What Is Claimed Is:

1. 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 according to a function defined based on a value associated with each attribute of the set of attributes and is recorded as the metadata of the token, the method comprising:

generating a proof for proving that the token recorded on the blockchain system complies with a metadata schema defined for the token and the metadata of the token is calculated according to the function defined based on the value associated with each attribute of the set of attributes, wherein the function is further defined based on a cryptographic nonce when calculating the privacy-preserving representation; and

providing the proof 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.

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 according to a function defined based on a value associated with each attribute of the set of attributes and is recorded as the metadata of the token, the method comprising:

receiving a proof for proving that the token recorded on the blockchain system complies with a metadata schema defined for the token and the metadata of the token is calculated according to the function defined based on the value associated with

each attribute of the set of attributes, wherein the function is further defined based on a cryptographic nonce when calculating the privacy-preserving representation;

obtaining the token recorded on the blockchain system; and

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

3. The method of claim 1 or 2, wherein the function comprises a Merkle tree root hash function that calculates a Merkle tree root hash based on the value associated with each attribute of the set of attributes.

4. The method of claim 3, further comprising: storing on a leaf node of the Merkle tree a hash corresponding to the value associated with each attribute of the set of attributes.

5. The method of claim 4, further comprising: storing on a node of the Merkle tree a hash corresponding to the cryptographic nonce.

6. The method of claim 1 or 2, wherein the proof is a zero-knowledge proof.

7. The method of claim 1 or 2, wherein a smart contract is deployed in the blockchain system to verify the validity of the token.

8. 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 7.

9. An apparatus for processing a token, the apparatus comprising a plurality of modules for performing the method of any of claims 1 to 7.

10. 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 7.