

BLOCKCHAIN MIDDLEWARE

TECHNICAL FIELD

[0001] The present disclosure relates generally to blockchains and more specifically to cybersecurity of blockchains.

5 BACKGROUND

[0002] As blockchain technology becomes increasingly prevalent in wide variety of applications involving financial transactions, personal data, and other confidential information, cybersecurity of blockchains also grows in importance. The volume of blockchain transactions is expected to grow exponentially even as digital transactions dominate every sphere of human
10 activity in this information technology-intense era.

[0003] As a result, there will be an exponentially increasing number of instances where users' confidential information will be stored in public blockchains or in third party-controlled data storage. Although blockchains are designed to be inherently immutable, there is also a growing awareness of cybersecurity risks associated with blockchains.

15 [0004] It is particularly challenging to balance strong cybersecurity measures with the flexibility and speed required in practical implementation of blockchain technology across a wide range of diverse applications.

SUMMARY

[0005] In one aspect, the present disclosure provides a blockchain middleware operable by one
20 or more processors according to instructions stored in at least one tangible, non-transitory, computer-readable storage medium coupled with the one or more processors, the middleware being configured to perform a method comprising: establishing connections with at least a first software component and a second software component over a network; in response to an initiation of a transaction between the first software component and the second software
25 component, the transaction involving a file originating from the first software component, generating a root hash based on a plurality of identifiers, each of the plurality of identifiers being tagged to a partial copy of the file; and generating a block based on the root hash and a hash of a prior block in a blockchain, wherein the prior block is part of a ledger accessible by the second software component.

[0006] The blockchain middleware according to any described above, the method further comprising: obtaining a first plurality of segments, wherein each of the first plurality of segments corresponds to a part of the file, and wherein the first plurality of segments collectively corresponds to one complete copy of the file.

- 5 [0007] The blockchain middleware according to any described above, wherein the method comprises: encrypting the file to obtain an encrypted file; and splitting the encrypted file into multiple parts to obtain the first plurality of segments.

- [0008] The blockchain middleware according to any described above, the method further comprising: at least a step of making a predetermined number of replicates of each of the first
10 plurality of segments to obtain a second plurality of segments, wherein each of the plurality of identifiers is tagged to one of the second plurality of segments.

- [0009] The blockchain middleware according to any described above, the method further comprising: forming a first generation of hashes based on hashing the plurality of identifiers; and iteratively forming subsequent generations of hashes, wherein each subsequent generation
15 of one or more hashes is based on hashing one or more groups of hashes of a preceding generation, wherein a last subsequent generation generates the root hash.

[0010] The blockchain middleware according to any described above, wherein each subsequent generation generates fewer hashes than the preceding generation.

- [0011] The blockchain middleware according to any described above, the method further
20 comprising: generating more than one root hash for the file, wherein each of the more than one root hash is based on a group of identifiers randomly selected from the plurality of identifiers.

[0012] The blockchain middleware according to any described above, the method further comprising: appending the more than one root hash to more than one blockchain.

- [0013] In another aspect, the present disclosure provides a method executable by the
25 blockchain middleware according to any described above, in which the method includes: in response to instructions to store the file, applying an encryption algorithm to the file to obtain an encrypted file; splitting the encrypted file into a first plurality of fragments; making a predetermined number of replicates of each of the first plurality of fragments to obtain a second set of fragments, the second set of fragments having a second plurality of fragments;

configuring the second set of fragments as a randomly ordered sequence; and distributing the second set of fragments among multiple storage nodes for blockchain storage such that respective parts of the randomly ordered sequence are stored in different storage nodes.

5 [0014] The method according to any above, further comprising: forming a first generation of hashes based hashing the plurality of identifiers, wherein each of the first and/or second plurality of fragments is tagged by one of the plurality of identifiers; and iteratively forming subsequent generations of hashes, wherein each subsequent generation of one or more hashes is based on hashing one or more groups of hashes of a preceding generation, wherein a last subsequent generation generates the root hash. The method according to any described above,
10 wherein each subsequent generation generates fewer hashes than the preceding generation.

[0015] The method according to any described above, further comprising: generating more than one root hash for the file, wherein each of the more than one root hash is based on a group of identifiers randomly selected from the plurality of identifiers.

15 [0016] The method according to any described above, further comprising: appending the more than one root hash to more than one blockchain.

[0017] The method according to any described above, further comprising: enabling user selection of at least one node cluster for the blockchain storage.

[0018] The method according to any described above, further comprising: enabling user configuration of the predetermined number of replicates.

20 [0019] The method according to any described above, further comprising: enabling user configuration of respective locations of at least some of the multiple storage nodes, wherein the at least some of the multiple storage nodes are provided on at least one private server.

[0020] The method according to any described above, wherein the at least one node cluster further comprises at least one third party-operated storage provided as a cloud-based storage-
25 as-a-service.

[0021] The method according to any described above, wherein the distributing comprises distributing different parts of the randomly ordered sequence to the at least one private server and the at least one third party-operated storage respectively for the blockchain storage, wherein each of the at least one private server corresponds to at least one of the node clusters,

and wherein each of the at least one third party-operated storage corresponds to one of the node clusters.

[0022] The method according to any described above, wherein the at least one private server comprises at least one local server and at least one remote server, such that the at least one local server and the at least one remote server are each configured for the blockchain storage.

[0023] In another aspect, there is provided a computer-implemented system, comprising: one or more processors; and one or more computer-readable memory coupled with the one or more processors, the one or more computer-readable memory storing instructions executable by the one or more processors to perform the method of the middleware according to any described above.

BRIEF DESCRIPTION OF DRAWINGS

[0024] Fig. 1A and Fig. 1B illustrate a cybersecurity framework according to an embodiment of the present disclosure;

[0025] Fig. 2A and Fig. 2B are schematic block diagrams of a blockchain middleware according to embodiments of the present disclosure;

[0026] Fig. 3 illustrates a part of a method according one embodiment of the present disclosure;

[0027] Fig. 4 illustrates another part of the method according to an embodiment of the present disclosure; and

[0028] Fig. 5 is a schematic representation of an embodiment according to the method of Fig. 3 and Fig. 4.

[0029] Fig. 6 illustrates a method according to yet another embodiment of the present disclosure.

DETAILED DESCRIPTION

[0030] Reference throughout this specification to “one embodiment”, “another embodiment” or “an embodiment” (or the like) means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment. Thus, the appearance of the phrases “in one embodiment” or “in an embodiment” or the like in various

places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the described features, structures, or characteristics may be combined in any suitable manner in one or more embodiments. In the following description, numerous specific details are provided to give a thorough understanding of embodiments. One skilled in the relevant art will recognize, that the various embodiments be practiced without one or more of the specific details, or with other methods, components, materials, etc. In other instances, some or all known structures, materials, or operations may not be shown or described in detail to avoid obfuscation.

[0031] The word “exemplary” is used herein to mean “serving as an example, instance, or illustration.” Any embodiment described herein as “exemplary” is not necessarily to be construed as preferred or advantageous over other embodiments. As used herein, the singular ‘a’ and ‘an’ may be construed as including the plural “one or more” unless apparent from the context to be otherwise.

[0032] Terms such as “first” and “second” are used in the description and claims only for the sake of brevity and clarity, and do not necessarily imply a priority or order, unless required by the context. The terms "about" and "approximately" as applied to a stated numeric value encompasses the exact value and a reasonable variance as will be understood by one of ordinary skill in the art, and the terms “generally” and “substantially” are to be understood in a similar manner, unless otherwise specified.

[0033] Fig. 1A shows a cybersecurity framework (100) configured with enhanced security for data storage (200) in a network according to some embodiments of the present disclosure. The enhanced security for data storage (200) is implemented by a blockchain middleware (230) according to an embodiment of the present disclosure. The blockchain middleware (230) may be realised in the form of software. In some examples, the blockchain middleware (230) is configured for deployment between user devices (120) and at least one network (140). As illustrated schematically in Fig. 1B, the blockchain middleware (230) may be configured for deployment between a client application server (210) and one or more storage nodes (240). The blockchain middleware (230) is configured to act as a bridge between a client application server (210) and the storage nodes (240). The blockchain middleware (230) may reside at a second server operable independently of the client application server (210) and the server(s) managing the plurality of storage nodes (240).

