ATMChain: Blockchain-Based Security Architecture for Air Traffic Management in Future

XIN LU
Shanxi College of Technology, Shanxi, China

ZHIJUN WU
Civil Aviation University of China, Tianjin, China

JUNBIN CAO
Shanxi College of Technology, Shanxi, China

The air traffic management (ATM) is a comprehensive information-based intelligent system that provides seamless services and dynamic integrated management of air traffic and airspace through the cooperation of all relevant parties in civil aviation. The composition of the ATM is wide and complex, and contains many business systems and user types. In the face of the increasingly serious information security threats, the business collaboration of ATM and the shared use of ATM data are subject to certain restrictions and challenges. According to the Aviation Network Security Strategy released by International Civil Aviation Organization (ICAO) in 2019, there is an urgent need to research the basic theories, core methods and key technologies for ATM information security assurance that are compatible with the characteristics of ATM composition and information security assurance needs. From the core research objective of ATM information security assurance, this paper designs a future ATM security architecture based on blockchain technology, referred to as ATMChain, to meet the real operational needs of ATM trustworthiness, security and availability. ATMChain takes ATM trustworthy services as the core and builds an ATM information security base with "endogenous security" features. Then, three security function modules, namely, trusted authentication, data sharing, and access control, are designed to realize the 4A (Authentication, Account, Audit, Authorization) security functions of ATM. Finally, this paper provides a comprehensive analysis and performance evaluation of ATMChain security architecture. The results show that the research will help solve the current bottlenecks in ATM information security assurance, promote technological innovation.

Manuscript received 20 March 2023; revised 22 August 2023 and 14 December 2023; accepted 17 February 2024. Date of publication 29 February 2024; date of current version 9 August 2024.

DOI. No. 10.1109/TAES.2024.3371396

Refereeing of this contribution was handled by G. Chen.

This work was supported in part by the National Key R&D Program of China under Grant 2022YFB3904503, in part by the National Natural Science Foundation of China under Grant 62172418, in part by the Natural Science Foundation of Tianjin, China under Grant 21JCZDJC00830, in part by the Scientific Research Start-up Funding Program of Shanxi College of Technology under Grant 200102 and Grant 009012, and in part by the Research Funding for Introduced Talents in Shanxi under Grant 004031.

Authors' addresses: Xin Lu and Junbin Cao are with the School of Information Engineering, Shanxi College of Technology, Shanxi 036000, China, E-mail: (2018071030@cauc.edu.cn; junbincao@139.com); Zhijun Wu is with the School of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China, E-mail: (zjwu@cauc.edu.cn). *(Xin Lu and Zhijun Wu are co-first author.) (Corresponding author: Zhijun Wu.)*

I. INTRODUCTION

The air traffic management (ATM) is a comprehensive system for dynamic and integrated management of air traffic and airspace with the goal of achieving trusted, secure, and available air traffic services, airspace management, and air traffic flow management [1]. ATM is also a space–air–ground integrated intelligent information network that connects space satellite (communication and navigation) network, airborne network, and ground computer network through ground–space data chain [2]. From the perspective of system and network, ATM is wide-area large, complex in composition, heterogeneous and open, such characteristics make it pay particular attention to information security and security interactions during its operation, which also brings a greater pressure on information security assurance for ATM in countries around the world [3]. With the popularization of internet technologies such as Big Data [4], Internet of Things [5], cloud computing [6], and artificial intelligence [7] in ATM, the ATM which is characterized by networking, with highly integrated information, rapid network scale expansion, increasing demand for network interconnection, and increasingly complex network structure and network applications, the information security of ATM is facing serious challenges. In addition, with the widespread use of mobile devices, smart terminals, sensors, and other network and communication technologies in ATM, the scale of ATM business data is growing rapidly, and a series of information security risks and hidden dangers affecting the secure operation of ATM are emerging gradually, so the traditional means of ATM information security can no longer gradually meet the security and safety needs it faces [8].

Blockchain, as an emerging technology that has developed relatively rapidly in recent years, can be regarded as an Internet-based distributed database management method, a new computer technology model application, from its essence [9]. The technical characteristics of blockchain make it uniquely advantageous in creating an open, equal, and win–win cooperative trust scenario in the new era. The application mode of blockchain varies for different application scenarios and mainly includes three types: public blockchain, federated blockchain, and private blockchain. In the context of the ATM research in this article, it is the model of federated blockchain that is used. In this article, blockchain technology is considered as a security assurance concept for information system rather than a specific technology. Unlike the traditional centralized network architecture, blockchain weakens the concept of a central server, giving it a decentralized character. Moreover, blockchain overturns the traditional account model, and data information is no longer recorded by a single institution, but by each node in the distributed network of blockchain, which

TABLE I
Comparison of the Research Work in This Article With the Previous Research

Schemes	[15]	[16]	[17]	ATMChain
Extent of research	Simple and not comprehensive	Not systematic and not comprehensive	Systematic and not comprehensive	Systematic and comprehensive
Contribution of research	Conceptual Model	Simple scenario design and application	Application architecture design	General architecture and specific method implementation
Difficulty of application	Difficult	Difficult	Difficult	Easier

makes each node in the network have a complete backup of the ledger. Furthermore, blockchain hashes the block data by hash algorithm, which cryptographically gives the chain-data structure formed by sequentially linked blocks tamper-evident and easily traceable. The core of blockchain technology is the "proof of storage" and "proof of circulation," and the consensus mechanism formed on this basis [10]. The consensus mechanism is the algorithm that reaches consensus on the order of blockchain transactions over a period of time and eventually forms blocks. Finally, in the whole blockchain system, various applications based on information flow are realized through smart contracts [11], which give value to "information" and eventually realize the restructuring of production relations in social organizations [12].

The civil aviation transportation industry is technology-intensive, and at the advent of the fourth data-centric industrial revolution, there is a large scope for technological upgrades in the security assurance of in ATM. According to the Aviation Network Security Strategy released by International Civil Aviation Organization (ICAO) in 2019, there is an urgent need to research the basic theories, core methods, and key technologies for ATM information security assurance that are compatible with the characteristics of ATM composition and information security assurance needs [13]. Compared to other common business systems, ATM has its special characteristics in that it is widely distributed. And the presence of many real-time applications in ATM using proprietary protocols has further led to the creation of a number of unanticipated security threats. In addition, the security measures currently in place are often based on finding a problem and correcting it, and constantly "patching" the original technology, which not only increases the complexity of the ATM, but can even cause unnecessary security risks. In current ATM, information security for ATM services focuses on three main areas: authentication, authorization, and accounting. Although audit is often considered part of accounting, accounting tends to focus more on recording while audit focuses more on monitoring. ATM as a digital intelligent network system, with monitoring getting more and more attention in ATM, its information security measures are mainly built on the 4A (authentication, authorization, accounting, audit) unified security management platform solution commonly recognized by the international network security community [14]. However, the current 4A traditional centralized architecture and technical implementation is not compatible with the distributed feature of ATM, but also increasingly unable to meet the business development and security control requirements of ATM. In turn, in terms of reliability (lowest possible system failure rate) and security (lowest possible information security risks), a distributed infrastructure security architecture that meets the essential characteristics of ATM is needed to meet the future development needs of a more secure, adaptable, and scalable ATM. Therefore, this article combines blockchain with 4A information security assurance concept, builds a trustworthy model of ATM with distributed characteristic, makes innovative breakthroughs in the research of security assurance methods in three dimensions: trusted authentication, data sharing, and access control, then forms a blockchain-based ATM security architecture, and finally achieves the goal of trustworthy, secure, and available ATM information security assurance.

Previously, there have been three papers [15], [16], [17], published by us around the fusion of ATM and blockchain to enhance ATM information security assurance capability, and part of the work and the establishment of the research ideas in this article are precisely based on the previous research. However, this article is not a simple expansion or supplement of the previous papers. It is more comprehensive and systematic in terms of modeling and method design. Compared with the previous study, as shown in Table I, there are three important innovations in this article. First, it presents a clearer ATM information security assurance model rather than a conceptual model, which is more valuable for practical applications. Second, it combines the 4A information security assurance concepts currently used for ATM with blockchain, which is more feasible and easier to deploy and apply in the future. Finally, it provides a detailed design of three key ATM information security assurance methods and conducts simulation experiments, which is work not yet covered in previous papers.

The relevance of the research contents in this article is shown in Fig. 1. Around the ATM information security assurance needs, this article constructs a trusted model of ATM based on blockchain, designs a security architecture (ATMChain) based on the trusted model, and implements three security function modules: trusted authentication (referred to as T-ATMChain), data sharing (referred to as S-ATMChain), and access control (referred to as A-ATMChain). The three modules together realize the "4A" security function and form a trusted, secure, and available ATM information security mechanism. Based on the logical sequence of the research content of this article, Section II introduces the feasibility and suitability of the integration of blockchain and ATM security from several aspects. Then, Section III proposes the blockchain-based security architecture, ATMChain. The specific design of three security modules is given in Section IV. Section V provides a comprehensive analysis and performance evaluation

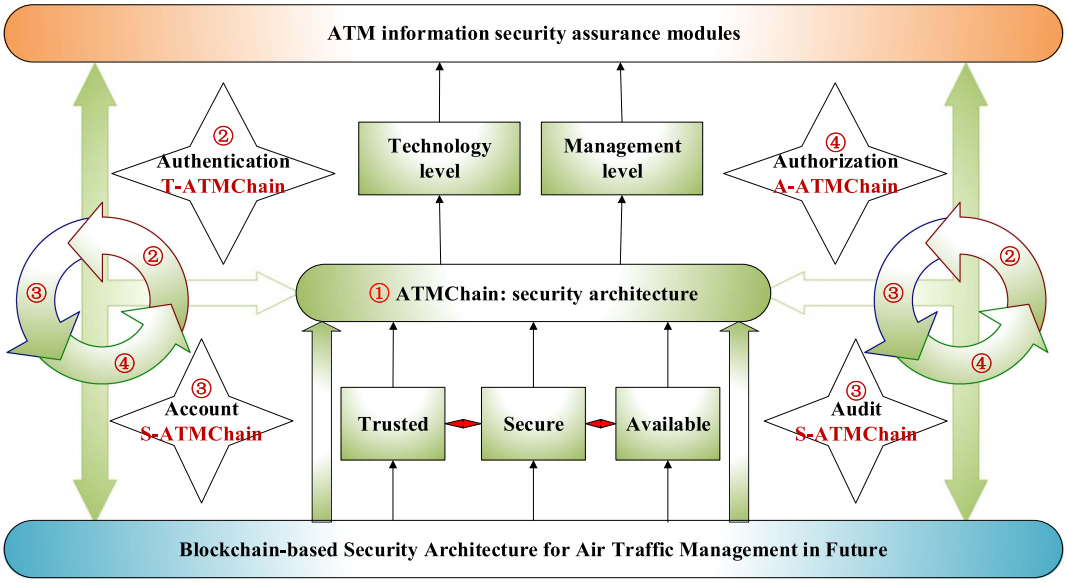


Fig. 1. Research contents of this article and their interrelationship.

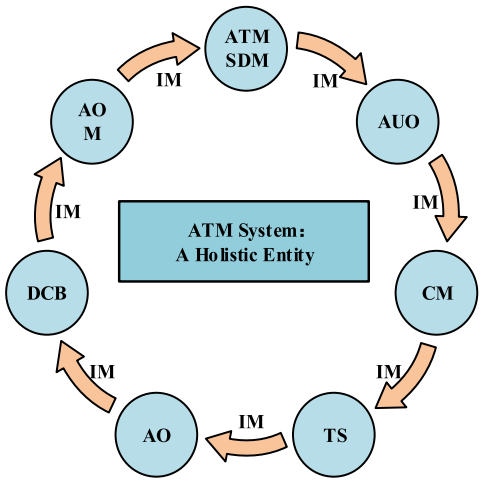
of the ATMChain scheme. Section VI summarizes and elaborates the research work in the full paper and provides possible future research directions.

II. WHEN ATM SYSTEM MEETS BLOCKCHAIN

A. Requirement of ATM Information Security Assurance

Since ATM plays a vital role in securing civil aviation transportation, the reliability and security of ATM is very important. Generally, there are two possible consequences of ATM failures or errors: one is a large delay or cancellation at civil airports, resulting in stranded passengers at airports, which results in huge economic losses and negative social impacts; the other is a dangerous civil aviation accident syndrome or a catastrophic civil aviation accident. The ICAO in the Global Air Traffic Management Concept of Operations (Doc 9854) [1] specifies that the ATM concept of operation consists of seven components: airspace organization and management, aerodrome operation, demand and capacity balancing, traffic synchronization, conflict management, airspace user operation, and ATM service delivery management, all of which operate on the basis of information management (as shown in Fig. 2). The management, utilization, and transmission of ATM data is critical to the proper functioning of these components. The foundation and prerequisite for information management is information security assurance. Security is the highest priority for ATM and only when comprehensive security measures are implemented to ensure the security operation of the ATM, can the ATM system achieve efficient and effective civil aviation transportation control services.

As early as 1996, ICAO pointed out that ATM information transmitted through the data chain is at risk of tampering, replay and forgery attacks, while further stating that all ATM applications have the possibility of experiencing distributed denial of service (DDoS) attacks. In recent years, information security incidents in the global civil



AOM — Airspace organization and management
DCB — Demand/capacity balancing
AO — Aerodrome operation TS — Traffic synchronization
CM — Conflict management AUO — Airspace user operation
ATM SDM — ATM service delivery management
IM — Information Management

Fig. 2. ATM concept defined by ICAO.

aviation industry have gradually increased, causing serious economic losses and even affecting flight safety. In addition, the critical role of air traffic service provider (ATSP) has become more frequent in some national security-related operations. For example, in disaster prevention and emergency response operations, which often require the use of ATM procedures (e.g., temporary airspace/flight restrictions, etc.) to provide required safety and security measures, even if certain activities and operations are not intended for civil aviation systems, they may still have an impact on ATM if not managed properly. As a result, relevant government departments, research institutions, experts and

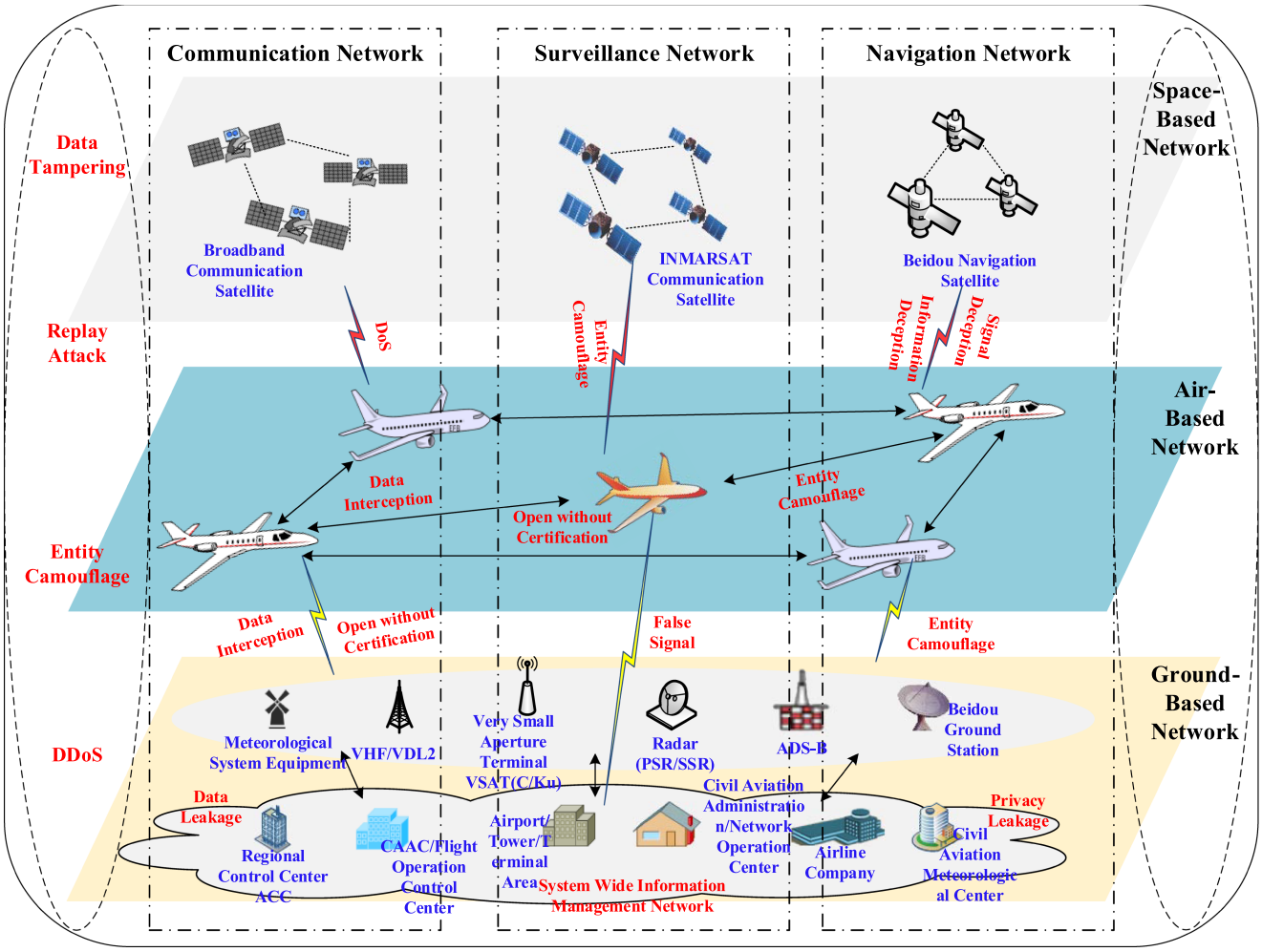


Fig. 3. ATM system security threats.

scholars around the world have expressed concern about the possibility of cyber-attacks on ATM system, and the protection of ATM from information security threats has become an issue of concern.

