

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.

According to an aspect, there is a method for using digital signatures for signing blockchain transactions, comprising:

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, wherein each member public key is received from an associated member of a blockchain network and is a public key in a key pair comprising the member public key and a member private key corresponding to the associated member;

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, wherein the transaction block includes a plurality of blockchain transaction values and a hash signed using the member private key corresponding to the specific member;

signing, by the signing module of the processing server, the received transaction block using the domain private key;

electronically transmitting, by a transmitting device of the processing server, the signed transaction block;

electronically transmitting, by the transmitting device of the processing server, each signed member public key to one or more members of the blockchain network;

5 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

10 electronically transmitting, by the transmitting device of the processing server, the signed new transaction block for validation by a member of the blockchain network.

According to an aspect, there is a method for signing blockchain transactions, comprising:

15 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;

20 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;

25 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;

30 signing, by a signing module of the processing server, the generated second hash value using the generated member private key;

electronically transmitting, by the transmitting device of the processing server, the new transaction block and signed second hash value to the signing authority;

5 receiving, by the receiving device of the processing server, a signed transaction block and signed domain public key from the signing authority, wherein the signed transaction block includes the new transaction block and signed second hash value;

applying the member public key to the signed second hash value to yield the second hash value; and

10 validating the yielded second hash value as corresponding to the generated second hash value to validate the signed transaction block for addition to the blockchain.

According to an aspect, there is a system for using digital signatures for signing blockchain transactions, comprising:

15 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;

20 a receiving device of the processing server configured to receive a plurality of member public keys, wherein each member public key is received from an associated member of a blockchain network and is a public key in a key pair comprising the member public key and a member private key corresponding to the associated member; and

25 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, wherein the transaction block includes a plurality of blockchain transaction values and
30 a hash signed using the member private key corresponding to the specific member,

the signing module of the processing server is further configured to sign the received transaction block using the domain private key,

the transmitting device of the processing server is further configured to electronically transmit the signed transaction block, and

electronically transmit each signed member public key to one or more members of the blockchain network,

5 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

10 the transmitting device of the processing server is further configured to electronically transmit the signed new transaction block for validation by a member of the blockchain network.

According to an aspect, there is a system for using digital signatures for signing blockchain transaction, comprising:

15 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;

20 a generation module of the processing server configured to generate a member key pair comprising a member private key and a member public key;

a transmitting device of the processing server configured to electronically transmit the generated member public key to a signing authority associated with a blockchain network;

25 a receiving device of the processing server configured to receive a plurality of blockchain transaction values comprising a new transaction block; and

a hashing module of the processing server configured to generate 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, wherein

30 the generation module of the processing server is further configured to generate a second hash value, wherein the second hash value corresponds to the first hash value,

the signing module of the processing server is configured to sign the generated second hash value using the generated member private key, and

the transmitting device of the processing server is configured to electronically transmit the new transaction block and signed second hash value to the signing authority.

5 A method for using digital signatures for signing blockchain transactions 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, wherein each member public
10 key is received from an associated member of a blockchain network and is a public key in a key pair comprising the member public key and a member private key corresponding to the associated member; 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
15 server, a transaction block from a specific member of the blockchain network, wherein the transaction block includes a plurality of blockchain transaction values and a hash signed using the member private key corresponding to the specific member; signing, by the signing module of the processing server, the received transaction block using the domain private key; and electronically transmitting, by a transmitting device
20 of the processing server, the signed transaction block.

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
25 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

What is claimed is:

1. A method for using digital signatures for signing blockchain transactions, comprising:
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, wherein each member public key is received from an associated member of a blockchain network and is a public key in a key pair comprising the member public key and a member private key corresponding to the associated member;
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, wherein the transaction block includes a plurality of blockchain transaction values and a hash signed using the member private key corresponding to the specific member;
signing, by the signing module of the processing server, the received transaction block using the domain private key;
electronically transmitting, by a transmitting device of the processing server, the signed transaction block;
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 by a member of the blockchain network.
2. The method of claim 1, wherein the domain public key is signed by a public authority.

3. The method of claim 1, wherein the domain public key is signed by the signing module of the processing server.

4. The method of claim 1, further comprising:

receiving, by the receiving device of the processing server, authentication information from each member of the blockchain network; and

authenticating, by an authentication module of the processing server, each member of the blockchain network using the received authentication information prior to signing the associated member public key.

5. A method for using digital signatures for signing blockchain transactions, comprising:

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;

electronically transmitting, by the transmitting device of the processing server, the new transaction block and signed second hash value to the signing authority;

receiving, by the receiving device of the processing server, a signed transaction block and signed domain public key from the signing authority, wherein the signed transaction block includes the new transaction block and signed second hash value;

applying the member public key to the signed second hash value to yield the second hash value; and
validating the yielded second hash value as corresponding to the generated second hash value to validate the signed transaction block for addition to the blockchain.

6. The method of claim 5, wherein the second hash value is generated via application of the one or more hashing algorithms to the received new transaction block.

7. The method of claim 5, further comprising:
electronically transmitting, by the transmitting device of the processing server,
authentication information to the signing authority.

8. The method of claim 5,
wherein the signed transaction block is signed using a domain private key corresponding to the signed domain public key; and the method further comprises:
validating, by a validation module of the processing server, the signed transaction block using the member public key and signed domain public key.

9. The method of claim 8, wherein validating the signed transaction block includes:
applying the signed domain public key to the signed transaction block to yield the new transaction block and signed second hash value.

10. A system for using digital signatures for signing blockchain transactions, comprising:
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, wherein each member public key is received from an associated member of a blockchain network and is a public key in a key pair comprising the member public key and a member private key corresponding to the associated member; 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, wherein the transaction block includes a plurality of blockchain transaction values and a hash signed using the member private key corresponding to the specific member,

the signing module of the processing server is further configured to sign the received transaction block using the domain private key,

the transmitting device of the processing server is further configured to electronically transmit the signed transaction block, and

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 by a member of the blockchain network.

11. The system of claim 10, wherein the domain public key is signed by a public authority.

12. The system of claim 10, wherein the domain public key is signed by the signing module of the processing server.

13. The system of claim 10, further comprising:

an authentication module of the processing server, wherein

the receiving device of the processing server is further configured to receive authentication information from each member of the blockchain network; and

the authentication module of the processing server is configured to authenticate each member of the blockchain network using the received authentication information prior to signing the associated member public key.

14. A system for using digital signatures for signing blockchain transactions, comprising:
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 configured to generate a member key pair comprising a member private key and a member public key;
a transmitting device of the processing server configured to electronically transmit the generated member public key to a signing authority associated with a blockchain network;
a receiving device of the processing server configured to receive a plurality of blockchain transaction values comprising a new transaction block; and
a hashing module of the processing server configured to generate 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, wherein
the generation module of the processing server is further configured to generate a second hash value, wherein the second hash value corresponds to the first hash value,
the signing module of the processing server is configured to sign the generated second hash value using the generated member private key, and
the transmitting device of the processing server is configured to electronically transmit the new transaction block and signed second hash value to the signing authority.

15. The system of claim 14, wherein the second hash value is generated via application of the one or more hashing algorithms to the received new transaction block.

16. The system of claim 14, wherein the transmitting device of the processing server is further configured to electronically transmit authentication information to the signing authority.

17. The system of claim 14,
wherein
the signed transaction is signed using a domain private key corresponding to the signed domain public key, and

the validation module of the processing server is configured to validate the signed transaction block using the member public key and signed domain public key.

18. The system of claim 17, wherein validating the signed transaction block includes: applying the signed domain public key to the signed transaction block to yield the new transaction block and signed second hash value.