WHAT IS CLAIMED IS:

1. A method for adding a block to a permissioned blockchain using an efficient consensus mechanism, comprising:

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 the generation module of the processing server, a proposal number, wherein the proposal number is a numeric value of a digital signature generated for a proposed block header that includes a previous hash value and a Merkle root generated for the plurality of transaction messages;

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 a confirmation hash value and the 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.

2. The method of claim 1, wherein

each of the plurality of transaction messages further includes a specific slot identifier,

the proposed block header, prepare message, response message, accept message, confirm message, and new block header each include the specific slot identifier, and

the block header included in the recently added block includes a different slot identifier.

3. The method of claim 1, wherein the Merkle root is generated using the transaction value included in each of the plurality of transaction messages.

4. The method of claim 1, further comprising:

generating, by the hashing module of the processing server, a transaction reference associated with the transaction value included in each of the plurality of transaction messages by hashing the respective transaction value using a predetermined hashing algorithm, wherein

the Merkle root is generated using the transaction reference included in each of the plurality of transaction messages.

5. The method of claim 1, further comprising:

storing, in the memory of the processing server, a consensus delay time, wherein

each of the plurality of transaction messages further includes a common identification value associated with a time, and

the Merkle root is generated after expiration of the consensus delay time after the time associated with the common identification value.

6. The method of claim 1, further comprising:

sorting, by the querying module of the processing server, a transaction reference associated with the transaction value included in each of the plurality of transaction messages based on a natural ordering prior to generating the Merkle root.

7. The method of claim 1, further comprising:

electronically transmitting, by the transmitting device of the processing server, a proposal message to the plurality of consensus nodes, wherein the proposal message includes at least the generated Merkle root.

8. The method of claim 1, further comprising:

receiving, by the receiving device of the processing server, a proposal message from each of the plurality of consensus nodes, wherein the proposal message includes at least a proposed Merkle root; and

verifying, by a verification module of the processing server, that the generated Merkle root is equivalent to at least a majority of the proposed Merkle roots included in the received proposal messages.

9. The method of claim 1, wherein

the proposal number is further generated using a nonce in combination with the digital signature,

the prepare message further includes the nonce,

each response message further includes an associated nonce, and

the accept message, confirm message, and new block header further include the nonce associated with the agreed proposal number.

10. The method of claim 1, further comprising:

storing, in the memory, a public key associated with the processing server, wherein

the digital signature is generated for the proposed block header using the public key,

the prepare message further includes the public key,

each response message further includes an associated public key used in generation of the associated accepted proposal number, and

the accept message, confirm message, and new block header further include the public key associated with the agreed proposal number.

11. The method of claim 1, further comprising:

sorting, by the querying module of the processing server, the generated proposal number and the accepted proposal number included in each response message based on the respective numeric value, wherein

the agreed proposal number is identified based on the sorting and a predetermined criteria.

12. The method of claim 11, wherein the predetermined criteria is selecting the highest numeric value.

13. A system for adding a block to a permissioned blockchain using an efficient consensus mechanism, comprising:

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; and

a generation module of the processing server configured to generate

a proposal number, wherein the proposal number is a numeric value of a digital signature generated for a generated proposed block header that includes a previous hash value and a Merkle root generated for the plurality of transaction messages, wherein

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 a generated confirmation hash value and the 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, and

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.

14. The system of claim 13, wherein

each of the plurality of transaction messages further includes a specific slot identifier,

the proposed block header, prepare message, response message, accept message, confirm message, and new block header each include the specific slot identifier, and

the block header included in the recently added block includes a different slot identifier.

15. The system of claim 13, wherein the Merkle root is generated using the transaction value included in each of the plurality of transaction messages.

16. The system of claim 13, wherein the hashing module of the processing server is further configured to generate a transaction reference associated with the transaction value included in each of the plurality of transaction messages by hashing the respective transaction value using a predetermined hashing algorithm, and

the Merkle root is generated using the transaction reference included in each of the plurality of transaction messages.

17. The system of claim 13, wherein

the memory of the processing server is further configured to store a consensus delay time,

each of the plurality of transaction messages further includes a common identification value associated with a time, and

the Merkle root is generated after expiration of the consensus delay time after the time associated with the common identification value.

18. The system of claim 13, wherein the querying module of the processing server is further configured to sort a transaction reference associated with the transaction value included in each of the plurality of transaction messages based on a natural ordering prior to generating the Merkle root.

19. The system of claim 13, wherein the transmitting device of the processing server is further configured to electronically transmit a proposal message to the plurality of consensus nodes, wherein the proposal message includes at least the generated Merkle root.

20. The system of claim 13, further comprising:

a verification module of the processing server, wherein

the receiving device of the processing server is further configured to receive a proposal message from each of the plurality of consensus nodes, wherein the proposal message includes at least a proposed Merkle root, and

the verification module of the processing server is configured to that the generated Merkle root is equivalent to at least a majority of the proposed Merkle roots included in the received proposal messages.

21. The system of claim 13, wherein

the proposal number is further generated using a nonce in combination with the digital signature,

the prepare message further includes the nonce,

each response message further includes an associated nonce, and

the accept message, confirm message, and new block header further include the nonce associated with the agreed proposal number.

22. The system of claim 13, wherein

the memory is further configured to store a public key associated with the processing server,

the digital signature is generated for the proposed block header using the public key,

the prepare message further includes the public key,

each response message further includes an associated public key used in generation of the associated accepted proposal number, and

the accept message, confirm message, and new block header further include the public key associated with the agreed proposal number.

23. The system of claim 13, wherein

the querying module of the processing server is further configured to sort the generated proposal number and the accepted proposal number included in each response message based on the respective numeric value, and

the agreed proposal number is identified based on the sorting and a predetermined criteria.

24. The system of claim 23, wherein the predetermined criteria is selecting the highest numeric value.