[0034] The network (140) may be referred to as the infrastructure and may be in the form of one or more servers configured with storage nodes. The storage nodes where the users (110) store their data may be wholly or partially on-premises, off-premises or cloud-based. The storage nodes may include cloud storage provided by third-party service providers, including cloud storage provided as a storage-as-a-service. In such situations, the third party, such as a cloud storage service provider, has ownership over the server level cybersecurity (142). At the infrastructural or server level, network security software is therefore directed at handling server level issues, for example, firewalls, specific software to deflect distributed denial-of-service (DDoS) attacks, etc. In an example where the user subscribes to a cloud storage provided by a third party, it can be understood that the user is not able to control protection measures at the infrastructural level. From the perspective of the users (110), users typically have ownership only at the personal level cybersecurity (112) and the device level cybersecurity (122). The personal level (112) of cybersecurity refers the use of passwords and two-factor authentication, etc. It may also refer to physical security measures that limit personnel access to a defined physical location, for example, by using an identification card to validate a user's identity. The device level (122) of cybersecurity refers to measures such as biometric authentication and/or hardware access keys and physical locks, etc.

[0035] According to embodiments of the present disclosure, the blockchain middleware (230) is configured to implement several levels of data protection. According to embodiments of the present disclosure, the blockchain middleware (230) is configured to implement several levels of data protection. This is schematically illustrated in Fig. 2A. The blockchain middleware (230) is configured to integrate data protection at a data level (242), at a network level (244), and at an infrastructural level (246). This is a departure from the way conventional cybersecurity is configured for the data storage space. Under the conventional approach, each level of cybersecurity is owned by and/or controlled by a corresponding party. In contrast, the blockchain middleware (230) of the present disclosure expands the reach and control of a user beyond the conventional data level (242). Through the blockchain middleware (230) of the present disclosure, a data owner can extend control over the cybersecurity at the network level (244) and/or at the workflow engine (246). What this means in practical implementation is that the user or the data owner can enforce an added layer of cybersecurity independently of third-party vendors and independently of the cybersecurity measures implemented by the third party.

[0036] By reimagining the way traditional cybersecurity is configured for the data storage

space, the blockchain-based middleware of the present disclosure is conceived and deployable in a network to enhance security. An algorithmic workflow is implementable by the blockchain middleware to encrypt any file, splitting the encrypted file; making a predetermined number of replicates to obtain fragments; and distributing the fragments among multiple storage nodes.

- 5 The identity of the fragments is hashed and stored in a blockchain, making them immutable. By harnessing the power of blockchain, the blockchain middleware acts as an additional security protocol on top of the existing cybersecurity protocols by means of immutability, traceability, and improved security.

- [0037] In one aspect, the blockchain middleware (230) of the present disclosure
10 advantageously provides user-controllable aspects (130) at an infrastructural level or the server level. That is, according to embodiments of the present disclosure, the blockchain middleware provides a degree of data security independent of that provided at the personal level of cybersecurity. In other words, in an extreme case where the personal level of cybersecurity measures is very weak (e.g., use of weak passwords), the blockchain middleware of the present
15 disclosure provides a layer of cybersecurity regardless of the level of cybersecurity at the infrastructural or server level (142), and that is simultaneously over and above the personal level of cybersecurity measures.

- [0038] Referring to Fig. 2B, the blockchain middleware (230) may be described as being configured to provide at least the following aspects: storage management (232), active
20 monitoring (234), and a response workflow (238). The response workflow (238) may be user-configurable to suit the different needs of different types of users. In some examples, the response workflow (238) includes an option for automated recovery (236). In some examples, the response workflow (238) may be configured with an alert process (239) in which one or more alarms or notifications are triggered and sent to one or more designated parties.

- 25 [0039] In actual implementation, the blockchain middleware (230) operates in an integral manner, such that there may not be a clear distinction between the hardware components and/or processes (300) involved in each of these different aspects of the blockchain middleware (230). In some instances, the blockchain middleware (230) may be provided by a computer-readable memory storing instructions, such that a processor (coupled to the computer-readable memory)
30 is configured to execute the instructions. In another aspect, there is provided a computer-implemented system, comprising: one or more processors; and one or more computer-readable memory coupled with the one or more processors, the one or more computer-readable memory

storing instructions executable by the one or more processors to execute the middleware according to any described above.

