CLAIMS

What is claimed is:

1. An artwork validation system comprising:

a public tag (110) physically attached to an asset (105) comprising a first unique identifier (210) associated with the asset;

a certificate of authenticity (185) comprises a second unique identifier (215); and,

a centralized server (140) comprises:

a communication module (125) configured to transmit and receive data via a communication network (145);

a data store (315, 325) comprising a program of instructions and an asset profile (350) comprises an ownership information and registered association between the first unique identifier and the second unique identifier; and,

a processor (305) operably coupled to the data store such that, when the processor executes the program of instructions, the processor causes operations to be performed to automatically authenticate an ownership of the asset attached to the public tag, the operations comprising:

receive, from a user device, a private scan data from the certificate of authenticity via the communication module (805), wherein the private scan data comprises a private unique identifier;

authenticate of the certificate of authenticity using an authentication engine as a function of the private unique identifier (810) and user input;

after the certificate of authenticity is authenticated, generate a request signal to the user device to request a public scan data (820);

receive, by scanning the public tag, a public scan data from the users device within a predetermined time via the communication network (825); and,

authenticate the public tag as a function of a public unique identifier of the received public scan data and the asset profile (830);

if, based on the uniquely registered association, the public unique identifier is associated with the private unique identifier, generate a signal granting modification rights to the user device to the asset profile (835), such that a modification to the ownership information of the asset is generated only when the centralized authentication server validates the certificate of authenticity and the public tag within the predetermined time period.

2. The artwork validation system of claim 1, wherein the public tag further comprises a position sensor configured to transmit a location of the asset to the central authentication server, and a gyroscope configured to activate the position sensor upon detection of movement, wherein:

upon receiving the location of the asset, the central authentication server is configured to determine whether the location is within a predetermined geofence, and generate a signal to block future modifications of the asset profile if the location is out of the predetermined geofence, such that potential theft of the asset is prevented.

3. The artwork validation system of claim 2, wherein the position sensor comprises a GPS tracker device.

4. The artwork validation system of claim 1, wherein the public tag comprises a RFID chip.

5. The artwork validation system of claim 1, wherein the second unique identifier is stored in a cryptographic format in that certificate of authenticity, such that the unique identifier is revealed only upon decryption using a private key received from the user device.

6. The artwork validation system of claim 1, wherein the operations comprise:

upon receiving a modification to the ownership information of the asset, generate an authorization request signal to a current owner's device to complete the modification.

7. The artwork validation system of claim 1, wherein the asset profile further comprises a ledger data comprising transaction history of the asset, wherein, after a transfer of ownership of the asset is completed, the operations further comprises generating new entries at the ledger data based on a set of predetermined compensation rules associated with selected entities comprise historical owners of the asset, galleries associated with the asset, and a creator of the asset.

8. The artwork validation system of claim 1, wherein the asset profile further comprises a public narrative customizable by an authenticated user associated with the asset, wherein:

when the public scan data is received from a mobile device before any private scan data is received from the mobile device, the processor is configured to perform public narrative operations comprise:

determine an asset associated with the public scan data based on a unique identifier decrypted from the public scan data, and,

generate a display comprising the public narratives associated with the asset at the mobile device.

9. A computer-implemented method performed by at least one processor to automatically authenticate an ownership of an asset attached to a public data chip (110), the method comprising:

receive, from a user device, a private scan data of a certificate of authenticity of a private data chip (805), wherein the private scan data comprises a private unique identifier (215);

authenticate of the certificate of authenticity using an authentication engine as a function of the private unique identifier and user input (810);

after the certificate of authenticity is authenticated, generate a request signal to the user device to request a public scan data (820);

receive, from the user device, a public scan data by operating a public tag fixedly attached to a tangible asset within a predetermined time period (825);

retrieve a uniquely registered association between the private unique identifier and an associated unique identifier (830); and,

if the associated unique identifier is equal to a unique identifier (210) of the received public scan data (835), authenticate the public tag and generate a signal granting modification rights to the user device to an asset profile (350) comprising an ownership information (385) of the tangible asset, such that a modification to the ownership information of the asset is generated only when both the certificate of authenticity and the public tag are validated within the predetermined time period.

10. The computer-implemented method of claim 9, further comprises:

receiving a location signal of the public tag, wherein the location signal is activated upon detection of movement; and,

determine whether the location is within a predetermined geofence; and,

generate a signal to block future modifications of the asset profile if the location is out of the predetermined geofence, such that potential theft of the asset is prevented.

11. The computer-implemented method of claim 9, wherein the public tag comprises a RFID chip.

12. The computer-implemented method of claim 9, wherein the private unique identifier is stored in a cryptographic format in that certificate of authenticity, such that the unique identifier is revealed only upon decryption using a private key received from the user device.

13. The computer-implemented method of claim 9, further comprising,

upon receiving a modification to the ownership information of the asset, generate an authorization request signal to a current owner's device to complete the modification.

14. The computer-implemented method of claim 9, wherein the asset profile further comprises a public narrative customizable by an authenticated user associated with the tangible asset, wherein the method further comprises:

upon receiving the public scan data from a mobile device before any private scan data is received, determine an asset associated with the public scan data based on a unique identifier decrypted from the public scan data, and,

generate a display comprising the public narratives associated with the asset at the mobile device.

15. A computer program product comprising a program of instructions tangibly embodied on a non-transitory computer readable medium wherein, when the instructions are executed on a processor, the processor causes authentication operations to be performed to automatically authenticate an ownership of an asset attached to a public data chip, the operations comprising:

receive, from a user device, a private scan data of a certificate of authenticity of a private data chip (805), wherein the private scan data comprises a private unique identifier (215);

authenticate of the certificate of authenticity using an authentication engine as a function of the private unique identifier (810) and user input;

after the certificate of authenticity is authenticated, generate a request signal to the user device to request a public scan data (820);

receive, from the user device, a public scan data by operating a public tag fixedly attached to a tangible asset within a predetermined time period (825);

retrieve a uniquely registered association between the private unique identifier and an associated unique identifier (830); and,

if the associated unique identifier is equal to a unique identifier (210) of the received public scan data, authenticate the public tag and generate a signal granting modification rights to the user device to an asset profile (835) comprising an ownership information of the tangible asset, such that a modification to the ownership information (385) of the asset is generated only when both the certificate of authenticity and the public tag are validated within the predetermined time period.

16. The computer program product of claim 15, further comprises:

receiving a location signal of the public tag, wherein the location signal is activated upon detection of movement; and,

determine whether the location is within a predetermined geofence; and,

generate a signal to block future modifications of the asset profile if the location is out of the predetermined geofence, such that potential theft of the asset is prevented.

17. The computer program product of claim 15, wherein the public tag comprises a RFID chip.

18. The computer program product of claim 15, wherein the private unique identifier is stored in a cryptographic format in that certificate of authenticity, such that the unique identifier is revealed only upon decryption using a private key received from the user device.

19. The computer program product of claim 15, further comprising,

upon receiving a modification to the ownership information of the asset, generate an authorization request signal to a current owner's device to complete the modification.

20. The computer program product of claim 15, wherein the asset profile further comprises a public narrative customizable by an authenticated user associated with the tangible asset, wherein the operations further comprise:

upon receiving the public scan data from a mobile device before any private scan data is received, determine an asset associated with the public scan data based on a unique identifier decrypted from the public scan data, and,

generate a display comprising the public narratives associated with the asset at the mobile device.