

SYSTEM AND METHOD OF PACKAGING, AUTHENTICATING AND DETERMINING SPOT PRICES OF FUNGIBLE BASKETS OF INVESTMENT GRADE GEMSTONES AND PRECIOUS METALS

5 Field of Disclosure

The invention relates to system and method of developing, packaging, tracking and/or authenticating investment grade, fungible and standardised packages containing gemstones and/or precious metals, for use as financial instruments in commercial trading in physical and/or electronic marketplace and/or exchange, system and method of
10 establishing spot price discovery of gemstone packages, and aspects thereof.

Background

Stock exchanges around the world provide an open and transparent way of discovering market prices of company stocks and trading them. It is also easy to discover
15 prices and trade standardized gold and silver. Their values and authenticity can be determined easily through commodity exchanges.

In contrast, diamond prices are less transparent because diamonds are not traded in an open and transparent way until a commodity exchange, e.g. Singapore Diamond Investment Exchange, was set up to provide a fair, orderly and transparent marketplace
20 where sellers and buyers place their sell and buy orders anonymously, and their bid, ask and traded prices are published to all the participants in the marketplace. The spot/market price of diamonds is established when there is a cross/match between a bid and an ask price.

Generally, even when prices of single diamonds are published, their values could
25 not be used as a benchmark since prices of individual diamonds vary even when key attributes, for example, carat, cut, clarity and colour, are the same. However, baskets of diamonds traded on the commodity exchange are fungible – one basket of diamonds conforming to the specifications defined by the exchange is exchangeable at the same price for another basket of the same specifications. For example, each basket offered at
30 the exchange may comprise a mix of 0.5 carat and 1.0 carat diamonds or all 1.0 carat diamonds or higher carat value diamonds of the same or similar characteristics. Price variation of the diamonds will compensate each other, resulting in a consistent price for diamond baskets of the same diamond composition. The exchange may allow for a

multiplicity of standardized basket specifications to be traded, wherein each basket specification may be represented by a nominal monetary value.

While some investors would vault their diamond baskets with a trusted and secured depository, there are other investors who might prefer to trade over-the-counter and require a quick and reliable way of authenticating the product.

Existing publications such as US Patent No. 8,239,211 B2 and US 2015/0223580 A1 describe standardized baskets of diamonds for marketplace trading, however, they do not provide a quick and reliable way of authenticating the product, and they have other drawbacks.

The possibility of counterfeit diamonds and inconvenience and cost of certifying diamonds deter people from purchasing and investing in diamonds. Another factor deterring investors from purchasing high value diamonds is that diamond ownership cannot be tracked easily and therefore subject to money laundering issues.

Summary

According to a first aspect of the invention, a method of authenticating a fungible gemstone package is provided. The method comprises:

receiving, from an Near Field Communication (NFC) enabled device, encrypted data, a key identifier and a tag identifier, which are detected from the gemstone package, wherein the tag identifier is associated with a NFC tag arranged within the gemstone package;

retrieving, from a key database, a key associated with the key identifier;

using the key, decrypting the encrypted data to produce a decrypted tag identifier and a decrypted package identifier;

verifying the decrypted tag identifier against the tag identifier;

verifying the decrypted package identifier against a registered package identifier retrieved from a tag identifier database in which the registered package identifier is stored in association with the tag identifier, wherein the registered package identifier is associated with the gemstone package; and

successfully authenticating the gemstone package if the decrypted tag identifier matches the tag identifier and if the decrypted package identifier matches the registered package identifier.

5 In one embodiment, after successfully authenticating the gemstone package, the method further comprising:

retrieving, from an inventory database, data of the gemstone package, wherein the data of the gemstone package includes at least one basket code of gemstones comprised in the gemstone package;

10 based on the decrypted package identifier and the at least one basket code, retrieving, from a price database, spot prices of the gemstone package and/or the at least one basket code; and

transmitting the spot prices to the NFC-enabled device.

15 In one embodiment, receiving, from the NFC-enabled device, encrypted data, a key identifier and a tag identifier includes receiving geolocation data of the gemstone package, the method further comprising: storing the geolocation data in the tag identifier database and in association with the tag identifier.

20 In one embodiment, the method further comprises: generating an authentication failure message and transmitting the authentication failure message to the NFC-enabled device if the decrypted tag identifier and the tag identifier differ or if the decrypted package identifier and the registered package identifier differ.

According to a second aspect of the invention, a system for authenticating a fungible gemstone package is provided. The system comprises:

an authentication server and a tag identifier database communicably coupled thereto;

25 a key management server and a key database communicably coupled thereto, wherein the key management server is communicably coupled to the authentication server;

wherein the authentication server is configured to:

receive, from an Near Field Communication (NFC) enabled device, encrypted data, a key identifier and a tag identifier, which are detected from the gemstone package, wherein the tag identifier is associated with a NFC tag arranged within the gemstone package;

5 wherein the key management server is configured to:

retrieve, from the key database, a key associated with the key identifier;

wherein the authentication server is configured to:

using the key, decrypt the encrypted data to produce a decrypted tag identifier and a decrypted package identifier;

10 verify the decrypted tag identifier against the tag identifier;

verify the decrypted package identifier against a registered package identifier retrieved from the tag identifier database in which the registered package identifier is stored in association with the tag identifier, wherein the registered package identifier is associated with the gemstone package; and

15 successfully authenticate the gemstone package if the decrypted tag identifier matches the tag identifier and if the decrypted package identifier matches the registered package identifier.

