

TOKEN ALLOCATION, PHYSICAL ASSET TRANSFERRAL AND INTERACTION MANAGEMENT

Field

The present invention relates to the allocation of tokens to physical assets, tracking physical assets along a supply chain and remote interactions with those assets.

Background

The world of counterfeit goods is expanding. There is increasing difficulty in determining whether goods are legitimate or counterfeit. This problem is exacerbated with goods, such as bulk goods, that can be broken down or apportioned and legitimate portions of the bulk goods are augmented or distributed with counterfeit portions. For example, in the distribution of foodstuffs, a particular type or varietal may have high value and be sold mixed with a lower grade or lower cost analogue. As such, the total volume of product ultimately sold exceeds the original volume and the consumer has been misled into buying counterfeit goods – which, presently, is taken to include any goods the consumer was misled into acquiring.

In addition, for businesses that host or lease remote assets – e.g. remote servers in co-location, and other resources – there is similar difficulty encountered in verifying that the assets actually allocated to the business are those the subject of the lease.

It would be desirable therefore to provide a system or method to alleviate one or more of the above problems, or at least provide a useful alternative. Ideally, so as to secure networks of heterogenous resources, such a system should be implementable atop existing infrastructure with the minimal requirement that the underlying hardware and software components integrate the solution.

Summary of invention

Described herein is a computer-implemented method for allocating tokens to multi-order quantities of goods, comprising:

generating a first token for association with a first physical quantity of a good (**first quantity**), wherein:

the first token is associated with a first digital token; and

the first digital token is associated with one or more product properties, at least one said product property being the first quantity;
generating two or more second tokens for association with second physical quantities of the good (**second quantities**), the second quantities being portions of the first quantity, wherein:
each second token is associated with a second digital token;
each second digital token is associated with one or more product properties, at least one said product property in each case being the respective second physical quantity of the good,
wherein a sum of all the second quantities associated with the second tokens does not exceed the first quantity.

As used herein, the term “multi-order quantity” refers to a quantity of a good that is sufficient to satisfy multiple separate orders or to otherwise be divisible for transport, sale or use in portions. For example, a pallet of disinfectant bottles may constitute a multi-order quantity (that is allocated a first token) as it can be divided into smaller quantities of bottles (that are allocated second tokens). Similarly, a multi-order quantity of a good may be a bulk good (this is allocated a first token), such as ginseng, liquids, grains, powders, chemicals and the like, from which aliquots are taken (that are allocated second tokens).

The second quantities:

- may be equal quantities;
- may be unequal quantities; or
- may comprise a plurality of different quantities.

In addition, the sum of all the second quantities may be equal to the first quantity.

Each of said first token and second tokens may be unique. Similarly, each of said first digital token and second digital tokens may be unique.

Advantageously, the above computer-implemented method enables codes, such as quick response (QR) codes, barcodes, RFID tags, and the like to be allocated to multi-order quantities of goods such as bulk goods. The first token is allocated to the multi-order quantity of the goods, and the second tokens are generated and allocated to sub-quantities or second quantities that are taken from the first quantity. In this manner, the original, first quantity of goods can be separately packaged. Moreover, by disabling tokens on redemption or

validation, the maximum quantity of goods that can be validated is equal to the first quantity of those goods. This reduces the opportunity for counterfeiting.

At least one said product property associated with each second digital token may be the first digital token. This ensures the sub-quantity of the good is associated with the original quantity. Notably, properties of the produce may be the type of product, the geographical origin of the product, its quality or rating and other characteristics or unique identifying information and data such as the bioinformetric or organic qualities of the product itself, or may be the packaging date, the digital token or physical token associated with the product and so on. The bioinformetric information pertaining to or describing the product's morphology, colour, pattern, discernable texture, or a combination of these and similar characteristics may also be encoded. Bioinformetric data may replace the need for a physical tag on the product itself and/or may be used to sign digital tokens. The same is true for unique artifacts of manufacture which may be intentional or accidental such as the brush strokes of a painting, a creator's physical signature — applied to batch-produced copies or individual examples of a work — or tooling and finishing marks left on a product's surface.

Also disclosed is a computer-implemented method for transferring a physical asset, comprising:

- generating a public indicium and a private indicium;
- applying the public indicium to a visible location associated with the physical asset;
- applying the private indicium to a further location associated with the physical asset, the further location being a tamper-evident location;
- generating a digital token associated with the public indicium and private indicium, the digital token being associated with one or more product properties, at least one said product property being current owner information of a transferor;
- the method further comprising:
 - receiving a request for transferral of the physical asset, the request comprising the public indicium and owner information of a transferee;
 - verifying the public indicium; and
 - updating the current owner information with the owner information of the transferee.

Verifying the public indicium may comprise verifying the public indicium using the private indicium.

The "indicium" may be a token as used in the computer-implemented methods above, or may be some other form of indicium, visible or otherwise — e.g. barcodes, QR-codes radio

frequency identification (RFID) tags, infometric/bioinfometric data, and so on. Some of the indicia may be encrypted, and others may not be.

