Lightweight blockchain to solve forgery and privacy issues of vehicle image data

Dongjun Na and Sejin Park

Department of Computer Engineering, Keimyung University, Korea.
nadongjun@kmu.kr, baksejin@kmu.ac.kr

***Abstract*—This paper proposes a method of using a blockchain to solve the privacy problem and forgery of black box image data, which plays an essential role in determining the responsibility for traffic accidents and preventing accidents. Blockchain that can operate inside vehicle black box IoT or connected car is used, and for this purpose, the size is reduced for operation in low-power, low-capacity devices. By enabling consensus, security problems can be solved through a lightweight blockchain that can operate inside a black box device. As a result of the experiment, it was confirmed that the IPFS upload and download delay time increased linearly, and the proposed consensus algorithm decreased 63% compared to PBFT.**

Keywords—lightweight blockchain, consensus algorithm, event data recorder, video event data recorder

I. Introduction

In the event of a recent traffic accident, it is possible to easily determine the responsibility of the accident, and to record the traffic accident situation in public transportation facilities such as taxis and buses and private vehicles for reasons of high accident prevention effect. Vehicle video recording black box (VEDR: Video Event Data Recorder) and accident recording device (EDR, Event Data Recorder) that can store driving information and check the stored information for a certain period of time before and after the accident of the vehicle are increasing. have. As a result of a survey of 1,000 adult men and women nationwide who drive directly more than once a month on average by the market research company Trend Monitor[1], 95.3% answered that they needed a black box, and they thought it was necessary. It was "to cover up the errors in the occurrence of an accident" and "to use them as evidence in case of denying the wrongs". Black box video is essential for evidence of accidents in traffic accidents, and security for video data is important. However, according to [2], there is a security problem for vehicle black box data. The most direct problem among security problems is the forgery and alteration of image data stored in the black box. In the case of vehicle black box image data, it is used as a reference for identifying the cause of an accident and judging the accident situation, and the accident data can also be used as legal evidence. Since the vehicle black box is accessible only to limited users, such as the vehicle owner or driver, it has perfect access rights to the black box image data attached to the vehicle, and there is no time constraint required to perform an attack. Therefore, general vehicle black box data is always exposed to the possibility of forgery and alteration. Vehicle black box image data uses its own memory or SSD memory, and if necessary, the stored data may damage the memory itself and interfere with the use of the image data if the user is unfavorable. Although the standard for preventing forgery and alteration has been added to the actual KS standard [3], the possibility of forgery and alteration still exists. In addition, some image data stored in the memory can be partially deleted, forged, or changed according to the user's interests. Also, the black box has privacy issues. In the case of a black box attached to a commercial vehicle to accurately identify an accident in the event of an accident, personal information such as phone records and conversations of users in an enclosed space can be recorded by recording video and audio inside the vehicle, which may infringe on privacy. In addition to commercial vehicles, black boxes used in personal vehicles also start to operate, and the driving route and driving habits of the driver are stored in the server. If the information stored in the black box is leaked through an unintended route, it may invade the driver's privacy. In order to solve this problem, reliability, integrity, and confidentiality of the black box image data are required. Blockchain[4] technology and PKI (Public Key Infrastructure) encryption technology are suitable for solving this problem. Blockchain technology does not use a central server and stores the managed data in a distributed data storage environment based on a chain-type link created based on the P2P method, so that the managed data is stored in a distributed data storage environment. It is a ledger management technology based on distributed computing technology that allows you to view the results. However, in order to apply the blockchain, the following problems must be solved