In a networked ATM, information security is essential to ensure its operational safety. As ATM networking and informatization continue to deepen, the devices involved in ATM become diverse and complex, the ATM user groups becomes increasingly large, the ATM network size expands rapidly, and the ATM network structure and service applications become increasingly diverse, ATM faces huge security threats and serious security challenges. In the past, ATM information security has gone through a security construction process from a single virus defense system to a simple stack of information security products. However, with the increasingly close connection among civil aviation, ATM and other departments, the volume of information exchange between military and civil aviation is also gradually increasing, and the networked ATM is becoming bloated under the addition of various new technologies (such as Big Data, cloud computing, artificial intelligence, etc.). The information security situation of the ATM has become more complex, resulting in more security threats, which are mainly summarized in four aspects, including data tampering, replay attacks, entity disguise, and DDoS attacks (see Fig. 3). Accordingly, the networked ATM information security development needs can be targeted to the following four corresponding points.

First of all, it is necessary to build a trusted networked ATM security assurance model in order to carry out research on key ATM information security technologies on this basis, and then fundamentally build an ATM security assurance architecture that can resist DDoS attack. Currently, the entire ATM lacks a unified information security assurance strategy, and malicious attackers may choose aspects with weaker guarantees for intrusion. The wide-area distribution of ATM leads to the scattering of its network equipment, making it difficult for its information security assurance personnel to effectively operate and monitor these network equipment. Most of the transmission networks in ATM use dedicated lines to build a special internal network isolated from the Internet and relatively closed to the outside world. For external network threats, ATM security can be ensured by installing, for example, firewalls and intrusion detection systems to block illegal end-user intrusion (e.g., hacking, malicious code and virus injection, etc.). However, security threats on the intranet still cannot be ignored, mainly illegal outreach from computers, virus proliferation from mobile memory, and unauthorized access from legitimate terminals, which may lead to leakage or tampering of confidential

information in the system. In addition, due to the business development of ATM, some internal networks are connected to the external Internet. The openness of the Internet increases some of the security vulnerabilities, which may lead to network viruses entering the ATM and directly causing the leakage of flight information or other important data.

Second, trusted security certification is the first step in the construction of ATM information security assurance system, which can prevent and eliminate security threats such as entity masquerade and replay attacks. Networked ATM is a system that integrates network space (space–air–ground integrated network) and physical space (civil airports, airlines, and operation centers) through "satellite communication and navigation technology, ground-air data chain transmission technology and computer network technology," and its openness causes the lack of trusted security authentication. On one hand, due to the openness and wide area distribution of the ATM, the trust relationship among the participants in the system is complex, and the authentication architecture based on public key infrastructure (PKI) is increasingly difficult to meet the growing demand for authentication of ATM services. On the other hand, a portion of current civil aviation communications is unauthenticated, and the ability to respond and coordinate in the face of unforeseen situations can be constrained accordingly. For example, DDoS attacks against the core/distribution network of an ATSP facility: due to the lack of trusted authentication, the ground control center of the ATM cannot determine whether the message came from the target aircraft. Although the ground can verify the authenticity of the information by comparing flight plans, if the attacker sends a large amount of data, it can lead to the control center being paralyzed.

Furthermore, the operation of ATM system requires cross-region and cross-department data sharing, and guaranteeing its data sharing process in a secure and effective manner to avoid intrusion and attack is a proper part of its information security assurance. However, the large number of ATM departments and complex coordination, coupled with the fact that the security and privacy issues in the data sharing process have not been fully resolved, which often leads to its poor data sharing and creates the problem of difficult data sharing. In addition, due to the sensitivity and heterogeneity of ATM data, ATM departments in various countries or regions are generally reluctant to share them out, further leading to problems such as low utilization and low trustworthiness of ATM data. The security challenges in ATM data sharing mainly include the lack of data privacy protection means, the unmet demand for data authenticity and traceability, and the insufficient guarantee of data consistency and availability, etc. ATM data storage is scattered, and a large amount of ATM data cannot be effectively protected and shared in a timely manner, and ATM data sharing method needs to be researched and designed to address the security challenges in ATM data sharing. That makes ATM data sharing one of the core key issues that need to be addressed for networked ATM information security assurance.

Finally, to ensure the sharing and security of ATM data, secure and flexible access control method must be employed. Although ATM system builds a dedicated internal network for confidential and sensitive information transfer and sharing, unauthorized interception or interference can still occur. Currently, the access control techniques used in ATM system have to establish a centralized authorization decision entity that makes decisions based on access control policies and other attribute information, which is risky and the process is more or less problematic in terms of authorization management, fine-grained access control, access control policy description, data privacy protection, and difficulty of access control implementation in distributed architecture. Meanwhile, in the access control of ATM data, some new features and requirements are gradually presented, such as diversification of decision basis, ambiguity of decision result, and integration of multiple access control techniques. Therefore, it is necessary to research and design more flexible, more trustworthy, and more secure controlled access authorization mechanisms by integrating the characteristics of ATM data multisource, ATM user diversity, and the demand of ATM data privacy protection.

B. Issues of ATM Information Security Assurance

Combined with the construction and development of China's ATM, the current major ATM information security assurance research work is categorized and compared (see Table II). From the relevant comparisons in the table, it can be seen that there are four issues that need to be addressed in the current ATM information security assurance research.

The first issue is the lack of systematic ATM information security assurance. All along, the ATM industry mainly determines the security measures it adopts based on the information security assurance needs of each regional ATM department itself, and local ATM departments tend to focus only on the security of local information resources and lack cooperation with other regional stakeholders. The serious impact of ATM information security on the safe operation of ATM system (operational security) has not been emphasized by the management and technical departments at all levels of ATM system, and the analysis and research on ATM information security assurance are scattered and not systematic. The information sharing interactions among ATM service providers rely only on point-to-point bilateral connections, and interconnections with nonstakeholders are often based on ad hoc setups or the open Internet. As for the proposition of ATM information security, domestic and foreign research works often only put forward targeted solutions for a certain level or business link of ATM information security, but lack systematic research works combining with the distributed characteristics of ATM system and security requirements, and the effect of the implemented local security measures is often unsatisfactory in the overall application of the whole domain.

The second issue is that there is no ATM trusted model applicable to networked ATM. Taking trustworthiness as the basic principle, constructing ATM trustworthy model is the first step to solve the problem of ATM information security assurance. "Trustworthiness" comes from the trust relationship between each ATM logical entity providing ATM services, and the construction of the trust relationship is closely related to the organizational relationship of ATM departments. Take ISS in the United States as an example, in order to provide credible, security and reliable ATM services, it has formed a relatively perfect trust system, which mainly relies on the two modes of "trust transfer" and "trust contract." Specifically, they are "trust transfer"

TABLE II
Classification and Comparison of Typical ATM Information Security Assurance Research Works

Typical Research	Research Object	Research Method	Benefits	Weaknesses
[18]	ATM in USA	Construct PKI-based structure/operation/processing model to form a trustworthy system	Expanding the information security guarantee capability to the air-sky-ground three-dimensional space of ATC, covering all levels of CNS/ATM	The plan was put forward earlier, and the information security guarantee technology is gradually not compatible with the characteristics of networked ATM
[19]	ATC/airborne system	Developing an attack and defense scenario to collaboratively conduct cybersecurity vulnerability mining and penetration testing	Enhanced information security assurance capability of ATC, etc.	Information security assurance for single ATM business system
[20]	ATM in Europe	Network security management/assessment and testing methodologies	Comprehensive assessment of potential security threats and vulnerabilities in European ATM	The project focuses on ATM information security assessment, with little coverage of information security assurance technologies
[21]	ATM in China	From policy formulation to operational concepts, to specific infrastructure construction, and finally to the formation of ATM efficient service guarantee capability	A systematic ATM development plan from strategy to tactics, from macro to micro	Being implemented, in the initial stage
[22]	ATM in China	Based on safety system engineering SSE theory and system dynamic control DSC idea	ATM information security assessment model, ATM information security level assessment method, ATM data access method are proposed	The research focuses mainly on ATM information security assessment
[23]	CNS/ATM	Secure prototyping methodology for ATM	Dividing CNS/ATM into separate subsystems for security assessment	Overall security assessment models and methods have not been proposed
[24]	CNS/ATM	Based on hierarchical analysis method AHP and fuzzy inference system FIS	Consistent description of security risk attributes of CNS/ATM has been conducted	The research only focuses on the risk assessment aspect of ATM information security assurance

mode constructed on the basis of PKI and "trust contract" mode constructed on the basis of mutual endorsement by functional authorities, which both modes need to rely on credible third-party organizations and have certain security risks. ATM needs to integrate new technologies to build an interactive and trustworthy model compatible with its distributed and networked characteristics, and to form an overall ATM information security research consciousness and thinking from top-level model research to key security technology design.

The third issue is the limited capacity and scope of ATM information security assurance, which aims to systematically increase the security technologies and measures for information security assurance and form an assurance system for all key equipment, information resources and information systems of the ATM system. However, with the popularization of automation, artificial intelligence, Internet of Things, and other new technologies in the ATM, the characteristics of ATM networked and distributed have become more and more obvious, which are gradually incompatible with the existing rigid and strictly controlled information security assurance architecture. In general, the current ATM information security is often in a passive state, basically following the traditional "patching" mode of "security problems—solve security problems." It is necessary to build an overall networked information security assurance architecture that incorporates the attribute of "security" into the ATM system.

The fourth issue is the existence of bottlenecks in the traditional key technologies of ATM information security assurance. The ATM system is large in scale, involves many applications, has a wide range of users, and has a high degree of business interdependence, and these characteristics of ATM make the key information security assurance technologies for the application of which have higher requirements. The different component solutions of ATM based on

the realization of 4A security are constructed individually, and there is a lack of effective interactions among them, and the different solutions lead to system security dispersion and incompatibility. The system security dispersion and incompatibility caused by different programs cannot adapt to the characteristics of ATM networking, cannot meet the information security guarantee requirements of networked ATM, and cannot adapt to the development needs of ATM's increasingly complex information security situation. From a comprehensive point of view, it is necessary to break through the research bottlenecks in the realization of ATM information security guarantee 4A security functions by introducing new technologies and new concepts, and then build a complete networked ATM system security solution to realize the integration of security protection of different components, ensure the credible identity authentication of ATM business participants, ensure the effective control and traceability audit of the ATM data sharing process, and ensure the credibility, security, and automation of the ATM data access authorization to ultimately ensure the overall security of the ATM system.

C. Integration of ATM and Blockchain

Civil aviation is a technology-intensive industry, and technological innovation is an important mean and aspect for the development of civil aviation industry. Civil aviation-related companies and research institutes have been seeking improvements and breakthroughs in ATM information security research by introducing many new technologies. Compared with relatively mature technologies such as cloud computing and Internet of Things, emerging technologies such as blockchain have also received a lot of attention in recent years. In 2017, French airlines began exploring the use of blockchain technology to track aircraft maintenance workflows [25], and civil aviation companies in the Middle East conducted a pilot study of blockchain for air transportation [26]. In 2018, the Society International Telecommunication Aeronautic (SITA) launched the "Aviation Blockchain Sandbox" to promote the application of blockchain technology in the civil aviation sector, and SITA also pioneered the concept of Smart Path with blockchain technology [27]. In 2019, NASA proposed the application of blockchain technology to the Automatic Dependent Surveillance—Broadcast (ADS-B) system, which uses an open-source licensed blockchain framework to enable privacy and anonymity protection of flight data while providing a secure and efficient method for trusted air traffic services, operational support, or communication with other authorized entities [28]. Concomitantly, the European also established the research project "ATM Operations Improvement Based on Blockchain Technology and Joint Machine Learning Platform with Privacy Protection" to propose a new digital information management concept based on joint machine learning and blockchain to promote the construction and development of the ATM information security assurance system [29]. In China, in 2022, the China Civil Aviation Information Group (CCAIG) held a conference in Beijing, and its independently built blockchain service platform for civil aviation, the "Travel Chain," was officially unveiled [30]. Based on the aviation travel chain, CCAIG has launched "travel pass," "declaration pass," "cross-border pass," and a digital RMB payment platform based on smart contract of blockchain. It attempts to utilize the characteristics of blockchain in data sharing and traceability to help civil aviation participants to upchain the key nodes and data.

Compared with the civil aviation sector, the research results in combining blockchain with civil aviation and ATM in academia appeared relatively about a year later, and the research content is mainly divided into two aspects: research on the general architecture model and research on the application of specific business scenarios. In the field of blockchain architecture design research, the literature [31] and [32] surveyed blockchain-related research and applications for the civil aviation industry, and gave relevant development trends and recommendations for the civil aviation sector. The literature [33] proposed a collaborative blockchain architecture to achieve dynamic information sharing and thus meet the demand of information security assurance for collaborative flight operation. In addition, Ju et al. [34] designed and constructed a model framework for the civil aviation security information sharing problem, which is not much different from the research idea of literature [35]. The literature [36] proposed a blockchain-based security architecture for ticket sales from exploring the new model of air-rail intermodal ticketing. In the study of specific business application scenarios, scholars around the world have made research breakthroughs and achievements in fly data sharing [37], flight data sharing [38], civil aviation seat false occupancy problem solving [39], civil aviation passenger baggage tracking [40], aircraft maintenance task release [41], and flight weather data sharing incentives [42]. The literature [43], [44], [45] combined with blockchain to design security methods for air traffic flow management system, ADS-B system, airport collaborative decision making, and system wide information management, respectively. These results are all in the theoretical research stage and have not advanced to the practical deployment and application stage.

The ATM system is an important support point for the development of civil aviation, and the information security of ATM is an important part of civil aviation security, and the key technology of ATM information security is the focus of civil aviation network security construction. In the application scenario of widely distributed ATM system, it is feasible and meaningful to incorporate the characteristics and advantages of blockchain into the study of ATM information security assurance, reconstruct the existing collaborative management model among ATM departments, and form a "decentralized" ATM with the characteristics of "co-construction, co-sharing, co-management, and co-governance." From a comprehensive point of view, the benefits of combining ATM system with blockchain are at least in three aspects.

1) The number of ATM system participants is increasing, the information interaction mode is becoming more and more complex, and the trustworthiness problem needs to be solved. The timestamp-based "block+chain" data structure of blockchain, which is tamper-proof and traceable, can effectively solve the trust problem among ATM system participants, enhance the trustworthy collaboration among them, and provide an innovative solution to the trustworthiness problem of ATM services.

