electronics

MDPI

Article

Transforming Airport Security: Enhancing Efficiency through Blockchain Smart Contracts

Ioannis Karamitsos [1,*], Maria Papadaki [2,3], Khalil Al-Hussaeni [4] and Andreas Kanavos [5]

[1] Graduate Programs and Research, Rochester Institute of Technology, Dubai 341055, United Arab Emirates
[2] Faculty of Business and Law, BUiD Center for Risk and Innovation, British University in Dubai, Dubai 345015, United Arab Emirates; maria.papadaki@buid.ac.ae
[3] Department of Mechanical, Aerospace and Civil Engineering, University of Manchester, Manchester M139PL, UK
[4] Computing Sciences, Rochester Institute of Technology, Dubai 341055, United Arab Emirates; kxacad@rit.edu
[5] Department of Informatics, Ionian University, 49100 Corfu, Greece; akanavos@ionio.gr
* Correspondence: ixkcad1@rit.edu

Abstract: In the aviation industry, the issuance of airside passes often encounters significant delays, posing logistical challenges and hindering crucial operations. This study delves into the potential of implementing blockchain technology, particularly smart contracts, to streamline and expedite airport security processes. Our analysis of data from leading UK airports reveals notable inefficiencies in the current airside pass issuance procedures, necessitating a transformative solution. We advocate for the integration of blockchain smart contracts as a pioneering approach to substantially reduce processing times. By automating execution based on predefined conditions, smart contracts have the potential to revolutionize airport security operations. This research signifies a groundbreaking advancement in the use of smart contracts within the airline industry, underscoring the substantial efficiency improvements that can be achieved. As we conclude this study, we foresee further research and practical implementations to unlock the full transformative impact of blockchain technology on aviation security.

Keywords: airport; airside pass; blockchain; keyless signature infrastructure (KSI); operation; oracle; smart contract

Citation: Karamitsos, I.; Papadaki, M.; Al-Hussaeni, K.; Kanavos, A. Transforming Airport Security: Enhancing Efficiency through Blockchain Smart Contracts. *Electronics* **2023**, *12*, 4492. https://doi.org/10.3390/electronics12214492

Academic Editors: Amin Karami, Mustansar Ali Ghazanfar and Muhammad Awais Azam

Received: 20 September 2023
Revised: 18 October 2023
Accepted: 27 October 2023
Published: 1 November 2023

1. Introduction

The aviation industry undergoes constant evolution, driven by technological advancements and lessons learned from past incidents. Within this industry, procedures and standards are vital components ensuring safety and security. Over the past decade, the aviation sector has witnessed rapid transformation, fueled by external factors and innovative digital technologies [1]. Notably, the COVID-19 pandemic has triggered an economic crisis in the tourism industry, intensifying the urgency of digitizing the entire tourism ecosystem [2].

Given the aviation sector's inherent sensitivity, encompassing economic stability and security, there is a growing imperative for aviation professionals to lead in the digital revolution [3]. The integration of new digital technologies can yield significant benefits, including improved operational efficiency; cost-effectiveness; and enhanced safety measures. Aviation is a complex, dynamic industry with diverse stakeholders and high stakes tied to safety and security [4]. Given its international nature and the dispersion of stakeholders, data-driven decision-making has become paramount, necessitating swift and reliable data exchange solutions.

Aviation has always been a pioneer in innovation, contributing significantly to global trade and the economy [4]. Artificial intelligence (AI) and data science have gained prominence, offering insights into traffic analysis, predictions, and decision-making [1]. However, the adoption of blockchain technologies remains relatively unexplored in aviation.

This paper is a detailed investigation of the impact of blockchain technology on airport security, focusing on the critical area of airside airport operations. Due to strict security policies in airside areas, anyone with an airside pass must undergo a rigorous background check by the airport ID office. Ensuring the security of the airside pass issuance process requires validation from various third parties. This process, currently lasting from 1 to 3 months and relying on trust between parties for information, is prone to errors and the misuse of authority.

Among the time-consuming processes in airport operations, the issuance of identification passes stands out. There are two distinct areas within airports where employees work, with each requiring different types of passes: landside passes, which are less restrictive, and airside passes, which demand thorough security checks due to access to restricted and security-sensitive areas [5]. For this research, we focus on full airside passes for practical implementation purposes.