A. Problems

(1) Blockchain size problem: Blockchain is a decentralized data storage technology in which all nodes in the network store the same blockchain ledger. Because of this, all nodes must store the same blockchain, so it is not possible to maintain the blockchain within the black box device due to the constantly increasing blockchain size. (2) Consensus Algorithm Latency Problem: The blockchain consensus algorithm uses an algorithm that uses a lot of CPU and memory, such as PoW. The PBFT consensus algorithm, which only agrees through network communication, also has a latency problem in the wireless network situation of the black box due to the amount of traffic of N^2. (3) Data privacy problem: In the blockchain, data is transparently disclosed to all nodes because all nodes store the same

blockchain, so there is a data privacy problem. Blockchain nodes are operated in places such as black box IoT(Internet of things)[5] and connected cars[6], which have limitations in performance due to the problem of increasing the size of the block chain and CPU and memory usage of the consensus algorithm. Cloud[7] or edge computing[8] technology is used, and the blockchain full node cannot operate, and the problems caused by the existing centralization cannot be solved.

B. Contribution

In this paper, we solve the aforementioned problems (1), (2), and (3) to solve the forgery and falsification and privacy problems of black box data. **(1) Off-chain solution** : To reduce the size of the blockchain, use the InterPlanet File System (IPFS) to distribute and store black box image data to reduce the weight. **(2) Self-Validating Consensus Algorithm** : In order to solve the problem of blockchain consensus algorithm latency, we propose a new consensus algorithm that makes consensus with lighter network traffic.**(3) Encription :** To solve the privacy problem of black box data, data is encrypted with a public key through PKI so that only specific users with private keys can access the data.

This paper is written in the following order, explaining the blockchain, consensus algorithm, IoT, and connected car, the architecture and consensus algorithm of the proposed blockchain, and an experiment for performance measurement.

II. Related Work

This section describes the blockchain, consensus algorithm, and IoT, connected car blockchain.

A. Consensus algorithm

In PBFT (Practical Byzantine Fault Tolerance) [10], one participant in the network becomes the leader and sends a request to all participants including themselves. After the result of the request is aggregated, the block is confirmed using multiple values. If the number of illegal nodes is n, the number of nodes must be 3n + 1, and n + 1 or more nodes are required for confirmation.

PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain proposes a lightweight consensus algorithm for the scalability of IoT devices[11]. In this paper, based on Hyperledger Fabric's consensus algorithm, an agreement is reached through a total of three steps 4. As the network is divided into Node/Peer Network and Session Nodes, if the Src and Dst devices belong to the same node, a local agreement is reached, and if not, the delay time is reduced by executing PoBT by verifying through the chaincode.

B. IoT Blockchain

- IoT refers to a technology that connects various objects through wireless communication by connecting to the Internet by embedding sensors and communication functions in various objects. Internet-connected objects exchange data and provide the user with the information they have analyzed and learned by themselves, or the user can remotely control it. In the case of IOTA[12], a blockchain platform for IoT was developed. However, it uses PoW as the consensus algorithm and has a high hardware requirement, so it is not suitable for operation in IoT devices.

III. Architecture

A. Architecture

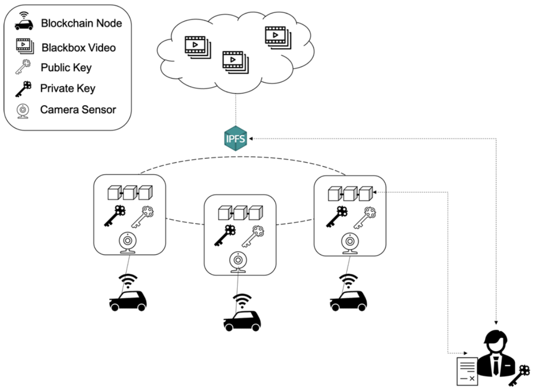

Fig. 1. Architecture

Fig 1. is the architecture of the blockchain proposed in this paper. Blockchain nodes operate on the in-vehicle IoT device or on-board of a connected car, maintain the blockchain, upload images and encrypt them with public keys to create transactions. IPFS is a distributed storage of image data generated by blockchain nodes. After that, it plays a role of lightning with IPFS hash. Users can access the black box video data by decrypting the IPFS hash stored in the blockchain only if they have the private key and have the authority.

