

Claims

1. A computer-implemented method of recording, in one or more blockchain transactions, contributions to a work by contributors having respective levels in a defined hierarchy, in which one or more lower-level contributors provide, to a higher-level contributor, one or more lower-level contributions respectively, and the higher-level contributor provides a higher-level contribution responsive to one or more lower-level contributions, the method comprising:
- at computer equipment of the higher-level contributor, creating or modifying a higher-level contributor transaction to evidence the higher-level contribution, the created or modified higher-level contributor transaction comprising:
- one or more inputs comprising:
- one or more pointers to one or more spendable outputs of one or more lower-level contributor transactions, the one or more lower-level contributor transactions containing one or more lower-level contribution commitments evidencing the one or more lower-level contributions respectively, and
- one or more transaction signatures of the higher-level contributor satisfying one or more signature challenges of the one or more spendable outputs,
- wherein the higher-level contributor transaction contains a higher-level contribution commitment computed from the higher-level contribution, wherein the one or more pointers and the contribution commitments represent the relationship between the higher-level contributor and the one or more lower-level contributors within the defined hierarchy, and the one or more transaction signatures prove that relationship.
2. The method of claim 1, wherein the one or more lower-level contributors comprise first and second lower-level contributors, the one or more lower-level contributions comprising first and second lower-level contributions of the first and second lower-level contributors respectively, the one or more lower-level contribution commitments comprising first and second lower-level contribution commitments evidencing the first and second lower-level contributions respectively.

3. The method of claim 1 or 2, wherein the higher-level contributor transaction contains one or more proofs of receipt of the one or more lower-level contributions.
4. The method of claims 2 and, wherein the one or more proofs of receipt comprise:
5 a first proof of receipt of the first lower-level contribution, and
a second proof of receipt of the second lower-level contribution.
5. The method of claim 3 or 4, wherein the one or more proofs of receipt are contained in the one or more inputs and satisfy, respectively, one or more proof-of-receipt challenges
10 of the one or more spendable outputs of the one or more lower-level contributor transactions.
6. The method of any preceding claim, wherein the higher-level contributor transaction contains a proof-of-receipt challenge for the higher-level contribution.
15
7. The method of any preceding claim, wherein the higher-level contributor transaction contains a transaction signature challenge for a receiving entity.
8. The method of claim 7, wherein the receiving entity is an even higher-level
20 contributor in the hierarchy, the higher-level contributor being an intermediate contributor between the lower-level contributors and the even higher-level contributor.
9. The method of any preceding claim, wherein the higher-level contributor transaction contains a discretionary signature generated by applying a signature function to a private
25 key of the higher-level contributor and a proof of the higher-level contribution, the proof of the higher-level contribution being the higher level contribution or a hash or other function thereof, wherein the proof of the higher-level contribution is not contained in the higher-level contributor transaction.
- 30 10. The method of any preceding claim, wherein the contribution commitments are contribution hashes.

11. The method of claims 9 and 10, wherein the higher-level contribution hash is a hash of the proof of the higher-level contribution.

12. The method of claim 11, wherein the proof of the higher-level contribution is the higher-level contribution and the higher-level contribution hash is a single hash of the higher-level contribution; or

wherein the proof of the higher-level contribution is a single hash of the higher-level contribution and the higher-level contribution hash is a double hash of the higher-level contribution.

13. The method of any of claims 6 to 12, wherein the proof-of-receipt challenge, the transaction signature challenge for the receiving entity and/or the discretionary signature are contained in one or more outputs of the higher-level contributor transaction.

14. The method of claim 13 when dependent on claims 6, 7 and 9, wherein at least the proof-of-receipt challenge and the transaction signature challenge are comprised in an output of the one or more outputs, which is spendable independently of the discretionary signature.

15. The method any preceding claim, wherein the one or more outputs comprise:
a summary hash computed by hashing a concatenated string comprising a single or multi-hash of the first lower-level contribution and a single or multi-hash of the second lower-level contribution, the spendable output being spendable independently of the summary hash.

16. A computer-implemented method of recording, in one or more blockchain transactions, contributions to a work by contributors having respective levels in a defined hierarchy, in which first and second lower-level contributors provide, to an intermediate-level contributor, first and second lower-level contributions respectively, and the intermediate-level contributor provides, to a higher-level contributor, an intermediate-level contribution responsive to the first and second lower-level contributions, the method comprising:

at computer equipment of the intermediate-level contributor, creating or modifying a blockchain transaction, the created or modified blockchain transaction comprising:

one or more inputs comprising:

- a first proof of receipt of the first lower-level contribution,
- 5 a second proof of receipt of the second lower-level contribution, and
- a transaction signature of the intermediate-level contributor;

one or more outputs comprising:

- a proof-of-receipt challenge for the intermediate-level contribution,
- a transaction signature challenge for the higher-level contributor, and
- 10 a discretionary signature;

wherein the discretionary signature is generated by applying a signature function to a private key of the intermediate-level contributor and the intermediate-level contribution or a hash thereof; and

15 wherein at least the proof-of-receipt challenge and the transaction signature challenge are comprised in an output of the one or more outputs, which is spendable independently of the discretionary signature.

