Hindawi
Security and Communication Networks
Volume 2022, Article ID 8542876, 11 pages
https://doi.org/10.1155/2022/8542876

Research Article

ATMChain: Blockchain-Based Security Framework for Cyber-Physics System in Air Traffic Management

Xin Lu and Zhijun Wu

School of Safety Science and Engineering, Civil Aviation University of China, Tianjin, China

Correspondence should be addressed to Zhijun Wu; zjwu@cauc.edu.cn

Received 16 November 2021; Revised 24 December 2021; Accepted 14 February 2022; Published 10 March 2022

Academic Editor: Yuling Chen

The air traffic management (ATM) system is an intelligent system that integrates the ground computer network, the airborne network, and the space satellite (communication and navigation) network. It has remarkable characteristics of cyber-physical system (CPS). The development of ATM system is inseparable from the application of new technologies. This paper proposes a security framework based on blockchain for CPS in the ATM system. Through the research on the characteristics of blockchain and CPS, this paper analyzes the necessity of integrating them into the research of the ATM system, demonstrates the feasibility of combining them, and then constructs the ATMChain framework mechanism to realize the in-depth integration of blockchain and CPS in ATM. On this basis, this paper gives the overall design architecture and implementation steps of the scheme. In addition, this paper also makes a series of analysis and demonstration from the perspective of scheme security. The research scheme will help to improve the security, reliability, and scalability of ATM services and provide a new reference for establishing a more security and efficient ATM system.

1. Introduction

As a large-scale key infrastructure for the safe operation of civil aviation, the air traffic management (ATM) system includes a large number of heterogeneous functional subsystems, which constitutes a typical complex system [1]. With the continuous improvement of the informatization and networking degree of the ATM system, the interaction between its components is closer, the data in the system need to be highly shared, and the functions of each subsystem need to support each other, which has the typical characteristics of the cyber-physical system (CPS) [2]. The CPS is a comprehensive system that involves computer algorithms and cyber and physical objects. The CPS monitors and perceives the objects of the physical world and controls the behavior of physical entities by mining and analyzing the rich data contained in the physical world, so as to realize the efficient operation of the physical world [3, 4]. As a typical CPS complex system, the interwound systems of systems have brought great security pressure to ATM systems all over the world because of its complexity [5]. In order to deal with and solve the security risks in the ATM system, experts and scholars in academic and aviation circles began to introduce mature and widely applied new technologies, such as microservice, cloud computing, edge computing, big data, Internet of things, artificial intelligence, and blockchain, into ATM field, providing reference and ideas for the further development of civil aviation informatization [6, 7]. It will promote the construction and development of the ATM system.

At this stage, the concept of CPS has become one of the core guiding ideology adopted by Federal Aviation Administration (FAA) in deploying NextGen, the third generation ATM system [8, 9]. It boldly changes the traditional mode of ATM system deployment and more deeply implements the concept of safe and green system construction integrating human, machine, environment, and management. Secondly, for the typical CPS system, some relevant scholars have carried out research from the perspective of blockchain distributed architecture to eliminate some

potential security risks in the CPS system [10–14]. Finally, relevant researchers consider using blockchain technology to solve the related security problems faced in the ATM system [15–17]. However, there is no research on the integration of CPS and blockchain in the ATM system. Therefore, combined with relevant research, taking the ATM system as the research background and from the perspective of CPS, this paper integrates the distributed architecture idea and principle of blockchain into the security framework research of the ATM system, so as to solve the bottleneck problems existing in the current theoretical research, promote technological innovation, and promote the application of basic research. Furthermore, it can also contribute to promoting the development and construction goal of "smart ATM" of International Civil Aviation Organization (ICAO).

As a highly informative industry, civil aviation has always attached great importance to information security and information value transmission [18]. Coincidentally, blockchain technology has greater value in both of these areas. The characteristics of the blockchain provide possibilities for its application in the field of ATM. This paper is committed to building a CPS security architecture based on blockchain for the ATM system. The structure of the paper is as follows. The second part describes the research status of the ATM system, blockchain, and CPS. The third part gives the CPS security architecture in ATM based on blockchain and describes the scheme in detail from three aspects: the scheme background, scheme framework, and the information sharing algorithm. The fourth part analyzes the security of the scheme framework proposed in the previous part. The fifth part provides the conclusion and prospect and discusses the next research direction and focus.

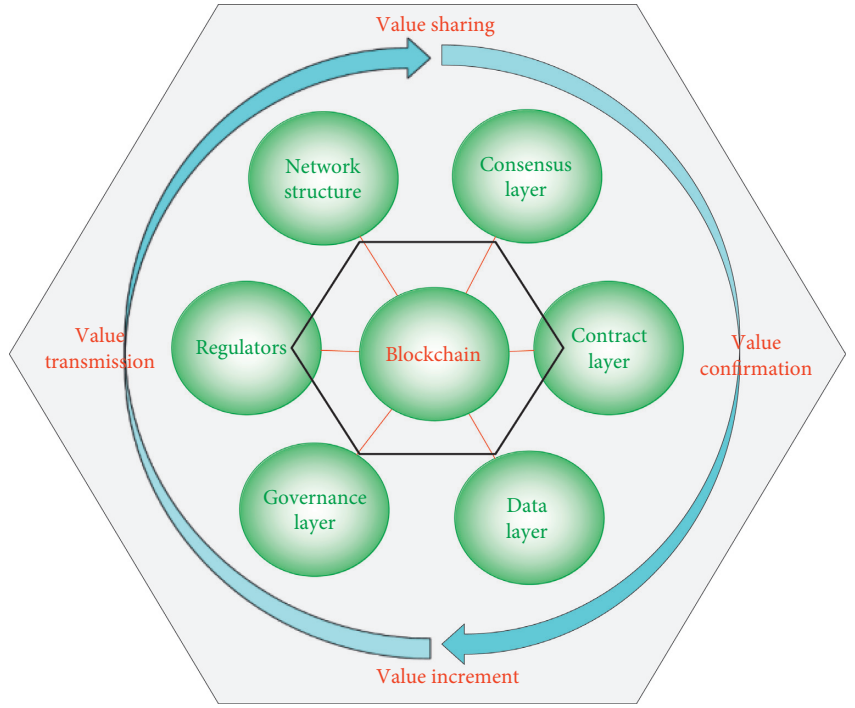
2. Background

This part starts from two aspects. On the one hand, it introduces the essence of blockchain and CPS. On the other hand, as for the special research background of the ATM system, it points out the feasibility of using blockchain technology from the perspective of CPS in ATM.