TABLE III
Comparison of the Research Work in This Article With Typical Schemes

Schemes	[19]	[46]	[5]	ATMChain
Certification	√	√	√	√
Accounting	×	√	×	√
Audit	√	×	×	√
Authorization	√	√	√	√
Centralized/Distributed Architecture	Centralized	Centralized	Distributed	Distributed
Single-function assurance/Systematized assurance	Systematized assurance	Systematized assurance	Single-function assurance	Systematized assurance

2) Blockchain network is decentralized, it is a peer-to-peer distributed network, and its automated consensus account model can be a more perfect match with the widely distributed mesh information interaction model of ATM system. ATM system based on blockchain is more trustworthy, secure and available, and can avoid the potential single point of failure problem of centralized architecture and other security risks.
3) Blockchain-based security authentication method will help improve authentication security and efficiency issues in ATM system; blockchain-based data sharing method will help facilitate data sharing and audit among ATM departments; blockchain-based access control method will help ensure flexible authorization and controlled interaction of ATM data.

In summary, combined with the relevant contents of Table II, here the ATMChain scheme is compared with the typical ATM information security assurance scheme, given in Table III. It can be concluded that ATMChain addresses the realistic needs of ATM information security assurance, incorporates the trustworthy concepts and security advantages of blockchain, and constructs the ATMChain that is compatible with the distributed characteristics of the ATM system, which opens up the complete chain of ATM information security assurance research from model to method. In terms of feasibility, advancement and application prospect, the research work of this article has formed a distributed systematic ATM information security assurance, which is adapted to the increasingly complex ATM information security situation and development trend in the future.

III. ATMCHAIN: SECURITY ARCHITECTURE

Information security assurance of ATM is to systematically add various security technologies and measures on the basis of ATM system to form a security system for each key system equipment, information resources, and information transmission channels of ATM. Many common security technologies have been deployed in current ATM system, such as firewall, intrusion detection, emergency security and emergency response and other conventional security components, etc., but these are not the focus of this article. The focus is to study the trustworthiness, security, and availability of ATM system with an overall ATM information assurance service and system security in mind, and to build a future-oriented ATM security architecture. This part of the research work takes ATM trusted services as the core, integrates ATM system with blockchain mathematical model, builds ATM trusted model (ATMChain) based on blockchain, designs ATMChain security architecture with "endogenous security" features based on ATMChain, and then realizes the trustworthiness of ATM services, the security of trusted services, and the availability of secure services, eventually forming a trusted ecology of the ATM system cyberspace.

A. Construction of ATM Trusted Model

To achieve the vision of global ATM interoperability proposed by ICAO, ATM and its associated portfolio of business applications should meet the diverse needs of ATM users. Ensure that ATM users safely and securely provide and use ATM services globally, which include air traffic control and information processing, etc. Here, an infinite state machine (six-tuple) is used to describe, as in the following:

$$\left(\sum, S_{\mathrm{ATM}}, F, s_{\mathrm{ATM0}}, \Omega, E\right) \tag{1}$$

where $\sum$ is the set of ATM resource devices; S_{ATM} is the set of ATM service applications; F is the set of ATM service characteristics; s_{ATM0} is the initial state of the ATM system; Ω is the state transition function that represents the association relationship between ATM constituent device elements, i.e., $S_{\mathrm{ATM}} \times \sum^{\Omega} \rightarrow S_{\mathrm{ATM}}$; and E is the termination state (null).

The trusted service-oriented ATM system model treats all resources, especially the equipment sensors (e.g., VHF stations, ADS-B stations, and primary and secondary radars, which can be considered as sensors) that enable communication, navigation, surveillance, and automation functions, etc., as part of the ATM system, as in the following:

$$\sum = (C, N, S, A, O) \tag{2}$$

where C is the collection of devices that realize the communication function; N is the collection of devices that realize the navigation function; S is the collection of devices that realize the monitoring function; A is the collection of

devices that realize the system automation function; and O is the collection of devices that realize other auxiliary functions (not further subdivided and defined here).

The mission of ATM is to effectively maintain and promote the safety and security of civil aviation air transportation, maintain air traffic order, and ensure the smooth flow of air traffic. ATM can be divided into three parts from the perspective of business-oriented applications: air traffic services, air traffic flow management, and airspace management, as in the following:

$$S_{\mathrm{ATM}} = (S_{\mathrm{ATS}}, S_{\mathrm{ATFM}}, S_{\mathrm{AM}}) \tag{3}$$

where S_{ATS} indicates air traffic services, ATM units should provide air traffic control services, flight information services, and warning services for aircraft in flight; S_{ATFM} indicates air traffic flow management services, which is to ensure that the maximum use of air traffic control services under the legal and regulatory conditions and the capacity of the services set; S_{AM} indicates airspace management services, which needs to ensure that all types of aircraft in the legal and regulatory flight airspace activities.

ATM is an open network, and its related parties may face interference damage when interacting with information, such as passing malicious information data. In terms of trustworthiness, from the user's perspective, all parties involved in ATM services, whether they are ATM service providers or users, expect effective, guaranteed, controllable, and traceable ATM trustworthiness services. In terms of security, ATM system should be able to meet the functional and performance requirements of its users, but also to achieve active security in terms of confidentiality, integrity, and controllability. In terms of availability, ATM users can autonomously determine whether the entities they interact with are trustworthy, autonomously ensure whether the interactions in the spatial-temporal environment are secure, and autonomously audit whether the obtained ATM data and services meet their requirements. Therefore, ATM services should have the characteristics of trustworthiness, security, and availability, i.e., ATM trusted services should be provided to ATM users in a secure manner, while ATM users can autonomously ensure the availability of the obtained services, which is described using the following:

$$F = (T_{ru}, S_{ec}, A_{va}) \tag{4}$$

where T_{ru} is the trustworthy attribute of ATM service, specifically including environment trustworthiness, subject trustworthiness, data trustworthiness, and behavior trustworthiness; S_{ec} is the security attribute of ATM service, specifically including confidentiality, integrity, controllability, and nonrepudiation; and A_{va} is the available attribute of ATM service, specifically including autonomy to judge, autonomy to ensure, and autonomy to audit.

For networked, information-based ATM, the resource devices are not externally seemingly isolated from each other, but are closely interacting with each other to form a network that adapts to specific ATM services. These networks can represent the association relationships between ATM resource devices as in the following:

$$\Omega = (S_{\mathrm{net}}, A_{\mathrm{net}}, G_{\mathrm{net}}, D_{\mathrm{net}}, O_{\mathrm{net}}) \tag{5}$$

where S_{net} denotes the space navigation and communication network; A_{net} denotes the airborne network; G_{net} denotes the ground computer network; D_{net} denotes the ground-air data link network; and O_{net} denotes other ATM service networks.

Blockchain is a distributed ledger technology with decentralized, tamper-evident, secure and reliable features, which stores a "state" that can be changed by the transactions performed in the blockchain. Referring to (1), it is also described by an infinite state machine (six-tuple), as in the following:

$$(T, B, b, \mathcal{E}, S_{ar}, E) \tag{6}$$

where T denotes the set of transactions in the block; Bdenotes the set of blocks, which are organized in a chain structure to form a blockchain; b is the initial state of the blockchain, i.e., the initial block resulting from the completion of the blockchain construction; $\mathcal{E}$ denotes the state transition function implemented by the consensus algorithm, i.e., $B \times T^{\mathcal{E}} \rightarrow B$; S_{ar} denotes the set of smart contracts in the blockchain; and E is the termination state (empty).

Each transaction in the blockchain contains at least four parts, and the transaction T_i with serial number i in any block can be described by the following:

$$T_i = \left(V_{er}, T_{\mathrm{in}}, T_{\mathrm{out}}, T_{\mathrm{timestamp}}\right) \tag{7}$$

where V_{er} denotes the version number of the transaction; T_{in} denotes the input of the transaction; T_{out} denotes the output of the transaction; and $T_{\mathrm{timestamp}}$ denotes the timestamp of the transaction.

The blocks are linked in chronological order to form a blockchain, and they are chained back and forth. The node participants in the blockchain can trace and locate any data in the block, and the abstract expression of block B_j at moment j is as follows:

$$\begin{aligned} B_j = \mathrm{Hash}([jT_1, jT_2, \ldots, jT_n,] \left|\right| B_{j-1} \left|\right| j) \\ + \left[jT1, jT2, \ldots, jTn\right] \end{aligned} \tag{8}$$

where the transaction with serial number n in block j is denoted as jTn; Hash() denotes the hash algorithm used in the blockchain.

The state transition function E is the consensus mechanism of the blockchain, which is expressed as follows:

$$\mathcal{E} = (\mathrm{PBFT}, \mathrm{Raft}, \mathrm{PoW}, \mathrm{PoS}, \mathrm{DPoS}) \tag{9}$$

where PBFT, Raft, PoW, PoS, DPoS are all consensus algorithms used in blockchain platforms [47]. Since consensus algorithms are not the focus of this article, and there are many research papers introducing blockchain consensus algorithms, we will not explain their meanings one by one here.

A smart contract is essentially a special piece of code, or in many cases a special function, that records and modifies the "state" of the blockchain as an application [11]. There are many smart contracts stored in the blockchain, each of which implements a different function and business, and smart contract k is described as follows:

$$S_{ark} = (R_{ul}, R_{es}, S_{ta}, V_{al}) \tag{10}$$

where R_{ul} denotes the conditions for invoking the smart contract to operate on the blockchain data; R_{es} denotes the processing rules for invoking the smart contract to generate transactions; S_{ta} denotes the state information of the smart

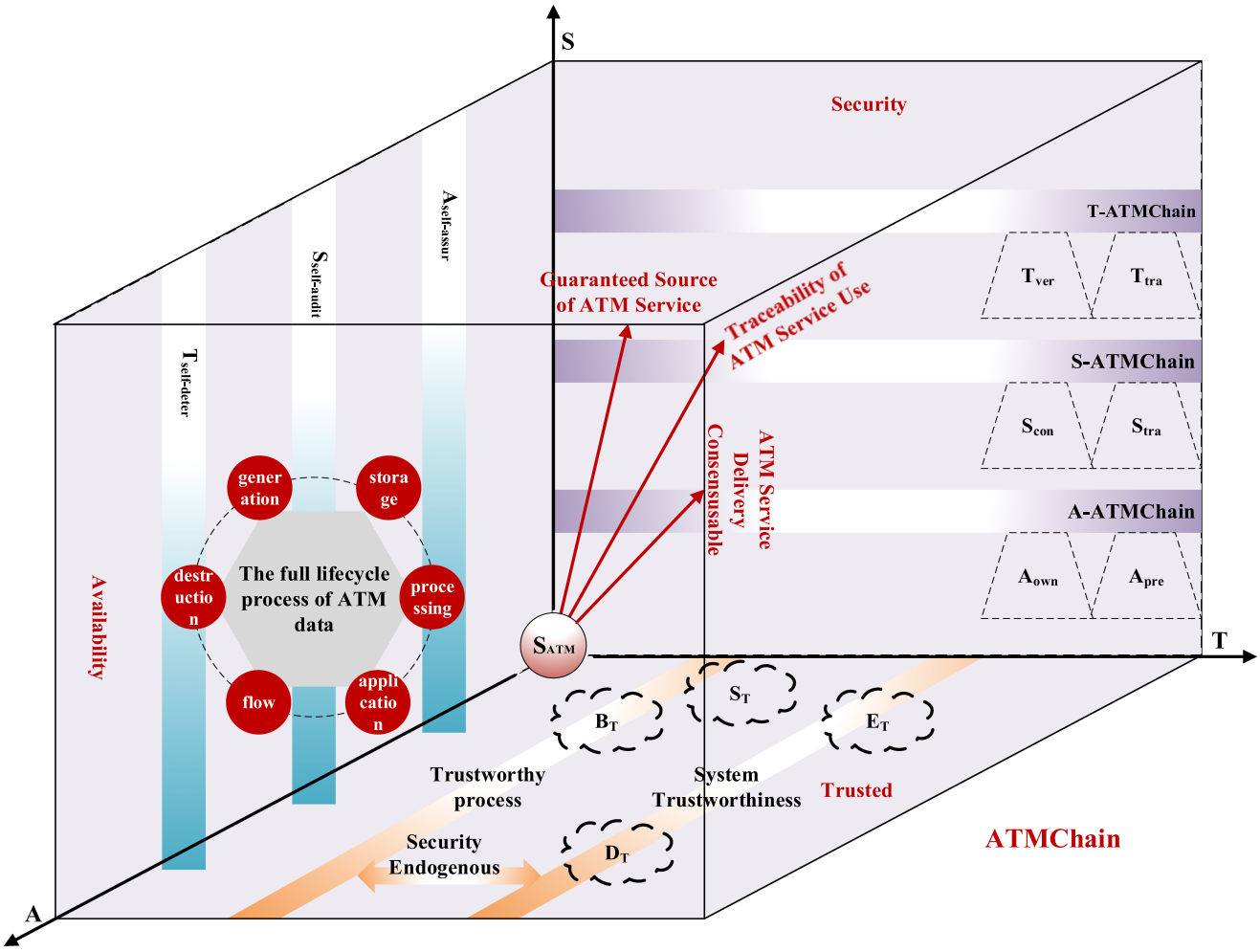


Fig. 4. Trusted model of ATMChain.

contract; and V_{al} denotes the special value saved by the smart contract.

The blockchain-based ATM trustworthy model essentially incorporates the relevant features of blockchain into the ATM system and can be described by the following:

$$\text{ATMChain} = \left(\sum, S_{\text{ATM}}, F, s_{\text{ATM0}}, \Omega, E\right) \times (T, B, b, \varepsilon, S_{ar}, E) \tag{11}$$

where the ATM is deployed with a federated blockchain architecture since most of the participating subjects are organizations; it uses the node access mechanism b to ensure that the nodes involved in ATMChain $\sum$ identity security and trustworthiness; it uses the consensus mechanism $\mathcal{E}$ to enable each ATMChain node to quickly reach agreement on the key ATM data added and updated; it uses smart contracts S_{ar} to automatically execute the security audit and access control functions of relevant ATM services S_{ATM} according to the preset transaction rules; it uses cryptographic algorithms to achieve the sharing and tracing of ATM data flow, service flow, and control flow; it provides trusted, secure, and available ATM service guarantee F for the stable operation of ATM.

The design schematic of ATMChain model is shown in Fig. 4. In this article, it is designed as a "three-dimensional Cartesian product" information security assurance model. In ATMChain, the ATM service S_{ATM} is the origin, and Trusted (T), Security (S), and Availability (A) are its three-dimensional axes, thus realizing the trustworthiness of ATM services, the security of trusted services and the availability of secure services, as in the following:

$$S_{\text{ATM}} \times F = \text{ATMChain}\,(T, S, A) \tag{12}$$

where S_{ATM} and F are the ATM services and their desired attributes defined in (3) and (4).

While audit is often considered part of accounting, there is a subtle difference between the two. Since blockchain is a distributed and monitorable ledger of records, this article describes the two differently, taking into account the difference between accounting and audit. Specifically, in ATMChain, accounting refers to recording the process of ATM service operation and its results, while audit puts more emphasis on monitoring the authenticity and legality of the ATM operation process. Therefore, in ATMChain, the 4A security function is implemented based on blockchain as in the following:

$$\begin{aligned}&\text{Authentication} + (\text{Accounting} + \text{Audit})\\ &+ \text{Authorization} = T - \text{ATMChain}\\ &+ S - \text{ATMChain} + A - \text{ATMChain}\end{aligned}$$

$$= \text{ATMChain}\,(T, S, A) \tag{13}$$

where, $T-$ ATMChain is responsible for implementing the authentication function in ATMChain, and it is the trusted authentication module in Section IV of this article; $S-$ ATMChain is responsible for implementing the account and audit function in ATMChain, and it is the data sharing module in Section IV of this article; $A-$ ATMChain is responsible for implementing the authorization function in ATMChain, and it is the access control module in Section IV.

In (4), the trusted attribute T_{ru} of ATM service is divided into four levels, and ATMChain echoes to achieve the trusted goal of ATM service at four levels, as in the following:

$$T_{ru} \leftarrow (E_T, S_T, D_T, B_T) = \text{ATMChain}\,(T, A) \tag{14}$$

where the decentralized ATMChain architecture will reduce the security pressure on the ATM application server side of the previous centralized architecture, avoid single point of failure, enhance the defense capability of DDoS attack, and create a more trusted ATM network information space environment, thus achieving the environment trusted (E_T) goal of ATM services; the identity and certificate information of ATM entities are managed by T-ATMChain to achieve lightweight security authentication, thus realizing the subject trusted (S_T) goal of ATM services; S-ATMChain uses blockchain to store, manage, and share ATM data to ensure that ATM data is tamper-proof, easily traceable, and auditable, thus meeting the data trusted (D_T) goal of ATM services; A-ATMChain provides flexible and controllable access control based on smart contract in ATM to ensure the secure and controllable management of ATM data and services, thus achieving the behavior trusted (B_T) goal of ATM services.

