

Claims

1. A computer-implemented method of performing a knowledge proof using a set of transactions for recording in a blockchain maintained in a blockchain network, the method comprising:

determining, by a challenger, a competition challenge, the competition challenge having a challenge solution derivable therefrom;

at a challenger device, determining a signature challenge for the competition challenge; and

submitting, to the blockchain network, the signature challenge in at least one challenge transaction for recording in the blockchain;

wherein the competition challenge is communicated to a plurality of competing challengees, without communicating the challenge solution directly, thereby causing the competing challengees to compete to derive, from the competition challenge, independent instances of the challenge solution, wherein the independent instances of the challenge solution are the same and equal to the challenge solution;

wherein a first of the challengees to successfully derive an independent instance of the challenge solution uses the independent instance of the challenge solution or data derived from the independent instance of the challenge solution as a secret challengee key to sign at least one message at a challengee device, and thereby generate at least one transaction signature, and submits the at least one transaction signature and the at least one message to the blockchain network in at least one proof transaction, thereby causing a node of the blockchain network to determine whether the at least one transaction signature satisfies the signature challenge.

2. The method of claim 1, wherein the signature challenge comprises public signature-verification data, wherein the challenger determines the challenge solution and uses data of the challenge solution as a secret challenger key to generate the public signature-verification data, whereby the node is caused to verify the transaction signature based on the message and the public signature-verification data.

3. The method of claim 1 or 2, wherein the transaction signature is generated using an Elliptic Curve Digital Signature Algorithm, ECDSA.

4. The method of claim 2 and 3, wherein the secret challenger key and the secret challengee key are used as ephemeral keys, the public signature-verification data being published r-part data derived from the secret challengee key, wherein the node determines whether the at least one transaction signature satisfies the signature challenge by applying a signature verification function to: (i) an s-part of the transaction signature, and (ii) one of:
 - (iia) an r-part of the transaction signature, and in that event the node is further caused to check that the published r-part data matches the r-part of the transaction signature, or
 - (iib) a published r-part of the published r-part data of the at least one challenge transaction.

5. The method of claim 4, wherein the published r-part data comprises a published r-part hash, and the node verifies the transaction signature by:
 - applying the signature verification function to the r-part and the s-part of the transaction signature,
 - computing a transaction r-part hash based on the r-part of the transaction signature,
 - and
 - determining whether the transaction r-part hash matches the published r-part hash.

6. The method of claim 4 or 5, wherein the transaction signature is verified using a public key identified by the at least one proof transaction but which is not specified by the at least one challenge transaction, whereby any private key may be used to generate at least one transaction signature which satisfies the signature challenge.

7. The method of any of claims 3 to 5, wherein the at least one proof transaction comprises a second transaction signature, wherein the transaction signature and the second transaction signature are generated using a common private key, but the second transaction signature uses a different ephemeral key.

8. The method of claim 2 or claim 3 when dependent on claim 2, wherein the secret challenger key and the secret challengee key are used as private keys, the public signature-verification data being published public key data derived from the secret challengee key, wherein the node verifies the transaction signature by applying a signature verification function to: (i) the transaction signature, and (ii) one of:

(iia) a public key associated with the transaction signature, and in that event the node is further caused to determine whether the associated public key matches the published public key data, or

(ii) a published public key of the published public key data of the at least one challenge transaction.

9. The method of claim 8, wherein the published public key data comprises a published public key hash, and the node verifies the transaction signature by:

applying the signature verification function to the transaction signature and the public key associated with the transaction signature,

computing a transaction public key hash based on the public key associated with the transaction signature, and

determining whether the transaction public key hash matches the published public key hash.

10. The method of any preceding claim, wherein a hash of the challenge solution is used as the secret challenger key, and a hash of the independent instance of the challenge solution is used as the secret challengee key.

11. The method of any preceding claim, wherein the competition challenge is communicated to the competing challengees via one or more side channels independent of the blockchain network.

12. The method of any of claims 1 to 11, wherein the at least one challenge transaction has the effect of communicating the competition challenge to the competing challengees.

13. A computer-implemented method of performing a knowledge proof using a set of transactions for recording in a blockchain maintained in a blockchain network, the method comprising:

receiving, by a challengee, a competition challenge, wherein the competition challenge has a derivable challenge solution but the challenge solution is not communicated to the challengee directly, wherein the challengee competes with one or more other challengees to derive an independent instance of the challenge solution from the competition

challenge, wherein the independent instances of the challenge solution are the same and equal to the challenge solution; and

wherein, upon the challengee successfully deriving the independent instance of the challenge solution before any of the other one or more challengees, the challengee uses the independent instance of the challenge solution or data derived from the independent instance of the challenge solution as a secret challengee key to sign at least one message at a challengee device, and thereby generate at least one transaction signature, and submits the at least one transaction signature and the at least one message to the blockchain network in at least one proof transaction, thereby causing a node of the blockchain network to determine whether the at least one transaction signature satisfies a signature challenge of a challenge transaction indicated by the at least one proof transaction.

14. The method of claim 13, wherein the transaction signature is generated using an Elliptic Curve Digital Signature Algorithm, ECDSA, the challengee key being an ephemeral key used in conjunction with a private key to generate the transaction signature, wherein the private key is freely determined by the challengee, without being specified by the challenge transaction.

15. The method of claim 14, wherein the transaction signature consists only of an s-part.

16. The method of claim 14, wherein the transaction signature comprises an s-part and an r-part.

17. The method of claim 1, wherein the challenge solution is unknown to the challenger when determining the signature challenge.