BLOCKCHAIN-BASED SECURE MANAGEMENT FRAMEWORK FOR UNMANNED VEHICLES, INTERNET OF THINGS AND AVIATION

İNSANSIZ ARAÇLAR, NESNELERİN İNTERNETİ VE HAVACILIK İÇİN BLOKZİNCİR-TABANLI GÜVENLİ YÖNETİM ÇERÇEVESİ

OZAN ZORLU

ASSOC. PROF. DR. ADNAN OZSOY

Supervisor

Submitted to

Graduate School of Science and Engineering of Hacettepe University

as a Partial Fulfillment to the Requirements

for the Award of the Degree of Doctor of Philosophy

in Computer Engineering

May 2024

ABSTRACT

BLOCKCHAIN-BASED SECURE MANAGEMENT FRAMEWORK FOR UNMANNED VEHICLES, INTERNET OF THINGS AND AVIATION

Ozan ZORLU

Doctor of Philosophy, Computer Engineering

Supervisor: Assoc. Prof. Dr. Adnan OZSOY

May 2024, 132 pages

Data management is a crucial requirement due to the autonomous and constrained nature of Unmanned Aerial Vehicles (UAVs), Internet of Things (IoTs), and the aviation domain. The autonomous and restricted nature of these sectors increases the need for a shared, distributed database, strong access control management, consensus in autonomous decision-making, and effective communication across diverse protocols and devices. This research presents a comprehensive approach and offers a new viewpoint to the field of blockchain while establishing a fundamental baseline for future improvements in data management systems and addressing the shortcomings of previously proposed existing frameworks in order to fulfill the complex needs of secure data management. This study contributes to the advancement of secure and efficient data management systems by implementing robust data monitoring for error detection, ensuring data integrity, and enabling encrypted or anonymous data sharing based on sensitivity levels. Additionally, the integration of diverse devices, enforcement of immutable regulations compliance, and development of permissioned blockchain systems for identity management further enhance the system's capabilities, offering comprehensive solutions for modern data management challenges.

In our tests, the proposed framework showed increased successful transactions in all rate controllers. Besides, effect of the validator number on throughput and latency is tested and analyzed thoroughly.

Keywords: Unmanned Systems, Flight Management System, Data Security, Blockchain Framework, Autonomous Decision-making, Access Control, Secure Communication and Storage

ÖZET

İNSANSIZ ARAÇLAR, NESNELERİN İNTERNETİ VE HAVACILIK İÇİN BLOKZİNCİR-TABANLI GÜVENLİ YÖNETİM ÇERÇEVESİ

Ozan ZORLU

Doktora, Bilgisayar Mühendisliği

Danışman: Doç. Dr. Adnan OZSOY

Mayıs 2024, 132 sayfa

İnsansız Hava Araçları (İHA), Nesnelerin İnterneti (IoT) ve havacılık alanındaki otonom ve kısıtlanmış doğası nedeniyle veri yönetimi hayati bir gerekliliktir. Bu sektörlerin otonom ve sınırlı doğası, paylaşılan, dağıtılmış bir veritabanı, güçlü erişim kontrol yönetimi, otonom karar alma süreçlerinde uzlaşma ve çeşitli protokoller ve cihazlar arası etkili iletişim ihtiyacını artırmaktadır. Bu araştırma, blok zinciri alanına kapsamlı bir yaklaşım sunmakta ve veri yönetim sistemlerinde gelecekte yapılacak iyileştirmeler için temel bir çerçeve oluştururken, güvenli veri yönetimi ihtiyaçlarını karşılamak üzere önerilen mevcut çerçevelerin eksikliklerini gidermeyi amaçlamaktadır. Bu çalışma, hata tespiti için güçlü veri izleme, veri bütünlüğünün sağlanması ve duyarlılık düzeylerine bağlı olarak şifreli veya anonim veri paylaşımının mümkün kılınması yoluyla güvenli ve etkin veri yönetim sistemlerinin gelişimine katkıda bulunmaktadır. Ayrıca, çeşitli cihazların entegrasyonu, değiştirilemez düzenlemelere uyumun sağlanması ve kimlik yönetimi için izinli blok zinciri sistemlerinin geliştirilmesi, sistem kapasitesini daha da artırarak modern veri yönetimi zorlukları için kapsamlı çözümler sunmaktadır. Yapılan testlerde, önerilen çerçeve tüm hız kontrol cihazlarında artan başarılı işlem oranları göstermiştir. Bunun yanı sıra, doğrulayıcı

sayısının işlem hacmi ve gecikme süresi üzerindeki etkisi de detaylı bir şekilde test edilmiş ve analiz edilmiştir.

Keywords: İnsansız Sistemler, Uçuş Yönetim Sistemi, Veri Güvenliği, Blok Zinciri Çerçevesi, Otonom Karar Alma, Erişim Kontrolü, Güvenli İletişim ve Depolama

ACKNOWLEDGEMENTS

To my beloved ones...

CONTENTS

Page

TABLES

FIGURES

ABBREVIATIONS

IoT	:	**I**nternet **o**f **T**hings
UAV	:	**U**nmanned **A**erial **V**ehicles
FOQA	:	**F**light **O**perations **Q**uality **A**ssurance
PKI	:	**P**ublic **K**ey **I**nfrastructure
PoW	:	**P**roof **o**f **W**ork
PoA	:	**P**roof **o**f **A**uthority
PoS	:	**P**roof **o**f **S**take
IBFT	:	**I**stanbul **B**yzantine **F**ault **T**olerance
PBFT	:	**P**ractical **B**yzantine **F**ault **T**olerance
SPoF	:	**S**ingle **P**oint **o**f **F**ailure
GPS	:	**G**lobal **P**ositioning **S**ystem
INS	:	**I**nertial **N**avigation **S**ystem
NavDB	:	**Nav**igation **D**ata**b**ase
PerfDB	:	**Perf**ormance **D**ata**b**ase
ICAO	:	**I**nternational **C**ivil **A**viation **O**rganization
CIA	:	**C**onfidentiality, **I**ntegrity, **A**vailability
TLS	:	**T**ransport **L**ayer **S**ecurity
RSA	:	**R**ivest **S**hamir **A**dleman
CoAP	:	**C**onstrained **A**pplication **P**rotocol
EC	:	**E**lliptic **C**urve
CA	:	**C**ertification **A**uthority
PSK	:	**P**re-**S**hared **K**ey
OTP	:	**O**ne-**T**ime **P**assword
GCM	:	**G**alois/**C**ounter **M**ode
AES	:	**A**dvanced **E**ncryption **S**tandard
CBC	:	**C**ipher **B**lock **C**haining

MAC	:	**M**essage **A**uthentication **C**ode
UAS	:	**U**nmanned **A**erial **S**ystem
ABAC	:	**A**ttribute-**B**ased **A**ccess **C**ontrol
RBAC	:	**R**ole-**B**ased **A**ccess **C**ontrol
Cap-BAC	:	**Cap**ability-**B**ased **A**ccess **C**ontrol
TTP	:	**T**rusted **T**hird **P**arty
WSNs	:	**W**ireless **S**ensor **N**etworks
FMS	:	**F**light **M**anagement **S**ystem
ARINC	:	**A**eronautical **R**adio, **INC**orporated
LoRA	:	**Lo**ng **R**ange
BFOD	:	**B**lockchain-**B**ased **F**light **O**peration **D**ata
ATM	:	**A**ir **T**raffic **M**anagement
HIE	:	**H**ealth **I**nformation **E**xchange
CPS	:	**C**yber-**P**hysical **S**ystems
MSLShard	:	**MSLShard** architecture
ACL	:	**A**ccess **C**ontrol **L**ists
IDE	:	**I**ntegrated **D**evelopment **E**nvironment
FMC	:	**F**light **M**anagement **C**omputer
CDU	:	**C**ommon **D**isplay **U**nit
js	:	**J**ava**S**cript
I_eC	:	**I**nter-**c**luster **B**lockchain
R_A	:	**R**ole of the **M**anagement of **P**rivate **B**lockchain
R_DM	:	**R**ole of **D**ata **M**anagement
R_L	:	**R**ole of **L**istener
QBFT	:	**Q**uorum **B**yzantine **F**ault **T**olerant
K_PR	:	**P**rivate **K**ey
K_PU	:	**P**ublic **K**ey
API	:	**A**pplication **P**rogramming **I**nterface
IPFS	:	**I**nter**P**lanetary **F**ile **S**ystem

1. INTRODUCTION

Blockchain technology, recognized for its inherent decentralization, absence of reliance on trust, immutable storage, and capacity to anonymously transmit information, is increasingly being adopted across various industries. Common applications include insurance [1], healthcare [2], land registry cadastre [3], voting [4], industry [5], finance [6], supply chain [7], social media [8], and ticket sales [9]. Its burgeoning popularity in specialized sectors such as aviation, the Internet of Things (IoT), and unmanned aerial vehicles (UAVs) domain underscores the critical importance of maintaining data precision and trustworthiness in these autonomous and restricted fields [10].

The efficacy of blockchain is demonstrated by its heightened security attributes, including immutability, authentication, authorization, and encryption. These features are especially well-suited for tackling the challenges encountered in sectors where safeguarding privacy and data security are of utmost importance [11, 12]. This technology has a wide range of uses and has the potential to completely transform present operational systems because of its benefits, including improved security, decentralization, and fault tolerance.

Entities in the aviation, IoT, and UAV industries sometimes operate in clusters or independently, as illustrated in Figure 1.1. Attributes such as data integrity, confidentiality, availability, increased access control, traceability, and seamless integration are vital in these sectors. Blockchain's inherent characteristics effectively address these issues. For instance, Umran et al. utilized blockchain to enhance privacy and security in IoT data exchanges [13], while Raj et al. developed a customized access control system for healthcare monitoring [14]. These applications validate the technology's suitability and effectiveness. Despite these advances, a significant gap remains in developing a comprehensive framework to manage the intricate requirements for secure data management in these critical fields [15, 16].

The scholarly focus on blockchain indicates a broader transition toward a secure and interconnected digital future, highlighting its pivotal role in creating safe, streamlined, and user-centric digital frameworks. An analysis of the literature reveals insights into specific

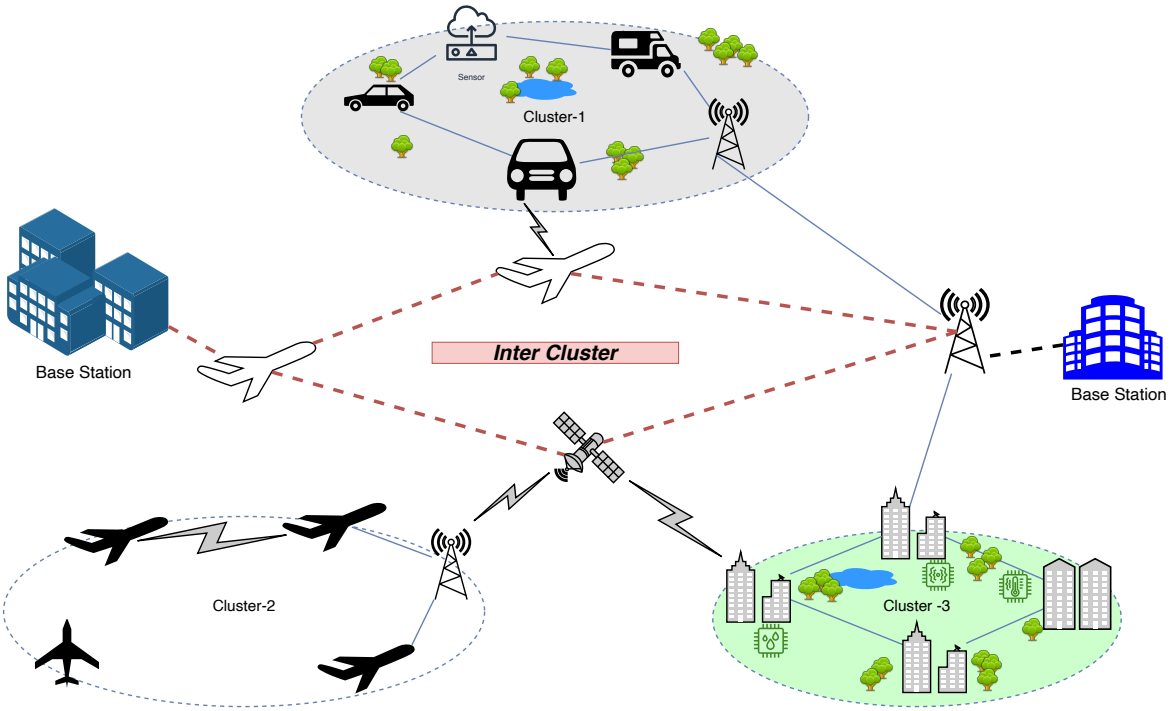

Figure 1.1 An overview of clustered structure of problem domain.

blockchain applications and challenges encountered in these areas. Hirtan et al. [17] describe a blockchain-based architecture for privacy protection in intelligent transportation, which necessitates robust communication and processing capabilities. This architecture changes central authority while maintaining its presence, recommending deployment in trusted or permissioned environments to ensure identity anonymity.

The impact of blockchain on managing crises such as the COVID-19 pandemic has also been explored in literature. A bibliometric study identified key areas of blockchain application in organizational settings, focusing on artificial intelligence research methodologies, addressing business sustainability during the pandemic, and studying its effects on the supply chain industry [18]. Further research is dedicated to improving privacy protection and data management in the domains of intelligent transportation and aviation [19]. Concerns about maintaining privacy in smart city contexts, especially in systems using UAVs, remain a significant challenge [20].

In the aviation sector, blockchain has been used to replay flight events in compliance

with Flight Operations Quality Assurance (FOQA) criteria [21, 22], and to manage and safeguard flight data, demonstrating its operational efficiency [23]. The cross-sectoral interaction and integration of blockchain applications underscore its versatility and potential as a fundamental component of future digital systems. This is further exemplified by its use in enhancing security within the Industrial IoT for Electric Smart Grid [24]. Despite the success of pilot projects and theoretical support for blockchain's value, it is crucial to recognize that the technology is still in the early stages of practical application in industry and commerce [25]. Nevertheless, blockchain is advancing significantly towards achieving the development level necessary for its widespread implementation in industrial and commercial environments.

After conducting a comprehensive analysis of the key topics discussed in section following sections, it has been determined that the fields of aviation, the IoT, and UAVs face various obstacles such as inadequate storage capacity, unreliable communication links, insecure data-sharing channels that prioritize data confidentiality, substantial administrative requirements for maintaining connectivity, lack of transparency in central authority management for users, and numerous other challenges. Despite notable advancements in blockchain applications, there is a requirement for a comprehensive framework that integrates the underlying principles of blockchain to adequately tackle the overarching challenges of data management. The objective of this research is to rectify this inadequacy by presenting a comprehensive framework that ensures both security and confidentiality. Additionally, it facilitates smooth communication across various protocols, maintains self-management in accordance with confidentiality requirements, and preserves unchangeable data in a distributed domain. This configuration necessitates the implementation of a distributed database, streamlined data management, collaboration, safe data transfer, decentralized decision-making, and communication across several protocols and devices. Although there has been much research on data management in several sectors, a comprehensive framework is not specifically developed to address these challenges in data management.

This study introduces a comprehensive and adaptable framework that seeks to address

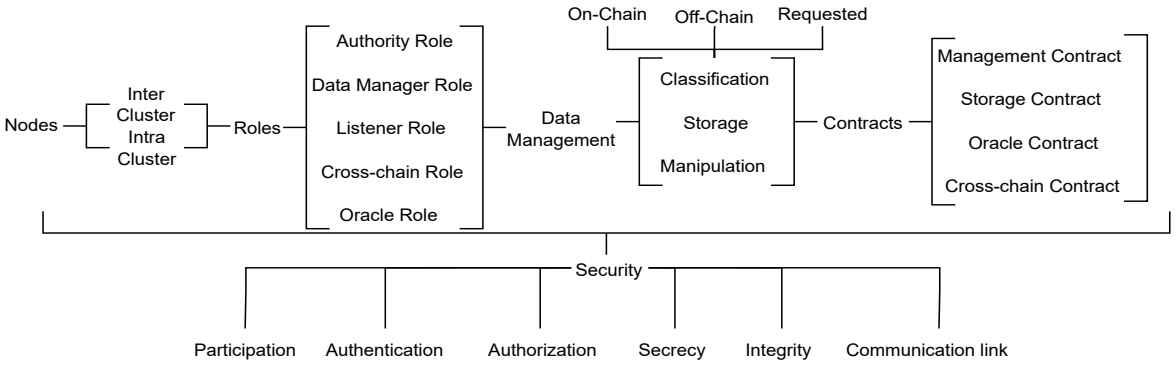

Figure 1.2 The system model of the proposed blockchain-based secure management framework.

the previously mentioned challenges and build a strong basis for future enhancements, as illustrated in Figure 1.2. The framework is specifically designed to guarantee the secure management of data. Blockchain technology is utilized in the aviation, IoT, and unmanned systems sectors to create this framework. The architecture is designed in a clustered manner to address deficiencies in current research, enhance scalability, and efficiently handle the intricacies of node interactions in large networks. This architectural style enables the incorporation of customized consensus mechanisms that are specifically designed to fit the unique operational needs of the framework. The system employs a rigorous methodology to safeguard data from both internal and external threats. The framework ensures comprehensive security by incorporating role-based access control, authentication, and authorization mechanisms, which are essential for handling sensitive data and meeting crucial security requirements.

Moreover, the model's hierarchical structure enables smooth integration and ongoing development, showcasing its capacity to predict technological changes and the necessity for digital adaption. The categorization of segments into inter- and intra-cluster groups, along with a modular organization of contracts and responsibilities, guarantees efficient and safe data storage and retrieval. Moreover, this attribute provides the flexibility necessary to accommodate the distinct requirements of various industries. The suggested framework aims to resolve existing and anticipated challenges in data management across many industries by employing a clustering methodology, implementing stringent security measures, and offering a customizable design, hence creating a resilient and flexible solution. The study presents

a blockchain-based architecture that sets itself apart from existing systems by introducing numerous notable advancements. The system utilizes a modular and layered architecture, dividing it into separate layers for blockchain, data management, access management, communication, and presentation. This approach improves scalability, maintenance, and interoperability when compared to typical monolithic systems. The framework utilizes a hybrid storage technique that combines on-chain, off-chain, and dynamically requested data storage. This approach optimizes data availability and integrity, resulting in a more versatile and efficient system compared to traditional methods. In addition, the framework integrates sophisticated clustering techniques such as inter-cluster, intra-cluster, and hybrid clustering, which enhance the efficiency and capability of managing greater workloads. The incorporation of this intricate framework into contemporary systems is anticipated to make a substantial contribution to the advancement of self-governing, protected, and effective digital infrastructures. The main contributions of this research are:

- Facilitating the secure transmission of data between nodes using cryptographic techniques entails permitting data sharing in either encrypted or anonymous formats, depending on the level of sensitivity of the information. This strategy entails safeguarding the integrity of the data, ensuring that it remains unaltered, undamaged, and immune to any unauthorized interventions or alterations.

- The integration of a diverse array of devices, including drones, IoT devices, and airplanes, is being done. Each device is specifically built to do certain duties, and they vary in terms of their processing capabilities and access to blockchain technology. This involves ensuring that all participants adhere to immutable regulations throughout the entire procedure.

- Updating databases efficiently is achieved by leveraging the distributed framework's structure and reducing storage needs through inter-cluster and intra-cluster designs. This entails enabling seamless communication and information sharing within and among clusters, potentially incorporating diverse blockchain technology.

- Developing a tailored blockchain platform with limited entry, specifically engineered for the purpose of overseeing IDs. This solution provides restricted visibility to safeguard the confidentiality of either private or sensitive corporate data. This involves the implementation of authentication and authorization systems to fulfill access management requirements. Designated individuals are granted explicit authorization to conduct data inquiries on the blockchain. They can employ monitoring systems to assess activities and guarantee adherence to regulations. Furthermore, the inclusion of data monitoring capabilities enables the identification of faults, enabling analysis in both online and offline scenarios.

- The suggested architecture exhibited a greater number of successful transactions across all rate controllers. An investigation is conducted to examine the influence of the validator number on both throughput and latency.

The remaining portions of this research are organized as follow: Section 2. provides the background in the field and our motivation, focusing on the difficulties and proposed solutions discussed in the existing literature. A thorough examination of the literature is conducted in Section 3. to identify similar studies, followed by a full comparison and analysis. The system concept of the secure management framework based on blockchain is thoroughly explained in Section 4. in the themes depicted in Figure 1.2. Ultimately, our proposed framework is implemented, an experimental analysis is carried out, and our obtained results are presented in Section 5. in order to verify its suitability, usability, and relevance.

In order to evaluate our proposed framework an Ethereum platform is employed to construct a consortium network of blockchains, where experiments are conducted to initialize data on the chain in Section 6.. The evaluation bed is initialized and tests are run using our developed application that utilizes Hyperledger Caliper to benchmark the framework in terms of throughput and latency. As stated in Section 7., the findings demonstrate that the suggested framework is applicable, suitable, acceptable, scalable, and viable. Moreover, additional

assessments and improvements are planned to ensure the level of preparedness for actual deployment in real-life implementation.

2. BACKGROUND OVERVIEW

2.1. Blockchain Fundamentals

Bitcoin is a digital currency system introduced in 2008 by an individual or group known as Satoshi Nakamoto [26]. The exact nature of this entity or entities remains uncertain. The concept established the blockchain as a data format for storing monetary transactions, in addition to an agreement to guarantee the chain's reliability. The contributors conceived the blockchain as a database that adheres to a sequential arrangement of blocks. Every block includes cryptographic hashes that establish a connection between the previous and current blocks, ensuring the integrity and immutability of the blockchain. The Bitcoin network employs this database to store contractual agreements and financial transactions. The technology facilitates decentralized electronic payments between peers in an immediate and safe way, depending on electronic evidence instead of trust. The consensus mechanism, facilitated by a distributed ledger, forms the fundamental basis of Bitcoin's operation [27]. The ledger hold data that is safeguarded from deletion, alteration, and tampering [28].

While the distributed ledger innovation was originally developed for Bitcoin, it has applications that extend beyond the scope of Bitcoin. This is because of the intrinsic characteristics of the blockchain, which is a decentralized database that is copied and maintained around a network of nodes. Each block in the chain consists of a body and a header.

Blockchain technology utilizes a network of interconnected blocks, with each block being successively linked in a chain, as depicted in Figure 2.1 [29]. Every individual block comprises transaction data that has undergone authentication by network nodes, preamble information that validates the preceding block's integrity, and the Merkle root, an indispensable component for transaction validation. The use of cryptographic techniques such as public key infrastructure (PKI) and hash algorithms in this architecture guarantees the permanence of data, which is why this technology is gaining increasing traction.

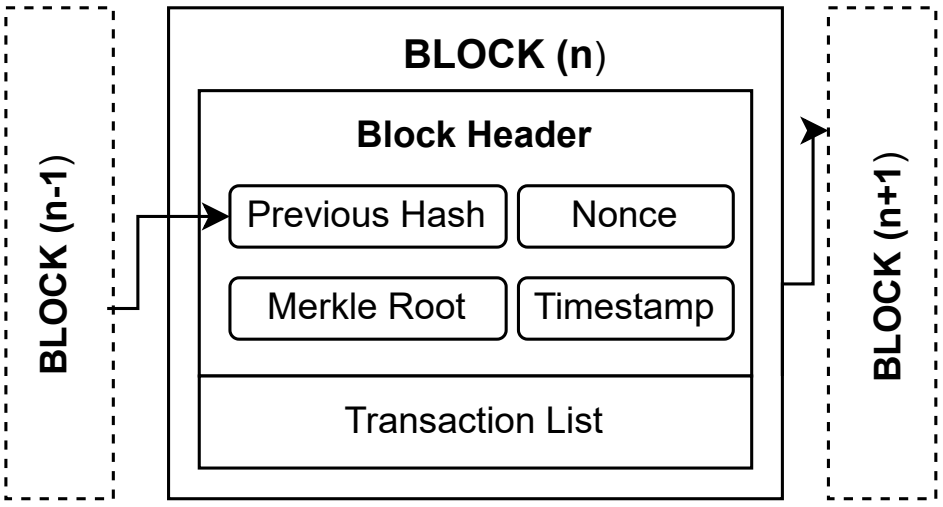

Figure 2.1 Block elements

The key feature of blockchain is its decentralized governance structure, which eliminates the requirement for central authorities and instead use consensus methods to verify transactions and generate new blocks [30]. These methods are essential for preserving the network's integrity and functionality. Proof of Work (PoW) is a consensus mechanism that uses computationally demanding activities to build blocks, while Proof of Authority (PoA) only allows authorized nodes to validate transactions. Proof of Stake (PoS) presents an alternative method in which the likelihood of validating transactions is directly linked to the quantity of currency held by a node. This system encourages the security and involvement of stakeholders with greater wealth.

Considerable research is being directed towards improving the speed and efficiency of consensus algorithms in order to enhance the scalability and performance of blockchain systems [31]. Finality denotes the irrevocable verification that a block of transactions is legitimate and endorsed by the network. Blockchain consensus solutions guarantee finality by proving that once a block is appended to the chain, it becomes unchangeable and cannot be undone. Although PoW offers a level of certainty that a block can be reversed with sufficient processing power, the Istanbul Byzantine Fault Tolerance (IBFT) algorithm, which is a modified version of the Practical Byzantine Fault Tolerance (PBFT), guarantees immediate finality. Under the IBFT consensus algorithm, once a transaction is recorded on

the blockchain, it becomes immutable, ensuring robust protection against tampering. This security feature remains effective even if up to one-third of the nodes in the network are faulty or dishonest [32].