2.1. Blockchain and Cyber-Physical System. Blockchain technology, which appeared in 2008, is a decentralized, tamper proof, forgeable, and collectively maintained distributed database management method [19]. It is a new computer technology application mode integrating distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm (Figure 1(a)). In this paper, the blockchain technology is regarded as the integration and addition of multiple technologies, a security concept of information system, rather than a specific technology. From the perspective of data recording, blockchain is a chain data structure formed by connecting and combining data blocks in sequence according to time, which ensures its tamper ability and unforgeability as a distributed ledger in a cryptographic way [20]. Bookkeeping is accompanied by the development history of human society. The evolution process of bookkeeping form is from single ledger to double ledger and then to digital ledger. At present, it has developed to distributed ledger. Blockchain technology is a representative technology of distributed ledger. The core of blockchain technology is the deposit-certificate and value-certificate, as well as the consensus mechanism formed on this basis, that is, the algorithm to reach a consensus on the sequence of things over a period of time. Furthermore, in the whole blockchain system, various application services based on information flow are realized in the form of smart contract, which endows "information" with value and reconstructs the current centralized social organization production relationship. When the data that can reflect the facts are fixed, value is generated from it. Data are the means of production in the era of digital economy, and the algorithm is a productivity tool for data processing. The blockchain adds a dimension of trust to the existing data, improves the flow efficiency, and completes the reconstruction of decentralized production relations.

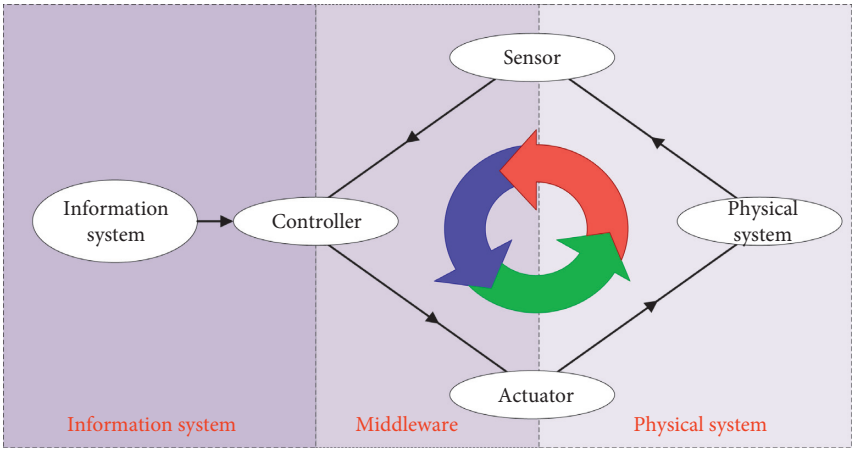
By combing the relevant theoretical viewpoints, it is not difficult to find that CPS uses perception, communication, network, and other technical means to realize the perception and digital presentation of the physical world, so as to form the data projection in the information world (as shown in Figure 1(b)). Then, the advanced computer algorithm is used to optimize the operation process of the physical world, and a closed loop of mutual influence and interaction between the actual entity world and the cyber world is formed. Its key core features are integration, diversity, and intelligence. The CPS is a complex system with close integration of the physical system and information system. It can be divided into information system, physical system, and middleware, which advances the close interaction between actual system and information system. Different from the traditional independent physical system and information system, the CPS emphasizes the strong interaction between them. The development trend of close integration has led to a leap of quality in the development of physical systems. By means of the computing and storage capacity of information systems for large-scale information, the level of intelligence, automation, and systematization of physical systems has been further improved. The middleware is the key component to promote the integration of CPS, including controller, sensor, and actuator. The controller is a component for data preprocessing and instruction forwarding. It plays a control function and closely couples the information system with the middleware. Sensor is an important input unit for collecting physical system state data, which provides important data support for CPS [21–23]. The actuator is the driving unit that acts on the physical system. The sensor and actuator closely couple the physical system with the middleware.

2.2. Air Traffic Management. The ATM system is a large CPS system integrating space-based network, air-based network, and land-based network (as shown in Figure 2). Its information system is composed of ground control station and data fusion center, which can generate intelligent decision results through the comprehensive analysis of aviation data and meteorological data. The intermediate components



Basic composition of blockchain

(a)



Basic composition of CPS

(b)

Figure 1: (a) Basic composition of blockchain. (b) Basic composition of CPS.

include a sensor network composed of ADS-B (Automatic Dependent Surveillance-Broadcast) sensors, radars, satellites, and so on and an actuator network composed of aircraft and so on. Its physical systems include aircraft and airports. The various parts of the whole ATM system are deeply integrated with the continuous improvement of its automation level. Accordingly, the ATM system also contains some subsystems that can be regarded as CPS. For example, the aircraft is a small CPS system. Its information system is composed of decision-making units of the airborne avionics system. The intermediate part includes airborne sensor unit and actuator unit, including sensors such as aircraft state information acquisition and environmental parameter acquisition and actuators that drive changes in flight course and speed. Its physical system includes aircraft engine and fuselage. The subsystems of the whole aircraft are highly coordinated, which enhances the intelligence of flight with the support of information. In short, the ATM system is a complex system with the characteristics of wide spatial distribution, complex functions, time delay sensitivity, and high security requirements. It is a large CPS as a whole, including some small CPSs. Therefore, the ATM system is the CPS of CPSs, which has the characteristics of extremely obvious information physical system.