Hence, this study aims to improve the existing airside pass issuance process by identifying stakeholders and activities that can be replaced through blockchain technologies (smart contracts). It also presents a practical approach to replace human trust with cryptographic validation and reduce issuance time.

This study contributes to our understanding by addressing three key issues:

- Evaluating the processes and stakeholders involved in the airport ID issuance process in three different UK airports.
- Highlighting the vital role blockchain technology can play in the aviation industry.
- Providing practical use cases using smart contracts to bridge the gap between academia and practitioners.

The paper is organized as follows: Section 2 discusses the significance of aviation security and current practices and regulations associated with airport security checks. Section 3 outlines the research methodology employed, detailing the investigative approach and data collection methods used to analyze the integration of blockchain technology in airport security operations. Section 4 provides an overview of relevant studies that highlight the potential of blockchain technologies in the aviation industry and offers detailed discussions on these technologies. Section 5 presents a comprehensive use case involving three major UK airports in the issuance of airside passes, encompassing discussions on the existing process and the proposed blockchain-based process. In Section 6, we delve into the technical implementation details, providing insights into the tools, technologies, and methodologies employed in deploying the blockchain-based system for airside pass issuance. Furthermore, Section 7 offers a thorough discussion of the system's performance and its implications in the aviation industry. Finally, Section 8 concludes this paper by summarizing the key findings and insights acquired from this study, along with suggestions for future research in the field.

2. Related Work

The preservation of individuals' privacy and the assurance of information security have emerged as critical concerns across various industries, prompting extensive research efforts [6–9]. For instance, Qiu et al. [8] introduce a privacy-preserving monitoring system tailored for dietary intake, addressing the confidentiality of sensitive dietary data. Similarly, these works [7,10] put forth blockchain-based approaches to ensure the authenticity and traceability of information, contributing to data security. Nonetheless, this section underscores the context of privacy and security within the aviation industry, offering a focused perspective on addressing the unique challenges and requirements of this sector [11].

2.1. Aviation Security

The evolution of security procedures in aviation often stems from specific security incidents that trigger responses from the public [12]. This means that improvements in the aviation security landscape tend to be reactive rather than proactive [13]. Given the costs

associated with implementing changes in aviation security systems, it is crucial to ensure that the benefits outweigh the expenses.

The era of air travel saw rapid advancements in aircraft development following World War I as nations like France, Germany, and the United Kingdom competed to dominate the skies. With the emergence of international passenger flights, governments recognized the urgent need for international regulations governing air travel. The 1944 Chicago Convention gave birth to the International Civil Aviation Organization (ICAO), responsible for setting minimum standards for its 193 member nations [14]. These standards primarily addressed aviation safety and security and were subsequently adopted, adapted, and enforced by national governments, such as the US Congress in the United States and the European Parliament and Council in the European Union. National aviation authorities retain the right to impose stricter regulations if deemed necessary.

In the European Union, the European Union Aviation Safety Agency (EASA) was established in 2002 [15], while in the United States, the Federal Aviation Administration (FAA) was founded in 1958 [16] to monitor, standardize, and regulate safety measures. In response to the Pan Am Airways Flight 103 terrorist attack, the US Congress passed the Aviation Security Improvement Act of 1990 in 1990 [17]. This act mandated the "testing of security systems" and the strengthening of "control over individuals with access to aircraft".

The state of security preparedness is under constant scrutiny through security audits to ensure that standards are met. For instance, a 1993 audit of the FAA's Airport Security Program in four major US airports reported that 15 out of 20 attempts to gain access to restricted airport areas succeeded. The audit also highlighted the lack of reliable security systems. In 2016, approximately 300 passes for Sodexo catering firm's employees at Heathrow Airport were suspended on suspicion of fraudulent activities [18], and in 2019, an individual was arrested at Delhi's Indira Gandhi Airport for impersonating a Lufthansa pilot while dressed in a pilot's uniform and carrying a fake Lufthansa ID card acquired in Thailand [19].

These security measures come at a significant economic cost to municipalities and airlines, often diverting resources from other areas. The implementation of the 2012 ICAO Aviation Security Plan of Action, for example, was estimated to cost 17 million [20]. Airports typically fund new security developments by imposing higher airport taxes on passengers, which can lead to increased ticket prices for airlines, potentially affecting their competitiveness in the international market [13]. The challenge lies in deciding where to allocate resources to achieve cost-effectiveness and maximize security [21].

