DataLok's Paper, Version 1.0.0.

The future of data protection & data leak tracking mechanisms.

Nathan Trudeau
BB INVENTIONS INC.

Table of Contents

Introduction

Prior Art & Issues

The market value of digital assets is increasing every year as they become more popular. Generally, a digital asset is a digital file that comes with ownership, rights of use and has an associated value. Digital assets can be traded, for instance via blockchains such as Ethereum™, FLOW™, Tezos™, and Solana™, which advantageously allow tracking records of ownership of the digital asset. Since the ownership of a digital asset is typically limited to a single owner, a certain value can be associated with the digital asset which a buyer would have to trade for in order to acquire the ownership of the digital asset.

The proof of ownership of a digital asset is usually established in the form of a transaction. Yet, such a transaction usually limits the digital asset to a pure commodity, and the authenticity of the digital asset is not considered, due to a lack of traceability. For instance, one could simply copy a publicly available digital asset, mint the digital asset in a blockchain, and sell the digital asset to a buyer without giving credit to the original creator and the previous owners of the digital asset. Such cases of fraud within the digital asset industry, particularly NFTs, has been widely reported. While being operational, such systems omit the authenticity aspect of the transaction of a digital asset, which is a serious drawback.

Digital assets can also be important sets of sensitive data, such as keycard data or biometric security systems. Such systems are at high risk of attack.

DataLok – Overview

DataLok enables the creation, trading, and tracking of a given (trackable) digital asset. This means that when you have a digital file, like a picture or video, you can embed data in it that can be used to determine the authenticity of the asset, i.e., identifying fakes and whatnot, as well as track it, for example, in several implementations, across the web, in case of an unauthorized use/leak. You can then encrypt the file so that only people with the password can access it.

The authenticity of a given digital asset can be achieved by comparing one or more hashes of one or more portions of the trackable asset with one or more hashes of one or more portions of a given (digital) asset which the authenticity has to be establish, as well as by other integrated mechanisms such as steganography. DataLok's use goes from blockchains and NFTs to confidential data tracking and trading for corporations with such a need.

Further utility of the DataLok system is in physical security. For example, a secure door inside of a bank which requires a specific keycard or fingerprint to access must be connected to a secure data storage system. DataLok can create, manage, and track such sensitive access information. This application reaches far across the physical security industry and would be a useful tool for Banks, Prisons, Government Facilities, and other Public and Private security measures.

Creating

Pre-Creation Information

Pre-creation information is data that is required to include in an asset in order for said asset to be effectively trackable. This data is generated and/or obtained prior to other creation processes. Pre-creation information will vary greatly from one implementation to another.

For example, it can comprise things like the asset owner's (AO) name, AO's public key (in the case of a blockchain using DataLok), an upload time, the marketplace's name, the AO's email address, an ID of a reference to the asset, or a portion thereof, in a database, file information of the asset (for example, resolution if the asset is an image file), an indication of uses the AO allows buyer(s) / user(s) to do with the asset, an indication of where and/or why and/or how the asset was created for using DataLok in the first place, and any other relevant information. In one or more implementations, this information will be hashed, and the hash will also be used as pre-creation information.

Preprocessing

A given asset usually has to be processed before any other step can be done. For example, in one or more implementations where an NFT marketplace is using DataLok, preprocessing is relevant as the data received is of unknown origin and may be corrupted. The processing can also apply to a given physical asset, according to the implementation.

Digital

The preprocessing of a digital asset is done to, for example, verify the asset's integrity and convert it to a file format that is suitable for further processing, if necessary. In some implementations, the digital asset is also compressed to reduce its size. In the case of an image or video, the preprocessing can also include cleaning the metadata and repairing headers, normalizing the video/audio encoding(s), normalizing the file type, and/or the like.

Physical

The preprocessing of a physical asset involves digitalizing the physical asset, thereby allowing DataLok to be used on the physical asset. Said digitalizing involves, for example, taking picture(s) or video(s) of the physical asset from multiple angles under specific conditions, 3D scanning the physical asset, or using special equipment used for digitalization thereof. Digitalizing can take various forms based on the implementation of DataLok and for which purpose DataLok is used and implemented.

In one or more implementations, digitalization involves inserting a readable chip in the physical item, where the readable chip will contain pre-creation information.

In one or more implementations, digitalization involves generating instructions that allow the exact reconstruction of the physical item. For example, a physical item being generated using a specialized automated device taking instructions as parameters and generating a precisely calculated device based on said parameters could benefit from such digitalization.

Hybrid

In some implementations of DataLok, a given asset can be both physical and digital. For example, in an online game, a player may want to trade their in-game avatar, which is a 3D model that exists both in the game (digital form) and as a 3D printed object (physical form). In this case, the preprocessing of the asset would involve taking pictures or videos of the 3D-printed object from multiple angles under specific conditions as well as, for example, getting, updating, and/or normalizing data from the game server that corresponds to the in-game avatar.

