Received: 10 April 2023 | Revised: 7 February 2024 | Accepted: 9 February 2024

DOI: 10.1002/cpe.8057

RESEARCH ARTICLE

WILEY

BLOCKBOX: Blockchain based black box designing and modeling

Cagatay Korkuc[1] | Nilay Aytas Korkmaz[2] | Yasin Genc[1] | Ahmet Akkoc[1] | Erkan Afacan[1] | Erdem Yazgan[3]

[1]Electrical and Electronics Engineering, Gazi University, Ankara, Turkey

[2]Electrical and Electronics Engineering, Kirikkale University, Kirikkale, Turkey

[3]Electrical and Electronics Engineering, TED University, Ankara, Turkey

Correspondence
Cagatay Korkuc, Electrical and Electronics Engineering, Gazi University, Ankara, Turkey.
Email: cagatay.korkuc1@gazi.edu.tr

Summary

With the development of technology, data has become more accessible. The storage of critical and valuable information is getting harder and harder with the increase of cyber attacks and vulnerabilities of network and internet. The centralized storage of data causes security and privacy problems. As a remedy to these problems, blockchain has occurred. The reliability, transparency, integrity and confidentiality of the data have been increased with the blockchain technology. Blockchain maintains the immutability of the data with cryptographic hash algorithms. The data is kept in distributed structures with the consensus algorithms so that it is not lost. Projects and studies using blockchain technology have shown that data stored in centralized structures is not as reliable as data that is distributed and secured by cryptographic algorithms, smart contracts, and consensus. The data of flights, which is a critical data, has a great place in world transportation. The parameters inside the black boxes guide us on why the aircrafts have crashed: whether the responsibility belongs to the manufacturer, to the pilot, or to the aircraft technicians. In this way, the real reasons of the accident may be determined and measures can be taken for the accidents that may occur afterwards. In addition, the safe delivery of all black box data to the interested parties and its storage in a way that is immutable will not only benefit to the manufacturer's self-development by processing the data, but also help flight companies to find optimum flight data. Both the flight companies and the manufacturer will be able to read the black box data, thus the suspicion of data manipulation will be eliminated and the data will become more transparent. In this study, a system is proposed in which an aircraft's black box data can be saved safely and securely with the help of blockchain technology.

KEYWORDS

black box, black box modeling, blockchain, hyperledger

1 | INTRODUCTION

With advances in information and communication technology (ICT), the data which is circulated on any network became more vulnerable because of cyber attacks and threats. Nowadays, with the increase in cyber attacks and cyber threats, many security products such as firewalls, intrusion detection and prevention systems (IDS-IPS), endpoint security products, data loss prevention systems (DLP) have been developed and continue to be developed in the field of cyber security. The security of data that is on the internet or on any network has become a matter of discussion. The

investments made by companies and even countries for data security continue to increase day by day. Both penetration and service interruption attempts such as denial of service (DoS) and distributed denial of service (DDoS), have reduced the trust in central systems.

This is how the idea of using distributed systems instead of centralized systems emerged.[1] If the attacker wanted to manipulate the data, he/she had to capture all the nodes at once or attack all the systems at the same time. With distributed ledgers, it has become almost impossible to change the information stored. But this time other problems occurred: In which centers was the data held correct? How did a change in one of the distributed ledgers affect the entire data? How was the network protected and how did the nodes or peers maintain their own security? The answers to all of these questions were found in the article "Bitcoin: A peer to peer electronic cash system" by a person named Satoshi Nakamoto in 2008.[2] Bitcoin, the first example of blockchain, seems like an interpersonal money transfer, actually became an answer for many unknowns in the world. The money transfer between people has been called as a transaction and it continues until the size of transactions reaches a certain amount. Then, they must be written in a block. Block is a structure that includes all the transactions. This block is linked to previous block by adding the hash algorithm of the previous block and a chain is formed in this way. These transactions are kept in distributed ledgers called miners around the world, and are confirmed by consensus of miners.

In Reference 3, it is claimed that this technology can be used not only in money transfers but also in asset transfer after Bitcoin, and a different perspective has been brought to the blockchain. In fact, the starting point is to establish a network where blockchain applications that uses smart contracts can run. Smart contracts are code pieces, stored in the blockchain network that automate the execution of a contract when predetermined conditions are met. Today, many applications run on the Ethereum network.

In the light of all this information, many applications are working with blockchain today. There are applications using blockchain technology in many sectors such as money transfer, data transfer, banking, finance, currency, voting, energy, supply chain, accounting, healthcare, insurance, energy, Internet of Things (IoT), real estate.[4,5] Some of these applications work on open blockchain networks such as Ethereum, Solona, Polkadot while others work on closed blockchain networks such as hyperledger. In open (permissionless) blockchain networks, everyone can participate consensus process to validate transactions, on the other hand, in closed (permissioned) blockchain networks, only participants who are allowed by administrators can join the network.

As it is well known, all aircrafts have to keep many flight data in devices called black boxes. Although the number of parameters to be kept from aircraft to aircraft varies, it is mandatory to keep the data in accordance with the legislation. Flight data recorder (FDR) and cockpit voice recorder (CVR) devices, which are called black boxes, play an important role in illuminating the accidents and determining the person responsible. If the black box is not found or becomes unusable, the cause of the accident may not be clarified. Since it is not clear whether the accident was caused by pilot error, weather conditions or the manufacturer, sometimes no precaution can be taken for the next accident and people lose their lives. The black box is only read by the manufacturer, so flight companies suspect that the information may have been manipulated.

In Reference 6, a tamper proof and verifiable blockchain based event recording system model, which can keep accident and records of autonomous vehicles is presented. The recording black boxes of trains which are named as juridial recording unit, are designed on blockchain network in Reference 7. Zugchain is a blockchain based train event logger that contains communication layer with Byzantine fault tolerance. This project accelerates the digitalization of railway systems and ensures the safe export of data. In Reference 8, it is explained how blockchain can be applied to vehicular networks (VANET). In this study, for a secure and distributed storage, Hyperledger Iroha is used because of its simplicity and unique design for good working with IoT applications. We have extended the propositions given in References 6–8 to aviation. A blockchain based data recorder using cloud systems is proposed in Reference 9. It is mentioned that open blockchain network is not appropriate for FDR because of transaction fees and time response but if smart contract can be applied on closed networks, it can be a useful for FDR.

The primary motivation for this research stems from the current limitations in FDR data management. Traditionally, only aircraft manufacturers can access this data, which poses significant risks in case of loss, leading to uncertainties in accident investigations and accountability. The post-accident research and the process to retrieve the black box incur substantial costs. Consequently, the study advocates for a shift from local storage to a distributed ledger architecture, ensuring data immutability, resistance to manipulation, and cost-effectiveness. The proposed solution involves securing FDR data against cyber threats like 'man-in-the-middle' attacks through cryptographic algorithms during transfer and storage. Establishing a consensus mechanism within the distributed ledger is crucial to validate data accuracy. Additionally, advanced software should manage authentication and data access.

Traditional methods can be used to retrieve data, but proof must be provided that the data received on existing storage units over the internet has not been altered. Moreover, if the data is transmitted in cleartext while being transmitted peer to peer, it becomes vulnerable to attacks and interception. If it is stored in a central structure rather than in distributed structures, it becomes a target against cyber attacks. If it is stored in cloud storage instead of traditional storage architecture, there is a need for a separate software that can act as a smart contract, perform both authentication and authorization management, and control data access. If FDR data will be transmitted, stored and accessed with an approach different from blockchain, there is a need to develop specialized software where only relevant flight companies can see the data of their own aircraft, and manufacturers can see the data of the aircraft they manufacture. The storage units where the data will be stored must be kept in a storage area that can only be accessed by flight companies and aircraft manufacturers and must be located in an isolated network that cannot be accessed by

anyone except the relevant companies. Even in such a case, it is almost impossible to ensure that traditionally stored data is secure, transparent and immutable.

