often takes upwards of ten minutes. In many instances, this length of time may be unacceptable for a blockchain implementation.

Thus, there is a need for a technical solution for a consensus mechanism for a blockchain that can be performed quickly, efficiently, and with a minimal amount of processing power as compared to existing blockchain implementations and consensus mechanisms. A faster, more efficient consensus mechanism may enable a blockchain to be implemented more easily and distributed among computing devices with lower system specifications, while also ensuring consensus for new transactions and other records added to the blockchain more quickly.

SUMMARY

The present disclosure provides a description of systems and methods for adding blocks to a permissioned blockchain using an efficient consensus mechanism.

In one aspect, the present disclosure refers to a method for adding a block to a permissioned blockchain using an efficient consensus mechanism includes: storing, in a memory of a processing server, a blockchain comprising a plurality of blocks including a recently added block, the recently added blocking including at least a block header and one or more transaction values; receiving, by a receiving device of the processing server, a plurality of transaction messages from one or more consensus nodes associated with the blockchain, wherein each transaction message includes at least a transaction value; generating, by a hashing module of the processing server, a Merkle root for the plurality of transaction messages using a transaction reference associated with the transaction value included in each of the plurality of transaction messages; generating, by the hashing module of the processing server, a previous hash value via application of a hashing algorithm to the block header included in the recently added block; generating, by a generation module of the processing server, a proposed block header, wherein the proposed block header includes at least the previous hash value and the generated Merkle root; generating, by the hashing module of the processing server, a confirmation hash value via application of the hashing algorithm to the generated proposed block header; generating, by the generation module of the processing server, a proposal number, wherein the proposal number is a

numeric value of a digital signature generated for the generated proposed block header; electronically

transmitting, by a transmitting device of the processing server, a prepare message to a plurality of auditing nodes associated with the blockchain, wherein the prepare message includes at least the generated confirmation hash value and generated proposal number; receiving, by the receiving device of the processing server, a response message from at least a majority of the plurality of auditing nodes, wherein each prepare response message includes at least the generated confirmation hash value and an accepted proposal number; identifying, by a data identification module of the processing server, an agreed proposal number based on the numeric value of the generated proposal number and a numeric value of the accepted proposal number included in each response message and a predetermined criteria; electronically transmitting, by the transmitting device of the processing server, an accept message to the plurality of auditing nodes, wherein the accept message includes at least the generated confirmation hash value and the identified agreed proposal number; electronically transmitting, by the transmitting device of the processing server, a confirm message to a plurality of consensus nodes associated with the blockchain, wherein the confirm message includes at least the generated confirmation hash value and the identified agreed proposal number; and executing, by a querying module of the processing server, a query on the memory to add a new block to the blockchain, the new block including at least the transaction value included in each of the plurality of transaction messages a new block header including at least the previous hash value, the generated Merkle root, and the agreed proposal number.

In another aspect, the present disclosure refers to a system for adding a block to a permissioned blockchain using an efficient consensus mechanism includes: a transmitting device of a processing server; a data identification module of the processing server; a querying module of the processing server; a memory of the processing server configured to store a blockchain comprising a plurality of blocks including a recently added block, the recently added blocking including at least a block header and one or more transaction values; a receiving device of the processing server configured to receive a plurality of transaction messages from one or more consensus nodes associated with the blockchain, wherein each transaction message includes at least a transaction value; a hashing module of the processing server configured to generate a Merkle root for the plurality of transaction messages using a transaction reference associated with the transaction value included in each of the

plurality of transaction messages, and a previous hash value via application of a hashing algorithm to the block header

included in the recently added block; and a generation module of the processing server configured to generate a proposed block header, wherein the proposed block header includes at least the previous hash value and the generated Merkle root. The hashing module of the processing server is further configured to generate a confirmation hash value via application of the hashing algorithm to the generated proposed block header. The generation module of the processing server is further configured to generate a proposal number, wherein the proposal number is a numeric value of a digital signature generated for the generated proposed block header. The transmitting device of the processing server is configured to electronically transmit a prepare message to a plurality of auditing nodes associated with the blockchain, wherein the prepare message includes at least the generated confirmation hash value and generated proposal number. The receiving device of the processing server is further configured to receive a response message from at least a majority of the plurality of auditing nodes, wherein each prepare response message includes at least the generated confirmation hash value and an accepted proposal number. The data identification module of the processing server is configured to identify an agreed proposal number based on the numeric value of the generated proposal number and a numeric value of the accepted proposal number included in each response message and a predetermined criteria. The transmitting device of the processing server is further configured to electronically transmit: an accept message to the plurality of auditing nodes, wherein the accept message includes at least the generated confirmation hash value and the identified agreed proposal number; and a confirm message to a plurality of consensus nodes associated with the blockchain, wherein the confirm message includes at least the generated confirmation hash value and the identified agreed proposal number. The querying module of the processing server is further configured to execute a query on the memory to add a new block to the blockchain, the new block including at least the transaction value included in each of the plurality of transaction messages a new block header including at least the previous hash value, the generated Merkle root, and the agreed proposal number.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

The scope of the present disclosure is best understood from the following detailed description of exemplary embodiments when read in conjunction with the accompanying drawings. Included in the drawings are the following figures: