Technical Disclosure Commons

Defensive Publications Series

December 10, 2018

Content provenance attribution and verification via blockchain certification

Daniel Golovin

Daniel Klein

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Golovin, Daniel and Klein, Daniel, "Content provenance attribution and verification via blockchain certification", Technical Disclosure Commons, (December 10, 2018)
https://www.tdcommons.org/dpubs_series/1766

This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Content provenance attribution and verification via blockchain certification

ABSTRACT

Content such as images is sometimes used online without proper permission or attribution by parties other than content creators and owners. Prior to use, such parties may also alter the content as well as associated metadata. Such practices subvert rights of the content creators and owners and can mislead readers due to a lack of cues that can help determine the provenance, veracity, and credibility of the content.

This disclosure describes a mechanism to track, verify, and attribute provenance to content such as images. Per techniques of this disclosure, provenance information signed with a user's private key is included in the EXIF block of an image. With the user's permission, the image is uploaded to a globally trusted party that uses blockchain to certify the signed provenance information. Other parties can then traverse the certified blockchain to verify provenance.

KEYWORDS

- Image provenance
- Photo provenance
- EXIF
- Image metadata
- Blockchain
- Trusted party
- Content attribution
- Content verification
- Copyright

BACKGROUND

Online or other digital media content, such as photos, audio recordings, text, etc. can be easily copied by parties other than the owner. Such parties may use the content without proper permission and/or attribution. Prior to use, such parties may also alter the content as well as associated metadata. Such practices subvert rights of the content creators and owners and can mislead readers due to a lack of cues that can help determine the provenance, veracity, and credibility of the content.

DESCRIPTION

This disclosure describes a mechanism to track, verify, and attribute provenance to content such as photos. With a user's permission, salient details about photos posted by the user are stored in the EXIF metadata block of the image file. These details can include metadata such as a cryptographic hash of the file bits, a timestamp associated with the photo (e.g., that indicates when the photo was taken), GPS coordinates or other information regarding the location where the photo was taken, information regarding local wireless access points, encrypted user information obtained from the user's account, etc. Users are provided with options to selectively include such a metadata block, to not provide certain details, and to select individual pieces of metadata that are included.

The data included in the EXIF block is signed with the user's private key and the signature is appended to the EXIF block. If the user permits, the photo is uploaded to a globally trusted party that uses blockchain to stamp the signed provenance information in the EXIF block with its imprimatur along with signed verification information, such as upload date, network address of the device that performed the upload, permitted user account information, etc.

As long as the stamping party can be trusted, the signed provenance can no longer be altered since the upload can occur only after image creation and the included user account information is verifiable. The original photo with the provenance information in the EXIF block may be uploaded to multiple trusted parties for respective stamping, thus providing a more verifiable provenance chain. The trusted parties can be incentivized to provide such stamping services based on collective benefits, similar to PGP.

Once photo provenance has been stamped by one or more trusted parties, the user can provide the signed version to interested parties, such as newspapers or websites that publish the image. Similarly, publishers can use blockchain to chain the signed version of each photo they use. Instead of crediting the photo with the name of the content creator or owner, such signed photos can be credited via a URL that serves as a unique ID to the blockchain-signed image that can then be used for determining veracity.

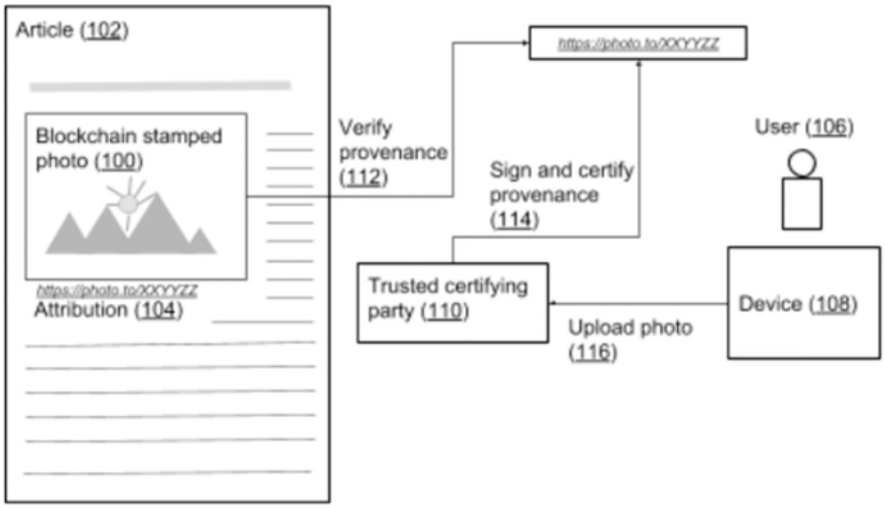

Fig. 1. Attributing and verifying photo content via blockchain signed provenance information

Fig. 1 shows an example implementation of the techniques described herein. An online publisher utilizes a blockchain stamped photo (100) in an article (102) posted on its site. The

photo is accompanied by an attribution (104) that includes a unique URL that points to the certified photo. Blockchain information in the photo can be decoded to verify its provenance (112) indicating that the photo was taken by a user (106) with a device (108) and uploaded (116) to a trusted party (110) that signed and certified the provenance (114).

In certain cases, publisher needs may necessitate altering the original photo. For instance, the photo may require resizing, cropping, blurring, removing identifiable information, etc. In such cases, the publisher can generate the provenance information for the new photo derived from the original and get it signed and stamped from the trusted certifying party. The publisher can then simply append the provenance blockchain of the original photo to the certified provenance of the derived photo. As a result of including the entire blockchain in the derived photo, the provenance is traceable back to the original photo, thus making it possible to verify the photo's origins. In contrast, publishers that publish original or derived photos without the corresponding provenance blockchain risk jeopardizing their credibility because people may not trust the veracity of the photos. In addition to supporting credibility verification, the provenance blockchain provides a mechanism for photo creators and owners to establish their claim over a photo and obtain appropriate credit and compensation.

Practical implementation and adoption of the techniques of this disclosure requires minor modifications to existing software and systems for photo capture (e.g., cameras), photo editing (e.g., image editing applications), and storage . Also, the techniques can be packaged as an external plugin as long as the relevant EXIF information is appropriately preserved.

The techniques can be utilized by any online publisher, such as newspapers, magazines, websites, blogs, etc. With slight modification or via an external plugin, a web browser can automatically traverse the provenance blockchain and signal the results to the users via

appropriate indicators and warnings, e.g., similar to the operation of SSL certificate chain verification for encrypted content. For example, if the blockchain provenance cannot be verified, the browser can provide a warning such as “Warning: This photo may not be trustworthy because the source could not be verified.” Similar warnings can be displayed if attribution information is missing altogether.

Although the above description is based on photo content, the mechanism can be extended to apply to any digital content. For instance, the techniques could be used for text reports, email threads, citations, audio recordings, music, etc.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (e.g., information about a user’s social network, social actions or activities, profession, a user’s preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user’s identity may be treated so that no personally identifiable information can be determined for the user, or a user’s geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

This disclosure describes mechanisms to track, verify, and attribute provenance to content such as images. Provenance information signed with a user’s private key is included in the EXIF block of an image. With the user’s permission, the image is uploaded to a globally

trusted party that uses blockchain to certify the signed provenance information. The user can provide the signed version to publishers and publishers can use blockchain to chain the signed version of each image they use, either unaltered or in a derived form. Signed photos can be credited via a URL that serves as a unique ID to the blockchain signed image that can then be used for determining veracity. In addition to supporting credibility verification, the provenance blockchain provides a mechanism for creators and owners to establish their claims over content.