

CLAIMS

1. A method of managing ownership data of a product including an electronic tag, the method comprising:
 - obtaining from the electronic tag:
 - a tag-specific identifier;
 - a signature that is generated based on the tag-specific identifier;
 - and
 - a product-specific datum;
 - comparing the signature and the product-specific datum with corresponding expected signature and product-specific datum for the product;
 - and
 - associating the product with a user in an ownership record if the obtained signature and product-specific datum match the expected signature and product-specific datum respectively.
2. A method of managing ownership data according to Claim 1, wherein product-specific datum comprises a unique product identifier.
3. A method of managing ownership data according to Claim 2, wherein the unique product identifier comprises an SKU and a running number.
4. A method of managing ownership data according to Claim 3, wherein the product-specific datum further comprises a random number.
5. A method of managing ownership data according to Claim 4, wherein the product-specific datum further comprises a UUID.
6. A method of managing ownership data according to Claim 1, wherein the product-specific datum from the electronic tag is obtained only after it is determined that there is a match between the obtained signature and the expected signature.

7. A method of managing ownership data according to Claim 6, wherein the tag-specific identifier, the signature, and the product-specific datum are obtained by a reader in data communication with the product; and the tag-specific identifier and the signature are obtained via a first communication session and the product-specific datum is obtained via a second communication session that is different from the first communication session.
8. A method of managing ownership data according to any one of Claims 1-7, wherein product-specific datum is an encrypted string.
9. A method of managing ownership data according to Claim 8, wherein the encrypted string is stored in a password-protected memory of the electronic tag; and the method further comprises providing a valid password to the electronic tag so as to be able to obtain the encrypted string from the password-protected memory.
10. A method of managing ownership data according to any one of Claims 1-9, wherein the ownership record comprises one of an ownership record in a centralized server and a token in a distributed ledger network.
11. A method of managing ownership data according to Claim 10, wherein the token is a non-fungible token.
12. A system for managing ownership data of a product including an electronic tag, comprising:
 - a centralized server that is operable to:
 - receive from the electronic tag:
 - a tag-specific identifier;
 - a signature that is generated based on the tag-specific identifier; and
 - a product-specific datum;
 - compare the received signature and product-specific datum with corresponding expected signature and product-specific datum for the product stored thereon; and

associate the product with a user in an ownership record on one of the centralized server and a distributed ledger network if the received signature and product-specific datum match the expected signature and product-specific datum for the product respectively.

13. A system for managing ownership data of a product according to Claim 12, wherein the product-specific datum comprises a unique product identifier.

14. A system for managing ownership data according to Claim 13, wherein the unique product identifier comprises an SKU and a running number.

15. A system for managing ownership data according to Claim 14, wherein the product-specific datum further comprises a random number.

16. A system for managing ownership data according to Claim 15, wherein the product-specific datum further comprises a UUID.

17. A system according to Claim 12, further comprising:
a distributed ledger network in data communication with the centralized server, the distributed ledger network comprising at least two nodes, the distributed ledger network operable to:
execute a smart contract to create a token to associate the product with the user.

18. A system according to Claim 17, further comprising:
at least one user device operable to:
obtain the tag-specific identifier, the signature, and the product-specific datum from the electronic tag; and
send the tag-specific identifier, the signature, and the product-specific datum to the centralized server.

19. A program storage device readable by a centralized server, tangibly embodying a program of instructions, executable by the centralized server to perform a method of managing ownership data of a product, the method comprising:

- receiving a tag-specific identifier, a signature that is generated based on the tag-specific identifier and a product-specific datum;

- comparing the signature and the product-specific datum with corresponding expected signature and product-specific datum for the product;
- and

- associating the product with a user in an ownership record if the obtained signature and product-specific datum match the expected signature and product-specific datum respectively.

20. A method of authenticating a product including an electronic tag, the method comprising:

- obtaining a tag-specific identifier from the electronic tag;

- obtaining a signature from the electronic tag, the signature being generated based on the tag-specific identifier;

- generating an expected signature from the obtained tag-specific identifier;

- comparing the obtained signature with the expected signature;

- providing the tag with a password if the obtained signature matches the expected signature;

- obtaining a product-specific datum from the electronic tag;

- comparing the obtained product-specific datum with an expected product-specific identifier for the product;

- determining that the product is authentic only if the read product-specific datum matches the expected product-specific datum.