[0040] The blockchain middleware (230) may be configured to carry out a method (300, 300') involving security enhancement to strengthen protection of a file stored in a network. The blockchain middleware (230) may be configured to carry out security enhancement as a routine and/or in response to one or more specific situations. In some embodiments, the blockchain middleware (230) optionally includes an active monitoring module (234). In one example, the blockchain middleware (230) is configured to carry out security enhancement in response as part of an optional response workflow (238) to detecting an unauthorised attempt to access or to tamper with data which has been stored according to embodiments of the present disclosure. In another example, the blockchain middleware (230) is configured to carry out security enhancement in response to detecting an anomaly in the course of active monitoring (234). In yet another example, the blockchain middleware (230) is configured to carry out security enhancement in response to being alerted to an attack on a server corresponding to a storage node, and it is determined that the security of data stored at related storage nodes may be at risk. In yet another optional response workflow, the blockchain middleware (230) may be configured to perform automated recovery (236) as part of security enhancement. The following also describes the embodiments of the present disclosure with reference to an example in which a file (an affected copy of the file or an affected file) is the target of a suspected unauthorised attempt to tamper with stored data. It will be understood that embodiments of the present disclosure are not limited to such.

[0041] Referring to Fig. 3 and Fig. 5, according to one embodiment of the present disclosure, the blockchain middleware (230) is configured to perform a method (400). A part of the method (300) includes establishing connections with at least a first software component and a second software component over a network (310). The blockchain middleware may be configured to include obtaining a first plurality of segments (320). Each of the first plurality of segments corresponds to a part of the file. Each of the first plurality of segments collectively corresponds to one complete copy of the file. The blockchain middleware may be configured to perform the method in which the method includes encrypting the file to obtain an encrypted file (320); and splitting the encrypted file into multiple parts to obtain the first plurality of segments.

[0042] The blockchain middleware may be configured to further perform the method including at least a step of making a predetermined number of replicates of each of the first plurality of

segments to obtain a second plurality of segments (330), wherein each of the plurality of identifiers is tagged to one of the second plurality of segments (340).

[0043] In some examples, the segments are replicated based on Reed-Solomon erasure coding. The blockchain middleware (230) enables the user to select or to define a redundancy factor (user configuration of the predetermined number of replicates per segment). As a non-limiting example, the user may choose to apply a redundancy factor of 10 using the blockchain middleware. Assuming that a first plurality of 20 segments has been obtained from the ciphertext, the blockchain middleware will generate 10 replicates of each segment of ciphertext and, in total, generate 200 segments based on the original file. If an encrypted file is split into ten segments, and from each segment nine replicas are created, there would be a total number of a hundred segments stored. For the sake of brevity, the collection of replicated segments is referred to as a second plurality of segments. In various embodiments of the present disclosure, the blockchain middleware may be configured to perform the replication iteratively or progressively. The blockchain middleware may be configured such that the user may determine the number of replicas of each segment, or default settings may be applied.

[0044] In one aspect of the method (300') as illustrated in Fig. 4 and Fig. 5, the present disclosure provides a blockchain middleware (230) operable by one or more processors according to instructions stored in at least one tangible, non-transitory, computer-readable storage medium coupled with the one or more processors. The blockchain middleware (230) is configured to perform a method (400) in which the method includes establishing connections with at least a first software component and a second software component over a network (310). The blockchain middleware is configured to generate a root hash (350) in response to an initiation of a transaction between the first software component and the second software component. The transaction may involve a file originating from the first software component. The root hash may be generated (350) based on a plurality of identifiers, in which each of the plurality of identifiers is tagged to a partial copy of the file (340). The blockchain middleware is configured to generate a block (360) based on the root hash and a hash of a prior block in a blockchain, wherein the prior block is part of a ledger accessible by the second software component.

[0045] According to some embodiments, the blockchain middleware (230) is configured to perform a method (400) as schematically represented in Fig. 5. The method (400) includes encrypting a file (410) and splitting (403) the encrypted file (410) to obtain parts (420) of the

encrypted file. In other words, the method includes splitting the encrypted file into multiple parts to obtain a first plurality of segments (420). Each of the first plurality of segments corresponds to a part of the file. The first plurality of segments collectively corresponds to one complete copy of the file. The method (400) further includes replicating (404) each part (420) of the encrypted file to obtain multiple copies of the parts (420) of the encrypted file. In other words, the method (400) includes at least a step of making a predetermined number of replicates (404) of each of the first plurality of segments to obtain a second plurality of segments (405). The method (400) includes tagging (406) each of the second plurality of segments with an identifier (430). A plurality of identifiers is thus obtained, in which each of the plurality of identifiers corresponds with a segment of the file. The identifiers (430) may be defined with respect to the encrypted file. In some examples, the identifiers are defined to be unique with respect to each immediate output of the splitting (403) step. In some examples, the identifiers are defined to uniquely identify a segment of the encrypted file.