The feasibility of this proposal is examined through the hyperledger fabric architecture, a permissioned blockchain network known for its immutability, transparency, and distributivity features. It employs membership service provider (MSP) and digital identity library for identity management, with digital certificates issued by a certificate authority (CA). The architecture, including CA, peers, orderers, MSP, and digital identity library, is deployed on Docker containers. CA provides the basis for an organization's actors to have a verifiable digital identity. Public key cryptography is used to prevent data interception, with practical Byzantine fault tolerance (pBFT) as the consensus mechanism. A smart contract, developed in Golang, manages authentication and data access. Distributed ledgers will ensure that data is immutable and they will be held on the centers decided by flight companies and manufacturers, which are currently located in different parts of the world. Instead of establishing a new network, existing systems will be used, thus it is expected that the costs will be reduced.

To the authors knowledge, blockchain technology has not been previously designed and realized in FDR technology. In this study, we propose that the black boxes data are kept in blockchain network. Considering that the data is encrypted and stored in the network in an immutable way, it is thought that it would be beneficial to use the blockchain technology. Section 2 presents the related works on the subject. Section 3 presents black box technologies, Section 4 presents blockchain technology and hyperledger. Section 5 explains project details for black box modeling. Section 6 mentions limitations and future works and the comments and results will take place in the Section 7.

2 | RELATED WORKS

In the literature, a lot of studies have been done on the development of black box technology: black box search,[10,11] cyber security of aviation technology,[12,13] new approaches for black box design.[14–17] Over time, black box technologies have been developed and legal tightening has been made.

FDR has been developed over time, both physically and with legislation. Current aircraft accidents and disasters drive the improvement for protection of the aircraft data log and the flight data log. The last known idea introduced a concept for ground collecting and analysing flight data. The main idea of this system is that all information about the aircraft and flight would be transferred online using ground communication stations or satellite networks and then stored at the ground monitoring station for later analysis. Special software identifies a non-standard behavior of the aircraft in real time and apply a relevant corrective action if needed.[10] In Reference 11, it is proposed that the strengthening of underwater signals is required in order to find black boxes more easily. It shows that to find black boxes is a real case for flight companies and also for manufacturers. Obtaining flight recorder data is an important problem for both the manufacturer and the flight company. These data are important both in the prevention of accidents and in accessing the aircraft after the accident.

In Reference 12, cyber security and cyber terrorism on aviation is investigated. This study mentioned about to identify critical aviation information systems, to review the effectiveness of existing mitigation measures, to identify any vulnerabilities in current security arrangements, to learn good practices on how to address these vulnerabilities and determine how to better manage the identified residual risk. Air traffic management risks, cyber security problems in aviation technologies and how they are important for flights and human life are mentioned in Reference 13.

The idea of carrying aircraft black boxes data wirelessly is mentioned in Reference 14. The architecture and modeling of receiving data online, rather than locally, is explained. There are four main motivations in this article. Data recording is so important on airplanes because if the FDR gets lost, the last data will be accessible. In an emergency, if pilot did not notice the problem, pilot can be informed or alerted about the problem. This system can prevent the accidents which is caused by pilot errors. Also via this study, reason of accidents can be found and it can prevent future accidents. In Reference 15, a method has been proposed for making a backup of flight data. It is about the development of an incremental clustering method for anomaly detection with dynamically growing dataset. This method is proposed for emerging clusters and updating existing clusters. The main aim of this study is to prevent the loss of information. The authors analyze the information for flight traffic management and pre-warning systems and gives an example of anti-collision warning system design in Reference 16. This study is about to analyze the inputs and outputs of the unmanned traffic management system of the fuzzy assurance monitor. It tests the ability to determine if there is an impact on safety or efficiency and then assigns the relevant risk. A flight data analysis system is designed in Reference 17, to show real statistics of flight data. This analysis will include crew operational behaviors, flight performance and engine status. The main aim of this article is the elimination of security risks and ensurance of the aviation safety.

Also there are lots of studies about blockchain based data recorders,[6–9] data protection with blockchain,[18] blockchain for data integrity,[19] blockchain for data and network security.[20,21]

In Reference 18, sensitive and personal data privacy and security is explained. The users should own and control their data without compromising security or limiting the ability of companies and authorities to provide personalized services. Users do not need to trust any third party and are always aware of the data collected about them and how it is used. Reference 19 explains the problems such as scaling problem, security problems

arising from central architecture, problems experienced when devices talk to each other securely. This article focuses on a blockchain-based security protocol to solve these problems and protect data integrity. In Reference 20, network authentication and secure data transfer using blockchain technology is proposed. The algorithm mentioned in the article, shows that the implementation of blockchain for IoV communication and security management can be an important problem. The article[21] focuses on the availability issues of network storage service. The authors use blockchain for double-server storage model and also propose secure deduplication and share auditing using a novel deduplication protocol to protect users from losing data using duplicate faking attack or single point of failure.

When the studies on the aircraft FDR are examined, it is seen that most of the studies are on data protection, data accessibility, online viewing of the data and searching the black box. These studies have generally focused on bringing data to the real world instantly with hardware or software. Because if an aircraft's data recorder cannot be reached, an accident may not be clarified and it is unknown whether it was due to production or pilot error. For this reason, sometimes the manufacturers or flight companies may confront with difficult situations. There is a need for software or hardware that will enable the data to be viewed by both the flight company and the manufacturer without being corrupted or manipulated. Although there have been studies so far, a solution to this problem has still not been found.

It has been observed that blockchain is a useful solution in both closed and open networks for data recording and asset transfer problems. The fact that a data recorded in this technology cannot be changed afterwards, that all data from the past to the future are recorded and this recorded data is kept in a distributed architecture, the blocks are depended to a consensus while forming, both authorizations and contracts can be made with smart contracts have shown that blockchain technology can be a solution to mentioned problems.

In this study, a solution to this problem is proposed in which both the manufacturer and the flight company can monitor flight data on a closed blockchain network. They can use this data to eliminate pilot errors, manufacturing errors, to maintain flight optimization, fuel efficiency and also to research about the possible causes of accidents.

3 | BLACK BOX TECHNOLOGY IN AVIATION

In aviation industry, FDR and CVR which are known as black box by public, are the most mentioned components of aircraft especially after aircraft accidents. Actually, these data boxes are not black, they are orange, but because of bad news, they are named as black boxes. FDR is the recording device that records many parameters of flight, such as speed, acceleration, altitude, angles of flight control surfaces and so forth. A typical FDR is shown in Figure 1.

The Federal Aviation Administration (FAA) has made it mandatory for all aircraft to have a FDR and a CVR for each aircraft engaged in transportation. Since it first came out with the developing technology, it can save much more data today and it has been made much more durable physically. The parameters collected in the FDR are used not only for the investigation of the accident, but also for the improvement of the performance of the aircraft. The flight performance and fuel performance of the aircraft during the flight phases can be observed and it can be determined whether there is any malfunction in the aircraft and whether the software is working efficiently.

Due to the accidents between 1988-1997, the number of FDR parameters which should be recorded according to the production years of the aircraft were determined. The number of the parameters required to be recorded for passenger airplanes that have received type approvals according to their production years in 1997 has been determined by the FAA. Parameter numbers according to production years are shown in Table 1. Thus, regardless of the year of manufacturing, it has become mandatory to record the first 18 parameters in the rules.[10,22] With the studies carried out in the following years, the recording times of the devices and the number of parameters were increased and efforts were made to increase their durability against physical damage.

