RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

How Blockchain can be used for Verifying the Authenticity of Video/Image

Ajad, C S Raghuvanshi, Hari Om Sharan
Faculty of Engineering & Technology, Rama University,Mandhana, Kanpur 209217, INDIA
Email Id: *ajad126@gmail.com*

***Abstract*—With the explosive advancement of modern technolog y we heavily rely upon digital data in the form of video and image. Digital content has been the norm for quite a few years in all aspects of modern society for ease of use and conveniences. Relevant visual information may be utilised in a range of settings, such as the media, law enforcement, publications, legal procedures, medical imaging, the military, and consumer museums. Though the development of advanced technology with the help of sophisticated artificial intelligence(AI) algorithms have opened the door to temper digital data and contents. [1] This misinterpretation of advanced technolog y has made the integrity of the video/image file questionable. [2] In the context of using the video/image file in court or any other places for presenting proof have been disputable. In this research article I present a framework for verifying the authenticity of video/image using blockchain technolog y. Using this framework the deep-fake problems can be countered and a layer of trust can be established verifying the integrity of the visual contents. The IoT device capturing the image or video file computes a hash before the data leaves the device. Then the hash is stored in a blockchain system to provide a transparent way to check the integrity of the file.**

***Index Terms*—Blockchain, video/image integrity verification, Security**

I. INTRODUCTION

Blockchain technology has been popular for some years now due to the boom of digital curren-cies like Bitcoin, Etherium etc. The core idea of blockchain is to get rid of any mediator to establish a proof of transaction. In the realm of cryptocur-rency blockchain has thus been capable of providing a peer to peer direct transfer of funds without the need for a mediator. This solves two major problems - i. The integrity of the transaction or the validity of the transaction is established without the chance of any conflict between the two parties ii. The chance of fraudulent of the mediator comes to zero as the mediator is not needed while doing the transaction using blockchain system. [3] There have been multiple research on how blockchain technology can be used in various fields of trans-action or the places where a proof of transaction is a must. Modern society heavily rely upon digi-tal data. But the rise of sophisticated technologies capable of altering a video or image file has made any video or image questionable. There is multiple ways of forging a visual content with the help of latest technology. Some techniques that can alter a visual content are inter- frame video counter-fitting, frame insertion, frame deletion, frame duplication, frame manipulation etc. In this paper we will try to understand how a blockchain can help us combat digital content forgery. The main purpose of this article is to provide a way to establish the veracity of visual materials that utilizes blockchain technology in conjunction with visual content forensics. In this method the image or video segments are hashed and then saved in a chronological sequences as chain of blocks. These blocks are traceable but cannot be altered in any method. This ensures that the information stored in the block is genuine and accurate that have not been tempered with.

II. BACKGROUND

A. Blockchain Technology

Blockchain technology consists of blocks that are connected with each other and contains hash and the hash of the previous block. It is possible to create a new block but it is impossible to alter data in an existing block of a blockchain. [4] The

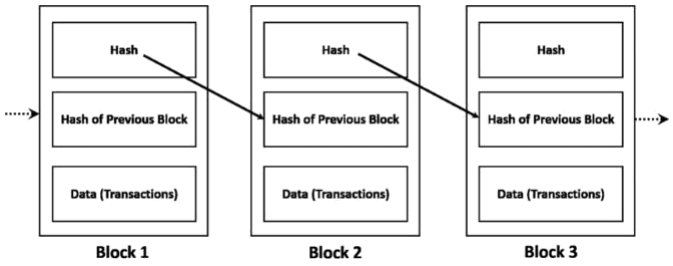

Fig. 1. Blockchain nodes

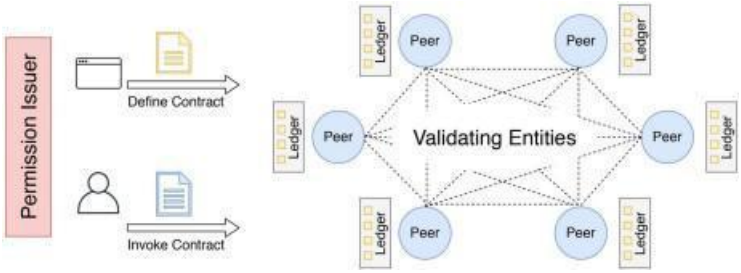

Fig. 2. Hyperledger platform

integrity of a blockchain is maintained at its core and it uses public key encryption for all network interactions and updates. Blockchain is build upon a decentralized ledger where each block has a own copy of transaction details and records.