Blockchain technology combines sophisticated cryptographic techniques with reliable consensus algorithms to provide a secure and transparent way of conducting transactions without the requirement of centralized supervision. Due to its essential qualities of trust, integrity, and accessibility, this technology serves as a fundamental tool for a wide range of applications, including financial services and supply chain management.

Consensus algorithms play a crucial role in blockchain technology by guaranteeing the reliable and consistent processing of all transactions across a distributed network. These techniques facilitate consensus among network participants regarding the present condition of the distributed ledger, thereby deterring fraudulent activities and assuring synchronization of all ledger copies. Here are some of the key consensus algorithms commonly employed in blockchain technologies:

2.1.1. Proof of Work (PoW)

PoW is a consensus technique that necessitates a member node to solve an intricate mathematical problem in order to authenticate transactions and generate new blocks. The act of resolving this issue is referred to as mining. PoW ensures security by imposing a high computational cost on any attempt to modify any part of the blockchain. The initial node that successfully resolves the problem is granted the authority to append a block to the blockchain and receives a compensation in the form of cryptocurrency. The complexity of the difficulties guarantees that the addition of fraudulent blocks is not feasible because of the significant computing expense.

2.1.2. Proof of Stake (PoS)

PoS is a consensus algorithm that chooses transaction validators based on the amount of coins they are prepared to stake or lock up as a kind of security. In the PoS consensus mechanism, a node's probability of being selected to validate transactions and generate new blocks increases in proportion to the number of coins it has staked. Unlike PoW, PoS does not necessitate significant computational effort, hence rendering it more energy-efficient [33].

2.1.3. Proof of Authority (PoA)

PoA is a consensus process that relies on the reputation of transaction validators, who are chosen in advance based on their identity and reputation. PoA is seen superior to PoW and PoS due to its reliance on the credibility of designated validators rather than computational capacity or the quantity of staked coins. This approach is well-suited for permissioned blockchains, as it enhances accountability by providing openness regarding the identities of validators [34].

2.1.4. Practical Byzantine Fault Tolerance (PBFT)

PBFT is specifically designed to function in asynchronous systems and has the capability to handle a maximum of $\frac{n-1}{3}$ malicious nodes, where n represents the total number of nodes. PBFT operates through a series of consecutive processes that involve the selection of a principal node responsible for proposing the value to be unanimously agreed upon. Subsequent nodes verify and transmit this proposition to achieve a consensus. PBFT is especially advantageous in settings that necessitate minimal delay and maximum data processing capacity [35].

2.1.5. Istanbul Byzantine Fault Tolerance (IBFT)

IBFT is a modified version of the PBFT algorithm designed specifically for the Ethereum blockchain. It is capable of functioning in both permissioned and public blockchain networks. IBFT guarantees that all transactions are approved by a supermajority and offers instant transaction finality, ensuring that once a block is added, it becomes immutable. This serves as a preventive measure against forks, a frequent occurrence in PoW blockchains [36].

2.1.6. Quorum Byzantine Fault Tolerance (QBFT)

QBFT is an enhanced variation of the IBFT algorithm that improves its performance and fault tolerance. QBFT improves upon the constraints of IBFT by enhancing the consensus process to increase transaction throughput and minimizing the communication overhead between nodes[37].

Each of these consensus techniques possesses unique strengths and applications that are contingent upon the specific requirements of the blockchain system, including factors such as speed, security, and decentralization. As the technology of blockchain advances

2.2. Blockchain as Emerging Technology

Bitcoin presents the initial blockchain solution to the problem and is promoted as a feasible financial substitute for conventional currencies by reducing the requirement for a central bank [38]. Financial money transactions may only be made in an anonymous, decentralized, and immutable manner [39]. When the benefits came to the fore after releasing Bitcoin, different blockchain technologies emerged with diverse capabilities [40]. Ethereum's use of smart contracts has significantly expanded the application scope of blockchain technology, making it a pioneering breakthrough [41]. While Bitcoin technology is only capable of creating unspent transaction output (UTXO) to store monetary transactions, Ethereum blockchain is a Turing complete, programmable, solution that enables building distributed

trusted applications. In other words, blockchain technology has advanced from being an unchangeable cryptocurrency trade ledger into a programmable interactive environment [42]. Another initiative, Hyperledger, develops a business consortium blockchain to address all types of requirements for an open-source, cryptocurrency-supported, adaptable, and secure blockchain [43].

Conventional information technology systems, social media platforms, and other services that depend on users' data necessitate obtaining consent before utilizing the data, and preserving the secrecy of this information is crucial. Nevertheless, as demonstrated by the Wikileaks incident, the act of revealing sensitive and classified information can result in detrimental consequences for the economy, politics, and human rights [44]. Facebook's influence was evident in both the 2016 US presidential election and the Taiwanese presidential election, as highlighted by several sources [45, 46]. These occurrences highlighted the need to treat every piece of data as valuable and refrain from sharing it without the owner's consent. Information has become a potent force and a valuable resource on a global scale. Blockchain is a potential remedy for these problems, as it is known for safeguarding the confidentiality of personal information by employing cryptographic identification and access control methods that ensure anonymity.

Blockchain is being utilized across various areas, including IoT, aviation, and UAV to tackle privacy breaches in both academic and business environments. The smart cities community is primarily focused on safeguarding the personal data that is processed, exchanged, or stored [11]. Moreover, the utilization of IoT devices has created novel study prospects in the domain of smart cities, which are regarded as intricate and challenging. Ensuring data confidentiality is of utmost importance since individuals with access to personal navigation or location monitoring data can disclose information about their habits, acquaintances, employment, preferred places to visit, interests, and other potential issues.

2.3. Flight Management System (FMS)

The aviation sector has greatly benefited from technology improvements, including the creation of the Flight Management System (FMS), which has improved safety, efficiency, and regulatory compliance. The FMS, which was first introduced in 1982 [47], was created with the purpose of minimizing the workload of pilots by automating crucial duties during flights. Over time, the Flight Management System (FMS) has developed to have a considerable influence on different elements of aviation, enhancing approach speeds, flight patterns, and compliance with strict regulatory criteria.

A contemporary Flight Management System has various essential subsystems, including the Control Display Unit (CDU), flight plan management module, performance and guiding module, and navigation module. These components function collaboratively, aided by networked databases that guarantee streamlined data transmission, as seen in Figure 2.2.

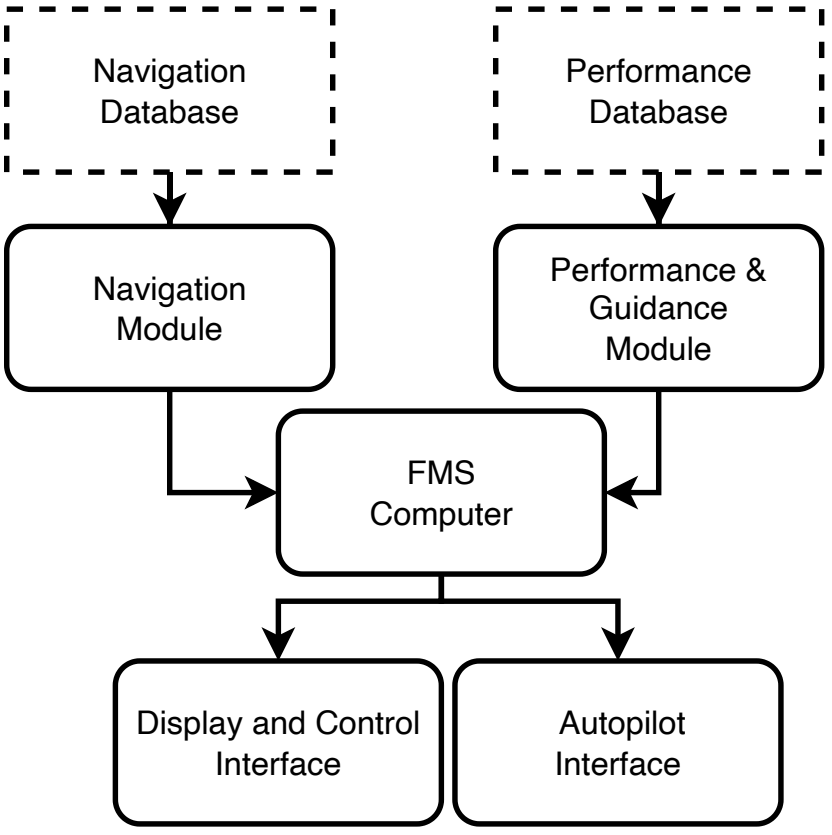

Figure 2.2 Flight Management System (FMS) Modules and Interaction with Databases

The Flight Management System (FMS) improves automation throughout every stage of a flight, starting from takeoff and ending with landing, and plays a crucial role in contemporary aviation avionics. The system utilizes data from many sensors, including the Global Positioning System (GPS) and Inertial Navigation System (INS), to precisely calculate and direct the aircraft's path. Furthermore, the system is essential in determining the best route by utilizing comprehensive navigation and performance databases to reduce mistakes and improve flight safety through meticulous data integration and analysis.

The functionality of the FMS relies on data from several sources, such as the performance database (PerfDB), navigation database (NavDB), numerous sensors, and pilot inputs. The NavDB, which comprises crucial aeronautical information, is a vital asset for FMS producers, aviation management, and pilots. The software complies with the ARINC 424 standard, which governs the structure of flight plans and necessitates updates every 28 days as specified by the International Civil Aviation Organization (ICAO). The dependability, uninterrupted availability, and trustworthiness of the NavDB are of utmost importance in order to minimize potential delays in aviation operations.

Extensive research has been performed to address the issues involved with efficiently maintaining NavDB data, recognizing its value [48]. There is a growing interest in investigating blockchain technology as a possible solution to these difficulties [49]. Subsequent research has extensively investigated the security requirements of aviation communication systems, specifically emphasizing availability, authentication, authorization, secrecy, integrity, privacy, and non-repudiation [50]. The objective of these studies is to enhance comprehension of intricate matters associated with these systems.

Conventional airline communication networks, commonly dependent on radio or Wi-Fi signals, are vulnerable to security risks. Although traditional approaches are available to reduce the effects of cyber-attacks, the introduction of blockchain technology presents potential improvements in data security and user privacy in peer-to-peer aviation networks. Conventional systems are typically centralized and lack strong protocols to guarantee safe communication between different parties, such as authorities, service providers, and

end-users. In addition, current systems frequently lack efficient means to enforce airspace laws. Contemporary literature promotes the implementation of decentralized protocols to oversee the allocation of airspace usage rights and ensure security goals including confidentiality, reliability, and accessibility [51]. The purpose of these decentralized protocols is to improve the overall security and guarantee compliance with regulations in the aviation industry.

2.4. Access Control Management

One of important aspect of security is the authorization of nodes, that is, the act of permitting or refusing access to network services depending on the identification and credentials of the node making the request. Authorization offers a vital role in controlling access to resources and functionalities among IoT ecosystems that utilize blockchain technology. Once a node is successfully authenticated and deemed a legitimate participant, the process of authorization begins. Authorization is the process of either allowing or refusing access privileges to specific resources or functionalities within the network. In the context of blockchain-enabled IoTs, authorization can be enforced through the utilization of smart contracts. Smart contracts define rules and conditions for accessing and utilizing network resources. These contracts can specify which nodes have permission to perform particular operations, access certain data, or control specific network functionalities. By utilizing smart contracts for authorization, IoTs can ensure that only authorized nodes can access and manipulate resources, enhancing security and maintaining the integrity of the network and its generated data.

Studies in this area mainly focus on authentication, authorization, security issues, different architecture proposals, and device or network limitations. These concepts are categorized as the following: authentication and authorization, security considerations, and system architectures. This subsection discusses these categories with respect to their relation to the authentication and authorization schemes.

2.4.1. Authentication and Authorization

In some studies, authorization is not thought of beyond authentication. Such systems simply accept the traffic from authenticated devices and drop that of unauthenticated devices. In [52–55]; however, various authorization schemes that are applicable post-authentication are discussed. Access to different services supplied by various organizations is required and who can access what is determined by policies deployed on the chain. In addition, there are further requirements or expectations from such a system:

2.4.1.1. Single-Sign-On Even if the services are from different organizations or systems the same credentials should be applicable to all of them [52].

2.4.1.2. Scalability The system should be city-scale scalable so that it can work with millions of devices or different policies, [53].

2.4.1.3. Delegated Policies In some cases, it might be desired that when a certain entity is given some kind of an access right, this access right should be also able to be used by a related entity, such as an underling. This comes with its own issues such as non-interactivity and out-of-order delegations [53].

For the implementation of policies, various access control mechanisms for example Attribute-Based Access Control (ABAC), Role-Based Access Control (RBAC), and Capability-Based Access Control (Cap-BAC) etc. are available. The traditional implementations of these cannot be employed as that would endanger decentralization and scalability. However, blockchain technology offers also a beneficial solution for this kind of cases. As with blockchain, replicates of data, distributed over different nodes while being consistent with other replicates can be stored [52]. Furthermore, blockchain allows updating policies consistently on all nodes of the system. Thus, if some policy cannot be verified by one verifier because that verifier is unavailable, another verifier of the system can do the verification as they have the exact same policy data.

2.4.2. Attribute-Based Access Control (ABAC)

A full authentication and authorization system for smart city applications that utilizes OAuth2 and OpenID Connect has been proposed in the literature [52]. OpenID Connect is employed in a way that authorization has identity claims where stolen access tokens cannot be used without proving the identity. Access control is realized by eXtensible Access Control Markup Language (XACML) compliant ABAC policies. According to the study, OAuth2 protocol can realize delegated access but it is not clear in the article whether the proposed implementation has this feature or not. The blockchain utilization in the study is for data decentralization and not directly linked to the authentication and authorization mechanisms.

2.4.3. Role-Based Access Control (RBAC)

The study in [53] implements an RBAC based authorization system, called WAVE, that considers many important use cases. In the system, blockchain is not accessed or modified frequently, rather it is only used to store the permissions. All privileged access occurs outside the blockchain thus blockchain does not slow down the system. The system has also role delegations which are implemented using smart contracts. These are called Delegations of Trust (DoTs) and they can be visualized as a graph. Features offered by DoTs could be summarized as follows:

2.4.3.1. Non-Interactivity: Assume there is a role delegation from entity A to B. This delegation is non-interactive role delegation if it can be carried out successfully even if both A and B are offline. When entity B is online again, delegated permissions can be utilized.

2.4.3.2. Out-of-order Delegations: Assume an entity A delegates one of its roles, call R, to entity B. Next, assume that R is given further access to a previously non-existent resource. Now B, which has delegated role R, must also immediately have access to this new resource.

2.4.3.3. Revocation: A permission can be granted or revoked and this may be triggered by another entity or the permission itself might have a limited life time such that it expires eventually.

2.4.3.4. Private Permissions: Since permissions are stored on blockchain, and blockchain is accessible, all permissions are visible. This creates a security hole as permission content may contain sensitive data, such as permission to Alice's office that is described as "BuildingCENG/PartB/Room201". Anyone who can see that Alice has access to this room will know that Alice is likely to work there ([53]). However, the system employs identity-based encryption to permissions. Thus, only the identified related user can decrypt their permissions.

Due to the above-mentioned features, the system initially looks promising for IoT ecosystems and is implemented and emulated in a 150-node network over 500 hundred days. Additionally, the authors claim that the system supports city-scale deployment while being low cost such that it can even be deployed on the Ethereum main chain.

2.4.4. Capability-Based Access Control (Cap-BAC)

The study in [56] implements a Cap-BAC system on parity consortium blockchain with PoA consensus mechanism. Unlike most other studies reviewed, the implementation is highly interactive. In the system, owners register themselves, their devices and the capabilities of the devices to the smart contracts on the blockchain. Owners can give access to their devices by registering capabilities for other users. These capabilities are invalidated when they expire or when they are revoked. Users with capabilities can access the device through a server after proving that they have access. If an owner loses their Decentralized Identifier (DID), they can recover their identifier by creating a recovery request and subsequent voting process.

2.4.5. Security Considerations

Security considerations of studies in the field mainly focus on the security of IoT communications and secure authentication as some systems consider authenticated nodes as authorized and vice versa. Without proper security measures, IoTs and their integral part WSNs are vulnerable to a range of attacks, such as eavesdropping, tampering, denial-of-service or routing attacks [57, 58]. In the following paragraphs of this subsection, some of the key security considerations that must be taken into account when implementing authentication mechanisms in IoT ecosystems using blockchain and other approaches are discussed.

2.4.5.1. Key Management: One of the most critical aspects of authentication in IoTs is key management. Since IoT ecosystems typically consist of managed and unmanaged devices, it is essential to ensure that cryptographic keys employed for authentication are secure and protected against theft, loss, or compromise. This can be achieved through the use of secure key generation, distribution, and storage mechanisms. Numerous proposals related to this consideration reside in the literature and interested readers may refer to [59] for a sample study which utilizes PKI.

2.4.5.2. Data Integrity: Data integrity is another critical security consideration in IoT ecosystem. The data collected by nodes is often sensitive and can be abused for malicious activities if it is tampered with or altered in any way. Therefore, it is essential to ensure data protection against tampering using mechanisms such as digitally signed messages, message authentication codes, and hashing techniques. An example architecture of digital signatures and elliptic curve methodology is implemented by [60] and an example of using hash functions is proposed by [61].

2.4.5.3. Attack Detection and Mitigation: Since the ecosystem is sensitive to various attacks, to integrate lightweight defense and mitigation mechanisms in place in order to

detect and counter such attacks is crucial. This can be accomplished by utilizing intrusion detection and prevention technologies which can perform network surveillance to detect any signs of potentially malicious behavior and take necessary action in real or near-real time. Because the IoT ecosystem has limited resources, lightweight mechanisms for detection of malicious intent and activities are gaining interest among researchers lately. With the implementation of such low-cost techniques, the network can revoke the node to ensure the safety of ecosystem when detected.

2.4.5.4. Privacy: Another crucial consideration in the ecosystem is privacy, particularly in applications where sensitive data and/or Personally Identifiable Information (PII) is being disseminated. In such environments, it is essential to ensure that the privacy of users is protected, and their data is not exposed to unauthorized parties.

2.4.5.5. Scalability: Finally, scalability is a critical security consideration when implementing authentication mechanisms in the ecosystem. Since IoTs can consist of thousands or even millions of nodes, it is essential to ensure that the utilized mechanisms are scalable and can handle the high volume of traffic that could be generated by such dense or sparse networks.

Considering the security concerns outlined before, it is feasible to establish a robust security framework in an IoT ecosystem, enabling its use for many applications.

2.5. Airport Access Management Control with Blockchain

Airports are classified as restricted facilities due to their use for air travel and logistics, which necessitate a tight policy of zero tolerance. One of the key challenges in these facilities is the monitoring and reporting of various types of information, as well as keeping track of workers' access records. This issue has also been highlighted in the literature [62]. In this study, we focus on airports that are distinct, isolated facilities without direct interconnections,

mirroring typical real-life scenarios. Within mentioned problem area, admission logs are reported on an specific basis as depicted in Figure 2.3.

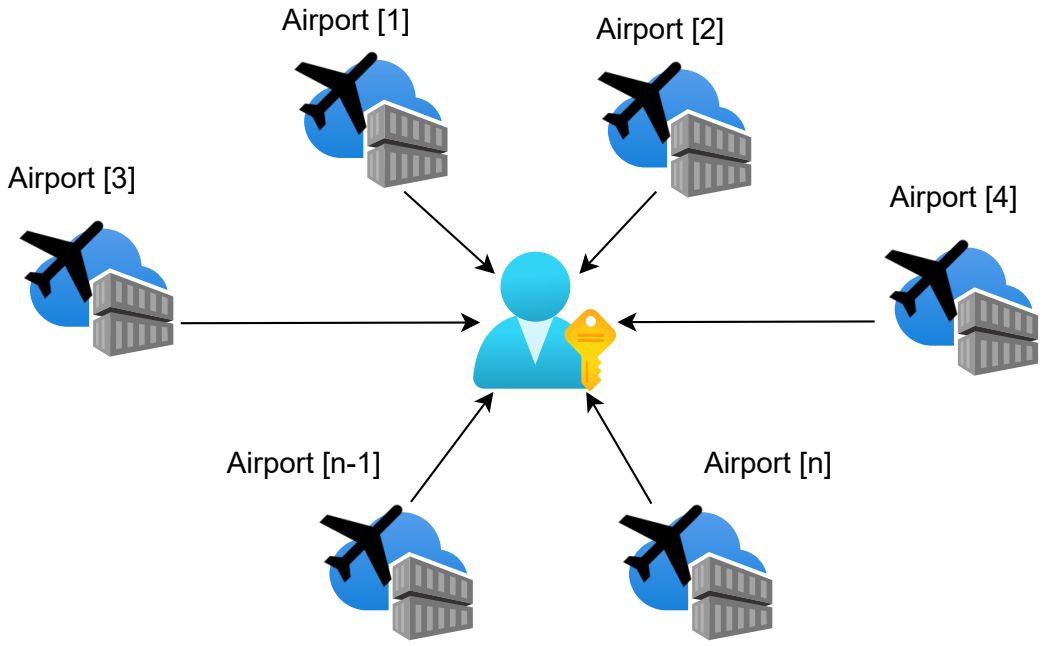

Figure 2.3 Illustration of the access management control problem domain.

The subject of security of airport is a matter of concern and has been extensively examined in the literature. Recent advancements in technology have surfaced, leading to the recognition of their advantages. Various solutions have been devised to address the aforementioned challenges, particularly in the realm of airport security, with a particular focus on ensuring data security. Qingbin et. al. proposed a blockchain-based approach to tackle the difficulties and barriers encountered by airport managers, authorities, and regulators. This system is regarded as a proficient substitute for conventional methods due to its decentralized and autonomous nature, high level of confidentiality, openness, and ability to safeguard against altered data [63]. The consortium blockchain guarantees the protection of data and efficiently carries out the tasks of monitoring and traceability.

[64] offers a comprehensive elucidation of the fundamental principles of blockchain technology in the context of the IoT. Moreover, this study proposes an optimal framework for improving security and constructing a reliable architecture. The main obstacles in the

IoT usually revolve on the capacity for data processing and the duration of battery life. The recommended architecture should have robust security measures while also preserving a streamlined design. The paper explores the concerns related to security, trust, and identification that arise with IoT devices, and subsequently presents a solution that utilizes blockchain technology. Next, the methods for combining IoT and blockchain are analyzed. By employing Swarm technology, they were able to circumvent the need for a private blockchain. Their investigation, which compares the setups of public and private networks, shows that reveals that nearly all categories of nodes' private blockchains use less storage as well as memory. The allocation of responsibilities within the blockchain network for IoT devices has been identified, with power consumption emerging as the key concern. Therefore, the utilization of Blockchain technology in conjunction with Long Range (LoRA) for the purpose of linking IoT devices, as well as utilizing Swarm for data storage, were suggested as promising areas for future investigation.

A dedicated access control application has been developed exclusively for Hyperledger Fabric [65]. Hyperledger Composer is employed for the management of access to physical locations. They employed blockchain technology to meet the requirements of non-repudiation and enduring record-keeping. This technology offers a distributed and unchangeable data records. Components are compact modular entities that are bundled as a singular entity and disseminated over the network. The main elements of the composer module consist of an access control language, a query file, and JavaScript files. The access control policies were implemented in the access control language module. Then the authors examined performance metrics and resource utilization. Their suggested model, when assessed against a benchmark for comparison, showcases its feasibility as a solution for the specific situation at hand. The outcomes validate that the model remains consıstent and exhibits the possibility for scalability.

Zhang et.al. have presented a smart contract for the purpose of access control for IoT devices [66]. A smart contract is created in the study to oversee designated responsibilities in the context of access management. The proposal involves the registration and adjudication of contracts to achieve decentralization of access management. Hardware-based testing are

performed and the resulting evaluation outcomes indicate that the contracts are suitable for real-world situations.

Access control methods are extensively employed to safeguard important data and vital infrastructure, such as facilities. The authors of this study, Maesa et al. (cite), suggest a mechanism for access control on a blockchain that is based on policies. Established protocols ensure that policies stored on the blockchain are openly available and observable. The proposed methodology significantly enhances audibility. In addition, any malevolent entities are unable to refuse the privileges that have been given. To verify the audibility and consistency of policy checks. Another advantage of utilizing public and distributed policies is the enhanced audibility.

3. RELATED WORK

In recent times, the aviation and UAV sectors have started utilizing blockchain technology to improve the administration, security, and efficiency of data. The unchangeable and distributed characteristics of blockchain are being utilized to enhance regulatory adherence, guarantee the authenticity of flight information, and effectively and securely handle air traffic. These technological breakthroughs have resulted in creative solutions that specifically tackle the distinct obstacles encountered by the aviation sector, including the secure exchange of data, dependable storage of flight records, and the efficient administration of UAV operations.

With the ongoing expansion of the IoT, there is a growing demand for strong and secure authentication methods. Authentication is a fundamental component of authorization, which controls access to IoT resources and guarantees the security and privacy of data. Integrating blockchain technology into IoT ecosystems has emerged as a promising approach to tackle security concerns. It provides decentralized, tamper-proof, and secure infrastructures.

This section examines the current body of literature on the use of blockchain technology in many fields, with a specific emphasis on its impact on improving aviation, UAV operations, and IoT security. Our objective in this section is to demonstrate the current status of research and highlight the impact of our proposed framework in these important disciplines by conducting a thorough review of their contributions.