FIGURE 1 Flight data recorder.

TABLE 1 Number of FDR parameters by aircraft manufacturing years.

Manufacturing year	Number of parameters to be applied
Before 1991	At least 18–22 parameters
Between 1991 and 2010	At least 34 parameters
After 2010	At least 57 parameters
After 2012	At least 88 parameters

4 | BLOCKCHAIN TECHNOLOGY AND HYPERLEDGER

Blockchain is a cryptographically verifiable digital distributed data recording method with sequential and ascending blocks. The blocks in the blockchain that contain the data are linked to each other by cryptographic hash algorithms.[23] On the blockchain network, there are smart contracts that enable the transfer of valuable assets or data. Before data transfer, errors are reset through consensus and the transfer process is performed. The hash value of the transaction is recorded in many decentralized ledgers in a distributed structure. In other words, blockchain is a technology that uses distributed ledger technology (DLT). In blockchain technology, while the data of the transfer transaction is recorded in the ledgers, the transaction is kept secure by using cryptographic algorithms. In short, blockchain is a distributed ledger that is cryptographically secure, very difficult or impossible to change, and whose updating depends on consensus or smart contracts.[23–25]

The history of blockchain technology can be divided into pre-Bitcoin and post-Bitcoin. Bitcoin has shown the world that the blockchain technology works correctly and has introduced this technology to the world, so Bitcoin can be considered as a milestone in the historical development of blockchain. Before Bitcoin, the concept of digital signature was mentioned in the prevention of tracking payments and money transfers. The article[26] can be considered as the first step in the history of blockchain. In Reference 27, the time-stamped and cryptographic signing of a digital document is proposed which is similar to the blockchain technology because it includes the concept of timestamp and cryptographic algorithms.

Bitcoin transactions are kept in ever-growing digital ledgers. Digital ledgers are copies of each other and exist in a distributed structure. Transactions in the ledgers are kept in blocks and the blocks continue to increase. Each block contains the information of the previous block, summarized with hash algorithms, so that a chain of blocks is formed. Bitcoin uses the distributed ledger structure, cryptology, game theory as the basic components and verifies the blockchain technology.[2,24]

Another revolution and perspective of blockchain technology is the Ethereum blockchain network. The Ethereum network was announced to the world with an article in 2014 and started to work actively in 2015. Ethereum works as the world's largest virtual server.[3] It is a crypto operating system with its own programming language (solidity), which allows the development of decentralized software, applications and smart contracts in a distributed structure. The number of applications and software running on the Ethereum network is increasing day by day.

Blockchain technology, integrating cryptography, consensus mechanism, DLT, and peer-to-peer communication, is recognized as a modular and evolving technology. Recent studies in blockchain, contribute to its development by proposing new access control schemes, secure transaction systems, and encryption methods. In Reference 28, it is proposed a blockchain based access control scheme which hides attributes with a decryption method. The attribute-based access control model is deployed for access control, the authors have designed and implemented a blockchain-based secure storage system by utilizing distributed consensus to realize data security, traceability, and immutability in Reference 29. In Reference 30, a blockchain based peer to peer multiparty transaction scheme is proposed which allows multiple users to participant in one transaction simultaneously. They offer a new solution for the key exchange for encryption via the blockchain scheme, design and implement format-preserving, Feistel-based encryption, with multiple implementation variances algorithms, for enhancing automatic dependent surveillance-broadcast (ADS-B) security in Reference 31. Furthermore, in the following fields IoT and blockchain work together: in Reference 32, a blockchain based scheme for secure authentication, data sharing and nonrepudiation, in Reference 33 a time-bounded secure attribute-based online/offline signature with constant message size and blockchain-assisted hierarchical attribute-based encryption scheme for secure information[34] are proposed. While some of these studies appear as security schemes,[35] some appear as decryption methods. These advancements, while varying in application, reinforce the core attributes of blockchain technology: transparency, immutability, and decentralized architecture.

Hyperledger is an open source platform developed by the Linux Foundation (LF) that enables private (closed) blockchain networks to work. Today, many applications are running on the Hyperledger architecture. The hyperledger platform also has very similar components, such as open blockchain networks.[36]

5 | BLOCKCHAIN BASED BLACK BOX MODELING

In this section, all elements of our hyperledger blockchain network will be explained: peers, client application, ledger and block structure, transactions, channel and organization, endorsement policy and consensus algorithm, transaction management process. Project details of components, case study and security analysis are also given.

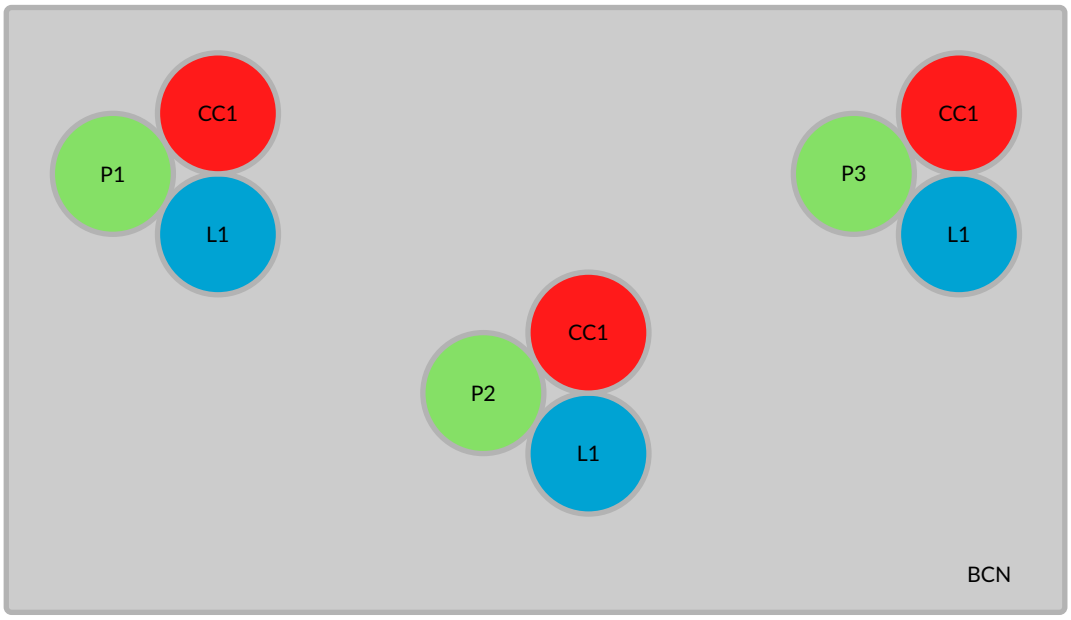

FIGURE 2 Peers on hyperledger.

5.1 | Peers

Peers are the components where the data is recorded with ledgers on them. Peers are the most fundamental and most important components in both open and closed blockchain networks. With the smart contract they have on them, they ensure that the recorded data is irreversible and ensure the process of transaction proposal and endorsement policy. Also peers have lots of services on them, as fabric gateway. Ledger, chaincode and services are accessible from peers, because of this, administrators of system and client applications should interact with peers to access these sources.[23,37] Figure 2 show peers (P), smart contract (CC1), ledger (L1) in blockchain network (BCN).

Orderer peers are responsible for packaging transactions and delivering them to the peers. A single peer can interact with a client or can query a transaction on its own. But ledger update transaction is different from other transactions because only one peer cannot do this process. For ledger update, more peers are required to approve this process. In blockchain networks, this process is called as consensus. Each peer has a different identity which is given by digital client library. Certificate authority provides digital certificates for each peer which is regardless of orderers or peers.

