

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a validation computer, an authorization request message from a user
3 device, wherein the authorization request message comprises a user state and a user proof,
4 wherein the user state comprises a first user state element and a second user state element, and
5 wherein the user proof comprises a first user proof element, a second user proof element, and a
6 third user proof element;
7 computing, by the validation computer, a first verification value by multiplying
8 the first user proof element raised to the power of the second user state element, and the second
9 user proof element raised to the power of the first user state element;
10 computing, by the validation computer, a second verification value by raising the
11 second user proof element to the power of the second user state element;
12 comparing, by the validation computer, the first verification value to a first
13 accumulated state element of an accumulated state;
14 comparing, by the validation computer, the second verification value to a second
15 accumulated state element of the accumulated state; and
16 authorizing, by the validation computer, the authorization request message if the
17 first verification value matches the first accumulated state element and the second verification
18 value matches the second accumulated state element,
19 wherein the validator computer maintains a blockchain in a verification network,
20 wherein the accumulated state is stored in each block of the blockchain.

1 2. The method of claim 1, wherein the authorization request message
2 comprises an interaction amount, and wherein the method further comprises:
3 updating, by the validation computer, the accumulated state based on the
4 interaction amount.

1 3. The method of claim 2, wherein updating the accumulated state based on
2 the interaction amount further comprises:

3 computing, by the validation computer, an updated first accumulated state
4 element by multiplying 1) the first accumulated state element and 2) the second user proof
5 element raised to the power of the interaction amount.

1 4. The method of claim 1, wherein the first user state element is an amount
2 associated with a user, the second user state element is a random number, and the third user
3 proof element indicates a number of entries in the accumulated state.

1 5. The method of claim 1, wherein prior to receiving the authorization
2 request message, the user device generates the authorization request message requesting
3 authorization for an interaction between the user device and a receiver device.

1 6. The method of claim 1 further comprising:
2 comparing, by the validation computer, the third user proof element to a third
3 accumulated state element of the accumulated state.

1 7. The method of claim 6, wherein authorizing the authorization request
2 message includes:
3 authorizing, by the validation computer, the authorization request message if the
4 first verification value matches the first accumulated state element, the second verification value
5 matches the second accumulated state element, and the third user proof element matches the
6 third accumulated state element.

1 8. The method of claim 1, wherein the first user proof element is derived
2 from a plurality of first user state elements and a plurality of second user state elements
3 associated with a plurality of user states, and wherein the second user proof element is derived
4 from the plurality of second user state elements associated with the plurality of user states.

1 9. A validation computer comprising:
2 a processor;
3 a memory; and
4 a computer-readable medium coupled to the processor, the computer-readable
5 medium comprising code executable by the processor for implementing a method comprising:

6 receiving an authorization request message from a user device, wherein
7 the authorization request message comprises a user state and a user proof, wherein the
8 user state comprises a first user state element and a second user state element, and
9 wherein the user proof comprises a first user proof element, a second user proof element,
10 and a third user proof element;
11 computing a first verification value by multiplying the first user proof
12 element raised to the power of the second user state element, and the second user proof
13 element raised to the power of the first user state element;
14 computing a second verification value by raising the second user proof
15 element to the power of the second user state element;
16 comparing the first verification value to a first accumulated state element
17 of an accumulated state;
18 comparing the second verification value to a second accumulated state
19 element of the accumulated state; and
20 authorizing the authorization request message if the first verification value
21 matches the first accumulated state element and the second verification value matches the
22 second accumulated state element,
23 wherein the method further comprises:
24 retrieving, by the validation computer, the accumulated state comprising
25 the first accumulated state element and the second accumulated state element from a
26 previous block in a blockchain maintained by the validation computer.

1 10. The validation computer of claim 9, wherein the first user state element is
2 an amount associated with a user, the second user state element is a random number, the third
3 user proof element indicates a number of entries in the accumulated state, and wherein the first
4 user proof element is derived from a plurality of first user state elements and a plurality of
5 second user state elements associated with a plurality of user states, and wherein the second user
6 proof element is derived from the plurality of second user state elements associated with the
7 plurality of user states.

1 11. The validation computer of claim 9, wherein the authorization request
2 message is a request to authorize an interaction and comprises an interaction amount.

1 12. The validation computer of claim 11, wherein the user device updates the
2 user proof based on the interaction amount, and wherein the method further comprises:
3 updating, by the validation computer, the accumulated state based on the
4 interaction amount.

1 13. A validation computer comprising:
2 a processor;
3 a memory; and
4 a computer-readable medium coupled to the processor, the computer-readable
5 medium comprising code executable by the processor for implementing a method comprising:
6 receiving an authorization request message from a user device, wherein
7 the authorization request message comprises a user state and a user proof, wherein the
8 user state comprises a first user state element and a second user state element, and
9 wherein the user proof comprises a first user proof element, a second user proof element,
10 and a third user proof element;
11 computing a first verification value by multiplying the first user proof
12 element raised to the power of the second user state element, and the second user proof
13 element raised to the power of the first user state element;
14 computing a second verification value by raising the second user proof
15 element to the power of the second user state element;
16 comparing the first verification value to a first accumulated state element
17 of an accumulated state;
18 comparing the second verification value to a second accumulated state
19 element of the accumulated state; and
20 authorizing the authorization request message if the first verification value
21 matches the first accumulated state element and the second verification value matches the
22 second accumulated state element,
23 wherein the authorization request message is a request to authorize an interaction
24 and comprises an interaction amount, and
25 wherein after authorizing the authorization request message, the method further
26 comprises:

27 including, by the validation computer, at least the interaction amount into a new
28 block of a blockchain maintained by the validation computer.

1 14. The validation computer of claim 9, wherein after authorizing the
2 authorization request message, the method further comprises:
3 generating, by the validation computer, an authorization response message
4 indicating whether or not the authorization request message is authorized; and
5 providing, by the validation computer, the authorization response message to the
6 user device.

1 15. The validation computer of claim 14, wherein the user device provides the
2 authorization response message to a receiver device with which the user device initiated an
3 interaction.

1 16. A method comprising:
2 generating, by a user device, an authorization request message comprising a user
3 state and a user proof, wherein the user state comprises a first user state element and a second
4 user state element , and wherein the user proof comprises a first user proof element, a second
5 user proof element, and a third user proof element;
6 providing, by the user device, the authorization request message to a validation
7 computer of a plurality of validation computers, wherein the validation computer 1) computes a
8 first verification value by multiplying the first user proof element raised to the power of the
9 second user state element , and the second user proof element raised to the power of the first user
10 state element, 2) computes a second verification value by raising the second user proof element
11 to the power of the second user state element, 3) compares the first verification value to a first
12 accumulated state element of an accumulated state, 4) compares the second verification value to
13 a second accumulated state element of the accumulated state, and 5) authorizes the authorization
14 request message if the first verification value matches the first accumulated state element and the
15 second verification value matches the second accumulated state element; and
16 receiving, by the user device, an authorization response message from the
17 validation computer, wherein the authorization response message indicates whether or not the
18 authorization request message was authorized, wherein the method further comprises:

19 prior to generating the authorization request message, updating, by the user
20 device, the user proof based on interactions included in a blockchain since a last time the user
21 proof was updated.

1 17. The method of claim 16, wherein the authorization request message
2 requests authorization for an interaction between the user device and a receiver device, wherein
3 the authorization request message comprises an interaction amount, and wherein the method
4 further comprises:
5 providing, by the user device, the authorization response message to the receiver
6 device.