METHOD AND SYSTEM FOR AN EFFICIENT CONSENSUS MECHANISM FOR PERMISSIONED BLOCKCHAINS USING AUDIT GUARANTEES

ABSTRACT OF THE DISCLOSURE

A method for addition of a block to a permissioned blockchain using efficient consensus includes: storing a blockchain; receiving transaction messages having transaction values from consensus nodes; generating a Merkle root for the transactions messages using transaction references; generating a proposed block header having the Merkle root and a hash of the header of the most recently added block in the blockchain; hashing the proposed block header; transmitting a proposal message having a digital signature and the hashed proposed block header to auditing nodes; receiving a response message accepting the digital signature from a majority of auditing nodes; transmitting an accept message to the auditing nodes; transmitting a confirmation message to the consensus nodes including the hashed proposed block header and digital signature; and writing a new block to the blockchain having the transaction values from the transaction messages and a header including the proposed block header and digital signature.

[FIG. 1]