trusted participants may ensure that new blocks are reliable and secure, while enabling the blocks to be suitably verified for inclusion in a blockchain, while also requiring significantly less computational power. In addition, by utilizing only trusted entities, the participant pool may be limited, which may decrease the amount of energy wasted to produce new blocks for the blockchain. Thus, there is a need for a technical solution that utilizes a trusted pool of participants and digital signatures for the signing of blockchain transactions.

SUMMARY

The present disclosure provides a description of systems and methods for using digital signatures for signing blockchain transactions.

In one aspect, this disclosure provides a method for using digital signatures for signing blockchain transactions which includes: generating, by a generation module of a processing server, a domain key pair comprising a domain private key and a domain public key, wherein the domain public key is signed after generation; receiving, by a receiving device of the processing server, a plurality of member public keys; signing, by a signing module of the processing server, each member public key of the plurality of member public keys using the domain private key; receiving, by the receiving device of the processing server, a transaction block from a specific member of the blockchain network; electronically transmitting, by the transmitting device of the processing server, each signed member public key to one or more members of the blockchain network; receiving, by the receiving device of the processing server, a new transaction block and a signed second hash value from the specific member of the blockchain network; signing, by the signing module of the processing server, the received new transaction block using the domain private key; and electronically transmitting, by the transmitting device of the processing server, the signed new transaction block for validation of the blockchain transactions by a member of the blockchain network.

In one example, another method for using digital signatures for signing blockchain transactions includes: storing, in a memory of a processing server, a blockchain, wherein the blockchain includes a plurality of transaction blocks, each transaction block including at least a plurality of blockchain transaction values; generating, by a generation module of the processing server, a member key pair comprising a member private key and a member public key; electronically

transmitting, by a transmitting device of the processing server, the generated member public key to a signing

authority associated with a blockchain network; receiving, by a receiving device of the processing server, a plurality of blockchain transaction values comprising a new transaction block; hashing, by a hashing module of the processing server; a first hash value via application of one or more hashing algorithms to a specific block of the plurality of transaction blocks included in the blockchain; generating, by the generation module of the processing server, a second hash value, wherein the second hash value corresponds to the first hash value; signing, by a signing module of the processing server, the generated second hash value using the generated member private key; and electronically transmitting, by the transmitting device of the processing server, the new transaction block and signed second hash value to the signing authority.

In another aspect, this disclosure provides a system for using digital signatures for signing blockchain transactions which includes: a transmitting device of a processing server; a generation module of the processing server configured to generate a domain key pair comprising a domain private key and a domain public key, wherein the domain public key is signed after generation; a receiving device of the processing server configured to receive a plurality of member public keys; and a signing module of the processing server configured to sign each member public key of the plurality of member public keys using the domain private key, wherein the receiving device of the processing server is further configured to receive a transaction block from a specific member of the blockchain network, the transmitting device of the processing server is further configured to electronically transmit each signed member public key to one or more members of the blockchain network, the receiving device of the processing server is further configured to receive a new transaction block and a signed second hash value from the specific member of the blockchain network, the signing module of the processing server is further configured to sign the received new transaction block using the domain private key, and the transmitting device of the processing server is further configured to electronically transmit the signed new transaction block for validation of the blockchain transactions by a member of the blockchain network.

In another example, another system for using digital signatures for signing blockchain transactions includes: a signing module of a processing server; a memory of the processing server configured to store a blockchain, wherein the blockchain includes a plurality of transaction blocks, each transaction block including

at least a plurality of blockchain transaction values; a generation module of the processing server