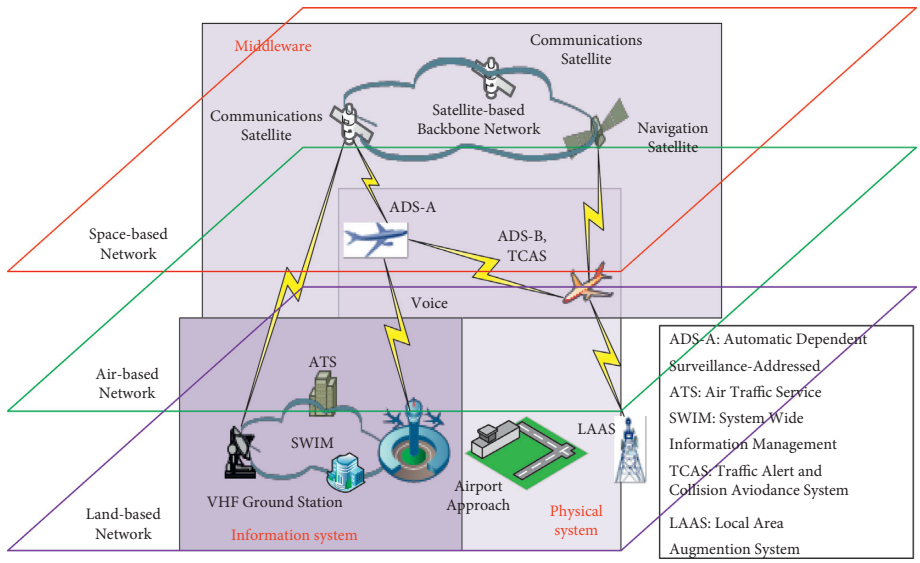


Figure 2: Basic composition of the ATM system.

The ATM plays an important role in the sustainable development of aviation safety because it is directly related to the efficiency and safety of air transportation [24–28]. However, when building ATM networks, software engineering designers generally do not pay enough attention to information security. For instance, in the case of the public unencrypted broadcast protocol ADS-B, any external party can eavesdrop, tamper, and delete ADS-B information with relative ease [16, 29]. At the same time, the widely distributed composition and the multisource heterogeneous data of the ATM system have a natural unity with the decentralized and distributed bookkeeping characteristics of blockchain. For the ATM, how to design a reliable and secure information delivery and sharing approach by using blockchain technology and combining the CPS features of ATM is the main problem addressed in this paper. Next, the feasibility is discussed from three aspects:

(1) In the development of the ATM system, the biggest problem faced by the cooperation between ATM departments all over the world, even in different regions of a single country, is security and privacy protection. At present, the main threats faced by the ATM system are data leakage, data deception, entity camouflage, and denial of service (DoS). These security threats are distributed in the information system, middleware, and physical system of the ATM system. At present, many research studies are to solve the challenges from the traditional security strategies and methods. The emergence of blockchain technology provides a useful tool to solve the trust problem of human society, and it has become one of the primary application technologies to solve the issues of security and privacy protection.

(2) According to the different object-oriented of blockchain, it includes three kinds: public chain, private chain, and federated chain. Public blockchain is open to all, and nodes can join at will. Private blockchain is only open to individual entities, such as the interior of a company or organization. Alliance blockchain will be open to a specific industry organization. Alliance blockchain refers to a blockchain in which several institutions participate in bookkeeping; that is, industry alliance members reach a consensus through trust in multicenters. This feature is just suitable for the distributed and multicenter network of the ATM system. In addition, compared with the public blockchain, the very important feature of the alliance blockchain is the node access control and national security standard support. This ensures that authenticated access and regulatory rules are developed in compliance with regulatory requirements and increases the speed of transactions based on trusted security. The security framework of this paper is designed based on alliance blockchain.

(3) From the current research results of system design, the architecture of the distributed system can better meet the requirements of users for system robustness and controllability than the central architecture. Therefore, the obvious research trend is to establish a strong and secure ATM framework from the viewpoint of multilevel overall system layout design, combined with the concept of CPS. As a representative decentralized information storage solution, blockchain coincides with such a research trend, and it is also necessary to apply it to ATM.

3. The Design of Security Framework

Starting from the business characteristics of the ATM system, combined with the concept of blockchain and CPS, this paper proposes an ATM-CPS security architecture based on alliance blockchain, abbreviated as ATMChain. The following describes the ATMChain security framework from three aspects: scheme background, scheme framework, and the information sharing algorithm.

3.1. The Background of ATMChain. With the rise of intelligent transportation technology all over the world, civil aviation is developing in the direction of information sharing, structure, and function dependence through 3C (computing, communication, and control) technology. Among them, the ATM system has the characteristics of typical CPS. Using CPS modelling theory to model the ATM system can fully analyse the interactions between its cyber system and physical system. It can also make up for the one sidedness of the existing research after separating the information system and the actual system and enhance the pertinence of system analysis. At the same time, the decentralized framework adopted by the blockchain provides a novel view for ATM infrastructure layout optimization. The basic level of the ATM system takes the sensing device as the physical carrier to store its function information and environment sensing information. The ground control station is responsible for processing the information delivered by ATM equipment at each basic level. Here, these information processing centers will serve as the nodes of the alliance blockchain, promote the interconnection of ATM information in the whole region, and provide value data services to ATM users on this basis. This distributed architecture can effectively prevent the dysfunction of local ATM nodes, so that the global ATM system can run efficiently and securely. In addition, blockchain technology's chain construction method and decentralized storage provide a novel way to implement information governance traceability. Therefore, in order to better achieve the goal of "smart ATM," two challenges still need to be met.

(1) CPS digitally presents and intelligently manages the real ATM system. A lot of reliable information in the physical world will be stored in the information system. Once the system is attacked, it will not only cause information leakage but also cause a large number of actual parties to be utilized by attackers, resulting in great damage to enterprises and society. The traditional information system storage model adopts the centralized storage mode. Once the central system is attacked, the whole system will face the disaster of destruction.

(2) The integration of multiple technologies has become a challenge for the development of the ATM system. Internet of things (IoT) is the data source, big data is the basic resource, cloud computing is the infrastructure, and artificial intelligence is the core algorithm. Blockchain creates conditions for the transformation of ATM business infrastructure and operation mechanism. The CPS is a comprehensive technical system based on automatic data flow between information space and physical space, including state perception, real-time analysis, scientific decision-making, and accurate execution. The comprehensive application, cross support, and virtuous iteration of cyclic evolution of these new technologies will actively promote the development of ATM intelligence.

3.2. The Framework of ATMChain. In the ATM system, there is often a lack of corresponding encryption technology in the key information delivery link, which makes data tampering and privacy disclosure a major threat. This article presents a security framework to protect the rights and interests of all participants in the information flow of the ATM system. The scheme is designed based on the HyperLedger Fabric of the alliance blockchain architecture. In this paper, ATM is separated into basic physical layer, information processing layer, and information delivery layer. ATMChain framework based on the principle of blockchain distributed architecture is proposed to optimize the layout of ATM-CPS and enhance the overall robustness of the system. Integrating blockchain technology with ATM at all layers and establishing a robust and dependable cyber system will significantly enhance the information security of ATM and optimize the layout of the information system.

