CLAIMS

1. A method for appending a block record to a blockchain stored on mining nodes of a network, the block record comprising payload data, a proof-of-work, and a unique identifier of a preceding block record of the blockchain, wherein the method comprises:

receiving a data package from an authority server, the data package comprising a plurality of datasets, wherein each of the plurality of datasets comprises signal information;

analysing the data package to convert the signal information of each dataset to a corresponding data output;

communicating the plurality of data outputs to the authority server, the plurality of data outputs for use in establishing a proof-of-work for appending a block record to the blockchain.

2. A method according to claim 1, further comprising:

receiving a signed token from the authority server;

creating a block record for the blockchain using the signed token as the proof-of-work; and

communicating the created block record to at least a mining node of the network.

3. A method according to claim 2, wherein the signed token comprises a signed hash of the analysed data package.

4. A method according to claim 2 or claim 3, wherein creating a block record for the blockchain includes:

consulting a version of the blockchain stored in one or more machine readable storage media to extract the unique identifier of the preceding block of the blockchain; and

retrieving payload data from a data pool of unprocessed payload data.

5. A method according to any preceding claim, wherein the signal information of each dataset is representative of a polynucleotide sequence; and

wherein converting the signal information of each dataset to a corresponding data output comprises converting the signal information of each dataset to a corresponding read, each read of the plurality of reads describing the respective polynucleotide sequence; and

wherein communicating the plurality of data outputs to the authority server comprises communicating the plurality of reads to the authority server.

6. A method according to claim 5, wherein the polynucleotide sequence comprises a deoxyribonucleic acid, DNA, sequence or a ribonucleic acid, RNA, sequence.

7. A method according to claim 5 or 6, wherein signal information representative of a polynucleotide sequence comprises raw data produced by a nanopore sequencer.

8. A method according to any of claims 5 to 7, wherein signal information representative of a polynucleotide sequence comprises current information corresponding to current flow through a nanopore and a polynucleotide translocating through the nanopore.

9. A method according to any preceding claim, wherein:

a unique identifier of a preceding block record of the blockchain comprises a hash of the preceding block record of the blockchain or a hash of a header of the preceding block of the blockchain; or

wherein the payload data comprises at least one of transaction data or a smart contract.

10. A method according to any preceding claim, wherein the receiving a data package from the authority server is in response to requesting a data package from the authority server.

11. A method according to any preceding claim, wherein the authority server is not a mining node of the network.

12. Computing apparatus for appending a block record to a blockchain stored on mining nodes of a network, the block record comprising payload data, a proof-of-work, and a unique identifier of a preceding block of the blockchain, wherein the computing apparatus comprises:

one or more processors; and

one or more machine readable storage media having instructions stored thereon which, when processed by the one or more processors, cause the one or more processors to:

receive a data package from an authority server, the data package comprising a plurality of datasets, wherein each of the plurality of datasets comprises signal information;

analyse the data package to convert the signal information of each dataset to a corresponding data output; and

communicate the plurality of data outputs to the authority server, the plurality of data outputs for use in establishing a proof-of-work for appending a block record to the blockchain.

13. A method, the method performed by an authority server, the authority server trusted by mining nodes of a network to authenticate a block record of a blockchain, the method comprising:

communicating a first data package to a first mining node of the network, the first data package comprising a plurality of datasets, wherein each of the plurality of datasets comprises signal information for conversion to a data output;

receiving information containing a first plurality of data outputs from the first mining node, each data output of the first plurality of data outputs determined from the first data package analysed by the first mining node,;

verifying the first plurality of data outputs; and

in response to verifying the first plurality of data outputs, digitally signing a unique token to be used as proof-of-work in a block record of the blockchain.

14. A method according to claim 13, further comprising:

sending the signed token to the first mining node to be used as proof-of-work in the block record of the blockchain.

15. A method according to claim 13 or 14, wherein verifying the first plurality of data outputs comprises determining that a corroboration condition has been met.

16. A method according to claim 15, wherein determining that the corroboration condition has been met comprises determining that each data output of the first plurality of data outputs has been corroborated by a threshold number of further mining nodes of the network.