Meanwhile, the security property S_{ec} in (4) can be expressed as follows:

$$\begin{aligned} S_{ec} \leftarrow\ & (T - \text{ATMChain}(T_{\text{ver}}, T_{\text{tra}}) \\ & S - \text{ATMChain}(S_{\text{con}}, S_{\text{tra}}) \\ & A - \text{ATMChain}(A_{\text{own}}, A_{\text{pre}})) \\ & = \text{ATMChain}\,(T, S) \end{aligned} \tag{15}$$

where, ATMChain's distributed architecture is more reliable and enhances the security of ATM services; T-ATMChain achieves secure and lightweight authentication of ATM entity identities based on blockchain, ensuring that the authenticity of both parties interacting in the ATM environment can be verified (T_{ver}) and the trust relationship can be transmitted (T_{tra}); S-ATMChain uses a cloud-chain convergence architecture to ensure that ATM data sharing can be confirmed (S_{con}) and the data sharing process can be traced (S_{tra}). A-ATMChain applies smart contracts to meet the definition of ATM data ownership (A_{own}) and data leakage prevention (A_{pre}).

The available property A_{va} in (4) can be expressed as follows:

$$\begin{aligned} A_{va} \leftarrow\ & \left(T - \text{ATMChain}(T_{\text{self}-\text{deter}}\right) \\ & S - \text{ATMChain}(S_{\text{self}-\text{audit}}) \\ & A - \text{ATMChain}(A_{\text{self}-\text{assur}})) \\ & = \text{ATMChain}\,(A, S) \end{aligned} \tag{16}$$

where ATMChain is a distributed blockchain network with peer-to-peer nodes, and the full lifecycle (generation, storage, processing, application, flow, and destruction) process of ATM data is secure and transparent, which enhances the availability of ATM services; T-ATMChain enables providers and users of ATM services to autonomously determine ($T_{\text{self}-\text{deter}}$) the trustworthiness of the identity of the adversaries with whom they interact; S-ATMChain enables autonomous tracing and auditing ($S_{\text{self}-\text{audit}}$) of the usage process of ATM service data; A-ATMChain relies on smart contract to control the ATM service data without external influence, and the interacting parties can autonomously ensure ($A_{\text{self}-\text{assur}}$) the authenticity of their services.

In addition, ATMChain logically sets up ATM services with three different types of participants, recorders, verifiers, and regulators, as in the following:

$$\begin{aligned} \text{ATMChain} = & (P_{\text{rec}}, P_{\text{ver}}, P_{\text{sup}}) \\ & \times (T, B, b, \mathcal{E}, S_{ar}, E) \end{aligned} \tag{17}$$

where the participant of record type (P_{rec}) will apply for block-entry rights and record relevant ATM service data (such as flight and weather information), and can authorize or revoke access to the data; the participant of verification type (P_{ver}) needs to verify the data blocks generated by the recorder; the participant of supervision type (P_{sup}) has the right to view and audit the block data in accordance with the law and regulations. The three types of ATMChain participants do not correspond to each other in the objective world of ATM, but each of them will jointly build, maintain, and mutually verify and supervise the operation of the entire ATMChain blockchain. In other words, any ATM service participant in ATMChain can have the functions of recording, verifying, and supervising at the same time in different situations.

In summary, the ATM trusted model ATMChain empowers ATM information security assurance with "trust" and promotes trusted service collaboration among ATM departments, ATM data security sharing and privacy protection. In turn, it has formed a trust network, data network, and regulatory network for ATM information security assurance, in which technology is integrated into management, regulation is penetrated into management, and security is given to management.

1) Trust Network—Guaranteed Source of ATM Service ATMChain architecture makes ATM services change from weak trust to strong trust, and the transparent and traceable tamper-proof ATM service collaboration model greatly increases the attack cost of potential saboteurs inside and outside the system. Combined with lightweight security authentication, flexible and controllable authorization mechanism, and secure and available data sharing mechanism, the problem of information silos in ATM services is alleviated, and a trust network in ATM business ecology takes shape.

2) Data Network—Consensusablility of ATM Service Delivery Blockchain, as a trusted linker, interconnects data processing and storage centers built by regional ATM bureaus, airlines, airports, and other relevant ATM service assurance units in a decentralized manner by building a common governance ATMChain blockchain platform, while each participant confirms and protects their respective data, thus sharing data in a secure and controlled

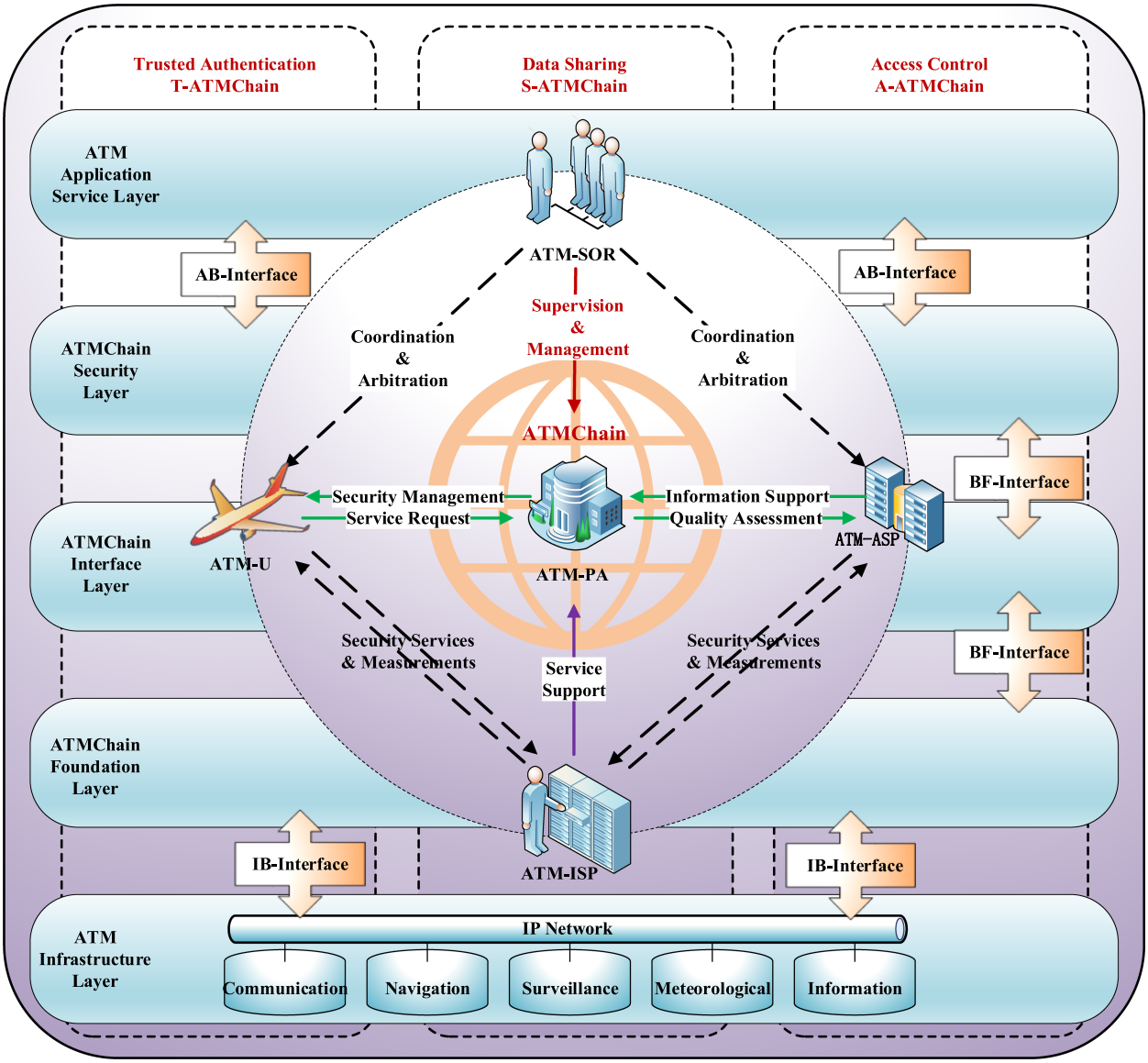


Fig. 5. Security architecture of ATMChain.

manner, and laying a data foundation for ATM business collaboration and innovation.

3) Supervisory Network—Traceability of ATM Service Use ATM is a field that focuses on security and supervision. We build a supervisory network for trust network and data network to ensure trustworthy ATM and trustworthy ATM service process, and resolve the problem of untimely, insufficient, and inadequate supervision of existing ATM operation through the whole life cycle control of ATM data flow, and then complete the efficient and comprehensive supervision of ATM application services (such as control services, traffic management, airspace management, flight planning, airline operation and maintenance, airport field management, airport operation management, etc.).

B. Construction of ATMChain Security Architecture

The ATMChain security architecture is built based on the ATMChain model described in the previous section, as shown in Fig. 5, which includes five types of ATM logical entities, three security function modules, five ATM capability layers, and three types of interface components. The ATMChain security architecture is designed and deployed to satisfy three security assumptions, which are as follows:

1) the ATMChain security architecture is trusted at the beginning of its establishment, and its ATM participating nodes are trusted when they join the network;
2) the cryptographic algorithm underlying the architecture is secure, both the hash algorithm and the key cannot be analyzed and breached, and the communication channel can be secured by encryption measures;
3) a potential ATM saboteurs can eavesdrop, intercept, and tamper with communication interactions between ATM participating entities, but they cannot control more than 1/3 of ATM entity nodes in

ATMChain, 1/3 of which is determined by the consensus algorithm used in ATMChain's underlying blockchain platform fabric [48].

In ATMChain, all ATM-related participants are divided into five types of logical entities, which can perform any of the role functions in (17). The five ATM logical entities are as follows:

1) ATM application service provider (e.g., air traffic authority, national timing center, meteorological center, etc., or *ATM-ASP*);
2) ATM service user (user of various civil transportation services, or *ATM-U*);
3) ATM service platform administrator (international or regional organization, e.g., ICAO, or *ATM-PA*);
4) ATM infrastructure service providers (e.g., telecommunication operators, civil aircraft manufacturers, computing storage service providers for clouds, etc., abbreviated as *ATM-ISP*);
5) ATM security operation regulators (e.g., national or regional civil aviation administrations, etc., abbreviated as *ATM-SOR*).

The interaction and functions of the five ATM logical entities can be described in five specific ways as follows:

1) *ATM-ASP* provides trusted ATM management and control services to *ATM-U*, and must ensure that these services are accurate and effective, timely updated, secure and reliable;
2) *ATM-U* obtains and uses ATM services within the scope of authorization;
3) *ATM-PA* is responsible for building, administering, and operating ATMChain security service architecture to provide security support services for ATM services;
4) *ATM-ISP* provides ATM service security, ATM data computation storage, and privacy protection of ATM-related communications for *ATM-ASP*, *ATM-U*, and *ATM-PA*;
5) *ATM-SOR* monitors and supervises the ATM business activities of the remaining four types of ATMChain logical subjects in accordance with national or regional legal policies and is responsible for coordinating and resolving business conflicts between them.

In addition, this article further divides the ATMChain security architecture into five ATM capability layers, which are ATM infrastructure layer, ATMChain foundation layer, ATMChain interface layer, ATMChain security layer, and ATM application service layer.

First, the ATM infrastructure layer includes various ATM terminal edge devices and data computing storage facilities, which form the various ATM service networks as described in (5). It is the foundation of ATMChain security architecture, and this layer is indistinguishable from the current ATM infrastructure layer. Specifically, this layer is responsible for collecting and storing ATM basic service support data and information, such as communication, navigation, surveillance, meteorological, and intelligence data, and interacting with each of the other ATM capability layers through the network connectivity communication technology IP network.

Second, the ATMChain foundation layer covers key blockchain technologies, such as cryptographic algorithm, consensus mechanism, and smart contract. The main function of this layer is to bind the traditional ATM infrastructure services and data to the blockchain, giving ATM services the blockchain security features of trustworthiness, traceability, and tamper-proof. As mentioned earlier, there are multiple virtual logical entities in the ATMChain security architecture, and the ATMChain interface layer defines three types of interaction interfaces to meet the communication and interoperability needs among ATM entities. Specifically, the IB-interface (infrastructure-blockchain interface) is responsible for data interaction between the ATM infrastructure layer and the ATMChain blockchain layer, mainly including data upload interface and data download interface, etc.; the BF-interface (blockchain-foundation interface) is used for the implementation of common functions of blockchain, such as smart contract class interface, event class interface and state class interface, etc.; the AB-interface (application-blockchain interface) is used to implement ATM application service calls in ATMChain security architecture, including trusted authentication class interface, data sharing class interface, and access control class interface. These three types of interfaces among the various ATM capability layers require specific protocols to implement, which is not the focus of this article and will not be discussed in detail here.

Third, for the ATMChain security layer, it covers three blockchain-based security function modules, that is, trusted authentication (abbreviated as T-ATMChain), data sharing (abbreviated as S-ATMChain), and access control (abbreviated as A-ATMChain), which will be described in the next section.

Finally, the ATM application service layer is not fundamentally different from the current ATM business application system and mainly provides ATM users with services such as airspace management, control services, scenario services, flight plan management, airline operation, and maintenance monitoring.

C. Operation Flow of ATMChain

The operation process of ATMChain security architecture includes two phases, which are system initialization phase and ATM information security assurance operation phase.

1) *System Initialization Phase:* The ATMChain requires basic initialization operations before it can run, mainly including the initialization of the ATM trusted environment and the initialization of the three blockchain-based security function modules

1) $\text{ATMChain}_{\text{net}} = \begin{Bmatrix} P_{\text{rec1}}, P_{\text{rec2}}, \ldots, P_{\text{rec}n}, \\ P_{\text{ver1}}, P_{\text{ver2}}, \ldots, P_{\text{ver}m}, \\ P_{\text{sup1}}, P_{\text{sup2}}, \ldots, P_{\text{sup}k} \end{Bmatrix}$ where $\text{ATMChain}_{\text{net}}$ is the set of all trusted ATM nodes in the ATMChain architecture, with the total number of nodes being $(n+m+k)$. At this point, the trusted ATM nodes establish the initial trusted environment.
2) $T-\text{ATMChain}_{\text{net}} = \{TP_1, TP_2, \ldots, TP_{n1}\}$: where $T-\text{ATMChain}_{\text{net}}$ is a collection of trusted authentication federation blockchain network nodes with the number of nodes $n1$. At this point, T-ATMChain is initialized and relevant functional nodes join to

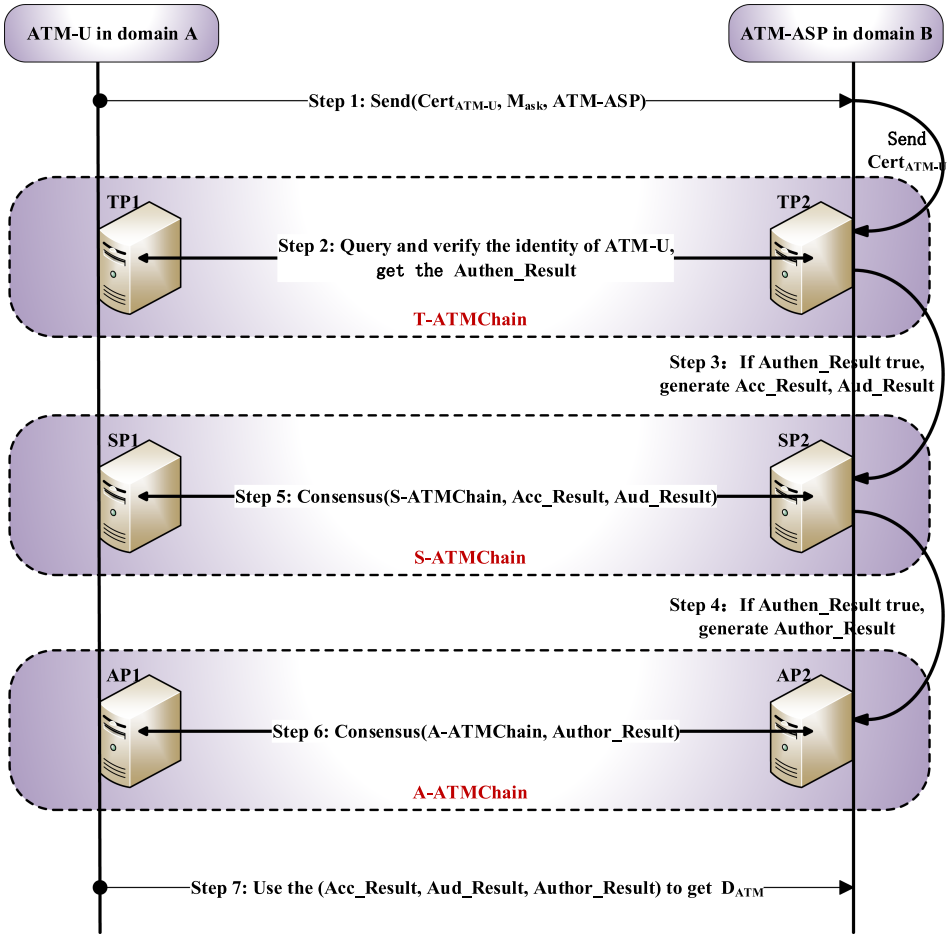


Fig. 6. ATMChain operation flow.

provide trusted authentication services for the entire ATMChain environment.

3) $S-\text{ATMChain}_{\text{net}} = \{SP_1, SP_2, \ldots, SP_{n2}\}$: where $S-\text{ATMChain}_{\text{net}}$ is a collection of data sharing federation blockchain network nodes with $n2$. At this point, S-ATMChain is initialized and relevant functional nodes join to provide account and audit services for the data sharing process of air management logical entities in ATMChain.

4) $A-\text{ATMChain}_{\text{net}} = \{AP_1, AP_2, \ldots, AP_{n3}\}$: where $A-\text{ATMChain}_{\text{net}}$ is a collection of access control federation blockchain network nodes with $n3$. At this point, A-ATMChain is initialized and relevant functional nodes join to provide authorization services for ATM data resource access in ATMChain.

2) *ATM Information Security Assurance Operation Phase:* After ATMChain is initialized and in normal operation, there is an *ATM-U* in domain *A* requesting access to the ATM data resources of an *ATM-ASP* in domain *B*, as shown in Fig. 6.

1) Send($T-\text{Cert}_{\text{ATM}-\text{U}}, M_{\text{ask}}, \text{ATM}-\text{ASP}$): ATM-U sends a message to ATM-ASP, where $T-\text{Cert}_{\text{ATM}-\text{U}}$ is ATM-U's digital identity certificate and M_{ask} is ATM-U's ATM data resource request message.

2) $\text{ATM}-\text{ASP} \rightarrow TP_2 \rightarrow TP_1$ $\begin{pmatrix} T-\text{ATMChain}, \\ T-\text{Cert}_{\text{ATM}-\text{U}}, \\ \text{Authen\_Result} \end{pmatrix}$: After receiving the ATM data request message, the ATM-ASP sends a $T-\text{Cert}_{\text{ATM}-\text{U}}$ to the TP_2 node of its identity management domain to verify the identity of the ATM-U. TP_2 queries the trusted authentication record reached with the TP_1 node of the identity management domain to which the ATM-U belongs to verify the identity of the ATM-U. If the verification is legitimate and the Authen_Result is true, the next step is performed; otherwise, the ATM-U access request is denied.

3) $\text{ATM}-\text{ASP} \rightarrow SP_2$ $\begin{pmatrix} S-\text{ATMChain}, M_{\text{ask}}, D_{\text{ATM}}, \\ \text{Acc\_Result}, \text{Aud\_Result} \end{pmatrix}$: ATM-ASP performs the operation of the relevant ATM data D_{ATM} share on its blockchain deployment node SP_2 of the data sharing domain, generating the corresponding ATM data sharing log Acc_Result and audit result Aud_Result.

4) $\text{ATM}-\text{ASP} \rightarrow AP_2 \begin{pmatrix} A-\text{ATMChain}, M_{\text{ask}}, \\ D_{\text{ATM}}, \text{Author\_Result} \end{pmatrix}$: ATM-ASP generates the corresponding access control policy and access control log Author_Result

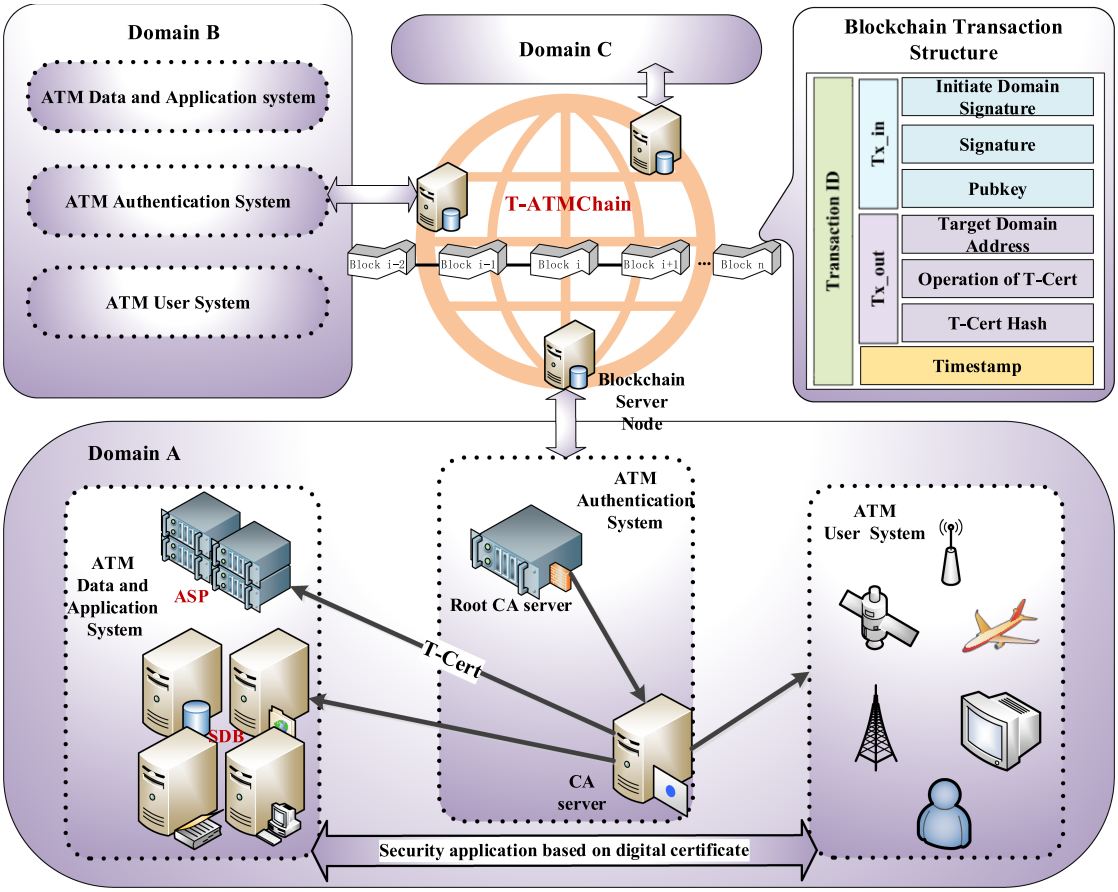


Fig. 7. T-ATMChain trusted authentication module.

on the blockchain deployment node AP_2 of the access control domain it belongs to.

5) $SP_2 \rightarrow SP_1$ then Consensus $\left(\begin{array}{l} S-\text{ATMChain}, \\ \text{Acc\_Result}, \\ \text{Aud\_Result} \end{array}\right)$:
SP_2 and SP_1 reach consensus on Acc_Result, Aud_Result.

6) $AP_2 \rightarrow AP_1$ then Consensus $\left(\begin{array}{l} A-\text{ATMChain}, \\ \text{Author\_Result} \end{array}\right)$:
AP_2 and AP_1 reach consensus on Author_Result.

7) Receive$\left(\begin{array}{l} \text{Acc_Result}, \\ \text{Aud_Result}, \\ \text{Author_Result} \end{array}\right) \rightarrow D_{\text{ATM}}$: ATM-U queries Acc_Result, Aud_Result, Author_Result on SP_1 and AP_1, and finally gets D_{ATM}.

IV. SECURITY FUNCTION MODULES OF ATMCHAIN

In this article, we combine blockchain with 4A security assurance concept, and design three security modules based on ATMChain security architecture, namely trusted authentication, data sharing, and access control. The first security module implements the authentication function of 4A security, the second security module implements the accounting and audit function of 4A security, and the third security module implements the authorization function of 4A security.

A. Trusted Authentication Module—T-ATMChain

Authentication is an indispensable and fundamental security module in every computer network system. However, the current PKI/CA (public key infrastructure/certificate authority) authentication model widely used in ATM suffers from the problem of difficult certificate path construction. Therefore, this article designs an authentication method T-ATMChain with distributed features based on the overall architecture of ATMChain. As shown in Fig. 7, ATM is divided into different authentication domains according to different services or geographic areas, and each authentication domain has three subsystems: authentication, data application, and ATM user system. The authentication subsystem includes RCA/CA servers; the data application subsystem includes SDB (shared database) and ASP (application service provider) servers; and the ATM user subsystem includes various ATM terminal sensors and devices. The authentication subsystem is responsible for issuing device certificates and user certificates. In this way, the authentication security of ATM users accessing the SDB/ASP servers is ensured. T-ATMChain is the trust-building mechanism in this ATMChain, which is built from multiple ATM authentication domains. The intradomain authentication structure and trust logic of each authentication domain retains the current traditional PKI/CA architecture. The trust between authentication domains relies on the trustworthiness of the ATMChain blockchain. Trust

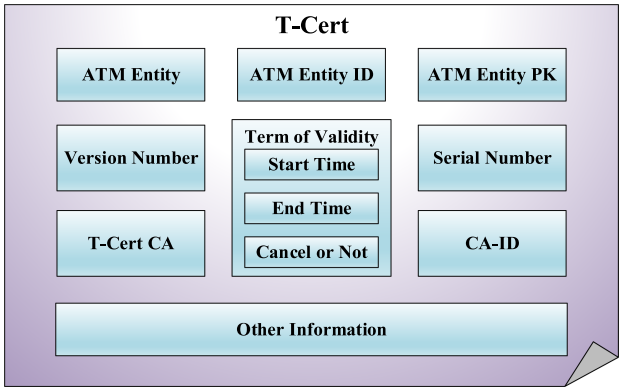


Fig. 8 T-Cert structure.

construction between authentication domains is achieved by the RCAs of each authentication domain issuing trusted certificates to each other. In other words, in T-ATMChain, for the RCA of domain A to build a trust relationship with domain B, it is only necessary to treat the domain B RCA as a user to issue a trusted certificate for it. The root CA of each authentication domain joins the blockchain network as the node of T-ATMChain, constitutes the trusted authentication channel of ATMChain, and realizes the trusted authentication function of ATMChain.

In the design of the T-ATMChain trusted authentication module, the management of the entire life cycle of the trusted authentication digital certificate (T-Cert) and the management of the trust relationship between authentication domains is achieved by assembling the T-Cert of each ATM logical entity into the blockchain transaction. The format and content of the T-Cert digital certificate are shown in Fig. 8. Compared with the X.509 certificate generated by the PKI/CA authentication system, the T-Cert digital certificate does not have a signature and signature algorithm module. In addition, there is no certificate revocation checking service, uniform resource locator module in the structure of T-Cert digital certificates, so there can be no T-Cert certificate revocation checking within each ATM authentication domain. Unlike X.509 certificates, T-Cert adds term of validity module, which records the validity period of T-Cert certificates and information on whether they have been revoked. When a T-Cert is revoked or expired, the cancel or not in the term of validity module will be marked as yes, and this process will be recorded in T-ATMChain. At this time, when the T-CertH of the T-Cert is retrieved again, its revocation or expiration record will be retrieved. The PKI authentication method of ATM ensures that the binding of the identity of the digital certificate holder and the public key is real and trustworthy by using digital signatures, and makes the digital certificates forgery-proof, so that it can be judged whether the certificate has been tampered with or not. In T-ATMChain, only the T-Cert of the ATM entity access requestor is hashed to generate T-CertH (T-Cert Hash), which is consistently compared with the corresponding T-CertH stored on the complete authentication node of T-ATMChain, and the trusted identity authentication of ATM users can be completed.

The blockchain transaction structure in T-ATMChain consists of ten elements (see Fig. 8). The RCA of each ATM authentication domain, i.e., the full blockchain server node that records all authentication information, encapsulates the output of all transactions in T-ATMChain into a special key-value pair data structure. They are stored independently in a dataset called T-CertH-Set, which is implemented by the Fabric state database, similar to Bitcoin's UTXO design [49]. When performing intradomain authentication, the CA node of the ATM authentication domain will hash the T-Cert of the authentication requestor to generate the T-CertH and retrieve the T-CertH in the T-CertH-Set to determine whether the authentication is passed or not; when performing cross-domain authentication, the operation is similar. The only different operation in cross-domain authentication is that the T-CertH of both the authentication requestor and the RCA of the authentication domain to which it belongs needs to be verified. It is worth noting that when a T-Cert is revoked or expires, a transaction such as $Tx(Tx\_\text{in}, Tx\_\text{out}(\text{targetdomainaddress}, 0, \text{T} - \text{CertH}))$ will be created and recorded on the T-ATMChain. Setting the operation type of a T-Cert certificate transaction to 0 means that the T-Cert is revoked or expired. Afterward, the invalid or expired T-CertH will be removed from the T-CertH-Set, which is dynamically changing and is potentially increasing or decreasing compared to the expanding block data of T-ATMChain.

B. Data Sharing Module - S-ATMChain

Due to the lack of trust mechanism, a separate database is required for each ATM department in each region or business domain. However, data discrepancies easily occur among the many databases, which is not conducive to ATM data sharing, traceability and audit. Considering the current situation that most of the ATM data sharing and storage use cloud platforms, this article designs an ATM data sharing method based on ATMChain, S-ATMChain, as shown in Fig. 9, which is divided into two main steps: 1) ATM data up-chain; and 2) ATM data acquisition.

1) *Process of ATM Data Upchain:* When ATM data are uploaded/updated to the cloud (where ATM-ISP provides related services), ATM-ASP signs the ATM data after hashing it. ATM-ISP verifies the ATM-ASP identity and ATM data, then generates $Data_{addr}$, the ATM data storage address in the cloud, and returns it to ATM-ASP. ATM-ASP receives $Data_{addr}$ and sends (ATM-ASP_ID, $Data_{addr}$) to ATM-PA, where ATM-ASP_ID is the identity label of ATM-ASP. Subsequently, the ATM-PA generates ATM data upchain transactions (*Trans_ID* is its transaction number) after broadcasting and consensus in S-ATMChain, assembles the *Key (ATM-ASP_ID, Trans_ID)* and stores the key-value pair *(Key,* $Data_{addr}$*)* in the state database of S-ATMChain for query retrieval. The *(Key, Value)* is also returned to *ATM-ASP*. In this process, a data distribution smart contract (*DD-SC*) is called to "anchor" the ATM data on the blockchain. *DD-SC* contains three smart contract functions, *Verify_TCert()*, *Write_load()*, and *Return_metadata()*: *Verify_TCert()* is responsible for the trusted authentication of *ATM-ASP* identity, which can be implemented by T-ATMChain security module; after passing the authentication, *DD-SC* will execute *Write_load()* to package *(Trans_ID, ATM-ASP_ID,* $Data_{addr}$*)* into a transaction and broadcast it in the federated blockchain; when the transaction is consensus, *DD-SC* will execute

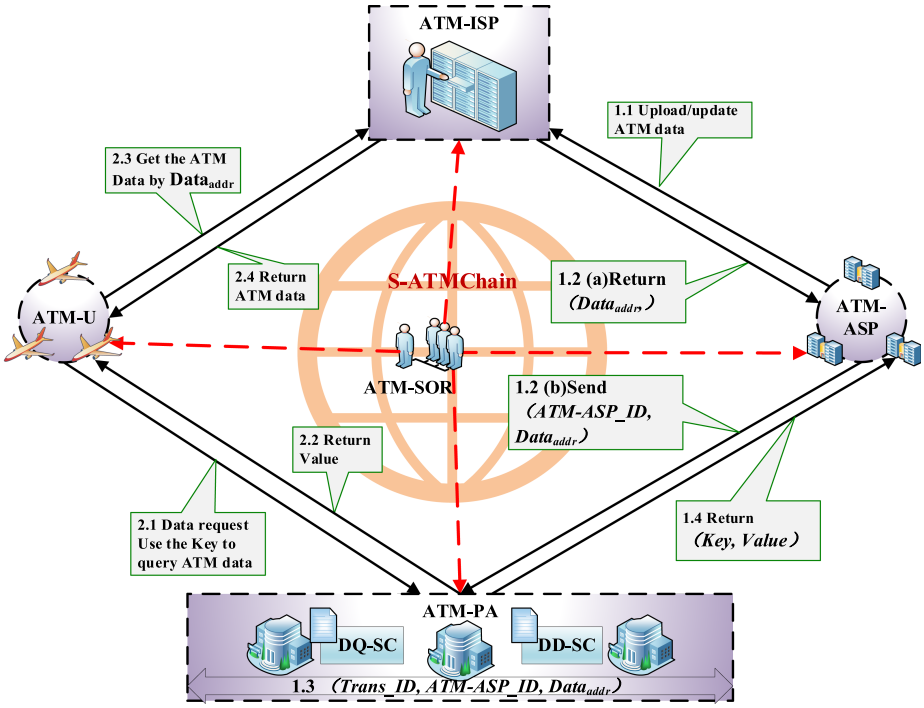


Fig. 9. S-ATMChain data sharing module.