In one embodiment, the system further comprises:

20 an inventory server and an inventory database communicably coupled thereto; and

a price server and a price database communicably coupled thereto,

wherein the inventory server is configured to:

25 after successful authentication of the gemstone package, retrieve, from the inventory database, data of the gemstone package, wherein the data of the gemstone package includes at least one basket code of gemstones comprised in the gemstone package;

wherein the inventory server is configured to:

based on the decrypted package identifier and/or the at least one basket code, retrieve, from the price database, spot prices of the gemstone package and/or the at least one basket code; and

wherein the authentication server is configured to:

- 5 transmit the spot prices received from the inventory server to the NFC-enabled device.

10 In one embodiment, the authentication server is configured to: receive, from the NFC-enabled device, geolocation data of the gemstone package; and store the geolocation data in the tag identifier database and in association with the tag identifier.

15 In one embodiment, the authentication server is configured to: generate an authentication failure message and transmit the authentication failure message to the NFC-enabled device if the decrypted tag identifier and the tag identifier differ or if the decrypted package identifier and the registered package identifier differ.

According to a third aspect of the invention, a fungible gemstone package comprises:

a casing;

20 a gemstone pouch and a Near Field Communication (NFC) tag which are arranged within the casing; and

a plurality of gemstones arranged in the gemstone pouch;

25 wherein the NFC tag includes a micro-chip and an antenna communicably coupled thereto, wherein the micro-chip includes a first memory area hardcoded with a tag identifier associated with the NFC tag and a second memory area storing both the tag identifier and a package identifier as encrypted data and storing a key identifier,

30 wherein the gemstone package is configured to be authenticated by decrypting the encrypted data using a key, which is stored external of the gemstone package and associated with the key identifier, to produce a decrypted package identifier and a decrypted tag identifier, by verifying the decrypted tag

identifier against the tag identifier which is stored in the first memory area, and by verifying the decrypted package identifier against a registered package identifier which is stored external of the gemstone package and in association with the tag identifier.

5 In one embodiment, the casing includes a metal material to prevent detection of the NFC tag by an NFC-enabled device, and wherein an opening is formed in the metal material to allow detection of the NFC tag therethrough.

10 In one embodiment, the gemstone package further comprises: a cover movably coupled to the casing, wherein the cover is at least movable between a first position in which the opening is exposed and a second position in which the opening is concealed.

15 In one embodiment, one of the casing and the cover is provided with a projection portion, and the other of the casing and the cover is provided with a complementary groove portion, wherein the projection portion and the groove portion are arranged in sliding engagement.

20 In one embodiment, the gemstone pouch includes a pouch support and a gemstone holder which is arranged within the pouch support and retains the gemstones, wherein the NFC tag is securely interposed between the pouch support and the gemstone holder, and is predisposed to result in breakage of the antenna when the NFC tag is separated from the pouch support.

25 In one embodiment, the NFC tag includes a ferrite material to increase readability of the NFC tag.

 In one embodiment, the metal material includes gold, silver, platinum, or any combination thereof.

30 In one embodiment, a spot price of the gemstone package is determined by a spot price of at least one basket of gemstones corresponding to the gemstones arranged in the gemstone pouch or package and a spot price of the metal material.

35 In one embodiment, the gemstones include diamonds.

Brief Description of Drawings

The invention will be described in detail with reference to the accompanying drawings, in which:

5 Figure 1A shows a gemstone package having a cover arranged in one open position according to one embodiment;

 Figure 1B shows the gemstone package of Figure 1A having the cover arranged in one closed position;

 Figure 1C shows the gemstone package of Figure 1A being removed of the cover;

10 Figure 1D shows an exploded side view of the gemstone package of Figure 1A;

 Figure 1E shows an exploded view of a gemstone pouch which is comprised in the gemstone package of Figure 1A;

 Figure 1F shows a casing and a cover of a gemstone package wherein the casing and the cover are configured to be arranged in sliding engagement according to one
15 embodiment of the invention;

 Figure 1G shows a gemstone having its table inscribed with a gemstone identifier;

 Figure 2 shows a memory comprised in an NFC tag;

 Figure 3 shows a registration server which is communicably coupled to a tag identifier database;

20 Figure 4 shows a gemstone package inventory server which is communicably coupled to an inventory database;

 Figure 5 shows a registration server which is communicably coupled to a tag identifier database, an inventory server which is communicably coupled to an inventory database, and a key management server which is communicably coupled to a key
25 database;

 Figure 6A shows an authentication server which is communicably coupled to a tag identifier database, an inventory server which is communicably coupled to an inventory database, a key management server which is communicably coupled to a key database, and a price server which is communicably coupled to a historical price database and/or
30 an exchange trading server which provides real-time or live price data; and

 Figure 6B shows a flow chart relating to a method of authenticating gemstone packages.

Detailed Description

In the following description, numerous specific details are set forth in order to provide a thorough understanding of various illustrative embodiments of the invention. It will be understood, however, to one skilled in the art, that embodiments of the invention may be practiced without some or all of these specific details. It is understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to limit the scope of the invention. In the drawings, like reference numerals refer to same or similar functionalities or features throughout the several views.

Embodiments described in the context of one of the devices or methods are analogously valid for the other devices or methods. Similarly, embodiments described in the context of a device are analogously valid for a method, and vice versa.

Features that are described in the context of an embodiment may correspondingly be applicable to the same or similar features in the other embodiments. Features that are described in the context of an embodiment may correspondingly be applicable to the other embodiments, even if not explicitly described in these other embodiments. Furthermore, additions and/or combinations and/or alternatives as described for a feature in the context of an embodiment may correspondingly be applicable to the same or similar feature in the other embodiments.