In this study, we assume that peers may be anywhere in the world. It can be stored on cloud services or it can be on physical servers of manufacturers or flight companies. It will depend on project's details. But it should not be forgotten that peers must be distributed and physically secured. For example a physical server of manufacturer or a virtual server of a flight company can be a peer for the network. The fact that flight companies have centers almost all over the world will help the peer structure to be distributed.

5.2 | Client application

Fabric applications are applications that have an interface where people can see and query transactions occurring in the blockchain network. These applications can be written in NodeJS, Java, Go or Python. Developing an application is easy for developers because APIs and SDKs are open source. All clients in network have these SDK and these applications should always be up to date. Client application is used to communicate with peers and to use services on them. Fabric gateway service which is on peers will supply connection between client and peers to use chaincode and also ledger. Also they are used to connect to the fabric network to use the gRPC protocol. gRPC is a high performance, open source remote method invocation which was developed by Google in the C programming language in 2015.[37,38]

In this study, an aircraft with a black box is called as a client or user. Client application will be set up on aircrafts. These applications will not be open to internet, they will work only in closed blockchain network. Each client should have the parameters and components given below:

- A client id (from client identity library).
- Client application.

- Own digital signature (from certificate authority).
- Chaincode.

5.3 | Ledger and block structure

In hyperledger fabric, a ledger has two important components to become a blockchain ledger. First one is known as "world state" which is a database that holds values. States are expressed as key-value pairs. World state is global method for ledgers and states can be modified, deleted or created. But as well known, blockchain ledger is immutable.[36,38] Blockchain ledgers consist of a combination of world state and block structure. An example about world state expression is given below:

{key = TK1033 and value = {model:airbus, owner = X_airlines}}
{key = QA1067 and value = {model:boeing, owner = Y_airlines}}
{key = QA2073 and value = {model:airbus, owner = Y_airlines}}
{key = AA3042 and value = {model:boeing, owner = Z_airlines}}

Blocks are also fundamental components of blockchain. The blocks that keep records of transactions on the network form a chain. The header of each block contains a hash of the block transactions and a hash of the header of the previous block, so the blocks are linked to each other cryptographically. Hash of the transactions in the block ensures that all transactions in the ledger are ordered.[2,37,39] The block with the number 0 at the beginning of the chain is called the starting block or the genesis block. Each block consists of three parts. In Figure 3, a block structure is shown which consists of block header, block data and block metadata parts.

Block data is formed by writing the records of the transactions in order. Block metadata contains the timestamp of the block, the signature of the block author and the public key. As seen in Figure 4, the block header consists of the block number, the hash of the current block and the hash of the previous block.

For the mentioned network, the first block of blockchain is created first of all. For every block, block size is limited with 1 MB data. The first block of blockchain is named as "genesis block." Genesis block contains channel and peer information and its own block id. For ledger infrastructure, CouchDB is used. Figure 5 shows the creation of genesis block.

5.4 | Channel and organization

Channel can be considered as a subnetwork in hyperledger blockchain network. If a peer joins a channel, it will access to channel's ledger and it has to obey channel's set of rules. A peer can join more than one channel, however it will obey all channels' rules. Thus, a peer which joins more

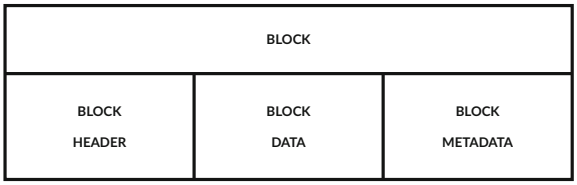

FIGURE 3 Block structure.

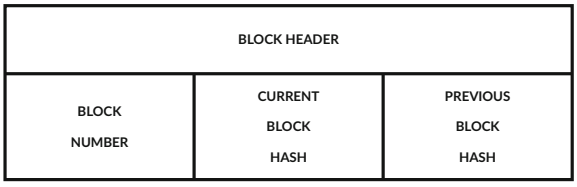

FIGURE 4 Block header structure.

```
================ Generating crypto ================
thy.com
qatar.com
================ Writing Genesis Block ================
2020-12-13 16:21:41.388 UTC [common.tools.configtxgen] main -> INFO 001 Loading configuration
2020-12-13 16:21:41.577 UTC [common.tools.configtxgen.localconfig] completeInitialization -> INFO 002 orderer type: solo
2020-12-13 16:21:41.579 UTC [common.tools.configtxgen.localconfig] Load -> INFO 003 Loaded configuration: /vagrant/network/config/configtx.yaml
2020-12-13 16:21:41.624 UTC [common.tools.configtxgen] doOutputBlock -> INFO 004 Generating genesis block
2020-12-13 16:21:41.626 UTC [common.tools.configtxgen] doOutputBlock -> INFO 005 Writing genesis block
================ Writing airlinechannel ================
2020-12-13 16:21:41.712 UTC [common.tools.configtxgen] main -> INFO 001 Loading configuration
2020-12-13 16:21:41.903 UTC [common.tools.configtxgen.localconfig] Load -> INFO 002 Loaded configuration: /vagrant/network/config/configtx.yaml
2020-12-13 16:21:41.904 UTC [common.tools.configtxgen] doOutputChannelCreateTx -> INFO 003 Generating new channel configtx
2020-12-13 16:21:41.947 UTC [common.tools.configtxgen] doOutputChannelCreateTx -> INFO 004 Writing new channel tx
================ Generate the anchor Peer updates ======
2020-12-13 16:21:42.015 UTC [common.tools.configtxgen] main -> INFO 001 Loading configuration
2020-12-13 16:21:42.199 UTC [common.tools.configtxgen.localconfig] Load -> INFO 002 Loaded configuration: /vagrant/network/config/configtx.yaml
2020-12-13 16:21:42.200 UTC [common.tools.configtxgen] doOutputAnchorPeersUpdate -> INFO 003 Generating anchor peer update
2020-12-13 16:21:42.230 UTC [common.tools.configtxgen] doOutputAnchorPeersUpdate -> INFO 004 Writing anchor peer update
2020-12-13 16:21:42.325 UTC [common.tools.configtxgen] main -> INFO 001 Loading configuration
2020-12-13 16:21:42.522 UTC [common.tools.configtxgen.localconfig] Load -> INFO 002 Loaded configuration: /vagrant/network/config/configtx.yaml
2020-12-13 16:21:42.523 UTC [common.tools.configtxgen] doOutputAnchorPeersUpdate -> INFO 003 Generating anchor peer update
2020-12-13 16:21:42.549 UTC [common.tools.configtxgen] doOutputAnchorPeersUpdate -> INFO 004 Writing anchor peer update
```

FIGURE 5 Creation of first block of blockchain (Genesis block).

