the first block of key information. The first block of key information may be a previous or a preceding block of key information in relation to a second block of key information. The second block of key information may be a next block of key information succeeding the first block of key information.

[0209] In general, in implementations of the disclosure there may be any number of blocks of key information.

[0210] For instance, in some examples, the second state author vector may be linked to another timestamp of the content different from the timestamp of the first state author vector.

[0211] In some examples, the second block of key information may further comprise information about numbering of the second block of key information, and/or the first state author vector, and/or the second certificate for verification of the first digital signature. The numbering of the second block of key information in relation to the first block of key information may be incremented by one.

[0212] In the first aspect, the disclosure additionally relates to a device for providing of a content author for authentication, comprising a content fragment unit, configured to obtain a first author fragment of content. The device further comprises an author state recognition unit, configured to generate a first state author vector from the first author fragment of content, and a first output unit, configured to create a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and the first digital signature.

[0213] According to an embodiment, the device may further comprise an author communication unit, configured to request from a key center a first certificate to create a first digital signature for the first author fragment of content.

[0214] According to an embodiment, the device may further comprise an author vector replacing unit, configured to replace the first state author vector by a first database state author vector, wherein the first database state author vector may be a vector of a state vectors database wherein a metric between the first state author vector and the first database state author vector may lie below a pre-defined threshold value.

[0215] In an example, the device may further comprise a second output unit, configured to generate the first author fragment after passing a pre-defined time of content prior to obtaining the first author fragment of content.

[0216] Alternatively, the device may further comprise a biometrics data providing unit, configured to provide biometrics vector data of the content author; a sending unit, configured to send the biometrics vector data for verification and confirmation of the identity of the content author to the key center, the sending unit, further configured to send instructions to store verified biometrics vector data of the content author in a biometrics vector database.

[0217] According to an embodiment, the content fragment unit may further be configured to obtain a second author fragment of content; the author state recognition unit may be further configured to generate a second state author vector from the second author fragment of content; the author communication unit may be further configured to request from the key center a second certificate to create a second digital signature for the second author fragment of content; the first output unit may be further configured to create a second block of key information based on the second author fragment of content, wherein the second block of key information comprises information of the second state author vector and the second digital signature, wherein the second author fragment may be a subsequent fragment of the first author fragment of content, wherein the first author fragment of content and the second author fragment of content may be connected sequentially.

[0218] In a second aspect, the disclosure relates to a computer-implemented method for authenticating a provided content of a content author, comprising: receiving, by the content user, content of the content author; requesting from a key center information of a first block of key information based on a first author fragment of content, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature; obtaining a first user fragment of content, wherein the first user fragment of content corresponds to the first author fragment of content; and authenticating the content by checking the correctness of the first digital signature.

[0219] The second aspect of the disclosure aims at authenticating the provided content of the content author.

[0220] According to an example, the method according to the second aspect of the disclosure, may further comprise: Verifying the first digital signature using a first certificate retrieved from the first block of key information.

[0221] The first block of key information may further comprise information of a first certificate.

[0222] The first certificate may comprise a public key of the content author.

[0223] In the case of untampered content, when the user fragment of content corresponds to the author fragment of content, the user fragment of content and the author fragment of content may be identical.

[0224] According to an example, the method according to the second aspect of the disclosure, may further comprise: obtaining, by the content user, a first biometrics vector from the first user fragment of content; comparing the first biometrics vector with biometrics vector data of the content author stored in a biometrics vectors database.

[0225] The method according to the second aspect of the disclosure may further comprise: verifying the biometrics vector and the first state user vector, wherein the verifying of the first state user vector and the biometrics vector is independent of each other.

[0226] According to an embodiment, the received content may be fragmentized in a plurality of fragments prior to obtaining the first author fragment of content, wherein the first author fragment of content may be one of the plurality of fragments.

[0227] In some examples, the received content may be pre-recorded.