17. A method according to claim 16, wherein determining that each data output of the first plurality of data outputs has been corroborated by a threshold number of further mining nodes of the network comprises:

comparing the first plurality of data outputs with one or more further pluralities of data outputs, each of the one or more further pluralities of data outputs received from a corresponding further mining node of the network;

wherein the further pluralities of data outputs have been determined from further data packages analysed by the corresponding further mining nodes, the further data packages each containing a plurality of datasets each comprising signal information, one or more datasets overlapping with those comprised within the first data package.

18. A method according to any of claims 16 to 17, wherein determining that each data output of the first plurality of data outputs has been corroborated by a threshold number of further mining nodes of the network comprises determining that each data output of the first plurality of data outputs has been corroborated within a predefined error threshold by a threshold number of further mining nodes of the network.

19. A method according to any of claims 13-18, wherein receiving the information containing the first plurality of data outputs is in response to:

wherein communicating the data package to the first mining node is in response to receiving a request for a data package from the first mining node.

20. A method according to claim 19, further comprising, prior to communicating the first data package to the first mining mode:

receiving multiple pre-processed data items from multiple data sources;

dividing the multiple pre-processed data items into independently processable datasets;

packaging a selection of the independently processable datasets into a data package; and

storing metadata concerning which independently processable datasets are included in the data package.

21. A method according to any of claims 13 to 20, wherein the first data package analysed by the first mining node also comprises decoy datasets, and wherein verifying the first plurality

of data outputs includes checking decoy data outputs of the first plurality of data outputs against a local register of data outputs.

22. An authority server, the authority server trusted by mining nodes of a network to authenticate a block record of a blockchain, each mining node comprising computing apparatus for appending a block record to the blockchain, the authority server comprising:

one or more processors; and

one or more memory units, the memory units having instructions stored therein which, when processed by the one or more processors, cause the one or more processors to:

communicate a first data package to a first mining node of the network, the first data package comprising a plurality of datasets, wherein each of the plurality of datasets comprises signal information for conversion to a data output;

receive information containing a first plurality of data outputs from the first mining node, each data output of the first plurality of data outputs determined from the first data package analysed by the first mining node,;

verify the first plurality of data outputs; and

in response to verifying the first plurality of reads, digitally sign a unique token to be used as proof-of-work in a block record of the blockchain.

23. A system for processing signal information as proof-of-work for appending a block record to a blockchain, the system comprising:

an authority server, the authority server comprising one or more processors; and

a network of mining nodes, wherein each mining node comprises one or more processors; and

wherein a mining node is configured to:

receive a data package from the authority server, the data package comprising a plurality of datasets, wherein each of the plurality of datasets comprises signal information;

analyse the data package to convert the signal information of each dataset to a corresponding data output;

communicate the plurality of data outputs to the authority server;

receive a signed token from the authority server;

create a block record for the blockchain using the signed token as the proof-of-work; and

communicate the created block record to at least a second mining node of the network; and

wherein the authority server is configured to:

receive information containing the plurality of data outputs from the mining node;

verify the plurality of data outputs;

in response to verifying the plurality of data outputs, digitally sign a unique token; and

send the signed token to the mining node to be used as proof-of-work in a block record of the blockchain.

24. Computing apparatus according to claim 12, further comprising

one or more machine readable storage media having stored thereon:

a first set of instructions for processing a data package received from the authority server, the first set of instructions requiring an encryption key; and

a second set of instructions which, when processed by the one or more processors, implement the steps of:

receiving a data package from the authority server, the data package comprising an encryption key and a plurality of datasets, wherein each of the plurality of datasets comprises signal information;

processing the first set of instructions using the received encryption key, to convert the signal information of each dataset to a corresponding encrypted data output; and

communicating the plurality of encrypted data outputs to the authority server, the plurality of encrypted data outputs for use in establishing a proof-of-work for appending a block record to the blockchain.

25. Computing apparatus according to claim 24, the computing apparatus further configured to:

receive a signed token from the authority server;

create a block record for the blockchain using the signed token as the proof-of-work; and

communicate the created block record to at least a mining node of the network.

26. Computing apparatus according to claim 25, wherein the signed token comprises a signed hash of the analysed data package or a signed hash of the encrypted data outputs.