As used herein, tamper evident locations are locations that cannot be accessed without it being evident to a third party that such access has been made. For example, a private indicium may be hidden beneath a scratch panel, or within sealed packaging or under a label comprising the public indicium where the label must be removed to expose the private indicium.

The computer-implemented method may further comprise uploading the digital token to a multi-node network, and wherein:

- receiving the request for transferral further comprises receiving a hash from the transferor;

- verifying the public indicium comprises using the hash to verify the public indicium;
- and

- updating the current owner information with the ownership identifier comprises updating the current owner information with the hash and the ownership identifier.

The hash may be used to verify the public indicium comprises using the hash to verify the transferor is a current owner of the physical asset. The hash may comprise a hash of at least the current owner information and the digital token.

Advantageously, the tokens may therefore be uploaded to a block-chain or other distributed ledger technology or network.

The computer-implemented methods may further comprise uploading the digital token to a multi-node network, and wherein:

- receiving the request for transferral comprises receiving the digital token and the current owner information;

- verifying the public indicium comprises verifying, using a ledger stored on a node in the multi-node network, the public indicium is associated with the digital token and the current owner information;

- updating the current owner information with the ownership identifier comprises updating the ledger with the owner information of the transferee.

The computer-implemented method described above may be implemented on a block-chain.

The computer-implemented methods described above may be combined. For example, the method for transferring a physical asset may require the public indicium and digital token to be allocated according to the method of allocating tokens to multi-order quantities of goods, wherein:

- the first token comprises at least the public indicium;
- the first quantity comprises the physical asset; and
- the digital token comprises the first digital token.

The first token may comprise both the public indicium and private indicium.

Generating a public indicium and private indicium may comprise generating pairs of indicia, each pair comprising a said public indicium and a said private indicium, each pair being associated with a corresponding digital token, wherein the pairs of indicia and digital tokens are allocated according to the above method for allocating tokens to multi-order quantities of goods, and wherein:

- each second token comprises at least the public indicium of a respective pair of said pairs of indicia;
- the second quantity associated with each second token comprises the respective physical asset; and
- the digital token associated with said respective pair of indicia comprises the respective first digital token.

Each respective digital token may comprise both the public indicium and private indicium.

The computer-implemented methods described above may further comprise retiring the digital token upon determining an expiry date of the physical asset associated with the respective digital token has expired. The computer-implemented methods described above may further comprise retiring the digital token upon successful verification of the public indicium.

In the computer-implemented methods, when applied to multi-order quantities of goods, all digital tokens may be retired where those digital tokens have not been verified (**unverified digital tokens**) and are tokens for which the second quantity associated with the respective unverified digital token is greater than the first quantity minus the second quantities associated with all digital tokens that have been successfully verified.

Advantageously, this enables digital tokens to be retired where the total amount of goods associated with validated tokens equals or exceeds the first quantity. This reduces the scope

for counterfeiting since counterfeit goods cannot be repeatedly produced carrying the same validation markings or tokens.

Also disclosed is a computer-implemented method for managing interactions with an asset, comprising:

- generating a physical token associated with a physical asset;
- generating a digital token associated with the physical token, the digital token being associated with product properties including:
 - owner information of an owner of the physical asset; and
 - a description of the physical asset;
- receiving a request for at least partial control of the physical asset (**requested control**), the request comprising a hash;
- verifying the hash using at least one of the digital token and owner information; and
- upon verification of the hash, transferring requested control to a transferee.

The product properties may comprise a plurality of controllable objects each associated with a usage flag having an active state and an inactive state, the requested control comprises a request for control of one or more of the controllable objects (**requested controllable objects**), the method further comprising:

- upon verification of the hash, allocating control to only those said requested controllable objects for which the usage flag is in the inactive state; or
- preventing verification of the hash if the requested controllable objects comprise at least one object for which the usage flag is active.

Advantageously, this ensures only one person or authorized process may have control of the asset, or parts of the asset.

Receiving the request for at least partial control may comprise receiving transferee information of the transferee, the method further comprising:

- storing transferee information of transferees permitted to have the requested control; and
- preventing transferring of the requested control if the transferee does not match transferee information stored for the requested control.

Advantageously, this ensures only certain parties may have control of the asset or part thereof.

The computer-implemented method may further comprise:

- receiving, upon completion of usage of requested control, a request to relinquish the requested control, the request comprising a relinquishment hash;
- verifying the relinquishment hash using at least one of the digital token and transferee information of the transferee; and
- upon verification of the relinquishment hash, relinquishing the requested control.

Advantageously, this enables control to be transferred back while the block-chain or DLT records control transfers or control transactions.

Also disclosed herein is a system comprising:

- memory; and
- at least one processor, the memory storing instructions that, when executed by the at least one processor, cause the at least one processor to perform the computer-implemented method described above.

Also disclosed is a non-transitory computer-readable medium having instructions stored thereon that, when executed by a system comprising a processor, cause the system to performed the computer-implemented method described above.