B. Consensus protocol

In a blockchain a new node is added through a protocol. In that protocol the insertion of a new node is approved within the block and provides an agreement on the last state of blockchain. There are mainly two types of blockchain mechanism based on blockchain structure, Permissioned and Public. The most popular blockchain technology used in today's world, the cryptocurrencies, fall into public blockchain category. The consensus is established by the mechanism called proof of work.

[5] This proof of work forms a hash puzzle and it requires previously computed hash value. This type of consensus brings a solid security chain. Apart from that a permissioned blockchain utilizes some byzantine fault tolerant voting system which does not require heavy computational resources for hash puzzles. This makes permissioned blockchain less time consuming system, Though more than two thirds of total nodes permissions are required to make the blockchain trustworthy. [6]

C. Hyperledger

Hyperledger is an open source community built on linux foundation for developing blockchains, projects, frameworks and tools. Hyper-ledger has been a successful open source project which is funded by big tech giants like Intel and IBM to create collaborative ledges. Hyperledger is a type of permissioned blockchain where only the blocks having required permission can access the blocks. This is different from the public blockchain system.

Applications that use hyperledger includes financial systems, banking, healthcare systems etc. The access permissions of blocks are calculated using a voting based consensus algorithm. If there are n number of nodes in a blockchain system, a consensus can be achieved if (2n-1)/3 numbers of nodes are true.

D. Device Fingerprint

Different digital content recording device has some different unique identification attributes. The video/image recording devices can be identified using hardware parameters of the device. some applications require determining extrinsic parameters. Such as focal length, scale factor etc for camera devices. [7]

III. BLOCKCHA IN BASED DIGITAL CONTENT VERIFICATION SYSTEM

A. Architecture

A camera embeded surveillance system records video footages and transmits that recorded footages over to a remote server. To accomplish the secu-rity standard of video verification unique signature by the recording device is utilized. The recording device uses cryptographic signature mechanism to securely sign the video footages while it leaves the device. When a device is set to be used to record video/image the unique identification key of that device is registered in the system. Apart from generating unique key for each device in the system a sample video is taken along with the fingerprint of that specific device. This can help in future to determine whether the source of the video footage is genuine or not. While recording a footage the device performs a secure hash function internally

and while transmitting the footage in the server. The blockchain can then use querying methods via smart contract to match the stored hash with the hash coming from the device while recording. This way the integrity of a video footage can be verified.

B. Segmentation

While recording a footage through a device there is two options in hand. One is to wait for the completion of the recording and then sending the video along with the required hash to the blockchain and another is instead of waiting for the video to be recorded completely sending the video footages or images in small chunks to along with the hash to the blockchain. The later approach is more convenient and efficient. In wireless systems and embedded recording devices there may arise multiple prob-lems. Such as hardware failure, network failure and other technical problems. In this case if we wait for the recording of the footage to be completed and in the middle some error occurs we loose the whole video. But if we set up the system in such a way that our device computes hashes for smaller segments of the recorded video and transmits the data to the blockchain we may not loose the previously recorded data if any failure occurs. [8] This type of video segmentation can be achieved in multiple ways inside the video/image recording device. There are many tools that can help us achieve this type of video segmentation. Such tools include opencv, mpeg-dash, ffmpeg streamer etc. Though this type of tools can make our recording device resource heavy but for low resolution footage it is feasible.

C. Sending video hash to blockchain

The device which is entitled to record the video footage transmits the hash and the video to the hyperledger system. The video integrity verification can be achieved by using the blockchain method to store the video or image content making it immutable. The device calculates a hash function every time data is fed into the blockchain. [9] It updates the hash value with new arriving data. h (a + b) = h.update (a) + h.update (b) .

