

What is claimed is:

1. A blockchain-based event processing method for processing an event involving a plurality of users in a blockchain, the method comprising:

generating, by a computing device of a user of the event, descriptive information of the event;

sending the descriptive information to a computing device of another user of the event through an off-chain channel for the another user to verify the descriptive information and to submit triggering information corresponding to the event to the blockchain after verifying the descriptive information; and

submitting, by the computing device of the user, triggering information associated with the user corresponding to the event to the blockchain for the blockchain to process the event according to the descriptive information after verifying all triggering information submitted by the plurality of users.

2. The method according to claim 1, wherein the triggering information comprises the descriptive information and a confirmation generated by the computing device of the user indicating that the user has verified the descriptive information.

3. The method according to any proceeding claim, wherein the descriptive information on the event comprises a variable, and wherein the event changes a state parameter recorded on the blockchain associated with each of the plurality users according to the variable.

4. The method according to claim 3, wherein the variable and the value of the state parameter are each a ciphertext calculated based on a homomorphic encryption algorithm or a homomorphic commitment algorithm.

5. The method according to any of the claims 3-4, wherein the descriptive information further comprises: a first proof proving that the variable is within a numerical range, and

in response to the event decreasing the value of the state parameter according to the variable, the triggering information comprises: a second proof proving that the value of the state parameter is not less than the decrease of the state parameter.

6. The method according to any of the claims 3-5, wherein in response to a transfer event, the plurality of users of the event comprise a remitter and a recipient; the variable comprises a transfer amount; and the state parameter comprises an account balance.

7. The method according to any of the claims 3-6, wherein in response to a remittance event, the plurality of users of the event comprise a remitter, n relays, and a recipient, the

variable comprises a transfer amount of a first-type asset between the remitter and the first relay, a transfer amount of an i^{th} -type asset between an $(i-1)^{\text{th}}$ relay and an i^{th} relay if $i > 1$, and a transfer amount of an $(n+1)^{\text{th}}$ -type asset between an n^{th} relay and the recipient, and the state parameter comprises an account balance, wherein $1 \leq i \leq n$.

8. The method according to any preceding claim, wherein the submitting triggering information associated with the user corresponding to the event to the blockchain comprises:

adding the triggering information to a waiting queue as a to-be-submitted transaction;

creating a merged transaction by including one or more to-be-submitted transactions selected from the waiting queue according to a predetermined rule; and

submitting the merged transaction to the blockchain for processing the one or more to-be-submitted transactions in the merged transaction in the blockchain.

9. A system for processing a blockchain-based event involving a plurality of users, 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 the claims 1 to 8.

10. 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 the claims 1 to 8.

11. A blockchain-based event processing method for processing an event involving a plurality of users in a blockchain, the method comprising:

obtaining, by a computing device of a user of the event, descriptive information of the event, the descriptive information being sent by a computing device of another user of the event through an off-chain channel; and

submitting, by the computing device of the user, triggering information associated with the user corresponding to the event to the blockchain after verifying the descriptive information for the blockchain to process the event according to the descriptive information after verifying all triggering information submitted by the plurality of users.

12. The method according to claim 11, wherein the triggering information comprises: the descriptive information and a confirmation generated by the computing device of the user indicating that the user has verified the descriptive information.

13. The method according to any of the claims 11-12, wherein the descriptive information comprises a variable, and wherein the event changes a state parameter recorded on the blockchain associated with each of the plurality of users according to the variable.

14. The method according to claim 13, the variable and the value of the state parameter are each a ciphertext calculated based on a homomorphic encryption algorithm or a homomorphic commitment algorithm.

15. The method according to any of the claims 13-14, wherein the descriptive information further comprises: a first proof proving that the variable is within a correct numerical range, and

in response to the event decreasing the value of the state parameter according to the variable, the triggering information comprises: a second proof proving that the value of the state parameter is not less than the decrease of the state parameter.

16. The method according to any of the claims 13-15, wherein

in response to a transfer event, the plurality of users of the event comprise a remitter and a recipient; the variable comprises a transfer amount; and the state parameter comprises an account balance; and

in response to a remittance event, the plurality of users of the event comprise a remitter, n relays, and a recipient; the variable comprises a transfer amount of a first-type asset between the remitter and the first relay, a transfer amount of an i^{th} -type asset between an $(i-1)^{\text{th}}$ relay and an i^{th} relay if $i > 1$, and a transfer amount of an $(n+1)^{\text{th}}$ -type asset between an n^{th} relay and the recipient; and the state parameter comprises: an account balance, wherein $1 \leq i \leq n$.

17. The method according to any of the claims 11-16, wherein the submitting triggering information associated with the user corresponding to the event to the blockchain comprises:

adding the triggering information to a waiting queue as a to-be-submitted transaction;

creating a merged transaction by including one or more to-be-submitted transactions selected from the waiting queue according to a predetermined rule; and

submitting the merged transaction to the blockchain for processing the one or more to-be-submitted transactions in the merged transaction in the blockchain.

18. A system for processing a blockchain-based event involving a plurality of users, 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 the claims 11 to 17.

19. 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 the claims 11 to 17.

20. A blockchain-based event processing method for processing an event involving a plurality of users on a blockchain, the method comprising:

verifying, by a blockchain node, triggering information submitted by a computing device of one of the plurality of users of the event, wherein the triggering information is submitted after the user verifies descriptive information on the event; and

processing the event based on the descriptive information after verifying all triggering information submitted by the plurality of users.

21. The method according to claim 20, wherein the triggering information comprises: the descriptive information and a confirmation generated by the computing device of the user indicating that the user has verified the descriptive information.

22. The method according to any of the claims 20-21, wherein the descriptive information on the event comprises a variable, and wherein the event changes a state parameter recorded on the blockchain associated with each of the plurality users according to the variable.

23. The method according to claim 22, wherein

in response to a transfer event, the plurality of users of the event comprise a remitter and a recipient; the variable comprises a transfer amount; and the state parameter comprises an account balance; and

in response to a remittance event, the plurality of users of the event comprise a remitter, n relays, and a recipient; the variable comprises a transfer amount of a first-type asset between the remitter and the first relay, a transfer amount of an i^{th} -type asset between an $(i-1)^{\text{th}}$ relay and an i^{th} relay if $i > 1$, and a transfer amount of an $(n+1)^{\text{th}}$ -type asset between an n^{th} relay and the recipient; and the state parameter comprises: an account balance, wherein $1 \leq i \leq n$.

24. The method according to any of the claims 20-23, further comprising:

receiving a merged transaction comprising one or more to-be-submitted transactions selected from a waiting queue, wherein the one or more to-be-submitted transactions

comprise the triggering information added to the waiting queue as a to-be-submitted transaction after the user verifies the descriptive information; and

processing each to-be-submitted transaction in the merged transaction.

25. A system for processing a blockchain-based event involving a plurality of users, 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 the claims 20 to 24.

26. 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 the claims 20 to 24.