CLAIMS

1. Method of securing a given original article of a batch of a plurality of original articles (A_1, A_2, A_3) against forgery or tampering, each original article of the batch having its own associated article data and corresponding article digital data (D_1, D_2, D_3), characterized by comprising the steps of:

for each original article of the batch, calculating by means of a one-way function an associated article digital signature (x_1, x_2, x_3) of its corresponding article digital data;

calculating a reference aggregated digital signature (B) corresponding to the batch of original articles from all the article digital signatures of the original articles of the batch by means of a one-way accumulator of said article digital signatures, and making available to a user the reference aggregated digital signature;

determining an article verification key (k_i) corresponding to the article digital signature of said given original article by means of a partial one-way accumulator of all the other article digital signatures used for calculating the reference aggregated digital signature, whereby a candidate article digital signature corresponds to that of an original article of the batch only if the reference aggregated digital signature is calculated from said candidate article digital signature and corresponding article verification key by means of the one-way function; and

applying on the given original article a corresponding machine readable security marking (110) including a representation of its associated article digital data and its corresponding article verification key, both included into the machine readable security marking via encoding,

thereby obtaining a marked original article of which article data is secured against forgery or tampering.

2. Method according to claim 1, wherein the reference aggregated digital signature associated with the batch of original articles is either published in a media accessible to the user, or stored in a searchable aggregated signature database accessible to the

user, or stored in a blockchain (260), or in a database secured by a blockchain, accessible to the user.

3. Method according to claim 2, wherein the marked original article further comprises aggregated signature access data marked thereto and containing information sufficient to access to the reference aggregated digital signature corresponding to the batch of original articles, said information being a link to an aggregated signature acquisition interface of, respectively, one of the following:
- the media wherein the reference aggregated digital signature is published, the media being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing article data, or a digital signature of said article data, obtained from a security marking of a marked original article, and send back a reference aggregated digital signature of associated batch;
- the searchable aggregated signature database wherein the reference aggregated digital signature is stored, the aggregated signature database being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing article data, or a digital signature of said article data, obtained from a security marking of a marked original article, and send back a reference aggregated digital signature of associated batch;
- the blockchain, respectively the database secured by the blockchain, wherein the time-stamped aggregated digital signature is stored, the blockchain, respectively the database secured by the blockchain, being accessible to the user via said aggregated signature acquisition interface operable to receive from the user an aggregated signature request containing article data, or a digital signature of said article data, obtained from a security marking of a marked original article, and send back a reference aggregated digital signature of associated batch.

4. Method according to any one of claims 1 to 3, wherein

a virtual article (A_v) is included into the batch of original articles, said virtual article having associated virtual article data and its corresponding virtual article digital data (D_v), and an associated virtual article digital signature (x_v) obtained by

means of the one-way function, said virtual article being not produced but only used for generating the associated virtual article digital signature from the corresponding virtual article digital data; and

the reference aggregated digital signature associated with said batch of original articles being calculated from all the article digital signatures of the original articles of the batch, including the virtual article digital signature, by means of the one-way accumulator.

5. Method according to any one of claims 1 to 4, wherein

the one-way function is a hash function (H) and an article digital signature of an original article is a sequence of a given plurality of bits of lower weights selected from the bits of a hash value of the corresponding article digital data.

6. Method according to any one of claims 1 to 5, wherein

additional article digital data corresponding to the article data associated with the marked original article are stored in a searchable information database (250) accessible to the user via an information database interface operable to receive from the user an information request containing article data, or corresponding digital signature data, obtained from a security marking of a marked original article, and send back corresponding additional article digital data.

7. Method according to any one of claims 1 to 6, wherein the marked original article further comprises a corresponding article data marking applied thereto, said article data marking including the corresponding article data associated with said marked original article.

8. Method according to any one of claims 1 to 7, wherein the article digital data of the marked original article includes reference physical characteristic digital data UPC of a corresponding unique physical characteristic of the marked original article, or of an associated object or individual.

9. Method according to claim 8, wherein the unique physical characteristic of the marked original article is that of a material-based security marking applied on the original article.

10. Method of verifying the authenticity of an article secured according to the method of any one of claims 1 to 9, or the conformity of a copy of such secured article with respect to the original one, characterized by comprising the steps of, upon viewing a test object being said article or said copy of the article:

acquiring a digital image of the security marking on the test object by means of an imager having an imaging unit, a CPU with a memory, and an image processing unit;

reading a representation of article digital data and of an associated article verification key on the acquired digital image of the security marking on the test object, and extracting respectively corresponding article digital data and article verification key from said read representation;

having stored in the memory a reference aggregated digital signature of a corresponding batch of articles, and having programmed in the CPU the one-way function and the one-way accumulator;

verifying that the extracted article digital data and associated article verification key indeed correspond to the stored reference aggregated digital signature by performing the steps of:

calculating a digital signature of the extracted article digital data with the one-way function;

calculating a candidate aggregated digital signature from the calculated digital signature of the extracted article digital data and the extracted article verification key with the one-way accumulator; and

checking that the obtained candidate aggregated digital signature matches the stored reference aggregated digital signature,

whereby, in case said aggregated digital signatures match, the article data on the test object is that of a genuine original article.