Brief description of the drawings

Some embodiments of the present invention will now be described, by way of non-limiting example only, with reference to the accompanying drawings in which:

Figure 1 is a flowchart of methods in accordance with the present teachings;

Figure 2 illustrates the principle functional modules and architecture of embodiments of the present invention;

Figure 3 depicts a subset of the layers of abstraction and encapsulation of embodiments of the invention;

Figure 4 depicts the encryption wrapper function that is used by the collected token to access the digital twin (e.g. an electronic description of particular attributes or characteristics of the asset) representing the underlying physical asset or the asset itself;

Figure 5 depicts how product property data from an off-chain buffer is encoded onto the token;

Figure 6 illustrates token collection; and

Figure 7 illustrates token validation.

Detailed description

Methods and systems disclosed herein enable a multi-order quantity of a good, (e.g. a bulk good such as ginseng) that is apportioned into smaller quantities in transit, to be monitored and to reduce the opportunity for sale of counterfeit quantities of the bulk good. In the description which follows, much of the discussion will make reference to a “bulk good” or “bulk goods”. It will be understood that this is for illustration purposes and the description should not be construed as being limited to bulk goods but instead to multi-order quantities of goods that can be divided – e.g. in the supply chain. Moreover, “bulk good” and “bulk goods” can mean the same thing, rather than the latter being the plural of the former, depending on context. Other methods and systems enable asset control and physical asset transfer, using a traceable pathway. Thus, embodiments enables product authentication (counterfeit detection), supply chain track and trace, and analytics of both engaged and converted customers.

The methods described herein may be implemented on a block-chain. Scalability, speed, and power consumption are dependent on the underlying block-chain selected for deployment. However, in point of principle, the present technology is block-chain agnostic.

Compared with alternative QR-tagging means, embodiments of the present technology require a second code/token — which may essentially be a private key — to be kept ‘private’ throughout the production of packaging or labels employing the technology. The present technology does not ensure that a ‘public’ QR code cannot be copied and/or reprinted on counterfeit goods. This may result in any public QR code being successfully reused in limited cases. However, because all instances of a public code will be invalidated by the first successfully scanned corresponding private code counterfeiting cannot successfully be achieved at scale and such counterfeits will be readily detectable.

Key to the technology is the allocation and maintenance of physical and digital tokens. A computer-implemented method 100 for allocating the tokens is provided in Figure 1. The method 100 applies to multi-order quantities of goods. The method 100 broadly comprises:

Step 102: generating a first token associated with a quantity of goods being sold – e.g. bulk goods or computer resources;

Step 104: generating two or more second tokens that are associated with the first token and respective quantities of the goods.

Step 102 involves generating first tokens that can be applied to first physical quantities of a good – hereinafter, the first physical quantity will be referred to as a "first quantity". The first physical quantity is a quantity of the good that can be separated into smaller quantities that can be separately sold or distributed. In the case of edible materials, for example, the first quantity may be a large volume of honey and the smaller, second quantities may be jars of honey that can be filled using the first quantity. In the case of physical computer resources, the first quantity may be processing time or capacity and the second quantities may be portions of the processing time or capacity.

After generating the first token, it is associated with the first physical quantity of a good (**first quantity**). That association can be on the first physical quantity of the good.

The first token is associated with a first digital token and with one or more product properties, the first quantity being at least one of said properties. Other properties include the provenance or origin of the first quantity of the first good, the first digital token, supply packaging date, expiry date and other properties depending on the goods in question.

Step 104 involves generating two or more second tokens for association with second physical quantities of the good (**second quantities**). The second quantities are portions of the first quantity. There may be any number of second tokens, from two to any greater number. In some instances, the maximum number of second quantities, and thus second tokens associated with the quantities, is dictated by the minimum saleable quantity of a particular good. For example, where the first quantity comprises a 20 L receptacle of honey, and the minimum saleable quantity of honey is 200 mL, the maximum number of second quantities and thus second tokens will be 100. Each second token is associated with a second digital token and each second digital token is associated with one or more product properties. As with the first tokens, at least one of the product properties for each second token is the respective second physical quantity of the good in question. Another product property for each

second token may be its respective second digital token. To avoid counterfeiting, the sum of all the second quantities associated with the second tokens cannot exceed the first quantity.

Without limitation, the second quantities may be equal, unequal or a plurality of different quantities as required. Moreover, a second quantity may itself be divided into further, smaller quantities. In other words, step 104 may be recursively applied to smaller and smaller quantities as needed. For each recursion, the "first token" and associated first quantity will be the second token and respective second quantity from the previous recursion – e.g., where the first recursion relates to the division of a first quantity into smaller second quantities, the next recursion will involve splitting one or more of the smaller second quantities into yet smaller quantities.

To further reduce the opportunity for counterfeiting, each of the first token and second tokens may be unique. Similarly, the digital tokens associated with the first token and second tokens may also be unique.

The principle components of a system 200 for implementing the method 100 – e.g. functional modules, which include physical components such as physical tokens – are presented in Figure 2. The system 200 comprises an encoding platform 202 that interfaces with a cloud system 204 to generate a given quantity of tokens corresponding to a quantity of bulk product or manufactured good (the "first quantity") – the "given quantity" may comprise second tokens or the first token and second tokens. The generated token may be transferred to a third party when the goods are purchased.