Another example of a hybrid asset would be a physical book that has an NFC tag embedded in it, said NFC tag storing data that corresponds to the digital version of the book. In this case, the preprocessing of the asset could involve taking pictures or videos of the book from multiple angles under specific conditions, as well as, for example, reading, writing, and/or normalizing the data from the NFC tag.

The preprocessing of a hybrid asset can take various forms and comprise several steps, mixing physical and digital assets preprocessing techniques. In one or more implementations, the preprocessing of a hybrid asset is done in two steps: first, the digital part of the asset is preprocessed, then the physical part is preprocessed. In one or more implementations, the digital and physical parts are preprocessed simultaneously. In one or more other implementations, the preprocessed digital (or physical) asset is used in the preprocessing of the physical (or digital) asset.

Preview Generation

In one or more implementations where a preview of the asset has to be available publicly, said preview generation is thereby initiated. A great example of an implementation in need of a preview would be an NFT marketplace.

Another great example would be an online store selling shoes that have been protected using DataLok.

The generation involves transforming the processed asset into a reduced form with no intrinsic value. In some implementations, the generation of the preview is done automatically by DataLok. In others, the AO has to trigger the generation manually. The preview can take various forms depending on the asset and/or the implementation.

For example, in an online game, a player's 3D avatar could be turned into a 2D picture or video as a preview.

Another example would be an online store that sells physical shoes; in this case, the preview could be a picture of one or both shoes.

Likewise, a person may wish to use blockchain accounting to store their will, in which case the details of the will would be private and viewable only by the attorney and the client. At the time of passing, the attorney would present the will as intended to the recipients. Another example could be the IP of a large corporation who wishes to share an example of what their IP is, but don't wish to reveal the entire IP. Using DataLok would allow for a seamless process of IP sharing, management, and sale.

Embedding

Once the preprocessed asset and, depending on the implementation, the preview is obtained, the pre-creation data is thereby embedded into one or more portions of the preprocessed asset using one or more techniques, such as steganography and, for example, in the metadata of the preprocessed asset.

The embedding of the data can be done in various ways depending on the asset, the implementation, and/or the type of data to be embedded.

Several steganography techniques, and/or a combination thereof, are possible to implement for various types of files used in a given DataLok implementation, but outside of the scope of this paper in order to keep said paper concise. DataLok is applicable to most types of files. To name a few, DataLok supports numerous types of image, video, and text-based files.

For example, in a cloud-based pictures storage system implementing DataLok, each picture would have one or more parts of pre-creation data embedded in it using advanced steganography techniques and, optionally but commonly, one or more other parts of publicly available pre-creation data in its metadata. Such steganography technique(s) would be intended to be resilient to cropping and resolution changes.

Another example would be an online store that sells physical shoes; in this case, pre-creation data could be encoded into a digitally readable chip, such as an NFC chip, which would then be embedded in both shoes, each chip further indicating to which shoe of the pair it belongs to. Each shoe could further be engraved with a given identifier linked to and/or also present in the NFC chip.

In one or more implementations, instead of embedding the raw pre-creation data, a representation thereof is embedded. For example, a mathematical formula allowing the calculation of a given portion of the pre-creation data could be embedded. Another example would be embedding an URL or an access point to the pre-creation data.

In one or more implementations, one or more portions of the pre-creation data (or representation thereof) are encrypted prior to embedding thereof. The encryption mechanism can vary greatly, from a closed-source mechanism only known by DataLok to one or more well-known algorithms such as AES256. The choice of the encryption mechanism can be decided by DataLok, by the AO, or a combination thereof. The type of encryption may also change based on various criteria, such as the pre-creation data, the AO, and/or the like, making a DataLok implementation more resilient against cases where one or more exploits would be found in one or more given encryption algorithms.

In one or more implementations, DataLok also supports the embedding on textual data using advanced techniques. This can be used to protect digital communications for corporations and other entities that need a secure way to communicate information. Such an implementation could include encoding pre-creation data into fonts that are then applied to text as part of a graphical representation. Additionally, DataLok can support other types of textual data such as code snippets, documents and the like. By combining these features with cryptographic encryption algorithms, DataLok can provide organizations with a comprehensive suite of tools designed to ensure secure communication in any environment.

Hashing

The trackable asset, with the pre-creation data now embedded in it, is then hashed using one or more hashing algorithms. The choice of hashing algorithm(s) can be decided by DataLok, by the AO, or a combination thereof. Depending on the implementation, all or only some portion(s) of the trackable asset can be hashed; for example, only a given portion of an image could be hashed while another given portion would remain untouched or vice-versa. It will be understood that the number of hashes performed is usually correlated with an increased quality of tracking later on, as if one part of a given leaked trackable asset is altered, it wouldn't necessarily impact other portions of the trackable asset, according to the way the hashes were computed in the first place.

The hashing algorithm used by DataLok may vary greatly based on the implementation. However, using a robust and proven algorithm such as SHA512 or SHA256 is recommended.

For example, in the case of an online store that sells physical shoes, a digitalized version of one or more portions of each shoe would be hashed using one or more hashing algorithms.

In another example of a cloud-based image storage system using DataLok, one or more portions, or the entirety thereof, of each image would be hashed.

Encrypting

After the trackable asset has been hashed, it is then encrypted using one or more encryption algorithms. As with the hashing algorithms, the choice of the encryption algorithm(s) can be decided by DataLok, by the AO, or a combination thereof. The encryption mechanism can vary greatly, from a closed-source mechanism only known by DataLok to one or more well-known algorithms such as AES256. The choice of the encryption mechanism can be determined by DataLok, by the AO, or a combination thereof. The type of encryption may also change based on various criteria, such as the pre-creation data, the AO, and/or the like, making a DataLok implementation more resilient against cases where one or more exploits would be found in one or more given encryption algorithms. It will be understood that one or more first portions of the trackable asset can be encrypted using a different method than one or more other portions of the trackable asset.

For example, in the case of the online store that sells physical shoes with chips embedded in them, the content of each chip would be encrypted using one or more encryption algorithms.

In another example of a cloud-based image storage system using DataLok, each image would be encrypted using one or more encryption algorithms during upload.

It is also possible to encrypt only a portion of the trackable asset instead of the full trackable asset, which can be useful, in some implementations, in the case where a trackable asset comprises multiple different assets. This can be useful, for example, if a vendor wants to store different types of documents such as images, audio and text files in one trackable asset.

The goal of encrypting the trackable asset is to make sure that only one or more specific individuals have access to the trackable asset, i.e., those with the decryption key. As such, in one or more implementations where the encrypted trackable asset has to be available publicly, such as an NFT in a blockchain, the encrypted nature of the trackable asset restrains its access, i.e., decryption.

For example, in the case of a file storage application using DataLok, each file would be encrypted using one or more encryption algorithms during upload. The access to these files could be protected by an authorization layer that requires users to authenticate themselves before they can view and/or download the file(s).

Storing

Once all the previous steps are done, the following are stored on one or more storage mediums which may or may not be available publicly, based on the implementation:

1. The encrypted trackable asset;
2. If used in the given implementation, the preview; and
3. The hash of the trackable asset;

In one or more implementations where a blockchain uses DataLok, IPFS is used as a storage medium.

In one or more implementations, for example, an implementation using readable and writable chip(s), such as NFC chip(s), embedded into physical item(s) or standalone chip(s) thereof, the storage medium is (are) said readable and writable readable chip(s). In one or more implementations, this method would therefore allow the transformation of a completely digital asset into a semi-digital (i.e., digitally stored on a physical device) one. This would particularly be useful for high-tech door-locking systems, and high-tech access granting systems thereof, using DataLok as its protection technique.

In one or more implementations, the encrypted trackable asset is physically provided. For example, a QR code, painted or engraved on a piece of aluminum. In this scenario, the encrypted trackable asset would not be stored on other storage mediums.

In one or more implementations, the encryption/decryption key (EDK) is transformed into a seed phrase which the AO can then take note of, preferably on an offline storage medium, like a piece of paper.

In one or more other implementations, the EDK is further encrypted, forming the encrypted encryption/decryption key (EEDK) (and stored on the AO's machine) with one of:

1. a password known by the AO; or
2. a fingerprint generated on the AO's machine, said fingerprint being obtain by using techniques such as in the "fingerprintjs/fingerprintjs" GitHub library, and/or any other relevant technique which may or may not be browser-based, according to the implementation.

The encryption mechanism for the EDK can vary greatly, from a closed-source mechanism only known by DataLok to one or more well-known algorithms such as AES256. The choice of the encryption mechanism can be determined by DataLok, by the AO, or a combination thereof.

In one or more implementations where a fingerprint is used to encrypt the EDK, a seed phrase generated from the fingerprint is also used and taken note of by the AO, preferably on an offline storage medium, like a piece of paper. This seed phrase would then allow the AO to recover the EDK if the fingerprint couldn't be automatically generated, such as if the AO changed device. In such a case where

the AO would change device and the fingerprint wouldn't be automatically generated, a system such as the following could be used:

1. The AO enters its seed phrase in the system;
2. The EEDK is decrypted using the fingerprint recovered from the entered seed phrase; and
3. The EDK is thereby re-encrypted using the fingerprint of the new device and stored on the AO's new device.

In one or more implementations, the AO's fingerprint can be obtained using one or more authentication schemes. For example, multi-factor authentication, certificate-based authentication, biometric authentication and token-based authentication can all be used to obtain the AO's fingerprint.