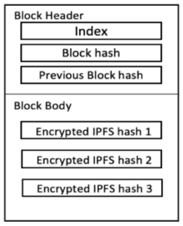

Fig. 2. Block structure of the proposed blockchain

Fig. 2 is the block structure of the blockchain proposed in this paper. In the block header, there is an index, which is the number of the block, and the hash value of the block before the block hash that hashed all the data in the block. In the Block Body, there is an IPFS hash value encrypted with the public key held by the nodes of the blockchain network. The user or administrator can access the black box image by decrypting it through the private key.

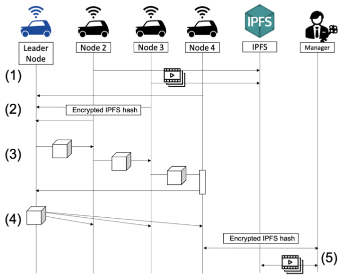

Fig. 3. Sequence diagram of the proposed blockchain

Fig. 3 is a blockchain sequence diagram proposed in this paper. Among the nodes of the blockchain network, (1) a leader node is randomly selected, and (2) the blockchain node uploads video data to IPFS, encrypts the returned IPFS hash, creates a transaction, and sends it to the leader node. (3) The leader node creates a block with the transmitted transaction, and all nodes decrypt the transaction sent by themselves, verify the IPFS hash, and send it to the next node. (4) After that, the last node transmits the block to the leader node, and when the leader node confirms that all transactions in the block have been verified, it propagates the block to all nodes. (5) User or administrator can receive video data by decrypting IPFS hash through a private key.

B. Consensus algorithm

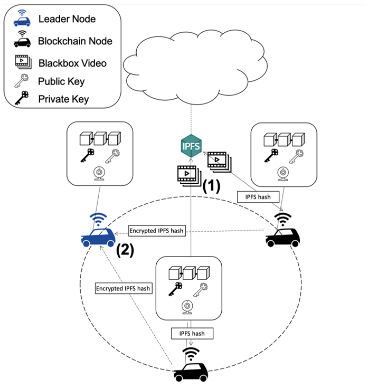

Fig. 4. Consensus Algorithm-Transaction Creation Process

Fig. 3 and 4 show the transaction and block generation process of the blockchain consensus algorithm to solve the network traffic proposed in this paper. (1) Blockchain nodes collect video data and upload the data to IPFS. After that, the IPFS hash is returned and stored in the local storage. (2) The IPFS hash is encrypted with a public key and the transaction is transmitted to a randomly selected leader node.

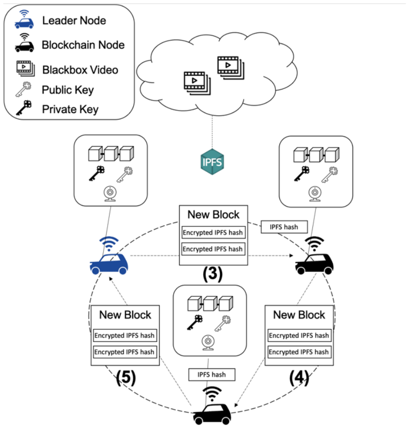

Fig. 5. Consensus Algorithm-Block Consensus Process

(3) The leader node creates a block through transactions transmitted by nodes in the blockchain network, receives blocks sequentially according to a preset path, and stores the IPFS hash value created by the node among the transactions in the block in the local storage. If the value is the same, it is verified and passed to the next node. Thereafter, after the same process in the order of **(3)**, **(4)**, **(5)**, the block is delivered to the leader node again, and when all nodes are verified, the block is propagated, and the node that received the block is stored in the local storage. Delete the IPFS hash value.

IV. EXPERIMENT

An experiment was conducted to evaluate the performance of the consensus algorithm and the degree to which it affects the performance by uploading the black box video to IPFS on the blockchain and measuring the download delay time. In this experiment, the delay time for upload and download by transmitting video data to an IPFS client was measured.