[0228] In some examples, the content may be fragmentized according to a pre-defined rule, and, optionally, wherein the pre-defined rule may comprise the fragmentation of content in a pre-defined number of equal fragments.

[0229] According to an example, the method of the second aspect may further comprise: generating a first state user vector from the first user fragment of content; and verifying the content by comparing information of the first state user vector with information of the first block of key information.

[0230] In some examples, the method of the second aspect may further comprise, prior to requesting from the key center information of the first block of key information based on the first author fragment of content: replacing the first state user vector by a first database state user vector, wherein the first database state user vector is a vector of a state vectors database wherein a metric between the first state user vector and the first database state user vector lies below a pre-defined threshold value.

[0231] The first database state user vector and the first database state author vector may be a vector from the same state vectors database.

[0232] According to an example, the method of the second aspect may further comprise: checking a plurality of blocks for the presence of missing and/or excess blocks of the plurality of blocks.

[0233] The plurality of blocks may refer to a plurality of blocks of key information that have been created based on the plurality of author fragments of content and contain the digital signature. The plurality of blocks may be received by the content user from the key center. The plurality of blocks may represent a continuous structure of the content. Excess blocks and/or missing blocks within the plurality of blocks may indicate a change in the continuous structure of the content and may indicate a tampering of the content, as fragments of content might have been added or removed from the plurality of blocks.

[0234] According to an embodiment, the content according to the second aspect of the disclosure may be received in real-time.

[0235] According to an example, the method of the second aspect may further comprise: requesting from a key center information of a second block of key information based on a second author fragment of content, wherein the second author fragment of content may be associated with the content author and wherein the second block of key information may comprise information of a second state author vector and a second digital signature; obtaining a second user fragment of content, wherein the second user fragment of content may correspond to the second author fragment of content; authenticating the content by checking the correctness of the second digital signature; and sending instructions to add the second block of key information to the first block of key information connecting the first block of key information and the second block of key information sequentially.

[0236] According to an example, the method of the second aspect may further comprise: generating a second state user vector from the second user fragment of content; and verifying the content by comparing information of the second state user vector with information of the second block of key information.

[0237] According to an example, the second block of key information according to the second aspect of the disclosure may be connected to the first block of key information through a hash value of the first block of key information.

[0238] The hash value, in the context of the present disclosure, is a cryptographic hash that may be a unique alphanumeric string generated by a hash function. The hash value may serve as a unique digital fingerprint for the contents of each block of key information and may carry information from the preceding block of key information, linking the blocks of key information together in a secure chain. The hash value may be used to ensure the integrity, security, and continuity of the content. The smallest changes to the block of key information would create a completely different hash value, making the network tamper-proof, as any changes would be noticeable. The hash value may be used for the maintenance, authentication, and validation processes of a distributed ledger.

[0239] In the second aspect, the disclosure additionally relates to a device for authenticating a provided content of a content author, comprising: a content receiving unit, configured to receive content of the content author; a user communication unit, configured to request from a key center information of a first block of key information based on a first author fragment of content, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature; an input unit, configured to obtain a first user fragment of content, wherein the first user fragment of content corresponds to the first author fragment of content; and an authentication unit, configured to authenticate the content by checking the correctness of the first digital signature.

[0240] In an example, the device of the second aspect may further comprise a biometrics vector obtaining unit, configured to obtain a first biometrics vector from the first author fragment of content; a first control unit, configured to compare the first biometrics vector with biometrics vector data of the content author stored in a biometrics vectors database.

[0241] In an example, the first control unit of the second aspect of the disclosure may be further configured to verify the biometrics vector.

[0242] In an example, the device of the second aspect may further comprise a user state recognition unit, configured to generate a first state user vector from the first user fragment of content.

[0243] In an example, the device of the second aspect may further comprise a user vector replacing unit, configured to replace the first state user vector by a first database state user vector, wherein the first database state user vector may be a vector of a state vectors database wherein a metric between the first state user vector and the first database state user vector may lie below a pre-defined threshold value.

