SYSTEM AND METHOD FOR AUTHENTICATING PROVENANCE OF DIGITAL TOKENS

FIELD OF THE INVENTION

[001] Present invention relates to a system and method for establishing provenance of blockchain based digital tokens and their underlying assets including the authentication of the transaction history and authorship of the digital tokens by maintaining immutable records.

BACKGROUND OF THE INVENTION

[002] Digital tokens/hashes of data are replacement of data, through cryptographic techniques, with unique identification symbols that retain all essential information about the data without compromising its security. The blockchain ecosystem allows the creation and transaction of the digital tokens such as Fungible and Non-Fungible Tokens (NFTs). Fungible tokens are interchangeable (identical) and divisible, while NFTs are unique digital items that represent ownership or proof of authenticity for digital or physical assets of an owner.

[003] Typically, the digital tokens are stored in a blockchain network. In a blockchain network the token creation process is referred to as minting. Once the digital token is minted, it can be made available to be transacted. For example, it can be published in a marketplace with its price and description as per owner's requirement. Digital tokens are synonymous with immutability, since they are minted in the blockchain.

[004] However, the security implicit in the blockchain does not carry over automatically to digital tokens, whose provenance falls only partially under the blockchain. These security challenges are numerous, leading to the proliferation of fake and duplicate digital tokens, even in the largest digital token marketplaces. There is also the problem of authenticating, accounting for and tracking multiple "digital tokens" pertaining to a digital asset, which may be traded across multiple marketplaces and / or blockchains. This is a common occurrence with intangible assets. The lack of a solution to this problem severely restricts trading of digital tokens on a global scale. Moreover, the underlying asset of the digital token, typically resides off-chain (for e.g., land records, contracts and commercial documents, KYC documents, and software) whose characteristics may legitimately change over time, while the corresponding digital tokens are static entities residing on the blockchain. Existing systems for creating digital tokens are incapable of tracking and

authenticating these changes. These problems become more acute when multiple digital tokens pertaining to the same underlying asset are involved.

[005] Thus, there is a need in the art for a system and a method for establishing the provenance of blockchain-based digital tokens and their underlying assets including the authentication of the transaction history and authorship of digital tokens that addresses at least the aforementioned problems and limitations.

SUMMARY OF THE INVENTION

[006] In one aspect, a system for authenticating provenance of a digital Token for a digital asset is disclosed. The system comprises a seller device communicatively coupled to a server and to a trading platform such as a digital marketplace. The seller device comprises a processor configured to create or select the digital asset to be traded on the digital marketplace and determine the asset metadata of the digital asset. The processor is then configured to generate a first hash of the asset metadata and a second hash of the digital asset through a hashing service on the server. A hash function is applied by the processor to the first hash and the second hash for generating a first metatoken and then store the first metatoken on the seller device and/or the server. Thereafter, the digital asset is embedded by the processor with the first metatoken to obtain a marked-up digital asset. The marked-up digital asset is then transmitted by the processor to the digital marketplace for minting the digital token of the digital asset along with the digital token metadata pertaining to the minted digital token. A third hash of digital token metadata pertaining to the minted digital token is then generated by the processor through the hashing service on the server. Subsequently, a hash function is applied by the processor to the third hash and the first metatoken to generate a second metatoken and store the second metatoken in the server. The second metatoken and the first metatoken are appended to the metadata of the minted digital token and stored on the digital marketplace, allowing a prospective buyer to authenticate provenance of the minted digital token based on the first metatoken and the second metatoken.

[007] In an embodiment, the processor is configured to receive the digital asset from the owner of the digital asset. The digital asset corresponds to one of an art, music, video, 3D metaverse, and documents. The asset metadata corresponds to owner ID, type of file, creation date, modification date, file size, title, asset dimensions, and digital information. The digital token metadata corresponds to attributes of the digital marketplace.

[008] In an embodiment, the processor is configured to embed the first metatoken with the digital asset as a binary data and store the marked-up digital asset in a storage unit of the seller device.