It should be understood that the articles “a”, “an” and “the” as used with regard to a feature or element include a reference to one or more of the features or elements. The term “and/or” includes any and all combinations of one or more of the associated feature or element. The terms “comprising,” “including,” and “having” are intended to be open-ended and mean that there may be additional features or elements other than the listed ones. Identifiers such as “first”, “second” and “third” are used merely as labels, and are not intended to impose numerical requirements on their objects, nor construed in a manner imposing any relative position or time sequence between limitations. Furthermore, terms such as “front”, “rear”, “top”, “bottom”, “side”, “under”, “over” used herein are merely for ease of description and may refer to the orientation of the features or elements as shown in the figures. It should be understood that any orientation of the features described herein is within the scope of the invention.

According to one or more aspects of the invention, gemstone packages, which are fungible, standardised and portable, are provided to be used as high-value financial instruments and/or investments for commercial trading, e.g. in a commodity exchange and/or over the counter. Each gemstone package is standardised according to a

predetermined specification, e.g. nominal value, gemological characteristics, optical characteristics, etc., or any combinations thereof.

Figure 1A shows a gemstone package 10 according to one embodiment of the invention wherein the gemstone package 10 may be provided with a cover 1 which is displaceable relative to a casing 8. The cover 1 is configured to expose (see Figure 1A) or conceal (see Figure 1B) the gemstones 11 to respectively allow or prevent detection by NFC-enabled devices and/or visual inspection. Other open and/or closed positions which are not illustrated in the drawings are also possible. Figure 1C shows the gemstone package 10 of Figure 1A having the cover 1 removed or separated from the casing 8. Figure 1D shows an exploded side view of the package of Figure 1B.

Referring to Figures 1A, 1B and 1D, the gemstone package 10 may comprise a metal casing 8, a metal plate 4, a glass plate 3, e.g. sapphire glass, a gemstone pouch 50, a plurality of gemstones 11 and a Near Field Communication (NFC) tag 6. The metal casing 8 may be secured to the metal plate 4 to provide a housing or body for the package 10. The glass plate 3 overlays the metal plate 4 and may be secured to the metal plate 4 and/or casing 8 to encase the gemstone pouch 50 and its contents. Referring to Figure 1E showing an exploded view of the gemstone pouch 50, the gemstone pouch 50 may comprise a pouch support 7 which may be attached to the casing 8 and/or metal plate 4, a gemstone holder 5 arranged within the pouch support 7 and a plurality of gemstones 11 retained or supported by or within the gemstone holder 5. The gemstone holder 5 may include a non-rigid material, e.g. soft, sponge-like material, which may be provided with a plurality of openings in which the gemstones 11 are arranged or embedded.

25

The metal casing 8 and metal plate 4, which may substantially form most of the package body, prevent the NFC tag 6 from being read or detected by an NFC-enabled device. However, the metal plate 4 is provided with at least one opening 41 or window positioned over the gemstone pouch 50; the glass plate 3 overlays the metal plate 4 so that the gemstones 11 are visible through a front face of the casing 8, i.e. through the opening 41 in the metal plate 4 and glass plate 3 overlaying the opening 41. Accordingly, a NFC tag 6 arranged within the casing 8 can be read or detected through the opening 41. Inscription on the gemstones may be readable and visually authenticated through the opening 41. For example, inscription may be provided on the table of each gemstone

30

using thin-film nanotechnology marking process. These markings are visible such as by an optical reader and do not affect clarity of the gemstones 11.

Referring to Figures 1D and 1E, the NFC tag 6 may be securely interposed, e.g. adhered, between the gemstone holder 5 and the pouch support 7. The NFC tag 6 comprises a micro-chip and an antenna 13 communicably coupled thereto. The micro-chip may include a processor and at least one memory 12 communicably coupled thereto. The antenna 13 may be communicably coupled to the processor. The at least one memory 12 may include a plurality of memory areas, e.g. M1, M2, M3, M4, etc., for storing various data relating to the gemstone package 10, which will be discussed more fully in later paragraphs. The NFC tag 6 may be provided with a layer of ferrite soft material 61 to increase readability or detectability of the NFC tag 6. This layer of ferrite soft material 61 may be arranged between the NFC tag 6 and the metal casing 8 and/or pouch support 7. Securely interposing, e.g. adhering, the NFC tag 6 between the gemstone holder 5 and/or the pouch support 7 predisposes the antenna 13 to breakage upon removal or separation of the NFC tag 6 from the pouch support 7 and/or of the NFC tag 6 from the gemstone holder 5. Breaking the antenna 13 renders the NFC tag 6 unreadable or undetectable by an NFC-enabled device.

The cover 1 may be movably coupled to the casing 8, e.g. by a sliding mechanism. In one embodiment, as shown in Figure 1F, the casing 8 may be provided with grooves 21 on the package body, e.g. metal casing 8, while the cover 1 is provided with complementary projections 22. The cover 1 may be placed over the metal casing 8 with its projections 22 arranged in sliding engagement with the grooves 21 such that the cover 1 is displaceable relative to the casing 8, at least between a first or open position (see Figure 1A) in which gemstones 11 are exposed, e.g. visible for inspection by human or detection by a NFC-enabled device, and a second or closed position (see Figure 1B) in which gemstones 11 are concealed, e.g. not visible, to disallow visual inspection of the gemstones 11 and/or detection of NFC tag 6. In the closed position, the gemstone package 10 may be a contoured palm-sized package which is undetectable by NFC-enabled devices. In one embodiment, as shown in Figures 1D and 1F, a plate 2, e.g. metal plate, may be secured to the cover and provided with product information, e.g. logos of issuing exchange and/or grading laboratory, package identifier and/or any combination thereof. This plate 2 may be interposed between the cover 1 and a glass plate 3.