[0046] The blockchain middleware is further configured to perform the method (400) including forming a first generation of hashes (440) based on hashing the plurality of identifiers (430). The method may include iteratively forming subsequent generations of hashes (350), wherein each subsequent generation of one or more hashes is based on hashing one or more groups of hashes of a preceding generation. In some examples, in each subsequent generation of hashing, one or more selected hashes are selected from a plurality of hashes generated in the preceding generation, and the selected hashes are hashed to form a new hash. The selection and hashing are repeated until all hashes of the preceding generation has been selected and used in hashing. In some examples, a plurality of subsequent generation hashes are formed such that each of the plurality of subsequent generation hashes is a hash of a group of hashes of the preceding generation. In some examples, each of the hashes formed at the subsequent generation is a hash of a random selection of hashes from the immediately preceding generation of hashes. The method (400) may be such that the number of hashes in each generation progressively decreases with each iteration or with each subsequent generation of hashing. The blockchain middleware may further be configured such that each subsequent generation generates fewer hashes than the preceding generation. The method (400) includes iteratively forming subsequent generations (408) of hashes until there is only one hash (h0) formed in a generation (the last subsequent generation). Alternatively described, the generations of hashes end in a last subsequent generation in which a root hash (h0) is generated. The blockchain middleware may alternatively be configured to perform a method further including generating more than one

root hash (h0) based on the file (410). In some examples, each of the more than one root hash is based on a group of identifiers (430) randomly selected from the plurality of identifiers. The blockchain middleware may further be configured to perform a method including appending the more than one root hash to more than one blockchain (409). The blockchain middleware
5 may be configured such that all hashes based on the same file are eventually “incorporated” into one root hash (h0), and the root hash is presented for hashing with a prior block (h1) to form a new block (h0h1) on a blockchain. Alternatively, the blockchain middleware (230) may be configured such that hashes based on the same file (410) are eventually “incorporated” into more than one root hashes (h0), and each of the root hashes are severally used to generate
10 multiple blocks for multiple blockchains respectively (409).

[0047] As a non-limiting example, a first generation of 100 hashes may be generated based on the identifiers corresponding to respective segments of ciphertext. The blockchain middleware may be configured to generate a second generation of 20 hashes, in which each second generation hash is a hash of five hashes selected from the first generation. The blockchain
15 middleware may be configured to enable the selection of hashes from a preceding generation to be configurable, for example, in terms of the number of generations, in terms of whether the selection is random, etc.

[0048] In some embodiments, the blockchain middleware (230) is configured to perform a method (300) which includes a method of storage management. In response to instructions to
20 store a file, the method includes applying an encryption algorithm to a file to obtain an encrypted file. The file (or data) to be stored is first encrypted (320) by the blockchain middleware (230). The blockchain middleware (230) is configurable to accommodate use of different encryption methods. Examples of encryption methods compatible with the blockchain middleware (230) include (but are not limited to) 256-bit hashing (256 hashing), Threefish
25 cipher, and/or other encryption methods compliant with the 256-bit Advanced Encryption Standard (AES 256), etc.

[0049] Optionally, the blockchain middleware (230) is configured to enable the segments (of encrypted file) to be stored in a decentralised manner (330). Decentralised storage or distributed storage (330) refers to storing the segments of encrypted file in a plurality of storage
30 nodes such that not all of the segments are stored in the same storage node. In some examples, the storage nodes are related or connected (logically or physically) as clustered storage nodes, and the blockchain middleware (230) is configured to store the data in one or more storage

node clusters. The blockchain middleware (230) may be configured to store the segments on wholly or partially on-premises or cloud-based. The storage nodes may include cloud storage provided by third-party service providers, including cloud storage provided as a storage-as-a-service.