2.2. Airport Security Check

In 1987, David Burke, a former employee of Southwest Airlines, hijacked his former employer's passenger jet, leading to a tragic crash. Exploiting his familiarity with airport security procedures, Burke managed to bypass metal detectors and board Flight 1771 with a shotgun [22]. In response, stricter security policies were introduced for airport employees, emphasizing credentialing, which required employees to carry appropriate ID cards when entering restricted areas, and the implemention of rigorous background checks to obtain these ID cards [12].

The Aviation Security Improvement Act of 1990 [17] amended the Federal Aviation Act of 1958, mandating that individuals currently employed or seeking employment in positions with unescorted access to airport restricted areas must undergo an "identification and criminal history record check". Employers were expected to cover the costs of this check.

Regulation (EC) No 300/2008 of the European Parliament and the Council (2008) stated that individuals, including flight crew members, must successfully complete a background check before receiving a crew identification card or an airport identification card authorizing unescorted access to security restricted areas [23]. The Commission Implementing Regulation (EU) 2019/103 [23] amended this regulation, requiring individuals with access to security controls in security restricted areas to undergo an enhanced background

check. This enhanced check covers not only criminal records, employment history, and education but also includes intelligence information, reviewed annually. This process involves accessing government-held records in the UK (2022). However, not all countries can provide such information, posing challenges for flight crew who have worked in developing nations, potentially leading to employment termination if they fail the enhanced background check [24].

Obtaining relevant checks is a protracted process involving numerous independent parties and reliance on interacting databases, raising cybersecurity concerns [20]. This process heavily relies on trust, and even if the central authority is dependable, there is always a risk of data compromise by external parties [25]. Cyberattacks pose a significant threat to transportation databases, given the multitude of participants, such as transportation agencies and airlines, which are heavily dependent on data tracking and analysis systems for business operations [20]. Most internet systems were designed with practicality and cost-effectiveness in mind, often relying on a few critical nodes, rendering them vulnerable to cyberattacks [26].

In 2021, the U.S. Government Accountability Office (GAO) reported that U.S. government agencies still had cybersecurity weaknesses despite receiving GAO's list of 145 recommendations to improve cybersecurity [27].

Trust in government has been declining, prompting the exploration of decentralized infrastructure [28]. Governments recognize the shift in citizens' trust perception and the need for improved information exchange between the government and the public, enhancing public services [25]. An electronic ledger has the potential to facilitate information exchange among the public, government institutions, and businesses. The aim is not to eliminate public administration entirely but to enhance transparency, automation, and data integrity [28]. An electronic ledger can achieve higher data accuracy and consistency; eliminate errors; avoid fraudulent entries; and trace changes made to document issuance, such as certificates and ID cards, ensuring authenticity [29].

Finally, there is the issue of the time-consuming nature of background checks. In the age of digitalization, background checks in many countries still rely on manual database searches and the issuance of paper documents that require manual signatures and stamps from issuing institutions. In EU airports, a criminal record check must be obtained from any country where an individual has spent more than 6 months, a requirement set by the Aviation and Maritime Security Act 1990 in the UK [30]. This often involves checks in multiple countries for pilots. Depending on the country's rules, these checks must be obtained either from the country's police department or the embassy in the applicant's current location [30]. These documents must be original and not copies, obtained in person or via registered mail, as they contain confidential information. Depending on the language used by the issuing country, the document must be fully translated by a reliable source before submission. The examination of submitted criminal record check applications and other background checks by the airport ID Security Audit team can take up to 4 weeks [31]. Blockchain offers efficiency and cost savings by eliminating intermediaries from this process [32].

According to the IATA's Future of the Airline Industry report [33], 13 drivers of change will shape the aviation sector up to 2035, three of which directly impact aviation security: terrorism, cybersecurity, and the balance between data privacy and transparency. Blockchain technology has been identified as a major futuristic technology to drive these changes.

Blockchain technology can bring value to the aviation business in three categories, which are directly applicable to the airport employee credentialing process [34]:

- Simplifying business processes by reducing time and effort.
- Establishing a single source of truth for shared data, fostering industry collaboration.
- Providing a transparent and trusted proof of record.

3. Research Methodology

A systematic methodology was employed, involving a meticulous process for searching the existing body of related work, followed by a comprehensive evaluation and analysis of the literature. The systematic literature review followed four distinct steps.