This way the has function does not have to wait for the video to be recorded completely. The video is sent instantly form the recording device that is

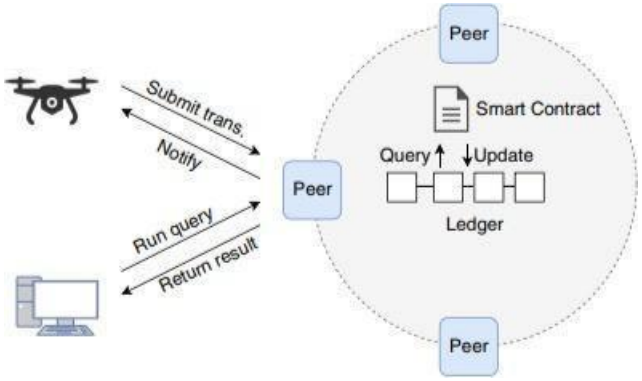

Fig. 3. end device interaction with hyperledger

enabled with streaming. There are multiple options for hash functions such as MD5, SHA2, SHA3 etc.

D. Integrity verification

Integrity verification process consists of some steps. The steps include has recalculation, query in the blockchain and validation. [10]

- The first step involved in verifying the integrity of the file is to compare the video segments in the blockchain. This method involves hash recalculation to verify the signature of the file.
- When a segment is queried in the blockchain the previous hash is queried with other saved metadata such as video Id and recording device fingerprints.
- The query in the blockchain will return the hash stored in the hyperledger. Then the retrieved hash and the computed hash are compared with each other. If the two hashes match we can say the video is authentic or has not been altered. But if the has does not match we can conclude that the video is altered and cannot be trusted.

IV. CONCLUSION

This paper presents a way to verify the integrity of a video/image file using the blockchain technology. In this method hyperledger technology is used to set up a blockchain system. This paper can help developing a trustworthy surveillance system that is transparent and trustworthy. I believe this paper makes new amends in the field of blockchain technology and the idea of integrity verification system using blockchain.

REFERENCES

[1]Rashid and M d M amunur, Lee, Suk-Hwan and Kwon, Ki-Ryong. (2021). Blockchain Technology for Combating Deep - fake and Protect Video/Image Integrity . Journal of Korea M ulti-media Society . 24. 1044-1058. 10.9717/kmms.2021.24.8.1044.

[2] Javed, Abdul Rehman, Jalil, Zunera, Zehra, Wisha,Gadekallu, Thippa , Suh, Doug , Jalil Piran, M d. (2021). A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions. Engineering Applications of Artificial Intelligence. 106. 104456. 10.1016/j.engappai.2021.104456.

[3] Zheng, Zibin and Xie, Shaoan and Dai, Hong-Ning and Chen, Xiangping and Wang, Huaimin. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[4] Xu, M ., Chen, X. Kou, G. A systematic review of blockchain. Financ Innov 5, 27 (2019). https://doi.org/10.1186/s40854-019-0147-z

[5] Lashkari, Bahareh and M usilek, Petr. (2021). A Comprehensive Review of Blockchain Consensus M echanisms. IEEE Access. PP. 1-1. 10.1109/ACCESS.2021.3065880.

[6] Ruihang Huang, Xiaoming Yang, P. Ajay, Consensus mechanism for software-defined blockchain in internet of things, Internet of Things and Cyber-Physical Systems, Volume 3, 2023, Pages 52-60, ISSN 2667-3452,

[7] Golj an, Mi rosl av F ri dri ch, J ess i ca F ill er, Tom a´s . (2009). Large scale test of sensor fingerprint camera identification. Proceedings of SPIE Conference on Electronic Imaging, Se-curity and Forensics of M ultimedia Contents XI. 7254. 72540. 10.1117/12.805701.

[8] Ngan, King Li, Hongliang. (2011). Video Segmentation and Its Applications. 10.1007/978-1-4419-9482-0.

[9] M acharia, Wahome. (2021). Cryptographic Hash Functions.

[10] Yong, KK Karuppiah, Ettikan. (2013). Hash match on GPU. 2013 IEEE Conference on Open Systems, ICOS 2013. 10.1109/ICOS.2013.6735065.