3.2.1. System Model. The system model diagram of the ATM-CPS security framework implemented by alliance blockchain technology is shown in Figure 3. Three parties are comprised in the system model: ATM user, ATM information processing entity, and ATM physical space entity. This paper adopts the PBFT [30] consensus mechanism which is most commonly used in alliance blockchain network. Since the consensus mechanism is not the focus of this paper, it will not be described in detail. Their functions are described as follows:

ATM User. It requests ATM message service, purchases information resources, and pays relevant fees.

ATM Information Processing Entity. As a full node operation in the ATMChain, it performs access control and information authorization through smart contracts [31]. It has the characteristics of intelligence and is the main carrier for executing ATM services.

ATM Physical Space Entity. It operates as a light node in ATMChain and encapsulates the information and data storage into the whole node. In addition, the node also collects various requests from the upper information processing entity.

3.2.2. System Framework. This paper focuses on the "value object" of "ATM information" and studies the ATMChain system framework, from information collection to information right confirmation and release, to information transmission, sharing, and use, and finally to the value-added feedback of information value. The intelligent ATM-CPS framework is constructed by tracing the records of the whole life cycle of ATM information. The ATMChain contains three types of nodes. One is the light node responsible for information collection in the ATM physical layer, and the other is the whole node that stores and processes all information and blocks. The third node is the ATM user, and this type of node does not participate in the task of block consensus and block storage. Therefore, ATMChain architecture can be divided into three levels [32–36].

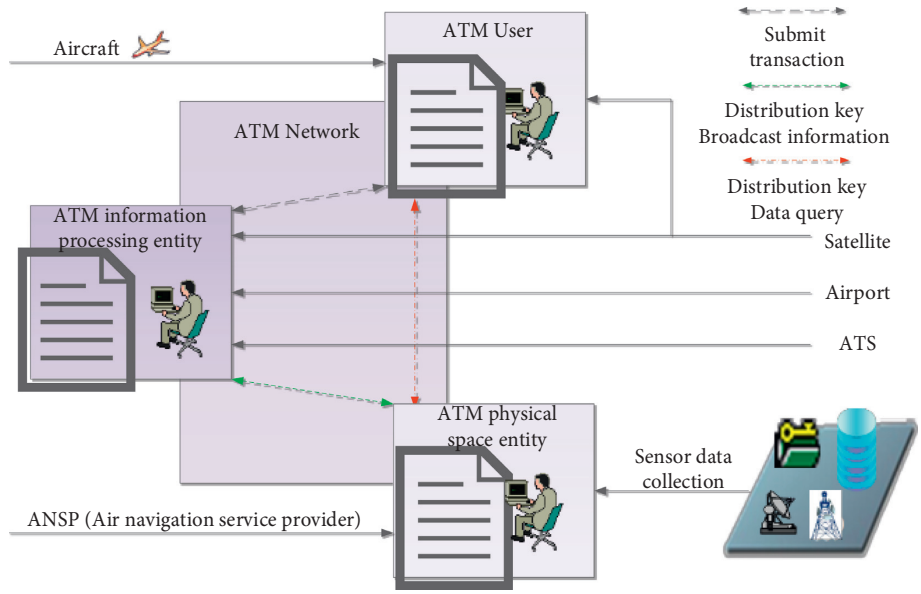


Figure 3: System model diagram of ATMChain.

Firstly, as the bottom support of the whole ATMChain, the CPS sensor physical layer equipment at the basic level not only has the basic sensing, information storage, and transfer functions of traditional CPS physical components but also needs to have the functions of information standardization, mutual data transmission information, and backup of transmission records. Secondly, the whole node of the integration level composed is based on the IoT that perceives the physical world. The nodes in this layer are not only required to achieve deep aggregation and interoperability of the ATMChain base layers, as well as the transfer of heterogeneous information, the allocation of response, speed and frequency of information query requests, but also to audit and authenticate the newly accessed CPS clients in the base layers. In addition, it is its task to unify information format or establish heterogeneous information transformation protocols, unify local scope linkage protocols, maintain block information of this layer, and record device linkage traces and so on. Finally, ATM users constitute the application layer of ATMChain architecture.

The ATMChain system scheme mainly includes six steps: system initialization stage, ATM information collection and uplink stage, ATM information release and authorization stage, ATM information sharing and use stage, block generation stage, and system consensus stage. The operation view of ATMChain system is shown in Figure 4. The definitions of some symbols are given as shown in Table 1. The steps of the system are described as follows.

Step 1. System initialization stage: At this stage, blockchain nodes will establish a blockchain-based ATM information sharing framework through the ECDSA signature algorithm and public key cryptography system. ATM users register in the ATMChain through *KYC* (know your customer) mechanism and their real identity. Among them, the user's key pair, certificate, and wallet address are $(pk_i, sk_i, cert_i, \text{and } WID_i)$, respectively. $Cert_i$ can only use the bound registration information to identify the user. According to the *ECDSA* algorithm, this scheme uses secure elliptic curve parameters, including curve $Ep\ (a, b)$ and base point G, then the U_i selects private key sk_i, and uses G to calculate public key pk_i as shown in the following formula:

$$\begin{cases} sk_i = k\,(k < n) \\ pk_i = kG, \end{cases} \tag{1}$$

U_i sends its wallet address WID_i to a third partner, which generates $(PKI, sk_i, cert_i, WID_i)$. When U_i runs system initialization, the wallet address used is selected from the nearest node account pool. After selection, U_i needs to check the integrity of the wallet and obtain the details. Among them, the account pool stores all transaction records. In addition, the key pair of ATM information processing node is $(sk_B, pk_B) = (k', k'G)$.

Step 2. ATM information collection and uplink stage: At this stage, the light nodes in the ATM physical space collect ATM data into the ATM information processing entity through various sensors. Before transmitting ATM information upward, these light nodes should standardize their own physically perceived data and realize consistent authentication by means of digital signature.