[009] In an embodiment, the processor is configured to receive a request for authenticating provenance of the digital token from a prospective buyer. The processor upon receiving the request is configured to generate a first reference metatoken by accessing the digital asset and a second reference metatoken based on the first reference metatoken and reference hash of the metadata of the digital token.

[010] In an embodiment, the processor is configured to determine the digital token to be authentic if the second reference metatoken matches with the second metatoken. The digital token is determined to be unauthentic if the first reference metatoken and the second reference metatoken do not match with the first metatoken and the second metatoken respectively. The digital token is determined to be altered if the first reference metatoken matches the first metatoken, while the second reference metatoken does not match with the second metatoken.

[011] In an embodiment, the processor is configured to generate and transmit a first transaction data along with the second metatoken to a buyer device upon purchase of the digital token. A first transaction hash pertaining to the first transaction data is then generated by the processor. Thereafter, a hash function is applied by the processor to the first transaction hash and the second metatoken to generate a third metatoken. The third metatoken is stored in the server by the processor. The processor then appends the digital token with the third metatoken to generate an appended digital token. The appended digital token with the third metatoken is stored in the digital marketplace by the processor.

[012] In an embodiment, the server corresponds to a first blockchain server and the digital marketplace corresponds to a second blockchain server.

[013] In another aspect, a method for authenticating provenance of a digital token for a digital asset is provided. The method comprises a processor of a seller device in communication with the server and the digital marketplace, that is configured to create or select the digital asset to be traded on the digital marketplace and determine the asset metadata of the digital asset. The processor is then configured to generate the first hash of the asset metadata and the second hash for the digital asset through the hashing service on the server. The hash function is applied by the processor to the first hash and the second hash for generating the first metatoken and store the first metatoken on the seller device and/or the server. Thereafter, the digital asset is embedded by the processor with the first metatoken to obtain the marked-up digital asset. The marked-up digital asset is then

transmitted by the processor to the digital marketplace for minting the digital token of the digital asset along with the digital token metadata pertaining to the minted digital token. The third hash of digital token metadata pertaining to the minted digital token is then generated by the processor through the hashing service on the server. Subsequently, the hash function is applied by the processor to the third hash and the first metatoken to generate a second metatoken and store the second metatoken in the server. The second metatoken and the first metatoken are appended to the minted digital token and stored on the digital marketplace, allowing a prospective buyer to authenticate provenance of the minted digital token based on the first metatoken and the second metatoken.

BRIEF DESCRIPTION OF THE ACCOMPANYING DRAWINGS

[014] Reference will be made to embodiments of the invention, examples of which may be illustrated in accompanying figures. These figures are intended to be illustrative, not limiting. Although the invention is generally described in context of these embodiments, it should be understood that it is not intended to limit the scope of the invention to these particular embodiments.

Figure 1 shows a block diagram of a system for establishing provenance of a digital token and its underlying asset, including the authentication of its transaction history and authorship, in accordance with an embodiment of the invention.

Figure 2 shows a flow diagram of a method for establishing the provenance of the digital token, in accordance with an embodiment of the invention.

Figure 3 shows a flow diagram of a method for establishing the provenance of the digital token, in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

[015] Various features and embodiments of the present invention here will be discernible from the following further description thereof, set out hereunder.

[016] The present invention is directed towards a system and a method for establishing the provenance of digital tokens such as Fungible tokens and Non-Fungible Tokens (NFTs) and their underlying assets, including the authentication of their transaction history and authorship, to be traded on a blockchain based trading platform such as a marketplace. The digital token generated can be authenticated by the invention, thereby ensuring transactions of genuine digital tokens in

the marketplace. The system and the method are also configured to track one or more multiple digital tokens pertaining to the digital asset which may be traded across multiple digital marketplaces.

[017] The system in the present invention comprises a processor of the seller device configured to create a digital token of a digital asset to be traded on the marketplace. A first hash of metadata of the digital asset and a second hash of the digital asset is generated or created by the processor. The processor is then configured to generate a first metatoken of the first and second hashes by applying a hash function. The processor is then configured to embed the digital asset with the first metatoken. The processor then transmits the marked-up digital asset to the marketplace for minting the digital token. Subsequently, the processor is configured to append the minted digital token with the first metatoken to the marketplace. The processor through the hashing service generates or creates a third hash of the metadata of the digital token minted in the marketplace. The processor then generates a second metatoken of the third hash along with the first metatoken. The processor then transmits the second metatoken to the server and also appends the second metatoken with the minted digital token and stores the appended second metatoken in the marketplace as well as the server.