Variations to the gemstone package 10 may be envisaged and implemented in some other embodiments.

5 In some embodiments, the cover may be movably coupled to the casing by a hinge mechanism such that the cover is displaceable relative to the casing 8 by pivotably moving the cover about the hinge. One example of such embodiments is a clam-shell container. In some embodiments, the hinge mechanism may be replaced with other securing mechanism. In some embodiments, the cover may be provided as a rigid or flexible sleeve such that the gemstone package 10 may be removably inserted into the sleeve and retained therein. In some embodiments, the gemstone package 10 may not include a cover, e.g. see Figure 1C.

15 In various embodiments, the gemstone packages 10 may be provided in a multiplicity of sizes e.g. credit-card size, palm size, and/or shapes, e.g. coin or circle, rectangle, square, contoured rectangle, and any combinations thereof.

In some embodiments, the metal casing 8 and/or metal plate 4 may include a precious metal, such as but not limited to gold, silver and platinum. In some embodiments, the metal casing 8 may include and be at least partially formed of a ceramic material. In some embodiments, the cover 1 may include a precious metal, such as but not limited to gold, silver and platinum.

25 In some embodiments, the layer of ferrite soft material may be omitted or replaced by other material which increases readability or detectability of the NFC tag.

In some embodiments, the NFC tag may be securely interposed between gemstone holder and the casing or metal plate. In some embodiments, the NFC tag may be secured to other parts of the gemstone package and/or arranged at other positions within the gemstone package.

30 In some embodiments, the gemstone pouch may be provided in other configurations or arrangements. In one example, the gemstone pouch may comprise a block having gemstones arranged therein wherein the NFC tag may be adhered to a bottom face of the block while the top face of the block allows visual inspection of the tables of the gemstones. The block may be fabricated by injection-molding. The block

may include a transparent, translucent and/or opaque material. Gemstones may be encapsulated within the block or at least partially embedded in the block.

It is to be appreciated that any of the above-described embodiments and/or variations are illustrative only and may be combined with one or more aspects of the invention as described in the present disclosure.

According to one or more aspects of the invention, system and method of developing and/or packaging gemstone packages are provided and are more fully described as follows.

Gemstones 11 which are to be assembled into various gemstone packages 10 may be selected from one or more exchange-defined baskets according to exchange-defined product specification. Gemstones comprised in a same exchange-defined basket have one or more similar characteristics and/or have similar or equivalent price. Source and/or price of gemstones in exchange-defined baskets are recorded or tracked, and therefore source and/or price information of gemstones 11 which are eventually selected to be assembled into a gemstone package 10 are traceable and transparent to interested parties of the gemstone package 10, e.g. owners, prospective owners. Each gemstone which is to be assembled into a gemstone package 10 may be inscribed with a unique gemstone identifier, e.g. Gemological Institute of America (GIA) report or certificate number, or any other unique number, on its table (see Figure 1G). This inscription process may take place at a grading laboratory after the gemstone is certified.

The selected gemstones may be secured to a gemstone holder 5. The gemstone holder 5 and the secured gemstones may be arranged within the pouch support 7. A NFC tag 6 and soft ferrite material 61 may be interposed between and secured to the gemstone holder 5 and the pouch support 7. The gemstone pouch 50 is suitably arranged within the casing 8 at a predetermined position. A metal plate 4 may be arranged over the gemstone pouch 50 such that the opening 41 in the metal plate 4 is aligned with the gemstones 11. A glass plate 3 may be arranged over the metal plate 4. The glass plate 3 and/or the metal plate 4 may be secured to the casing 8 to encase the gemstone pouch 50 and its gemstones 11 within a gemstone package 10. Assembly of the gemstone package 10 may further include providing unique package identifier, e.g. serial number, and other information on the gemstone package, e.g. on the casing 8, metal plate 2 or 4, or cover 1. Various data (e.g. unique gemstone identifiers of the packaged gemstones)

may be registered via a registration server 14 and stored in a gemstone package inventory database 17 in association with each package identifier. It is to be appreciated that the aforementioned steps may be modified and/or interchangeable as known to persons skilled in the art.

5

According to one aspect of the invention, system and method of configuring, registering and/or tracking gemstone packages 10 are provided and are more fully described as follows.

10 NFC tags 6, which are to be arranged within gemstone packages 10, are pre-configured to facilitate subsequent authentication of gemstone packages 10. Particularly, a tag identifier and predetermined gemstone package data, e.g. a package identifier, are stored and/or hard-coded or embedded in different memory areas or sectors 12 of the micro-chip in the NFC tag 6. This may be performed during manufacturing of NFC tags.