The initial step involved formulating the research questions outlined in Section 1 to guide the direction of the investigation.

The second step entailed the identification of papers using specific keywords, primarily "blockchain", "technology airport", "airport operations", and "aviation industry", alongside "solution for blockchain technology". These keywords were required to appear in the title, abstract, or keywords of the papers included in our research. This search was conducted using two widely accessible web search engines that specialize in academic contributions: the ISI Web of Science (WoS) and Google Scholar (GS).

The third step encompassed identifying the data sources and establishing inclusion and exclusion criteria. The inclusion criteria included (a) papers that proposed, implemented, or tested a blockchain model or framework; (b) papers that addressed specific challenges or issues with blockchain technology; (c) guidelines and technical reports from standardization bodies; and (d) journal and conference publications. Papers that fulfilled the inclusion criteria were prioritized based on their citation count and examined to assess their relevance to the defined research questions. Exclusion criteria involved (a) papers that provided general information without in-depth analysis and (b) non-English publications.

The fourth step encompassed an archival data analysis by thoroughly examining the websites of the UK airports' infrastructure related to the process of airside pass issuance. The empirical analysis conducted on the selected UK airports was characterized by the following phases.

Firstly, the website of the airport system was analyzed to identify the type of content and information provided, focusing on the utilization of blockchain technology, sustainable performance, and the mission and vision of the organization.

Secondly, reports and official documents related to airport operations were collected and scrutinized. Various sources, including websites, as well as all available published documentation such as reports, documents, archival data, were thoroughly examined and investigated. The aim was to gain comprehensive insights into the current practices and regulations related to airport security checks, focusing on the process of airside pass issuance.

4. Blockchain in Airport Operation

In the ever-evolving aviation industry, technological innovations are continually tested to streamline processes, reduce costs, and maintain safety and security standards. However, innovation in aviation faces hurdles, primarily due to the industry's heavy reliance on intermediaries who may resist change to protect their profits or operational stability [35]. For instance, the dominance of global distribution systems (GDSs) like Amadeus, Travelport, and Sabre, controlling 99% of the air market share, has led to dissatisfaction within the aviation sector [2]. Blockchain technology offers a solution by eliminating intermediaries and reshaping the industry's power dynamics [35].

The concept of removing intermediaries has gained traction across industries, initially driven by the desire to decentralize finance [36]. Blockchain's potential applications have expanded to various sectors [37]. The International Air Transport Association (IATA) identified several areas in the aviation industry where blockchain could be beneficial [38]:

1. **Securing Procure-to-Pay Processes:** Blockchain can facilitate secure transactions and automate payments in complex supply chains, involving aircraft manufacturers, airlines, suppliers, and more. Smart contracts can automatically execute payments upon service delivery. Companies like Winding Tree have explored these possibilities, with Air Canada and Air France-KLM partnering to innovate travel distribution [39,40]. In 2021, Winding Tree partnered with American Airways to enable corporate clients to make bookings without intermediaries.

2. **Monitoring and Tracking:** Blockchain can enhance the tracking of cargo and aircraft spare parts. Lufthansa is exploring blockchain for aircraft maintenance, allowing technicians to access component information, including manufacturing, repair, and maintenance history [41].
3. **Tokenizing Assets:** Blockchain can tokenize assets such as frequent flyer points to prevent double-spending. Singapore Airlines, for instance, introduced KrisPay, a digital wallet allowing customers to use air miles for everyday purchases [42].
4. **Employee Authentication:** Blockchain can secure employee authentication processes. Its transparency and data tracking capabilities provide an independent approach to managing employee identities, eliminating issues such as data accessibility, integrity, misuse, fraudulent identities, and security threats [43]. Blockchain can limit cyberattacks and data manipulations by unauthorized individuals [44].

The decision to implement blockchain in a specific process often hinges on the level of trust between involved parties. Blockchain offers an immutable and tamper-proof way to bypass third parties and streamline processes [45]. IATA is also developing a digital certification authority (DCA) backed by AI, blockchain, and biometrics. In the future, DCA could potentially identify various aviation stakeholders, including passengers, travel agents, and aircrew [38]. IATA's Travel Grid project aims to provide a platform-as-a-service (PaaS) with blockchain capabilities, fostering the development of applications for passenger and crew identification management, cargo and aircraft spare parts tracking, frequent flyer point programs, business-to-business smart contracts, and industry payment systems [38].