[018] The method in the present invention comprises creating the digital asset to be traded on a trading platform such as a marketplace by the processor of the seller device. The first hash of the metadata of the digital asset and the second hash of the digital asset is then generated or created by the processor. The processor then generates the first metatoken of the first and second hashes by applying a hash function. The processor then embeds the digital asset with the first metatoken. The processor then transmits the marked-up digital asset to the marketplace for minting the digital token. Subsequently, the processor appends the first metatoken to the minted digital token in the marketplace. The processor through the hashing service generates or creates a third hash of the metadata of the digital token minted in the marketplace. The processor then generates a second metatoken of the third hash along with the first metatoken. The processor then transmits the second metatoken to the server and also appends the second metatoken with the minted digital token.

[019] Figure 1 is a block diagram of a system 100 for establishing the provenance of a digital token such as a Fungible token and a Non-Fungible Token (NFT) and its underlying asset, including the authentication of its transaction history and authorship, to be traded in at least one blockchain-based digital marketplace 140 in accordance with an embodiment of the present invention. The digital asset includes assets such as video, image, document, data, social media

feed, 3D file and the like. The digital asset can include digitized/tokenized records of physical assets such as movable/immovable property - houses, cars, and documents.

[020] The system 100 comprises a seller device 110 and a buyer device 150 in communication with a blockchain-based server 120 and at least one blockchain based trading platform such as a digital marketplace 140. The seller device 110 may be a device of an owner of the digital asset wishing to generate the digital token, and the buyer device 150 may be a device of a user wishing to authenticate and/or purchase the digital token. The seller device 110 and the buyer device 150 can be selected from any electronic device such as a laptop, a desktop, or any other computing device that is capable of implementing instructions of system 100. Accordingly, the devices 110, 150 comprise a processor, memory, a storage unit, a communication module, a display device, input and output units etc. The seller device 110 through the communication module communicates with the server 120 and the digital marketplace 140. In an embodiment, the seller device 110 communicates with the server 120 and the digital marketplace 140 over a network (not shown). The network can be a wired network and/or a wireless network having a variety of network devices such as routers, bridges, modems and the like, and the communication module is configured based on the network requirements. The network can be implemented as intranet, Local Area Network (LAN), Wide Area Network (WAN), the internet and the like using different protocols for example Hypertext Transfer Protocol (HTTP), Transmission Control Protocol/Internet Protocol (TCP/IP), Wireless Application Protocol (WAP), and the like.

[021] In an embodiment, the seller device 110 may comprise a dedicated application 130 stored within the storage unit which when executed establishes a communication link with the server 120 and the digital marketplace 140. The seller device 110 through the application is configured to allow the owner to generate the digital token of the digital asset. In an embodiment, the digital marketplace 140 is connected with the server 120 via an Application Program Interface (API), wherein the server 120 comprises a hashing service.

[022] In an embodiment, the buyer device 150 may also comprise the dedicated application 130, which when executed establishes a communication link with server 120 and the digital marketplace 140. The buyer device 150 through the application may be configured to allow the buyer to access and check authenticity of the digital token of the digital asset prior to purchase.

[023] Further, the seller creates or selects the digital asset to be traded on the digital marketplace 140. Once the seller selects the digital asset, the processor of the seller device 110 is configured to instruct the dedicated application 130, within the storage unit to determine the asset metadata of

the digital asset. The asset metadata includes information pertaining to the digital asset for which the digital token is being generated. The asset metadata comprises information pertaining to type of file *i.e.* whether it is a video file, an audio file, or a document etc., size of the digital asset, name of author of the digital asset, time stamp of the digital asset, owner ID, modification date, title, asset dimensions, file type and the like. The asset metadata is transiently stored within the storage unit of the seller device 110.