Step 3. ATM information release and authorization stage: The processed ATM information is officially released to the ATMChain with the signature of publisher M. At this time, the specific content of ATM information is encrypted. If you want to use ATM information, you need to obtain M's authorization. All nodes back up and broadcast the published ATM information to each other, so that a wider range of ATM users can use it.

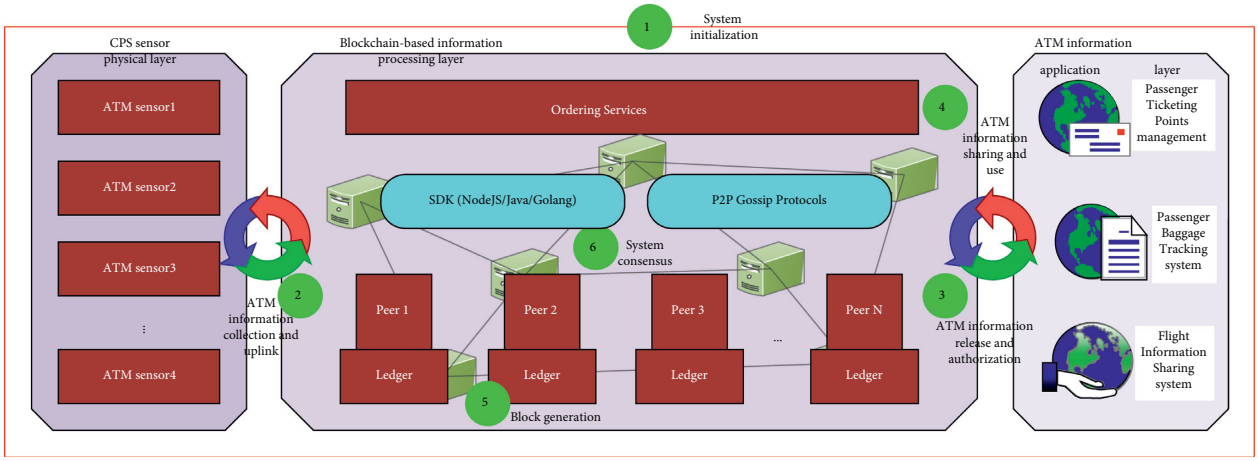


Figure 4: The operation view of the ATMChain system.

Table 1: Symbol definition of ATMChain.

Symbol	Definition
U_i	The ATM user of ATMChain
M	The ATM information processing entity
$Pk_{i/B}$, $sk_{i/B}$	The public and private keys of Ui or M
$cert_i$	Certificate of identity
WID_i	Wallet address of user with ID
$Hash$	The hash value of m
δ_i	User's signature in authorization information
t_1, t_2	The time stamp
$-1,0,1$	Status of information transaction
M	The transaction information

Step 4. ATM information sharing and use stage:At this stage, ATM users interact with ATM information processing node M by running a series of signature algorithms to complete the authorization of ATM information use. The specific process is that U_i sends a request for information authorization to nodes, and then nodes broadcast the message to M. M needs to provide timely feedback within a specified period of time. After receiving the feedback, nodes match U_i's request authorization information with M to complete the transaction.

Step 5. Block generation stage: Before running ATMChain, the nodes participating in the block consensus have been selected to join the system. In order to accomplish the target of more "distributed," the more consensus nodes, the stronger the robustness of the system. In particular, to ensure the authenticity and accuracy of the information, the node will collect all local transaction records and encrypt or sign them at each specific time, packaging them to generate ATM information transaction blocks. These transaction records construct new blocks that refer to the hash value of the previous block, and they will be stored in ATMChain in chronological order. Such a process ensures the traceability of the whole life cycle of ATM information transaction. At this point, the block generation phase ends.

Step 6. System consensus stage: At this stage, the nodes use the PBFT consensus algorithm to reach consensus, thus maintaining the reliable performance of the system. At present, the consensus mechanisms commonly used in alliance blockchain include Pool verification-pool and Byzantine fault-tolerant algorithm. The former is based on traditional distributed consistency technology and information verification mechanism. It can realize second level consensus verification and is suitable for multiparty Multi Center Alliance blockchain. The latter belongs to the state machine Byzantine protocol, which reduces the complexity of the algorithm from exponential level to polynomial level. The PBFT is a consensus algorithm implemented and recommended by HyperLedger Fabric. It adopts the scheme of "one node one vote" to determine the accounting results, with good performance. It is mainly used in alliance blockchain.

3.3. The Information Sharing Algorithm. The ATM information sharing is a crucial step in the whole ATMChain. The specific process is shown as follows:

Step 1. The U_i runs *ECDSA.UserSign* algorithm and enters his key pair (sk_i, pk_i) and relevant parameters, and then the algorithm will output the signature δ_i. The specific steps are as follows:

(a) Generate a random integer d ($d < n$ and n is the order of G), and calculate R and r according to the following formula:

$$\begin{cases} R(x, y) = \mathrm{d}G, \\ r = x \bmod n. \end{cases} \tag{2}$$

(b) The coordinate values of point $R\ (x, y)$ and ATM information m are set as parameters, and the hash value and s are calculated by formula (3) using the hash function SHA256:

$$\begin{cases} \mathrm{Hash} = \mathrm{SHA256}(m, x, y), \\ s = (\mathrm{Hash} + rk)d^{-1} \bmod n. \end{cases} \tag{3}$$

The signature $\delta_i = (s, d)$, and x and $Hash\ (m)$ should be rounded up.

Step 2. U_i sends $\{cert_i, pk_i, \delta_i, m\}$ to M and generates the information use authorization request by the following formula:

$$\mathrm{req}_i = \{\mathrm{cert}_i, pk_i, \delta_i\}. \tag{4}$$

Step 3. M needs to verify the received information after receiving the request. If $cert_i$ exists or authentication fails, the request is rejected. Of course, if $cert_i$ does not exist and the verification is successful, the request is accepted. The specific verification steps are shown in the following formulas:

(a) First, calculate the following:

$$\mathrm{Hash} = \mathrm{SHA256}(m, x, y), \tag{5}$$

$$\begin{cases} u = s^{-1}\mathrm{Hash}(m) \bmod n, \\ v = s^{-1}r \bmod n, \\ (x', y') = uG + vpk_i = uG + v(kG), \\ r' = x' \bmod n. \end{cases} \tag{6}$$

x and $Hash\ (m)$ should be rounded up.