TABLE I. DATASET

Resolution	***FPS(Frame Per Second)***
320x240px-2560x1440px	8-60

*The vertical resolution of the image * the horizontal resolution of the image * the color of the image (bits) * frames per second of the image / 8 = image capacity* (1)

Table 1. is the resolution and frame of the black box image data on the market, and (1) is the method of calculating the image capacity. The experiment was performed by calculating the size of the black box image data on the market using the equation. The video time was unified to 10 seconds. The fps of the video with the maximum resolution and the minimum resolution is 30fps, which is a video frame rate determined by the KS standard [14], and an image of 10 seconds before and after an accident was assumed. The resolution of the image is 1280x720 and the size is 20.4MB. In addition, by uploading and downloading video data of 10MB, 30MB, 40MB, and 50MB capacity, the increase in delay time according to the increase in capacity was confirmed.

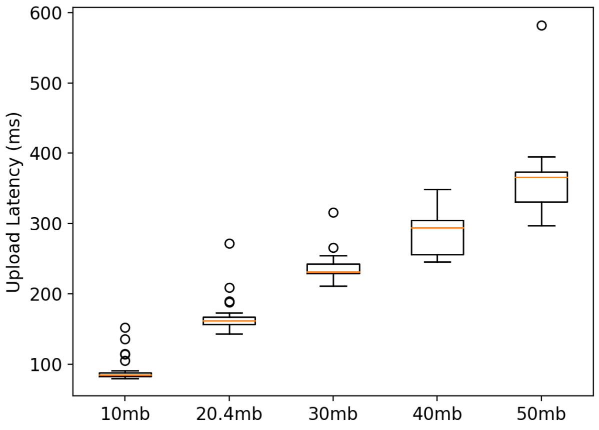

Fig. 6. Black box video upload delay time

Fig. 6 is a graph showing the delay time when uploading 10MB, 20.4MB, 30MB, 40MB, and 50MB of video data of the size included in the standard of black box video to IPFS. In the case of the standard size of 20.4MB, it took a minimum of 143 and a maximum of 272ms, and the increase according to the upload capacity also increased linearly.

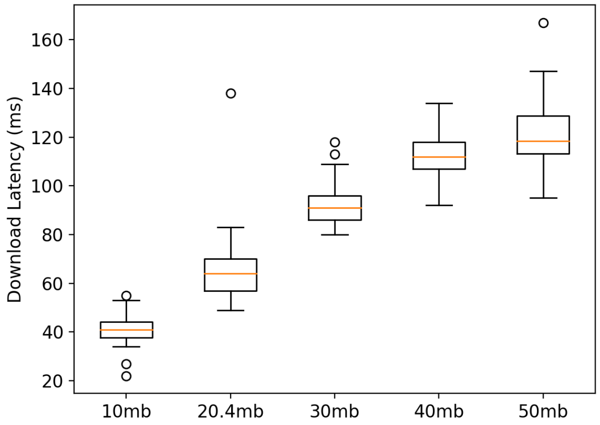

Fig. 7. Uploaded black box video download delay time

Fig. 7 is a graph when downloaded images of 10MB, 20.4MB, 30MB, 40MB, and 50MB as the IPFS hash value returned after uploading to IPFS. Downloading the standard size of 20.4MB took a minimum of 49 and a maximum of 138ms. In addition, as the download capacity increased by 10MB, the delay time increased linearly. From the results of both graphs, it was confirmed that the 20.4MB capacity for both upload and download took a delay time that did not affect performance, showed a linear increase, and was not significantly affected by the increase in size.