[024] As discussed hereinbefore, the seller device 110 is network connected with the server 120, wherein the server 120 comprises a hashing service. Upon selecting the digital asset, the seller device 110 through the hashing service is configured to generate/create a first hash of the asset metadata and a second hash of the digital asset. In the present scenario, the system 100 generates the first hash and the second hash of the asset metadata and the digital asset. The system 100 is then configured to generate a first metatoken of the first hash and the second hash. The first metatoken is generated by tokenizing/hashing of the first hash and the second hash together. The first metatoken is stored in the server 120 and in the storage unit of the seller device 110. In an embodiment, the first hash and the second hash are generated through one or more cryptographic techniques stored in the server 120.

[025] The processor of the seller device 110 is configured to instruct the dedicated application 130 to embed the digital asset with the first metatoken through one or more embedding techniques known in the art. In an embodiment, the processor is configured to instruct the dedicated application 130 to embed the first metatoken with the digital asset as binary data to generate a marked-up digital asset. The processor is also adapted to store the first metatoken in the storage unit of the seller device 110 and the server 120. The processor is also adapted to store the marked-up digital asset in the storage unit. The marked-up digital asset is then transmitted to the digital marketplace 140 for minting the digital token. The owner of the digital asset can include a price as well as a description of the digital token while transmitting or minting the digital token. The minting of the digital token by transmitting the marked-up digital asset is carried out by conventional techniques known in the art for minting the digital token in the digital marketplace 140.

[026] Subsequently, the system 100 is configured to append the minted digital token with the first metatoken and is sent to the digital marketplace 140. The system 100 thereafter transmits the minted digital token metadata to the seller device 110 from the digital marketplace 140. The seller device 110 through the hashing service generates/creates a third hash of the metadata of the digital

token minted in the digital marketplace 140. The system 100 is configured to generate a second metatoken of the third hash along with the first metatoken. The second metatoken ensures that the information pertaining to the minting of the digital token such as digital token ID, metadata of the digital token, attributes of the marketplace such as its ID and the like are captured. This process establishes a link between the owner, digital token and the digital asset in the seller device 110 and/or in server 120. In an embodiment, metadata of the digital token corresponds to attributes of the digital marketplace 140. The system 100 then transmits the second metatoken to server 120 and also appends the second metatoken with the minted digital token and stores the appended second metatoken in the digital marketplace 140 as well as server 120. Thus, a prospective buyer is able to check or determine the provenance of the digital token and the digital asset before purchasing it. Consequently, the possibility of a transaction with a counterfeit digital token is mitigated through the system 100.

[027] In an embodiment, if the digital token is a fungible token, the system 100 based on the first hash of the asset metadata, an asset valuation document hash and a compliance hash (embedded in the digital asset and/or stored in the server 120 and/or the seller device 110) generates the first metatoken. In an embodiment, the system 100 is configured to generate the second metatoken based on the first metatoken along with a token transaction hash and a smart contract type employed for transaction of the fungible token. In an embodiment, the term 'asset valuation document' is a valuation document of the digital asset (*e,g,* gold or property valuation). A hash of the valuation document is the "asset valuation document hash". In an embodiment, the term 'compliance" corresponds to a report issued by a financial institution or a regulatory institution pertaining to identity and adherence of the users i.e. the seller to financial regulations. The report is hashed to obtain the "compliance hash". Accordingly, the system 100 is configured to include data pertaining to asset valuation and compliance, if the digital token is a fungible token used for such assets and transactions.