[0244] In an example, the device of the second aspect may further comprise a second control unit, configured to check the content for connectivity of a plurality of blocks and/or the presence of missing and/or excess blocks of the plurality of blocks.

[0245] In an example, the user communication unit of the second aspect may be further configured to request from a key center information of a second block of key information based on a second author fragment of content, wherein the second author fragment of content may be associated with the content author and wherein the second block of key information may comprise information of a second state author vector and a second digital signature; the input unit may be further configured to obtain a second user fragment of content, wherein the second user fragment of content may correspond to the second author fragment of content; the authentication unit may be further configured to verify the content checking the correctness of the second digital signature; and wherein the authentication unit may be further configured to send instructions to add the second block of key information to the first block of key information connecting the first block of key information and the second block of key information sequentially.

[0246] In an example, the user state recognition unit may be further configured to generate a second state user vector from the second user fragment of content; and the first control unit may further be configured to verify the content by comparing information of the second state user vector with information of the second block of key information.

[0247] A further aspect of the disclosure refers to a computer program comprising computer-readable instructions that when executed by a computer cause the computer to carry out the method of the first and the second aspect or one of the implementations of the first and the second aspect.

[0248] All references, including publications, patent applications, and patents, cited herein are hereby incorporated by reference to the same extent as if each reference were individually and specifically indicated to be incorporated by reference and were set forth in its entirety herein.

[0249] The use of the terms "a" and "an" and "the" and "at least one" and similar referents in the context of describing the invention (especially in the context of the following claims) are to be construed to cover both the singular and the plural, unless otherwise indicated herein or clearly contradicted by context. The use of the term "at least one" followed by a list of one or more items (for example, "at least one of A and B") is to be construed to mean one item selected from the listed items (A or B) or any combination of two or more of the listed items (A and B), unless otherwise indicated herein or clearly contradicted by context. The terms "comprising," "having," "including," and "containing" are to be construed as open-ended terms (i.e., meaning "including, but not limited to,") unless otherwise noted. Recitation of ranges of values herein are merely intended to serve as a shorthand method of referring individually to each separate value falling within the range, unless otherwise indicated herein, and each separate value is incorporated into the specification as if it were individually recited herein. All methods described herein can be performed in any suitable order unless otherwise indicated herein or otherwise clearly contradicted by context. The use of any and all examples, or exemplary language (e.g., "such as") provided herein, is intended merely to better illuminate the invention and does not pose a limitation on the scope of the invention unless otherwise claimed. No language in the specification should be construed as indicating any non-claimed element as essential to the practice of the invention.

[0250] Preferred embodiments of this invention are described herein, including the best mode known to the inventors for carrying out the invention. Variations of those preferred embodiments may become apparent to those of ordinary skill in the art upon reading the foregoing description. The inventors expect skilled artisans to employ such variations as appropriate, and the inventors intend for the invention to be practiced otherwise than as specifically described herein. Accordingly, this invention includes all modifications and equivalents of the subject matter recited in the claims appended hereto as permitted by applicable law. Moreover, any combination of the above-described elements in all possible variations thereof is encompassed by the invention unless otherwise indicated herein or otherwise clearly contradicted by context.

What is claimed is:

1. A computer-implemented method for providing content of a content author for authentication, the method comprising:

obtaining a first author fragment of content by the content author;

generating a first state author vector from the first author fragment of content; and

creating a first block of key information based on the first author fragment of content;

wherein the first block of key information comprises information of the first state author vector and a first digital signature.

2. The method of claim **1**, further comprising:

obtaining a second author fragment of content from the content author;

generating a second state author vector from the second author fragment of content; and

creating a second block of key information based on the second author fragment of content;

wherein the second block of key information comprises information of the second state author vector and a second digital signature.