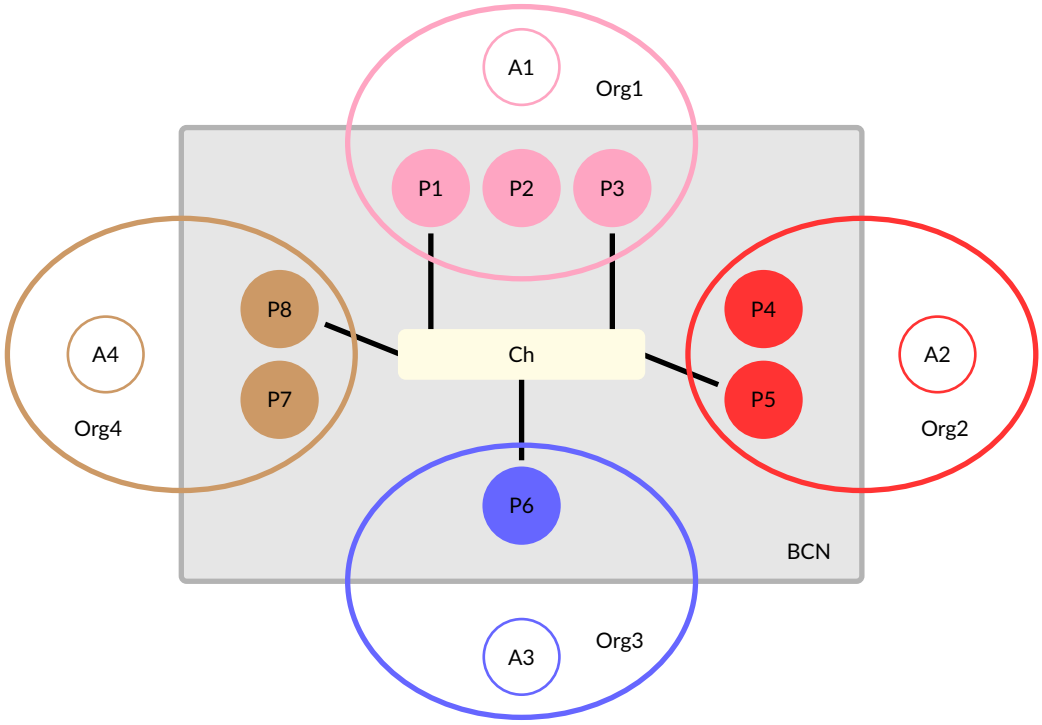

FIGURE 6 Channel and organization architecture.

than one channel will have all it's channels smart contracts and also ledgers. Channels are not physical subnetworks or structures, they are logical structures.[38] In a hyperledger blockchain network, there can be lots of organizations. Also one organization can join more than one channel. Every organization should have at least one peer and one client to be a piece of network. Figure 6 shows the hyperledger blockchain network architecture with peers (P), organizations (Org), channel (Ch), applications (A).

In this study, manufacturer companies will be both organizations and channels. For example; airbus will have organization and it will have peers and clients in the network and also one channel name will be airbus channel. An airbus aircraft (client) from X airlines will be in X organization and will join in airbus channel, so aircraft's company and manufacturer company will be able to see the data of this aircraft. Any aircraft company may be involved in more than one channel if it has aircrafts from different manufacturers. For example; X airlines has airbus and also Boeing aircrafts. This company will join both airbus and Boeing channels, but its clients will join only one channel. Airbus clients will be in airbus channel, Boeing clients will be in Boeing channel. Thus, a manufacturer cannot see another manufacturer's data.

5.5 | Transaction

Transaction is the process of transferring data from one peer to another peer in the blockchain network. All transactions from the beginning of the chain to the present are recorded in the blockchain, and these records are recorded at the distributed peers. All transactions in the blockchain network are confirmed after passing through the consensus protocol.[37,38] A transaction consists of five parts which are given below:

- Header.
- Signature.
- Proposal.
- Response.
- Endorsement.

In this study, transactions are taken as aircraft flight data. 1 MB transaction data will be written on a block. A transaction will be sent from client application and then it will be written to the ledgers on peers. This process will be called as "Transaction Management Process."

5.6 | Transaction management process

There are three main phases of management of a transaction. In this process, peers and orderer peers have the main roles on transaction proposal, endorsement, submission, ordering, validation, and commitment. Transaction management algorithm is shown in Algorithm 1. This algorithm highlights the critical steps in ensuring data integrity and consistency in a distributed ledger environment.

Phase 1—Transaction proposal and endorsement: Aircraft sends a transaction proposal message to endorsing peers to be confirmed. This message contains client's id, chaincode id, client's digital signature and transaction content. Transaction content is flight data which is written to black box.

Endorsing peers have their own digital signatures, endorsement policy and endorser ids. They add another information to proposal message such as endorser id and own digital signature and also simulate the transaction, using read/write data sets. The read dataset contains the necessary data to run the smart contract. The write dataset contains the data that is changed after the smart contract is run. Also they validate the client's digital signature. Then endorsing peers send the verified and signed message to the client. This process is shown in Figure 7.

Phase 2—Transaction submission and ordering: First, aircraft sends the message to fabric gateway service and gateway sends the message to orderer peer. Orderer peers verify the signatures and request broadcast transaction. Orderer peers add transaction to the next block and send to peers for validation and commitment.

Phase 3—Transaction validation and commitment: Each peer checks the signatures of both client and endorsing peers. Also peers check endorsement policy conditions and read/write data sets. If everything is right, peers mark each transaction as valid and then they send to ledgers

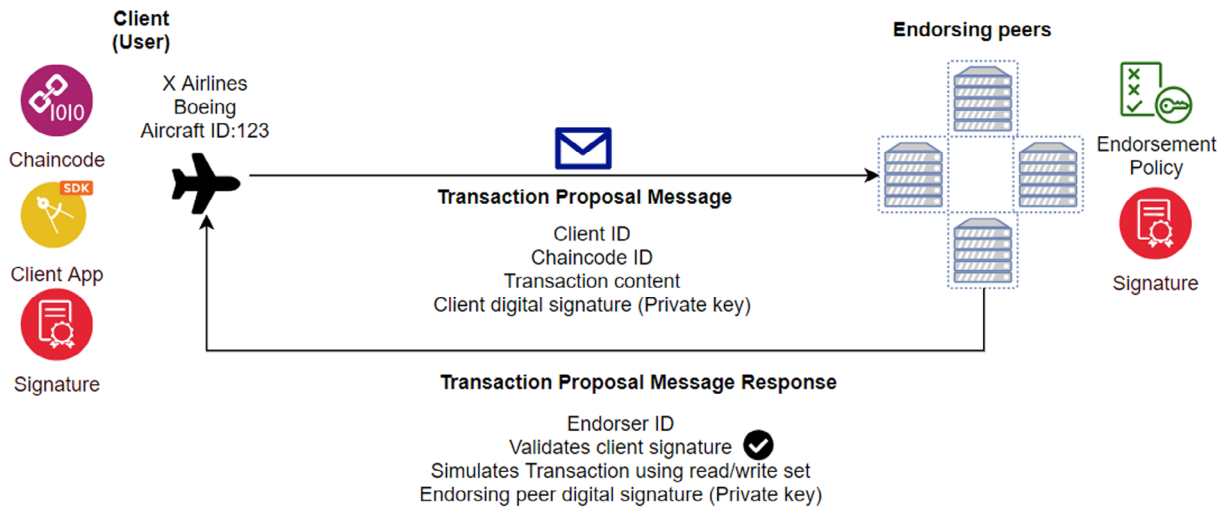

FIGURE 7 Transaction proposal process.