With further reference to Figure 1, in addition to implementing the method 100, the computer system 200 may also implement a computer-implemented method for transferring a physical asset. The method for transferal broadly involves:

- Step 102: generating public and private indicia – in embodiments, this is tantamount to generating a first token;

- Step 110: applying the indicia to the physical asset;

- Step 102: generating digital token(s) comprising at least current owner information the physical asset and being associated with, or comprising, the public and private indicia;

- Step 112: receiving a request to transfer the physical asset;

- Step 114: verifying the public indicium; and

- Step 116: updating ownership for the physical asset.

Step 102, when used in the context of asset transferal, involves generating a public indicium and a private indicium. The public indicium is available or accessible to third parties. This enables the public indicium to be verified by providing access to the private indicium. Therefore, ownership verification can be performed without necessarily having access to, and use or consumption of, the physical asset.

Generating a public indicium and private indicium per Step 102 in effect comprises generating a pair of indicia for each performance of the step. Each pair includes a public indicium and a private indicium and is associated with a corresponding digital token. The pairs of indicia and digital tokens are then allocated according to the method 100. In this case, each second token can include at least the public indicium of the relevant pair of indicia, the second quantity associated with each second token can include the respective physical asset, and the digital token associated with the relevant pair of indicia will comprise the first digital token.

To enable access to the public indicium, it is applied to a visible location associated with the physical asset per Step 110. For example public indicium may be applied on a locked, and tamper-proofed shipping container containing the physical asset or on the outside of sealed packaging containing the physical asset – similar to a barcode being available on the outside of packaging of goods bought of a supermarket. In contrast, the private indicium, while also applied to a location associated with the physical asset, is applied in a tamper-evident location. For example, the private indicium may only be accessible on breaking the tamper-proof seal on the shipping container mentioned above, or after opening the sealed packaging.

To ensure the public indicium, and thus ownership, can be verified, and to facilitate transferal of the asset, a digital token is generated per Step 102 – the one digital token may be generated for both the public and private indicia. The digital token is associated with both the public and private indicia and with one or more product properties. Given method 106 is a method for transferring ownership of the physical asset, at least one of the product properties the current owner information of a transferor – e.g. the owner of the physical asset.

On generation of the digital token associated with the public and private indicia, the digital token can be uploaded to a network – Step 118. Typical of block chain networks, the network may be a multi-node network. This enables ownership verification and other processes to be performed, and ownership details to be stored, at multiple nodes on the network. This makes falsification of ownership very difficult.

Once the digital token is accessible, a request for transferal of the physical asset can be received per Step 112. As mentioned above, ownership verification can be performed using the public indicium. As such, the request for transferal of the physical asset must include at least the public indicium and owner information of the transferee. On receipt of the request, the public indicium can be verified per Step 114 and current owner information can be updated with the owner information of the transferee.

The public indicium can be verified in a variety of ways. In one embodiment, the public indicium can be verified using the private indicium. In this case, the indicia form a pair and the person or party performing the verification will be the end user or their representative, since the private indicium is only available in the tamper-evident location – i.e. it will be evident if anyone other than the owner or their representative gains access to the private indicium.

In some embodiments, receiving the request for transferal according to Step 112 involves receiving a hash from the transferor, the hash being a hash of the digital token and/or ownership identifier of the transferor. The hash can then be verified according to Step 114, to verify the digital token and/or ownership identifier – i.e. the hash can be verified to verify the transferor is the current owner of the physical asset. Then, at Step 116, the current owner information can be updated using the owner information of the transferee,

Receiving the request for transferal per Step 112 may instead, or in addition, comprise receiving the digital token and current owner information. In this embodiment, verifying the public indicium according to Step 114 may comprise verifying, using a ledger stored on a node in the multi-node network, that the public indicium is associated with the digital token and the current owner information. In other words, verifying that the details are consistent. Assuming the verification is successful, the current owner information on the updated per Step 116 by updating the ledger with the owner information of the transferee.

The descriptions of the various steps set out above assumed that the verification steps are successful. It will be understood, that in the event that verification fails, no transferal or validation will take place.

Each token may be referenced by a two-part code having a public 206 and private 208 component (e.g. first token and second token, or "public indicium" and "private indicium" as described with reference to method 106). The token encapsulates a reference to a digital twin bearing one or more of the product's attributes or properties residing — if only implicitly — in the Digital Twin Runtime 210. At least one of the product properties will be its quantity. Interactions with the public code 206 on a product retrieve information from the scanning

hardware 212 and update the state of the digital twin 210. Analytics/artificial intelligence (AI) 214 engines may also update the state of the digital twin' — for example, invalidating codes on products that have exceeded their expiry date (also see 108 in Figure 1), have been reported as stolen, or that are flagged by the vendor as having been recalled. Scanning hardware or software 212 will alert the operator to critical changes in state when scanned. The private code or indicium 208 is essentially a private key that allows a recipient to collect the associated token. This act of token collection, whereby a transfer of the token on the block-chain 204 occurs, deactivates the public code 206 and retires the digital twin. Counterfeit copies of the public code will alert scanning hardware or software that the code is invalid when scanned.

