

Claims

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 first user of the event, descriptive information of the event, wherein the descriptive information comprises:

one or more blockchain account addresses of one or more second users of the plurality of users, and

for each of the second users, a variable representing an amount to be transferred into a blockchain account of the each second user, wherein the variable is encrypted with a homomorphic encryption algorithm or a homomorphic commitment algorithm based on a public key of the each second user, and a first range proof that the variable is within a numerical range;

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 first triggering information corresponding to the event to the blockchain after verifying the descriptive information; and

submitting, by the computing device of the first user, second triggering information associated with the first 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;

~~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,~~

~~wherein the variable and the value of the state parameter are each a ciphertext calculated based on a Pedersen commitment algorithm.~~

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

3. The method according to claim 1, 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 first triggering information comprises: a second proof proving that the value of the state parameter is not less than the decrease of the state parameter.

4. The method according to any of the claims 1 or 3, 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.

5. The method according to any of the claims 1 or 3-4, 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 $1 \leq i \leq n$.

6. The method according to any proceeding claim, wherein the submitting second triggering information associated with the first user corresponding to the event to the blockchain comprises:

adding the second 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.

7. 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 6.

8. 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 6.

9. 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, wherein the descriptive information comprises:

one or more blockchain account addresses of one or more users of the plurality of users including the user, and

for each of the second users, a variable representing an amount to be transferred into a blockchain account of the each second user, wherein the variable is encrypted with a homomorphic encryption algorithm or a homomorphic commitment algorithm based on a public key of the each second user, and a first range proof that the variable is within a numerical range; 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, wherein the triggering information comprises:

signature information generated for the descriptive information by the user through a private key of the user, and

a second range proof that a state parameter of the user stored in the blockchain is not less than an amount determined based on the variable

~~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;~~

~~the variable and the value of the state parameter are each a ciphertext calculated based on a Pedersen commitment algorithm.~~

10. The method according to claim 9, 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.

~~11. The method according to claim 9, 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.~~

~~12~~11. The method according to ~~any of the claims 9 or 11~~, 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 $1 \leq i \leq n$.

~~13~~12. The method according to any of the claims 9-~~12~~11, 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.

~~14~~13. 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 9 to ~~13~~12.

~~15~~14. 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 9 to ~~13~~12.

~~16~~15. 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, wherein the descriptive information comprises:

one or more blockchain account addresses of one or more users in the plurality of users including the user;

for each of the one or more users, a variable representing an amount to be transferred into a blockchain account of the each user, wherein the variable is encrypted with a homomorphic encryption algorithm or a homomorphic commitment algorithm based on a public key of the each user, and a first range proof that the variable is within a numerical range,

wherein the triggering information from the user comprises:

signature information generated for the descriptive information by the user through a private key of the user, and

a second range proof that a state parameter of the user stored in the blockchain is not less than an amount determined based on the variable; and

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

~~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,~~

~~the variable and the state parameter are each a ciphertext calculated based on a Pedersen commitment algorithm.~~

~~1716.~~ The method according to claim ~~1615~~, 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.

~~1817.~~ The method according to claim ~~1615~~, 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 $1 \leq i \leq n$.

~~1918.~~ The method according to any of the claims ~~1615-1817~~, 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.

~~2019~~. 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 ~~16-15~~ to ~~19~~18.

~~2120~~. 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 ~~16-15~~ to ~~19~~18.