- 5 [0050] In some examples, the storage nodes are related or connected (logically or physically) as clustered storage nodes (one or more node clusters). The blockchain middleware (230) may be configured to enable user selection of at least one node cluster for storing the file and its corresponding segments. The blockchain middleware may be configured to enable user configuration of respective locations of at least some of the multiple storage nodes, for example,
- 10 when the storage nodes are provided on one or more private server. The blockchain middleware may be configured for use with at least one third party-operated storage, for example, such as one in the form of a cloud-based storage-as-a service. The blockchain middleware may be configured to distribute part of the randomly ordered sequence to at least one private server or at least one third-party operated storage respectively for blockchain storage. The blockchain
- 15 middleware may be set up such that the private server corresponds to at least one of the node clusters. The blockchain middleware may be set up such that the third party-operated storage corresponds to one of the node clusters. The blockchain middleware may be configured to enable different parts of the segments to be stored in at least one local server and at least one remote server.
- 20 [0051] Optionally, as schematically illustrated by Fig. 6, the blockchain middleware (230) is configured to carry out a method (500) with real-time monitoring or active monitoring (510). In this document, an activity that is performed “actively” or in “real-time” refers to an activity that is performed concurrently or substantially at the same time as the normal operations of the client application server / user device. Activities performed in “real-time” can therefore include
- 25 activities that are performed iteratively, repeatedly, and/or periodically, while the client application server / user device is operational. Activities performed in “real-time” can also include activities that occur immediately following another specific event. For example, an activity may be described as “real-time” if it is performed immediately following an attempt to access a secure stored file (a data file that is stored according to any of the embodiments
- 30 described herein). Active monitoring at or near real-time may include checking for changes at a time at least partially concurrent with an attempt to access the data file, or at a time immediately sequential to an attempt to access the file.

[0052] Optionally, in some embodiments, if a change is traced to an unauthorised activity in relation to an affected file (or a possibly affected file), the blockchain middleware (230) is configured to immediately commence one or more of several possible response workflows. One possible response workflow is to provide an option for automated recovery (520) of the data or the file. The response workflow may include retrieving the original file from the plurality of storage nodes and performing automated recovery of the affected file. Another possible response workflow may include sending an alarm or a notification to selected stakeholders. This broadens the range of responses available to protect the stored data. Examples of stakeholders who may be identified for this purpose includes, but are not limited to, the data owner, the authorised user of the data, the system administrator, law enforcement, the third party operating or offering data storage-related services and/or premises, etc.

[0053] In a conventional distributed ledger system, protocols are designed to be immutable so that transactions stored in blocks are permanent, and the blocks cannot be deleted or edited. Any change would require consensus by all parties involved in the consensus protocol. In contrast, the blockchain middleware (230) of the present disclosure can be used to bridge between the client application server (210) and a blockchain platform, while at the same time providing enhanced security measures independently of the manner in which the blockchain platform has been configured. This enables the user to use the same blockchain middleware (230) with different blockchain platforms to meet different needs across the company, for example. The blockchain middleware (230) also provides the user with an enhanced measure of cybersecurity control over data stored in networks, such as (but not limited to) cloud storage offered by third-party service providers.

[0054] As non-limiting examples, embodiments of the present disclosure may be useful in situations where a first user needs to share confidential information with a second user, or where the first user needs to submit confidential information to a public agency. In addition to verifying the identities of the first user and the second user through digital certificates and two-factor authentication which provide a personal or device level of cybersecurity, the present blockchain middleware provides the user with an additional level of cybersecurity control.

[0055] All examples described herein, whether of apparatus, methods, materials, or products, are presented for the purpose of illustration and to aid understanding, and are not intended to be limiting or exhaustive. Various changes and modifications may be made by one of ordinary skill in the art without departing from the scope of the invention as claimed.

CLAIMS

1. A blockchain middleware operable by one or more processors according to instructions stored in at least one tangible, non-transitory, computer-readable storage medium
5 coupled with the one or more processors, the middleware being configured to perform a method comprising:

establishing connections with at least a first software component and a second software component over a network;

10 in response to an initiation of a transaction between the first software component and the second software component, the transaction involving a file originating from the first software component, generating a root hash based on a plurality of identifiers, each of the plurality of identifiers being tagged to a partial copy of the file; and

generating a block based on the root hash and a hash of a prior block in a blockchain, wherein the prior block is part of a ledger accessible by the second software component.

