What Is Claimed Is:

1. A computer-implemented method for generating a privacy-preserving token, the method comprising:

calculating a privacy-preserving representation of a set of attributes associated with an asset, wherein calculating the privacy-preserving representation comprises calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes, wherein the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, and the set of attributes comprises a signature attribute associated with a value signed by an author of the asset;

generating a non-fungible token representing the asset, wherein the non-fungible token comprises an identifier and metadata associated with the identifier, wherein the metadata comprises the privacy-preserving representation of the set of attributes; and

recording the non-fungible token on a blockchain system.

2. A computer-implemented method for verifying validity of a signature attribute of an asset represented by a privacy-preserving token, wherein the token is a non-fungible token recorded on a blockchain system and comprises an identifier and metadata associated with the identifier, a privacy-preserving representation of a set of attributes associated with the asset is calculated by calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes and is recorded as the metadata of the token, the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, and the

set of attributes comprises a signature attribute associated with a value signed by an author of the asset, the method comprising:

generating a proof for proving that the value associated with the signature attribute is a valid signature signed by the author of the asset; and

providing the proof to a verifier to facilitate a verification of whether the value associated with the signature attribute is the valid signature signed by the author of the asset without revealing the value associated with the signature attribute.

3. A computer-implemented method for verifying validity of a signature attribute of an asset represented by a privacy-preserving token, wherein the token is a non-fungible token recorded on a blockchain system and comprises an identifier and metadata associated with the identifier, a privacy-preserving representation of a set of attributes associated with the asset is calculated by calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes and is recorded as the metadata of the token, the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, and the set of attributes comprises a signature attribute associated with a value signed by an author of the asset, the method comprising:

receiving a proof for proving that the value associated with the signature attribute is a valid signature signed by the author of the asset; and

verifying whether the value associated with the signature attribute is the valid signature signed by the author of the asset without knowing the value associated with the signature attribute.

4. The method of any preceding claim, wherein the privacy-preserving representation is calculated by calculating the Merkle tree root hash based on a cryptographic nonce.

5. The method of claim 4, wherein a hash corresponding to the cryptographic nonce is stored on a node of the Merkle tree.

6. The method of claim 2, further comprising:

generating the proof based on a particular leaf node that stores the hash corresponding to the value associated with the signature attribute and an authentication path of the particular leaf node.

7. The method of claim 2, further comprising:

identifying a particular leaf node that stores the hash corresponding to the value associated with the signature attribute;

identifying an authentication path of the particular leaf node;

obtaining one or more hashes stored in one or more nodes on the authentication path; and

generating the proof based on the one or more obtained hashes.

8. The method of claim 7, further comprising:

forming a public input based on a public key of the author of the asset, a token identifier, and the metadata of the token;

forming a secrete input based on the value associated with the signature attribute and the one or more obtained hashes; and

generating the proof as a zero-knowledge proof based on the public input and the secrete input.

9. The method of claim 8, wherein the zero-knowledge proof proves that the metadata of the token is calculated based on the value associated with the signature attribute and the one or more obtained hashes, and that a function provided on the blockchain system has been utilized to verify that the value associated with the signature attribute is the valid signature signed by the author.

10. The method of claim 9, wherein the function determines whether the value associated with the signature attribute is the valid signature signed by the author based on the public key of the author of the asset and the token identifier.

11. The method of any of claims 6 to 10, wherein the authentication path of the particular leaf node comprises siblings of all nodes on a path from the particular leaf node to a Merkle tree root.

12. A device for verifying validity of a signature attribute of an asset, comprising:

one or more processors; and

one or more computer-readable memories coupled to the one or more processors and having instructions stored thereon that are executable by the one or more processors to perform the method of any of claims 1 to 11.

13. An apparatus for verifying validity of a signature attribute of an asset, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 11.

14. A non-transitory computer-readable medium having stored therein instructions that, when executed by a processor of a device, cause the device to perform the method of any of claims 1 to 11.