(b) Verify according to the following formula:

$$r \overset{?}{=} r'. \tag{7}$$

If equation (7) is satisfied, the message can be accepted; otherwise, it is invalid. After successful verification, M will accept the request and store the data $(cert_i, pk_B, pk_i, 1, 0)$ in the local account pool; among them, *1* represents the status of valid transaction and *0* represents the status of newly generated transaction that have not been transferred. In addition, *-1* represents the status of transaction awaiting transfer.

Step 4. M signs $(enroll, cert, pk_B, pk_i, t_1)$ by running *ECDSA.MerchantSign* algorithm (similar to *ECDSA.UserSign* algorithm) and using the private key sk_B, where t_1 represents the ATM information request time and *enroll* represents the information of U_i. Then, the $(\delta_i, request_1)$ is sent to the blockchain. The specific signing steps are as follows.

According to formulas (8) and (9), M runs the algorithm and signs m_1:

$$\begin{cases} R(x, y) = d_1 G, \\ r_1 = \overline{x} \bmod n, \end{cases} \tag{8}$$

$$\begin{cases} \mathrm{Hash}_1 = \mathrm{SHA256}(m_1, x, y), \\ s_1 \equiv d_1^{-1}(\mathrm{Hash}_1 + kr_1) (\bmod n), \end{cases} \tag{9}$$

where $m_1 = \{enroll, cert_i, pk_B, pk_i, t_1\}$ and x and $Hash\ (m_1)$ should be rounded up. The final signature is calculated as $\delta_i = (s_1, r_1)$. Then, U_i verifies the signature according to equations (5)–(7).

4. Security Analysis and Simulation

The ATM system is a security sensitive system, and its security objectives are consistent with those of other computer information systems, such as information confidentiality, integrity, availability, and traceability. Based on the research results in the academic field, this paper describes the security of ATM-CPS as security threat, system vulnerability, security attack, and security measures. Meanwhile, the security concerns are decomposed into security mechanisms and security objectives. Security measures refer to the measures to build a secure and robust ATM by integrating security mechanisms and security objectives. The ATMChain framework based on blockchain technology can be regarded as ATM security measures. Therefore, this paper will analyse the scheme from four dimensions: ATM information confidentiality, ATM information integrity analysis, ATM information availability, and ATM information traceability. Finally, the scheme is simply simulated from the perspective of communication cost.

4.1. Information Confidentiality Analysis of ATM. The first thing to measure the security of an information system is to ensure the confidentiality of information, and ATMChain is no exception. Information confidentiality refers to hiding information or resources. Confidentiality means that even if unauthorized persons or organizations are aware of the existence of information resources, they cannot obtain them. ATMChain integrates the principle of blockchain with CPS to give full play to the security mechanism of blockchain. In the blockchain, the data between nodes are backed up synchronously to ensure that the ATM participants entering the system share information. At the same time, the information is encrypted by the encryption algorithm and transmitted through asymmetric key pairs, which greatly improves the information confidentiality in the process of ATM information transmission.

4.2. Information Integrity Analysis of ATM. Information integrity refers to the credibility of data or resources, which is usually used to prevent improper modification of data or unauthorized tampering of data. Loss of integrity means that the information is subject to unauthorized tampering and information loss. In ATMChain, M can prove the

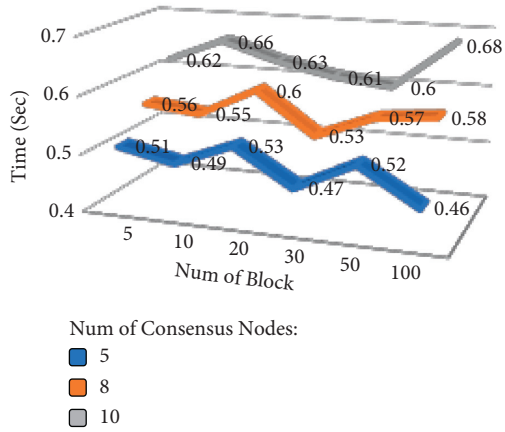


Figure 5: The generation time of block.

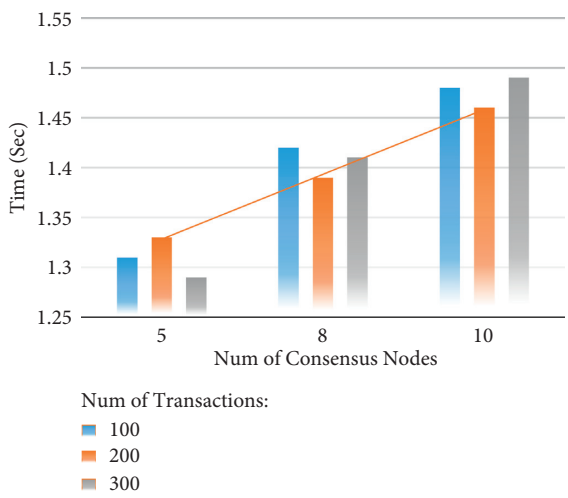


Figure 6: The time of transaction confirmation.

correctness of the signature of the authorized user and the authorization to request ATM information through the following formula. Therefore, when M verifies successfully, it indicates that the signature and the authorization information are legal and correct. Then, M will accept the request and store the information $(cert_i, pk_B, pk_i, 1, 0)$ in the local account pool and continue to execute the next algorithm. The verification mechanism avoids the deceptive attack of illegal nodes disguised as authorized nodes in central authorization. In addition, after the data blocks are added to the blockchain, each consensus node will also verify the block data. Only the verified data blocks can be added to the blockchain to guarantee the authenticity of the data. Last but not least, the unique tamper proof characteristics of the blockchain also greatly increase the stability of the data in the block.

4.3. Information Availability Analysis of ATM. Information availability refers to the ability to use the required information or resources. Loss of availability means that access to or use of information or information systems is blocked. Denial of service (DoS) is one of the most threatening security attacks faced by the ATM system. Therefore, the availability goal in ATMChain is to prevent DoS attacks to ensure the availability of information. Meanwhile, a remarkable feature of the ATM system is the integration of time and space, so ensuring the real-time operation is also an important aspect. Under the ATMChain framework, the blockchain distributed architecture can realize the interactive loop between the actual world and the cyber world, which is different from the traditional single centralized control, avoids the DoS attack of the attacker on the system, and ensures the availability of information. In ATMChain, the hysteresis caused by information perception, transmission, control, and optimization feedback is also compensated by the full sharing advantage of information to ensure real-time and field tracking.

