

ABSTRACT

The present invention is suitable for the technical field of block chains, and provides a consensus method and a consensus apparatus for a blockchain system. The consensus method includes: generating a subsequent proposal block by referencing a plurality of proposal blocks
5 and combining current transactions from clients in an $(n+x_2)$ -th consensus round; and achieving consensus on the preceding proposal block by using the subsequent proposal block as a certificate for the preceding proposal block. The plurality of proposal blocks are correspondingly generated by the plurality of validation nodes referencing a preceding proposal block in an n -th consensus round, and the preceding proposal block is generated in
10 an $(n-x_1)$ -th consensus round. In the consensus method of the present invention, there is no need to transmit a large amount of signature messages in the consensus process, and consensus on a specific block is achieved by establishing reference relationships between blocks generated in different consensus rounds. In this way, the overhead of transmitting and validating signature messages in the consensus process is reduced.

15

[Fig. 1]