Algorithm 1. Transaction management process

Require: Aircraft's flight data, client's ID, chaincode ID
Ensure: Secure and consistent recording of flight data in the ledger
Phase 1: Transaction Proposal and Endorsement
function TRANSACTIONPROPOSAL(flightData, clientID, chaincodeID)
proposalMessage ← createProposal(flightData, clientID, chaincodeID)
for all *endorsingPeer* in *endorsingPeers* **do**
endorsement ← endorsingPeer.endorse(*proposalMessage*)
verifiedMessage ← addEndorserInfo(*endorsement*, endorsingPeer)
send *verifiedMessage* to client
end for
end function
Phase 2: Transaction Submission and Ordering
function SUBMITTRANSACTION(*verifiedMessages*)
aircraft sends *verifiedMessages* to Fabric gateway
Fabric gateway forwards to *ordererPeer*
for all *ordererPeer* in *ordererPeers* **do**
ordererPeer.verifySignatures(*verifiedMessages*)
ordererPeer.addToBlock(*verifiedMessages*)
ordererPeer.broadcastBlockToPeers()
end for
end function
Phase 3: Transaction Validation and Commitment
function VALIDATEANDCOMMIT(*receivedBlock*)
for all *transaction* in *receivedBlock* **do**
valid ← validateSignatures(*transaction*)
if *valid* and checkEndorsementPolicy(*transaction*) **then**
mark *transaction* as valid
commit *transaction* to ledger
else
discard *transaction*
end if
end for
end function

for commitment which is an immutable process. After that the ledger is updated with valid transactions only. Invalid transactions are not included in the ledger. Phase 2 and 3 are shown at Figure 8.

5.7 | Endorsement policy and consensus algorithm

In the hyperledger fabric architecture, the consensus algorithm and trust authority are in the chaincode as "Endorsement Policy." In other words, endorsing peers are used as trust authorities. Endorsing peers use the endorsement policy embedded within the chaincode to confirm the transaction. An endorsement policy asks the transaction the following questions when confirming the transaction:

- Are all signatures and approvals received valid?
- Does it meet the terms of the "Endorsement Policy"?
- Does it come from the right source?

It is assumed that the endorsement policy uses a consensus function to determine the consensus of trust authorities to issue approval. As the consensus, PBFT is used.[40,41] The consensus function is given below:

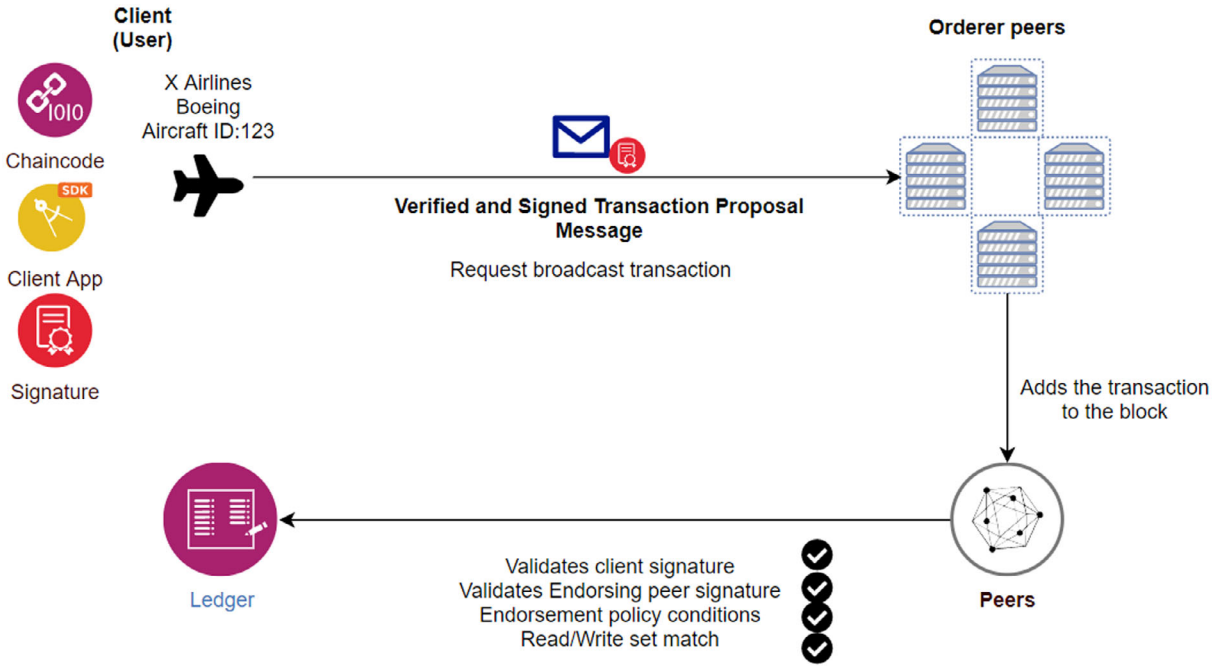

FIGURE 8 Transaction validation and commitment.

EXPR('thyMSP.Role', 'qatarMSP.Role', [EXPR(…)])

EXPR: The logic expressions (out of, or, and) of the consensus function
OrgMSP: Organization ID
Role: Roles in this network structure (members, clients, peers, admins, users etc.).

5.8 | Case study for application and network

For this network and application, a demo network has been built. For this demo network, there are tools, databases and software are used and listed below:

- Visual Studio.
- Docker.
- Docker Composer.
- Govendor.
- Hyperledger Explorer.
- NodeJS-NPM.
- GoLang.
- CouchDB.
- Fauxton/Futon.

After creation of genesis block, one channel which is named as "Airline channel" has been set up on demo network. Airline channel contains two peers on itself. For this channel, two peers (names: thy and qatar) and one orderer and endorser peer have been set up. Creation of peers, orderer peers, databases have been shown in Figure 9. Also two peers are joined to airline channel and the channel is updated.

After channel and peers are created, to see everything on a web interface, Hyperledger Explorer has been set up on network. Hyperledger Explorer is a tool that makes codes more visible on a web interface. It shows blocks, transactions, peers, chaincode and write-read sets on network. Web interface of the proposed study is shown in Figure 10.

```
================ Launch the network ================
Creating network "acloudfan_airline" with the default driver
Creating postgresql      ... done
Creating orderer.thy.com ... done
Creating explorer            ... done
Creating thy-peer1.thy.com   ... done
Creating qatar-peer1.qatar.com ... done
Peer Launch Mode=net
Done. Started the dev environment in Mode=net.
========= Submitting txn for channel creation as thyAdmin ============
2020-12-13 16:22:01.461 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-12-13 16:22:01.850 UTC [cli.common] readBlock -> INFO 002 Received block: 0
========= Joining the thy-peer1 to Airline channel ============
2020-12-13 16:22:07.098 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-12-13 16:22:07.245 UTC [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
2020-12-13 16:22:12.448 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-12-13 16:22:12.584 UTC [channelCmd] update -> INFO 002 Successfully submitted channel update
========= Joining the qatar-peer1 to Airline channel ============
2020-12-13 16:22:12.745 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-12-13 16:22:12.903 UTC [channelCmd] executeJoin -> INFO 002 Successfully submitted proposal to join channel
2020-12-13 16:22:18.107 UTC [channelCmd] InitCmdFactory -> INFO 001 Endorser and orderer connections initialized
2020-12-13 16:22:18.220 UTC [channelCmd] update -> INFO 002 Successfully submitted channel update
```

FIGURE 9 Creation of peers.

