

CLAIMS

What is claimed is:

1. A method for blockchain-based recordkeeping, implementable by a terminal device, the method comprising:

obtaining target data;

computing a data digest of the target data, and extracting a key segment from the target data;

signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature; and

submitting to a blockchain the data digest, the key segment, and the signature, for one or more nodes in the blockchain to verify the signature based on a public key corresponding to the private key, and to record the data digest and the key segment in the blockchain in response to the signature being verified to be valid.

2. The method according to claim 1, wherein the private key associated with the terminal device is stored in the secure operation environment.

3. The method according to claim 1 or 2, wherein the secure operation environment in the terminal device stores device authentication information and the device authentication information is signed based on the private key associated with the terminal device to generate another signature; and

signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature comprises:

verifying the another signature of the device authentication information based on the public key corresponding to the private key associated with the terminal device; and

in response to the another signature being verified to be valid, determining that the terminal device is a valid terminal device and signing, in the secure operation environment included in the terminal device, the data digest and/or the key segment based on the private key to generate the signature.

4. The method according to any one of the preceding claims, wherein signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature comprises:

signing, in the secure operation environment included in the terminal device, the data digest and the key segment as a whole based on the private key associated with the terminal device to generate the signature.

5. The method according to any one of the claims 1-3, wherein signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature comprises:

signing, in the secure operation environment included in the terminal device, the data digest based on the private key associated with the terminal device to generate the signature.

6. The method according to any one of the preceding claims, wherein the target data comprises video data; and

extracting a key segment from the target data comprises:

detecting an abnormal event in the video data; and

in response to an abnormal event being detected, extracting a video segment corresponding to an occurrence period of the abnormal event as the key segment.

7. The method according to any one of the claims 1-5, wherein the target data comprises audio data; and

extracting a key segment from the target data comprises:

detecting a preset keyword in the audio data; and

in response to the preset keyword being detected, extracting an audio segment of a preset length comprising the preset keyword as the key segment.

8. The method according to any one of the preceding claims, wherein signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature comprises:

obtaining identity information of a user using the terminal device;

authenticating the identity of the user based on the obtained identity information; and

signing, in the secure operation environment included in the terminal device, the data digest and/or the key segment based on the private key associated with the terminal device to generate the signature in response to the identity of the user being authenticated as valid.

9. The method according to any one of the preceding claims, wherein the method further comprises:

obtaining identity information of a user using the terminal device in response to the user using the terminal device for the first time;

authenticating the identity of the user based on the obtained identity information;
invoking a key generating algorithm to generate the private key and the public key in response to the identity of the user being authenticated as valid, wherein a key generating algorithm is stored in the secure operation environment included in the terminal device; and
associating the generated private key with the identity information of the user, and storing the generated private key associated with the identity information of the user in the secure operation environment.

10. The method according to claim 9, wherein signing, in a secure operation environment included in the terminal device, the data digest and/or the key segment based on a private key associated with the terminal device to generate a signature comprises:

obtaining identity information of a user using the terminal device;
determining whether a private key associated with the identity information is stored in the secure operation environment included in the terminal device; and
signing, in the secure operation environment included in the terminal device, the data digest and/or the key segment based on the private key associated with the identity information in response to the private key associated with the identity information being stored in the secure operation environment included in the terminal device.

11. The method according to any one of the preceding claims, wherein the terminal device comprises a body-worn camera or an event data recorder.

12. The method according to any one of the preceding claims, wherein the target data comprises video data, audio data, or image data, or a combination thereof.

13. A system for blockchain-based recordkeeping, comprising:
one or more processors; and
one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 12.

14. An apparatus for blockchain-based recordkeeping, comprising a plurality of modules for performing the method of any of claims 1 to 12.

15. A non-transitory computer-readable storage medium configured with instructions executable by one or more processors to cause the one or more processors to perform the method of any of claims 1 to 12.