

CLAIMS

What is claimed is:

1. A method for blockchain-based data verification, the method comprising:
 - obtaining target data submitted by a data submitter, wherein a first data digest of the target data is recorded in a blockchain;
 - computing a second data digest of the target data;
 - determining whether the second data digest matches the first data digest of the target data recorded in the blockchain; and
 - determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain.
2. The method according to claim 1, further comprising:
 - determining that the target data submitted by the data submitter is invalid in response to determining that the second data digest does not match the first data digest of the target data recorded in the blockchain.
3. The method according to claim 1 or 2, wherein the target data is acquired by a terminal device, the terminal device comprises a secure operation environment, and a private key of the terminal device is stored in the secure operation environment.
4. The method according to claim 3, further comprising:
 - obtaining the first data digest of the target data submitted by the terminal device to the blockchain,
 - wherein the first data digest is signed in the secure operation environment based on the private key of the terminal device to generate a signature; the signature of the first data digest is verified based on a public key corresponding to the private key; and the first data digest of the target data is recorded in the blockchain in response to the signature being verified to be valid.
5. The method according to claim 3 or 4, wherein the terminal device comprises a body worn camera or an event data recorder.
6. The method according to claim 5, wherein the target data comprises video data, audio data, or image data, or a combination thereof, which is acquired by the body worn camera or the event data recorder.
7. The method according to any one of the preceding claims, wherein determining whether the second data digest matches the first data digest of the target data recorded in the

blockchain comprises:

- verifying whether the second data digest has been recorded in the blockchain; and

- determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has been recorded in the blockchain.

8. The method according to claim 7, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises:

- determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to verifying that the second data digest has not been recorded in the blockchain.

9. The method according to any one of the preceding claims, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain comprises:

- obtaining the first data digest of the target data recorded in the blockchain;

- determining whether the first data digest of the target data is the same as the second data digest; and

- determining that the second data digest matches the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is the same as the second data digest.

10. The method according to claim 9, wherein determining whether the second data digest matches the first data digest of the target data recorded in the blockchain further comprises:

- determining that the second data digest does not match the first data digest of the target data recorded in the blockchain in response to determining that the first data digest of the target data is different from the second data digest.

11. The method according to any one of the preceding claims, wherein description data of the target data is recorded in the blockchain; and

- determining that the target data submitted by the data submitter is valid in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain comprises:

- in response to determining that the second data digest matches the first data digest of the target data recorded in the blockchain, determining whether description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain; and

determining that the target data submitted by the data submitter is valid in response to determining that the description data of the target data submitted by the data submitter matches the description data of the target data recorded in the blockchain.

12. The method according to claim 11, wherein the description data comprises: an acquisition time of the target data, an acquisition location of the target data, or an object related to the target data, or a combination thereof.

13. A system for blockchain-based data verification, 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 data verification, 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.