27. Computing apparatus according to claim 24, wherein:

a unique identifier of a preceding block record of the blockchain comprises a hash of the preceding block record of the blockchain or a hash of a header of the preceding block of the blockchain; or

wherein the payload data comprises at least one of transaction data or a smart contract.

28. Computing apparatus according to any of claims 24 to 27, wherein the receiving a data package from the authority server is in response to requesting a data package from the authority server.

29. Computing apparatus according to any of claims 24 to 28, wherein the authority server is not a mining node of the network.

30. A method according to any of claims 1 and 2, the method for performance by a mining node having computer-readable instructions to process the data package received from the authority server, the instructions requiring an encryption key, wherein the method comprises:

receiving the data package from the authority server, the data package comprising an encryption key and the plurality of datasets;

using the received encryption key, performing the computer-readable instructions to convert the signal information of each dataset to a corresponding encrypted data output; and

communicating the plurality of data outputs to the authority server, the plurality of data outputs for use in establishing a proof-of-work for appending a block record to the blockchain.

31. A computer readable medium having instructions stored thereon, which when executed by a processor, causes the processor to implement a method according to any of claims 1 to 11 and 30.

32. A method according to claim 20, the method further comprising:

generating an encryption key and corresponding decryption key;

and when packaging a selection of the independently processable datasets into a data package also package the encryption key into said data package, the independently processable datasets of the data package being from multiple data sources; the method then comprising;

communicating the data package to a mining node to convert the signal information of each dataset to a corresponding encrypted data output;

receiving information containing a plurality of encrypted data outputs; and

decrypting the encrypted data outputs using the generated decryption key.

33. A method according to claim 32, further comprising:

verifying the decrypted data outputs; and

in response to verifying the decrypted data outputs, digitally signing a unique token to be used as proof-of-work in a block record of the blockchain.c

34. A method according to any of claims 32 to 33, further comprising communicating the verified decrypted outputs to authorised users.

35. A method according any of claims 32 to 34, wherein the signal information of at least one of the data items comprises raw data produced by a nanopore sequencer, and wherein the signed token includes an identifier of the nanopore sequencer.

36. A method according to any of claims 32 to 35, wherein the encryption key comprises a distinct encryption key for each dataset of the data package.

37. A method according to any of claims 32 to 36, wherein the signal information of at least some of the data items is representative of a polynucleotide sequence; and wherein the decrypted data outputs comprise corresponding sections of the polynucleotide sequences.

38. A method according to claim 37, where the polynucleotide sequence comprises a deoxyribonucleic acid, DNA, sequence or a ribonucleic acid, RNA, sequence.

39. A method according to claims 37 or claim 38, wherein signal information representative of a polynucleotide sequence comprises raw data produced by a nanopore sequencer.

40. A method according to claim 39 further comprises storing an identifier of the nanopore sequencer.

41. A method according to any of claims 37 to 40, wherein the encrypted data outputs comprise sequences of letters, and wherein decrypting the encrypted data outputs comprises substituting the letters for IUPAC nucleotide codes.

42. A method according to any of claims 32 to 41, wherein the encrypted data outputs include decoy features and wherein decrypting the encrypted data outputs comprises removing the decoy features.

43. A method according to any of claims 32 to 42, wherein receiving data items from a data source comprises continuously receiving data items from that data source.

44. A method according to any of claims 32 to 43, further comprising storing metadata concerning which independently processable datasets are included in the data package.

45. A computer readable medium having instructions stored thereon, which when executed by a processor, causes the processor to implement a method according to any of claims 13 to 21 and 32 to 44.

46. An authority server according to claim 22, wherein the memory units having instructions stored therein which, when processed by the one or more processors, cause the one or more processors to, prior to the authority server receiving information containing a first plurality of data outputs,

divide received data items into independently processable datasets, the data items received from multiple data sources, the data items comprising signal information;

generate an encryption key and corresponding decryption key;

collect a selection of the independently processable datasets and the encryption key into a data package, the independently processable datasets of the data package being from multiple data sources;

communicate the data package to a mining node of a blockchain mining network to convert the signal information of each dataset to a corresponding encrypted data output; then

receive and process received information, the received information containing a plurality of encrypted data outputs, wherein processing the received information comprises decrypting the encrypted data outputs using the generated decryption key.