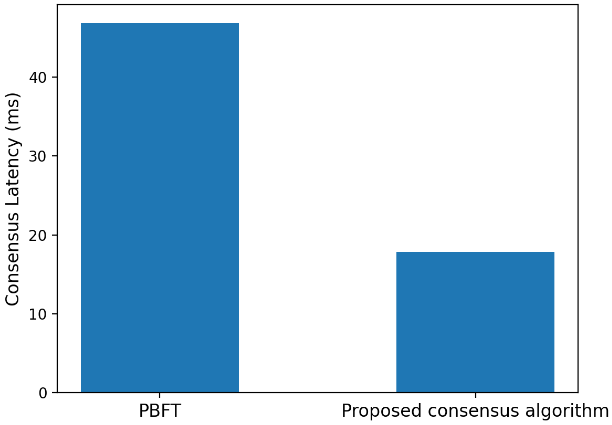

Fig. 8. Comparison of average delay time of consensus algorithm

Fig. 8 is a graph comparing the performance of the blockchain consensus algorithm proposed in this paper and the PBFT consensus algorithm. For the experiment, the consensus delay time was measured by connecting three blockchain nodes. The experiment was conducted using three RaspberryPi 4 B (System on Chip: Broadcom BCM2711, Quad core Cortex-A72 (ARM v8) Memory: 4 GB). As a result of the measurement, the PBFT took an average of 46ms, and the proposed blockchain consensus algorithm took only 17ms on average.

V. Conclusion

In this paper, a lightweight blockchain was proposed to solve the problem of forgery and alteration of black box image data and privacy. After uploading a video to IPFS, the video size is reduced to 46 bytes, which is the IPFS hash size, and is saved in the blockchain, and it was confirmed that the delay time of upload and download does not significantly affect the performance, and the increase in the delay time according to the capacity is also linear. In addition, through a new consensus algorithm, network traffic is reduced to reduce latency, and by encrypting the IPFS hash value stored in the blockchain with the user's public key, only users with a private key can access the video data, thereby ensuring privacy.

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2020-0-00936, (Core Technologies for 5G-Aware Blockchain Networks)

References

[1] Sejin Kim,datasom.(http://www.datasom.co.kr/news/articleView.html?idxno=99167)

[2] Kim, M. S., et al. "Security Issues and Trends in Automotive Black-box." Electronics and Telecommunications Trends 27.4 (2012): 123-129.

[3] Joins (https://news.joins.com/article/17356039)

[4] Blockchain. (https://en.wikipedia.org/wiki/Blockchain)

[5] Internet of things. (https://en.wikipedia.org/wiki/Internet_of_things)

[6] Tamás Bécsi; Szilárd Aradi; Peter Gáspár, "Security issues and vulnerabilities in connected car systems," 2015 International Conference on Models and Technologies for Intelligent Transportation Systems.

[7] Steve Ranger, What is cloud computing? Everything you need to know about the cloud explained, ZDNet(zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/).

[8] IBM, What is edge computing? (https://www.ibm.com/cloud/what-is-edge-computing)

[9] Sorin Zoican, Marius Vochin, Roxana Zoican, Dan Galatchi, "Blockchain and Consensus Algorithms in Internet of Things" in International Symposium on Electronics and Telecommunications ISETC 2018.

[10] C. Miguel and L. Barbara, "Practical byzantine fault tolerance," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, pp. 173-186, 1999.

[11] Sujit Biswas; Kashif Sharif; Fan Li; Sabita Maharjan; Saraju P. Mohanty; Yu Wang , "PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain", IEEE Internet of Things Journal (Volume: 7, Issue: 3, March 2020)

[12] I. Foundation. (2018) Iota. [Online]. Available: https://www.iota.org/

[13] Mumin Cebe; Enes Erdin; Kemal Akkaya; Hidayet Aksu; Selcuk Uluagac,"Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles", IEEE Communications Magazine (Volume: 56, Issue: 10, OCTOBER 2018)

[14] Vehicle black box video transmission and management system that ensures integrity, Jonghwan Hyun, Jaeyoon Jeong, Khan Lee, James Won-Ki Hong , KNOM Conference 2013, DaeGu, Korea, May 9-10, 2013, pp. 140-141. (WCU, CMEST support)