3. The method of claim **2**, wherein the second author fragment of content is a subsequent fragment of the first

author fragment of content, and wherein the first author fragment of content and the second author fragment of content are connected sequentially.

4. The method of claim **1**, further comprising replacing the first state author vector by a first database state author vector, wherein the first database state author vector is a vector of a state vectors database, and wherein a metric between the first state author vector and the first database state author vector lies below a pre-defined threshold value.

5. The method of claim **4**, wherein replacing the first state author vector by the first database state author vector precedes creating the first block of key information based on the first author fragment of content.

6. The method of claim **1**, further comprising passing a pre-defined time of content that is transmitted continuously prior to obtaining the first author fragment of content.

7. The method of claim **1**, further comprising:

providing, by the content author, biometrics vector data of the content author;

sending the biometrics vector data for verification and confirmation of the identity of the content author to the key center; and

sending instructions for storing verified biometrics vector data of the content author in a biometrics vector database.

8. A device for providing content of a content author for authentication, wherein the device comprises:

a content fragment unit configured to obtain a first author fragment of content;

an author state recognition unit configured to generate a first state author vector from the first author fragment of content; and

a first output unit configured to create a first block of key information based on the first author fragment of content, wherein the first block of key information comprises information of the first state author vector and a first digital signature.

9. A computer-implemented method for authenticating a provided content of a content author, the method comprising:

receiving content of the content author by the content user;

requesting from a key center information of a first block of key information based on a first author fragment of content, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature;

obtaining a first user fragment of content, wherein the first user fragment of content corresponds to the first author fragment of content; and

authenticating the content by checking the correctness of the first digital signature.

10. The method of claim **9**, further comprising:

requesting from the key center information of a second block of key information based on a second author fragment of content, wherein the second author fragment of content is associated with the content author and wherein the second block of key information comprises information of a second state author vector and a second digital signature;

obtaining a second user fragment of content, wherein the second user fragment of content corresponds to the second author fragment of content;

authenticating the content by checking the correctness of the second digital signature; and

sending instructions to add the second block of key information to the first block of key information connecting the first block of key information and the second block of key information sequentially.

11. The method of claim **9**, further comprising obtaining by the content user a first biometrics vector from the first user fragment of content; and comparing the first biometrics vector with biometrics vector data of the content author stored in a biometrics vectors database.

12. The method of claim **9**, further comprising verifying the biometrics vector and the first state user vector, wherein the verifying of the first state user vector and the biometrics vector is independent of each other.

13. The method of claim **9**, wherein the received content is fragmentized in a plurality of fragments prior to obtaining the first author fragment of content, wherein the first author fragment of content is one of the plurality of fragments.

14. The method of claim **9**, further comprising generating a first state user vector from the first user fragment of content; and verifying the content by comparing information of the first state user vector with information of the first block of key information.

15. The method of claim **10**, further comprising generating a second state user vector from a second user fragment of content; and verifying the content by comparing information of the second state user vector with information of a second block of key information.

16. A device for authenticating a provided content of a content author, wherein the device comprises:

a content receiving unit configured to receive content of the content author;

a user communication unit configured to request from a key center information of a first block of key information based on a first author fragment of content, wherein the first author fragment of content is associated with the content author and wherein the first block of key information comprises information of a first state author vector and a first digital signature;

an input unit configured to obtain a first user fragment of content, wherein the first user fragment of content corresponds to the first author fragment of content; and

an authentication unit configured to authenticate the content by checking the correctness of the first digital signature.

17. A computer program comprising computer-readable instructions that when the program is executed by a computer, cause the computer to carry out a method for providing content of a content author for authentication, the method comprising:

obtaining a first author fragment of content by the content author;

generating a first state author vector from the first author fragment of content; and

creating a first block of key information based on the first author fragment of content;

wherein the first block of key information comprises information of the first state author vector and a first digital signature.

* * * * *