WHAT IS CLAIMED IS:

1. A computer-implemented method comprising:

receiving, by a smart contract service provider comprising a trusted computation execution environment (TEE) from a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target blockchain network, wherein the smart contract service provider is off the target blockchain network;

sending, by the smart contract service provider to a data visiting service provider, a request for the cross-chain data;

receiving, by the smart contract service provider, the cross-chain data from the data visiting service provider;

generating, by the TEE, a result using the cross-chain data; and

returning, by the smart contract service provider, the result to the client.

2. The computer-implemented method of claim 1, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data.

3. The computer-implemented method of claim 2, wherein the smart contract computational logics for operating the cross-chain data are self-designed by the client.

4. The computer-implemented method of claim 2, wherein the result is generated by the TEE executing the smart contract computational logics using the cross-chain data.

5. The computer-implemented method of claim 2, further comprising proving, by the smart contract service provider to the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating cross-chain data.

6. The computer-implemented method of claim 1, further comprising:

prior to receiving a request for operating cross-chain data from the client, proving, by the smart contract service provider to the client, that the smart contract service provider includes the TEE.

7. The computer-implemented method of claim 1, further comprising:

proving, by the smart contract service provider to the data visiting service provider, that the smart contract service provider includes the TEE; and

verifying, by the smart contract service provider, that the data visiting service provider includes a TEE.

8. The computer-implemented method of claim 1, further comprising:

uploading, by the smart contract service provider, the result to the target blockchain network.

9. The computer-implemented method of claim 8, further comprising:

prior to uploading the result to the target blockchain network, proving, by the smart contract service provider to the target blockchain network, that the smart contract service provider includes the TEE.

10. The computer-implemented method of claim 1, wherein the smart contract service provider comprises a cloud-based server.

11. The computer-implemented method of claim 1, wherein the result is signed by the TEE using a private key.

12. The computer-implemented method of claim 1, wherein the cross-chain data are obtained from two or more blockchain networks.

13. A computer-implemented method comprising:

generating, by a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target

blockchain network, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data;

sending, from the client, the request for operating cross-chain data to a smart contract service provider comprising a trusted computation execution environment (TEE), wherein the smart contract service provider is off the target blockchain network; and

receiving, by the client, a result from the smart contract service provider, wherein the result is generated by the TEE using the cross-chain data obtained by the smart contract service provider.

14. The computer-implemented method of claim 13, further comprising, sending, by the client, the received result to the target blockchain network.

15. The computer-implemented method of claim 13, further comprising:
prior to sending the request for operating cross-chain data to the smart contract service provider, verifying, by the client, that the smart contract service provider includes the TEE.

16. The computer-implemented method of claim 15, further comprising:
verifying, by the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating the cross-chain data.

17. The computer-implemented method of claim 13, further comprising:
designing, by the client, the smart contract computational logics for operating the cross-chain data.

18. The computer-implemented method of claim 13, wherein the client comprises a software development kit (SDK).

19. The computer-implemented method of claim 13, wherein the result is signed by the TEE using a private key, the method further comprising decrypting, by the client, the received result using a public key corresponding to the private key.

20. The computer-implemented method of claim 13, further comprising:
prior to sending the request for operating cross-chain data to the smart contract service provider, encrypting, by the client, the request for operating cross-chain data.

21. The computer-implemented method of claim 13, wherein the cross-chain data are obtained from two or more blockchain networks.

22. A non-transitory computer-readable storage medium coupled to one or more computers and configured with instructions executable by the one or more computers to:

receive, by a smart contract service provider comprising a trusted computation execution environment (TEE) from a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target blockchain network, wherein the smart contract service provider is off the target blockchain network;

send, by the smart contract service provider to a data visiting service provider, a request for the cross-chain data;

receive, by the smart contract service provider, the cross-chain data from the data visiting service provider;

generate, by the TEE, a result using the cross-chain data; and

return, by the smart contract service provider, the result to the client.

23. The non-transitory computer-readable storage medium of claim 22, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data.

24. The non-transitory computer-readable storage medium of claim 23, wherein the smart contract computational logics for operating the cross-chain data are self-designed by the client.

25. The non-transitory computer-readable storage medium of claim 23, wherein the result is generated by the TEE executing the smart contract computational logics using the cross-chain data.

26. The non-transitory computer-readable storage medium of claim 23, further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating cross-chain data.

27. The non-transitory computer-readable storage medium of claim 22, prior to receive a request for operating cross-chain data from the client, further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the client, that the smart contract service provider includes the TEE.

28. The non-transitory computer-readable storage medium of claim 22, further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the data visiting service provider, that the smart contract service provider includes the TEE; and

verify, by the smart contract service provider, that the data visiting service provider includes a TEE.

29. The non-transitory computer-readable storage medium of claim 22, further configured with instructions executable by the one or more computers to:

upload, by the smart contract service provider, the result to the target blockchain network.

30. The non-transitory computer-readable storage medium of claim 29, prior to upload the result to the target blockchain network, further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the target blockchain network, that the smart contract service provider includes the TEE.

31. The non-transitory computer-readable storage medium of claim 22, wherein the smart contract service provider comprises a cloud-based server.

32. The non-transitory computer-readable storage medium of claim 22, wherein the result is signed by the TEE using a private key.