4.4. Information Traceability Analysis of ATM. Information traceability is an important information security goal in addition to confidentiality, integrity, and availability. Information traceability means that information can be tracked. In ATM, traceability means real-time tracking of the operation of physical entities. When there is a deviation in the operation state of the physical world, the time and cause of the deviation can be accurately found. In the ATMChain, each block includes two parts: block header and block body. The block header encapsulates the current block header value, preblock header hash value, timestamp, random number, and other ATM information. By encapsulating the hash value of the front block in each block, the current block is connected with its front block to form a chain structure. The sequence of blocks in the blockchain is confirmed by the time sequence stamped with time stamps, and it is consistent with the historical sequence of time stamps. Thus, the blockchain structure with time sequence is formed. The data are arranged in chronological order to ensure the historical traceability of the information. When there is a deviation in the operation state of the actual entity, the error information fed back to the ATM system can be found according to the chronological order. Meanwhile, the information in the basic layer CPS can be stored in the ATM information processing layer, so the deviation can be traced from the information processing layer.

4.5. Simulation. In terms of the communication cost of this scheme, that is, the interaction time of the whole algorithm during ATM information sharing, the main influencing factors are the transaction confirmation time and the block generation time. The scheme runs experiments on a genuine Intel computer device, using the programming language Python, the operating system is windows 10, CPU 2.5 GHz, and running memory 16 GB. We are concerned with the time required for ATM information sharing transactions to be confirmed and recorded on the blockchain. There are two signatures in the transaction confirmation process, one for U_i and one for M. There are also two signatures for verification.

In this paper, we first test the block generation time in ATMchain to test its throughput. Each experiment randomly generates a number of blocks (averaged as block generation time), and each block contains 5 transactions. As shown in Figure 5, under the condition that the number of consensus nodes is constant, the block generation time is independent of the frequency of initiated transactions, while with the increase in the number of consensus nodes, the block generation time also increases slightly, but all can meet the actual deployment requirements. Second, the time for transaction confirmation might be affected by the frequency of transactions and the number of consensus nodes under the condition that there are no errors in two message verifications. The results show that only the number of consensus nodes has an impact on the transaction confirmation time (as in Figure 6). Therefore, the relationship between the number of consensus nodes and the throughput needs to be balanced to obtain the best system performance. Finally, with a consensus node of 5, it can be estimated that the process of a single information sharing transaction from generating to recording on the blockchain takes about 1.82 s in total, which can meet the actual demand.

5. Conclusion

This paper presents a blockchain and CPS integration architecture for the ATM system. The purpose is to grasp the CPS characteristics of the ATM system, integrate the advantages of blockchain technology, promote the research and development, and improve the service processing capacity of existing ATM. In terms of ideas, firstly, after summarizing and analyzing the characteristics and research background, it leads to the benefits of the research thinking of blockchain and CPS to the development of the ATM system. Then, taking ATMChain security architecture as the core, this paper details the research background, framework, and key algorithm. Based on the traceability and nontamper ability of blockchain in data storage and sharing, the secure sharing of multiparty heterogeneous data in ATM environment is designed. Finally, the security of ATMChain framework is analysed from four dimensions, which are confidentiality, integrity, availability, and traceability of information security. This paper provides a novel useful idea for the construction, development, and research of the ATM system.

In the following research, firstly, the degree of decentralization of architecture design can still be further optimized, and the distributed subsystem can be used for cluster management. Secondly, it will be proposed to further optimize and refine the research design of ATMChain through the research on the consensus mechanism and smart contract of the blockchain. In addition, in terms of system security and privacy, we can integrate zero knowledge proof, homomorphic encryption, and other technologies with the system to realize data encryption and identity concealment, improve the privacy of the system, as well as the design of multilevel identity authentication and access control [37–39]. Finally, the concept of interaction and integration of human, machine, environment, and management, which has been emphasized in ATM system research, is still lacking in ATMChain design, which is also the direction of future efforts.

Data Availability

This paper is an article on the design of air traffic management architecture. At present, it has only carried out preliminary theoretical analysis and research and has not carried out experimental simulation based on actual data. In future research, the corresponding data sets can be shared.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the joint funds of the National Natural Science Foundation of China and Civil Aviation Administration of China (U1933108), the Scientific Research Project of Tianjin Municipal Education Commission (2019KJ117), and the Tianjin Research Innovation Project for Postgraduate Students (2021YJSB240).

References

[1] L. Bogoda, J. Mo, and C. Bil, "A systems engineering approach to appraise cybersecurity risks of CNS/ATM and avionics systems," *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, ICNS), in *Proceedings of the 2019 Integrated Communications, Navigation and Surveillance Conference*, pp. 1–15, April 2019.

[2] K. Sampigethaya and R. Poovendran, "Aviation cyber-physical systems: foundations for future aircraft and air transport," *Proceedings of the IEEE*, vol. 101, no. 8, pp. 1834–1855, 2013.

[3] K. Sampigethaya and R. Poovendran, "Cyber-physical integration in future aviation information systems," in *Proceedings of the 2012 IEEE/AIAA Thirty First Digital Avionics Systems Conference (DASC)*, pp. 7C2-1–12, Williamsburg, VA, USA, October 2012.

[4] W. Zhang, M. Kamgarpour, D. Sun, and C. J. Tomlin, "A hierarchical flight planning framework for air traffic management," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 179–194, 2012.

[5] ICAO, "Cybersecurity Strategy," 2019, https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx.

[6] M. Shengdong, X. Zhengxian, and T. Yixiang, "Intelligent traffic control system based on cloud computing and big data mining," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6583–6592, 2019.

[7] R. Sabatini, A. Roy, E. Blasch et al., "Avionics systems panel research and innovation perspectives," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 12, pp. 58–72, 2020.

[8] M. Mitici and H. A. P. Blom, "Mathematical models for air traffic conflict and collision probability estimation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 3, pp. 1052–1068, March 2019.

[9] P. Park and C. Tomlin, "Investigating Communication Infrastructure of Next Generation Air Traffic Management," in *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*, pp. 35–44, Beijing, China, April 2012.