[028] Further, the digital token and its underlying digital asset can be verified/authenticated by a prospective buyer on the digital marketplace 140 through the system of the present invention. The buyer through buyer device 150 can connect with the digital marketplace 140 to authenticate/verify and purchase the NFT. Firstly, the buyer through buyer device 150 logs into the digital marketplace 140 and makes a request for authentication of the digital token. Upon receiving the request, the system 100 provides a first reference metatoken to the prospective buyer (by transmitting the first reference metatoken to the digital marketplace 140) automatically or based on instructions from

the owner/seller for verifying the digital token. The first reference metatoken comprises information pertaining to the digital asset of the owner retrieved from the storage unit. This is achieved either by the system 100 being given access to the underlying digital asset in the storage unit of the seller and regenerating the first metatoken, or alternatively system 100 being given access to the first metatoken in the storage unit of the seller. The system 100 is then configured to generate a second reference metatoken of the minted digital token available in the digital marketplace 140. This is achieved by the system 100 by generating a reference hash of the first reference metatoken with the metadata of the minted digital token available in the digital marketplace 140. The second reference metatoken is then compared with the second metatoken in the storage unit of server 120 and with the second metatoken appended to the minted digital token in the digital marketplace 140. The processor is configured to determine whether or not the provenance of the digital token has been established. If the second reference metatoken matches the second metatoken, the provenance of the digital token stands established consequently, mitigating the need for comparison with the first metatoken, thereby ensuring computing efficiency.

[029] If the second reference metatoken does not match the second metatoken, the processor is configured to compare the first reference metatoken with the first metatoken. The processor is configured to determine that the underlying digital asset is unauthentic, when both the first reference metatoken and the second reference metatoken do not match with the first metatoken and the second metatoken respectively. Further, the processor is configured to determine that the digital token has changed when the first reference metatoken matches with the first metatoken, and the second reference metatoken does not match with the second metatoken.

[030] In an embodiment, the digital marketplace 140 may provide the first reference metatoken and the second reference metatoken to the prospective buyer during verification, so that the prospective buyer on their own can decide on the provenance of the digital token and/or the underlying digital asset by comparing them with the first metatoken and the second metatoken stored in the storage unit in the server 120.

[031] Furthermore, the processor is configured to generate and transmit the first transaction data along with the second metatoken to the buyer device 150 upon purchase of the digital token by the prospective buyer. As such, the details pertaining to the metadata of the digital token along with the details pertaining to the digital asset of the digital token are transferred to the buyer device 150 along with the first transaction data.

[032] A first transaction hash is thereafter generated by the system 100 for the first transaction data. A hash function is applied to the first transaction hash along with the second metatoken for generating a third metatoken. The third metatoken being indicative of information pertaining to the digital asset, the digital token and the transaction between the buyer and the owner of the digital token is stored in the server 120. As such, the information pertaining to the digital asset, the digital token and the transaction between the buyer and the owner of the digital token are recorded automatically by the system 100, thereby maintaining track of the transactions and/or change in ownership of the digital token or the digital asset.

[033] The processor then appends the digital token with the third metatoken and stores the appended digital token with the third metatoken in the digital marketplace 140. This ensures that the provenance of the transaction of the digital token is registered. Also, as the digital token with the third metatoken is stored in the marketplace, the system 100 establishes independence of checking provenance of the digital token. Similarly, the system 100 is configured to generate subsequent metatokens during each transaction and/or change in ownership of the digital token, which will thereafter be stored in the server 120 and also appended with the digital token and stored in the digital marketplace 140. The present invention thus provides provenance of the underlying digital asset, the digital token, and its transaction history. Moreover, the present invention is also capable of detecting and mitigating spoofing and tampering of the digital token, wherein 'spoofing' refers to duplicates of the digital token created by an attacker or impersonating the author of the digital token, and wherein tampering refers to manipulation of the digital asset or metadata stored outside the blockchain by the attacker.

[034] In an embodiment, the processor is embodied as a multi-core processor, a single core processor, or a combination of one or more multi-core processors and one or more single core processors. For example, the processor is embodied as one or more of various processing devices, such as a coprocessor, a microprocessor, a controller, a digital signal processor (DSP), a processing circuitry with or without an accompanying DSP, or various other processing devices including integrated circuits such as, for example, an application specific integrated circuit (ASIC), a field programmable gate array (FPGA), a microcontroller unit (MCU), a hardware accelerator, a special-purpose computer chip, or the like. In another embodiment, the processor is configured to execute hard-coded functionality.

