What Is Claimed Is:

1. A computer-implemented method for verifying an attribute value of a digital 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 digital asset is calculated as the metadata by calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes, 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:

generating a proof for proving that the metadata recorded on the blockchain system is calculated based on the value associated with a particular attribute of the set of attributes; and

providing the proof to a verifier to facilitate a verification of the value associated with the particular attribute without revealing the value associated with at least one other attribute of the set of attributes

wherein generating the proof comprises:

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

identifying an authentication path of the particular leaf node;

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

forming a secret input based on the one or more obtained hashes; and

generating the proof as a zero-knowledge proof based on the secret input.

2. A computer-implemented method for verifying an attribute value of a digital 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 digital asset is calculated as the metadata by calculating a Merkle tree root hash based on a value associated with each attribute of the set of attributes, 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 a proof for proving that the metadata recorded on the blockchain system is calculated based on the value associated with a particular attribute of the set of attributes;

obtaining the token recorded on the blockchain system; and

verifying whether the metadata of the token recorded on the blockchain system is calculated based on the value associated with the particular attribute without knowing the value associated with at least one other attribute of the set of attributes

wherein the proof is generated by:

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

identifying an authentication path of the particular leaf node;

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

forming a secret input based on the one or more obtained hashes; and

generating the proof as a zero-knowledge proof based on the secret input.

3. 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.

4. The method of claim 3, wherein a hash corresponding to the cryptographic nonce is stored on a node of the Merkle tree.

5. The method of any one of claims 1 and 2, 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.

6. A device for verifying an attribute value of a digital 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 5.

7. An apparatus for verifying an attribute value of a digital asset, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 5.

8. 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 5.