4.1. Smart Contract

Vitalik Buterin, co-creator of Ethereum, envisioned blockchain as more than just an electronic payment system. In 2014, he authored the Ethereum White Paper [46], introducing additional blockchain applications like smart contracts and systems for moving digital assets based on predefined rules. Smart contracts function on an "if"-"then"-"else" basis. The concept of smart contracts was initially introduced by Nick Szabo in 1996 [47]. Szabo defined them as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" [48]. Unlike traditional legal documents, smart contracts are coded, and once executed on the blockchain, their terms and conditions are unalterable [49]. What blockchain offers is the creation of a digital contract that is safeguarded from deletion and tampering while being stored transparently for public access [50].

The use of smart contracts can be both beneficial and risky due to the lack of formal governance over legal and regulatory aspects of this new technology. Furthermore, Buterin [46] introduced the idea of the decentralized autonomous organization (DAO), a system that governs an entire organization based on a long-term smart contract. Ethereum was created to provide a platform with a fully built-in programming language, enabling individuals and organizations to build and execute smart contracts [46].

Bambara and Allen [49] define a smart contract as a program run on a blockchain expressed as a self-executing contract. It allows for the automated fulfillment of an activity if predefined conditions are met. These conditions are coded and, because smart contracts operate on a blockchain, they cannot be changed, ensuring secure and immutable governance.

4.2. KSI Hash Mechanism

When handling sensitive data, ensuring its privacy and security is paramount. Keyless signature infrastructure (KSI), a blockchain system used by the Estonian government and NATO, provides a solution for ensuring the integrity of digital documents through a proof-of-existence mechanism [51]. KSI was developed by Guardtime Enterprise Blockchain in 2007 [52]. It was originally introduced to support the Estonian government's efforts to manage trust in digital systems [53]. Over time, KSI has found applications in various domains, including cybersecurity, auditing, and certification [52].

KSI relies on one-way cryptographic hash functions to protect data privacy. These functions create a secure and immutable structure known as a hash tree, as illustrated in Figure 1.

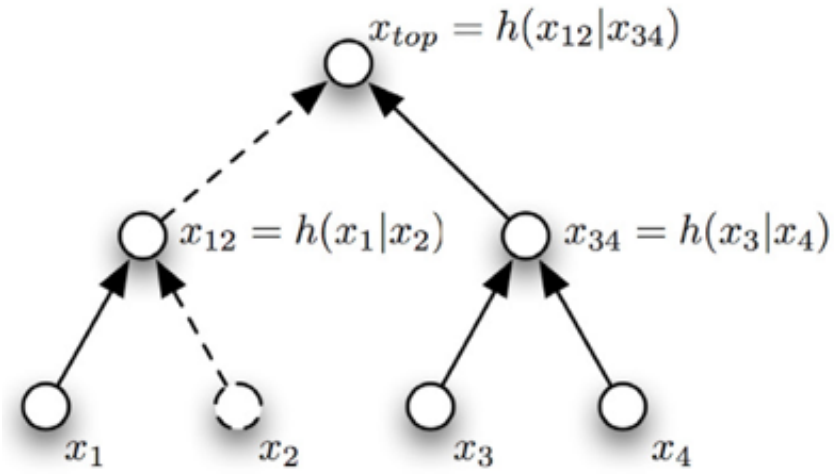

Figure 1. Hash tree in KSI.

In a hash tree, the hashes of multiple documents (y1–y4) are stored as leaves. Intermediate nodes are generated by hashing aggregated hashes from the layer below, and the top hash (ytop) represents the overall hash tree. This hierarchical structure allows for the efficient verification of data integrity by enabling rapid comparisons between hashes at different levels of the tree. If any part of the data changes, it will result in a cascade of hash value changes throughout the tree, making tampering evident during verification.

To further ensure data integrity, KSI employs timestamps. Data generated within the same time frame are stored within the same hash tree, preserving its state at a specific point on the timeline [32]. When data are submitted to the system, it is hashed into a string of keys known as a hash value. This hash value, along with a timestamp and the name of the signing authority, is added to the KSI Blockchain, as depicted in Figure 2.