15 Each NFC tag 6 is assigned a unique tag identifier (tag ID) which may be determined by the manufacturer of the NFC tag. Each gemstone package 10 is assigned a unique package identifier, e.g. serial number, and an exchange-defined code which may be determined by a commodity exchange, e.g. diamond trading exchange. The tag identifier may be hard-coded into a first memory area M1. The package identifier and a key

20 identifier may be written to the second memory area M2. An exchange-defined code may be written to the third memory area M3. These memory areas are not granted write access to prevent over-writing. These memory areas may be granted different read access. For example, the first memory area M1 may be readable by any NFC-enabled device; data in the second memory area M2 may be encrypted and therefore readable

25 only by certain NFC-enabled device installed with a predetermined application program, e.g. authentication program; data in the third memory area M3 may be encrypted and therefore only readable by certain NFC-enabled device installed with another predetermined application program, e.g. exchange depository application program which contains an appropriate key to unlock the data. Furthermore, for example, data in the third

30 memory area M3 cannot be copied and duplicated. Accordingly, counterfeits may be detected by reading the data stored in the third memory area M3 through an exchange depository application program. A gemstone package 10 may be ascertained as a counterfeit if it does not display the exchange-defined code.

35 Figure 3 shows a registration server 14 which is communicably coupled to a tag identifier database 15, e.g. UID register, and configured to read from and write into the

tag identifier database 15. The tag identifier database 15 is configured to store tag identifiers as well as other gemstone package data in association with each tag identifier. Such gemstone package data may include unique package identifier (e.g. serial number), status of tag identifier (e.g. activated or inactivated), geolocation of the gemstone package 10 (e.g. one or more previously detected geolocations), etc.

Figure 4 shows a gemstone package inventory server 16 which is communicably coupled to an inventory database 17, and configured to read from and write into the inventory database 17. The database 17 is configured to store gemstone package identifiers (e.g. serial number) as well as other data in association with each package identifier. Such data may include gemstone identifiers of the various gemstones selected for each gemstone package (e.g. GIA certificate number, identification number inscribed on the tables of each), exchange-defined basket codes of the various gemstones comprised in the package.

Figure 5 shows a registration server 14 which is communicably coupled to a tag identifier database 15, an inventory server 16 which is communicably coupled to an inventory database 17, and a key management server 18 which is communicably coupled to a key database 19 comprising private keys.

For each gemstone package 10 assigned with a package identifier e.g. serial number, and having an NFC tag 6 assigned with a tag identifier, the registration server 14 retrieves, from the key database 19, a key via the key management server 18 and uses the key to encrypt the tag identifier and package identifier to produce encrypted data. Access to the key database 19 may be provided through the key management server 18 to prevent direct manipulation of data in the key database 19. The registration server 14 writes the encrypted data and a key identifier associated with the key into the second memory area M2 of the NFC tag 6. Data in the second memory are "locked" and protected from being overwritten. This "locking" feature ensures that the encrypted data in the second memory area M2 are permanently encoded. Even if the encrypted data may be copied or written into another NFC tag, the tag identifier of this other NFC tag 6 will be different from that contained in the encrypted data and this discrepancy will be detected during authentication which will be discussed more fully in later paragraphs.

According to one or more aspects of the invention, system and method of authenticating and/or tracking gemstone packages are provided and are more fully described as follows.

5 Figure 6A shows an authentication server 20 (or authentication and information server) which is communicably coupled to a tag identifier database 15, an inventory server 16 which is communicably coupled to an inventory database 17, a key management server 18 which is communicably coupled to a key database 19, and a price server 21 which is communicably coupled to a historical price database 22 and/or an
10 exchange server 23 which provides real-time price data. Figure 6B shows a flow chart for a method of authenticating gemstone packages, which will be described with reference to Figure 6A.

 To verify the authenticity of a gemstone package 10, an NFC-enabled device 30, e.g. mobile device, phone or tablet, computer and terminal, which is installed with a
15 predetermined application program or software, e.g. authentication program, is provided. In one embodiment, the NFC-enabled device 30 is a mobile communication device which is installed with a prescribed authentication mobile app. Any NFC-enabled software or device may be able to read the NFC tag 6 but it would not be able to decipher the data.

 In block 601, the NFC-enabled device 30 reads the NFC tag 6 of the gemstone
20 package 10 to be authenticated. In particular, the NFC-enabled device 30 detects contents in the NFC tag 6, i.e. tag identifier stored in the first memory area M1 of the NFC tag 6 as well as encrypted data and key identifier stored in the second memory area M2 of the NFC tag 6. The tag identifier is associated with the NFC tag 6 arranged in this particular gemstone package 10. In some embodiments, the NFC-enabled device 30 may
25 also ascertain geolocation location of the gemstone package 10 as the current geolocation of the device 30.

 In block 602, the NFC-enabled device 30 transmits an authentication request to the authentication server 20 wherein the authentication request includes the detected tag
30 identifier, encrypted data and key identifier. In some embodiments, the authentication request may include the geolocation of the gemstone package 10.

 In block 603, the authentication server 20 receives the authentication request. The authentication server 20 extracts the key identifier from the request, generates a key

retrieval request, and transmits the key retrieval request, including the key identifier, to the key management server 18.

In block 604, the key management server 18 receives the key retrieval request.
5 Based on the key identifier included in the request, the key management server 18 retrieves, from the key database 19, the corresponding key which is associated with the key identifier. The key management server 18 then transmits the corresponding key to the authentication server 20.

10 In block 605, the authentication server 20 receives the corresponding key and uses it to decrypt the encrypted data, which was received from the NFC-enabled device 30 in block 603, to produce a decrypted tag identifier and a decrypted package identifier.

In block 606, the authentication server 20 verifies the decrypted tag identifier
15 against the tag identifier which was received from the NFC-enabled device 30 in block 603. If the decrypted tag identifier and the tag identifier received in block 603 match, verification at block 606 is successful and block 606 will proceed to block 607. If the decrypted tag identifier and the tag identifier received in block 602 differ, i.e. mismatch, verification at block 606 is unsuccessful and block 606 will proceed to block 606A.