15

2. The blockchain middleware according to claim 1, the method further comprising:
obtaining a first plurality of segments, wherein each of the first plurality of segments corresponds to a part of the file, and wherein the first plurality of segments collectively corresponds to one complete copy of the file.

20

3. The blockchain middleware according to claim 2, wherein the method comprises:
encrypting the file to obtain an encrypted file; and
splitting the encrypted file into multiple parts to obtain the first plurality of segments.

25

4. The blockchain middleware according to claim 3, the method further comprising:
at least a step of making a predetermined number of replicates of each of the first plurality of segments to obtain a second plurality of segments, wherein each of the plurality of identifiers is tagged to one of the second plurality of segments.

30

5. The blockchain middleware according to claim 4, the method further comprising:
forming a first generation of hashes based on hashing the plurality of identifiers;
and

iteratively forming subsequent generations of hashes, wherein each subsequent generation of one or more hashes is based on hashing one or more groups of hashes of a preceding generation, and wherein a last subsequent generation generates the root hash.

5 6. The blockchain middleware according to claim 5, wherein each subsequent generation generates fewer hashes than the preceding generation.

 7. The blockchain middleware according to claim 6, the method further comprising:
 generating more than one root hash for the file, wherein each of the more than one
10 root hash is based on a group of identifiers randomly selected from the plurality of identifiers.

 8. The blockchain middleware according to claim 7, the method further comprising:
 appending the more than one root hash to more than one blockchain.

15 9. A method executable by the blockchain middleware according to any one of claims
1 to 8, the method comprising:

 in response to instructions to store the file, applying an encryption algorithm to the
file to obtain an encrypted file;

 splitting the encrypted file into a first plurality of fragments;

20 making a predetermined number of replicates of each of the first plurality of
fragments to obtain a second set of fragments, the second set of fragments having a second
plurality of fragments;

 configuring the second set of fragments as a randomly ordered sequence; and

 distributing the second set of fragments among multiple storage nodes for
25 blockchain storage such that respective parts of the randomly ordered sequence are stored in
different storage nodes.

 10. The method according to claim 9, further comprising:

 forming a first generation of hashes based hashing the plurality of identifiers,
30 wherein each of the first and/or second plurality of fragments is tagged by one of the plurality
of identifiers; and

 iteratively forming subsequent generations of hashes, wherein each subsequent
generation of one or more hashes is based on hashing one or more groups of hashes of a
preceding generation, wherein a last subsequent generation generates the root hash.

11. The method according to claim 10, wherein each subsequent generation generates fewer hashes than the preceding generation.

5 12. The method according to claim 11, the method further comprising:
generating more than one root hash for the file, wherein each of the more than one root hash is based on a group of identifiers randomly selected from the plurality of identifiers.

10 13. The method according to claim 12, the method further comprising: appending the
more than one root hash to more than one blockchain.

14. The method of claim 13, further comprising:
enabling user selection of at least one node cluster for the blockchain storage.

15 15. The method of claim 14, further comprising: enabling user configuration of the
predetermined number of replicates.

20 16. The method of claim 15, further comprising: enabling user configuration of
respective locations of at least some of the multiple storage nodes, wherein the at least some of
the multiple storage nodes are provided on at least one private server.

17. The method of claim 16, wherein the at least one node cluster further comprises at
least one third party-operated storage provided as a cloud-based storage-as-a-service.

25 18. The method of claim 17, wherein the distributing comprises distributing different
parts of the randomly ordered sequence to the at least one private server and the at least one
third party-operated storage respectively for the blockchain storage, wherein each of the at least
one private server corresponds to at least one of the node clusters, and wherein each of the at
least one third party-operated storage corresponds to one of the node clusters.

30 19. The method of claim 18, wherein the at least one private server comprises at least
one local server and at least one remote server, such that the at least one local server and the at
least one remote server are each configured for the blockchain storage.

20. A computer-implemented system, comprising:
- one or more processors; and
 - one or more computer-readable memory coupled with the one or more processors,
- the one or more computer-readable memory storing instructions that, when executed by the
- 5 one or more processors, perform the method according to any one of the preceding claims.