3.1. Blockchain in Aviation and UAV Domains

There is a growing number of commercial applications in the aviation industry that are being developed to utilize blockchain technology for accurate data usage [67, 68]. The growing recognition of blockchain technology's ability to transform data management and bolster security in several industries is evident as we advance into the digital era. This recognition is demonstrated by a significant increase in academic research focused on solving industry-specific problems through the use of blockchain applications, leading to

a fundamental change towards systems that have improved security, transparency, and efficiency.

By performing a search on the Web of Science database using the specified keywords *aviation, blockchain, blockchains, data sharing, security, smart contract, smart contracts*, it is evident that there is a noticeable and distinct trend towards research in this field, as depicted in Figure 3.1. The inclination to investigate this domain is apparent from the publication dates of the uncovered works.

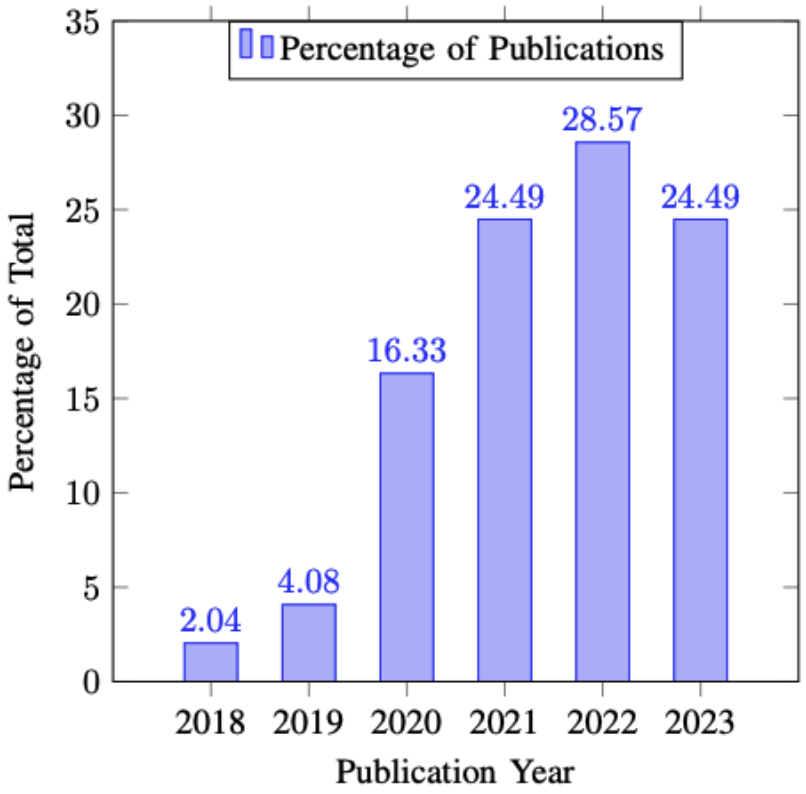

Figure 3.1 An overview of the prevailing areas of research in blockchain technology within the aviation industry. The percentage for each year is determined by its proportionate contribution to the overall number of papers identified in the search.

The rise in the quantity of such solutions can be attributed to the advancements achieved in the blockchain domain. Originally created as an immutable ledger for digital currency transactions, blockchain has undergone a substantial transformation and now functions as a flexible platform, especially with the integration of smart contracts [69]. These autonomous

code segments, deployed on platforms such as Ethereum, facilitate intricate computations. The convergence of blockchain technology improvements and the aviation industry's demand for consistent reliability has led to the development of innovative solutions aimed at tackling regulatory compliance and overcoming challenges in aviation.

Considering these essential factors, blockchain technology emerges as a resilient framework, consisting of unchangeable data records distributed in blocks, resistant to deliberate or accidental modifications [70]. The decentralized, trustless, and immutable structure of blockchain makes it inherently resistant to single points of failure (SPoF), making it a highly secure storage management solution for important information.

Scientists and companies are investigating the industrial uses of UAVs and drones [71]. The objective of Jensen et.al. is to showcase the practical use and technological progress of blockchain in terms of bolstering security, guaranteeing availability, and preserving immutability, surpassing conventional use cases and scenarios [72]. The study examines the potential utilization of blockchain technology in the mentioned domains, but it omits the actual execution or a comparison of various blockchain systems. Boeing and SparkCognition joined together to establish SkyGrid, a firm that provides a comprehensive solution for unmanned and autonomous aircraft in the aviation sector [25]. This is an another instance of the utilization of blockchain technology in commercial contexts. After the company is founded, its primary objective is to guarantee the safe and efficient management of package transfers using drones, as well as the operation and oversight of air taxis and other aircraft. Blockchain technology is being used to regulate unmanned aerial system (UAS) traffic, while artificial intelligence will help meet the needs of enterprises. Furthermore, they plan to engage in cooperation with regulatory agencies. Their infrastructure is specifically engineered to enable and support both commercial and personal aviation travel.

Given the emergence of solutions to known difficulties in the aviation and UAV arena, it was necessary to conduct a literature investigation in this field. Therefore a comprehensive academic study is conducted to ensure compliance with aviation regulations for the utilization of UAVs, drones, and airplanes, alongside the advancement of commercial

applications. UAVs are strictly forbidden by aviation regulatory agencies in the vicinity of airports, military zones, and essential infrastructure [73–75]. Moreover, the growing availability of economical and efficient drones has resulted in an uncertain airspace, necessitating more stringent rules. Clarke et.al. performed a thorough examination of the dangers that drones present to public safety and the protection of personal privacy in order to clarify these issues [76]. Wild et.al undertook a thorough examination of 152 events involving remotely piloted aircraft systems (RPASs) that took place from 2006 to 2015. The objective of this investigation was to identify and evaluate the potential hazards linked to unmanned vehicles, commonly referred to as drones, in order to devise efficient strategies for mitigating risks [77]. Their research illustrates that uncontrolled advancements in aviation technology present a higher level of danger compared to errors made by pilots. Regulating these miniature airborne vehicles is a current concern in the field of aviation safety. There have been numerous drone-related incidents in the aviation industry. In 2015, a drone and a plane collided during a drug smuggling operation in Mexico [78]. In 2017, a drone and an airplane collided in Canada [79]. Thankfully, the aircraft landed safely with minor harm, but the flight was later canceled. In 2018, the operations of over 58 aircraft at Gatwick Airport were disrupted as a result of the presence of two UAVs (drones) flying over the airport [80]. In 2019, Heathrow Airport in England had another occurrence of flight cancellations due to the presence of drones[81]. In order to address this issue, Kapitonov et. al. have developed a framework known as AIRA, which is designed to provide the accessibility of reliable data for the control of semi-autonomous robots [82]. The vulnerability of the environment in which robots function and plan their next move in the cyber-physical domain emphasizes the need of dependable data. The Drone Employee project use the AIRA protocol to authenticate that the UAV follows the assigned path by accessing information stored on the blockchain by the dispatcher [83]. The proposed protocol is simple and allows for the coordination of air traffic management and communication between numerous entities.

Drone or IoT device attacks can occur in two ways: through the transmission of gathered data from the drone to the central system, and through the receiving of new commands from the control center to the drone. Both forms of communication, encompassing data provenance

and permission, are vulnerable to modifications and adverse consequences [84, 85]. Ensuring the security of the channel is essential for protecting the storage, confidentiality, integrity, and availability of the information. Most IoT devices and UAVs are connected to each other and depend on cloud servers to fulfill their computing needs. The cloud infrastructure is regarded as secure and effectively resolves the storage limitations of small devices [86]. These devices are commonly used in regions that lack security or are vulnerable to attacks [87]. An additional crucial feature in the field is the precise placement and scope of their coverage, together with their level of connectivity [88]. In order to address these concerns DroneChain serves as an intermediary between the cloud server and the drones to address the issue of unsecured communication channels [89]. The goal is to ensure the integrity of the data and commands collected, rendering them resistant to alteration and accessible for scrutiny by external entities. The present study conducts a comprehensive analysis and evaluation of DroneChain in order to assess its efficacy in ensuring the integrity of drone data during the process of transferring and storing data in the cloud. In contrast, drones consistently receive instructions by storing hash values of directives from the central system or data from other drones. Nevertheless, due to its dependence on immutable data stored on the blockchain and in the cloud, the design fails to provide a comprehensive communication solution.

Flight Data Recorders (FDR) are primarily designed to securely retain data in a durable and easily accessible manner. They are also built to survive impact shock, penetration, static crushing, high-temperature fire, and immersion in liquid following an accident [90]. Another functionality is to offer comprehensive aeronautical data for subsequent playback of the flight. Technological advancements have enabled the conversion of flight data recorders (FDRs) into digital format. This allows for the analysis of recorded data to discover anomalies, hence enhancing flight safety in the future. The utilization of recorded onboard data analysis, investigations, and various anomaly detection techniques improves the Flight Operations Quality Assurance (FOQA) standards. The aviation industry predominantly utilizes blockchain technology to address several challenges related to data management, sharing, storage, and analysis. The Flight Data Recorder (FDR), a crucial component in

aviation, is designed to remain operational even in the event of an accident [23]. The system is accountable for overseeing aircraft, enhancing safety protocols, identifying issues, and foreseeing any future incidents. Studies have been carried out in the literature to reduce the size and weight of these bulky containers for UAVs. Over time, digital flight data recorders have advanced to store more precise information and allow for the analysis of flights to detect any irregularities pertaining to flight safety. The Red Cat firm has created a flight recorder for UAS that makes use of blockchain technology [91]. This recorder enables the examination and reproduction of flight data, which is encoded to ensure security. Moreover, the recorder is furnished with artificial intelligence (AI) functionalities to aid in diagnostics. Additionally, this article presents a decentralized storage framework built upon blockchain technology, which guarantees the safe transmission and retention of information through the utilization of encryption methods. The solution they offer features an open-source and flexible framework, with the goal of assisting regulators, insurance firms, and operators of drone fleets.

Analyzing the flight data is important to ensure the correctness of the information stored in the Flight Data Recorder (FDR) and to discover the causes of a crash or any abnormalities that occurred during the flight using deterministic playback. It serves a vital role in both the speed at which the data is obtained and the precision of the data that is captured. The research conducted to collect flight records and capture access status in the utilized data meticulously takes into account deterministic replay, operating system input and output (OS-I/O) management, and hardware support [22].

FlightChain, a research initiative introduced by SITA, seeks to leverage the inherent immutability of blockchain technology to securely store flight data within the aviation sector [92]. FlightChain specializes on utilizing blockchain technology for the purpose of data management, going beyond the capabilities of IoT devices and UAVs. Blockchain is commonly acknowledged as a distributed and immutable database. The suggested concept employs a permissioned blockchain architecture, which allows authorized entities to access data. The testing include British Airways, Geneva Airport, Heathrow, and Miami International Airport. FlightChain has employed smart contracts developed on

Ethereum and Hyperledger Fabric to alter and securely store more than two million flight records. FlightChain continues to experience unresolved issues without receiving satisfactory responses. The introduction of permissioned blockchain has resulted in management challenges arising from the system's inherent deficiency in self-management capabilities. Actually, it is not a challenge, but an opportunity to supervise a network that can be enlarged and has some level of transparency. This network also facilitates consensus on crucial managerial decisions by utilizing smart contracts. Hyperledger Fabric surpasses Ethereum in terms of sophistication and complexity. Nevertheless, it boasts an impressive transaction output of approximately 100,000 transactions per second, beyond any potential need for more. Testing relies solely on a restricted amount of flight data.

In the field of aviation management, blockchain technology is demonstrated through the implementation of the Blockchain-Based Flight Operation Data (BFOD) sharing scheme and the BlockTrust model [48]. The models illustrate the capacity of blockchain technology to guarantee the security of data and improve the efficiency of operations in the aviation sector [93]. The BFOD system employs cryptographic methods, like as zero-knowledge proofs, to strengthen the privacy of flight operational data. Empirical data has shown a substantial reduction in the time needed to reach an agreement. BlockTrust is a significant progress in the creation of dependable aviation information systems. It achieves this by establishing a secure protocol for transmitting data on Air Traffic Management (ATM) networks, even in the presence of communication delays resulting from the usage of blockchain technology.

Moreover, there is a specialized data-sharing platform designed exclusively for aviation vendors [94]. This platform demonstrates the application of blockchain technology to improve transparency and address the ongoing problem of limited information accessibility in supply chains. The combination of these achievements indicates a positive direction in aviation management towards a unified ecosystem facilitated by blockchain technology. This signifies a shift from individualized solutions to a holistic framework within the sector.

3.2. Blockchain in IoT Domain

An emerging trend in the use of blockchain technology inside an IoT environment is the idea of *blockchain-enabled* networks. This entails incorporating blockchain technology into these networks to establish a decentralized, tamper-resistant, and secure network infrastructure. The decentralized nature of blockchain guarantees that there is no central authority governing the network. All devices have the ability to participate in the decision-making process of the network according to their privileges, which are determined by the kind of blockchain. As a result, this enhances the network's ability to withstand and recover from attacks and failures. Moreover, the inherent tamper-resistant quality of blockchain technology guarantees that any data saved on the network cannot be modified or removed, thereby ensuring a superior level of data integrity and authenticity. The combination of these characteristics renders blockchain-enabled IoTs highly appealing and auspicious for use in applications that necessitate a robust level of security, privacy, and trust, such as critical infrastructure, healthcare, and supply chain management. By employing blockchain-enabled IoT technology, it is feasible to create a secure and reliable environment for gathering and analyzing data from various physical objects, including sensor nodes and other devices.

Similar with the IoT, the healthcare industry utilize blockchain technology to safeguard confidential patient information and empower individuals with more authority over their medical records. HierChain's hierarchical storage solution enhances the administration of health data across many blockchain platforms, ensuring a harmonious equilibrium between the security and efficiency of IoT networks [95]. The Health Information Exchange (HIE) is a patient-centered method for sharing health information at the same time. The utilization of smart contracts improves privacy and grants patients independent authority over their health records. The integration of blockchain technology, together with decentralized principles, in the healthcare industry highlights an upcoming future in which data management is not only highly safe but also places a strong emphasis on individuals' privacy. An example of this is the research undertaken by Nguyen et. al., which presented a resilient intrusion detection system that utilizes blockchain technology to provide safe data transmission [96]. The

researchers utilized a specialized categorization model tailored for Cyber-Physical Systems (CPS) in the healthcare industry. By conducting extensive simulations, they have proven that their proposed methodology is very accurate, effective, and feasible.

The IoT domain demonstrates how blockchain technology enhances data management and improves operational efficiency. The decentralization of data management is accomplished by the integration of clustering, edge computing, and blockchain in a three-tier architecture. Emerging designs are being developed to tackle the increasing concerns around privacy and trust in IoT networks [97]. The MSLShard architecture employs an advanced adaptive network sharding strategy to enhance the scalability and security of shared IoT resources. The complex interconnections of smart city infrastructures are of utmost importance [98].

There are numerous methods that utilize different features of blockchain technology. The swift progress in the IoT has transformed numerous businesses by facilitating effortless connectivity and data interchange across devices. Nevertheless, a key focus in this field is to guarantee safe and dependable authentication. Authentication is essential because it forms the basis for authorization, which determines the access and control of IoT resources. In order to tackle this crucial feature, a multitude of studies and research endeavors have been focused on creating strong authentication techniques. The objective of these initiatives is to strengthen security measures, safeguard confidential information, and deter unwanted entry, thereby guaranteeing the reliability and credibility of IoT systems. Newly developed methods range from using cryptocoin-like authentication where the nodes earn coins by verifying the messages on the network and get authenticated after earning enough coins [60] to using hash functions [61] that are lighter than other approaches. Moreover, in the literature, there are also studies that utilize the public key cryptography and elliptic curve algorithm [99].

In common sense, there are three requirements that an IoT system should fulfill to be referred to as secure. These requirements are also known as the CIA triad. In recent years, there have been significant advances in the development of security mechanisms for IoT ecosystems. These methods range from traditional access control models that use id-password pairs with

some additional layers as detailed in [100–103] to more advanced techniques such as the method that utilizes Reinforcement Learning (RL) [104].

Authentication is the procedure of recognizing users and nodes inside a network and authorizing access exclusively to authorized users and unaltered nodes. As stated in [105], authentication remains the predominant approach for access control and management, accounting for approximately 60% of all studies. It is a crucial part of security inside the IoT ecosystem. Authentication provides nodes with the assurance of the identity of the entities they are linked to. Having a master authority for authentication and trust management ensures a strong level of privacy and security in the network. Numerous research in the literature have been conducted on this particular form of authentication, which will be further upon in the subsequent paragraphs. Nevertheless, the primary governing body, which has the potential to become the sole weak link in the network and the central focus of security, also presents a significant risk. Due of the inability of any node to consistently supply connectivity, this method is not feasible in dispersed, decentralized, or large-scale ad-hoc networks. However, the master authority, which may serve as the network's single point of failure (SPoF) and the focal point of security, raises a serious concern too. Since no node can provide connectivity at all times, this strategy is not a viable option in a distributed, decentralized or large-scale ad-hoc networks.

In the literature, Transport Layer Security (TLS)-based solutions for IoT authentication were proposed in [106] and [107]. In these studies, Public Key Infrastructure (PKI)-provided certificates were employed. While these techniques do provide for secure data transmission and dependable authentication, the Rivest Shamir Adleman (RSA) and other asymmetric algorithms inherently necessitate a substantial investment of time and energy to carry out [108]. To address energy consumption concerns, a combination of Datagram TLS and Constrained Application Protocol (CoAP) [109] with the use of Elliptic Curve (EC) [110] was implemented [111]. The system's flexibility was reduced by the need for the root Certification Authority (CA).

In addition to the aforementioned investigations, a method based on a Pre-Shared Key (PSK)

and utilizing a One-Time Password (OTP) mechanism was suggested in the literature [112]. In order to achieve mutual authentication, the proposal necessitates the exchange of four messages between nodes. Furthermore, the Galois/Counter Mode (GCM) was developed as a way to ensure both the secrecy and integrity of data while using the Advanced Encryption Standard (AES) with Counter Cipher Block Chaining (CBC)-MAC modes of operation. This approach was implemented in order to provide a higher level of security for data protection [113].

The aforementioned solutions have shown to be reliable and efficient in terms of energy. The mobility of nodes is constrained by the distribution of PSKs, which is an impractical assumption for real-world scenarios. In addition, conventional protocols depend on Trusted Third Party (TTP) implementations, which render them vulnerable to Single Point of Failure (SPoF) [59].

In the ever-changing realm of IoT security, conventional authentication methods like single-factor identification employing ID-password combinations have been generally acknowledged as susceptible to identity theft and other security breaches. Although these strategies are widely used, they typically fail to adequately protect network resources from advanced threats. Researchers, such as Das et al. [100], have investigated improved protocols and put forth a two-factor authentication method that necessitates the use of both a password and a smart card. This system employs techniques similar to Elliptic Curve Cryptography (ECC), a widely used technology in blockchain applications, for the encryption and decryption of messages. While this approach represented progress, it was not completely resilient to security attacks. Nonetheless, it represented a noteworthy advancement in the sector.

Subsequent studies have sought to enhance these security methods even more. An example of an enhanced two-factor authentication technique was provided, which utilized sophisticated encryption algorithms based on ECC [101]. Researchers such as Li et al. [102] and Wang et al. [103] have recently suggested three-factor authentication techniques that combine ECC with fuzzy commitment schemes and the RSA cryptosystem, respectively. However, the

progress made in these areas was hindered by the significant storage requirements of IoT nodes and the weaknesses found in their local storage systems.

Cui et al. suggested a hierarchical identity management system for multi-Wireless Sensor Networks (WSNs) that is powered by blockchain technology. The purpose of this system is to investigate decentralized solutions. This approach utilized a reliable Base Station that functioned as a subnet manager. Although this facilitated network management, it compromised the decentralized character of blockchain by introducing potential vulnerabilities and single points of failure (SPoF) similar to prior implementations.

Chen et al. [114] extended the use of blockchain technology in wireless sensor networks (WSNs) by developing a Trust Relationship Graph (TRG) to improve network security against worm assaults. Their authentication technique, known as Blockchain-empowered Authentication technique (BAS), utilized a combination of linear blockchain and Directed Acyclic Graph (DAG) chain architectures to securely store and manage the identity authentication information of nodes. The trust levels are adjusted dynamically based on transaction histories and network feedback, showcasing a lightweight and efficient implementation of blockchain that is well-suited for contexts with limited resources.

A blockchain method is introduced to overcome limitations in node-centric WSN designs [60]. The authors emphasized the limitations of sensors' resources and asserted that blockchain offers a decentralized and safe alternative. Their solution incorporated a Hardware Authenticator (HA) that streamlined the encryption and authentication of network connections by integrating various control processes. However, this system had difficulties in terms of decentralization and vulnerability to specific sites of failure.

Tu et al. [104] conducted a study on impersonation attacks in fog computing by utilizing a Q-learning technique. The system detected potential security breaches by identifying anomalous user behavior. This approach employed the simulation of authentic user actions to identify any variations that may suggest impersonation, successfully addressing a crucial vulnerability in fog computing settings.

Mubarakali proposed employing blockchain and cryptographic hash functions to authenticate users and prevent replay attacks, a common occurrence in IoT applications [61]. The objective of this method is to optimize computational efficiency while also safeguarding against attackers attempting to replay legitimate transmissions. This is achieved by integrating distinct sequence numbers into every message.

Jerbi et al. [99] devised a blockchain-based authentication technique for WSNs that employs mobile data collectors, such as drones, to securely collect and send data across geographically distributed networks. This system efficiently managed the processes of registration, identification verification, and credential upgrades for mobile collectors. It ensured the safe and reliable transmission of data to the cloud and offered a dependable method for generating new credentials in the event of a security compromise.

It has been observed that many studies in the literature such as [61] and [133] make use of different types of nodes, which are mainly base stations (either static or mobile), coordinator nodes (like cluster heads in WSNs), and ordinary nodes (as leaf nodes or sensor nodes of WSNs). These node types are depicted in Figure 3.2, which is a comparable model proposed by [133] and adapted for sidechain visualizations. The initial chain in the concept is formed at the cluster level, where IoT devices are grouped together and roughly indicated in size using circles. Each network (NET) generates a second-level chain between its coordinators and the mobile base station. Additionally, each cluster has its own local chain connecting the indicated coordinator and its member nodes. Often, the second level chain is sufficient to verify the identity of a node within a single NET. However, an IoT ecosystem may include a number of linked networks, allowing for the creation of various degrees of sidechains based on the needs. In some systems, utilization of local chains, sometimes referred to as side chains, correspond to a cluster. Base stations initialize and maintain the local blockchain. Leaf nodes join the local blockchain and system end users communicate with them through the global blockchain. Cluster heads (coordinators) are utilized mainly for forwarding purposes and they are authenticated by the global blockchain as described in [59]. On the other hand, some other studies like [60] utilize fog computing or employs a Hardware Authenticator (HA). The system is assumed to be secure since it is offline. HA carries out

Table 3.1 Common and discriminating futures of reviewed research.

Study	Mechanism	Architecture	Sidechains	Policies
Das et al. [100]	Authentication	Traditional	No	No
Das et al. [101]	Authentication	Traditional	No	No
Li et al. [102]	Authentication	Traditional	No	No
Wang et al. [103]	Authentication	Traditional	No	No
Cui et al. [59]	Authentication	Hierarchical	Yes	No
Lau et al. [60]	Authentication, Authorization	Hybrid	No	No
Mubarakali [61]	Authentication, Authorization	Hybrid	Yes	No
Jerbi et al. [99]	Authentication, Authorization	Hybrid	No	No
Esposito et al. [52]	Through Policies	Not Categorized	No	Yes
Putra et al. [54]	Through Policies	Not Categorized	Yes	Yes
Chen et al. [55]	Through Policies	Not Categorized	No	Yes
Liu et al. [56]	Through Policies	No	No	Capability Based
Ismail et al. [115]	Authentication	Hierarchical	Yes	No
Milne et al. [116]	Authentication	Hybrid	No	No
Chen et al. [114]	Authentication	Hierarchical	No	Yes
Hammi et al. [117]	Authentication	Hybrid	No	Yes
Hammi et al. [118]	Authentication	Not Categorized	No	Yes
Velmurugadass et al. [119]	Authentication	Hierarchical	No	No
Jung et al. [120]	Through Server	Hybrid	No	No
Feng et al. [121]	Authentication	Hierarchical	No	No
Christo et al. [122]	Authentication	Hierarchical	No	No
Adil et al. [123]	Through Policies	Hierarchical	No	Yes
Maimoona et al. [124]	Authentication	Not Categorized	No	Yes
Fotohi et al. [125]	Authentication	Not Categorized	No	Yes
Asare et al. [126]	Authentication	Hybrid	No	No
Sharma et al. [127]	Authentication	Hybrid	No	No
Moinet et al. [128]	Authentication	Not Categorized	No	No
Lewison and Corella [129]	Authentication	Hybrid	No	No
Hakak et al. [130]	Authentication	Hierarchical	No	No
Goyat et al. [131]	Through Policies	Hybrid	No	Yes
Pan et al. [132]	Through Policies	Hierarchical	No	Yes

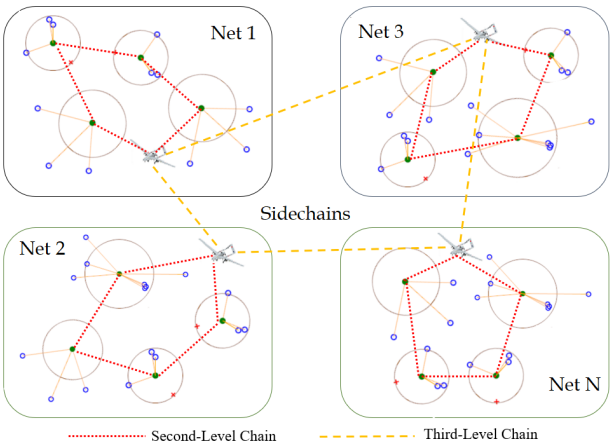

Figure 3.2 Node types and various levels of chains

the authentication process by coin delivery and nodes, having a copy of the blockchain, can compute which node has how many coins. If a node is deemed having enough coins, they are respected as authenticated.