[035] Figure 2 is a flow diagram of a method 200 for creating the digital token for a digital asset, such that the provenance of the digital token is established at any point in time, in accordance with

an embodiment of the present invention. In order to perform the method 200, a system such as the system 100 shown in the Figure 1 may be used. The method 200 starts at step 202 where the seller creates or selects the digital asset to be traded on the digital marketplace 140. The method determines asset metadata. The asset metadata includes information pertaining to type of file *i.e.* whether it is a video file, an audio file, or a text document etc., size of the digital asset, name of author of the digital asset, time stamp of the digital asset, owner ID, modification date, title, asset dimensions and the like. The asset metadata is transiently stored within the storage unit of the seller device 110.

[036] At step 204, the seller device 110 through the hashing service on the server 120 is configured to generate the first hash of the asset metadata and a second hash of the digital asset.

[037] At step 206, the system 100 applies the hash function to the first hash and the second hash for generating the first metatoken. The first metatoken is stored in the server 120 and in the storage unit of the seller device 110. In an embodiment, the first hash and the second hash and the hash function are carried out through one or more cryptographic techniques stored in the server 120.

[038] At step 208, the processor is configured to embed the first metatoken with the digital asset as binary data. The processor is configured to embed the first metatoken with the digital asset through one or more embedding techniques known in the art. In an embodiment, the processor is configured to embed the first metatoken with the digital asset as binary data. The processor is also adapted to store the marked-up digital asset in the storage unit of the seller device 110.

[039] At step 210, the marked-up digital asset is then transmitted by the processor to the digital marketplace 140 for minting its digital token. The owner of the digital asset can include a price as well as a description of the digital token while transmitting or minting the digital token. The minting of the digital token by transmitting the marked-up digital asset is carried out by conventional techniques known in the art for minting the digital token in the digital marketplace 140.

[040] At step 212, the method is configured to append the minted digital token with the first metatoken, which is stored in the digital marketplace 140. The method thereafter generates through the hashing service the third hash for the metadata of the digital token minted in the digital marketplace 140.

[041] At step 214, the hash function is applied to the third hash by system 100 along with the first metatoken for generating the second metatoken. The second metatoken ensures that the information pertaining to the minting of the digital token such as digital token ID, metadata of the

digital token, and the like along with ID of the digital marketplace 140 are captured. This process establishes a link between the owner, digital token and the digital asset in the seller device 110 and/or in the server 120. In an embodiment, metadata of the digital token corresponds to the attributes of the digital marketplace 140 such as its ID. The system 100 then appends the second metatoken with the minted digital token and stores the appended second metatoken in the digital marketplace 140 as well as the server 120. Such a step enables a prospective buyer to check provenance of the minted digital token and the underlying asset before purchasing it consequently, preventing transactions of counterfeit digital token in the digital marketplace 140.

[042] Figure 3 is a method 300 for establishing the provenance of the digital token, in accordance with an exemplary embodiment of the present invention. In order to perform the method 300, a system such as the system 100 shown in the Figure 1 may be used.

[043] At step 302, a prospective buyer logs into the digital marketplace 140 through the buyer device 150 and makes a request for authentication of the digital token. Upon receiving the request, the system 100 moves to step 304. At step 304, the system 100 provides the first reference metatoken of the minted digital token to the prospective buyer by transmitting the first reference metatoken to the digital marketplace 140, automatically or based on instructions from the owner/seller for verifying the digital token. The first reference metatoken comprises information pertaining to the digital asset of the owner retrieved from the storage unit. This is achieved either by the system 100 being given access to the underlying digital asset in the storage unit of the seller and regenerating the first metatoken, or alternatively system 100 being given access to the first metatoken in the storage unit of the seller.

[044] At step 304, the system 100 generates a reference hash of the first reference metatoken with the metadata of the minted digital token available in the digital marketplace 140. A hash function is then applied by the system 100 to the reference hash of the metadata of the digital token along with the first reference metatoken for generating the second reference metatoken at step 306.

[045] At step 308, the processor is configured to compare the second reference metatoken with the second metatoken. If the processor determines that the second reference metatoken matches with the second metatoken, the processor moves to step 312 to determine that the provenance of the digital token and its underlying asset is established. Such a step mitigates the need for comparison of the first metatoken, thereby ensuring computing efficiency.