20 In block 606A, the authentication server 20 generates an authentication failure message and transmits the message to the NFC-enabled device 30 in response to its authentication request in block 602. The authentication failure message may provide an alert or warning about the inauthenticity of the particular gemstone package 10. The
25 authentication application program in the NFC-enabled device 30 may then close.

In block 607, based on the decrypted tag identifier, the authentication server 20
retrieves, from the tag identifier database 15, a registered package identifier which is stored therein in association with the decrypted tag identifier. The authentication server
30 20 then verifies the decrypted package identifier against the registered package identifier. If the decrypted package identifier and the registered package identifier match, verification at block 607 is successful and block 607 will proceed to block 608. If the decrypted package identifier and the registered package identifier differ, i.e. mismatch, verification at block 607 is unsuccessful and block 607 will proceed to block 607A.

35

In block 607A, the authentication server 20 generates an authentication failure message and transmits the message to the NFC-enabled device 30 in response to its authentication request in block 602. The authentication failure message may provide an alert or warning about the inauthenticity of the particular gemstone package 10. The authentication application program in the NFC-enabled device 30 may then close.

If both verification processes in blocks 606 and 607 are successful, authentication of the particular gemstone package 10 is successful, i.e. authenticity of the gemstone package is established, and the flow chart proceeds to block 608. In block 608, geolocation data of the gemstone package 10, if available, may be written or stored in the tag identifier database 15. The geolocation data may have been received at the authentication server 20 in block 603.

In block 609, the authentication server 20 retrieves from the inventory database 17 various data associated with the package identifier, e.g. gemstone identifiers, exchange-defined basket codes of the gemstones contained in the package, etc, or any one or combination thereof. Based on these retrieved basket code(s) and/or package identifier, the authentication server 20 retrieves, from the historical price database 22 and/or exchange trading server 23, via the price server 21, spot or market prices of the identified exchange-defined basket code(s) and/or of the particular gemstone package 10. The exchange trading server 23 may provide live or real-time price information of baskets of gemstones identified by the retrieved basket codes and/or gemstone packages. In some embodiments, the spot price of a gemstone package may be determined by a sum of spot prices of the basket(s) of gemstones comprised in the gemstone package and, optionally, spot prices of the precious metal(s) forming the gemstone package.

In block 610, the authentication server 20 generates an informational message, including at least some of the retrieved data, e.g. spot or market prices of the basket(s) of gemstones comprised in the gemstone package and/or the gemstone package, and transmits the message to the NFC-enabled device 30 to be displayed thereon.

It is to be appreciated that the aforementioned steps may be modified and/or interchangeable as known to persons skilled in the art. For example, blocks 609 and 610 may precede block 608; blocks 606 and 607 may be interchangeable; block 608 may be omitted; and/or block 610 may be omitted.

The gemstone package 10 may be separately and/or further authenticated by a commodity exchange. In particular, an NFC-enabled device may detect contents in the NFC tag 6, i.e. exchange-defined code stored in the third memory area M3 of the NFC tag. The NFC-enabled device may be installed with another predetermined application program, e.g. exchange depository application program which has a private key to read or detect encrypted data in the third memory area M3. The NFC-enabled device may transmit the detected data to the authentication server 20 or another authentication server for verification. If the detected data conforms to or matches the data and/or data format or code predetermined by the commodity exchange, the gemstone package 10 is successfully authenticated. If the detected data differs from the data and/or data format or code predetermined by the commodity exchange, authentication of the gemstone package 10 is unsuccessful.

According to one or more aspects of the invention, method and system of obtaining and/or ascertaining market prices of a gemstone package and its basket(s) of gemstones at any time are provided.

Prices available in Rapaport are calculated prices rather than actual transaction prices. These calculated prices are therefore useful as reference prices but cannot be relied upon as spot prices. In order to ascertain market prices of gemstones, they must be listed on a commodity exchange where orders are placed and executed anonymously, and prices are published. As such, by listing the gemstone packages on a commodity exchange, spot prices of the gemstone packages and the baskets providing the gemstones forming the packages can be retrieved from a historical price database and/or an exchange server providing real-time prices.

According to one or more aspects of the invention, system and method of tracking ownership of gemstone packages are provided.

Every gemstone package received directly from the approved grading laboratory will be registered in a commodity exchange depository holdings database. The registration process includes recording an exchange's member and whether the gemstone package belongs to the member or its customer who would have been subjected to a Know Your Client (KYC) or Anti-Money Laundering (AML) verification check successfully (this may be an obligation of members of a commodity exchange as prescribed by its rules).

The depository holdings database records the owner which is identified by its depository account number. When the gemstone package is traded on the exchange, the seller's holding in the exchange depository holdings database will be reduced by the quantity of gemstone packages sold and the buyer's holding in the exchange depository holdings database will be increased by the quantity accordingly. The exchange settlement system may randomly select from the seller's gemstone package holdings the package identifier, e.g. serial number, to be delivered to the buyer. The depository holdings database records the change of ownership of the gemstone package bought and sold on the exchange until it is withdrawn from the exchange depository.