Trading

In one or more implementations, the encrypted trackable asset is made available for trading purposes by virtue of it being stored on a blockchain. This would be the case, for example, if an NFT were stored on a blockchain that uses DataLok to protect its content. In such cases, when an encrypted trackable asset stored on a blockchain is transferred to a new owner, the new owner would end up with, by either gathering or receiving using one or more communication mediums:

1. The encrypted trackable asset;
2. The EEDK;
3. The seed phrase allowing the reconstruction of the fingerprint which was used to generate the EEDK; and
4. The hash of the trackable asset.

It is strongly recommended to provide #2 to the new owner using a different communication medium than when providing #3 (and, when possible, at different intervals) in order to avoid possible attacks.

It will be understood that, in one or more implementations where the EDK is not encrypted, therefore the EEDK doesn't exist, then points #2 and #3 above would be replaced by a singular point being "2. The EDK".

Once the new owner has all of the relevant information, it will:

1. Reconstruct the fingerprint (i.e., the one used to generate the EEDK) using the provided seed phrase;
2. Decrypt the EEDK using the reconstructed fingerprint, thereby obtaining the EDK;
3. Decrypt the trackable asset using the EDK;
4. Validate the authenticity of the trackable asset (as elaborated upon under the "Authenticity Validating" section below);

5. Generate its own device fingerprint and its derived seed phrase thereof, and noting the seed phrase (preferably on offline storage);

6. Encrypt the EDK using the fingerprint generated at #5, thereby generating the new EEDK (NEEDK); and

7. Store the NEEDK on its device.

In one or more implementations, the following steps are also included after step #4 and before step #5:

5. Embed new trackable data inside the trackable asset in order to obtain the new trackable asset (NTA);

6. Compute the hash of the NTA;

7. Encrypt one or more portions of the NTA using a different key than the EDK and, optionally, different encryption algorithm(s). In the case of multiple encryption algorithms, a plurality of keys could thereby be generated and used thereof (the same goes for the original EDK: there could be a plurality of keys if multiple encryption algorithms are used on one or more portions, or the totality thereof, of the trackable asset);

8. Provide the NTA and the hash of the NTA to the system implementing DataLok, the system thereby updating and taking into consideration the newly provided data as the new asset.

It is to be noted that, in one or more implementations, for security reasons, it may also be recommended to execute these additional updating steps after each trade (or after a pre-defined number of trades).

DataLok Blockchain Marketplace Trading Examples

Here are a few other examples of doing trading when DataLok is involved. The examples will all use an offer-based mechanism. However, it will be understood that the process could, instead, consist of a bidding process, a buying process, or a trading process.

Offer-Based, Using Cryptocurrency (1)

As such, here is a concrete example of a DataLok process for trading an encrypted trackable asset for an implementation involving a blockchain:

According to processing step A1, a buyer sends an offer to a seller for purchasing a trackable digital asset in a first defined cryptocurrency and specifies a minimum price.

According to processing step A2, the seller accepts the offer of the buyer and chooses a second defined cryptocurrency to be received.

According to processing step A3, the seller decrypts and sends a first password to a first server, the first password being used for decrypting the trackable digital asset once encrypted. In one or more implementations, the first password is encrypted using a fingerprint associated with a seed phrase.

According to processing step A4, the first server encrypts the first password with one or more portions of a second password. In one or more implementations, the second password is randomly generated. In one or more implementations, the first password is encrypted using one or more portions of a fingerprint associated with one or more portions of a seed phrase.

According to processing step A5, a second server detects that the transaction is ready to process. In one or more implementations, the second server is the first server.

According to processing step A6, the second server instructs a first cryptocurrency exchange to obtain a first wallet to be associated with the buyer to obtain one or more assets in the first defined cryptocurrency.

According to processing step A7, the buyer provides the one or more assets to the first wallet.

According to processing step A8, the second server detects that the one or more assets are received in the first wallet and instructs the seller to transfer the one or more indications of the trackable digital asset, the one or more hashes of one or more portions of the trackable digital asset and/or the preview of the digital asset and/or the trackable digital asset to the buyer. In one or more implementations, the transfer is made to a third party before being transferred to the buyer. In one or more implementations, the trackable digital asset is not transferred, but instead only changes with respect to the ownership of and/or the access to the trackable digital asset.

According to processing step A9, once the transfer of the trackable digital asset is completed or is almost completed, the second server instructs the first cryptocurrency exchange to transfer and potentially convert one or more assets taken from one or more cryptocurrency wallets in the second defined cryptocurrency. In one or more implementations, the trackable digital asset is not digitally and/or physically transferred, but instead only the ownership of and/or the access to the trackable digital asset is provided to the buyer. In one or more implementations, the second defined cryptocurrency is the same as the first defined cryptocurrency, and no cryptocurrency conversion occurs in the process.

According to processing step A10, the second server instructs the first cryptocurrency exchange to transfer one or more second defined assets to a second wallet associated with the seller.