[046] If the processor determines that the second reference metatoken does not match with the second metatoken, the processor moves to step 310 to compare the first reference metatoken with

the first metatoken. If the first reference metatoken matches the first metatoken, the processor moves to step 314 to determine that the digital token is unauthentic.

[047] If the processor determines that the first reference metatoken and second reference metatoken do not match with first metatoken and second metatoken respectively, the processor moves to step 316 to determine that the underlying asset is unauthentic.

[048] In an embodiment, the present invention is configured to establish the provenance of digital tokens for multiple assets that are thematically related. For example, music album comprising multiple songs, whereby the music album as a whole is an asset and each individual song is also an asset. The present invention in such a scenario generates a first metatoken for each asset - song. The present invention also generates a first master metatoken for the album by hashing together each asset -song first metatoken. Thereafter, each asset -song is embedded with the respective first metatoken and first master metatoken and transmitted to the marketplace for generating the digital token for each asset. Simultaneously, all the first metatokens and the master metatoken are stored in the server 120. Once the digital token for each asset is created in the digital marketplace 140, the second metatoken is created for each digital token. The first metatoken, the first master metatoken and the second metatoken are appended with the digital token in the digital marketplace 140 and stored on server 120. During a prospective sale, all the metatokens will be regenerated and compared as discussed hereinbefore.

[049] Advantageously, the present invention through the system and the method is capable of establishing the provenance of the digital token and its underlying asset including authenticating the digital token, its transaction history and the authorship of the digital token by maintaining independent immutable records that can be instantaneously verified on demand. Consequently, the problems associated with counterfeit digital token in digital trading platforms are mitigated if not eliminated. Additionally, the system and method are capable of tracking and establishing the provenance of the digital tokens across multiple blockchains and/or digital trading platforms such as marketplaces. The present invention is also capable of detecting and mitigating spoofing and tampering of digital tokens.

[050] With some modification obvious to a person skilled in the art, the present invention is also capable of tracking, establishing the provenance of, detecting and mitigating spoofing and tampering of certain types of fungible tokens representing underlying physical or digital assets.

[051] The foregoing description of the invention has been set merely to illustrate the invention and is not intended to be limiting. Since the modifications of the disclosed embodiments

incorporating the spirit and substance of the invention may occur to the person skilled in the art, the invention should be construed to include everything within the scope of the invention.

CLAIMS:

1. A system (100) for authenticating provenance of digital tokens for a digital asset, the system (100) comprising:

a seller device (110) communicatively coupled to a server (120) and to a digital marketplace (140), the seller device (110) comprising a processor configured to:

create or select the digital asset whose digital token is to be traded on the digital marketplace (140) and determine the asset metadata of the digital asset;

generate a first hash of the asset metadata and a second hash of the digital asset through a hashing service on the server (120);

apply a hash function to the first hash and the second hash for generating a first metatoken, and storing the first metatoken on the seller device (110) and/or the server (120);

embed the digital asset with the first metatoken to obtain a marked-up digital asset;

make available the marked-up digital asset to the digital marketplace (140) for minting the digital token of the digital asset, and a digital token metadata pertaining to the minted digital token;

generate a third hash of the digital token metadata through the hashing service on the server (120); and

apply a hash function to the third hash and the first metatoken to generate a second metatoken and store the second metatoken in the server (120),

the second metatoken and the first metatoken are appended to the minted digital token and stored on the digital marketplace (140), allowing a prospective buyer to authenticate provenance of the minted digital token based on the first metatoken and the second metatoken.

2. The system (100) as claimed in claim 1, wherein the processor is configured to receive the digital asset from an owner of the digital asset,

wherein the digital asset corresponds to one of an art, music, video, 3D metaverse, and documents,

wherein the asset metadata corresponds to owner ID, type of file, creation date, modification date, file size, title, asset dimensions, and digital information, and

wherein the digital token metadata corresponds to attributes of the digital marketplace (140).

3. The system (100) as claimed in claim 1, wherein the processor is configured to embed the first metatoken with the digital asset as a binary data, and store the marked-up digital asset in a storage unit of the seller device (110).