Fog computing systems are found to be prone to impersonation attacks and some studies like [104] tries to address the issue. According to the study, Physical Layer Security (PLS) is mostly not considered for securing fog computing environment, and they are the first to consider PLS security through Q-Learning. These studies exemplify the ongoing endeavor to establish increasingly secure, efficient, and resilient settings for the IoT and Wireless Sensor Network (WSN). They achieve this by utilizing contemporary cryptographic and blockchain technology to address the complex issues of IoT security.

In summary, this analysis examines the related studies for IoT security considering four perspectives; mechanisms, architecture, sidechains and policies. The common and discriminating features of reviewed research are depicted in Table 3.1.

3.3. Comparison of Proposed Framework

Upon careful analysis, it is evident that blockchain technology primarily facilitates goals such as improving data accuracy, strengthening system resilience, and promoting scalability across diverse industries. Additionally, it emphasizes the benefits of decentralized and secure

systems that can easily adjust to intricate network operations, such as those encountered in aviation and IoT settings.

In previous sections several issues are addressed in current blockchain frameworks, including in the areas of scalability, security, and adaptation in complex network contexts such as those involving aviation, UAV and IoT domains. To address the aforementioned issues we developed a framework which details are given in Section 4. to handle these problems comprehensively. The remaining section provides a thorough analysis and assessment of the studies discussed in the preceding portion.

The evaluation of these studies was conducted by considering factors such as the *solution domain, layered structure, cluster methodology, storage capacity, access management capabilities, testbed applicability, and preservation of secrecy*. The findings of this methodical examination of literature, which offer a methodical comparison of relevant studies, are arranged in Table 3.2. This table presents a comprehensive evaluation of the suggested framework and additional research, emphasizing their degree of appropriateness or inadequacy. The abbreviation ”N/A” (Not Available) is used when a circumstance does not apply. Upon doing a comprehensive examination, it becomes clear that blockchain technology consistently facilitates the objectives of enhancing data precision, fortifying system robustness, and fostering scalability across diverse industries. These studies provide evidence for the concept of decentralized and secure systems that can adapt to the intricacies of modern networks, such as the complicated operations of aviation and the extensive networks of the IoT.

Table 3.2 A comparison of similar studies in the literature.

Paper	Solution Domain	Layer	Cluster Methodology	Storage Ability	Access Management Ability	Test Bed Applicability	Secrecy-Preserving
Proposed Framework	Aviation	Blockchain, Data management, Access management, Link, Presentation	Inter-cluster, Intra cluster, Hybrid	On-chain, Off-chain (proof On-chain), Requested Data	RBAC	YES	PKI, Offloading data, ACL
[48]	Aviation	N/A	N/A	Off-chain (local, cloud, proof On-chain)	RBAC	N/A	Zero-Knowledge Proofs
[93]	Aviation	N/A	N/A	On-chain	PKI	N/A	N/A
[134]	Aviation	N/A	N/A	On-chain	PKI	N/A	N/A
[135]	Aviation	N/A	N/A	On-chain	N/A	N/A	N/A
[136]	Healthcare	Application, Control, Infrastructure	N/A	On-chain	PBAC	YES	PKI
[137]	Healthcare	N/A	N/A	Off-chain (proof On-chain)	ACL	N/A	PKI
[138]	Healthcare	N/A	N/A	Off-chain (cloud, proof On-chain)	ACL	N/A	Zero-Knowledge Proofs
[139]	Supply Chain	Perception, Blockchain, Application, User	N/A	On-chain	ACL	N/A	PKI
[140]	Supply Chain	N/A	Global and Local	N/A	ABAC	N/A	N/A
[141]	IoT	N/A	N/A	Off-chain (proof On-chain)	RBAC	N/A	N/A
[142]	Industry	Perception, Off-chain, Blockchain, Application, Service	N/A	Off-chain (proof On-chain)	N/A	YES	PKI
[143]	Smart Cities	Detection, Security, Communication, Link	N/A	Off-chain(IPFS)	PBAC	N/A	N/A

Upon thorough review of the tabulated data, the ”Proposed Framework” is a strong and all-encompassing strategy for leveraging blockchain technology, particularly in the aviation sector. This paper presents a comprehensive technique that covers various aspects of system architecture, such as blockchain, data management, access management, networking, and display layers, in contrast to other scholarly contributions of the same time period. This integrative approach sets itself apart from other research in the study by consistently having a wider scope, covering various architectural levels, and demonstrating greater precision.

The ”Proposed Framework” demonstrates its methodological sophistication by employing inter-cluster, intra-cluster, and hybrid clustering methodologies, setting it apart from comparable studies that lack detailed study of data segregation and network management. This advanced method showcases improved efficiency and capability in managing larger workloads, so addressing a significant shortcoming in research. Furthermore, it utilizes a hybrid storage approach that combines on-chain, off-chain, and selectively requested data storage methods. This sophisticated approach sets itself apart from the primarily on-chain storage options identified in prior studies, thereby enhancing both the availability and integrity of data. This cutting-edge storage solution exceeds current systems by providing a customized method that can adapt to different data needs.

Regarding access management, the majority of the surveyed research, including our proposed framework, utilize Role-Based Access Control (RBAC). Furthermore, it enhances its usefulness by including Public Key Infrastructure (PKI) and Access Control Lists (ACLs). This demonstrates a dedication to creating several levels of security protocols, greatly improving the system’s ability to resist illegal entry. In addition, the ”Proposed Framework” stands out for its practical validation achieved by establishing a test bed, a characteristic that has not been clearly explained in previous studies. This empirical evidence showcases the efficacy of the subject in practical scenarios, a factor that is occasionally absent in theoretical research.

The design incorporates many strategies such as Public Key Infrastructure (PKI), data offloading, and Access Control Lists (ACLs) to prioritize the safeguarding of confidentiality

and data privacy. This approach sets itself apart from and exceeds earlier methodologies, such as Zero-Knowledge Proofs, by utilizing a more varied manner to ensure anonymity.

A thorough and sophisticated approach is introduced in Section 4. for utilizing blockchain technology in many industries, with a specific focus on the aviation sector, IoT, and UAVs. The system is distinguished by its comprehensive system design, sophisticated storage solutions, improved access control, empirical validation, and strong privacy safeguards. This research makes a significant contribution to the existing literature and fills gaps in information that were previously there. It showcases the system's preparedness for practical application and its capacity for scalability in real-world situations, indicating notable advancements in blockchain technology.

The proposed framework offers solutions by improving scalability, securing data, enhancing flexibility. Through a systematic approach to these concerns, the suggested framework not only resolves the challenges described in previous research but also enhances the utilization of blockchain technology in specific fields. This comparative research showcases the framework's capacity to enhance the shortcomings of prior studies, providing a strong, adaptable, and reliable solution specifically designed for the intricate requirements of contemporary networked systems.

4. METHODOLOGY

This section outlines the modular architecture of the proposed framework for managing data and implementing a blockchain. The blockchain is designed to securely store and retrieve specific data while ensuring confidentiality, availability, and integrity.

The primary factors influencing the framework's structure are given in Figure 4.1:

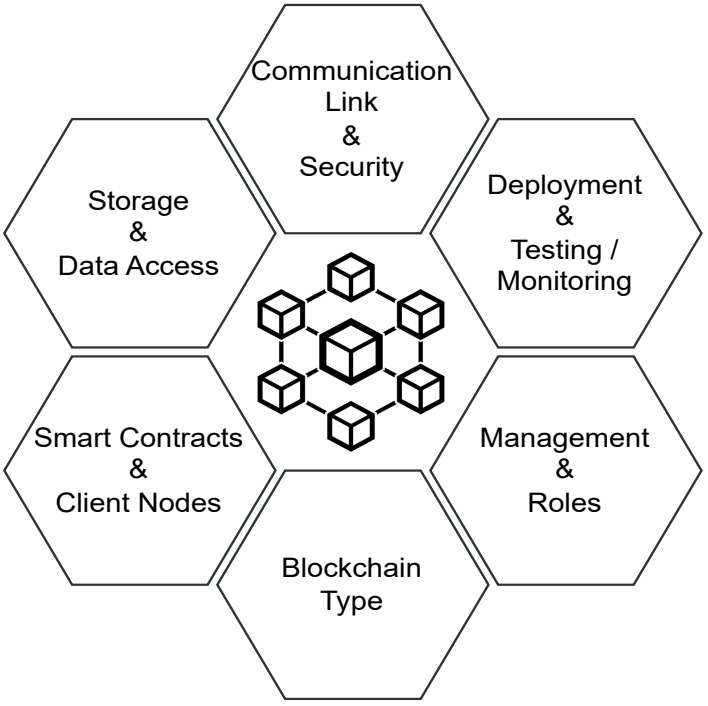

Figure 4.1 Main features that affect the structure of a framework.

The design of the contract creation, blockchain technology, management of external data requests, and storage systems employed ensures that they function as separate and easily interchangeable components. This customizable framework intends to provide flexibility, scalability, and support for applications utilizing various technologies and protocols.

Data management can be viewed as a less intrusive utilization of real-time and permanent records. Hence, for the purpose of storing and updating the data, it is necessary to maintain a clear distinction between the node communicating with the base station and the intermediate node. To clarify, the blockchain database (BCdb) will be divided into two distinct categories:

inter-cluster (I_eC) and intra-cluster (I_aC). The subsequent sections provide information that I_eC contains shared data for all participant nodes, whereas I_aC contains data specific to the cluster. It is advisable to explore alternative concepts due to the isolated nature of the data in the node systems, which are not susceptible to external interference. Additionally, there is a constant possibility of environmental factors leading to a decline in communication quality between the base station and the node. According to literature, the primary requirement is a distributed database that manages data, partners, roles, and identity. Additionally, there is a need for sharing, mutual agreement, autonomous or semi-autonomous decision-making, monitoring, and a reliable communication link between different protocols and devices.

The proposed technique entails the partitioning of the system's organization into numerous tiers, resulting in the formation of a stratified structure. Each layer is allocated unique responsibilities for various operations. The aforementioned design technique has several benefits, including the allocation of duties, efficient job management across different levels, and the flexibility to improve or modify one layer without affecting the others. There are multiple significant rationales for using a layered architecture in this framework:

- The principle of **separation of concerns** is accomplished by layering, which allows for the division of different components of blockchain functionality into distinct tiers, ensuring that each layer has a specialized and clearly defined job. For example, you may have separate layers particularly designated for the fundamental components of blockchain, storing data, managing access, and creating user interfaces or applications. This segmentation simplifies the overall organization and makes it easier to understand and maintain.

- **Modularity and scalability** are attained by allowing the autonomous development and change of each layer, separate from the others. The system's modularity enables seamless scalability, as new features or improvements may be integrated into a single layer without affecting the underlying blockchain base. Adaptability is crucial in the rapidly evolving field of blockchain technology, where frequent new requests and improvements may arise.

- The independent functioning of each layer significantly streamlines the process of maintaining and upgrading, resulting in **simplified maintenance and upgrades**. Modifications made to one layer do not always require changes to other layers, thus reducing the possibility of unforeseen outcomes. The convenience of maintenance is particularly advantageous for addressing security vulnerabilities, creating enhancements in performance, or introducing novel functionalities.

- **Interoperability** is improved by implementing a layered architecture, provided that the interfaces between the layers are clearly documented. This allows for the integration of external components or the replacement of specific levels with alternative implementations without causing any disturbance to the entire system. An effective development workflow is supported by a hierarchical structure, enabling developers to focus on each layer in a sequential manner. This promotes a systematic and organized approach to the development process, improving its effectiveness and decreasing the probability of mistakes.

In summary, a blockchain framework that incorporates a layered structure offers advantages in terms of separating roles, implementing a modular architecture, achieving scalability, coordinating tasks, maintaining the system, and ensuring compatibility. These benefits jointly improve the durability and adaptability of the blockchain system, allowing for both initial development and ongoing improvements.

Implementing a layered architecture is essential in building a blockchain framework because of the frequent introduction of new advancements and the requirement for ongoing enhancement. The design should possess adaptability, enabling the incorporation of novel functionalities and seamless assimilation of emerging technologies. The significance of a hierarchical arrangement in a blockchain framework, particularly when it is being introduced for the first time, cannot be overemphasized.

The selected layered architecture for the proposed blockchain-based framework conforms to the prevailing academic and practical agreement on organizing blockchain systems to tackle

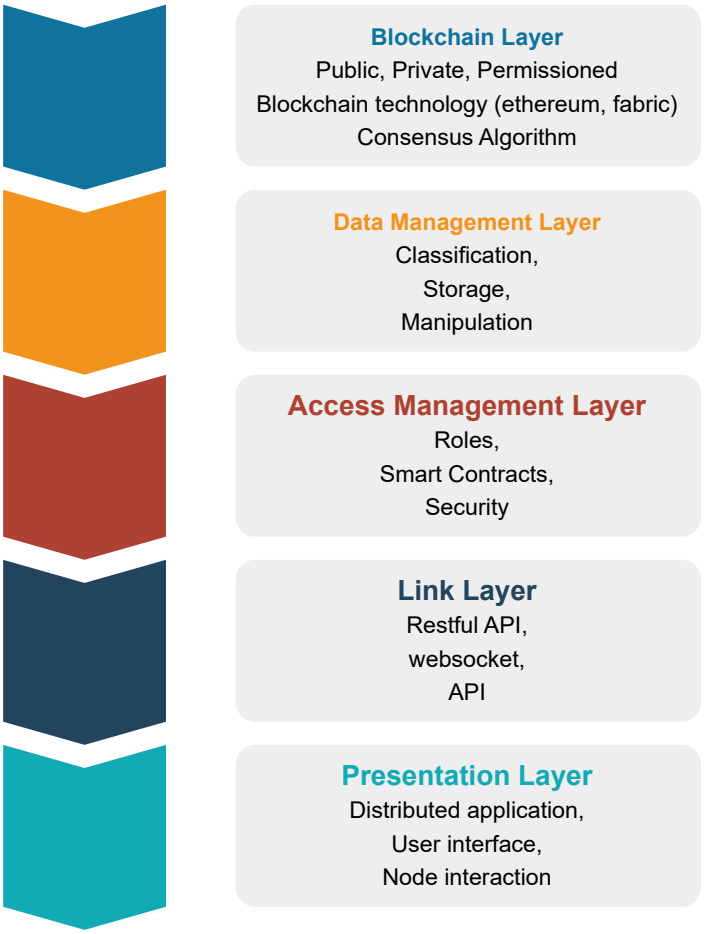

Figure 4.2 Proposed framework layer structure.

issues of scalability, security, privacy, and efficiency in data management. The selection of blockchain, data management, access management, connection, and display layers in this method is designed to address the specific functional requirements and challenges of distributed data management systems, as depicted in Figure 4.2. The application of clustering to delineate network segments, hybrid evolutionary algorithms for optimization, and strategic stacking for managing data, access, and interactions showcases the advanced integration of blockchain technology to fulfill intricate system needs. The chosen criteria in the proposed framework are essential for creating a robust, flexible, and secure blockchain-powered data management system. The framework's versatility in accommodating many issue areas is assisted by crucial elements such as contract generation, blockchain technology, management of external data requests, and storage systems. They allow for customization according

to specific needs, guaranteeing the adaptability and expandability of the framework. This method facilitates the integration of several technologies and protocols, enabling a less invasive consumption of data with secure and efficient storage and updating procedures. The modular design enables effortless adaptation and integration, rendering the framework valuable in diverse applications and environments.

The blockchain layer is crucial in ensuring the security and reliability of the system. It accomplishes this by selecting the appropriate type of blockchain (public, private, permissioned), consensus mechanisms, and underlying technologies (such as Ethereum, Hyperledger, etc.). Deciding between public, private, and permissioned blockchains enables the creation of tailored solutions that find a middle ground between transparency and control, based on specific domain needs for accessibility and privacy. Ethereum offers a robust framework for decentralized applications with its smart contract functionality, but Hyperledger excels in regulated enterprise environments that prioritize privacy and efficiency [144]. Consensus methods for example PoW, PoS, and Delegated Proof of Stake (DPoS) play a crucial role in guaranteeing the security, integrity, and efficiency of the blockchain. Choosing the correct algorithm is essential for guaranteeing the effectiveness and dependability of the system. The data management layer plays a vital role in managing data through organization, storage, and processing, while also addressing scalability and efficiency concerns. To achieve a balance between immutability and scalability in large-scale deployments, the system employs data categorization and utilizes many storage mechanisms, including both on-chain and off-chain approaches, to handle significant amounts of data.Provide a citation for an in-book source. Evolutionary clustering in IoT contexts use techniques to improve data management and network efficiency. By prioritizing the roles and smart contracts in the access management layer, we ensure that access control is both secure and adaptable to changing requirements. This pertains to the requirement for comprehensive access controls in domains like healthcare and IoT, where the obligations and authorizations of users must be meticulously managed to safeguard confidential information. The link layer addresses the practical challenges of network interoperability and connectivity in distributed systems by enabling communication between

diverse nodes. The blockchain framework can establish effective contact with other systems and devices by utilizing technologies such as RESTful APIs and WebSockets. This capability is crucial for IoT applications that necessitate efficient communication across diverse devices. The presentation layer serves as an intermediary between the blockchain system and users, ensuring that the benefits of the blockchain are readily accessible to end-users through user-friendly interfaces and distributed applications. Active user participation is essential in domains like healthcare, as it has a significant impact on the overall efficacy of the system.

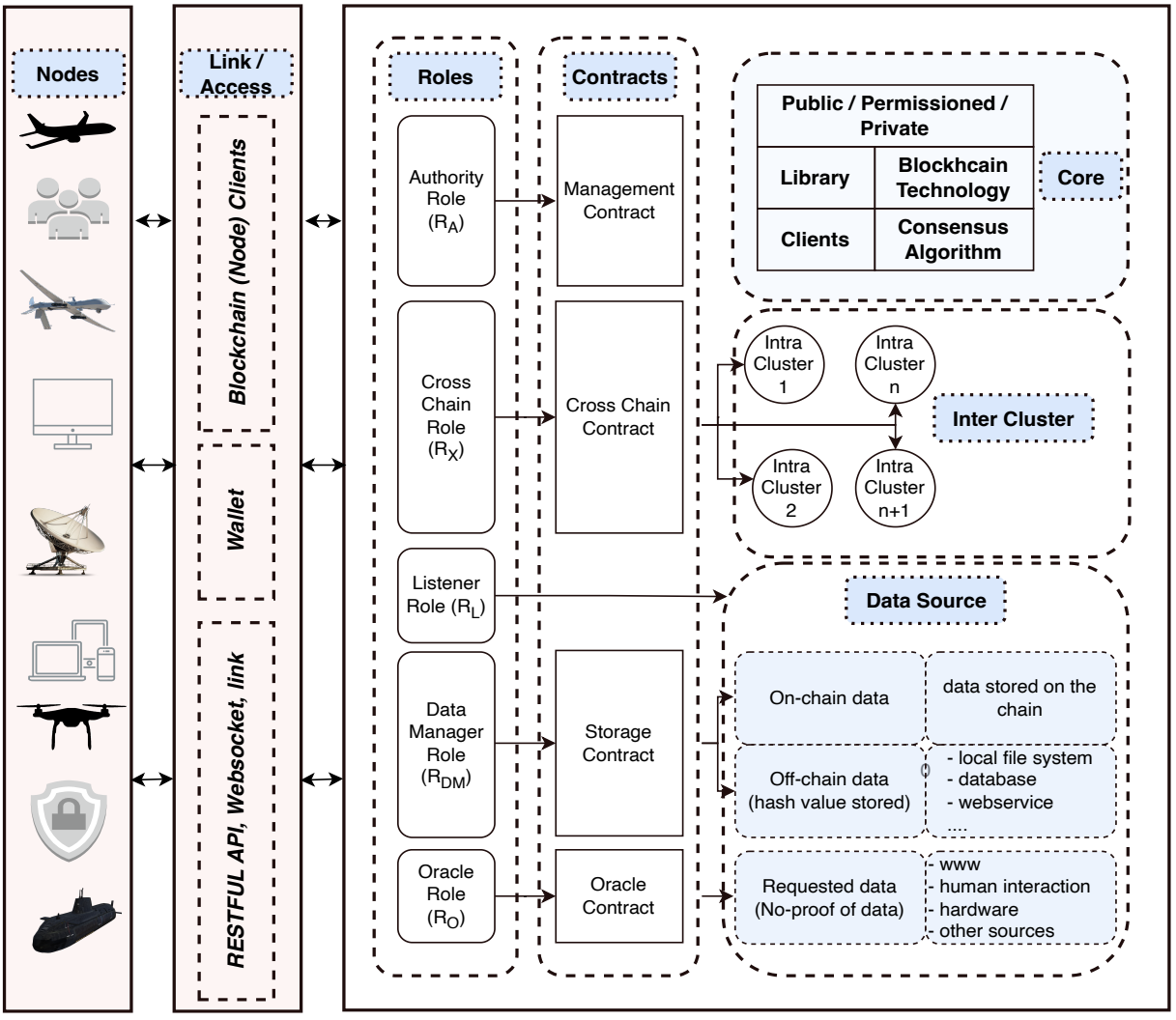

Figure 4.3 Modular architecture of the proposed framework.

In order to provide a description of the architecture of the proposed framework, as depicted in Figure 4.3, we will first discuss the structure of clusters, nodes, and roles. Next, the concept

of managed data is thoroughly explained. Subsequently, the contracts pertaining to design and security considerations are explained in detail.

4.1. Structure of Clusters, Nodes, and Roles

The blockchain network is specifically intended to facilitate both inter-cluster (I_eC) and intra-cluster (I_aC) operations, hence enhancing its adaptability. The I_eC functions as the primary data storage and acts as a central communication hub, facilitating connectivity amongst all participants. This framework is distinct from the intra-cluster model, I_aC, as it operates according to its own specific rules and structures that are tailored to meet its particular requirements.

The inter-cluster communication is essential for enabling effective connectivity between different intra-cluster entities , hence connecting numerous clusters. By dividing into inter and intra-clusters, it becomes possible to employ distinct blockchain technology and consensus algorithms that are customized to meet the individual needs of each cluster. A diverse range of blockchain technologies, each possessing unique capabilities, limitations, and strengths, need an adaptable approach. The I_eC and I_aC architecture assists in selecting blockchain solutions that align with the specific objectives of each cluster.

Moreover, the I_eC plays a vital role in minimizing potential delays in data transmission and database expansion caused by substantial data exchanges within the I_aC network. The integrity and immutability of data across the network are guaranteed by the I_eC by storing general-purpose data and preserving hash values of processed data within I_aCs.

The I_aC is designed to be adaptable, enabling the use of various consensus methods and blockchain technologies based on structural needs. To participate in or join the I_eC, it is necessary to adhere to the specified norms and procedures of the I_eC. This architecture ensures that the I_aCs have the ability to operate independently and preserves the integrity of the network by confining data proofs to the I_aCs in the I_eC. This method emphasizes the commitment to maintaining data accuracy throughout the clusters, showcasing the

framework's ability to fulfill diverse technological needs while yet maintaining centralized network management.

4.1.1. Inter-Cluster (I_eC) Architecture

The I_eC blockchain determines the common data for all nodes and provides an immutability proof (hash) of the I_aC data. The architecture facilitates the participation of I_eC as a communication bus between I_aCs, while also serving as the primary chain for the framework. The I_eC chain stores and updates often requested and general-purpose data that is needed by all nodes. The generation of the Common Operational Picture (COP) and Recognized Air Picture (RAP) is used to visually represent the data stored in I_eC. Aircraft, UAVs, IoTs, and other nodes, such as ground stations and base stations, have the responsibility of supplying navigational data to establish a Common Operational Picture (COP) or a Recognized Air Picture (RAP). Furthermore, any node that engages in the blockchain and functions in different branches can exchange relevant navigational data with the aircraft or any other node within the communication range. Currently, a subset of the data collected by the accountable I_aC is transferred to I_eC, where it is consolidated to retain the comprehensive view of COP or RAP.

4.1.2. Intra-Cluster (I_aC) Architecture

To effectively meet a wide range of operational requirements, it is essential to prioritize both flexibility and specificity. Each individual I_aC inside the system has the autonomy to tailor its consensus process according to its own aims, hence improving efficacy and adaptability. The I_aC framework enables customers to to decide on the most appropriate blockchain technology for their specific requirements, providing a customized approach to data management and security. The cluster I_aC possesses the ability to independently develop its own technology and implement regulations inside a separate framework from I_eC. While I_aC operates autonomously within its cluster, data processed in I_aC can be stored in I_eC to ensure data integrity, even while I_eC governs the cluster separately.

The I_aC chain is characterized by nodes that possess an equal amount of connectedness, creating a swarm-like environment. These nodes establish their own set of rules. The I_aC nodes and cluster rules may differ from the I_eC chain they are part of in terms of the consensus algorithm, blockchain technology, and other utilized technologies. By adopting this approach, the process of cluster creation can be orchestrated with greater adaptability and modularity. For example, military UAVs flying in groups and ground support units can create an interconnected network with faster and reliable nodes by using a limited quantity of validators or signers. However, a different interconnected network that operates in a challenging and hostile environment can utilize fully Byzantine Fault Tolerance (BFT) consensus algorithms to enhance trust, even if the rate of transaction processing decreases.