According to processing step A11, the second server instructs the first cryptocurrency exchange to transfer one or more first defined assets from the first wallet to a second cryptocurrency exchange. It will be appreciated that the one or more first defined asset corresponds to the value of the one or more assets transferred and potentially converted at processing step A9. In one or more implementations, the second cryptocurrency exchange is the first cryptocurrency exchange.

According to processing step A12, the second server instructs the first server to provide the encrypted first password, the one or more portions of the fingerprint, and/or the one or more portions of the seed phrase to the buyer via a first means of communication.

According to processing step A13, the second server instructs the first server to provide the one or more portions of the second password to the buyer via a second means of communication. In one or more implementations, the second means of communication is the first means of communication.

According to processing step A14, the buyer decrypts the first password using the one or more portions of the second password, and the buyer has now at least access to the trackable digital asset.

In one or more implementations, processing step A14 is processed prior to processing step A12.

Offer-Based, Using Fiat

As such, here is a second concrete example of a DataLok process for trading an encrypted trackable asset for an implementation involving a blockchain:

According to processing step B1, a buyer sends an offer to a seller for purchasing a trackable digital asset in a first defined cryptocurrency and specifies the minimum price.

According to processing step B2, the seller accepts the offer of the buyer and specifies that the one or more assets will be received in fiat currency.

According to processing step B3, the seller decrypts and sends a first password to a first server, the first password being used for decrypting the trackable digital asset once encrypted. In one or more implementations, the first password is encrypted using a fingerprint associated with a seed phrase.

According to processing step B4, the first server encrypts the first password with one or more portions of a second password. In one or more implementations, the second password is randomly generated. In one or more implementations, the second password is encrypted using one or more portions of fingerprint associated with one or more portions of seed phrase.

According to processing step B5, a second server notices that the transaction is ready to process. In one or more implementations, the second server is the first server.

According to processing step B6, the second server instructs a first cryptocurrency exchange to create a first wallet associated with the buyer to obtain one or more assets in the first defined cryptocurrency.

According to processing step B7, the buyer provides the one or more assets to the first wallet.

According to processing step B8, the second server detects that the one or more assets are received in the first wallet and instructs the seller to transfer the one or more indications of the trackable digital asset, the one or more hashes of one or more portions of the trackable digital asset and/or the preview of the digital asset and/or the trackable digital asset to the buyer. In one or more implementations, the transfer is made to a third party before being transferred to the buyer. In one or more implementations, the trackable digital asset is not transferred, but instead only changes with respect to the ownership of and/or the access to the trackable digital asset.

According to processing step B9, once the transfer of the trackable digital asset is completed or is almost completed, the second server instructs a first cryptocurrency exchange to provide one or more assets taken from one or more cryptocurrency wallets to an escrow. In one or more implementations, the escrow is a smart contract, a system manager, a server, a computing node, a processing device, a software, and/or a storage device.

According to processing step B10, the second server instructs the escrow to transfer one or more defined assets to the seller. In one or more implementations, the one or more defined assets transfer is processed via a digital dollar exchange.

According to processing step B11, the second server instructs the first cryptocurrency exchange to transfer the first defined cryptocurrency from the first wallet to the second cryptocurrency exchange. It will be understood that the one or more first defined cryptocurrencies' value corresponds to up to the value of the one or more assets provided at processing step B9.

According to processing step B12, the second server instructs the first server to provide the encrypted first password, the one or more portions of the fingerprint, and/or the one or more portions of the seed phrase to the buyer via a first means of communication.

According to processing step B13, the second server instructs the first server to provide the one or more portions of the second password to the buyer via a second means of communication. In one or more implementations, the second means of communication is the first means of communication.

According to processing step B14, the buyer decrypts the first password using the one or more portions of the second password and the buyer has now at least access to the trackable digital asset.

In one or more implementations, processing step B14 is processed prior to processing step B12.

Offer-Based, Using Credit Cards

As such, here is a third concrete example of a DataLok process for trading an encrypted trackable asset for an implementation involving a blockchain:

According to processing step C1, a buyer sends an offer to a seller for purchasing a trackable digital asset in a fiat currency and specifies a minimum price.

According to processing step C2, the seller accepts the offer of the buyer and specifies that the one or more assets will be received in fiat currency.

According to processing step C3, the seller decrypts and sends a first password to a first server, the first password being used for decrypting the trackable digital asset once encrypted. In one or more implementations, the first password is encrypted using a fingerprint associated with a seed phrase.

According to processing step C4, the first server encrypts the first password with one or more portions of a second password. In one or more implementations, the second password is randomly generated. In one or more implementations, the second password is encrypted using one or more portions of a fingerprint associated with one or more portions of a seed phrase.

According to processing step C5, a second server notices that the transaction is ready to process. In one or more implementations, the second server is the first server.

According to processing step C6, the buyer provides one or more assets with a credit card to a credit institution. In one or more implementations, the credit card transaction is processed using a credit card provider and further sent to a bank account.