Return_metadata() to generate *(Key, Value)* to return to *ATM-ASP*.

2) *Process of ATM Data Acquisition:* The *ATM-U* initiates a data request to the *ATM-ASP* and uses the returned *Key* to retrieve the required ATM data on the *ATM-PA*. After verifying that the relevant access control conditions are met (this step can be implemented by the A-ATMChain security module), the *ATM-PA* returns the *Value* to the *ATM-U*. The *ATM-U* parses the $Data_{addr}$ and obtains the required ATM data on the *ATM-ISP*. In this process, the data query smart contract (*DQ-SC*) needs to be called to obtain the ATM data storage address in the cloud. *DQ-SC* contains three smart contract functions, *Verify_TCert()*, *Query_key()*, and *Return_value()*: *Verify_ TCert()* is to authenticate the identity of *ATM-U* trustworthily; after the authentication is passed, *Query_key()* is responsible for querying the *Value* corresponding to the *Key* in the state database and broadcasting this query information as a transaction to the blockchain; after the consensus is completed, *Return_value()* returns the *Value* to *ATM-U*.

The root causes of poor ATM data sharing are summarized in three points: first, ATM departments are "unwilling" to share the data under their control for fear of losing control of the data; second, due to the sensitivity of ATM data, ATM departments often "dare not" to share their data; and third, ATM users "would not" use the ATM data shared by other departments, which they cannot effectively judge whether it is available or not. To address the problems of "unwillingness," " dare not," and " won't" in ATM data sharing, S-ATMChain utilizes the blockchain distributed architecture to alleviate the worries of ATM departments about losing data control and dominance, and confirms the rights of ATM data, making ATM departments "willing" to share data; it utilizes the cryptography technology and its traceability features in the blockchain to complete the privacy protection and security flow audit of ATM data, which makes the ATM department "dare" to share the data; it utilizes the blockchain to realize the usable validation of ATM data after sharing, which makes the ATM users "happy" to use the ATM data of other departments.

C. Access Control Module—A-ATMChain

With the development of ATM network informatization, the ATM involves more complex and diverse devices, and the user community becomes gradually larger, so the problem of illegal and noncompliant access to information becomes increasingly serious. While current ATM have installed firewalls and intrusion detection systems to prevent illegal end-user access to a certain extent, the traditional access control methods used to address problems such as overauthorization and underauthorization are ineffective. Attribute-based access control (ABAC) takes the attributes of the subject and object as the basic decision elements, and the attributes are inherent to the subject and object [50]. It is easy to manage. Therefore, ABAC is suitable for ATM system with a large number of nodes and many data types. In this article, we combine ABAC and ATMChain to design the A-ATMChain access control module to ensure that the data resources in ATM are used within the scope of legal compliance and to achieve data privacy protection.

In ABAC, it mainly consists of five core components: policy enforcement point (PEP), attribute authority (AA), point administration point (PAP), policy decision point (PDP), and policy information point (PIP). As shown in Fig. 10, AA is replaced by ATMChain, and the attribute information is stored in ATMChain to ensure the authenticity of the attribute information; PAP, PDP, and PIP are replaced by PAP smart contract, PDP smart contract, and

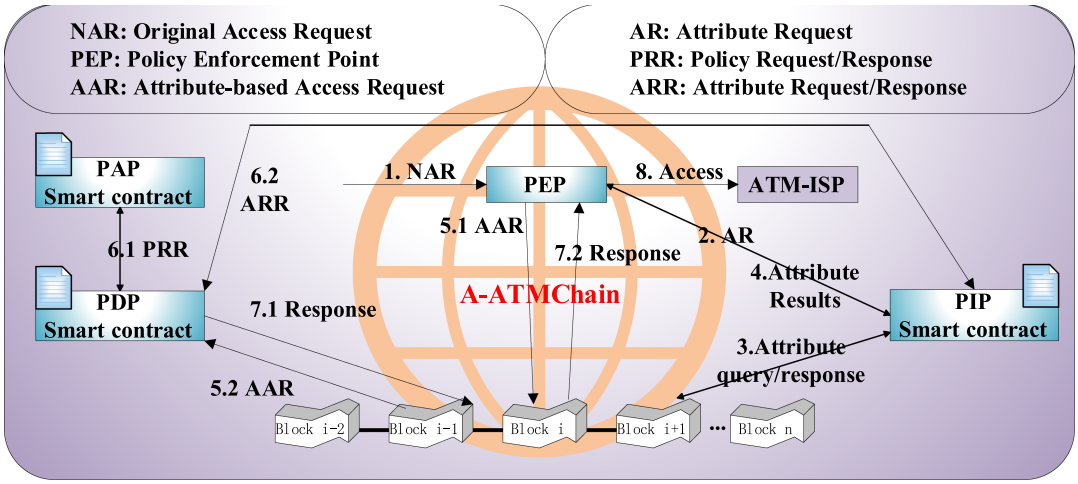


Fig. 10. A-ATMChain access control module.

PIP smart contract, respectively, and the smart contracts are stored in ATMChain. The participants in ATMChain can invoke the smart contracts to achieve the corresponding functions; the cross-domain nodes of each ATM business security domain act as PEP to receive access requests and execute the policy determination results. Specifically, PEP receives the access request NAR and then invokes the PIP smart contract to query the relevant attribute information stored in A-ATMChain based on the NAR, which is used to construct the attribute-based access request (AAR). After receiving the AAR, the resource owning domain invokes the PDP smart contract. Subsequently, the PDP smart contract invokes the PAP smart contract to obtain the policy set and the PIP smart contract to obtain the attribute information, which in turn determines the AAR and encapsulates the determination result as a response transaction to be broadcast and consensus through A-ATMChain. PEP receives the response transaction and executes the access control result, and if it passes, the ATM user can come to access the resource from *ATM-ISP*.

A-ATMChain effectively solves the demand difficulty of ATM data access control. First, the access control information on A-ATMChain is public, the ownership of ATM data resources is clear, the access behavior of ATM users will be recorded in the whole process, and combined with the blockchain's timestamp and signature information, violations such as overstepping the authority to access and leakage of data can be traced back and discovered in a timely manner. Second, the access control policies and permissions on A-ATMChain are trustworthy and verifiable, and there is no need for third-party endorsement by the two parties in communication. And the consensus attributes and policies are stored on the blockchain that are difficult to be tampered with, so that malicious attackers will not be able to carry out targeted tampering and deletion, which simplifies the process of ATM data authority management, provides security guarantee and reduces the cost of trust. Third, A-ATMChain's authorization decision-making power is decentralized in each node of the alliance chain, which enhances the reliability of the whole access control system and avoids the potential hidden danger of targeted attacks in the "centralized" access control model. Finally, A-ATMChain completes the core steps of ABAC with smart contract agents, realizing automated adjudication of access control policies, eliminating manual intervention, and reducing the difficulty of adjudication of access control.

V. ANALYSIS AND EVALUATION

This section provides a comprehensive analysis of ATMChain and tests its three security function modules.

A. Comprehensive Analysis

From the construction of ATM trusted model ATMChain to the ATM information security architecture designed based on ATMChain, this article always focuses on the realization of ATM trusted services as the core, around the three basic footholds of trustworthiness, security, and availability to carry out research. ATMChain integrates the trustworthiness and security features of blockchain for the real demand of ATM information security assurance, and reconstructs the 4A security function based on blockchain to finally achieve the goals of trustworthy ATM service, trustworthy service security, and secure service availability. The following is an overall analysis of ATMChain solution from three aspects: system trustworthiness analysis, system security analysis, and system availability analysis.

1) *Analysis of System Trustworthiness:* As a trust-creating machine, the trustworthiness of blockchain is mainly reflected in four aspects: distributed trust, traceability, tamper-proof, and resistance to collusion attacks, and the system trustworthiness analysis of blockchain-based ATMChain will also be carried out from these four aspects.

First, ATMChain implements distributed trust construction in ATM. In a widely distributed ATM environment, the participants of each ATM service will join ATMChain as nodes. On the basis of ensuring the security of ATM network operation, the unique consensus mode of blockchain transforms the traditional centralized trust into distributed trust for all trusted nodes in ATMChain, which in turn enables all ATM nodes to provide and use services, share and exchange data in a secure and trustworthy manner by building distributed trusted security authentication, distributed trusted data sharing, and distributed trusted authorization access.

At the same time, a regulator is introduced to supervise and control the whole process of ATM services, forming three mutually constrained and interdependent ATM trust network, ATM data network, and ATM supervision network, thus completing the construction of a trustworthy ecology for ATM information security.

Second, ATMChain enables traceability of ATM services. The trustworthiness of blockchain comes from the trusted arguments of mathematics and cryptography, which ensures the correct ownership of data on the blockchain and the trustworthiness of data. Attacks by malicious nodes are often accompanied by malicious behavior, and trusted behavioral audits can expose discover malicious behavior and thus malicious nodes. Figuratively, the blockchain is a storage structure linked by hashes, and once ATM service data are written to the blockchain, it can be traced back to the corresponding ATM service history along the blockchain.

Again, ATMChain achieves tamper-evident ATM services. Immutability is an important feature of blockchain that can be used to build a distributed trust network, which is guaranteed by the blockchain's data structure Merkle tree and the corresponding algorithm [51]. If a malicious attacker tampers with the ATM service data of a block in ATMChain, then the hash value of that block will change. In turn, the attacker would need to control most of the nodes in the ATMChain network in order to tamper with all subsequent blocks of that block, at which point the attack would take effect. But this process is impossible to achieve.

Finally, ATMChain is resistant to collusion attacks [52]. A collusion attack is an attack in which multiple malicious nodes collude with each other, guarantee each other, forge each other, and perjure each other to disrupt normal network behavior. In ATMChain, authentication, account, audit, and authorization are all distributed and decentralized, while collusion attacks must forge a large number of identities and control a large number of nodes, which is extremely difficult. At the meantime, the trustworthiness of blockchain also depends on the research results of game theory, economics and psychology. All parties involved in blockchain must cooperate with each other in good faith in order to maximize the overall benefit, and collusion attacks are, from another side, undermining the interests of the colluders themselves.

2) *Analysis of System Security:* With blockchain as the underlying technical support for ATM information security assurance, ATMChain inherits the security attributes of blockchain in many ways. Unlike traditional security assurance technologies and measures, the security attributes of ATMChain are endogenous. Endogenous security [53] is a new idea of network security construction, and the concept opposite to endogenous security is exogenous security. For ATM, the fundamental goal of ATM endogenous security is to secure trusted ATM services in all aspects, rather than simply securing ATM computer systems and equipment.

First of all, ATMChain is designed with the characteristics of ATM and its information security assurance needs, and security is an organic component of ATMChain. Synchronous planning is the key and starting point of ATMChain's endogenous security. Based on the realization of trusted ATM services, security is deeply integrated with ATM services to form a full coverage of ATM service process security assurance. Synchronized construction is the landing and guarantee of ATMChain endogenous security, combining 4A security capabilities with ATM services to form an intrinsic security mechanism for ATM information security assurance in three aspects: trusted authentication, data sharing, and access control. Synchronized operation is the lifeline of ATMChain's endogenous security. Based on the three networks of trust network, data network, and supervisory network, the three-core management and operation objectives of ATM service source assurance, ATM service delivery consensus and ATM service usage traceability are realized. By integrating security technology into the "human," "machine," "environment," and "management" of ATM, ATMChain achieves regulatory penetration management and gives management a security connotation, thus enabling the effective output of systematic security capabilities.

Next, ATMChain fulfills the "trusted enhancement" requirement of ATM endogenous security. The core idea of "trustworthy enhancement" is to establish a trust chain from the source to ensure the security and integrity of the system [54]. Combined with the aforementioned analysis of system trustworthiness and the description of (14), ATMChain enhances the trustworthiness of ATM system and ATM services in four aspects: environment trustworthiness, subject trustworthiness, behavior trustworthiness, and data trustworthiness, which reduces the possibility of malicious behavior from the source.

Lastly, ATMChain meets the "smart consensus" requirement of ATM endogenous security. "Smart consensus" refers to the distributed node architecture [55], in which multinode consensus is used to exclude external interference and provide more effective security for information and data [56]. ATMChain is mainly reflected in three levels: ATMChain consensual mechanism can ensure the consistency of ATM service data; ATMChain's underlying cryptography technology can provide better security for distributed ATM network; ATMChain's smart contract-based data sharing and access control can effectively ensure the up-chain of ATM data value and promote the controlled flow of ATM data.

In summary, ATMChain based on blockchain is more secure than current ATM information security solutions. ATMChain avoids the potential single point of failure and other security risks of centralized architecture, realizes a revolution from the bottom of the security infrastructure, reconstructs a new security ecology, and abandons the ineffective cycle of tinkering with the old structure, which is the endogenous value of ATMChain's security.

3) *Analysis of System Availability:* The introduction of blockchain will undoubtedly increase the operational cost and overhead of information security assurance of current ATM system, but ATMChain enables ATM to gain greater security, and the enhanced security can avoid greater possible economic loss due to potential security threats and attacks, so a certain blockchain cost overhead is inevitable and worthwhile. In order to describe it visually, this paper constructs an application scenario to analyze the availability of ATMChain.

a) *Application scenario:* Take China's ATM as an example, it consists of seven regional ATM administrations, each of which is under the jurisdiction of several ATM branch offices, and each ATM branch office contains different ATM

business departments, each of which has several computer terminals, and there are ATM data servers of different sizes in each ATM branch office. First, it is assumed here that each regional ATM bureau has 10 ATM branch offices, each ATM branch office has 10 ATM business departments, and each ATM business department has 10 computer terminals, so there are a total of 70 ATM branch offices, 700 ATM business departments, and 7000 computer terminals in the application scenario, and the ATM data servers are interconnected with the computer terminals. Second, each of the seven regional ATM authorities contributes three servers to form the distributed T-ATMChain Trusted Authentication Consortium blockchain, S-ATMChain Data Sharing Consortium blockchain and A-ATMChain Access Control Consortium blockchain. 70 ATM branch offices each contribute one computer terminal to join the three consortium blockchains according to ATM business needs. The computing terminals that join the blockchain network all need to perform the relevant blockchain operations through the blockchain client. Again, assuming that the block size is 1 MB, ATM data servers and computer terminals maintained by regional ATM authorities and ATM branch offices need to save the complete blockchain data; computer terminals of ATM business departments can save the complete blockchain data or partially save the blockchain data, such as saving only the block header of the blockchain. Finally, it is assumed that on average, ten terminals need to interact with the blockchain every minute.

b) *Operational costs:* The running cost of blockchain generally consists of three aspects, computational overhead, network overhead, and storage overhead. The computation overhead of blockchain system mainly depends on the consensus mechanism adopted by the blockchain system. ATMChain uses the official Raft consensus algorithm that comes with Fabric, which makes the number of nodes participating in complex consensus calculations greatly reduced, so it does not consume much computing power. The network overhead of blockchain is mainly influenced by the size of block data and the size and frequency of transactions. According to the assumptions of the application scenario, 70 federated blockchain nodes, 10 transactions per minute, and a block size of 1 MB, the network overhead per minute is: $1\,\text{MB} \times 70 \times 10 = 700\text{MB/min} = 11.67\,\text{MB/s}$. The implication is that the block generator propagates the new block to all federated blockchain nodes, the ATM network bandwidth is relatively large and can afford this network overhead. According to the analysis of network overhead, the whole ATMChain system adds 11.67MB of data per minute, which is about 5990 GB of data per year, which is also affordable.

c) *Availability:* System availability is a key requirement for any network deployment to work well. ATMChain is designed based on blockchain, and the blockchain system can be seen as a distributed redundant voting system implemented through a consensus mechanism. Under the condition that the availability of the federated blockchain nodes R is the same, "taking k out of n is good," the availability of ATMChain can be expressed as follows:

$$R_s = R_v \left[\sum_{i=0}^{n-k} C_n^i R^{(n-i)} (1-R)^i \right] \tag{18}$$

where R_s is the ATMChain system availability; and R_v is the consensus mechanism reliability. In the previous application scenario assumptions, ATMChain requires at least seven nodes to build, and the official statement given by Fabric's native PBFT consensus algorithm is that it can achieve a throughput of 350–500 transactions per second under normal circumstances. The Raft consensus algorithm used in Fabric v2.0 has even higher transaction performance. And in ATMChain, the various constituent nodes belong to the civil aviation industry, they share common industry troubles and pain points, and there is very little possibility of malicious nodes. For ATMChain, its main pursuit is the trustworthiness and security of ATM service data flow and control flow, which essentially focuses more on the integrity and immutability of the block data recorded in ATMChain, and requires less security and efficiency for the consensus algorithm. Even as time goes by, ATMChain has more and more participants and the blockchain log data becomes larger and larger, it is possible to consider changing and optimizing the consensus protocol to solve the related problems, such as adopting a consensus algorithm based on a directed acyclic graph DAG, etc. [57].