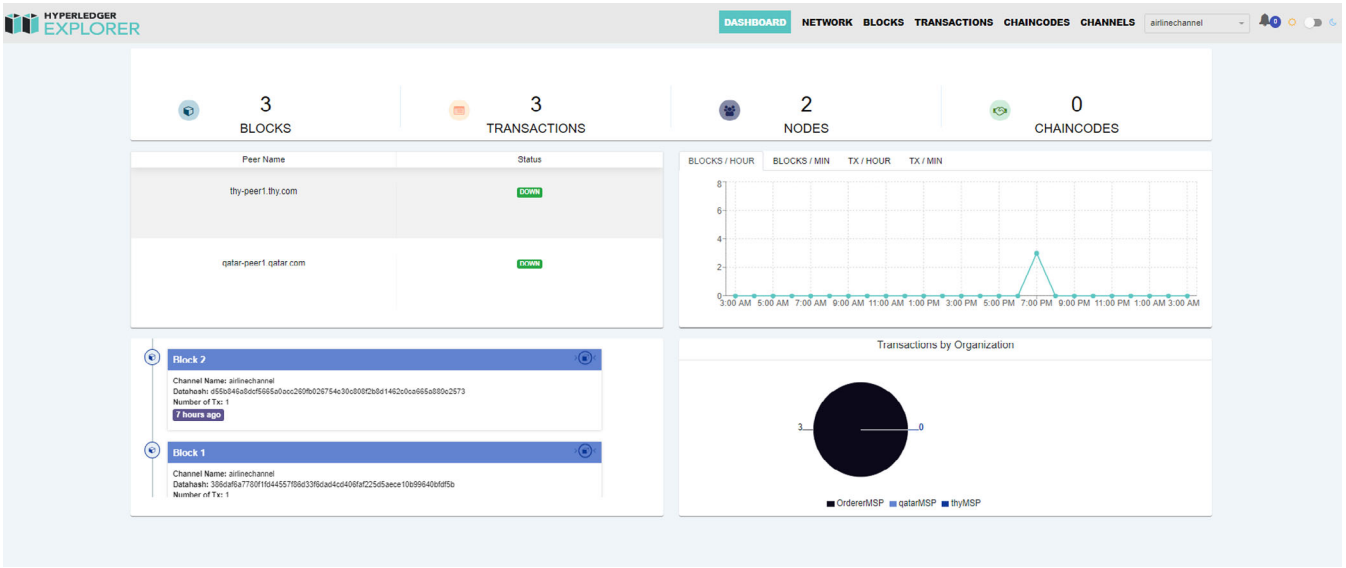

FIGURE 10 Web interface of Hyperledger Explorer.

5.9 | Security analysis

There can be always internet and network attacks to systems which are connected to any network. There are also special attacks for blockchain networks. Also there are scalability problems and fault tolerance.

5.9.1 | Network and internet attacks

If any system or device is connected to any network or internet, it will be open for cyber attacks. For service interruption attacks, DoS and DDoS attacks are the most popular attacks that use botnets. Botnet is a linked network that includes infected computers, phones or IoT devices. These attacks can be in three types: volumetric, protocol, and application layer attacks. In this study, as the network infrastructure, systems and servers of manufacturer and flight companies has been used. Because of that for DDoS and DoS, and also for other networks attacks (brute force, man in the middle attack, malwares etc.), the security policies and security products of the companies will be active.

5.9.2 | Blockchain attacks

Well known attacks on blockchain are sybil attack, pool attack and majority attack. Sybil attack is an attempt for manipulating peer to peer network using multiple fake identities. In blockchain network, if sybil nodes surround a node, they can prevent the node from connecting to honest nodes. Thus, the node cannot get or send any information to others. The pool attack is an attack that hackers want to manipulate the mining pool. And the majority attack that is also known as 51% attack is popular on blockchain networks. If attacker gains more than 50% of mining computer hash power, he will obtain access to all system and manipulate ledgers and blocks. This is the most dangerous attack type. These attack types are generally about open blockchain networks. In this study, closed blockchain network (hyperledger) has been used and almost all well known attacks will be useless for our network. Closed blockchain networks are closed to internet and protected by companies security products, so all peers will be protected by security policies of companies.

5.9.3 | Scalability and fault tolerance

Measurement of scalability in Hyperledger Fabric depends on in terms of the number of channels, organizations and peers per organization. Also endorsement policy conditions will have decisive effect on scalability. In this project, there can be lots of flight companies to become a member of network. With the increase in the number of organizations, peers and channels, there will be a latency in the process of distributing the blocks to all peers. In this study, 1 channel, 2 clients, 2 organizations, and 2 peers are used and because of this, there is no latency observed. Fault tolerance is another issue for security. Hyperledger fabric is capable about fault tolerance. If any node fails, others are capable about collecting endorsement from other available nodes. In this project, there will be lots of organization and node failure will not affect the performance of system and there will not any lost data. In this study, fault tolerance is fifty percent of peers, because of that if one peer is alive, our demo network is alive. In big scalability, this tolerance should be higher load.

6 | LIMITATIONS AND FUTURE WORKS

For practical application in aircraft black boxes, it is imperative to obtain consent and support from flight companies and manufacturers. Aircraft manufacturers need to be persuaded to share this data, which only they can read. Furthermore, there is a need for regulatory amendments to accommodate blockchain-based data collection and ledger recording in distributed architecture. Authorization of this collected data, new peer or orderer creation processes, and smart contract changes should be tied to specific procedures. Legally, the accuracy of blockchain-based collected data must be approved by the relevant authorities.

Looking ahead, the consensus mechanisms and cryptographic algorithms used in this study might evolve, drawing from recent research.[28–34] The usage of identity-based encryption[42] and blockchain-based methods together is planned. In addition, it is also considered to be used in blockchain-based applications with ECDSA,[43] which is a digital signature method that has become popular recently. At the same time, research is being conducted for blockchain-based applications in connected vehicles[44] and IoT.[45] Also different infrastructures can be used for the project. The implications of this study can be implemented not only to FDRs but also to trains' black boxes, other vehicular recorders, and even in broader vehicular network environments. Its application can be also expanded to unmanned aerial vehicles and military aircraft, showcasing the versatility and potential of blockchain technology in various domains.

7 | COMMENTS AND RESULTS

This study proposes a blockchain-based framework for keeping aircraft data traceable, immutable, transparent in a secure network. In this framework, pBFT was used as the consensus protocol, aircraft data and transaction management cycles were created. Data cannot be changed or manipulated because all data is written to distributed ledgers after validation by endorsing peers and verification by peers. By creating a sample smart contract and endorsement policy, a demo network was established and visualized via Hyperledger Explorer. It has been shown that an aircraft's black box data can be saved safely and securely using blockchain technology. This work can be a useful initiative for keeping aircraft black box data on the blockchain network. Data which is stored in blockchain network can be used for optimization besides accident investigation. Flight companies and manufacturers can use these data:

- to reduce fuel consumption,
- to observe aircraft's or pilot's performance,

- to notice effects of weather conditions on aircraft,
- to analyze all flight data,
- to compare different manufacturer's aircrafts performance,
- to optimize auto-pilot configuration,
- to evaluate the weather conditions of the routes,
- to optimize the components of aircrafts,
- to analyze the differences of several models,
- to review aircrafts malfunctions,
- to investigate accident reports.