[10] A. Kanak, N. Ugur, and S. Ergun, "Diamond Accountability Model for Blockchain-Enabled Cyber-Physical Systems," in *Proceedings of the 2020 IEEE International Conference on Human-Machine Systems (ICHMS)*, pp. 1–5, Rome, Italy, September 2020.

[11] A. Gu, Z. Yin, C. Fan, and F. Xu, "Safety framework based on blockchain for intelligent manufacturing cyber physical system," in *Proceedings of the 2019 First International Conference on Industrial Artificial Intelligence (IAI)*, pp. 1–5, Shenyang, China, July 2019.

[12] W. Zhao, C. Jiang, H. Gao, S. Yang, and X. Luo, "Blockchain-enabled cyber–physical systems: a review," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4023–4034, 2021.

[13] Z. Rahman, I. Khalil, X. Yi, and M. Atiquzzaman, "Blockchain-based security framework for a critical industry 4.0 cyber-physical system," *IEEE Communications Magazine*, vol. 59, no. 5, pp. 128–134, 2021.

[14] M. Y. Afanasev, Y. V. Fedosov, A. A. Krylova, and S. A. Shorokhov, "An Application of Blockchain and Smart Contracts for Machine-To-Machine Communications in Cyber-Physical Production Systems," in *Proceedings of the 2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pp. 13–19, St. Petersburg, Russia, May 2018.

[15] M. Dehez Clementi, N. Larrieu, E. Lochin, M. A. Kaafar, and H. Asghar, "When Air Traffic Management Meets Blockchain Technology: A Blockchain-Based Concept for Securing the Sharing of Flight Data," in *Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC)*, pp. 1–10, San Diego, CA, USA, September 2019.

[16] F. Hasin, T. H. Munia, N. N. Zumu, and K. A. Taher, "ADS-B based air traffic management system using ethereum blockchain technology," in *Proceedings of the 2021 International Conference on Information and Communication Technology for Sustainable Development*, pp. 346–350, ICICT4SD), Dhaka, Bangladesh, February 2021.

[17] I. S. Bonomo, I. R. Barbosa, L. Monteiro et al., "Development of SWIM registry for air traffic management with the blockchain support," in *Proceedings of the 2018 Twenty First International Conference on Intelligent Transportation Systems (ITSC)*, pp. 3544–3549, Maui, HI, USA, November 2018.

[18] A. Sternstein, "Exclusive: FAA computer systems hit by cyberattack earlier this year," 2015, https://www.nextgov.com/cybersecurity/2015/04/faa-computer-systems-hit-cyberattack-earlier-year/109384/.

[19] Y. Yuan and F. Wang, "Blockchain: the state of the art and future trends," *Acta Automatica Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[20] China Blockchain Technology and Industry Development Forum, "China blockchain technology and application development white paper," China Blockchain Technology and Industry Development Forum, China, (in Chinese), 2016.

[21] Z. Wu, T. Shang, and A. Guo, "Security issues in automatic dependent surveillance - broadcast (ads-B): a survey," *IEEE Access*, vol. 8, Article ID 122147, 2020.

[22] X. Koutsoukos, G. Karsai, A. Laszka et al., "SURE: a modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems," *Proceedings of the IEEE*, vol. 106, no. 1, pp. 93–112, 2018.

[23] B. Besselink, V. Turri, S. H. van de Hoef et al., "Cyber–physical control of road freight transport," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1128–1141, 2016.

[24] ICAO, *Global ATM Operational Concept*, International Civil Aviation Organization, Montreal, Canada, Doc I. 9854, 2005.

[25] ICAO, *Manual on ATM Requirements*, International Civil Aviation Organization, Montreal, Canada, Doc I. 9882, 2008.

[26] ICAO, *Manual on Collaborative Air Traffic Flow Management*, International Civil Aviation Organization, Montreal, Canada, Doc I. 9965, 2012.

[27] ICAO, *Global Air Navigation Plan*, International Civil Aviation Organization, Montreal, Canada, Doc I. 9750, 4 edition, 2013.

[28] Y. Wu, X. Lu, and Z. Wu, "Blockchain-based trust model for air traffic management network," in *Proceedings of the 2021 IEEE Sixth International Conference on Computer and Communication Systems*, pp. 92–98, ICCCS), Chengdu, China, April 2021.

[29] Y. Chen, S. Dong, T. Li, Y. Wang, and H. Zhou, "Dynamic multi-key FHE in asymmetric key setting from LWE," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 5239–5249, 2021.

[30] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer PBFT consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2021.

[31] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F. Wang, "An overview of smart contract: architecture, applications, and future trends," in *Proceedings of the 2018 IEEE Intelligent Vehicles Symposium (IV)*, pp. 108–113, Changshu, China, June 2018.

[32] T. Li, Z. Wang, G. Yang, Y. Cui, Y. Chen, and X. Yu, "Semi-selfish mining based on hidden Markov decision process," *International Journal of Intelligent Systems*, vol. 36, pp. 3596–3612, 2021.

[33] Y. Chen, J. Sun, Y. Yang, T. Li, X. Niu, and H. Zhou, "A source location privacy protection scheme based on sector phantom routing in WSNs," *International Journal of Intelligent Systems*, vol. 37, pp. 1–18, 2021.

[34] T. Li, Z. Wang, Y. Chen, C. Li, Y. Jia, and Y. Yang, "Is semi-selfish mining available without being detected?" *International Journal of Intelligent Systems*, vol. 36, pp. 1–22, 2021.

[35] X. Lu, Z. Wu, Y. Wu, Q. Wang, and Y. Yin, "ATMChain: Blockchain-Based Solution to Security Problems in Air Traffic Management," in *Proceedings of the 2021 IEEE/AIAA Fortyth Digital Avionics Systems Conference (DASC)*, pp. 1–8, San Antonio, TX, USA, October 2021.

[36] X. Lu and Z. Wu, "ATMCC: design of the integration architecture of cloud computing and blockchain for air traffic management," in *Proceedings of the 2021 IEEE International Symposium on Parallel and Distributed Processing with Applications*, pp. 37–43, New York City, NY, USA, October 2021.

[37] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured Internet of medical things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, Article ID 11717, 2021.

[38] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5522–5532, 2021.

[39] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in cyber physical systems: integration of blockchain and edge computing," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 1, pp. 43–57, 2020.