4.1.3. Communication Between Clusters

Each integrated circuit (IC) can be fabricated using a range of technologies. In a microservice architecture, we build connectivity between clusters by utilizing web sockets and RESTful APIs. This architectural choice facilitates efficient, scalable, and flexible communication between clusters. An I_aC node can engage in I_eC by utilizing a specialized connection adaptor designed for I_eC. Each node within a I_aC is possesses the capacity of establishing a connection with nodes in different clusters. However, often only one node is selected per cluster to handle this inter-cluster communication. The decision is determined by criteria for instance energy efficiency and the desire to minimize complexity, especially in applications like swarm flights.

Every I_aC contains a node that is responsible for maintaining communication with the I_eC. Otherwise, it forms its inter-cluster architecture and lacks a comprehensive verification of the data. There are three methods for doing data request or push:

- From inter-cluster to intra-cluster ($I_eC \longrightarrow I_aC$): This method entails transferring data from the inter-cluster network to a designated intra-cluster, enabling external data to be inputted into a cluster.

- From intra-cluster to inter-cluster ($I_aC \longrightarrow I_eC$): This entails transmitting data from an intra-cluster to the inter-cluster network, enabling a cluster to share its data with other clusters.

- Between intra-clusters through inter-cluster ($I_aC \longrightarrow I_eC \longrightarrow I_aC$): This technology enables data transmission between two intra-clusters via the inter-cluster network, enhancing communication between distinct clusters.

The desired data from the IoT devices and the orders sent by the governing bodies of the IoT are carried out on the nodes equipped with IoT adapters. Simultaneously, the data transmitted from the I_eC is transmitted in the I_aC due to necessity or the law of blockchain. Therefore, communication between different I_aCs is done via the I_eC chain as illustrated in Figure 4.4.

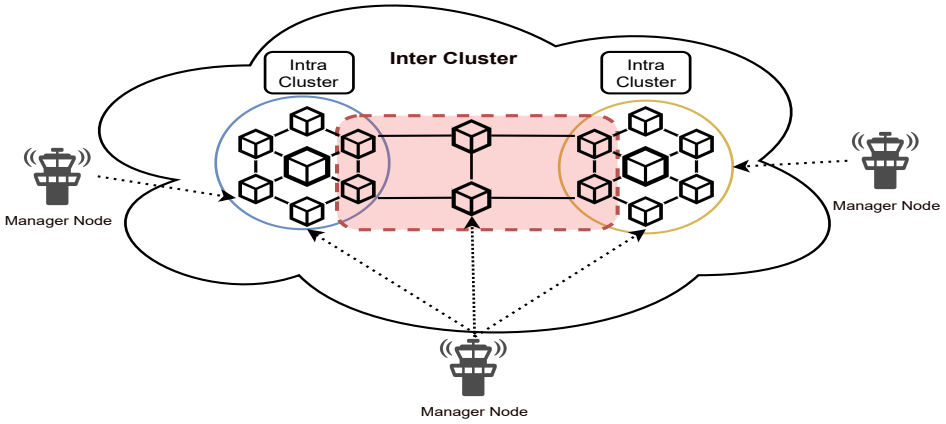

Figure 4.4 Communication between I_aCs through I_eC.

4.1.4. Node and Role Architecture

Nodes are divided into two as their involvement: Inter-cluster node (I_eC) and intra-cluster node (I_aC). Each node can have several roles: authority role (R_A), data manager role (R_{DM}), listener role (R_L), cross-chain role (R_X), and Oracle role (R_O). A summary of the roles that can be held by nodes is given in Table 4.1.

Table 4.1 I_aC and I_eC node roles.

	I_aC	I_aC and I_eC	I_eC
Authority Role (R_A)	✓	✓	✓
Data Manager Role (R_{DM})	✓	✓	✓
Listener Role (R_L)	✓	✓	✓
Oracle Role (R_O)	✓	✓	✓
Cross-chain Role (R_X)	X	✓	✓

4.1.4.1. Authority Role (R_A) : Responsible for managing the data, communication, and contracts both in inter or intra-cluster domains.

4.1.4.2. Data Manager Role (R_{DM}) : Responsible for storing and updating data as well as managing access to requested data.

4.1.4.3. Listener Role (R_L) : Solely listens to the blockchain for changes. In this role, a node does not have any privilege to update the state of the blockchain.

4.1.4.4. Cross-chain Role (R_X) : Responsible for preserving communication links among intra and inter-cluster chains.

4.1.4.5. Oracle Role (R_O) : Responsible for populating the requested untrusted off-chain data to nodes. Subscribes to Oracle contract, gets requested data and responses back. Can either be in an intra-cluster or inter-cluster chain.

4.1.4.6. Inter-cluster node (I_eC) : A node is a member of I_eC chain can have one or more of the listed roles: cross-chain (I_eC-X), authority (I_eC-A), data manager(I_eC-DM), Oracle (I_eC-O) and listener (I_eC-L).

4.1.4.7. Intra-cluster node (I_aC) : Communication between custom local chain except I_eC nodes takes part in here. Permissioned and private also customizable blockchain for

purpose can be deployed. Crosschain (I_aC-X), oracle (I_aC-O), authority (I_aC-A), data manager (I_aC-DM) ve listener (I_aC-L) roles can be obtained by the I_aC nodes.

4.2. Data Management

The data being considered differ in terms of the frequency of change, size, source, and legitimacy. While the storage of data on a blockchain ensures integrity, availability, and immutability, it comes at a high cost due to its replication across all participants. Hence, it is imperative to categorize the data, particularly in fields that typically have limited resources. Furthermore, through the process of classifying the data, one may accurately ascertain the required storage capacity and frequency of data updates. The approach offered under the classification, storage, and manipulation subsections provides a description of these features.

4.2.1. Categorization

The proposed framework classifies data into three categories: on-chain, off-chain, or requested, depending on factors such as data type, security requirements, and storage needs. On-chain data is consistently available and immutable on the blockchain, making it ideal for storing crucial or sensitive information that may take advantage of decentralized transparency and resistance to tampering. Off-chain data refers to data that is stored externally to the blockchain, while only the data's cryptographic proof is recorded on the network. This is achieved by using external storage systems such as the Inter Planetary File System (IPFS) to enhance scalability and flexibility. The integrity of the data is maintained through validation on the blockchain. This approach is suitable for larger files or supplementary data that does not require visibility on the blockchain. The requested data comprises live data acquired from external sources and is not stored on the blockchain. The integrity and quality of this data are upheld using an Oracle architecture that consolidates and verifies data from reliable sources, ensuring the reliability of external data such as meteorological information or wind speeds.

This approach allows the framework to leverage the benefits of each category, such as the secure and transparent nature of on-chain data, the ability to scale and adapt of off-chain data, and the dynamic characteristics of requested data.

4.2.1.1. On-chain data : The data is consistently accessible and kept immediately on the chain, ensuring its constant availability and updates. The proposed blockchain framework utilizes a dedicated storage contract to store data on the blockchain. This contract serves as a repository for data and establishes protocols for access based on predefined roles, thereby restricting access and modification of the information solely to authorized personnel. Access management is crucial for maintaining the integrity and confidentiality of on-chain data, which remains secure, transparent, and immutable due to its storage on the blockchain. Participants have the ability to query data at any time. This data is both decentralized and immutable, rendering it unalterable once it is stored in the blockchain. This indicates that the data cannot be modified immediately. Updates are managed by the smart contract by the creation of new transactions that incorporate the required alterations. These transactions are appended to the blockchain, creating a verifiable and sequential ledger of data updates. Authorized nodes are the only entities that can store and update on-chain data. In this case, these nodes are participants that own R_{DM}. On-chain data is commonly employed for highly important or confidential information. By storing this data on the blockchain, it guarantees transparency, trustworthiness, and resistance to tampering.

4.2.1.2. Off-chain data : The data is not saved on the blockchain itself, aside from the verification of the data by a hash, that is kept on the blockchain to ensure consistency, immutability, and integrity. Furthermore, off-chain data is considered trustworthy, similar to on-chain data, as the integrity of the data stored on the blockchain can be verified using a straightforward hash validation algorithm. The data is kept in the IPFS, database management system (DBMS), file servers, or other media. To guarantee the reliability of the data, a proof is maintained on the chain. Off-chain data encompasses larger files, metadata, or other information that complements on-chain data. Off-chain data is utilized to alleviate the

storage and processing limitations of the blockchain, while also accommodating data that does not necessitate the same degree of transparency or immutability. The data evidence, represented by a hash, along with the link to the data, is stored on the blockchain under the storage contract in this specific category. The files or information are stored in external or offline storage systems, such as conventional databases.

4.2.1.3. Requested Data: Requested data refers to information that is obtained or received from other sources in real-time as a result of specific searches or user requests. Both the data itself and evidence of the data are not stored on the chain, but rather retrieved when necessary. The main distinction is in the uncertainty surrounding the integrity, correctness, and validity of the data. Given the uncertainty surrounding the requested data, the suggested framework incorporates Oracle architecture to enable the use of non-deterministic requested data in a deterministic blockchain. The Oracle nodes collect the desired data from the relevant sources and utilize a smart contract to conduct a voting process, determining the most accurate data, as depicted in Figure 4.5. The data that is being requested is obtained in real-time from external sources and is not directly stored on the blockchain. Information regarding the retrieval of this data is transmitted on the blockchain, and the specifics can be obtained from query logs.

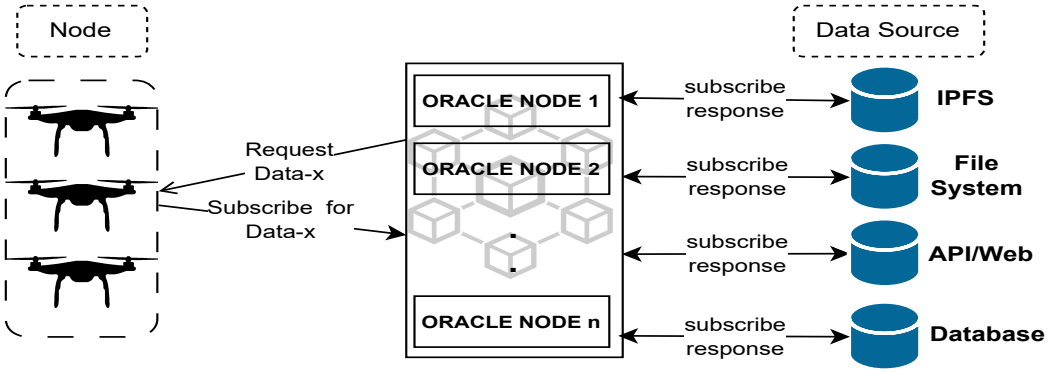

Figure 4.5 Requested data aggregation by Oracle nodes.

4.2.2. Storage

Blockchain systems provide the capability to store data in the form of logs, events, and contracts. Logs are an essential element of blockchain systems, constructed as a sequential series of entries, with each entry representing a distinct event or activity. They offer a clear and unambiguous account of network activity, enabling members to scrutinize and authenticate the sequential arrangement of events. Logs are typically available to all members in the blockchain network. Anyone can retrieve and examine the log entries, promoting transparency and accountability. Events are a more advanced concept that is built upon logs. They allow smart contracts in blockchain systems to interact with each other and inform relevant parties about certain events. Every event is assigned a unique name and can contain a distinct collection of indexed or non-indexed data, providing increased versatility in gathering valuable information. They allow individuals to subscribe to specific events and receive notifications when such events happen. When a smart contract produces an event, a corresponding log entry is generated and stored on the blockchain. Contract storage refers to the enduring storage capacity offered by a smart contract within a blockchain system. Contract storage functions as a key-value store within a smart contract. It allows for the creation and control of variables or data structures that store long-lasting state information. Contract storage is utilized to store and modify the actual state of the contract. It enables the retention of data that needs to be stored over multiple invocations or transactions.

Data is categorized into three forms based on its classification: on-chain storage, off-chain storage, and requested storage (temporary).

4.2.2.1. On-chain storage : On-chain data corresponds to always available and accessible data. This data is stored and updated by $IeCN$-*DMR* who owns R_{DM}. Data can be recorded on the network in the form of logs, events, and contract storage. Logs are an essential element of blockchain systems, constructed as a sequential series of entries, with each entry representing a distinct event or activity. Although querying logs for specific information can be resource-intensive, anybody can download and examine the log entries,

which promotes transparency and accountability. Events are a more advanced concept that is built upon logs. They allow smart contracts in blockchain systems to interact with each other and inform relevant parties about certain events. Querying is a more efficient method compared to logs since each event is assigned a specific name and can contain various indexed or non-indexed data. This enables better adaptability in gathering valuable information. Contract storage refers to the durable storage space offered by a smart contract for storing and modifying the contract's state. It allows for the creation and control of variables or data structures that store long-lasting state information. Storing data in contracts incurs higher costs compared to storing it in logs or events. When there is no need for anonymity, keeping data in logs is a more efficient method that allows for indexing log event topics, even with limitations. However, because to its universal accessibility to all nodes that have access to the blockchain, this approach may not always be preferable. Depending on the conditions, any strategy may be implemented in the approach being presented.

4.2.2.2. Off-chain storage: Blockchain systems acknowledge that it is not necessary to store all data directly on the chain. Blockchain can be utilized to incorporate decentralized file systems or distributed databases in order to manage larger or less often accessible data. These systems employ separate storage for data while leveraging the blockchain for the purposes of validation and verification. Unlike on-chain storage, this type of storage just retains the proof (hash value) of the data and access link information, rather than the complete dataset. The evidence of the data is recorded in either the logs, events, or contract. Put simply, the proof remains on the chain while the actual data is stored off the chain. This data possesses one or more of the following characteristics: high sensitivity, huge size, or rare utilization, which renders it not worth the regular inclusion in the chain's data size.

4.2.2.3. Requested storage : The requested data refers to data which does not exist within the network and is instead held off-chain, without a hash or access data saved on the network. This particular data is inherently different from both on-chain and off-chain data since it is actively acquired from other sources and not stored on the blockchain, as

elaborated in Section 4.2.1.. The Oracle architecture guarantees the integrity and reliability of requested data by employing a consensus mechanism across reliable nodes to authenticate and consolidate the most accurate data. This method ensures the integrity of requested data by eliminating the need for storing hashes directly on the blockchain, hence resolving concerns over data manipulation and alteration. An Oracle contract grants authorized nodes the ability to access and distribute this data, which may be queried and retrieved in any predetermined format.

4.2.3. Manipulation

The inherent decentralization and transparency of blockchain technology provide significant challenges for attackers attempting to modify data undetected. Blockchain systems possess a higher level of resistance against unwanted data manipulation attempts compared to typical centralized databases due to the immutability of past data and the consensus mechanisms employed by blockchains. The suggested framework's fundamental feature is authorization, which guarantees the accuracy and integrity of the data.

Roles serve multiple tasks, with R_{DM} specifically responsible for overseeing the approved alteration of data by nodes. The authorized node responsible for manipulating (inserting, updating, and deleting) the data, whether it is stored on-chain or off-chain, sends the required information through the established contract and guarantees that the data is stored according to its intended purpose.

Cluster nodes can retrieve on-chain data that has been updated by R_DM whenever necessary. When data is modified, the network disseminates the change information through events to minimize the network burden created by nodes that are requesting the necessary data to monitor the change. Consequently, listener nodes observe transmitted data change events to ensure that locally utilized data is updated or that local databases remain current. Nodes may be required to verify their receipt of the data change event in some cases. When R_DM asks for confirmation of a data change event, nodes respond by using contracts.

The process of providing evidence for off-chain data alteration is identical to that of on-chain data. Multiple storage devices can be utilized to store off-chain data copies to distribute the access load evenly. When data that is not stored on the blockchain is stored on other means and the evidence is altered, the blockchain sends out a data proof change event to guarantee that all copies of the data are updated.

4.3. Contracts

Smart contracts are software programs that enable two parties to establish a mutual understanding without the need for a third party's participation. This method allows for agreements to be made without the need for a reliable central point, such as a single authority. The agreed-upon actions can be automatically triggered when specified predetermined circumstances occur.

The contracts have enabled the provision of access management, data management, and communication connectivity, as elaborated in subsequent sections. The diagram in Figure 4.6 illustrates the interaction between contracts and roles. The details are explained below.

4.3.1. Management Contract

This contract is responsible for overseeing and regulating different parts of the system's functioning, primarily managing administrative functionalities and establishing the rules and norms for the entire blockchain network. The management contract defines the tasks, access limitations, and authorizations that any participating node in the blockchain can have, regardless of their status. This contract enables the specification and authorization of nodes that are allowed to access storage based on the data classification. Management contract serves as the primary governing body for decision-making, system configuration, and protocol upgrades. They also establish the responsibilities of various roles in carrying out multiple functions.

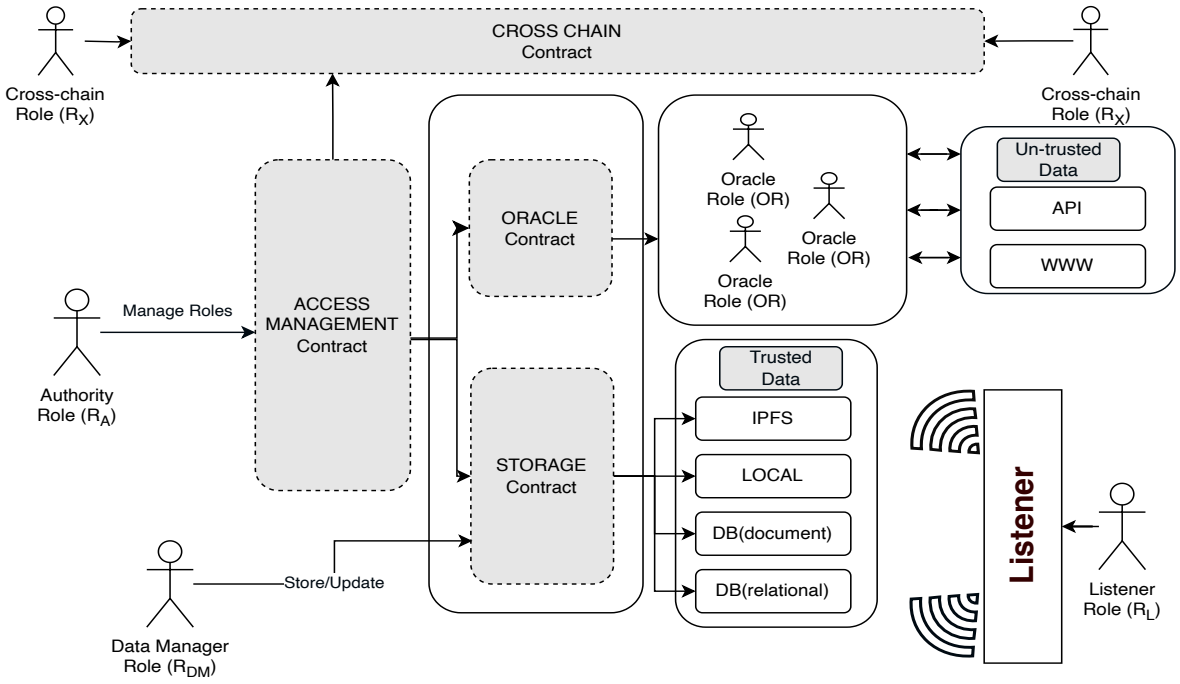

Figure 4.6 Proposed framework contract interaction according to defined roles.

4.3.2. Storage Contract

Storage contracts function as a centralized location for storing essential data and information that must be permanently kept on the blockchain. It guarantees the integrity, accessibility, and immutability of the data, enabling all participants to verify it. The type and structure of the data to be stored here may vary depending on the specific usage requirements. Once a contract has been deployed, it becomes immutable, meaning it cannot be altered. However, there are instances where bug fixes or upgrades may be necessary to address any identified vulnerabilities. Due to the implementation of the storage contract using the proxy contract design, it enables the implementation of necessary modifications or upgrades. The proxy contract pattern enables contract upgrades to occur without requiring a new address. Every instance of storage access must adhere to pre-established regulations.

4.3.3. Oracle Contract

The contract allows Oracle nodes, with roles specified by the management contract, to fulfill incoming data requests. Every Oracle contract request is disseminated to the Oracle nodes. Upon receiving a request, an Oracle node gathers data from multiple sources, then transmits collected data to the Oracle contract to finalize voting in order to ascertain the most precise and accurate response.

4.3.4. Cross-chain Contract

The cross-chain contract facilitates communication between distinct I_aCs and between I_aC and I_eC. The contract stores the address and identity of users for each cluster they are part of. Consequently, nodes possessing the R_X attribute are also part of the clusters they are affiliated with. They have the capability to execute operations and transmit data according to their designated functions inside each cluster.

4.4. Security

This section explores various crucial aspects of blockchain governance. The aspects encompassed are Participation, Authentication, Authorization, Secrecy, Integrity, and Communication Link Security. Authentication is the act of verifying identities to prevent unauthorized access, whereas participation focuses on certifying the legitimacy of individuals. ”Authorization” is the act of verifying that participants have the appropriate permissions, while ”secrecy” refers to the methods of controlling access and encrypting data in a private blockchain setting. The talk ends with Communication Link Security, which prioritizes secure communication methods and encryption to ensure confidentiality. The next topic of discussion is integrity, which refers to the unalterable sequence of blocks. The objective of this concise inquiry is to offer a comprehensive analysis of the significant matters pertaining to the governance of the proposed structure.

4.4.1. Participation

Ensuring the authenticity and integrity of individuals participating in the blockchain network is crucial to prevent unauthorized access and malicious activities. Parameters required for establishing a connection to a restricted private network are not needed for connecting to public networks. A virtual private network (VPN) is a network that facilitates the separation of a private network from others, hence enabling its segregation from other networks. In order to become a part of a private network, a node must go through a process of authentication and have specific values: the network's distinct identifier, the enode address, and the port information. In addition, the *nodiscover* parameter is used to prevent the private network from being detected, while the *net restrict ip list* is used to only allow connection requests from specific IP addresses. To verify the identity of members, digital signatures or public-key infrastructure (PKI) are used to guarantee that only approved entities are able to participate in the network. Administrator nodes are responsible for managing the inclusion of members in a private blockchain.

4.4.2. Authentication

This is a crucial procedure that verifies the identity of persons. It is crucial in thwarting unwanted access and safeguarding against potential scenarios where impersonation attacks may take place. The authentication method for both public and private blockchains is identical, as they both utilize addresses derived from public-key infrastructure (PKI) to provide a user-friendly representation of cryptographic public keys. When a transaction (tx) is being carried out, the sender uses their private key K_{pr} to sign it, and the receiver validates the transaction's authenticity by using the sender's public key K_{pu}. Validating the signed transaction is important to authenticate the sender's address. Administrators commonly have knowledge of the IP addresses of nodes within private networks.

4.4.3. Authorization

This ensures that participants have the necessary permissions and access rights to perform specific tasks within the blockchain network. The management contract is responsible for supervising the distribution and revocation of role grants to ensure appropriate authorization. The allocation of blockchain-defined roles is established by the blockchain authority, although they are typically overseen by role administrators.

4.4.4. Confidentiality

To establish a private blockchain environment, access authorizations are enforced according to specific roles, encryption technologies are employed, and participation rules are established. Authorization systems efficiently limit access to smart contracts and processes, whereas authentication methods authenticate individuals. Permissions are required to access blockchain data, specifically for tasks like as adding or editing data, uploading smart contracts, and activating their functions. While this research does not primarily focus on secrecy, this section does analyze secrecy criteria and how they could be applied in the suggested approach as future work.

Data confidentiality can be guaranteed by employing encryption methodologies or by storing the data outside the main blockchain network. When there is a need for data transparency, unencrypted data might be stored in transaction logs and contract storage. File systems, local systems, or private databases can be utilized as methods for protecting sensitive information. According to the IPFS structure, the suggested framework enables the storing of hash values and access link addresses of data rather than the data itself, hence assuring data security. Since every blockchain node has the capability to read all information shared in the public domain, it is crucial to either keep sensitive data in off-chain storage or in on-chain storage with encryption. Public Key Infrastructure (PKI) encryption necessitates greater data storage capacity in comparison to symmetric key encryption. For the nodes to access the encrypted

data, it is imperative that they exchange the symmetric key. The balance between security and resource allocation is under consideration.

4.4.5. Integrity

Every block is linked to the preceding block by encryption and hashing techniques, resulting in an immutable series of blocks. On-chain storage ensures data integrity using the inherent capabilities of the blockchain, while off-chain storage achieves this manually by conducting a comparison between the hash value recorded and the hash value of the data received. The data integrity level that is desired has not been discussed or considered. The desired data integrity is beyond the scope of this request.

4.4.6. Communication Links

To preserve the confidentiality of the channel, secure communication is ensured through the use of transport layer secure communication protocols. The use of permissioned blockchain restricts attacker access, while the secret data is encrypted before being transmitted. Firewall use and network segmentation are further methods used to guarantee the security of communication channels.

4.5. Thread Model Investigation

The safeguarding component of the proposed design outlines the utilization of the STRIDE threat model, a Microsoft-developed analytical tool [145]. This paradigm classifies security vulnerabilities into six categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. It helps in identifying these vulnerabilities within a system. By employing the STRIDE methodology, one may conduct a comprehensive and diverse assessment of potential vulnerabilities, thereby guaranteeing a thorough examination of both the system's architecture and its operating efficiency.

The STRIDE technique is highly proficient in assessing the security condition of infrastructures based on blockchain technology. It enables a comprehensive and systematic process of identifying and minimizing potential weaknesses across many threat categories. Through a comprehensive analysis of each component of the STRIDE framework's architecture and procedural dynamics, one may systematically assess the framework's ability to withstand common security threats. This analysis highlights both the security advantages of the framework and identifies potential vulnerabilities that may necessitate further precautions to enhance the system's overall defense mechanisms.

