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 a non-fungible token representing 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;

generating the 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 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 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, and the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, the method comprising:

identifying hashes stored on a plurality of nodes of the Merkle tree that can be utilized to calculate the Merkle tree root hash; and

providing the identified hashes stored on the plurality of nodes of the Merkle tree to a verifier, to facilitate a verification of the validity of the token without revealing the value associated with each attribute of the set of attributes.

3. A computer-implemented method for verifying validity of 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 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, and the value associated with each attribute of the set of attributes has a corresponding hash stored on a leaf node of the Merkle tree, the method comprising:

receiving hashes stored on a plurality of nodes of the Merkle tree that can be utilized to calculate the Merkle tree root hash;

calculating a root hash based on the hashes received;

obtaining the token recorded on the blockchain system; and

verifying the validity of the token based on the calculated root hash without knowing the value associated with each attribute of the set of attributes.

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 any preceding claim, wherein the hashes stored on the plurality of nodes of the Merkle tree that can be utilized to calculate the Merkle tree root hash comprise the hash stored on the leaf node of the Merkle tree that corresponds to the value associated with each attribute of the set of attributes.

7. The method of any preceding claim, wherein a smart contract is deployed in the blockchain system to verify the validity of the token.

8. The method of claim 3, wherein the verifying the validity of the token comprises:

comparing the calculated root hash based on the hashes received with the metadata of the token recorded on the blockchain system.

9. The method of claim 8, wherein the verifying the validity of the token further comprising:

accepting the token as valid in response to a determination that the calculated root hash matches the metadata of the token recorded on the blockchain system.

10. A device for processing a token, 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 9.

11. An apparatus for processing a token, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 9.

12. 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 9.