17. The method claim 16, wherein the one or more outputs comprise:

20 a summary hash computed by hashing a concatenated string comprising a single or multi-hash of the first lower-level contribution and a single or multi-hash of the second lower-level contribution, the spendable output being spendable independently of the summary hash.

18. The method of claim 16 or 17, in which a second intermediate-level contributor
25 provides a second intermediate-level contribution to the higher-level contributor;

wherein the one or more inputs of the blockchain transaction further comprise:

- a third proof of receipt of a third lower-level contribution,
- a transaction signature of the second intermediate-level contributor;

wherein the one or more outputs further comprise:

30 a proof-of-receipt challenge for the second intermediate-level contribution,
and
a second discretionary signature;

wherein at least the challenge for the second intermediate-level contribution is comprised in said spendable output of the one or more outputs or another spendable output of the one or more outputs;

5 wherein the second discretionary signature is generated by applying a signature function to a single or multi-hash of the second intermediate-level contribution and said private key or another private key of the intermediate-level contributor.

19. The method of claim 18, wherein the one or more outputs comprise a second summary hash, wherein the secondary summary hash is computed by hashing a preimage,
10 the preimage comprising a single or multi-hash of the third lower-level contribution.

20. The method of claim 19, wherein the one or more inputs of the blockchain transaction further comprise:

a fourth proof of receipt of a fourth lower-level contribution;
15 wherein the preimage hashed to compute the second summary hash is in the form of a second concatenated string comprising the single or multi-hash of the third lower-level contribution and a single or multi-hash of the fourth lower-level contribution.

21. The method of any preceding claim, wherein the discretionary signature is
20 comprised in one or more un-spendable outputs of the blockchain transaction.

22. The method of claim 21 when dependent on claim 17, wherein the one or more un-spendable outputs comprise the summary hash.

23. The method of claim 21 or 22, wherein the one or more un-spendable outputs also
25 comprise a single or multi-hash of the first lower-level contribution and a single or multi-hash of the second lower-level contribution.

24. The method of any of claims 16 to 20, wherein the discretionary signature is
30 comprised in the spendable output, the transaction signature challenge being a functional operand of a multi-signature check opcode and the discretionary signature being a dummy operand of the multi-signature check opcode.

25. The method of claim 24 when dependent on claim 17, wherein the summary hash is comprised in the spendable output as a dummy operand of the multi-signature check opcode.

5

26. The method of claim 24 or 25, wherein a single or multi-hash of the first lower-level contribution and a single or multi-hash of the second lower-level contribution are also included as dummy operands of the multi-signature check opcode.

10 27. The method of any preceding claim comprising the step of transmitting the blockchain transaction to a node of a blockchain network for processing at the node for recording in a blockchain.

28. The method of any of claims 1 to 26, comprising the step of sending the blockchain transaction to an off-chain system for processing.

29. The method of any preceding claim, wherein the higher-level contributor creates a second blockchain transaction for spending the spendable output, the second blockchain transaction comprising:

20 one or more inputs comprising:

the proof of receipt of the intermediate-level contribution,

a transaction signature of the higher-level contributor,

one or more outputs comprising:

a further proof-of-receipt challenge for a higher-level contribution of the

25 higher-level contributor,

a transaction signature challenge for a recipient of the higher-level

contribution,

a further discretionary signature;

wherein the further discretionary signature is generated by applying a signature

30 function to a private key of the higher-level contributor and a single or multi-hash of the higher-level contribution.

30. The method of claim 29, wherein the one or more outputs of the second blockchain transaction comprise a further summary hash computed by hashing a further concatenated string, the further concatenated string comprising the summary hash and a single or multi-hash of the contribution of the higher-level contributor.

5

31. The method of claim 29 or 30, wherein the higher-level contribution is in the form of a final work responsive to all contributions received from all contributors within the hierarchy, the further proof-of-receipt challenge being satisfied by a proof of receipt of the final work.

10

32. A blockchain transaction embodied in transitory or non-transitory media, the blockchain transaction evidencing a contribution of a higher-level contributor in a defined contributor hierarchy, the blockchain transaction comprising:

one or more inputs comprising:

15

a first proof of receipt of a first lower-level contribution,
a second proof of receipt of a second lower-level contribution, and
a transaction signature of the intermediate-level contributor;

one or more outputs comprising:

20

a proof-of-receipt challenge for an intermediate-level contribution,
a transaction signature challenge for a receiving entity, and
a discretionary signature verifiable based on a private key of the higher-level contributor and a proof of the intermediate-level contribution, the proof of the higher-level contribution being the higher-level contribution or a hash thereof, wherein the blockchain transaction does not contain the proof of the higher-level contribution;

25

wherein at least the proof-of-receipt challenge and the transaction signature challenge are comprised in an output of the one or more outputs, which is spendable independently of the discretionary signature.