The framework leverages the intrinsic attributes of blockchain, such as its immutability, encryption, and distributed consensus mechanisms, to tackle and alleviate the security vulnerabilities described by the STRIDE model.

4.5.1. Spoofing

The framework utilizes rigorous authentication protocols and role-based access control mechanisms to limit the dangers associated with identity forgery. Verifying the authenticity and reliability of individuals involved in the network acts as a protective measure against unauthorized entry and potentially harmful actions. The framework establishes prerequisites for nodes seeking to join permissioned private networks and open public networks. The network use virtual private networks (VPNs) to achieve network isolation and enhances security by utilizing certain criteria such as network ID, enode address, and port information. Authentication on both public and private blockchains depends on the use of public-key infrastructure (PKI) to provide secure transactions and verify the identity of participants. This system ensures that only authorized entities are able to engage in transactions on the network. During a transaction, the sender authenticates it by applying their private key K_pr, while the receiver checks the authenticity using the sender's public key K_pu. Validating the signed transaction is a necessary step in confirming the authenticity of the sender's address. Administrators possess information regarding the locations of nodes within private networks.

4.5.2. Tampering

The unchangeable characteristic of blockchain inherently safeguards against unauthorized alterations to data. Consensus among the network is essential for maintaining the integrity of data, as each block is cryptographically linked to the preceding one, creating an unchangeable chain. The framework enhances data security by employing off-chain storage alternatives and Oracle contracts to ensure the genuineness and dependability of data. The private blockchain environment is safeguarded via role-based access rules, encryption mechanisms, and tight participation guidelines. These measures ensure the security and privacy of confidential data.

4.5.3. Repudiation

The framework employs unchangeable transaction records to prevent denial and guarantee transparency and responsibility for all parties involved. Digital signatures and Public Key Infrastructure (PKI) are essential for verifying the identities of participants, while authorization mechanisms effectively control access rights and permissions within the network. The framework places a high importance on maintaining the secrecy of data by employing off-chain storage and encryption methods to safeguard sensitive information. Additionally, it takes into account the trade-off between security and the efficient use of resources.

4.5.4. Information Disclosure

The framework prioritizes data protection by employing encryption and secure communication protocols to thwart illegal access to information. Implementing techniques like as transport layer security (TLS), network segmentation, and firewalls is crucial for guaranteeing secure communication and protecting sensitive data in a permissioned blockchain environment.

4.5.5. Denial of Service (DoS)

The decentralized structure of the blockchain diminishes the probability of DoS assaults. Decentralization eliminates individual vulnerabilities, enhancing the system's capacity to endure adversities and operate reliably.

4.5.6. Information Disclosure

The framework employs role-based access controls and smart contract features to mitigate the risk of unauthorized privilege escalation. Users can only carry out actions for which they have received express authorization, ensuring strict control over system operations and access.

The proposed security technique significantly enhances the security of data management systems, particularly in businesses where data sensitivity and integrity are of utmost importance. By incorporating targeted security measures into the blockchain architecture, it is possible to successfully counteract a wide range of attacks, providing a robust defense mechanism. Nevertheless, further investigation and real-world application are necessary for future undertakings.

4.6. Integration and Challenges

Given the cited obstacles and the proposed blockchain-based framework in the article, the integration process may face specific and distinct challenges, along with their corresponding potential solutions:

4.6.1. Data Compatibility

The architecture of the blockchain framework may not instantly align with established data standards. **Solution:** The integration of the presentation layer in the proposed

framework enables the transformation or mapping of existing data formats into formats that are interoperable with blockchain technology. The link layer allows the construction of connections and offers data access in a predefined format for existing systems. The data can be easily transformed into different formats and used within the system.

4.6.2. Interoperability

Multiple systems may utilize different protocols that are not fundamentally compatible with the blockchain framework. **Solution:** The proposed approach entails the development or utilization of blockchain middleware capable of interfacing with various protocols and systems. This will facilitate seamless transmission of data across the proposed link layer. APIs and web sockets enable the exchange of data between preexisting systems, regardless of the protocols they employ.

4.6.3. Data Quality

The unchangeable characteristic of blockchain may impede the correction of data errors after they have been recorded. **Solution:** Developed smart contracts that integrate pre-validation of data before it is added to the blockchain, and also build and oversee off-chain data repositories for data that can be altered. Moreover, the proxy approach can be employed to implement modifications or updates to deployed contracts to guarantee the integrity of data. Data quality assurance can be accomplished by employing on-chain, off-chain, and requested data architecture.

4.6.4. Efficiency and Ability to Handle Increasing Workloads

Public blockchains, specifically, may have difficulties of scalability and performance. **Solution:** Select scalable blockchain solutions or hybrid models that combine the security of blockchains with the efficiency of traditional databases. The proposed inter and intra-cluster architecture enables the use of various blockchains and consensus methods to guarantee

scalability according to performance needs. Some blockchains demonstrate improved performance when handling large transaction volumes, whereas others do not. Thus, the selection of the intra-cluster consensus process and technology can be made separately from the primary inter-cluster, depending on the specific requirements.

4.6.5. Ensuring Security and Compliance

The inclusion of sensitive data into a blockchain system may raise issues related to adherence to regulations. **Solution:** Using private or permissioned blockchains that limit access and apply encryption to ensure compliance and protect data privacy.The access management layer of the offered frameworks tackles this problem, as demonstrated in the corresponding sections.

4.6.6. Organizational Change

The resistance to the adoption of blockchain technology stems from its inherent intricacy. **Solution:** Execute comprehensive training programs and demonstrate actual benefits to relevant stakeholders in order to encourage smoother integration.

To resolve these issues, utilizing a combination of technological, operational, and strategic approaches are needed. By integrating the blockchain architecture, existing data management systems will be enhanced and potential interruptions are likely to be reduced. The evaluation section showcases the suitability of the proposed framework for the previously mentioned domains. Nevertheless, we recognize that there is still potential for enhancement, and additional inquiries are necessary. Hence, this suggested paradigm serves as a commendable basis for data management.

Introducing the latest suggested systems or frameworks in practical situations may face early obstacles when discussing the need to integrate the new system with an existing one that is already well-known to everyone. This study presents a rationale for the requirement of the proposed framework and delineates the precise obstacles that must be systematically tackled.

Assessment of Existing Data Management Systems: This stage involves evaluating the current data management systems used in the unmanned vehicles and aviation industry. The proposed framework suggests the need to identify the functionality, data formats, protocols, and security mechanisms of these systems.

Identification of Integration Points: Once the current systems have been assessed, the next step is to pinpoint the precise areas where blockchain technology can be integrated to enhance or augment these processes. The study provides illustrations in several fields, including flight data recording, maintenance tracking, supply chain management, and regulatory compliance.

Data Mapping and Conversion: This pertains to the procedure of aligning the data structures and formats of existing systems with those that are compatible with blockchain technology. The essay suggests the development of mechanisms or middleware layers to provide seamless data interchange and conversion between the two systems.

Development of Blockchain Interfaces: In this stage, interfaces or APIs are developed and integrated to provide smooth communication and compatibility between the blockchain framework and existing data management systems. The focus is on ensuring interoperability with existing communication protocols and data exchange standards.

Integration Testing and Validation: Rigorous testing is conducted to confirm that the integrated system functions according to the intended design. The essay highlights the importance of thoroughly testing many components, including data exchange, transaction processing, smart contract execution, and data synchronization, to ensure the functionality, performance, and security of the integrated system. The combination of the presentation layer and connection layer enables seamless integration with the existing systems.

Deployment and Rollout Strategy: This involves devising a plan for implementing the integrated system in a manner that minimizes disruptions to ongoing operations. It is recommended to employ staggered deployment strategies, starting with pilot projects or proof-of-concept initiatives, before proceeding with full-scale implementation.

Training and Change Management: Stakeholders get extensive training sessions and change management initiatives to familiarize them with the integrated system. The article emphasizes the significance of educating consumers about the benefits, characteristics, and most effective approaches associated with the blockchain-based data management system.

Monitoring and Maintenance:

Procedures are established to monitor and maintain the ongoing performance, reliability, and safety of the integrated system. Continuous monitoring tools, security audits, and proactive maintenance procedures are employed to promptly detect and address any issues.

Compliance and Regulatory Alignment: This phase ensures that the integrated system complies with relevant aviation regulations, data privacy laws, and industry standards. Thorough assessments of regulatory requirements are conducted, and necessary actions are implemented to guarantee compliance. The combination of the presentation layer and connection layer enables seamless integration with the existing systems.

Iterative Improvement and Optimization: The integrated system undergoes continual improvement and optimization by analyzing user feedback, performance indicators, and incorporating emerging technology. The book suggests the concept of ongoing enhancement of the system to enhance its utility, user-friendliness, and efficiency throughout time.

Due to the strict restrictions in the aviation industry, the implementation of blockchain technology needs to be handled carefully to assure adherence to current standards. The aviation sector is highly regulated, with strict criteria for safety, maintenance, and operations. It also makes use of IoTs and UAVs. When implementing blockchain technology, it is essential to guarantee that adherence to current regulations is not compromised. This necessitates close collaboration with regulatory authorities. Incorporating the distinctive aspects of blockchain technology, such as its distributed ledger technology and smart contracts, into the regulatory framework requires collaboration with regulatory organizations to ensure safety and compliance with operating standards. The paper comprehensively analyzes the flexibility of the proposed framework, highlighting its ability to adhere to

existing and forthcoming laws. Nevertheless, the study also recognizes the necessity for additional investigation into the actual implementation and real-world consequences of the framework with regards to complying with legal and regulatory considerations.

In addition, the incorporation of the suggested framework, or any novel system, into current infrastructures presents additional obstacles, such as the requirement for both technical and non-technical user education. In order to tackle these problems, the framework highlights the significance of offering training to both personnel with technical expertise and those without technical expertise. While this study does not specifically address training, it is crucial to develop a training program that can cater to individuals who are not well-versed in technical matters. The paper emphasizes the importance of blockchain technology in relation to specific tasks, highlighting its advantages in improving data integrity, security, and transparency. Moreover, the framework offers comprehensive instructions on effectively utilizing the blockchain-based system for certain tasks and emphasizes the importance of implementing optimal security measures. The training program should include instructions on the responsibilities related to compliance and reporting. This lesson explains how blockchain architecture enables the fulfillment of regulatory requirements and the simplification of audit procedures.

The proposed framework's architecture is inherently hierarchical, making it easy for technical personnel to use and allowing for smooth integration with existing systems using technologies like APIs and WebSockets. This technique utilizes existing technology in fields such as monitoring and also allows for the creation of user-friendly interfaces at the presentation layer for persons who lack technical expertise. This enables both non-technical users to utilize the proposed framework autonomously or in combination with other systems.

4.7. Open Research Areas

The suggested framework, which utilizes blockchain technology, offers a secure method for managing Internet of Things (IoT), Unmanned Aerial Vehicles (UAVs), and the aviation industry. This framework shows potential for further investigation in several areas. These

areas of investigation are essential for improving the practical implementation, scalability, security, and integration of the framework with current technology.

Exclusive Testing Environment Researching the development of a thorough testing environment is of utmost importance. An advanced simulation and testing platform may greatly mitigate real-world risks and facilitate continuous research and development endeavors. This setting will enable the thorough assessment and improvement of the framework.

Practical Applications Validating the effectiveness of the framework is crucial by using it in real-world circumstances. This entails implementing the framework on tangible objects and systems, namely in the domains of Internet of Things (IoT), unmanned aerial vehicles (UAVs), and aviation. It also involves carrying out meticulous observations to gather pertinent data. Conducting real-world testing is crucial for discovering the required improvements and optimizations.

Testing the scalability and performance To overcome scalability restrictions, it is necessary to simulate the framework under high-demand scenarios utilizing technologies such as load balancers. This technique will facilitate the assessment of the framework's performance under stressful conditions and provide guidance for implementing targeted improvements to achieve strong scalability.

Improvements in Security Subsequent investigations will prioritize the development of automated and standardized security testing techniques rooted in threat modeling. This entails the synchronization of offensive actions according to established models of potential dangers and the observation of the system's reaction to improve its security features.

Edge computing is a technology that enables the processing and storage of data closer to the source, reducing latency and improving efficiency. Blockchain, on the other hand, is a decentralized and secure system for recording and verifying transactions. Combining these two technologies, blockchain for edge computing, allows Exploring the combination of blockchain with edge computing can improve the ability to handle data at the edge of a

network, resulting in better performance in terms of latency, bandwidth utilization, and data security for Internet of Things (IoT) applications.

Methods to Enhance Blockchain Scalability It is essential to explore different scalability options, such as sharding, layer-2 solutions (such as state channels and sidechains), and hybrid blockchain designs, in order to overcome the scalability constraints of existing blockchain systems.

Edge computing is a technology that enables processing and storage of data closer to the source, rather than relying on a centralized cloud infrastructure. Blockchain, on the other hand, is a decentralized and secure system for recording and verifying transactions. Combining blockchain with edge computing can enhance the security Exploring the fusion of blockchain with edge computing might bolster data processing capabilities at the edge of a network, hence enhancing latency, bandwidth utilization, and data security in Internet of Things (IoT) applications.

Regulatory and compliance frameworks refer to the set of rules and guidelines that organizations must follow in order to ensure they are operating within legal and ethical boundaries. Researching and creating rules and recommendations to guarantee that blockchain implementations adhere to both regional and international regulations is a crucial field of study. This involves examining the legal ramifications of smart contracts and ensuring adherence to data protection regulations, such as GDPR.

Decentralized Identity Management Studying decentralized identity management systems via blockchain technology can offer secure and user-managed identification solutions, which are especially valuable in industries such as aviation for ensuring secure and verified identity verification of both workers and gadgets.

Integration of Blockchain and AI Exploring the incorporation of blockchain technology with artificial intelligence (AI) can improve decision-making, automation, and security in Internet of Things (IoT) and Unmanned Aerial Vehicle (UAV) applications. This involves investigating the potential for utilizing artificial intelligence (AI) to enhance the efficiency

of blockchain operations, as well as the reciprocal possibility of leveraging blockchain technology to optimize AI processes.

5. EXPERIMENTAL RESULTS

5.1. Scenario

The Flight Management System (FMS) is a system composed of the Flight Management Computer (FMC), Common Display Unit (CDU), and a cross-talk bus. Comparison studies present that there are variations in pilot training, aircraft performance, and errors in data collection and processing according to developed FMS [146, 147]. Another problem is the capacity of the FMS which has limited storage to maintain the required data to FMS [148]. Using the FMS database populated from many sources, a common use of pilot entry can be considered to be met. As a result, the NavDB and PerfDB consist of the combination of various data that all the other modules are fed with. While the performance database is not shared publicly NavDB is common data for nodes in the aviation domain. NavDB is updated regularly by the aviation authorities and is the main source of flight planning. For these reasons, proof of concept evaluation is performed on the presented framework for storing NavDB, which is important in the aviation domain and is updated every 28 days. We obtained the real navigation data which contains files and approximately 1.240.158 bytes of formatted plain text data. Example data format is shown in Table 5.1.

Table 5.1 Navigation data formation.

NAV_IDENT	TYPE	CTRY	NAME	ICAO	WAC	FREQ		WGS_LAT	WGS_DLAT	WGS_LONG	WGS_DLONG	SLAVED_VAR	MAG_VAR	ELEV
ST	5	TU	ATATURK	LT	323	340000K	.....	N40574590	40.962.750	E028481350	28.803.750		E005522 0222	U
BCN	4	SP	BARCELONA	LE	319	116700M	.....	N41182560	41.307.111	E002062810	2.107.806	E00101220	E001320 0222	0
BML	9	US	BERLIN	KZ	263		.....	N44380072	44.633.533	W071111029	-71.186.192		W014459 0222	1730
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
ESB	4	TU	ESENBOGA	LT	323	112100M	.....	N40084780	40.146.611	E033004490	33.012.472	E00420112	E006056 0222	3150

It is ensured that NavDB is stored on the inter-cluster blockchain (IeC) so that data can be stored, updated, and deleted on the blockchain. The I_eC nodes are assumed to have provided their addresses and participated in the consisted blockchain network, which is designed to be private, and is structured parallel to security considerations. Each node has its own private-public key pair and an address derived from it. The blockchain also includes validator nodes with predefined nodes that are granted with R_A. The R_A node owns the right of the management of private blockchain and has deployed the management, storage, and

oracle contracts respectively. The NavDB data, which contained real data, was formatted and added to the storage contract by the node having the R_{DM}. The R_L nodes obtained the requested data by sending a read request to the NavDB data stored on the storage contract or by listening to the events that emitted from the chain.

5.2. Development environment

Applications and technologies developed for the realization of the scenario and a summary of them are given in Table 5.2.

Table 5.2 Blockchain tools for development, testing, and monitoring.

Environment	Tools
Integrated Dev. Env. (IDE)	VsCode, bash terminal, Solidity IDE
Development Environment	Truffle Suit, Remix, Metamask, HDwallet Node.js, JavaScript (js)
Library	web3.js, ether.js, custom scripts
Blockchain Client	HyperLedger Besu, Ganache
Testing Tools	HyperLedger Caliper, Truffle Suit
Monitoring Tools	Prometheus, Grafana, Web browser

The Ethereum blockchain network is used because it enables smart contracts, a well-known and preferred technology in the literature, and it is available to the public. The proposed framework is constructed as a private network. VsCode IDE, the Truffle suit extension, and Remix Ide are used for developing smart contracts in Solidity language. Smart contracts are tested on the Ganache Ethereum network before being deployed into production.

In order to address the security requirements of the production environment, the HyperLedger Besu client is utilized to establish the private blockchain. To test a single transaction to request or gather data, HDwallet and Metamask are used to sign and send transactions (txs). Node.js, web3.js, and ethers.js libraries are used to interact with the blockchain via web socket and API. Applications are developed using the Javascript language to initialize the proposed framework with its components and evaluate tests. Web socket, API, and web event handler applications are developed to realize access to on-chain,

off-chain, and requested data. Applications' responsibilities include serving the on-chain data as requested, listening to logs and events, gathering off-chain data from its address and checking its hash value for consistency, performing Oracle voting, and gathering it from different sources for requested data. With these applications, access to data in different structures such as IPFS, CouchDB [149], and PostgreSQL [150] is made possible. An auto-run application is developed to initialize the proposed blockchain framework and test it with flexible parameters. The developed applications, the used technologies, and their brief descriptions are given in Table 5.3.

Table 5.3 Developed programs and used technologies.

Data Type	Program	Description
On-chain	websocket	Program to access data on contract storage
off-chain	IPFS	Distributed data storage
	CouchDB	Document based database management system
	PostgreSql	Relational database management system
requested	API	event handler for requested API data with parameters
	web listener	js-based program for search data on www

*Used libraries: ipfs-http-client, body-parser, request, node-fetch, express, axios, dotenv

5.3. Test environment

The genesis block files of the IBFT 2.0 and QBFT consensus protocols are created in order to implement the proposed framework. PKI key pairs that are uniquely utilized by each node are generated and applications are developed to provide the necessary data communication among the nodes. Private key K_{PR} and public key K_{PU} are generated for each node with the help of the *'besu operator batch'*. Node.js 18, CouchDB, PostgreSQL, IPFS local clients, and the mentioned libraries are installed on the same workstation which is powered by Intel Core X-series processors, DDR4 4266 MHz 64 GB RAM.

Hyperledger Besu client parameters (chainId, milestone block, protocol, fixed difficulty, block period, epoch length, request timeout etc.) are defined in the genesis file according

to the consensus protocol. IBFT 2.0 and QBFT initial genesis file parameters are given in Figure 5.1.

```
{
"config": {
    "chainid": 2929,
    "berlinBlock": 0,
    "qbft": {
        "epochlength": 30000,
        "blockperiodseconds": 2,
        "requesttimeoutseconds": 4
    }
},
"nonce": "0x0",
"timestamp": "0x58ee40ba",
"extraData": "0xf87aa00...",
"gasLimit": "0x47b760",
"difficulty": "0x1",
}
```

Figure 5.1 QBFT genesis file parameters.

Since there is no generally accepted test benchmark in the literature, HyperLedger Caliper is preferred due to its applicability and the fact that it provides fundamental values such as throughput and latency metrics which are considered important for validating the framework.

Management, crosschain, storage, and oracle contracts. Users are created and roles are granted for testing purposes. The implemented framework is tested for usability. Storage contract NavDB initialization function is considered for performance testing of the proposed framework. The initialization function algorithm is given in Alg. 1.

To perform the specified tests, it is necessary to run several iterations in an automated environment. Obtained results must be recorded in an appropriate format in order to conduct a fair comparison. In addition, the same test scenario must be run at least three times so as to obtain a mean average for reliable data analysis regardless of the environment. To address the mentioned requirements, a novel automated testing application is developed in JavaScript language to test multiple scenarios as parameters are illustrated in Table 5.4. Each test is conducted on a newly created blockchain. Additionally, contract deployment and granting

Data: Valid Parameters including caller identity C, NavDB value identifier N_{id}, and NavDB data N_{data}.
Result: Initializes the NavDB structure with the given data and emits an event upon successful initialization, or returns an error on unauthorized access.
Input: C (Caller identity), N_{id} (NavDB value identifier), N_{data} (NavDB data)
Output: Response data indicating successful initialization or an error message

$C \leftarrow$ Caller;
`/* The entity attempting to perform the initialization. */`
$N_{id} \leftarrow$ NavDB value identifier;
`/* Unique identifier for the NavDB data entry. */`
$N_{data} \leftarrow$ NavDB data;
`/* The actual data to be stored in NavDB. */`

if C *can call method* **then**
    create Nav struct object (N_{id}, N_{data});
    `/* Initializes a new NavDB structure with the provided identifier and data. */`
    map object navdata[N_{id}] = nav;
    `/* Associates the NavDB identifier with the new data entry. */`
    emit event(NavDB_INITIALIZED, N_{id});
    `/* Signals the successful initialization of the NavDB entry. */`
else
    return error[Unauthorized access];
    `/* Ensures security by preventing unauthorized modifications. */`
end

Algorithm 1: NavDB *Initialize Function* algorithm.

roles are done in an automated manner. To the best of our knowledge, there is no automated application developed for these types of requirements.

The primary objective behind our experimental evaluation is to ensure that the developed framework is fit-for-purpose and fit-for-use, as well as to assess its suitability for the scenario presented. To that end, the proposed framework is tested on an active Ethereum network using the block creation time per second (bps) operator in the genesis file, the number of validator nodes, and a comparison of the IBFT 2.0 and QBFT consensus algorithms. On the other hand, Hyperledger Caliper benchmarking configurations and rate controllers

Table 5.4 Developed automated testing program parameters and definitions.

Parameter	Data Type	Description
folder_name	string	setting name of the top folder
create_folder	bool	option to creation of folder
node_count	int	set validator nodes number
i_q_bft	string	set consensus protocol
change_genesis	bool	set validators and consensuss
run_node_count	int	set running nodes count
run_prometheus	bool	run Prometheus data collection
tsdb_name	string	prometheus database name
run_report	bool	run HL Caliper for testing
report_name	string	set generated report name
promet_data_export	bool	export tsdb database
promet_db_delete	bool	delete prometheus database
migrate_change_config	bool	migrate contract, set config

are compared in the context of error rates. The effect of the number of workers (w) and transactions sent (tx) are also examined. Furthermore, five (5) different rate controller approaches are tested: fixed rate, fixed feedback rate, fixed load, maximum rate, and linear rate. Through the developed testing application, the necessary configurations for the HyperLedger Caliper to connect to the running Ethereum network are made, the reports are recorded for each case, and system resources are monitored for further investigation. Our obtained test results and discussion are provided in the following section.

6. DISCUSSION

PoA consensus protocols IBFT 2.0 and QBFT are tested sequentially on the utilized blockchain with the storage contract's initialized function. Storage contract has initialize function (F_{init}), update function (F_{update}), read function (F_{read}), and variations of them. The F_{init} is investigated to validate the proposed framework because it changes the state of the blockchain and is expected to consume more resources according to other functions.