Given the security and authentication features packaged in the gemstone package, after withdrawal, buyers of gemstone packages in the Over the Counter (OTC) market may choose to register the gemstone package with the exchange depository through a broker member of the exchange after undergoing a complete KYC/AML process. The same process of keeping track of the ownership and holdings will be in the exchange depository holdings database. This process will solve current KYC/AML issues relating to gemstones, e.g. diamonds, and address long standing KYC/AML concerns of Financial Action Task Force (FATF) and the relevant authorities of member countries in relation to diamonds.

For the purpose of any investigation on a particular gemstone package traded on the OTC market, the particular gemstone package may be traced through its records with the exchange depository holdings database. In the worst case scenario, it can be traced to the last owner registered with the exchange depository holdings database.

Embodiments of the invention provide several advantages including but not limited to the following:

- The gemstone package encases precious stones in a durable, hardy and aesthetically pleasing housing which can be visually inspected but tamper-evident.

- The gemstone package is embedded with an NFC tag having a micro-chip having a memory which is encoded with various information relating to the gemstone package and its component gemstones. The memory may be granted different access, e.g. at least part of the memory may be hard-coded to permanently encode information to prevent data loss; at least part of the memory may be locked to prevent over-writing; at least part

of the memory may be written with encrypted data which is decipherable with an appropriate key; and/or at least part of the memory may be prevented from read access by a non-prescribed application to prevent data duplication.

- 5 - With the NFC tag, the gemstone package is configured to communicate wirelessly with an NFC-enabled device when the package is brought into detection proximity of the NFC-enabled device and hence the gemstone package does not require a power source to enable communication.
- 10 - Various data of a gemstone package and its component gemstones may be stored or registered in appropriate databases, which are external of the gemstone packages, prior to its issuance or first sale. With the NFC tag, the gemstone package may be written or embedded with encrypted data for facilitating subsequent authentication of the gemstone package. During an authentication procedure, e.g. which may take place prior to a
- 15 prospective resale, data detected from the NFC tag of a particular gemstone package are verified against data stored or registered in the appropriate databases. If authentication is successful, various data of the particular gemstone are retrieved, e.g. spot or market prices, and transmitted to the party, e.g. NFC-enabled device, which requested the authentication procedure; also, geolocation of the particular gemstone package may be
- 20 updated into the appropriate database for record and tracking purpose.
- The gemstone package may be mostly formed of a metal material to prevent data theft, e.g. by a proximate NFC-enabled device to harvest or skim data from the NFC tag. Furthermore, the gemstone package may be provided with a cover which is configured to
- 25 reveal or conceal gemstones through an opening in the gemstone package to respectively allow or prevent detection by NFC-enabled devices. The cover provides privacy and protection to the gemstone package in that when the gemstones are concealed, the gemstone package is undetectable by NFC-enabled devices.
- 30 - Gemstones encased in the gemstone packages may be inscribed with unique gemstone identifiers on their tables, which are visible through the opening and visually detectable and verifiable such as by an optical reader.
- The gemstone package may be made of one or more precious metals which adds
- 35 prestige to the product and provides a hybrid product for hedging as precious metals have their intrinsic market value. As such, the price of a gemstone package may be determined

by the aggregated spot prices of the basket(s) of gemstones corresponding to gemstones arranged in the package or pouch and, optionally, spot prices of the precious metal(s).

5 - The gemstones are sourced from a commodity exchange and their basket codes are recorded in the inventory database. Accordingly, the prices of the gemstones or baskets are open and transparent and hence verifiable or traceable.

10 - Geolocation and/or ownership data may be recorded or registered in databases to allow tracing of location and/or owner data, and/or performing verification check to comply with KYC/AML rules prescribed by a commodity exchange.

 - Existing process of consigning diamonds or baskets to a commodity exchange for trading is time-consuming and costly. In contrast, the use of NFC tag in each gemstone package in conjunction with the authentication program and the table inscription on the gemstones enable the product to be consigned quickly and reliably.

15

 It is to be understood that the embodiments and features described above should be considered exemplary and not restrictive. Many other embodiments will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity,
20 and not to limit the disclosed embodiments of the invention.

25

30

What is claimed is:

1. A method of authenticating a fungible gemstone package, the method comprising:

5 receiving, by an authentication server, encrypted data, a key identifier and a tag identifier from an Near Field Communication (NFC) enabled device, wherein the encrypted data, the key identifier and the tag identifier are detected from the gemstone package, wherein the tag identifier is associated with a NFC tag arranged within the gemstone package;

10 retrieving, by a key management server which is communicably coupled to the authentication server, a key from a key database which is communicably coupled to the key management server, wherein the key is associated with the key identifier;

using the key, decrypting, by the authentication server, the encrypted data to produce a decrypted tag identifier and a decrypted package identifier;

verifying, by the authentication server, the decrypted tag identifier against the tag identifier;

15 verifying, by the authentication server, the decrypted package identifier against a registered package identifier retrieved from a tag identifier database in which the registered package identifier is stored in association with the tag identifier, wherein the registered package identifier is associated with the gemstone package; and

20 successfully authenticating, by the authentication server, the gemstone package if the decrypted tag identifier matches the tag identifier and if the decrypted package identifier matches the registered package identifier.

2. The method of claim 1 wherein after successfully authenticating, by the authentication server, the gemstone package, the method further comprising:

25 retrieving, by an inventory server which is communicably coupled to the authentication server, data of the gemstone package from an inventory database which is communicably coupled to the inventory server, wherein the data of the gemstone package includes at least one basket code of gemstones comprised in the gemstone package;

based on the decrypted package identifier and/or the at least one basket code, retrieving, by the authentication server via a price server which is communicably coupled to the authentication server, spot prices of the gemstone package and/or the at least one basket code from a price database and/or an exchange trading server which are
5 communicably coupled to the price server; and

transmitting, by the authentication server, the spot prices to the NFC-enabled device.