Figure 3 depicts a subset of the layers of abstraction and encapsulation. A Physical Product 302 — which may represent a bulk good or bulk goods — corresponds to a physical tag (first token or public indicium – 208), which corresponds to a virtual token (first digital token – hosted in runtime 210), which identifies a unique digital twin of unspecified fidelity (e.g. product description or set of attributes). For example, a 100kg barrel of Manuka honey may be represented by a 100kg discrete token (T_0), and a unique digital twin encapsulating the products properties — its certifications, Unique Manuka Factor (UMF), residue tests, country of origin certificate, obfuscated geolocation of corresponding bee hive, etc. — combined with the product's state — its age, current location, data from associated IoT sensors, etc. The product's 100kg token may be transferred at time of purchase to a bottler who might divide the product into 1,000 100g bottles. Each bottle may be encoded with a division of T_0 , thus limiting the number of products that may bear that mark – the sum of all the bottles (i.e. second quantities) associated with corresponding second tokens does not exceed the first quantity, i.e. 100kg. In the process of dividing T_0 , the corresponding twin (i.e. digital token) is also divided and provisioned in the runtime environment – i.e. the first quantity associated with the first token is divided into second quantities associated with second tokens and the digital token associated with the first token is similarly associated with corresponding second digital tokens associated with the second tokens. They inherit the properties of T_0 (possible with the exception of the size of the quantity) and abide until either the corresponding token has been collected, or the runtime flags the product as having expired or being otherwise removed from the supply chain.

Figure 4 depicts the encryption wrapper function 400 that is used by the collected token to access the digital twin. A key pair 402 and 404 provided by the token encrypts input and output to the runtime environment's secure process 406. Data 408 may be written from the

runtime process in either encrypted or unencrypted form — or otherwise displayed as unencrypted output 410.

Figure 5 depicts how product property data from an off-chain buffer is encoded onto the token. A key pair 500 controlled by the product producer is used to digitally sign data 501 – e.g. ownership details and/or quantity of goods and, in some embodiments, other product details etc – along with a hash of this data 502. A reference to this signed data — which may or may not also be encrypted — is stored on a DLT/Block-chain 504. The private key of the key-pair in data 502 is contained in QR Code 2 506 which is incorporated into product packaging or associated documentation in such a way so as to be physically obscured to all but the consumer/recipient – tamper-evident position associated with the assert. A scanning device scans the public code 500. If the associated private code has already been registered as having been collected, the product is deemed to be inauthentic. If the associated token is intact, the product is deemed to be authentic. The digitally-signed product properties may also be verified at this stage. This is set out in Figure 7, that illustrates process 700 in which a public code is scanned (702), if the private code has been collected (704) and the public code is flagged as invalid (706) and the process 700 ends. Otherwise, a check is conducted of whether the associated digital token is accurate (708). In the event that the digital token is inaccurate then the public code is flagged as invalid (706) in the process 700 ends. Otherwise, the code is validated (710).

Following Figure 6, token collection involves a reversal of this process, whereby the collecting device verifies the authenticity of the token — and thereby the associated product.

The tagging technology described above has the potential for broad application to physical products. Possible use cases include, but are not limited, to counterfeit detection, inventory management, asset management, and supply chain track and trace, parcel tracking, delivery receipt confirmation, aid distribution. The tagging system can also help facilitate the association of trusted digital twins with physical products and enable the registration of physical things on a block-chain.

In the context of counterfeit detection, at most only a single duplicate can be sold. On verifying the public and private keys/tokens, or first and second tokens, the keys/tokens may be retired, thereby preventing further verification of the same details. Moreover, the counterfeit cannot be beneficially generated by the owner since they cannot sell the legitimate asset after having sold the counterfeit. Counterfeits are therefore greatly limited in number and the parties that can derive benefit.

The above methods can be employed in distributed asset ownership networks. In this context, the token is essentially a static description of an 'object' – i.e. one or more product properties – in the context of object oriented programming and may be conveniently represented by JSON (JavaScript Object Notation), or other object notational code. In any case, the code is block-chain-secured or secure ledger secured so that instances of it cannot be arbitrary and must be authorised (either by the asset's owner directly or by an authorised piece of software that the owner authorises like a smart contract). The token implicitly cojoins *object* with *ownership*.

Software objects achieve their advantages most directly by encapsulating their data and implementation. Data is never manipulated directly — only through designated functions or 'methods' — and making use of an object does not require knowledge of how these methods operate internally. Only the existence of a given method, its accepted values, and its expected returned values need to be known.

The block-chain-secured token (uploaded under step 116 of Figure 1) instantiates the software object relating to the physical object while providing encrypted channels for interaction through a key pair — thus creating an interface analogous to an API. Access to this 'API' may be controlled according to the preferences or policies of the owner. Public access may be conditional and controlled through an instrument such as a smart contract.

The object may be a durable or consumable good, an aggregate quantity of goods in a tokenized package, or a machine capable of being interacted with. IoT instrumentation and control systems comprising or integrated with the product or machine may be accessed through the API provided by the token.