The proposed framework is utilized with IBFT 2.0 consensus algorithm, 4 validator nodes, and 2 block period seconds (bps) parameters. Blockchain is evaluated for number of workers

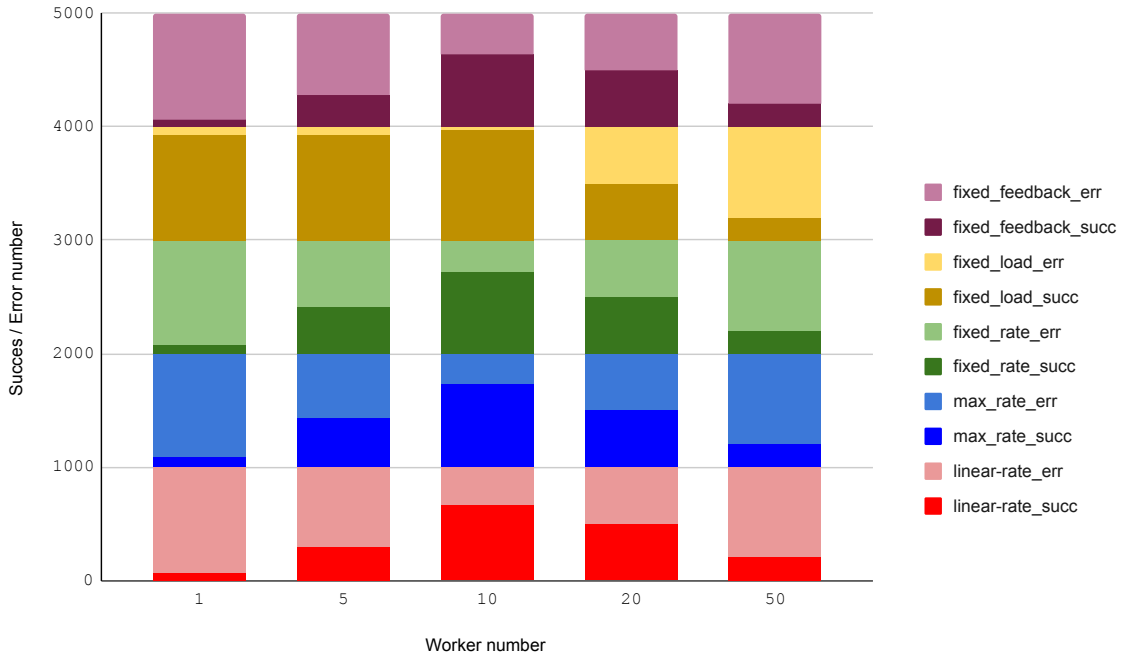

Figure 6.1 Rate controller success / error rates for IBFT 2.0.

success with 1, 5, 10, 20, and 50 workers numbers and under 1000 txs load. Also, the effect of different workloads on the transaction success is investigated. HyperLedger Caliper rate controllers are fixed feedback rate (fixed_feedback), fixed load rate (fixed_load), fixed rate (fixed_rate), max rate (max_rate) and linear rate (linear_rate). Obtained results are given in Figure 6.1. The x-axis represents the number of workers and the y-axis is the success and error number under load. Workload parameter error (_err) and success (_succ) values are represented by adding the end of the workload name such as fixed_feedback_err for fixed feedback rate error. Except for a fixed load rate of up to 10 workers, the number of successful transactions increases in all rate controllers. The fixed load rate controller performs similarly until 10 workers, beyond which the success rate diminishes. Furthermore, when all the rate controllers are run with 10 workers, the maximum number of successful transactions is observed, and after that point, there is a decline in the number of successful transactions. Consequently, it has been found that the optimal number of workers for further examination is 10.

The effect of the number of validators is another concern that has a direct impact on block

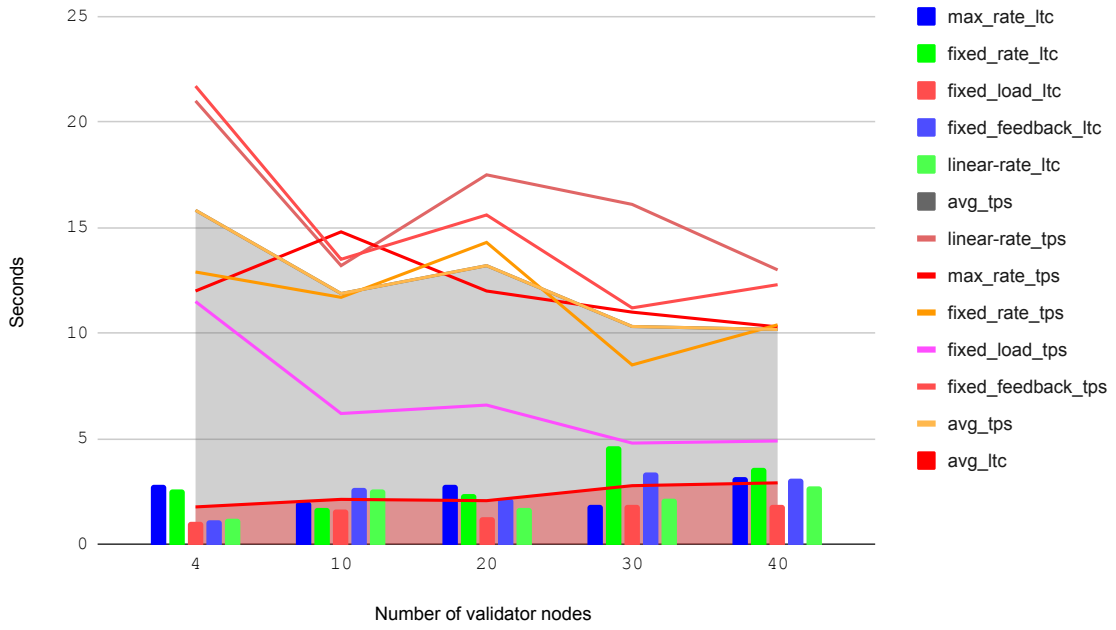

Figure 6.2 Effect of the validator number on throughput and latency.

creation time because it increases the time required to validate the blocks to be created. At least, three out of four validator nodes must validate the block in order to respect Byzantine Fault Tolerant (BFT). Figure 6.2 shows the test results for 50 tx, 2 bps, and 10 workers on an IBFT 2.0 network with 4, 10, 20, 30, and 40 validators. Even though increasing from 4 to 10 validators resulted in a decrease in throughput and an increase in latency. Increasing the number of validators to 20 resulted in the opposite, however, in a small difference. Throughput is decreased and latency is increased in tests with 30 and 40 validators, respectively. As a result, the expected decrease in throughput with increasing the number of validators in PoA algorithms is interpreted as an increase in latency. The fact that the throughput is higher with 10 validators than with 20 validators can be attributed to network resources, although this may be insignificant. The effect of the rate controller on transaction commit time can be seen as average throughput and average latency are represented as *avg_tps* and *avg_ltc*, respectively. To conclude, as the number of validator nodes increases, throughput decreases, and latency increases.

Block period seconds (bps) is the parameter defined in the genesis file to set the creation

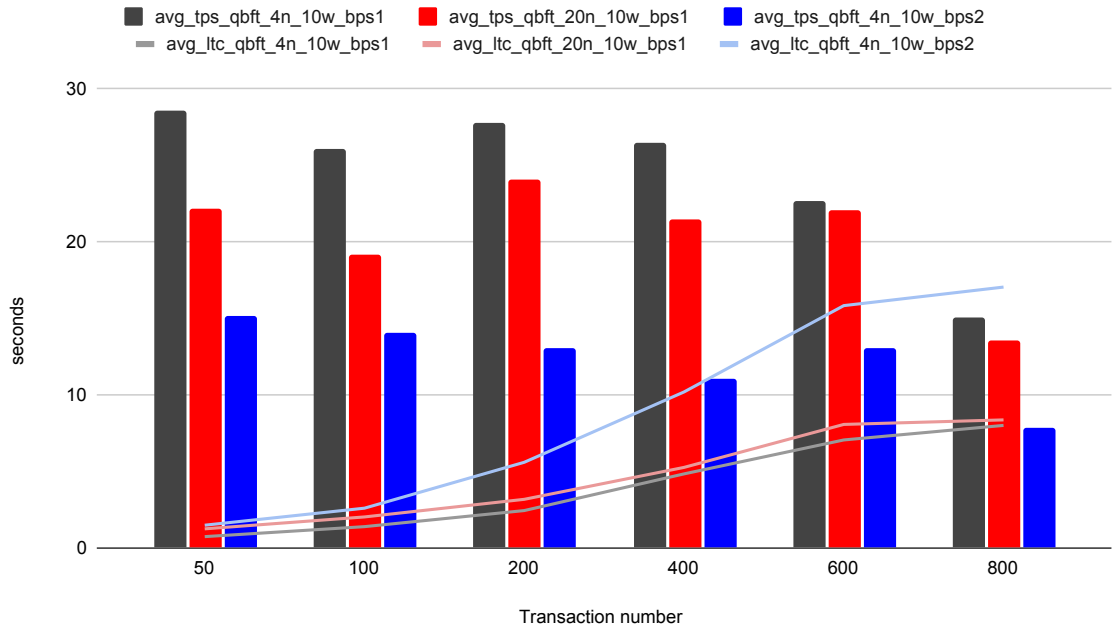

Figure 6.3 Effect of validator node number and bps over throughput and latency on QBFT.

time of a block even if there is no submitted transaction. QBFT algorithm is investigated for bps is 1 and 2 with 4 and 20 validator nodes to examine the correlation between them. Throughput is the highest for all transaction numbers in the test results with 4 validator nodes, 10 workers, and 1 bps, according to the results with the QBFT algorithm given in Fig 6.3. Then tests are conducted with 20 validator nodes, 10 workers, and 1 bps. The results of the tests with 4 validator nodes, 10 workers, and 2 bps show that the time it takes to create a block has a direct impact on throughput. Comparing the results validator increase has less effect than bps under 4 and 20 validator nodes. Throughput increases as bps decreases even with more validator nodes. *4n_10w_bps1* (4 nodes 10 workers 1 block period second) gives best throughput, *20n_10w_bps1* and *4n_10w_bps2* follows. At the same time, the latency in all configurations increases as the number of tx increases.

To evaluate the scalability of the proposed framework, a comparative analysis of consensus techniques is performed. For comparison of the QBFT and IBFT 2.0 algorithm on the proposed framework 4 validator nodes, 10 test workers, and 1, 2 bps are taken into consideration. Figure 6.4 shows that QBFT performs better than IBFT 2.0. But, when

comparing IBFT results for bps 1 outperforms bps 2 in difference with QBFT.

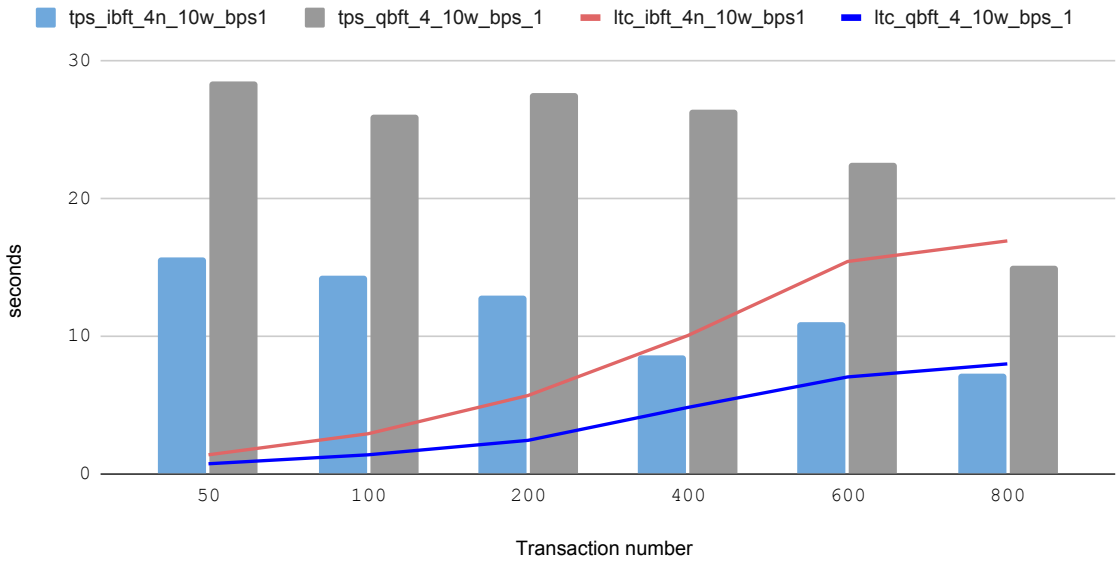

Figure 6.4 Comparison of IBFT 2.0 and QBFT consensus protocols.

The framework's scalability was thoroughly evaluated by changing the number of validator nodes and analyzing the effects on transaction throughput and latency. The tests were conducted to determine the framework's capacity to efficiently manage growing workloads without seeing a notable performance decline. The testing showed that the framework achieves a balance between throughput and latency until a specific threshold of validator nodes and workload intensity is reached. The study found that the most effective number of workers for testing was 10, resulting in the highest number of successful transactions across various rate controllers tested.

The framework's ability to handle significant transaction volumes was shown through performance testing in high-demand situations. The experiment assessed the framework using a specific amount of transactions under various configurations of the IBFT 2.0 and QBFT consensus algorithms, emphasizing block creation time and the number of validator nodes. The framework's performance is influenced by the consensus mechanism, block generation interval, and the number of validator nodes. A reduction in block period

seconds (bps) and an ideal number of validator nodes, discovered through testing, improved transaction throughput while keeping latency levels within acceptable limits.

7. CONCLUSION

The goal of the framework is to provide a structure that can be implemented in various domains for data management that are utilized in a clustered or in some conditions in a private environment but communicates with the external parties. As is seen in the obtained test results and also discussed; with the help of the proposed framework data can be transferred securely, structural decisions can be made autonomously within the intra-cluster blockchain, and the intra-cluster blockchain can interact with another blockchain that manages its own structure apart from any other blockchain through inter-cluster. Inter-cluster enables the communication between intra-clusters and stores common data needed by all participants. The inter-cluster is also responsible for participation in the blockchain, the management of general rules, and the provision of data access, exchange methods, and structures. On the other hand, data integrity has been ensured by introducing access and acquisition methods in accordance with the data structure. Access control and authentication procedures have also been utilized to assure access security. The technique given has resulted in a framework that is applicable and powerful, particularly in circumstances where there is internal management but also external control or a requirement for communication.

With developments in the field of blockchain and the growing demand for seamless performance in the business sector, plenty of uses can be created to effectively handle regulatory management and solving problems in the context of data management that are encountered in aviation, UAVs, IoTs, smart city applications, product tracing, passport validation, etc. is now possible with the help of the framework presented in this study. In the case of the passport control mechanism that uses the presented framework; each country stores its own passport information and this information is stored as private in intra-cluster. The inter-cluster holds the proof of the passport validation information and when all countries are members of this inter-cluster, one country can securely verify the passport information of another country.

There are similar frameworks in the literature, however, all of them are focused on a specific

problem or applied to a specific domain. To the best of our knowledge, there is no such framework that can effectively handle diverse applications in the literature. In this research, a baseline framework is presented that can be a remedy to various problems in numerous problem domains in the context of data management.

Experimental evaluation has shown that with the concept validation of the proposed framework, role-based access to data either on or off the blockchain can be provided in accordance with access control utilizing developed contracts and other components. Furthermore, a solution for gathering nondeterministic information from the chain is proposed.

Our research aims to implement and thoroughly test the suggested framework in real-life scenarios, with a particular focus on the IoT, UAVs, and the aviation industry as future work and open research areas. Our objective is to collect relevant data from real-world implementations by installing the framework onto actual devices and systems and conducting detailed observations. This data will be essential in identifying the necessary enhancements and optimizations, guaranteeing that the framework adequately fulfills the practical requirements of these advanced technical fields.

In addition to the focus on practical implementation, the creation of a dedicated testing environment has also become a secondary goal. While we have made some progress in developing a simulation and test environment to reduce real-world hazards, the many intricacies and contributions of this environment were not within the focus of our current study. Future research initiatives will focus on providing a comprehensive and major contribution to this test environment, developing a strong platform that will greatly help ongoing and future research and development efforts.

The framework's integration capabilities with current real-world systems have been greatly affected by engagements with prominent aviation corporations, namely in the areas of data storage and access procedures. Future endeavors will be focused on implementing the framework with tangible devices within these companies. This crucial milestone in achieving

practicality and verification is anticipated to strengthen the framework's significance and efficiency in real-life settings, thereby enabling a smooth integration with current systems.

Moreover, the ever-evolving domain of consensus algorithms presents a hopeful opportunity to improve the flexibility of the framework. Exploring new domain-specific consensus algorithms has the potential to utilize the inherent flexibility of the proposed framework, incorporating these technological breakthroughs to improve performance and efficiency. Future research will focus on expanding and speeding up these algorithms, to ensure that the framework remains at the forefront of technological progress.

To address the scalability limitations of the framework and assess its maturity, it will be necessary to simulate the framework under high-load situations, employing technologies like load balancers. This strategic approach aims to thoroughly evaluate the framework's performance in different stressful situations, enabling specific enhancements to ensure strong scalability. By conducting systematic testing and assessment, the framework's capacity to endure and function optimally in various settings will be greatly improved.

Finally, ensuring security is of utmost importance, and it is crucial to focus on developing automated and standardized security testing methods based on threat modeling. Our goal is to enhance the security characteristics of the framework by coordinating attacks based on known threat models and closely monitoring the system's overall response. The continuous effort to improve security measures aims to protect the system from constantly changing cybersecurity threats, offering a safe and dependable platform for users in different fields.

Future development includes implementing the system on test Ethereum networks and establishing it as a container, building upon the success of the framework. The objective is to introduce a framework that is simple to implement, practical, and can be expanded to address issues in different fields. Moreover, there is ongoing study in the field of boosting throughput and addressing other security concerns related to hostile actions. The objective is to assess the framework in a setting with many grouped drones powered by Nvidia Jetson Xavier, enabling data interchange during a partially autonomous swarm flight.

The suggested blockchain-based framework for IoT, UAVs, and aviation has numerous opportunities for additional research beyond the initial phase of deployment and testing. Combining blockchain technology with edge computing can optimize data processing at the periphery of the network, resulting in improved latency, more efficient utilization of bandwidth, and more data security. In addition, the utilization of privacy-preserving methods, such as zero-knowledge proofs and homomorphic encryption, can greatly improve the level of data privacy and security.

Conducting research on regulatory and compliance frameworks is crucial to guarantee that blockchain implementations comply with both local and global regulations. Moreover, the integration of blockchain and AI can improve decision-making, automation, and security in IoT and UAV applications, optimizing the functioning of both blockchain operations and AI processes. These study fields jointly contribute to improving and enhancing the capabilities and applications of the proposed framework.

REFERENCES

[1] F. Lamberti, V. Gatteschi, C. Demartini, M. Pelissier, A. Gómez, and Victor Santamaria. Blockchains can work for car insurance: Using smart contracts and sensors to provide on-demand coverage. *IEEE Consumer Electronics Magazine*, 7:72–81, **2018**.

[2] M. Mettler. Blockchain technology in healthcare: The revolution starts here. *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pages 1–3, **2016**.

[3] Meghali Nandi, Rajat Kanti Bhattacharjee, Amrit Kumar Jha, and F. A. Barbhuiya. A secured land registration framework on blockchain. *2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP)*, pages 130–138, **2020**.

[4] N. Kshetri and J. Voas. Blockchain-enabled e-voting. *IEEE Software*, 35:95–99, **2018**.

[5] Samir M. Umran, Songfeng Lu, Zaid Ameen Abduljabbar, Jianxin Zhu, and Junjun Wu. Secure data of industrial internet of things in a cement factory based on a blockchain technology. *Applied Sciences*, 11(14), **2021**. ISSN 2076-3417. doi:10.3390/app11146376.

[6] Brad Chase and Ethan MacBrough. Analysis of the XRP ledger consensus protocol. *CoRR*, abs/1802.07242, **2018**.

[7] Feng Tian. An agri-food supply chain traceability system for china based on rfid blockchain technology. In *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pages 1–6. **2016**. doi:10.1109/ICSSSM.2016.7538424.

[8] E. Pimenidis and N. Polatidis. Secure social media spaces for communities of vulnerable people. In *2019 IEEE 12th International Conference on Global*

Security, Safety and Sustainability (ICGS3), pages 1–5. **2019**. doi:10.1109/ICGS3.2019.8688027.

[9] J. D. Preece and J. M. Easton. Blockchain technology as a mechanism for digital railway ticketing. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 3599–3606. **2019**. doi:10.1109/BigData47090.2019.9006293.

[10] Lixia Xie, Ying Ding, Hongyu Yang, and Xinmu Wang. Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets. *IEEE Access*, 7:56656–56666, **2019**. doi:10.1109/ACCESS.2019.2913682.

[11] N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, **2018**. doi:10.1109/TDSC.2016.2616861.

[12] Xinyue Zhang, Jingyi Wang, Haijun Zhang, Lixin Li, Miao Pan, and Zhu Han. Data-driven transportation network company vehicle scheduling with users' location differential privacy preservation. *IEEE Transactions on Mobile Computing*, 22(2):813–823, **2023**. doi:10.1109/TMC.2021.3091148.

[13] Samir M. Umran, SongFeng Lu, Zaid Ameen Abduljabbar, Zhi Lu, Bingyan Feng, and Lu Zheng. Secure and privacy-preserving data-sharing framework based on blockchain technology for al-najaf/iraq oil refinery. In *2022 IEEE Smartworld, Ubiquitous Intelligence & Computing, Scalable Computing & Communications, Digital Twin, Privacy Computing, Metaverse, Autonomous & Trusted Vehicles (SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta)*, pages 2284–2292. **2022**. doi:10.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00325.

[14] Anu Raj and Shiva Prakash. A privacy-preserving authentic healthcare monitoring system using blockchain. *Int. J. Softw. Sci. Comput. Intell.*, 14(1):1–23, **2022**. ISSN 1942-9045. doi:10.4018/IJSSCI.310942.

[15] Ozan Zorlu and Adnan Ozsoy. An immutable navigation database on blockchain. In *2023 10th International Conference on Recent Advances in Air and Space Technologies (RAST)*, pages 1–6. **2023**. doi:10.1109/RAST57548.2023.10197941.

[16] Ozan Zorlu, Adnan Ozsoy, and Seyyit Alper Sert. A role-based access control management model on blockchain for restricted facilities: An airport example. In *2023 10th International Conference on Recent Advances in Air and Space Technologies (RAST)*, pages 1–6. **2023**. doi:10.1109/RAST57548.2023.10197974.

[17] L. Hîrtan and C. Dobre. Blockchain privacy-preservation in intelligent transportation systems. In *2018 IEEE International Conference on Computational Science and Engineering (CSE)*, pages 177–184. **2018**. doi:10.1109/CSE.2018.00032.

[18] José Manuel Guaita Martínez, Patricia Carracedo, Dolores Gorgues Comas, and Carlos H. Siemens. An analysis of the blockchain and covid-19 research landscape using a bibliometric study. *Sustainable Technology and Entrepreneurship*, 1(1):100006, **2022**. ISSN 2773-0328. doi:https://doi.org/10.1016/j.stae.2022.100006.

[19] Simeon Okechukwu Ajakwe, Dong-Seong Kim, and Jae-Min Lee. Drone transportation system: Systematic review of security dynamics for smart mobility. *IEEE INTERNET OF THINGS JOURNAL*, 10(16):14462–14482, **2023**. ISSN 2327-4662. doi:10.1109/JIOT.2023.3266843.

[20] X. Zhou, W. Li, and L. Zhong. A supervised privacy preservation transaction system for aviation business. *Peer-to-Peer Networking and Applications*, **2024**. doi:10.1007/s12083-024-01647-5.

[21] S. Das, S. Sarkar, A. Ray, A. Srivastava, and D. L. Simon. Anomaly detection in flight recorder data: A dynamic data-driven approach. In *2013 American Control Conference*, pages 2668–2673. **2013**. doi:10.1109/ACC.2013.6580237.

[22] M. Xu, R. Bodik, and M. D. Hill. A "flight data recorder" for enabling full-system multiprocessor deterministic replay. In *30th Annual International Symposium on Computer Architecture, 2003. Proceedings.*, pages 122–133. **2003**. doi:10.1109/ISCA.2003.1206994.

[23] BEA. Flight data recorder read-out technical and regulatory aspects. **2005**.

[24] Samir M. Umran, SongFeng Lu, Zaid Ameen Abduljabbar, and Xueming Tang. A blockchain-based architecture for securing industrial iots data in electric smart grid. *Computers, Materials & Continua*, 74(3):5389–5416, **2023**. ISSN 1546-2226. doi:10.32604/cmc.2023.034331.

[25] Aerialos, skygrid , "https://www.skygrid.com/".

[26] C.S. Wright. Bitcoin: A peer-to-peer electronic cash system. Technical report, Social Science Research Network, **2008**. doi:10.2139/ssrn.3440802.

[27] I. Eyal, A.E. Gencer, E.G. Sirer, and R. Van Renesse. Bitcoin-ng: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation*, pages 45–59. **2016**.

[28] M. Iansiti and K.R. Lakhani. The truth about blockchain. *Harvard Business Review*, 95(1):118–127, **2017**.

[29] Konstantinos Christidis and Michael Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, **2016**. doi:10.1109/ACCESS.2016.2566339.

[30] Riaan Bezuidenhout, Wynand Nel, and Jacques M. Maritz. Permissionless blockchain systems as pseudo-random number generators for decentralized consensus. *IEEE Access*, 11:14587–14611, **2023**. doi:10.1109/ACCESS.2023.3244403.

[31] Wangxi Jiang, Xiaoxiong Wu, Mingyang Song, Jiwei Qin, and Zhenhong Jia. A scalable byzantine fault tolerance algorithm based on a tree topology network. *IEEE Access*, 11:33509–33519, **2023**. doi:10.1109/ACCESS.2023.3264011.

[32] Roberto Saltini. Ibft liveness analysis. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 245–252. **2019**. doi:10.1109/Blockchain.2019.00039.

[33] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. **2012**.

[34] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. In *Italian Conference on Cybersecurity*. **2018**.

[35] G. Indra Navaroj, E. Golden Julie, and Y. Harold Robinson. Adaptive practical byzantine fault tolerance consensus algorithm in permission blockchain network. *International Journal of Web and Grid Services*, 18(1):62–82, **2022**. doi:10.1504/IJWGS.2022.119273.

[36] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Sirer. *Decentralization in Bitcoin and Ethereum Networks*, pages 439–457. **2018**. ISBN 978-3-662-58386-9. doi:10.1007/978-3-662-58387-6_24.

[37] Luc Gerrits, Cyril Naves, Roland Kromes, François Verdier, Severine Glock, and Guitton Patricia. Experimental scalability study of consortium blockchains with bft consensus for iot automotive use case. pages 492–498. **2021**. doi:10.1145/3485730.3493374.

[38] Satoshi Nakamoto. Bitcoin : A peer-to-peer electronic cash system. **2009**.

