CLAIMS

1. A method for processing blockchain data, applied to a terminal device provided with a trusted execution environment, the method comprising:

acquiring, from a blockchain, data to be verified of a target service, the data to be verified comprising circulation data generated during execution of the target service and recorded in the blockchain;

determining, based on the target service, a relevant third-party authority for verifying authenticity of the data to be verified, and acquiring benchmark circulation data generated during the execution of the target service and recorded in the third-party authority;

transferring the data to be verified and the benchmark circulation data to the trusted execution environment of the terminal device through a first trusted application for performing data verification processing on the terminal device, wherein the trusted execution environment is provided with a verification rule for performing data verification on the data to be verified for the first trusted application; and

determining whether the data to be verified meets the verification rule by using the trusted execution environment and based on the circulation data in the data to be verified and the benchmark circulation data, and outputting a verification result of the data to be verified.

2. The method according to claim 1, wherein the data to be verified comprises at least one of resource transfer data corresponding to the target service or logistics data corresponding to the target service; and

the determining, based on the target service, the relevant third-party authority for verifying authenticity of the data to be verified, and acquiring the benchmark circulation data generated during the execution of the target service and recorded in the third-party authority comprises at least one of:

determining, based on the resource transfer data corresponding to the target service, a relevant third-party authority for verifying authenticity of the resource transfer data as a resource storage institution, acquiring benchmark resource transfer data generated during the execution of the target service and recorded in the resource storage institution, and using the benchmark resource transfer data as the benchmark circulation data; or

determining, based on the logistics data corresponding to the target service, a relevant third-party authority for verifying authenticity of the logistics data as a traffic regulatory institution, acquiring benchmark logistics data generated during the execution of the target service and recorded in the traffic regulatory institution, and using the benchmark logistics data as the benchmark circulation data.

3. The method according to claim 2, wherein the resource transfer data comprises at least one of a resource transfer value or a resource transfer time, and the logistics data comprises at least one of information about a logistics path or a time for passing through a predetermined node in the logistics path.

4. The method according to claim 1, wherein the data to be verified comprises a fundraising resource transfer value and a fundraising resource transfer time; and

the determining, based on the target service, the relevant third-party authority for verifying authenticity of the data to be verified, and acquiring the benchmark circulation data generated during the execution of the target service and recorded in the third-party authority comprises:

determining, based on the fundraising resource transfer value and the fundraising resource transfer time, a relevant third-party authority for verifying authenticity of the data as a resource storage institution; and

acquiring a benchmark fundraising resource transfer value and a benchmark fundraising resource transfer time generated during the execution of the target service and recorded in the resource storage institution, and using the benchmark fundraising resource transfer value and the benchmark fundraising resource transfer time as the benchmark circulation data.

5. The method according to claim 1, further comprising:

acquiring the verification result of the data to be verified from the trusted execution environment based on the first trusted application, and uploading the verification result of the data to be verified to the blockchain.

6. The method according to claim 1, wherein the transferring the data to be verified and the benchmark circulation data to the trusted execution environment of the terminal device through the first trusted application for performing data verification processing on the terminal device comprises:

transferring the data to be verified and the benchmark circulation data to the trusted execution environment of the terminal device in a ciphertext manner through the first trusted application for performing data verification processing on the terminal device.

7. The method according to claim 1, wherein the transferring the data to be verified and the benchmark circulation data to the trusted execution environment of the terminal device through the first trusted application for performing data verification processing on the terminal device comprises:

acquiring the data to be verified and the benchmark circulation data through a trusted program corresponding to the first trusted application for performing data verification processing on the terminal device, and transferring the data to be verified and the benchmark

circulation data to the trusted execution environment of the terminal device through the trusted program corresponding to the first trusted application.

8. The method according to claim 1, further comprising:

receiving an update request for the verification rule in the trusted execution environment of the terminal device, the update request comprising rule data to be updated, and the rule data to be updated being ciphertext;

transferring the rule data to be updated to the trusted execution environment of the terminal device through the first trusted application; and

decrypting the rule data to be updated in the trusted execution environment, and updating the verification rule based on the decrypted to-be-updated rule data.

9. The method according to claim 8, wherein the verification rule is set based on one or more of:

a data verification rule for the target service in the blockchain;

a time condition for data generation in the blockchain; and

an identity verification rule for a user uploading data in the blockchain.

10. The method according to claim 1, wherein the data to be verified and the benchmark circulation data are ciphertext, and the determining whether the data to be verified meets the verification rule by using the trusted execution environment and based on the circulation data in the data to be verified and the benchmark circulation data comprises performing in the trusted execution environment:

respectively decrypting the data to be verified and the benchmark circulation data to obtain decrypted to-be-verified data and decrypted benchmark circulation data;

processing the decrypted to-be-verified data and the decrypted benchmark circulation data respectively based on the verification rule to obtain first sub-data to be verified contained in the decrypted to-be-verified data and corresponding second sub-data to be verified contained in the decrypted benchmark circulation data; and

matching the first sub-data to be verified and the corresponding second sub-data to be verified respectively, and determining, based on matching results, whether the data to be verified meets the verification rule.