In one example, an owner of a fleet of vehicles (physical assets), having been so tokenised, may have private access whereby they may allow or disallow their operation. An owner may delegate access to certain features like maintenance staff to monitor vehicle systems and operations staff to monitor location, and may grant access to certain information to third parties willing to accept owner-defined access terms: insurers, planners, analysts, etc. In this way, third-party access to controlled information about these resources may be monetized.

In another example, in a property development, individual properties can similarly be tokenised. Possession of or delegated access to the token would allow interacting with the IoT-enabled appliances of a property to control lighting levels, monitor surveillance, and so

on. The token could also be linked to registration of ownership and represent a functional 'smart deed'. Anonymised and aggregated data on occupancy characteristics could be sold to developers, property speculators, city planners, insurers, and marketers to better understand the use and value of properties at the discretion of the token owner by enabling such access.

The benefits of access to such data include reduced risk, reduced data collection costs and increased response rates compared with surveys, alternatives to data streams — such as those available through cellular telephones. Owners may benefit from an additional income stream, reduced insurance premiums, reduced security costs with increased efficiency.

In yet a further example, a datacenter may tokenize bare-metal computing resources and transfer their tokenized representations to customers for interacting with these systems. A block-chain-secured token linked to a particular set of hardware would allow customers to be assured their application was hosted on a private system if required for security, compliance, or performance. Access to such verifiable resources could be sold upstream for connection to a leading cloud vendor. Access computer resources performing high-density compute services (engineering simulation, video compression, 2D or 3D rendering, AI, crypto currency mining, etc.) could be transferred or leased to operators through the exchange of the tokenized interface.

In the above example, such tokens may also be used to securitize assets whereby the token (e.g. second token) would represent a share in the ownership of an asset, and revenue generated from the operation of that asset may be transmitted or made available to the token holder through means of the described API.

A plurality of tokens may be aggregated together in a software 'wallet' such as that indicated by 212 in Figure 2, and form a composite API allowing collectivized interaction. Extending the example above, the collective memory, computing power, or disk space of all tokenized resources may be displayed as if they were a single integrated system. This allows for the verifiable presence and capacity of computing resources, having benefits in resource management, insurance, compliance, auditing, and so on. It will also ensure that when assets are replaced or repaired, the repaired asset matches that which was removed for repairs and asset replacements meet or exceed the specifications of the assets they replace.

In a further example in which there are beehives in an apiary — particularly those devoted to high-value terroir honey — equipped with IoT instrumentation recording sound, light, humidity, temperature, weight, geolocation, the presence of particular honey bee pheromones, and so on, the data may be similarly tokenized to provide collective monitoring, leased operation, and validation of the product of those hives. Moreover, by providing verifiable and non-falsifiable references to the underlying assets, such a token provides a mechanism for distributing the ownership of assets and thereby spreading risk.

In all of the above examples, digital twins of the respective assets may be instantiated in a runtime environment from the object representations encoded on their respective block-chain-secured tokens. These instantiations may replicate the functioning of their physical objects in digital space or be used to run simulations of how different scenarios may effect the physical objects in questions. In all cases, a clear distinction is made between the verifiable identity of authentic twins — as linked to a block-chain-secured token — and copies of that instance that may exist for purposes of simulations.

The digital token should be linked with physical assets, as described with reference to Figure 1. The digital token application program interface (API) may be linked to a machine or other physical asset (particularly an internet-enabled one) through a software module, plugin, or device driver installed as part of the hardware, software, or firmware of that machine. The plugin verifies the profile of the hardware, and integrates with a Trusted Computing Platform (TCP), if available or other Entity Attestation Token (EAT). The code of the associated plugin should be publically available and formally verifiable — i.e. public token. Its primary function is to associate hardware identifying characteristics — which may be in the form of hardware profiles, operating parameters, operating cycles, or unique serial numbers. This is facilitated by the fact that network connected hardware already includes individually unique hardware addresses like media access control (MAC) addresses or wireless IDs or operating parameters and characteristics as determined by a silicon batch. The platform may thereby readily detect if a given hardware profile has substantially deviated from its unique network ID. This plugin component shall be minimal and portable to readily facilitate vendor integration. It may also be documented in such a way that hardware vendors may supply their own implementations, provided such code is public and verifiable.

The present tagging technologies provide a large number of benefits, particularly low cost, flexibility of implementation, and integration with existing technology. The tagging technology requires, at minimum, only printable barcodes (conventional or matrix) or other printable indicium and can be printed directly onto product packaging or etched into material

surfaces. Higher levels of security and additional features may be achieved through the use of RFID tags or other types of programmable tags, but these are not required. It is expected that all such variations of the type of visible indicia will be apparent to the skilled person in view of the present teaching.

The tagging medium is not fixed and tags could also be implemented through intaglio printing processes, laser etching, holograms, or other any other process capable of imprinting barcode or matrix barcode data. This feature lends a flexibility of implementation to the tagging technology. Tags may be attached to product labels if printing technology of a customer does not support variable data printing (VDP).

