Claims

1. An Intellectual Property (IP) blockchain method comprising:

processing a IP file with a hash function to obtain an IP digest by a platform system;

determining a previous block digest from a previous IP blockchain by the platform system; ~~and~~

appending the previous block digest and an IP reference dataset to the IP digest to obtain an IP datablock by the platform system, the IP reference dataset being associated with the IP file; and

one of encrypting the IP file for storage in an IP repository and digitally shredding the IP file in response to one of the IP datablock being generated, the encrypted IP file being associated with the IP datablock, the IP reference dataset comprising indication of storage of the IP file in an IP repository,

wherein the previous IP blockchain is updatable with the obtained IP datablock to obtain an updated IP blockchain.

2. The method as in claim 1, further comprising:

updating the previous IP blockchain with the obtained IP datablock to obtain the updated IP blockchain.

3. The method as in claim 2, further comprising:

validating the IP datablock against a predefined data structure prior to updating the previous IP blockchain with the obtained IP datablock.

4. The method as in claim 1, the IP reference dataset comprising at least one of:

counter value indicative of ordinal position of the IP datablock amongst a plurality of datablocks constituting the previous IP blockchain;

version number of at least one of protocol and software employed by the platform system for performing the IP blockchain method;

identity of at least one owner of the IP file;

title of the IP file; and

at least one of date and time of creation of the IP datablock~~; and~~

~~indication of storage of the IP file in an IP repository~~.

5. The method as in claim 1, further comprising:

matching the IP datablock with a candidate IP digest for verifying validity of the candidate IP digest.

6. The method as in claim 5, further comprising:

processing a candidate IP file with the hash function to obtain the candidate IP digest.

7. The method as in claim 1, further comprising:

updating a ledger with at least one of the IP datablock and the updated IP blockchain in response to the previous IP blockchain being updated .

8. The method as in claim 7~~1~~, further comprising:

distributing the updated ledger to a plurality of distributed databases in data communication with the platform system in response to the ledger being updated.

~~9. The method as in claim 1, further comprising:~~

~~encrypting the IP file for storage in an IP repository, the encrypted IP file being associated with the IP datablock.~~

9~~10~~. The method as in claim 1~~9~~, the IP file being encrypted by at least one of private key cryptography, public key cryptography or quantum cryptography.

~~11. The method as in claim 1, further comprising:~~

~~digitally shredding the IP file in response to one of the IP datablock being generated and the updated IP blockchain being obtained~~.

102. The method as in claim 1, the IP file containing matter relating to at least one of patents, registered designs, trademarks, copyrights, trade secrets, plant breed dataset, electronic masks and documented intellectual assets.

113. The method as in claim 1, the hash function being one of SHA1, SHA256, SHA3, BLAKE and BCRYPT.

124. A machine-readable medium having stored therein a plurality of programming instructions, which when executed, the instructions cause the machine to:

process a IP file with a hash function to obtain an IP digest;

determine a previous block digest from a previous IP blockchain; ~~and~~

append the previous block digest and an IP reference dataset to the IP digest to obtain an IP datablock, the IP reference dataset being associated with the IP file; and

one of encrypting the IP file for storage in an IP repository and digitally shredding the IP file in response to one of the IP datablock being generated, the encrypted IP file being associated with the IP datablock, the IP reference dataset comprising indication of storage of the IP file in an IP repository,

wherein the previous IP blockchain is updatable with the obtained IP datablock to obtain an updated IP blockchain.

135. The machine readable medium of claim 124, the plurality of programming instructions when executed, further cause the machine to:

update the previous IP blockchain with the obtained IP datablock to obtain the updated IP blockchain.

146. The machine readable medium of claim 135, the plurality of programming instructions when executed, further cause the machine to:

validate the IP datablock against a predefined data structure prior to updating the previous IP blockchain with the obtained IP datablock.

15~~7~~. The machine readable medium of claim 12~~4~~, the IP reference dataset comprising at least one of:

counter value indicative of ordinal position of the IP datablock amongst a plurality of datablocks constituting the previous IP blockchain;

version number of at least one of protocol and software employed by the machine;

identity of at least one owner of the IP file;

title of the IP file; and

at least one of date and time of creation of the IP datablock~~; and~~

~~indication of storage of the IP file in an IP repository~~.

16~~8~~. The machine readable medium of claim 12~~4~~, the plurality of programming instructions when executed, further cause the machine to:

match the IP datablock with a candidate IP digest for verifying validity of the candidate IP digest.

17~~9~~. The machine readable medium of claim 12~~4~~, the plurality of programming instructions when executed, further cause the machine to:

process a digital IP file with the hash function to obtain the candidate IP digest.

18~~20~~. The machine readable medium of claim 12~~4~~, the plurality of programming instructions when executed, further cause the machine to:

update a ledger with at least one of the IP datablock and the updated IP blockchain in response to the previous IP blockchain being updated; and

distribute the updated ledger to a plurality of distributed databases in data communication with the platform system in response to the ledger being updated.

19~~21~~. The machine readable medium of claim 12~~4~~, ~~the plurality of programming instructions when executed, further cause the machine to:~~

~~encrypt the IP file for storage in an IP repository, the encrypted IP file being associated with the IP datablock, and~~ the IP file being encrypted by at least one of private key cryptography, public key cryptography or quantum cryptography.

~~22. The machine readable medium of claim 14, the plurality of programming instructions when executed, further cause the machine to:~~

~~digitally shred the IP file in response to one of the IP datablock being generated and the updated IP blockchain being obtained.~~

20~~3~~. The machine readable medium of claim 1~~2~~4, the IP file containing matter relating to at least one of patents, registered designs, trademarks, copyrights, trade secrets, plant breed dataset, electronic masks and documented intellectual assets.

21~~24~~. The machine readable medium of claim 1~~2~~4, the hash function being one of SHA1, SHA256, SHA3, BLAKE and BCRYPT.

22~~5~~. An Intellectual Property (IP) blockchain system comprising:

a first database module for providing an IP file to be processed;

a second database module for providing auxiliary information dataset associated with the IP file, the auxiliary information dataset comprising identity of at least one owner of the IP file and title of the IP file;

a third database module for providing a previous IP blockchain; and

a controller module in data communication with the first database module, the second database module and a third database module, the controller module for:

processing the IP file with a hash function to obtain an IP digest;

determining a previous block digest from the previous IP blockchain;

appending the previous block digest and an IP reference dataset to the IP digest to obtain an IP datablock;

one of encrypting the IP file for storage in an IP repository and digitally shredding the IP file in response to one of the IP datablock being generated, the encrypted IP file being associated with the IP datablock, the IP reference dataset comprising indication of storage of the IP file in an IP

repository, the IP reference dataset comprising indication of storage of the IP file in an IP repository, and

updating the previous IP blockchain of the first database module with the obtained IP datablock,

wherein the IP reference dataset comprises at least one of counter value indicative of ordinal position of the IP datablock amongst a plurality of datablocks constituting the previous IP blockchain, version number of at least one of protocol and software employed by the platform system for performing the IP blockchain method, at least one of date and time of creation of the IP datablock, indication of storage of the IP file in an IP repository, the identity of at least one owner of the IP file, and the title of the IP file.