According to processing step C7, the second server detects that the one or more assets are received at the credit institution or receives at least an indication of a confirmation from the credit institution, and instructs the seller to transfer the one or more indications of the trackable digital asset, the one or more hashes of one or more portions of the trackable digital asset, and/or the preview of the digital asset

and/or the trackable digital asset to the buyer. In one or more implementations, the transfer is made to a third party before being transferred to the buyer. In one or more implementations, the trackable digital asset is not transferred, but instead only changes with respect to the ownership of and/or the access to the trackable digital asset.

According to processing step C8, once the transfer of the trackable digital asset is completed or is almost completed, the second server instructs a first cryptocurrency exchange to provide one or more assets to an escrow. It will be appreciated that the provided one or more assets correspond up to the one or more assets provided to the credit institution.

According to processing step C9, the second server instructs the escrow to transfer one or more assets to the seller. In one or more implementations, the one or more assets transfer is processed by an automated clearing house (ACH) network. In one or more other implementations, the one or more assets transfer is processed via bank transfer, Interac, and the like.

According to processing step C10, the second server instructs the first server to provide the encrypted first password, the one or more portions of the fingerprint, and/or the one or more portions of the seed phrase to the buyer via a first means of communication.

According to processing step C11, the second server instructs the first server to provide the one or more portions of the second password to the buyer via a second means of communication. In one or more implementations, the second means of communication is the first means of communication.

According to processing step C12, the buyer decrypts the first password using the one or more portions of the second password, and the buyer has now at least access to the trackable digital asset.

In one or more implementations, processing step C12 is processed prior to processing step C10.

Offer-Based, Using Cryptocurrency (2)

As such, here is a fourth concrete example of a DataLok process for trading an encrypted trackable asset for an implementation involving a blockchain:

According to processing step D1, a seller creates a first offer for a trackable digital asset in a marketplace and specifies the minimum price.

According to processing step D2, a buyer provides, in a first cryptocurrency, a second offer to the seller for the trackable digital asset, with a price at least equal to the minimum price defined by the seller.

According to processing step D3, the seller accepts the second offer in a second cryptocurrency. In one or more implementations, the second cryptocurrency is similar to the first cryptocurrency.

According to processing step D4, the seller provides a first encrypted first password and a seller identifier to a first server that has access to an encrypted version of the trackable digital asset.

According to processing step D5, the first server attempts to decrypt the encrypted trackable digital asset using a decrypted first encrypted first password, the decrypted first encrypted first password being decrypted using the seller identifier. If the decrypted first encrypted first password fails to decrypt the encrypted trackable digital asset, the first server requests from the seller a first recovery identifier

therefrom and reattempts to decrypt the encrypted trackable digital asset using the decrypted first encrypted first password, the decrypted first encrypted first password being decrypted using the first recovery identifier.

According to processing step D6, a second server obtains a second password and a related second recovery identifier and encrypts the decrypted first encrypted first password using the second password, thereby obtaining a second encrypted first password. In one or more implementations, the second password is randomly generated. In one or more implementations, the second server is the first server.

According to processing step D7, the buyer receives the second recovery identifier via a first means of communication.

According to processing step D8, the buyer transfers one or more assets in the first cryptocurrency to a third server. In one or more implementations, the third server is the first server and/or the second server.

According to processing step D9, the first server is informed that the third server has received the one or more assets in the first cryptocurrency and requests the seller to transfer an ownership of and/or an access to the trackable digital asset to the buyer.

According to processing step D10, the first server is informed that the ownership of and/or access to the trackable digital asset has been transferred to the buyer and acquires the one or more assets in the first cryptocurrency from the second server.

According to processing step D11, the first server converts the one or more assets in the first cryptocurrency into a defined asset according to the second defined cryptocurrency.

According to processing step D12, the first server provides the second encrypted first password to the buyer via a second means of communication and the defined asset to the seller. In one or more implementations, the second means of communication is the first means of communication

According to processing step D13, the buyer decrypts the second encrypted first password using the second recovery identifier.

According to processing step D14, the buyer encrypts the decrypted second encrypted first password using a buyer identifier.

Specifications

With regard to the above examples, a reward would be attributed to one or more parties involved in the trade, such as the seller and, according to the implementation, the owner(s) of a marketplace where one or more of the examples would occur. The reward may be, but is not limited to, a fiat currency amount, a number of cryptocurrencies, one or more assets, granted rights in a blockchain, and the like. In one or more implementations, the one or more assets received by the seller are different from what is described in the transaction offer by the buyer, due to various fees in the process, such as gas fees, wire fees, usage fees, and the like.

In one or more implementations, the one or more assets are provided in the form of any given asset(s), such as, for instance, digital assets, wire fees, a number of cryptocurrencies, permissions in a blockchain, and the like.