Moreover, organic materials – e.g. wood grains or other plant specimens, food stuffs, minerals, and so on, or manufactured goods with intrinsic and reliable irregularities such as tooling and finishing marks, brush strokes, inscriptions, and so on, having fixed and unchanging physical characteristics — which may be visible to the naked eye, microscopic, or nano-structural may be understood to be implicitly 'tagged' by virtue of their unique characteristics which may be recordable and storable in the form of a digital token. In such a case, no physical tag may be required and the discernible attributes of the given material (in this embodiment being the generated public token) may be encoded in a digital token through reference to a designated portion or specimen. In this case the object or material's unique discernible qualities constitute the public indicium and thus there is no required outward physical tag. A private indicium will be integrated with the product as before for purposes of recording and transferring ownership.

Because tags are not 'activated' on the block-chain until the finished product is accepted into the supply chain, the block-chain records are protected from errors arising from human error, misprints, or other malcoding. If a misprint occurs, the manufacturer does not absorb the cost of an encoded product.

In some embodiments, the present tag includes an imbedded token block-chain-secured token which can be collected by the purchaser. This token collection functions to alert the platform of the acquisition of a product, implement an incentive mechanism increasing consumer engagement and brand loyalty, and enabling fine-grained data collection of data on customers who have actually purchased a good.

The present product tagging scheme is able to record proof of receipt or proof of consumption of a good, thus enabling a higher fidelity of supply chain insight. The present focus on

enabling digital twinning also provides a degree of interaction, visualization, and simulation currently unavailable for consumer products.

In some embodiments, the public indicium and private indicium (public-private QR code) may be serialized. This can assist with proving consumption, customer conversion analytics, providing a robust mechanism for deactivating public code thus preventing public code duplication and enabling smart packaging features.

The private indicium may comprise a non-replicable token. For example, a non-replicable token may be embedded in private QR code. This can provide an incentivizable mechanism for ensuring consumer engagement.

The presently disclosed process of digital twinning of tokenized assets provides enhanced business intelligence, scenario testing, and supply chain modelling, AR/VR visualisation.

Token possession may be used to read or set attributes of product's digital twin. This facilitates enablement of smart packaging features: e.g., if a product is recalled, that change in state may be communicated to all effected products instantly. In addition, if the tokenized item is a machine, computer system, or smart contract, possession of the token may enable secure access to device management and outputs.

With further reference to Figure 1, each of the above examples may be implemented through various paths of flow chart 100. At step 102, a first token is generated. The paths of the flow chart include methods computer-implemented methods for allocating token to quantities of bulk goods such as honey or ginseng, for transferring a physical asset or control thereof or for managing interactions with an asset (i.e a physical asset). The first token may be associated (e.g. attached to) a physical quantity of a bulk good (first quantity) such as honey or ginseng, a vehicle in a fleet, a computer or other system capable of remote operation. The first token is, as context provides, a physical token such as a QR-code, barcode, RFID tag and the like, and as such constitutes a public indicium (e.g. public key, for encrypted indicia/tokens, or both public and private keys/indicia for some embodiments where dual-tokenisation is provided).

The first token is associated with a first digital token. The first digital token may be referred to as a digital twin, and may provide access to a product description comprising one or more product properties or characteristics – e.g. type of product, volume or weight of product, expiry date, vehicle make, vehicle year, and so on. For the first digital token, one property may be the second digital tokens for quantities of bulk good taken from the original quantity. Similarly,

for second digital tokens, a property may be the corresponding first digital token. This enables tracing of provenance.

Step 104 comprises generating second token(s). In the case of separating bulk goods into smaller quantities, there will be plural second tokens each of which is associated with a respective second digital token generated at step 106, and a second quantity of the bulk good that is less than the first quantity. As such, each second digital token is associated with a similar product description to that provided for the first digital token.

Relevantly, the second quantities may be equal, unequal or simply of various different quantities as required. Importantly, however, the sum total of the second quantities associated with the apportioned bulk good cannot exceed the original quantity. In the above Manuka honey example, the total weight of Manuka honey associated with the second tokens must not exceed 100kg. If that weight is exceeded, it is known that some counterfeiting is likely to have taken place – e.g. non-Manuka honey sold as Manuka honey.

Per step 108, digital tokens may be retired upon validation, upon determining an expiry date of the physical asset associated with the respective digital token, such as Manuka honey or ginseng, has expired. In other embodiments, on point-of-sale or transfer of ownership, step 108 may involve retiring all digital tokens that have not been verified (**unverified digital tokens**) for which the second quantity associated with the respective unverified digital token is greater than the first quantity minus the second quantities associated with all digital tokens that have been successfully verified. This ensure that, for example, 100kg of Manuka honey can ultimately only be associated with 100kg of Manuka honey sold.

To reduce the likelihood that counterfeit products can be sold and validated in advance of legitimate products, by reproduction of the second tokens, each first token and/or second token may be unique. Uniqueness may result from the tokens not being sequential or otherwise forming a series. Similarly, each first digital token and/or second digital token may be unique.

Where the first token is a public indicium, the second token may be a private indicium (e.g. private key). This may be stored inside packaging, on a tear-away wrapper and the like, as discussed above, so that only the public indicium is accessible without tampering with the asset or bulk good, or its packaging. Thus, per step 110, the public indicium is applied to a visible location associated with the physical asset – e.g. on an outer surface of the product

packaging – and the private indicium is placed in a tamper-evident location – e.g. within the packaging prior to the packaging being sealed.