33. The non-transitory computer-readable storage medium of claim 22, wherein the cross-chain data is obtained from two or more blockchain networks.

34. A non-transitory computer-readable storage medium coupled to one or more computers and configured with instructions executable by the one or more computers to:

generate, by a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target blockchain network, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data;

send, from the client, the request for operating cross-chain data to a smart contract service provider comprising a trusted computation execution environment (TEE), wherein the smart contract service provider is off the target blockchain network; and

receive, by the client, a result from the smart contract service provider, wherein the result is generated by the TEE using the cross-chain data obtained by the smart contract service provider.

35. The non-transitory computer-readable storage medium of claim 34, further configured with instructions executable by the one or more computers to:

send, by the client, the received result to the target blockchain network.

36. The non-transitory computer-readable storage medium of claim 35, further configured with instructions executable by the one or more computers to:

prior to sending the request for operating cross-chain data to the smart contract service provider, verify, by the client, that the smart contract service provider includes the TEE.

37. The non-transitory computer-readable storage medium of claim 34, further configured with instructions executable by the one or more computers to:

verify, by the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating the cross-chain data.

38. The non-transitory computer-readable storage medium of claim 34, further configured with instructions executable by the one or more computers to:

design, by the client, the smart contract computational logics for operating the cross-chain data.

39 The non-transitory computer-readable storage medium of claim 34, wherein the client comprises a software development kit (SDK).

40. The non-transitory computer-readable storage medium of claim 34, wherein the result is signed by the TEE using a private key, further configured with instructions executable by the one or more computers to:

decrypt, by the client, the received result using a public key corresponding to the private key.

41. The non-transitory computer-readable storage medium of claim 34, further configured with instructions executable by the one or more computers to:

prior to sending the request for operating cross-chain data to the smart contract service provider, encrypt, by the client, the request for operating cross-chain data.

42. The non-transitory computer-readable storage medium of claim 34, wherein the cross-chain data are obtained from two or more blockchain networks.

43. A system for providing smart contract service, comprising:

an interface configured to receive, from a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target blockchain network; wherein the system is off the target blockchain network; and

a trusted computation execution environment (TEE), wherein the TEE comprises:

one or more computers; and

one or more computer-readable memories coupled to the one or more computers and configured with instructions executable by the one or more computers to:

send a request for the cross-chain data to a data visiting service provider;

receive the cross-chain data from the data visiting service provider; and

generate a result using the cross-chain data; and

wherein the interface configured to return the result to the client.

44. The system of claim 43, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data.

45. The system of claim 44, wherein the smart contract computational logics for operating the cross-chain data are self-designed by the client.

46. The system of claim 44, wherein the result is generated by the TEE executing the smart contract computational logics using the cross-chain data.

47. The system of claim 44, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating cross-chain data.

48. The system of claim 43, prior to receive a request for operating cross-chain data from the client, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the client, that the smart contract service provider includes the TEE.

49. The system of claim 43, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the data visiting service provider, that the smart contract service provider includes the TEE; and

verify, by the smart contract service provider, that the data visiting service provider includes a TEE.

50. The system of claim 43, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

upload, by the smart contract service provider, the result to the target blockchain network.

51. The system of claim 50, prior to upload the result to the target blockchain network, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prove, by the smart contract service provider to the target blockchain network, that the smart contract service provider includes the TEE.

52. The system of claim 43, wherein the smart contract service provider comprises a cloud-based server.

53. The system of claim 43, wherein the result is signed by the TEE using a private key.

54. The system of claim 43, wherein the cross-chain data are obtained from two or more blockchain networks.

55. A system, comprising:

one or more computers; and

one or more computer-readable memories coupled to the one or more computers and configured with instructions executable by the one or more computers to:

generate, by a client associated with a target blockchain network, a request for operating cross-chain data of one or more blockchain networks different from the target blockchain network, wherein the request for operating cross-chain data comprises smart contract computational logics for operating the cross-chain data;

send, from the client, the request for operating cross-chain data to a smart contract service provider comprising a trusted computation execution environment (TEE), wherein the smart contract service provider is off the target blockchain network; and

receive, by the client, a result from the smart contract service provider, wherein the result is generated by the TEE using the cross-chain data obtained by the smart contract service provider.

56. The system of claim 55, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

send, by the client, the received result to the target blockchain network.

57. The system of claim 56, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prior to sending the request for operating cross-chain data to the smart contract service provider, verify, by the client, that the smart contract service provider includes the TEE.

58. The system of claim 55, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

verify, by the client, that the TEE comprises a virtual machine operable to execute the smart contract computational logics in the request for operating the cross-chain data.

59. The system of claim 55, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

design, by the client, the smart contract computational logics for operating the cross-chain data.

60. The system of claim 55, wherein the client comprises a software development kit (SDK).

61. The system of claim 55, wherein the result is signed by the TEE using a private key, the computer-readable memories are further configured with instructions executable by the one or more computers to:

decrypt, by the client, the received result using a public key corresponding to the private key.

62. The system of claim 55, wherein the computer-readable memories are further configured with instructions executable by the one or more computers to:

prior to sending the request for operating cross-chain data to the smart contract service provider, encrypt, by the client, the request for operating cross-chain data.

63. The system of claim 55, wherein the cross-chain data are obtained from two or more blockchain networks.