[39] Xiaohong Deng, Kangting Li, Zhiqiang Wang, Juan Li, and Zhiqiong Luo. A survey of blockchain consensus algorithms. In *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, pages 188–192. **2022**. doi:10.1109/ICBCTIS55569.2022.00050.

[40] Joe Abou Jaoude and Raafat George Saade. Blockchain applications – usage in different domains. *IEEE Access*, 7:45360–45381, **2019**. doi:10.1109/ACCESS.2019.2902501.

[41] Vitalik Buterin. A next generation smart contract & decentralized application platform. **2015**.

[42] Ray Neiheiser, Gustavo Inácio, Luciana Rech, Carlos Montez, Miguel Matos, and Luís Rodrigues. Practical limitations of ethereum's layer-2. *IEEE Access*, 11:8651–8662, **2023**. doi:10.1109/ACCESS.2023.3237897.

[43] Hyperledger, the open global ecosystem for enterprise grade blockchain technologies.

[44] Christopher Hood. From foi world to wikileaks world: A new chapter in the transparency story. *Governance*, 24(4):635–638, **2011**. doi:https://doi.org/10.1111/j.1468-0491.2011.01546.x.

[45] S. Alashri, S. S. Kandala, V. Bajaj, R. Ravi, K. L. Smith, and K. C. Desouza. An analysis of sentiments on facebook during the 2016 u.s. presidential election. In *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, pages 795–802. **2016**. doi:10.1109/ASONAM.2016.7752329.

[46] M. Tsai and Y. Zhang. How the innovation diffusion of facebook changed internet usage and expression of public opinion in taiwan: Using voters' internet and facebook usage during the 2016 taiwanese presidential election

as an example. In *2017 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 1–8. **2017**. doi:10.23919/PICMET.2017.8125347.

[47] Philippe Goupil. Airbus state of the art and practices on fdi and ftc in flight control system. *Control Engineering Practice*, 19(6):524–539, **2011**. ISSN 0967-0661. doi:https://doi.org/10.1016/j.conengprac.2010.12.009. SAFEPROCESS 2009.

[48] Xinyan Li, Huimin Zhao, and Wu Deng. Bfod: Blockchain-based privacy protection and security sharing scheme of flight operation data. *IEEE Internet of Things Journal*, 11(2):3392–3401, **2024**. doi:10.1109/JIOT.2023.3296460.

[49] Jing Li, Zhenzhen Peng, Ao Liu, Long He, and Yi Zhang. Analysis and future challenge of blockchain in civil aviation application. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, pages 1742–1748. **2020**. doi:10.1109/ICCC51575.2020.9345297.

[50] Sana Hafeez, Ahsan Raza Khan, Mohammad M. Al-Quraan, Lina Mohjazi, Ahmed Zoha, Muhammad Ali Imran, and Yao Sun. Blockchain-assisted uav communication systems: A comprehensive survey. *IEEE Open Journal of Vehicular Technology*, 4:558–580, **2023**. doi:10.1109/OJVT.2023.3295208.

[51] Ruba Alkadi and Abdulhadi Shoufan. Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain. *IEEE Transactions on Network and Service Management*, 20(1):201–215, **2023**. doi:10.1109/TNSM.2022.3201817.

[52] C. Esposito, M. Ficco, and B.B. Gupta. Blockchain-based authentication and authorization for smart city applications. *Information Processing and Management*, 58:102468, **2021**. doi:10.1016/j.ipm.2020.102468.

[53] M. P. Andersen et al. Wave: A decentralized authorization system for iot via blockchain smart contracts. Tech. rep., University of California at Berkeley, **2017**.

[54] G.D. Putra, V. Dedeoglu, S.S. Kanhere, et al. Trust-based blockchain authorization for iot. *IEEE Transactions on Network and Service Management*, 18:1646–1658, **2021**. doi:10.1109/tnsm.2021.3077276.

[55] E. Chen, Y. Zhu, Z. Zhou, et al. Policychain: A decentralized authorization service with script-driven policy on blockchain for internet of things. *IEEE Internet of Things Journal*, 9:5391–5409, **2022**. doi:10.1109/jiot.2021.310914.

[56] Y. Liu, Q. Lu, S. Chen, et al. Capability-based iot access control using blockchain. *Digital Communications and Networks*, 7:463–469, **2021**. doi:10.1016/j.dcan.2020.10.004.

[57] T. Nandy, M.Y.I. Idris, R.M. Noor, et al. Review on security of internet of things authentication mechanism. *IEEE Access*, 7:151054–151089, **2019**. doi:10.1109/access.2019.2947723.

[58] S.A. Sert, A. Yazici, and A. Cosar. Impacts of routing attacks on surveillance wireless sensor networks. In *International Wireless Communications and Mobile Computing Conference (IWCMC)*, pages 910–915. **2015**. doi:10.1109/iwcmc.2015.7289204.

[59] Z. Cui, F. Xue, S. Zhang, et al. A hybrid blockchain-based identity authentication scheme for multi-wsn. *IEEE Transactions on Services Computing*, 1:241–251, **2020**. doi:10.1109/tsc.2020.2964537.

[60] C.K.M. Lau, K.-H.Y. Alan, and F. Yan. Blockchain-based authentication in iot networks. In *IEEE Conference on Dependable and Secure Computing (DSC)*, pages 1–8. **2018**. doi:10.1109/DESEC.2018.8625141.

[61] A. Mubarakali. An efficient authentication scheme using blockchain technology for wireless sensor networks. *Wireless Pers Commun*, 127:255–269, **2022**. doi:10.1007/s11277-021-08212-w.

[62] Kuo-Hsiung Tseng, Kuo-Hui Chen, and Chih-Lin Chu. Design and implementation of flight information management system. In *2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA)*, pages 61–65. **2016**. doi:10.1109/ICIEA.2016.7603552.

[63] Chen Qingbin and Xu Dangen. Research on application of blockchain technology in airport aviation security. In *2021 IEEE 3rd International Conference on Civil Aviation Safety and Information Technology (ICCASIT)*, pages 454–459. **2021**. doi:10.1109/ICCASIT53235.2021.9633615.

[64] Kazim Rifat Ozyilmaz and Arda Yurdakul. Designing a blockchain-based iot with ethereum, swarm, and lora: The software solution to create high availability with minimal security risks. *IEEE Consumer Electronics Magazine*, 8(2):28–34, **2019**. doi:10.1109/MCE.2018.2880806.

[65] Sara Rouhani, Vahid Pourheidari, and Ralph Deters. Physical access control management system based on permissioned blockchain. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1078–1083. **2018**. doi:10.1109/Cybermatics_2018.2018.00198.

[66] Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, and Jianxiong Wan. Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, 6(2):1594–1605, **2019**. doi:10.1109/JIOT.2018.2847705.

[67] Project wing, ”https://www.iotforall.com/drone-delivery-system”.

[68] Googlex project, ”https://www.iotforall.com/drone-delivery-system”.

[69] Saqib Ali, Guojun Wang, Md Zakirul Alam Bhuiyan, and Hai Jiang. Secure data provenance in cloud-centric internet of things via blockchain smart contracts. In *2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 991–998. **2018**. doi:10.1109/SmartWorld.2018.00175.

[70] Yuvaraj Rajendra, Venkatesan Subramanian, and Sandeep Kumar Shukla. Blockpaas: Blockchain platform as a service. In *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, pages 204–206. **2023**. doi:10.1109/COMSNETS56262.2023.10041392.

[71] Quentin F.M. Dupont, David K.H. Chua, Ahmad Tashrif, and Ernest L.S. Abbott. Potential applications of uav along the construction's value chain. *Procedia Engineering*, 182:165 – 173, **2017**. ISSN 1877-7058. doi:https://doi.org/10.1016/j.proeng.2017.03.155. 7th International Conference on Engineering, Project, and Production Management.

[72] I. J. Jensen, D. Selvaraj, and P. Ranganathan. Blockchain technology for networked swarms of unmanned aerial vehicles (uavs). In *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, pages 1–7. IEEE Computer Society, Los Alamitos, CA, USA, **2019**. doi:10.1109/WoWMoM.2019.8793027.

[73] Arthur P. Cracknell. Uavs: regulations and law enforcement. *International Journal of Remote Sensing*, 38(8-10):3054–3067, **2017**. doi:10.1080/01431161.2017.1302115.

[74] Rocci Luppicini and Arthur So. A technoethical review of commercial drone use in the context of governance, ethics, and privacy. *Technology in Society*, 46:109 – 119, **2016**. ISSN 0160-791X. doi:https://doi.org/10.1016/j.techsoc.2016.03.003.

[75] Claudia Stöcker, Rohan Bennett, Francesco Nex, Markus Gerke, and Jaap Zevenbergen. Review of the current state of uav regulations. *Remote Sensing*, 9(5):459, **2017**. ISSN 2072-4292. doi:10.3390/rs9050459.

[76] Roger Clarke. Understanding the drone epidemic. *Computer Law and Security Review*, 30(3):230 – 246, **2014**. ISSN 0267-3649. doi:https://doi.org/10.1016/j.clsr.2014.03.002.

[77] Graham Wild, John Murray, and Glenn Baxter. Exploring civil drone accidents and incidents to help prevent potential air disasters. *Aerospace*, 3(3), **2016**. ISSN 2226-4310. doi:10.3390/aerospace3030022.

[78] The meth-toting drone that crashed in tijuana, the whashington post.

[79] Drone collides with commercial aeroplane in canada, bbc [online].

[80] The mystery of the gatwick drone, the guardian [online].

[81] Heathrow airport: Drone sighting halts departures, bbc [online].

[82] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman. Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of uavs. In *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*, pages 84–89. **2017**. doi:10.1109/RED-UAS.2017.8101648.

[83] Drone employee: we help businesses hire drones. [online]. available: http://drone-employee.com/.

[84] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In *2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 468–477. **2017**. doi:10.1109/CCGRID.2017.8.

[85] X. Liang, S. Shetty, L. Zhang, C. Kamhoua, and K. Kwiat. Man in the cloud (mitc) defender: Sgx-based user credential protection for synchronization applications in cloud computing platform. In *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, pages 302–309. **2017**. doi:10.1109/CLOUD.2017.46.

[86] A. R. Biswas and R. Giaffreda. Iot and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pages 375–376. **2014**. doi:10.1109/WF-IoT.2014.6803194.

[87] O. Zorlu and O. K. Sahingoz. Increasing the coverage of homogeneous wireless sensor network by genetic algorithm based deployment. In *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pages 109–114. **2016**. doi:10.1109/DICTAP.2016.7544010.

[88] O. Zorlu, S. Dilek, and A. Özsoy. Gpu-based parallel genetic algorithm for increasing the coverage of wsns. In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, pages 640–647. **2017**. doi:10.1109/ICPADS.2017.00088.

[89] X. Liang, J. Zhao, S. Shetty, and D. Li. Towards data assurance and resilience in iot using blockchain. In *MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM)*, pages 261–266. **2017**. doi:10.1109/MILCOM.2017.8170858.

[90] ED-112 EUROCAE. Minimum operational performance specification for crash protected airborne recorder systems. **2004**.

[91] Dronebox, red cat holdings, https://www.redcatholdings.com.

[92] Flightchain whitepaper, sita, ,https://www.sita.aero/globalassets/docs/white-papers/flightchain-whitepaper.pdf".

[93] Yanhan Wu, Xin Lu, and Zhijun Wu. Blockchain-based trust model for air traffic management network. In *2021 IEEE 6th International Conference on Computer and Communication Systems (ICCCS)*, pages 92–98. **2021**. doi:10.1109/ICCCS52626.2021.9449156.

[94] Pengyong Cao, Guijiang Duan, Jianping Tu, Qimei Jiang, Xianggui Yang, and Chen Li. Blockchain-based process quality data sharing platform for aviation suppliers. *IEEE Access*, 11:19007–19023, **2023**. doi:10.1109/ACCESS.2023.3246984.

[95] Vidushi Agarwal and Sujata Pal. Hierchain: A hierarchical-blockchain-based data management system for smart healthcare. *IEEE Internet of Things Journal*, 11(2):2924–2934, **2024**. doi:10.1109/JIOT.2023.3295847.

[96] Gia Nhu Nguyen, Nin Ho Le Viet, Mohamed Elhoseny, K. Shankar, B.B. Gupta, and Ahmed A. Abd El-Latif. Secure blockchain enabled cyber–physical systems in healthcare using deep belief network with resnet model. *Journal of Parallel and Distributed Computing*, 153:150–160, **2021**. ISSN 0743-7315. doi:https://doi.org/10.1016/j.jpdc.2021.03.011.

[97] Dorcas Dachollom Datiri and Maozhen Li. A cluster enabled blockchain-based data management for iot systems. In *2023 24th International Carpathian Control Conference (ICCC)*, pages 88–92. **2023**. doi:10.1109/ICCC57093.2023.10178949.

[98] Jin Tian, JunFeng Tian, and RuiZhong Du. Mslshard: An efficient sharding-based trust management framework for blockchain-empowered iot access control. *Journal of Parallel and Distributed Computing*, 185:104795, **2024**. ISSN 0743-7315. doi:https://doi.org/10.1016/j.jpdc.2023.104795.

[99] W. Jerbi, O. Cheikhrouhou, A. Guermazi, H. Hamam, and H. Trabelsi. A blockchain based authentication scheme for mobile data collector in iot.

In *International Wireless Communications and Mobile Computing (IWCMC) Conference*, pages 929–934. **2021**. doi:10.1109/IWCMC51323.2021.9498656.

[100] Manik Lal Das. Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, 8(3):1086–1090, **2009**. doi:10.1109/TWC.2008.080128.

[101] Ashok Kumar Das, Saru Kumari, Vanga Odelu, Xiong Li, Fan Wu, and Xinyi Huang. Provably secure user authentication and key agreement scheme for wireless sensor networks. *Security and Communication Networks*, 9(16):3670–3687, **2016**. doi:https://doi.org/10.1002/sec.1573.

[102] Xiong Li, Jieyao Peng, Mohammad S. Obaidat, Fan Wu, Muhammad Khurram Khan, and Chaoyang Chen. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Systems Journal*, 14(1):39–50, **2020**. doi:10.1109/JSYST.2019.2899580.

[103] Chenyu Wang, Ding Wang, Guoai Xu, and Debiao He. Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0. *Science China Information Sciences*, 65(1):112301, **2021**. doi:10.1007/s11432-020-2975-6.

[104] Shanshan Tu, Muhammad Waqas, Sadaqat Ur Rehman, Muhammad Aamir, Obaid Ur Rehman, Zhang Jianbiao, and Chin-Chen Chang. Security in fog computing: A novel technique to tackle an impersonation attack. *IEEE Access*, 6:74993–75001, **2018**. doi:10.1109/ACCESS.2018.2884672.

[105] Mardiana binti Mohamad Noor and Wan Haslina Hassan. Current research on internet of things (iot) security: A survey. *Computer Networks*, 148:283–294, **2019**. ISSN 1389-1286. doi:https://doi.org/10.1016/j.comnet.2018.11.025.

[106] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brünig, and Georg Carle. Dtls based security and two-way authentication for the internet of

things. *Ad Hoc Networks*, 11(8):2710–2723, **2013**. ISSN 1570-8705. doi:https://doi.org/10.1016/j.adhoc.2013.05.003.

[107] Mukul Panwar and Ajay Kumar. Security for iot: An effective dtls with public certificates. In *2015 International Conference on Advances in Computer Engineering and Applications*, pages 163–166. **2015**. doi:10.1109/ICACEA.2015.7164688.

[108] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 26:96–99, **1978**.

[109] Zach Shelby, Klaus Hartke, and Carsten Bormann. The constrained application protocol (coap). RFC 7252, IETF, **2014**.

[110] Darrel Hankerson, Alfred Menezes, and Scott A. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, **2004**.

[111] Angelo Capossele, Valerio Cervo, Giuseppe De Cicco, and Chiara Petrioli. Security as a CoAP resource: An optimized DTLS implementation for the IoT. In *IEEE International Conference on Communications (ICC)*, pages 549–554. **2015**. doi:10.1109/ICC.2015.7248379.

[112] M.T. Hammi, E. Livolant, P. Bellot, et al. A lightweight iot security protocol. In *Cyber Security in Networking Conference (CSNet2017)*, page 7. **2017**. doi:10.1109/CSNET.2017.8242001.

[113] M.J. Dworkin. Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac. Special Publication SP 800-38D, NIST, Gaithersburg, **2007**. doi:10.6028/NIST.SP.800-38D.

[114] Y. Chen, X. Yang, T. Li, et al. A blockchain-empowered authentication scheme for worm detection in wireless sensor network. *Digital Communications and Networks*, **2022**. doi:10.1016/j.dcan.2022.04.007.

[115] S. Ismail, D. Dawoud, and H. Reza. Towards a lightweight identity management and secure authentication for iot using blockchain. In *2022 IEEE World AI IoT Congress (AIIoT)*, pages 077–083. Seattle, WA, USA, **2022**. doi:10.1109/AIIoT54504.2022.9817349.

[116] A.T. Milne, A. Beckmann, and P. Kumar. Cyber-physical trust systems driven by blockchain. *IEEE Access*, 8:66423–66437, **2020**. doi:10.1109/access.2020.2984675.

[117] M.T. Hammi, P. Bellot, and A. Serhrouchni. Bctrust: A decentralized authentication blockchain-based mechanism. In *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. **2018**. doi:10.1109/WCNC.2018.8376948.

[118] M.T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni. Bubbles of trust: A decentralized blockchain-based authentication system for iot. *Computers & Security*, 78:126–142, **2018**. doi:10.1016/j.cose.2018.06.004.

[119] P. Velmurugadass, S. Dhanasekaran, S. S. Anand, and V. Vasudevan. Quality of service aware secure data transmission model for internet of things assisted wireless sensor networks. *Transactions on Emerging Telecommunications Technologies*, 34(1):e4664, **2023**. doi:10.1002/ett.4664.

[120] J. Jung, J. Kim, Y. Choi, and D. Won. An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks. *Sensors*, 16:1299, **2016**. doi:10.3390/s16081299.

[121] L. Fengi, H. Zhang, L. Lou, and Y. Chen. A blockchain-based collocation storage architecture for data security process platform of wsn. In *IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 75–80. **2018**. doi:10.1109/CSCWD.2018.8465319.

[122] M.S. Christo, V.E. Jesi, U. Priyadarsini, et al. Ensuring improved security in medical data using ecc and blockchain technology with edge devices. *Security and Communication Networks*, pages 1–13, **2021**. doi:10.1155/2021/6966206.

[123] M. Adil, M.S. Khan, M.A. Jadoon, et al. An ai-enabled hybrid lightweight authentication scheme for intelligent iomt based cyber-physical systems. *IEEE Transactions on Network Science and Engineering*, pages 1–1, **2022**. doi:10.1109/tnse.2022.3159526.

[124] M.B.E Sajid, S. Ullah, N. Javaid, et al. Exploiting machine learning to detect malicious nodes in intelligent sensor-based systems using blockchain. *Wireless Communications and Mobile Computing*, pages 1–16, **2022**. doi:10.1155/2022/7386049.

[125] R. Fotohi, S.F. Bari, and M. Yusefi. Securing wireless sensor networks against denial-of-sleep attacks using rsa cryptography algorithm and interlock protocol. *International Journal of Communication Systems*, 33, **2019**. doi:10.1002/dac.4234.

[126] B. T. Asare, K. Quist-Aphetsi, and L. Nana. Towards a secure communication of data in iot networks: A technical research report. In M. Qiu, editor, *Algorithms and Architectures for Parallel Processing (ICA3PP) Lecture Notes in Computer Science*, volume 12454. Springer, Cham, **2020**. doi:10.1007/978-3-030-60248-2_39.

[127] P.K. Sharma, M.Y. Chen, and J.C. Park. A software defined fog node based distributed blockchain cloud architecture for iot. *IEEE Access*, 6:115–124, **2018**. doi:10.1109/access.2017.2757955.

[128] A. Moinet, B. Darties, and J. L. Baril. Blockchain based trust & authentication for decentralized sensor networks. arXiv preprint arXiv:1706.01730, **2017**. doi:10.48550/arXiv.1706.01730.

[129] K. Lewison and F. Corella. Backing rich credentials with a blockchain pki. Pomcor. com, **2016**.

[130] S. Hakak, W.Z. Khan, G.A. Gilkar, et al. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. *IEEE Network*, 34:8–14, **2020**. doi:10.1109/mnet.001.1900178.

[131] T-H. Kim, R. Goyat, M.K. Rai, et al. A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks. *IEEE Access*, 7:184133–184144, **2019**. doi:10.1109/access.2019.296060.

[132] J. Pan, J. Wang, A. Hester, et al. Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, 6:4719–4732, **2019**. doi:10.1109/jiot.2018.2878154.

[133] Seyyit Alper Sert. A multi-level blockchain-based nodeauthentication approach for uav-assisted wirelesssensor networks. In *2023 10th International Conference on Recent Advances in Air and Space Technologies (RAST)*, pages 1–6. **2023**. doi:10.1109/RAST57548.2023.10197943.

[134] Gao Liu, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. B4sdc: A blockchain system for security data collection in manets. *IEEE Transactions on Big Data*, 8(3):739–752, **2022**. doi:10.1109/TBDATA.2020.2981438.

[135] M. Satheesh Kumar, S. Vimal, N.Z. Jhanjhi, Shanmuga Sundar Dhanabalan, and Hesham A. Alhumyani. Blockchain based peer to peer communication in autonomous drone operation. *Energy Reports*, 7:7925–7939, **2021**. ISSN 2352-4847. doi:https://doi.org/10.1016/j.egyr.2021.08.073.

[136] Wajid Rafique, Maqbool Khan, Salabat Khan, and Juma Said Ally. Securemed: A blockchain-based privacy-preserving framework for internet of medical things. *Wireless Communications and Mobile Computing*, 2023:2558469, **2023**. ISSN 1530-8669. doi:10.1155/2023/2558469.

[137] Yan Zhuang, Lincoln R. Sheets, Yin-Wu Chen, Zon-Yin Shae, Jeffrey J.P. Tsai, and Chi-Ren Shyu. A patient-centric health information exchange framework using blockchain technology. *IEEE Journal of Biomedical and Health Informatics*, 24(8):2169–2176, **2020**. doi:10.1109/JBHI.2020.2993072.

[138] Shrabani Sutradhar, Sudipta Majumder, Rajesh Bose, Haraprasad Mondal, and Debnath Bhattacharyya. A blockchain privacy-conserving framework for secure medical data transmission in the internet of medical things. *Decision Analytics Journal*, 10:100419, **2024**. doi:10.1016/j.dajour.2024.100419.

[139] Xugang Zhang, Xinbiao Feng, Zhigang Jiang, Qingshan Gong, and Yan Wang. A blockchain-enabled framework for reverse supply chain management of power batteries. *Journal of Cleaner Production*, 415:137823, **2023**. ISSN 0959-6526. doi:https://doi.org/10.1016/j.jclepro.2023.137823.

[140] Aaliya Sarfaraz, Ripon K. Chakrabortty, and Daryl L. Essam. Accesschain: An access control framework to protect data access in blockchain enabled supply chain. *Future Generation Computer Systems*, 148:380–394, **2023**. ISSN 0167-739X. doi:https://doi.org/10.1016/j.future.2023.06.009.

[141] Yongjun Ren, Ding Huang, Wenhai Wang, and Xiaofeng Yu. Bsmd:a blockchain-based secure storage mechanism for big spatio-temporal data. *Future Generation Computer Systems*, 138:328–338, **2023**. ISSN 0167-739X. doi:https://doi.org/10.1016/j.future.2022.09.008.

[142] X.L. Liu, W.M. Wang, Hanyang Guo, Ali Vatankhah Barenji, Zhi Li, and George Q. Huang. Industrial blockchain based framework for product lifecycle management in industry 4.0. *Robotics and Computer-Integrated Manufacturing*, 63:101897, **2020**. ISSN 0736-5845. doi:https://doi.org/10.1016/j.rcim.2019.101897.

[143] Wenjuan Li, Christian Stidsen, and Tobias Adam. A blockchain-assisted security management framework for collaborative intrusion detection in smart

cities. *Computers and Electrical Engineering*, 111:108884, **2023**. ISSN 0045-7906. doi:https://doi.org/10.1016/j.compeleceng.2023.108884.

[144] Rajesh Kumar and Rewa Sharma. Leveraging blockchain for ensuring trust in iot: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10, Part A):8599–8622, **2022**. ISSN 1319-1578. doi:https://doi.org/10.1016/j.jksuci.2021.09.004.

[145] Adam Shostack. *Threat Modeling: Designing for Security*. Wiley, **2014**. ISBN 9781118809990.

[146] A. A. Herndon, M. Cramer, K. Sprong, and R. H. Mayer. Analysis of advanced flight management systems (fms), flight management computer (fmc) field observations trials, vertical path. In *2007 IEEE/AIAA 26th Digital Avionics Systems Conference*, pages 4.A.4–1–4.A.4–12. **2007**. doi:10.1109/DASC.2007.4391899.

[147] A. A. Herndon, M. Cramer, and T. Nicholson. Analysis of advanced flight management systems (fms), flight management computer (fmc) field observations, trials; lateral and vertical path integration. In *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*, pages 1.C.2–1–1.C.2–16. **2009**. doi:10.1109/DASC.2009.5347572.

[148] A. A. Herndon. Flight management computer (fmc) navigation database capacity. In *2012 Integrated Communications, Navigation and Surveillance Conference*, pages M6–1–M6–9. **2012**. doi:10.1109/ICNSurv.2012.6218426.

[149] An open-source document-oriented nosql database. `https://couchdb.apache.orgh`. Accessed: 2023-04-23.

[150] A free and open-source relational database management system. `https://www.postgresql.org`. Accessed: 2023-04-23.