Under the condition that the availability R_i of the federated blockchain nodes is different from each other and the consensus mechanism is completely reliable, the "two out of three" availability of ATMChain system can be expressed as the following equation:

$$\begin{aligned} R_s(t) = {} & R_1(t)R_2(t) + R_1(t)R_3(t) \\ & + R_2(t)R_3(t) - 2R_1(t)R_2(t)R_3(t). \end{aligned} \tag{19}$$

Blockchain, as a distributed database, has a large amount of data. However, the operations related to trusted authentication, data sharing, and access control security functions implemented in ATMChain are not directly facing all blockchain data. Moreover, according to the previous analysis, the growth rate of block data is 11.67 MB/s, and general servers have the ability to parse these blockchain data in real time. In ATMChain, the block update process mainly occurs on the node that stores all blockchain data, and general computing terminals do not need to maintain all block data. Therefore, when they need to perform trusted authentication, data sharing, and access control, they are able to perform these operations within a time overhead of seconds.

B. Performance Evaluation

ATMChain is deployed on the HyperLedger Fabric federated blockchain platform, and Fabric provides a unique elastic and scalable architecture that allows it to be adapted for specific application scenarios. The ATMChain build process includes writing configuration files, launching Docker containers and organizational nodes in ATMChain, the creating channels, nodes joining channels, and installing functional smart contracts in instantiated channels, etc. ATMChain creates three ATM security functional business channels responsible for implementing three security functional modules, T-ATMChain, S-ATMChain, and A-ATMChain. In the simulation experimental tests, the smart contract tests rely on the HyperLedger Caliper tool [58]. Because of the random nature of transaction sequencing in blockchain networks, the confirmation time of transactions generally fluctuates within a certain range, each performance test performed is

TABLE IV
Experimental Environment Configuration

Configuration	Version	Note
Operation system	Ubuntu 20	Linux, running in a virtual machine, VMware, with 16GB of RAM allocated to it, and a host processor that is an Intel i7-10875H, Fabric's operating environment
Fabric	Fabric v2.3	A release of the Fabric blockchain, which is the foundation for blockchain application development
Fabric CA	Fabric CA v1.4	It is the certificate authorization center of the Fabric blockchain network, providing registration and enrollment of identity information, issuance and management of digital certificates for nodes in the Fabric network
SDK	Fabric-SDK-Go	It is the official Go language development kit provided by Fabric, which is used by blockchain applications to interact with the Fabric network and access the chain code (smart contracts)
Golang	v1.15.5	The development language of the chain code (smart contract) in Fabric
Docker	V20.10.7-ce	Docker the basic operating environment for storing data and running services on the nodes of the Fabric blockchain network.
Docker-Compose	v1.25.0	It is a flexible Docker container management tool that facilitates developers to manage distributed services consisting of multiple Docker instances, to be compatible with Docker

repeated 20 times and its time overhead is averaged. The configuration of our experimental environment is shown in Table IV.

1) *Performance Evaluation of T-ATMChain:* The generation time and authentication response time of T-Cert are important performance indicators of T-ATMChain security module. The T-Cert generation process for each ATM logical entity consists of three main phases, and the experimental test results are shown in Fig. 11(a). It can be concluded that the application and return time of T-Cert does not change with the increase of the number of authentication domains, because at this time no consensus of the blockchain nodes is required and the communication process only occurs between a single authentication domain and two authentication domains. With the increase of the number of ATM authentication domains, the time of T-Cert certificate confirmation increases slightly, because at this time consensus of the authentication domain nodes in the blockchain is required and its time consumption can be approximately equal to the block generation time. The authentication response process of the T-ATMChain security module is to retrieve and match the corresponding T-CertH in the T-CertSet of the ATM authentication domain blockchain node. Here, the relationships among the authentication response time, the number of authentication domains, and the number of T-CertHs are tested, as shown in Fig. 11(b) and (c). The experimental results show that: the authentication response time is almost independent of the number of authentication domains because the T-CertH retrieval in the authentication response is done within the domain; the authentication response time tends to increase slightly with the number of T-CertHs; because two T-CertHs need to be retrieved for cross-domain authentication, the authentication response time is relatively longer than that for intradomain authentication. In conclusion, T-Cert generation is more efficient and can meet the practical application needs in the range of seconds. ATMChain's authentication response time is in the millisecond range, which can meet the actual authentication requirements.

2) *Performance Evaluation of S-ATMChain:* The time cost of ATM data upchain in the simulation test is shown in Fig. 12(a), where the horizontal coordinate is the data size and the vertical coordinate is the time overhead. From the test results, it can be seen that there is a positive relationship between the time overhead of ATM data up-chain and the size of ATM data. This is because as the ATM data is larger, more time overhead is required for ATM data upchain. In addition, the process of data upchain includes the time for one authentication. The time to upload ATM data is also positively correlated with the number of organizations in S-ATMChain, i.e., the number of ATM data sharing domains, because the more nodes need consensus, the more consensus time overhead is required. ATM data upchain can be completed within milliseconds, which can meet the demand for ATM data up-chain. The time cost of ATM data acquisition in the simulation test is shown in Fig. 12(b), whose horizontal coordinate is the number of key and vertical coordinate is the time overhead. Analyzing the experimental results, we can see that the time overhead of ATM data acquisition increases with the increase of the number of *(Key, Value)* in the blockchain state database, and also with the increase of the number of ATM data sharing domains. ATM data acquisition can be completed within millisecond time range, which can meet the demand of ATM data sharing.

3) *Performance Evaluation of A-ATMChain:* In order to test the policy determination time and success rate of the A-ATMChain access control security module, the number of consensus nodes in the A-ATMChain blockchain network is set to 4, the transaction concurrency per second is set to 10, 10 access control requests are randomly constructed, and 16 sets of experiments are set to test. The number of policies tested is increased incrementally, and the number of attributes to be queried in the access control requests is also increased incrementally, and each test is repeated 20 times to take the average value. As shown in Fig. 13(a), the results show that the latency of policy determination increases slowly with the increase of the number of policies, and the average time consumed for policy determination increases

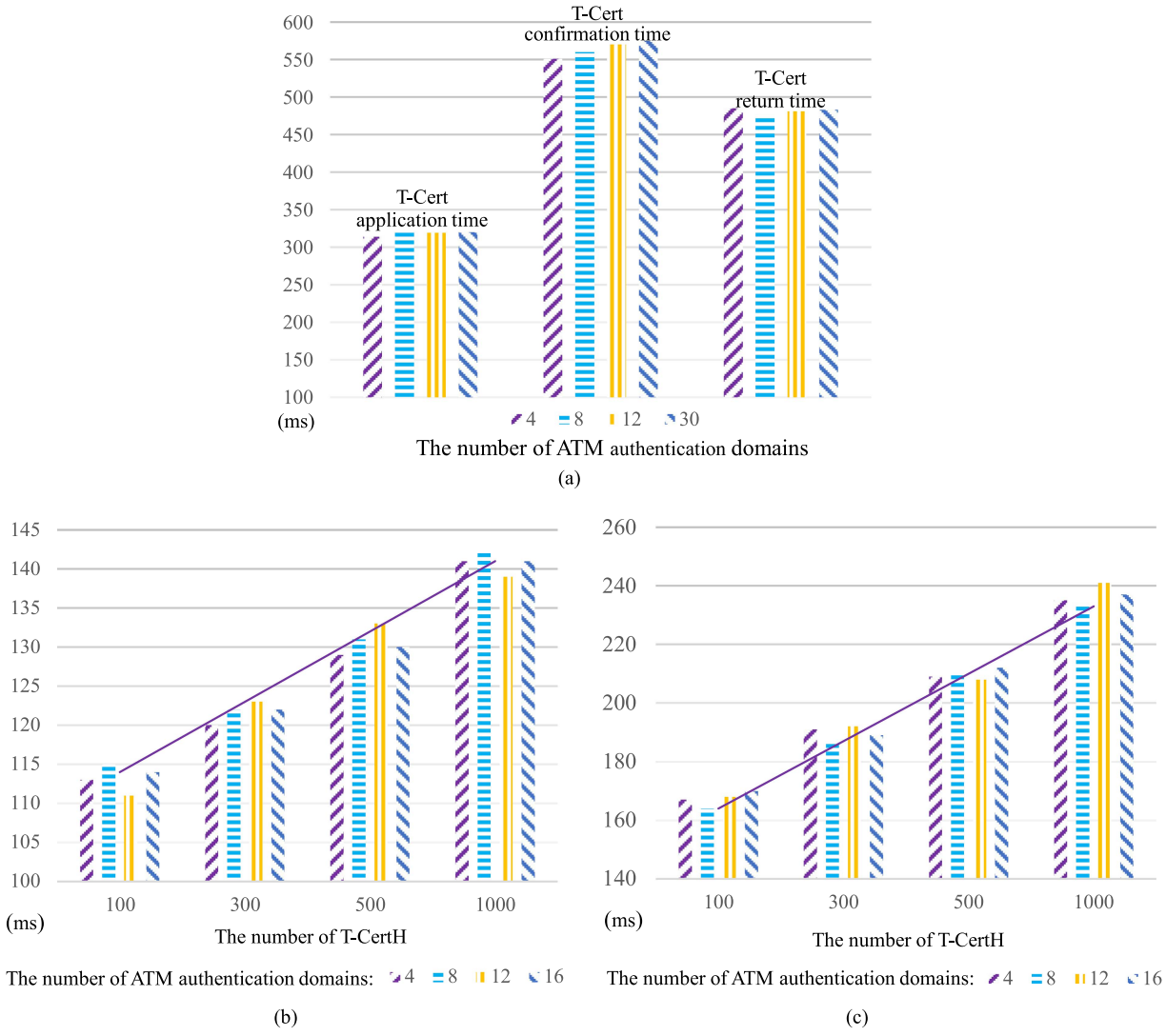


Fig. 11. Performance test of T-ATMChain. (a) T-Cert generation time. (b) Intradomain authentication time. (c) Cross-domain authentication time.

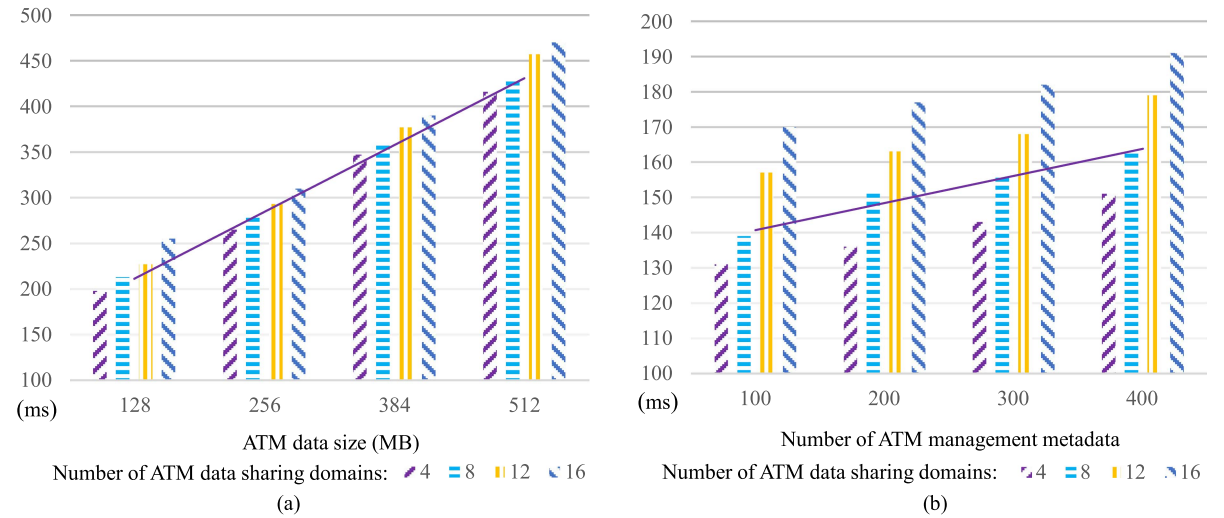


Fig. 12. Performance test of S-ATMChain. (a) ATM data up-chain time. (b) ATM data acquisition time.

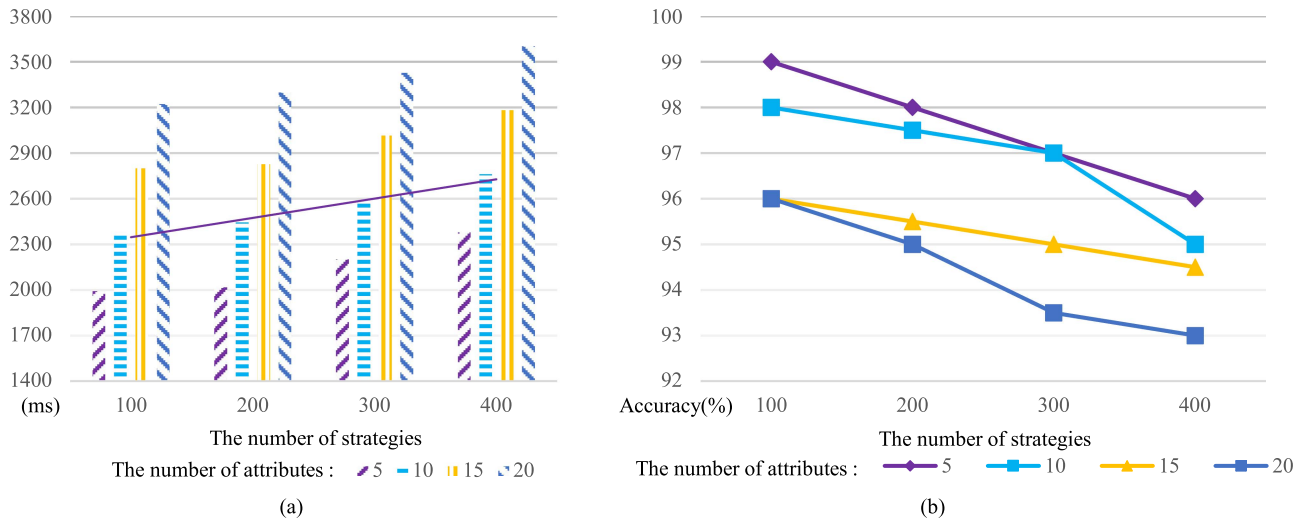


Fig. 13. Performance test of A-ATMChain. (a) Policy decision time. (b) Policy decision success rate.

faster with the increase of the number of attributes. As Fig. 13(b) shows, the success rate of policy determination decreases with the increase of the number of policies; and the success rate of policy determination also decreases with the increase of the number of attributes. This is because there are certain policy conflicts in the set of policies constructed by the experimental simulation, and the PDP smart contract cannot get an accurate judgment result. Taken together, the A-ATMChain access control can be completed within a time frame of seconds and has practicality.