4. The system (100) as claimed in claim 1, wherein the processor is configured to:

receive a request for authenticating provenance of the digital token from a prospective buyer;

generate a first reference metatoken by accessing the digital asset; and

generate a second reference metatoken based on the first reference metatoken and reference hash of the metadata of the digital token.

5. The system (100) as claimed in claim 4, wherein the processor is configured to:

determine the digital token to be authentic if the second reference metatoken matches with the second metatoken;

determine the digital token to be unauthentic, if the first reference metatoken and the second reference metatoken do not match with the first metatoken and the second metatoken respectively; and

determine the digital token to be altered if the first reference metatoken matches with the first metatoken, while the second reference metatoken does not match with the second metatoken.

6. The system (100) as claimed in claim 5, wherein the processor is configured to:

generate and transmit a first transaction data along with the second metatoken to a buyer device (150) upon purchase of the digital token;

generate a first transaction hash pertaining to the first transaction data (T1);

apply a hash function to the first transaction hash and the second metatoken to generate a third metatoken, and storing the third metatoken in the server (120);

append the digital token with the third metatoken to obtain an appended digital token; and

store the appended digital token with the third metatoken in the digital marketplace (140).

7. The system (100) as claimed in claim 1, wherein the server (120) corresponds to a first blockchain server and the digital marketplace (140) corresponds to a second blockchain server.

8. A method (200) for authenticating provenance of a digital token for a digital asset, the method (200) comprising:

creating or selecting (202), by a processor of a seller device (110) in communication with a server (120) and to a digital marketplace (140), the digital asset to be traded on the digital marketplace (140);

generating (204), by the processor, a first hash of an asset metadata of the digital asset and a second hash of the digital asset through a hashing service on the server (120);

applying (206), by the processor, a hash function to the first hash and the second hash to generate a first metatoken and storing the first metatoken on the seller device (110) and/or the server (120);

embedding (208), by the processor, the digital asset with the first metatoken to obtain a marked-up digital asset;

transmitting (210), by the processor, the marked-up digital asset to the digital marketplace (140) for minting the digital token of the marked-up digital asset, and a digital token metadata pertaining to the minted digital token;

generating (212), by the processor, a third hash of the digital token metadata through the hashing service on the server (120); and

applying (214), by the processor, a hash function to the third hash and the first metatoken to generate a second metatoken, and store the second metatoken in the server (120),

the second metatoken and the first metatoken are appended to the minted digital token and stored on the digital marketplace (140), allowing a prospective buyer to authenticate provenance of the minted digital token based on the first metatoken and the second metatoken.

9. The method (200) as claimed in claim 8 comprising embedding, by the processor, the first metatoken with the digital asset as a binary data and storing the marked-up digital asset in a storage unit of a seller device (150).

10. The method (200) as claimed in claim 8 comprising:

receiving, by the processor, a request for authenticating provenance of the digital token from a prospective buyer;

generating, by the processor, a first reference metatoken by accessing the digital asset; and

generating, by the processor, a second reference metatoken based on the first reference metatoken and reference hash of the metadata of the digital token.

11. The method (200) as claimed in claim 10 comprising:

determining (312), by the processor, the digital token to be authentic if the second reference metatoken matches with the second metatoken;

determining (316), by the processor, the digital token to be unauthentic if the first reference metatoken and the second reference metatoken do not match with the first metatoken and the second metatoken respectively; and

determining (314), by the processor, the digital token to be altered if the first reference metatoken matches with the first metatoken, while the second reference metatoken does not match with the second metatoken.

12. The method (200) as claimed in claim 11 comprising:

generating and transmitting, by the processor, a first transaction data along with the second metatoken to a buyer device (150) upon purchase of the digital token;

generating, by the processor, a first transaction hash pertaining to the first transaction data;

applying, by the processor, a hash function to the first transaction hash and the second metatoken to generate a third metatoken and storing the third metatoken in the server (120);

appending, by the processor, the digital token with the third metatoken; and

storing, by the processor, the appended digital token with the third metatoken in the digital marketplace (140).