In one or more implementations, the trading of the digital asset does not involve funds or any given asset in exchange for the trackable digital asset, as the seller provides the trackable digital asset for free to the buyer. In one or more implementations, the seller provides funds or any given asset to the buyer along with the trackable digital asset. It will be understood that providing the trackable digital asset may comprise transferring the trackable digital asset to the buyer, as long as the buyer is the new owner or has access to the trackable digital asset.

DataLok Blockchain Updating Examples

Example 1

Hereinbelow is disclosed an example of a DataLok process for updating an encrypted trackable digital asset. It will be understood that the updating of the encrypted trackable digital asset is performed in response to a given event. In one or more implementations, the given event is selected from a group consisting of a transaction related to the encrypted trackable digital asset, a determined amount of time that has elapsed since the last given event, a request from a smart contract, a computing node, a processing device, a software, a storage device, a system manager, a request from a user and/or the like.

According to processing step E1, a trackable digital asset current owner decrypts a first encrypted trackable digital asset using a first password.

According to processing step E2, the current owner obtains a second password.

According to processing step E3, the current owner provides the second password to a user, a computing node, a smart contract, a system manager, a processing device, a storage device, a software, and/or the like.

According to processing step E4, the current owner provides a second encrypted trackable digital asset encrypted using the second password to a smart contract, a computing node, a system manager, a processing device, a storage device, and/or the like.

According to processing step E5, the second encrypted trackable digital asset is decrypted using the second password.

According to processing step E6, the trackable digital asset is authenticated.

According to processing step E7, upon authentication of the trackable digital asset, the smart contract, the computing node, the system manager, the storage device, and/or the like is informed that the trackable digital asset is authentic.

According to processing step E8, the first encrypted trackable digital asset is replaced by the second encrypted trackable digital asset.

Example 2

Hereinbelow is disclosed a second example of a DataLok process for updating an encrypted trackable digital asset. It will be understood that the updating of the encrypted trackable digital asset is performed in response to a given event. In one or more implementations, the given event is selected from a group consisting of a transaction related to the encrypted trackable digital asset, a determined amount of time that has elapsed since the last given event, a request from a smart contract, a computing node, a system manager, a processing device, a software, a storing device, a request from a user and/or the like.

According to processing step F1, a defined user decrypts a first encrypted trackable digital asset using a first password. In one or more implementations, the defined user is a previous owner of the first encrypted trackable digital asset.

According to processing step F2, the user obtains a second password.

According to processing step F3, the user provides the second password to a current owner.

According to processing step F4, the user provides a second encrypted trackable digital asset encrypted using the second password to a smart contract, a computing node, a system manager, a processing device, a software, a storage device, and/or the like.

According to processing step F5, the current owner decrypts the second encrypted trackable digital asset using the second password.

According to processing step F6, the current owner authenticates the digital asset (as elaborated upon under the "Authenticity Validating" section below).

According to processing step F7, upon authentication of the trackable digital asset, the smart contract, computing node, system manager, storage device, and/or the like is informed that the trackable digital asset is authentic.

According to processing step F8, the first encrypted trackable digital asset is replaced by the second encrypted trackable digital asset.

Example 3

Here is a DataLok process for updating one or more indications of a first encrypted trackable digital asset. The process comprises, in response to a given event, obtaining and decrypting the first encrypted trackable digital asset using a first password, the trackable digital asset being encrypted according to the “Creating -> Encrypting” section. The process further comprises encrypting one or more portions of the decrypted first encrypted trackable digital asset using a second password, thereby generating a second encrypted trackable digital asset. The process further comprises providing one or more indications of the second encrypted trackable digital asset to a smart contract, a system manager, a server, a processing device, a storage device, a software, a computing node, a blockchain, and/or the like. The process further comprises updating the one or more indications of the first encrypted trackable digital asset with the one or more indications of the second encrypted trackable digital asset.

Specifications

In one or more implementations of a DataLok process for updating an encrypted trackable digital asset, the process further comprises embedding data suitable for identifying the given event in the obtained and/or decrypted first encrypted trackable digital asset, the second encrypted trackable digital asset, one or more preview of the obtained and decrypted first encrypted trackable digital asset, an obtained preview of the obtained digital asset and/or one or more previews of a decrypted second encrypted trackable digital asset. In one or more implementations, the method for updating an encrypted trackable digital asset further comprises updating the one or more hashes of one or more portions of the trackable digital asset and/or providing one or more hashes associated with the trackable digital asset.

In one or more implementations of a DataLok process for updating an encrypted trackable digital asset, the providing of the one or more indications of the second encrypted trackable digital asset further comprises decrypting the second encrypted trackable digital asset and authenticating the decrypted second encrypted trackable digital asset.

In one or more implementations, a plurality of encrypted trackable digital assets, once decrypted, may be combined to provide a trackable digital asset.

Authenticity Validating

Hereinbelow is disclosed an example of a DataLok authentication of a given digital asset (GA).