To monitor the transferal of goods down a distribution channel, one of the product properties associated with the digital token generated at step 102 may be current owner information of a transferor – i.e. a party that is to transfer the associated asset to another party.

To transfer the asset, a request for transferral of the physical asset is received per step 112. The request will typically include the public indicium and owner information of a transferee. The public indicium can be supplied since it is visible on the packaging. Since the private indicium remains inaccessible, ownership can be transferred by verifying the public indicium – per step 114 – without any party requiring access to the private indicium. On transferral, the current owner information is updated with the owner information of the transferee – step 116.

In some cases, such as at point-of-sale, the asset travelling with the public indicium is desired to be verified as authentic. To do so, step 116 may actually involve verifying the public indicium using the private indicium as shown in Figure 4. For example, the public indicium on the outside of packaging may be verified by opening the packaging and scanning the private indicium accessible therein.

The track the ownership of a product the digital token may be uploaded to a multi-node network per step 118. In this regard, receiving the request for transferral further can include receiving a hash from the transferor, verifying the public indicium can include using the hash to verify the public indicium, and updating the current owner information with the ownership identifier can include updating the current owner information with hash and the ownership identifier. In some cases, the hash is used to verify the transferor is a current owner of the physical asset. For example, where the multi-node network is a block-chain or distributed ledger, the hash may comprise a hash of at least the current owner information – e.g. name or key – and the digital token. The hash can then be rehashed with the next owner's information so that previous hash results cannot be changed without changing all related, previous hash values in the network.

In other embodiments, a centralized trust server can be used in place of repeated hashing, to verify ownership. For example, receiving the request for transferral can include receiving the digital token and the current owner information, and verifying the public indicium can then comprise verifying, using a ledger stored on a node in the multi-node network (e.g. a centralised trust server node), the public indicium is associated with the digital token and the

current owner information. Thereafter, as per the method previously described, the current owner information can be updated with the ownership identifier comprises updating the ledger with the owner information of the transferee.

While ownership tracking has been described in relation to a single asset, it will be understood that the second tokens, described with reference to apportionment of bulk goods, may be a pair of indicia comprising a public indicium or key, and a private indicium or key. The pairs are then associated with a respective digital token and distributed as described above for step 106. Thus, each digital token comprises or is associated with a public-private indicium pair.

In managing interactions with an asset, the first token can be associated with the asset and the corresponding first digital token can be associated with the product properties – e.g. owner information and description of physical asset. In some instance, such as remote monitoring of vending machines, remote interaction with computer resources and the like, a request will be received for at least partial (which includes full) control of the physical asset – e.g. from a remote location – per step 120. In this case, to enable implementation on a block-chain or distributed ledger, the request may comprise a hash.

The hash may be verified per step 122, as discussed above, using the digital token and owner information and, upon verification of the hash at step 124, the requested control can be transferred to the transferee or requestor.

Where the product properties make evident that the asset has multiple, separately controllable components or objects – e.g. partitions in a computer resource – each component or object may have a usage flag associated with it. The usage flag can be used to indicate whether or not the particular component or object is in use – the "active" state – or whether it is available for use – the "inactive" state. Therefore, transferal of control may involve transferal of control of only the specific objects or components identified in the request, and only if those objects or components are in the inactive state. Where only some objects or components are in the inactive state, control may only be transferred for those inactive components. Similarly, per step 128 control may be prevented where one or more of the objects or components is in the active state.

Moreover, some assets and components thereof should only be controlled by particular parties. To this end the request received at step 120, may include transferee information of a transferee or requestor. Information for authorised parties – e.g. transferees or requestors who may have access to the asset or its components – may be stored in memory (e.g. on the

RootChain Cloud 2), with control being prevented for all transferees whose information does not appear in that memory against the particular asset or components for which control is sought.

Upon completion of usage of the control of the asset, the previous transferee, now the transferor, may send a request to relinquish the requested control – step 130. The request may include a relinquishment hash that can be verified using the digital token and the transferee's (now transferor) information per step 132 and, upon verification control can be relinquished – i.e. returned to the original transferor or owner per step 134.

The paths shown in Figure 1 may be implemented on the system shown in Figure 2, comprising the memory provided in the RootChain cloud 2 or elsewhere, and the processor or processors available in the RootChain Cloud 2 or in the front end. Similarly, the instructions for performing those methods may be readily contained in a computer-readable medium, for transferal to, or execution by, a computer system.

Throughout this specification and the claims which follow, unless the context requires otherwise, the word “comprise”, and variations such as “comprises” and “comprising”, will be understood to imply the inclusion of a stated integer or step or group of integers or steps but not the exclusion of any other integer or step or group of integers or steps.

The reference in this specification to any prior publication (or information derived from it), or to any matter which is known, is not, and should not be taken as an acknowledgment or admission or any form of suggestion that that prior publication (or information derived from it) or known matter forms part of the common general knowledge in the field of endeavour to which this specification relates.