11. A device for processing blockchain data, the device being provided with a trusted execution environment and comprising:

a processor; and

a memory storing instructions executable by the processor,

wherein the processor is configured to:

acquire, from a blockchain, data to be verified of a target service, the data to be verified comprising circulation data generated during execution of the target service and recorded in the blockchain;

determine, based on the target service, a relevant third-party authority for verifying authenticity of the data to be verified, and acquire benchmark circulation data generated during the execution of the target service and recorded in the third-party authority;

transfer the data to be verified and the benchmark circulation data to the trusted execution environment of the device through a first trusted application for performing data verification processing on the device, wherein the trusted execution environment is provided with a verification rule for performing data verification on the data to be verified for the first trusted application; and

determine whether the data to be verified meets the verification rule by using the trusted execution environment and based on the circulation data in the data to be verified and the benchmark circulation data, and output a verification result of the data to be verified.

12. The device according to claim 11, wherein the data to be verified comprises at least one of resource transfer data corresponding to the target service or logistics data corresponding to the target service; and

the processor is further configured to perform at least one of:

determining, based on the resource transfer data corresponding to the target service, a relevant third-party authority for verifying authenticity of the resource transfer data as a resource storage institution, acquiring benchmark resource transfer data generated during the execution of the target service and recorded in the resource storage institution, and using the benchmark resource transfer data as the benchmark circulation data; or

determining, based on the logistics data corresponding to the target service, a relevant third-party authority for verifying authenticity of the logistics data as a traffic regulatory institution, acquiring benchmark logistics data generated during the execution of the target service and recorded in the traffic regulatory institution, and using the benchmark logistics data as the benchmark circulation data.

13. The device according to claim 12, wherein the resource transfer data comprises at least one of a resource transfer value or a resource transfer time, and the logistics data comprises at least one of information about a logistics path or a time for passing through a predetermined node in the logistics path.

14. The device according to claim 11, wherein the data to be verified comprises a fundraising resource transfer value and a fundraising resource transfer time; and the processor is further configured to:

determine, based on the fundraising resource transfer value and the fundraising resource transfer time, a relevant third-party authority for verifying authenticity of the data as a resource storage institution; and

acquire a benchmark fundraising resource transfer value and a benchmark fundraising resource transfer time generated during the execution of the target service and recorded in the resource storage institution, and use the benchmark fundraising resource transfer value and the benchmark fundraising resource transfer time as the benchmark circulation data.

15. The device according to claim 11, wherein the processor is further configured to:

acquire the verification result of the data to be verified from the trusted execution environment based on the first trusted application, and upload the verification result of the data to be verified to the blockchain.

16. The device according to claim 11, wherein the processor is further configured to:

transfer the data to be verified and the benchmark circulation data to the trusted execution environment of the device in a ciphertext manner through the first trusted application for performing data verification processing on the device.

17. The device according to claim 11, wherein the processor is further configured to:

acquire the data to be verified and the benchmark circulation data through a trusted program corresponding to the first trusted application for performing data verification processing on the device, and transfer the data to be verified and the benchmark circulation

data to the trusted execution environment of the device through the trusted program corresponding to the first trusted application.

18. The device according to claim 11, wherein the processor is further configured to:

receive an update request for the verification rule in the trusted execution environment of the device, the update request comprising rule data to be updated, and the rule data to be updated being ciphertext;

transfer the rule data to be updated to the trusted execution environment of the device through the first trusted application; and

decrypt the rule data to be updated in the trusted execution environment, and update the verification rule based on the decrypted to-be-updated rule data.

19. The device according to claim 18, wherein the verification rule is set based on one or more of:

a data verification rule for the target service in the blockchain;

a time condition for data generation in the blockchain; and

an identity verification rule for a user uploading data in the blockchain.

20. A non-transitory computer-readable storage medium having stored therein instructions that, when executed by a processor of a terminal device, cause the terminal device to perform a method for processing blockchain data, the terminal device being provided with a trusted execution environment, the method comprising:

acquiring, from a blockchain, data to be verified of a target service, the data to be verified comprising circulation data generated during execution of the target service and recorded in the blockchain;

determining, based on the target service, a relevant third-party authority for verifying authenticity of the data to be verified, and acquiring benchmark circulation data generated during the execution of the target service and recorded in the third-party authority;

transferring the data to be verified and the benchmark circulation data to the trusted execution environment of the terminal device through a first trusted application for performing data verification processing on the terminal device, wherein the trusted execution environment is provided with a verification rule for performing data verification on the data to be verified for the first trusted application; and

determining whether the data to be verified meets the verification rule by using the trusted execution environment and based on the circulation data in the data to be verified and the benchmark circulation data, and outputting a verification result of the data to be verified.