According to a first processing step, the GA to authenticate and one or more hashes of one or more portions of a trackable digital asset (H1) are obtained, wherein H1 has been generated previously upon creation or updating thereof.

According to a second processing step, one or more hashes of one or more portions of the GA (H2) to authenticate are obtained.

According to a third processing step, an indication of a comparison between the H1 and the obtained H2 to determine the GA's authenticity is obtained.

It will be understood that the comparing would involve performing a hash comparison between the H1 and the H2. In the case where the hash comparison succeeds, the GA is determined to be authentic. In the case where the hash comparison fails, the GA is determined to be unauthentic.

According to a fourth processing step, the indication of the comparison is provided. In one or more implementations, the obtaining of the digital asset comprises digitalizing an asset. For instance, an asset, such as a painting or a book, may be physically provided and digitalized, thereby creating a corresponding digital asset. In one or more implementations, the providing of the encrypted trackable digital asset further comprises transforming the encrypted trackable digital asset into a trackable asset, such as by printing, 3D printing, and the like.

It will be understood that an asset may be obtained in the form of a photograph, a painting, a written or printed document, and/or the like. In one or more implementations, the asset may be obtained in the form of a quick response (QR) code, a magnetic storage, a barcode, and other relevant types of assets.

For instance, an encrypted trackable asset may be digitalized, decrypted digitally, and authenticated by validating the data embedded in the asset. Thus, it will be understood that DataLok can be used for various purposes and in various ways.

The authenticity of the GA can be established in a number of ways, according to the GA and DataLok's implementation. For instance, in the example where the GA is a pair of shoes with chips, such as NFC chips, in them, the authenticity can be established by validating the data embedded in the shoes. The data may include, for example, a manufacturer's name, a size, a color, a style, etc. In one or more implementations, the data may be encrypted and/or hashed, or an indication thereof (for example an URL). In one or more implementations, the authenticity is further established using physical engraving and/or physical steganography on said shoes. For example, an unalterable element, such as a QR code or barcode, may be engraved in the shoes. Another example would be to include a unique identifier, such as a serial number, in the shoes. This could even extend to alterations in color and/or pattern in the shoes.

Tracking

It will be understood that a trackable digital asset may be tracked in a number of ways. For instance, an asset owner may use scraping techniques to locate the asset online. Once the asset owner locates the asset online, he or she may then validate that the one or more asset hashes are the correct ones and/or that the embedded pre-creation data is present in the trackable digital asset. In this way, the asset owner may be able to track the asset and determine its authenticity. Additionally, other tracking methods may be used in conjunction with or instead of scraping techniques. For instance, an asset owner may use a search engine to locate the asset online, or he or she may use a tracking service that is designed to track assets. Regardless of the method used, it will be understood that tracking a trackable digital asset is possible and that doing so may help to determine the asset's authenticity.

Physical assets may also be tracked in a number of ways. For instance, in a situation where a given asset using DataLok involves said asset connecting to the world wide web, tracking said asset may be performed similarly to tracking a trackable digital asset. That is, an asset owner may use scraping techniques, a search engine, or a tracking service to locate the asset online.

DataLok – Advantages

A first advantage of DataLok is that it enables the preservation of the authenticity of a digital asset when trading thereof, thus enabling the trading of digital assets similarly to the trading of physical assets, thereby adding value to the digital assets. For instance, a person purchasing a digital asset that is known to be authentic will tend to give a greater value to the digital asset than if the authenticity cannot be established or confirmed. Further, the fact that the digital asset is trackable encourages buyers and, if and when applicable, artists to join a system using trackable digital assets compared to one not using DataLok. Furthermore, knowing that a digital asset is authentic and that the digital asset has been indeed originally created by its creator prevent the trade of fraudulent digital assets.

A second advantage of DataLok is that encrypting the trackable digital asset and/or the password to encrypt the trackable digital asset enables to secure a digital transfer while minimizing the risk of theft. In addition, because of data embedded in the digital asset and the one or more hashes of one or more portions of the trackable digital asset, if the digital asset and/or the trackable digital asset is leaked by a buyer and/or a seller, malicious individuals will be unable to claim ownership of the digital asset and/or the trackable digital asset.

A third advantage of DataLok is that it is possible to track digital assets with the data embedded therein, thus possibly enabling imposing limitations on the use and trade of trackable digital assets, such as, and without being limited to, preventing the trackable digital assets to be stored in determined databases or prohibiting the trade of non-trackable digital assets and/or trackable digital assets in determined blockchains or marketplaces.

A fourth advantage of DataLok is that, in one or more implementations, it is possible to decrypt an encrypted trackable digital asset without a user having to remember a password that encrypts the trackable digital asset, since an identifier encrypting the password may be automatically used to recover the password and therefore enables to decrypt the encrypted trackable digital asset without having the user to provide the password.