11. Method according to claim 10, wherein the article is secured by storing the reference aggregated digital signature associated with the batch of original articles in a searchable aggregated signature database accessible to the user according to the method of claim 2, and the imager is further equipped with a communication unit operable to send and receive back data via a communication link, comprising the steps of:

sending with the communication unit via the communication link a request to said aggregated signature database, and receiving back the reference aggregated digital signature associated with the batch of original articles; and

storing the received aggregated digital signature in the memory of the imager, which precede the steps recited in claim 10.

12. Method according to claim 10, wherein the article is secured according to the method of claim 3 and the imager is further equipped with a communication unit operable to send and receive back data via a communication link, comprising the steps of:

reading the aggregated signature access data marked on the test object with the imager;

sending with the communication unit via the communication link an aggregated signature request to said aggregated signature acquisition interface containing the article data, or a digital signature of said article data, obtained from the security marking on the test object, and receiving back a corresponding reference aggregated digital signature of an associated batch; and

storing the received aggregated digital signature in the memory of the imager, which precede the steps recited in claim 10.

13. Method according to any one of claims 10 to 12, wherein the article is secured according to the method of claim 6 and the imager is further equipped with communication means operable to send to the information database interface an information request containing article data, or corresponding digital signature data, obtained from the security marking on the test object, and receive back corresponding additional article digital data.

14. Method according to any one of claims 10 to 13, wherein the article is secured according to the method of claim 7, comprising the further steps of:

reading article data marked on an article data marking on the test object with the imager; and

checking that the article data read from the article data marking correspond with the article digital data extracted from the security marking on the test object.

15. Method according to any one of claims 10 to 14, wherein the article is secured according to the method of any one of claims 8 and 9 and the imager is further equipped with a sensor operable to detect a unique physical characteristic of a marked original article, or of an associated object or individual, and the CPU is programmed to extract corresponding unique physical characteristic digital data from a detection signal received from the sensor, the imager having stored in the memory reference physical characteristic digital data UPC corresponding to said unique physical characteristic of the marked original article, or of the associated object or individual, comprising the further steps of, upon viewing a subject being said article or said associated object or individual:

detecting with the sensor a unique physical characteristic of the subject and extracting corresponding candidate unique physical characteristic digital data UPC^c;

comparing the obtained candidate unique physical characteristic digital data UPC^c with the stored reference physical characteristic digital data UPC; and

in case the candidate unique physical characteristic digital data UPC^c is similar to the stored reference physical characteristic digital data UPC, within a given tolerance criterion, the subject is considered as genuine.

16. Marked article belonging to a batch of a plurality of original articles and secured against forgery or tampering according to the method of any one of claims 1 to 9, each original article of the batch having its own associated article data and corresponding article digital data, said batch having a corresponding reference aggregated digital signature, comprising:

a machine readable security marking applied on it and including a representation of its associated article digital data and a corresponding article verification key.

17. Marked article according to claim 16, wherein the article digital data of the marked article include reference physical characteristic digital data UPC of a corresponding unique physical characteristic of the marked article, or of an associated object or individual.

18. Marked article according to claim 17, wherein the unique physical characteristic of the marked article is that of a material-based security marking applied on the marked article.

19. System for verifying the authenticity of a marked original article secured according to the method of any one of claims 1 to 9, or the conformity of a copy of such article with respect to the original one, comprising an imager having an imaging unit, a CPU with a memory, and an image processing unit, the memory storing a reference aggregated digital signature of a corresponding batch of articles, and the one-way function and the one-way accumulator being programmed in the CPU, operable to:

acquire a digital image of the security marking on a test object being said article or said copy of the article;

read a representation of article digital data and of an associated article verification key on the acquired digital image of the security marking on the test object, and extract respectively corresponding article digital data and article verification key from said read representation;

verify that the extracted article digital data and associated verification key indeed correspond to the stored reference aggregated digital signature by executing on the CPU the further programmed steps of:

calculating a digital signature of the extracted article digital data with the one-way function;

calculating a candidate aggregated digital signature from the calculated digital signature of the extracted article digital data and the extracted verification key with the one-way accumulator; and

checking that the obtained candidate aggregated digital signature matches the stored reference aggregated digital signature,

whereby, in case said aggregated digital signatures match, the system is operable to deliver an indication that the article data on the test object is that of a genuine original article.

20. System according to claim 19, for verifying an article secured according to the method of any one of claims 8 and 9, wherein the imager is further equipped with a sensor operable to detect a unique physical characteristic of a marked original article, or of an associated object or individual, and the CPU is programmed to extract corresponding unique physical characteristic digital data from a detection signal received from the sensor, the imager having stored in the memory reference physical characteristic digital data UPC corresponding to said unique physical characteristic of the marked original article, or of associated object or individual, the system being further operable to:

detect with the sensor a unique physical characteristic of a subject being said article or said associated object or individual, and extract corresponding candidate unique physical characteristic digital data UPC^c;

compare the obtained candidate unique physical characteristic digital data UPC^c with the stored reference physical characteristic digital data UPC; and

in case the candidate unique physical characteristic digital data UPC^c is similar to the stored reference physical characteristic digital data UPC, within a given tolerance criterion, deliver an indication that the subject is considered as genuine.