CONFLICT OF INTEREST STATEMENT

All authors declare that the authors have no competing interests, or other interests that might be perceived to influence the results and/or discussion reported in this article.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Cagatay Korkuc https://orcid.org/0000-0003-0007-2154
Nilay Aytas Korkmaz https://orcid.org/0000-0002-8305-1641
Yasin Genc https://orcid.org/0000-0003-2271-9668
Ahmet Akkoc https://orcid.org/0000-0002-8121-7599
Erkan Afacan https://orcid.org/0000-0003-4025-6847
Erdem Yazgan https://orcid.org/0000-0003-4957-1173

REFERENCES

1. Maull R, Godsiff P, Mulligan C, Brown A, Kewell B. Distributed ledger technology: applications and implications. *Strateg Chang*. 2017;26(5, SI):481-489. doi:10.1002/jsc.2148
2. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *White Paper*; 2008:1-9.
3. Buterin V. A next-generation smart contract and decentralized application platform. White Paper; 2014: 1–36.
4. Foroglou G, Tsilidou AL. Further applications of the blockchain. 12th Student Conference on Managerial Science and Technology, Vol 9; 2015.
5. Abou Jaoude J, Saade RG. Blockchain applications—usage in different domains. *IEEE Access*. 2019;7:45360-45381. doi:10.1109/ACCESS.2019.2902501
6. Guo H, Meamari E, Shen CC. Blockchain-inspired event recording system for autonomous vehicles. In: Kai L, ed. *Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking (HOTICN 2018)*. IEEE; 2018:218-222.
7. Ruesch S, Bleeke K, Messadi I, et al. ZUGCHAIN: blockchain-based juridical data recording in railway systems. *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2022)*. IEEE; 2022:67-78.
8. Vieira AR, Farias CM, Melo WS, Madruga EL. BEDR: blockchain event data recorder. *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE; 2022:2716-2721.
9. D'Angelo G, Ferretti S, Marzolla M. A blockchain-based flight data recorder for cloud accountability. *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*. ACM; 2018:93-98.
10. Dub M, Pařízek J. Evolution of flight data recorders. *Adv Mil Technol*. 2018;13(1):95-106.
11. Liu WY, Jih R, Chen CF. Underwater positioning study of flight recorder. *IEEE Underwater Technology (UT)*. IEEE; 2019:1-5.
12. Abeyratne R. Cyber terrorism and aviation-national and international responses. *J Transp Secur*. 2011;4(4):337-349. doi:10.1007/s12198-011-0074-3
13. Lykou G, Iakovakis G, Gritzalis D. Aviation cybersecurity and cyber-resilience: assessing risk in air traffic management. *Critical Infrastructure Security and Resilience*. Springer; 2019:245-260.
14. Ashish A, Chougule SB. Wireless flight data recorder (FDR) for airplanes. In: Zhang C, ed. *Materials Science and Information Technology, PTS 1-8*. Advanced Materials Research. Vol 433-440. Singapore Inst Elect.; 2012:6663-6668.
15. Zhao W, Li L, Alam S, Wang Y. An incremental clustering method for anomaly detection in flight data. *Transp Res Part C Emerg Technol*. 2021;132:103406. doi:10.1016/j.trc.2021.103406
16. Hamilton D, Watkins L, Zanlongo S, et al. Assuring autonomous UAS traffic management systems using explainable, fuzzy logic, black box monitoring. *2021 10th International Conference on Information and Automation for Sustainability (ICIAfS)*. IEEE; 2021:470-476.
17. Zhang C, Chen S, Li Q, Bin Z. Design and application of civil aircraft flight recorder information analysis system. *2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*. IEEE; 2021:361-366.
18. Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops (SPW)*. IEEE; 2015:180-184.
19. Hang L, Kim DH. Design and implementation of an integrated IoT blockchain platform for sensing data integrity. *Sensors*. 2019;19(10):2228. doi:10.3390/s19102228

20. Arora A, Yadav SK. Block chain based security mechanism for internet of vehicles (IoV). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT); 2018:26-27.
21. Tian G, Hu Y, Wei J, et al. Blockchain-based secure deduplication and shared auditing in decentralized storage. *IEEE Trans Dependable Secure Comput*. 2022;19(6):3941-3954. doi:10.1109/TDSC.2021.3114160
22. Grossi DR. Aviation recorder overview. International Symposium on Transportation Recorders; 1999.
23. dDC L, Stalick AQ, Jillepalli AA, Haney MA, Sheldon FT. Blockchain: properties and misconceptions. *Asia Pacific J Innov Entrep*. 2017;11(3):286-300. doi:10.1108/APJIE-12-2017-034
24. Antonopoulos AM. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Inc.; 2014.
25. Bashir I. *Mastering Blockchain*. Packt Publishing Ltd; 2017.
26. Chaum D. *Blind Signatures for Untraceable Payments*. Springer; 1983:199-203.
27. Haber S, Stornetta W. How to TIME-stamp a digital document. *Conference on the Theory and Application of Cryptography*. Lecture Notes in Computer Science. Vol 537. Springer; 1991:437-455.
28. Wu N, Xu L, Zhu L. A blockchain based access control scheme with hidden policy and attribute. *Future Gener Comput Syst*. 2023;141:186-196.
29. Li D, Han D, Crespi N, Minerva R, Li KC. A blockchain-based secure storage and access control scheme for supply chain finance. *J Supercomput*. 2023;79(1):109-138.
30. Hong H, Sun Z. A secure peer to peer multiparty transaction scheme based on blockchain. *Peer Peer Netw Appl*. 2021;14:1106-1117.
31. Habibi Markani J, Amrhar A, Gagné JM, Landry RJ. Security establishment in ADS-B by format-preserving encryption and blockchain schemes. *Appl Sci*. 2023;13(5):3105.
32. Khan AU, Javaid N, Khan MA, Ullah I. A blockchain scheme for authentication, data sharing and nonrepudiation to secure internet of wireless sensor things. *Clust Comput*. 2023;26(2):945-960.
33. Hong H, Sun Z. TS-ABOS-CMS: time-bounded secure attribute-based online/offline signature with constant message size for IoT systems. *J Syst Archit*. 2022;123:102388.
34. Sasikumar A, Ravi L, Devarajan M, et al. Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial Internet of Things. *IEEE Access*. 2024;12:12586-12601.
35. Korkuc C, Dogantuna T, Afacan E, Bostanci E. Blockchain based network access control (NAC) management solution and architecture. *2021 29th Signal Processing and Communications Applications Conference (SIU)*. IEEE; 2021:1-4.
36. Cachin C. Architecture of the hyperledger blockchain fabric. Workshop on Distributed Cryptocurrencies and Consensus Ledgers; 2016:1-4.
37. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. *Proceedings of the Thirteenth EuroSys Conference*. ACM; 2018:1-15.
38. Baset SA, Desrosiers L, Gaur N, et al. *Blockchain Development with Hyperledger: Build Decentralized Applications with Hyperledger Fabric and Composer*. Packt Publishing Ltd; 2019.
39. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. *IEEE Trans Knowl Data Eng*. 2018;30(7):1366-1385. doi:10.1109/TKDE.2017.2781227
40. Castro M, Liskov B. Practical byzantine fault tolerance. *USENIX Association Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI '99)*. USENIX Association; 1999:173-186.
41. Sukhwani H, Martinez JM, Chang X, Trivedi KS, Rindos A. Performance modeling of pBFT consensus process for permissioned blockchain network (hyperledger fabric). *2017 IEEE 36TH International Symposium on Reliable Distributed Systems(SRDS)*. IEEE; 2017:253-255.
42. Genc Y, Korkuc C, Aytas N, Afacan E, Sazli M, Yazgan E. A novel identity-based privacy-preserving anonymous authentication scheme for vehicle-to-vehicle communication. *Elektron Elektrotech*. 2023;29(2):69-77.
43. Genç Y, Afacan E. Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. IEEE; 2021:1-6.
44. Genc Y, Aytas N, Akkoc A, Afacan E, Yazgan E. ELCPAS: a new efficient lightweight certificateless conditional privacy preserving authentication scheme for IoV. *Veh Commun*. 2023;39:100549.
45. Genç Y, Afacan E. Identity-based encryption in the Internet of Things. *2021 29th Signal Processing and Communications Applications Conference (SIU)*. IEEE; 2021:1-4.

How to cite this article: Korkuc C, Aytas Korkmaz N, Genc Y, Akkoc A, Afacan E, Yazgan E. BLOCKBOX: Blockchain based black box designing and modeling. *Concurrency Computat Pract Exper*. 2024;36(13):e8057. doi: 10.1002/cpe.8057