

WHAT IS CLAIMED IS:

1. A computer-implemented method for facilitating a consensus process in a blockchain network based on practical Byzantine fault tolerance (PBFT), comprising:
 - 5 setting, by a first consensus node, a first timer that initiates a view change upon timeout;
 - setting, by the first consensus node, a second timer that expires before the first timer;
 - in response to the second timer expiring, sending, to a second consensus node, a request for one or more missing consensus messages, wherein the one or more missing consensus messages were previously transmitted to the first consensus node, but not received by the first
 - 10 consensus node;
 - receiving, from the second consensus node, the one or more missing consensus messages each digitally signed by a private key of a corresponding consensus node that generates the one or more missing consensus messages; and
 - determining that a block of transactions is valid, if a quantity of commit messages included
 - 15 in the one or more missing consensus messages is greater than or equal to $2f + 1$, where f is a maximum number of faulty nodes that is tolerable by the blockchain network based on PBFT, and wherein n is a total number of consensus nodes in the blockchain network and f is a largest integer less than or equal to $(n-1)/3$.
- 20 2. The computer-implemented method of claim 1, wherein the request includes a sequence number that indicates a number of a consensus round.
3. The computer-implemented method of claim 1, wherein the one or more missing consensus messages include one or more of pre-prepare messages, prepare messages, and commit messages
- 25 missing by the first consensus node.
4. The computer-implemented method of claim 1, wherein the one or more missing consensus messages are stored in one or more consensus nodes in which they are generated or stored, until a stable checkpoint is reached.

30

5. The computer-implemented method of claim 1, further comprising receiving one or more sequence numbers corresponding to the one or more missing consensus messages, wherein each sequence number indicates a number of a consensus round associated with a corresponding consensus message.

5

6. The computer-implemented method of claim 1, further comprising submitting the block of transactions to a blockchain and a status database, if the block of transactions is determined valid.

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

10 sending, to a third consensus node, a request for a second one or more missing consensus messages by the second consensus node in response to the second timer expiring and if the block of transactions is determined invalid;

receiving, from the third consensus node, the second one or more missing consensus messages each digitally signed by a private key of a corresponding consensus node that generates
15 the second one or more missing consensus messages; and

determining that the block of transactions is valid, if a quantity of commit messages included in the one or more missing consensus messages and the second one or more missing consensus messages is greater than or equal to $2f + 1$.

20 8. A non-transitory computer-readable storage medium coupled to one or more processors and having instructions stored thereon which, when executed by the one or more processors, cause the one or more processors to perform operations in accordance with the method of one or more of claims 1-7.

25 9. A system, comprising:

a computing device; and

a computer-readable storage device coupled to the computing device and having instructions stored thereon which, when executed by the computing device, cause the computing device to perform operations in accordance with the method of one or more of claims 1-7.