

CLAIMS

Therefore, the following is claimed:

1. A system, comprising:
 - a computing device comprising a processor, a memory, and a display; and
 - machine-readable instructions stored in the memory that, when executed by the processor, cause the computing device to at least:
 - receive, from a client device, a smart contract address and a non-fungible token (NFT) identifier for an NFT;
 - execute a function of a smart contract located at the smart contract address to obtain an owner address for the NFT, wherein the NFT identifier is provided as an argument to the function of the smart contract;
 - validate the owner address for the NFT by causing the computing device to at least:
 - send a request to a wallet application hosted by the computing device to sign a transaction;
 - receive the signature of the transaction from the wallet application;
 - determine a wallet public key based at least in part on the signature of the transaction;
 - derive a wallet address from the wallet public key; and
 - determine that the wallet address matches the owner address; and
 - in response to validation of the owner address for the NFT, cause a media file represented by the NFT to be presented.

2. The system of claim 1, wherein the machine-readable instructions that cause the media file represented by the NFT to be presented, when executed, further cause the computing device to at least:

identify a uniform resource locator (URL) included in metadata of the NFT, the URL specifying a location where the media file is located; and

retrieve the media file from the location specified by the URL.

3. The system of claim 1, wherein the computing device further comprises an indicator light that, when active, represents that the media file is authentic, and the machine-readable instructions, when executed by the computing device, further cause the computing device to at least activate the indicator light in response to validation of the owner address for the NFT.

4. The system of claim 1, wherein the client device is in communication with the computing device via a BLUETOOTH or near-field communication (NFC) connection and the smart contract address and the NFT identifier are received via the BLUETOOTH or the NFC connection.

5. The system of claim 2, wherein the NFT includes a hash, and the machine-readable instructions, when executed, further cause the computing device to at least:
 - determine that the hash included in the NFT matches a hash of the media file; and
 - wherein the media file is retrieved from the location specified by the URL in response to a determination that the hash included in the NFT matches the hash of the media file.
6. The system of claim 1, wherein the NFT is stored on the ETHEREUM blockchain.
7. A method, comprising:
 - receiving, from a client device, a smart contract address and a non-fungible token (NFT) identifier for an NFT that represents a media file;
 - executing a function of a smart contract located at the smart contract address to obtain an owner address for the NFT, wherein the NFT identifier is provided as an argument to the function of the smart contract;
 - validating the owner address for the NFT;
 - in response to validating the owner address for the NFT, presenting the media file represented by the NFT; and
 - activating an indicator light of a presentation device in response to validation of the owner address for the NFT.

8. The method of claim 7, wherein presenting the media file further comprises:
 - identifying a uniform resource locator (URL) included in metadata of the NFT, the URL specifying a location where the media file is located; and
 - retrieving the media file from the location specified by the URL.
9. The method of claim 7, wherein the smart contract address and the NFT identifier are received via the BLUETOOTH or the NFC connection with the client device.
10. The method of claim 7, wherein validating the owner address for the NFT further comprises:
 - sending a request to a wallet application hosted by the computing device to sign a transaction;
 - receiving the signature of the transaction from the wallet application;
 - determining a wallet public key based at least in part on the signature of the transaction;
 - deriving a wallet address from the wallet public key; and
 - determining that the wallet address matches the owner address.

11. The method of claim 8, wherein the NFT includes a hash, and the method further comprises:

determining that the hash included in the NFT matches a hash of the media file;
and

wherein retrieving the media file from the location specified by the URL occurs in response to determining that the hash included in the NFT matches the hash of the media file.

12. The method of claim 7, wherein the NFT is stored on the ETHEREUM blockchain.

13. The method of claim 7, wherein the indicator light, when active, represents that the media file is authentic.

14. A non-transitory, computer-readable medium, comprising machine-readable instructions that, when executed by a processor of a computing device, cause the computing device to at least:

- receive, from a client device, a smart contract address and a non-fungible token (NFT) identifier for an NFT;

- execute a function of a smart contract located at the smart contract address to obtain an owner address for the NFT, wherein the NFT identifier is provided as an argument to the function of the smart contract;

- validate the owner address for the NFT by causing the computing device to at least:

 - send a request to a wallet application hosted by the computing device to sign a transaction;

 - receive the signature of the transaction from the wallet application;

 - determine a wallet public key based at least in part on the signature of the transaction;

 - derive a wallet address from the wallet public key; and

 - determine that the wallet address matches the owner address; and

- in response to validation of the owner address for the NFT, cause a media file represented by the NFT to be presented.

15. The non-transitory, computer-readable medium of claim 15, wherein:
- the NFT includes a hash; and
 - the machine-readable instructions that cause the media file represented by the NFT to be presented, when executed, further cause the computing device to at least:
 - identify a uniform resource locator (URL) included in metadata of the NFT,
 - the URL specifying a location where the media file is located;
 - retrieve the media file from the location specified by the URL; and
 - determine that the hash included in the NFT matches a hash of the media file.