VI. CONCLUSION AND PROSPECT

In order to break through the bottleneck effect of the current ATM security service assurance capability, and prevent and solve the information security threats that appear or potentially appear in ATM, this article uses the trustworthiness and security features of blockchain, integrates it with the 4A information security assurance concept, and constructs a trustworthy model of ATM with distributed characteristics. In turn, innovative breakthroughs are made in the research of three dimensions: credible authentication, data sharing, and access control, forming a future ATM security assurance architecture based on blockchain, and finally reaching the goal of credible, secure, and available ATM information security assurance. Based on the actual situation and with an eye on the future, this article constructs ATMChain, which is compatible with the distributed characteristics of ATM, thus opening up the complete link of ATM information security research from model to architecture. ATM security architecture designed based on ATMChain trustworthy model has the feature of "endogenous security," which realizes 4A security functions based on blockchain through three security modules: T-ATMChain, S-ATMChain, and A-ATMChain, changing the situation of passive security assurance. In terms of feasibility, advancement and application prospect, the research in this article not only satisfies and balances the needs of ATM information security and ATM operation efficiency, but also adapts to the increasingly complex ATM information security situation and development trend in the future.

The research work in this article is centered on ATM information security, and applying blockchain to it is a brand-new research direction. In addition to the research work covered in this article, there are still some aspects that cannot be ignored and deserve more in-depth research and discussion in the future. Here, the future research ideas will be launched from two aspects: the construction of ATM information security guarantee system and the security and application issues of blockchain itself. On one hand, ATM is a complex system with complicated composition and wide geographical distribution. Therefore, the construction of ATM information security assurance system is a complex system engineering. From the macro level, ATM information security assurance system should be composed of three key parts: ATM information security assurance strategy, ATM information security assurance plan, and ATM information security assurance key technology. From a strategic height, the strategic planning into tactical plans, and then to the application of specific key technologies, only so that unfolded one by one, in order to build a comprehensive, comprehensive, orderly, and constantly evolving ATM information security assurance system. From the micro level, centering on the core of "security," ATM information security assurance should start from the analysis and extraction of security threats, to the deployment and implementation of security measures, to the evaluation of the effect of security assurance, and finally to the evaluation and prediction of the security situation, so as to form a loop, and continue to be iterated, improved, and perfected. On the other hand, to apply blockchain to solve the problems related to the ATM information security field, the security of blockchain itself is a factor that cannot be ignored, and it has an important impact on the real implementation and application of ATMChain solution, which is also an issue not covered in this article. Furthermore, when blockchain is to be applied to solve problems related to the field of information security, the security of blockchain itself is a factor that cannot be ignored, and it is the cornerstone and prerequisite for

guaranteeing the security of the entire information system. From the perspective of data security, the data security of blockchain completely relies on cryptography technology, and in order to meet the higher privacy protection needs, it is necessary to introduce privacy protection technologies such as ring signature, zero-knowledge proof, and multi-party secure computing. From the perspective of network security, the consensus mechanism of blockchain is the core of the distributed nodes that can work together, but there is no perfect consensus mechanism that can be applied to all application scenarios, and it is necessary to design a suitable consensus mechanism according to the application environment and network topology of the blockchain platform. From the perspective of application security, the smart contract of blockchain is an important grip for the realization of its diverse applications, and tools for detecting contract security loopholes and the design of formal verification methods are needed to enhance the security audit of the smart contract and thus ensure the security of blockchain applications. However, these issues do not affect the value of blockchain in the research of information security mechanism and the construction of security service capacity, or its value in establishing a trusted network ecology in an untrusted network.

REFERENCES

[1] Global Air Traffic Management Operational Concept, Int. Civil Aviation Org., Montreal, QC, USA, 2005, pp. 1–14.

[2] Manual on ATM Requirements, Int. Civil Aviation Org., Montreal, QC, USA, 2008, pp. 8–17.

[3] F. Shaikh, M. Rahouti, N. Ghani, K. Xiong, E. Bou-Harb, and J. Haque, "A review of recent advances and security challenges in emerging E-enabled aircraft systems," *IEEE Access*, vol. 7, pp. 63164–63180, 2019.

[4] Y. Chen, L. Zhou, J. Yang, and Y. Yan, "Big data platform of air traffic management," in *Proc. IEEE 1st Int. Conf. Civil Aviation Saf. Inf. Technol.*, 2019, pp. 137–141.

[5] M. Akhtar, M. Raffeh, F. ul Zaman, A. Ramzan, S. Aslam, and F. Usman, "Development of congestion level based dynamic traffic management system using IoT," in *Proc. Int. Conf. Elect., Commun., Comput. Eng.*, 2020, pp. 1–6.

[6] L. Zhou, H. Zhang, K. Zhang, B. Wang, D. Shen, and Y. Wang, "Advances in applying cloud computing techniques for air traffic systems," in *Proc. IEEE 2nd Int. Conf. Civil Aviation Saf. Inf. Technol.*, 2020, pp. 134–139.

[7] G. Gui, Z. Zhou, J. Wang, F. Liu, and J. Sun, "Machine learning aided air traffic flow analysis based on aviation big data," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 4817–4826, May 2020.

[8] P. Montefusco, R. Casar, R. Koelle, and T. H. Stelkens-Kobsch, "Addressing security in the ATM environment: From identification to validation of security countermeasures with introduction of new security capabilities in the ATM system context," in *Proc. 11th Int. Conf. Availability, Rel. Secur.*, 2016, pp. 532–541.

[9] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Trans. Syst., Man, Cybern.: Syst.*, vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[10] G. Praveen, S. P. Singh, V. Chamola, and M. Guizani, "Novel consensus algorithm for blockchain using proof-of-majority (PoM)," *IEEE Netw. Lett.*, vol. 4, no. 4, pp. 208–211, Dec. 2022.

[11] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, "An overview of smart contract: Architecture, applications, and future trends," in *Proc. IEEE Intell. Veh. Symp.*, 2018, pp. 108–113.

[12] M. Ramkumar, "A blockchain based framework for information system integrity," *China Commun.*, vol. 16, no. 6, pp. 1–17, Jun. 2019.

[13] Aviation Cybersecurity Strategy, Int. Civil Aviation Org., Montreal, QC, Canada, 2019, pp. 1–8.

[14] Air Traffic Management Bureau of Civil Aviation Administration of China, "Technical specification of air traffic management information system for civil aviation," (in Chinese), Beijing, China: China Standard Publishing House, 2004, pp. 22–17.

[15] X. Lu, Z. Wu, Y. Wu, Q. Wang, and Y. Yin, "ATMChain: Blockchain-based solution to security problems in air traffic management," in *Proc. IEEE/AIAA 40th Digit. Avionics Syst. Conf.*, 2021, pp. 1–8.

[16] Y. Wu, X. Lu, and Z. Wu, "Blockchain-based trust model for air traffic management network," in *Proc. IEEE 6th Int. Conf. Comput. Commun. Syst.*, 2021, pp. 92–98.

[17] X. Lu and Z. Wu, "ATMCC: Design of the integration architecture of cloud computing and blockchain for air traffic management," in *Proc. IEEE Intl Conf Parallel Distrib. Process. with Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw.*, 2021, pp. 37–43.

[18] Z. J. Wu and K. Li, "A study of information security assurance program for U.S. civil aviation," (in Chinese), *Inf. Secur. Res.*, pp. 562–567, 2016.

[19] ATC (Air Traffic Control) Cyber Security Project, Cyber Secur. Forum Initiative, Montreal, QC, Canada, 2015, pp. 19–27.

[20] H. Asgari et al., "Provisioning for a distributed ATM security management: The GAMMA approach," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 11, pp. 5–21, Nov. 2017.

[21] Y. J. Yan and G. Cao, "Next-generation air traffic control system operation concept and its key technologies," *Command Inf. Syst. Technol.*, pp. 8–17, 2018.

[22] L. Ma, "Research on SSE-based information security assurance method for air traffic management ATM," doctoral thesis, Tianjin Univ., Tianjin, China, 2011, pp. 23–57.

[23] T. H. Stelkens-Kobsch, M. Finke, and N. Carstengerdes, "A comprehensive approach for validation of Air Traffic Management security prototypes: A case study," in *Proc. IEEE/AIAA 36th Digit. Avionics Syst. Conf.*, 2017, pp. 1–10.

[24] L. Bogoda, J. Mo, and C. Bil, "A systems engineering approach to appraise cybersecurity risks of CNS/ATM and avionics systems," in *Proc. Integr. Commun., Navig. Surveill. Conf.*, 2019, pp. 1–15.

[25] W. Bellamy, III, "Air France KLM is evaluating MRO potential for blockchain [EB/OL]," 2017. [Online]. Available: http://www.aviationtoday.com/2017/10/03/air-France-klm-evaluating-mro-potential-blockchain/

[26] DNATA, "Anata successfully tests the use of blockchain technology with its program epartners [EB/OL]," 2017. [Online]. Available: https://www.dnata.com/media-centre/dnata-cargo-successfully-tests-the-use-of-blockchain-technology-with-its-programme-partners

[27] SITA, "Smart Path TM- biometrics at every step of the journey [EB/OL]," 2018. [Online]. Available: https://www.sita.aero/pressroom/news-releases/sita-smart-path-biometrics-at-every-step-of-the-journey

[28] R. Reisman, "Air traffic management blockchain infrastructure for security, authentication, and privacy," *Comput. Sci.*, pp. 1–14, 2019.

[29] SESAR, "AICHAIN – A platform for privacy-preserving federated machine learning using blockchain to enable operational improvements in ATM [EB/OL]," 2020. [Online]. Available: https://www.sesarju.eu/projects/aichain

[30] Punch.com, "China Aviation Trust holds aviation travel chain launch [EB/OL]," 2022. [Online]. Available: https://m.thepaper.cn/baijiahao_20561955.html

[31] T. S. Wang, J. Yang, and W. Yao, "Application of blockchain technology in civil aviation," (in Chinese), *Inf. Technol. Cybersecurity*, pp. 109–112, 2018.

[32] N. Wang, Y. Wang, and C. X. Zhang, "Blockchain technology aviation application and development prospect," (in Chinese), *Aviation Sci. Technol.*, pp. 7–13, 2020.

[33] T. Xu, Y. Yang, and T. Liu, "Architecture design of flight cooperative operation guarantee system based on blockchain technology," (in Chinese), *Comput. Appl. Softw.*, pp. 14–18, 2022.
[34] C. Y. Ju, W. G. Feng, and C. X. He, "Research on blockchain-based security information sharing model for civil aviation," (in Chinese), *J. Civil Aviation Univ. China*, pp. 43–48, 2021.
[35] T. Duong, K. K. Todi, U. Chaudhary, and H.-L. Truong, "Decentralizing air traffic flow management with blockchain-based reinforcement learning," in *Proc. IEEE 17th Int. Conf. Ind. Informat.*, 2019, pp. 1795–1800.
[36] H. Y. Wang, "Research on air-rail intermodal ticketing model based on blockchain technology," (in Chinese), *Inf. Technol. Cybersecurity*, pp. 109–112, 2018.
[37] 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 *Proc. IEEE/AIAA 38th Digit. Avionics Syst. Conf.*, 2019, pp. 1–10.
[38] J. H. Zhang, "Research on the solution of false seat occupation in civil aviation based on blockchain technology," master's thesis, Civil Aviation Univ. China, Tianjin, China, 2020, pp. 56–61.
[39] Y. X. Song and J. Lu, "Blockchain-based aircraft maintenance task release system," (in Chinese), *Exp. Technol. Manage.*, pp. 50–53+57, 2020.
[40] F. Hasin, T. H. Munia, N. N. Zumu, and K. A. Taher, "ADS-B based air traffic management system using Ethereum blockchain technology," in *Proc. Int. Conf. Inf. Commun. Technol. Sustain. Develop.*, 2021, pp. 346–350.
[41] H. A. Damis, D. Shehada, C. Fachkha, A. Gawanmeh, and J. N. Al-Karaki, "A microservices architecture for ADS-B data security using blockchain," in *Proc. 3rd Int. Conf. Signal Process. Inf. Secur.*, 2020, pp. 1–4.
[42] P. Zhenzhen, G. Xu, Z. Fudong, and L. Jing, "A blockchain-based airplane meteorological data sharing incentive system," in *Proc. IEEE 2nd Int. Conf. Inf. Technol., Big Data Artif. Intell.*, 2021, pp. 871–876.
[43] X. Zhang and X. Miao, "An optimization scheme for consortium blockchain in cf," in *Proc. IEEE 3rd Int. Conf. Civil Aviation Saf. Inf. Technol.*, 2021, pp. 247–251.
[44] Y. Zakir, K. S. Hasan, N. S. Wiggins, and A. Chatterjee, "Improving data security in message communication between ACT and aircraft using private blockchain," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur.*, 2019, pp. 506–513.
[45] I. S. Bonomo, "Development of SWIM registry for air traffic management with the blockchain support," in *Proc. 21st Int. Conf. Intell. Transp. Syst.*, 2018, pp. 3544–3549.
[46] D. Toratani, Y. Nakamura, and M. Oka, "Data-driven analysis for calculated time over in air traffic flow management," *IEEE Access*, vol. 10, pp. 78983–78992, 2022.
[47] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surv. Tuts*, vol. 22, no. 2, pp. 1432–1465, Apr.–Jun. 2020.
[48] R. H. Kim, H. Noh, H. Song, and G. S. Park, "Quick block transport system for scalable hyperledger fabric blockchain over D2D-assisted 5G networks," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1176–1190, Jun. 2022.
[49] Satoshi Nakamoto Institute, "Bitcoin: A peer-to-peer electronic cash system [EB/OL]," 2009. [Online]. Available: https://nakamotoinstitute.org/bitcoin/
[50] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[51] H. Liu, D. Han, and D. Li, "Fabric-IoT: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020.
[52] Y.-Q. Cai, E. Zhang, and P.-Y. He, "A (t,n) threshold signature scheme against collusive attacks," (in Chinese), *J. Beijing Univ. Technol.*, pp. 1231–1235, 2011.
[53] J. X. Wu, "Endogenous security development paradigm in cyberspace," (in Chinese), *Sci. China, Inf. Sci.*, pp. 189–204, 2022.
[54] A. Q. WuHu, L. T. WuFang, and T. WuLi, "Research on endogenous security defense system based on bionic mechanism," (in Chinese), *J. Netw. Inf. Secur.*, pp. 11–19, 2021.
[55] J. Zhiwen, L. Tao, and H. Aiqun, "Research on endogenous security methods of embedded system," in *Proc. IEEE 6th Int. Conf. Comput. Commun.*, 2020, pp. 1946–19502.
[56] T. Yun, J. Luo, B. Peng, and D. Yao, "Dynamic defense methods for endogenously secure industrial control networks," in *Proc. Chin. Automat. Congr.*, 2018, pp. 635–639.
[57] J. Hu, "Research on parallel blockchain consensus protocol based on directed acyclic graph," (in Chinese), master's thesis, Shanghai Normal Univ., Shanghai, China, 2020, pp. 40–51.
[58] Hyperledger Caliper [DB/OL], 2017. [Online]. Available: https://hyperledger.github.io/caliper/

Xin Lu received the Ph.D. degree in safety science and engineering from the Civil Aviation University of China, Tianjin, China, in 2023.

He is a Lecturer with the School of Information Engineering, Shanxi College of Technology, Shanxi, China. His current research interests include air traffic management system, blockchain, and cyber security.

Zhijun Wu received the B.S. degrees in information processing from Xidian University, Xi'an, China, in 1988, and the M.S. degrees in information processing from Xidian University, Xi'an, China, in 1996, and the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications, Beijing, China, 2004.

He is a Professor and Ph.D. Supervisor with the School of Safety Science and Engineering, Civil Aviation University of China, Tianjin, China. His research interests include denial-of-service attacks, and security in Big Data and cloud computing.

Junbin Cao received the Ph.D. degree in land resource management from the China University of Geosciences, Beijing, China, in 2017.

He is a Senior Engineer with the School of Information Engineering, Shanxi College of Technology, Shanxi, China. His current research interests include information systems and data security.