3. The method of claim 2 wherein receiving, by an authentication server, encrypted data, a key identifier and a tag identifier from an Near Field Communication (NFC) enabled
10 device includes receiving geolocation data of the gemstone package, the method further comprising:

storing, by the authentication server, the geolocation data in the tag identifier database and in association with the tag identifier.

4. The method of claim 1, further comprising:

15 generating, by the authentication server, an authentication failure message and transmitting the authentication failure message to the NFC-enabled device if the decrypted tag identifier and the tag identifier differ or if the decrypted package identifier and the registered package identifier differ.

5. A system for authenticating a fungible gemstone package, the system comprising:

20 an authentication server and a tag identifier database communicably coupled thereto;

a key management server and a key database communicably coupled thereto, wherein the key management server is communicably coupled to the authentication server;

25 wherein the authentication server is configured to:

receive, from an Near Field Communication (NFC) enabled device, encrypted data, a key identifier and a tag identifier, which are detected from the gemstone package, wherein the tag identifier is associated with a NFC tag arranged within the gemstone package;

wherein the key management server is configured to:

retrieve, from the key database, a key associated with the key identifier;

wherein the authentication server is configured to:

5 using the key, decrypt the encrypted data to produce a decrypted tag identifier and a decrypted package identifier;

verify the decrypted tag identifier against the tag identifier;

10 verify the decrypted package identifier against a registered package identifier retrieved from the tag identifier database in which the registered package identifier is stored in association with the tag identifier, wherein the registered package identifier is associated with the gemstone package; and

successfully authenticate the gemstone package if the decrypted tag identifier matches the tag identifier and if the decrypted package identifier matches the registered package identifier.

6. The system of claim 5, further comprising:

15 an inventory server and an inventory database communicably coupled thereto; and

a price server and a price database communicably coupled thereto, wherein the inventory server and the price server are communicably coupled to the authentication server,

20 wherein the inventory server is configured to:

after successful authentication of the gemstone package, retrieve, from the inventory database, data of the gemstone package, wherein the data of the gemstone package includes at least one basket code of gemstones comprised in the gemstone package;

25 wherein the authentication server is configured to:

based on the decrypted package identifier and/or the at least one basket code, retrieve via the price server, from the price database and/or an exchange trading server

which are communicably coupled to the price server, spot prices of the gemstone package and/or the at least one basket codes; and

transmit the spot prices received from the price server to the NFC-enabled device.

7. The system of claim 6, wherein the authentication server is configured to:

5 receive, from the NFC-enabled device, geolocation data of the gemstone package;
and

store the geolocation data in the tag identifier database and in association with the tag identifier.

8. The system of claim 5, wherein the authentication server is configured to:

10 generate an authentication failure message and transmit the authentication failure message to the NFC-enabled device if the decrypted tag identifier and the tag identifier differ or if the decrypted package identifier and the registered package identifier differ.

9. A fungible gemstone package comprising:

15 a casing;

a gemstone pouch and a Near Field Communication (NFC) tag which are arranged within the casing; and

a plurality of gemstones arranged in the gemstone pouch;

20 wherein the NFC tag includes a micro-chip and an antenna communicably coupled thereto, wherein the micro-chip includes a first memory area hardcoded with a tag identifier associated with the NFC tag and a second memory area storing both the tag identifier and a package identifier as encrypted data and storing a key identifier,

wherein the gemstone package is configured to be authenticated by having an authentication server

25 receive the encrypted data, the key identifier and the tag identifier from a Near Field Communication (NFC) enabled device,

decrypt the encrypted data using a key, which is stored external of the gemstone package and associated with the key identifier, to produce a decrypted package identifier and a decrypted tag identifier,

verify the decrypted tag identifier against the tag identifier, and

5 verify the decrypted package identifier against a registered package identifier which is stored external of the gemstone package and in association with the tag identifier.

10. The gemstone package of claim 9, wherein the casing includes a metal material to prevent detection of the NFC tag by an NFC-enabled device, and wherein an opening is formed in the metal material to allow detection of the NFC tag therethrough.

11. The gemstone package of claim 10, further comprising:

15 a cover movably coupled to the casing, wherein the cover is at least movable between a first position in which the opening is exposed and a second position in which the opening is concealed.

12. The gemstone package of claim 11, wherein one of the casing and the cover is provided with a projection portion, and the other of the casing and the cover is provided with a complementary groove portion, wherein the projection portion and the groove portion are arranged in sliding engagement.

13. The gemstone package of any one of claims 9 to 12, wherein the gemstone pouch includes a pouch support and a gemstone holder which is arranged within the pouch support and retains the gemstones, wherein the NFC tag is securely interposed between the pouch support and the gemstone holder, and is predisposed to result in breakage of the antenna when the NFC tag is separated from the pouch support.

14. The gemstone package of any one of claims 9 to 13, wherein the NFC tag includes a ferrite material to increase readability of the NFC tag.

15. The gemstone package of any one of claims 9 to 14, wherein the metal material includes gold, silver, platinum, or any combination thereof.

16. The gemstone package of claim 15, wherein a spot price of the gemstone package is
5 determined by a spot price of at least one basket of gemstones corresponding to the gemstones arranged in the gemstone pouch and a spot price of the metal material.

17. The gemstone package of any one of claims 9 to 16, wherein the gemstones include diamonds.

10