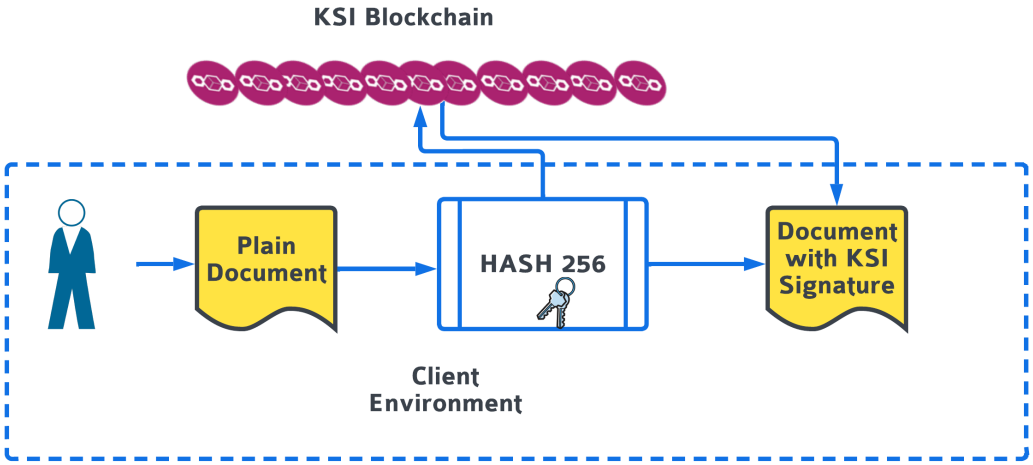

Figure 2. KSI blockchain.

This process creates a digital fingerprint that serves as proof of the document's integrity. Verification of the document can be achieved solely through the digital fingerprint, without the need to access the document itself. Importantly, using this type of blockchain ensures that the original data remains within the database, with only the hash being sent to the blockchain [54]. This approach safeguards against tampering with or compromising the original data.

The blockchain has evolved from being perceived as a speculative technology with ties to Bitcoin to becoming a business-focused solution with numerous practical applications [34]. Its appeal lies in its ability to guarantee data integrity, with each blockchain entry leaving a permanent record [32]. Achieved through a timestamp, where the hash of an entire block is published, this transparency allows anyone to verify precisely when data were published on the linear blockchain [55]. This feature is especially valuable for private or consortium-based blockchains and government use cases as data can remain private while integrity is ensured through timestamps [55].

For airport operation, an enhanced security method called homomorphic encryption (HE) is introduced. Homomorphic encryption is a groundbreaking cryptographic method that holds the promise of revolutionizing the way airports handle data privacy and security. In this paper, we delve into the intricacies of homomorphic encryption and its potential implementation in airside use cases. Traditional encryption methods require data to be decrypted before any meaningful operation can be performed on it. This act of decryption, albeit brief, exposes the data, rendering it vulnerable to cyber-attacks. Homomorphic encryption addresses this pitfall. It allows computations to be performed directly on encrypted data without ever needing to decrypt them. The result, when decrypted, remains accurate as if the operation were carried out on the raw data. In essence, HE ensures that data remain concealed throughout their lifecycle, irrespective of whether they are being transferred, stored, or processed. The benefits of implementing HE in airside use cases are as follows:

- **Enhanced Data Security:** HE ensures that sensitive data, whether its staff credentials, passenger information, or flight details, remain encrypted at all times. This provides a robust defense against potential data breaches or cyber-attacks.
- **Real-Time Operations:** Unlike traditional encryption methods, where the decryption process can introduce latency, HE facilitates real-time operations on encrypted data, ensuring that the pace of airside operations remains unhindered.
- **Regulatory Compliance:** With stringent data protection laws like GDPR in effect, airports need to be exceedingly cautious about how they handle personal data. HE offers a method to process these data without exposing it, aiding in regulatory compliance.
- **Trust and Reputation:** In an age where data breaches can tarnish reputations and lead to significant financial repercussions, adopting HE can bolster the trust of stakeholders, staff, and passengers in the airport's commitment to data privacy.

Homomorphic encryption, with its ability to perform computations on encrypted data, presents a golden opportunity for airports to enhance their security postures. By judiciously integrating HE into airside operations, airports can not only safeguard sensitive data but also usher in a seamless, efficient, and trust-enhancing operational paradigm.

4.3. Oracles

The issue with smart contracts is that a smart contract cannot trigger itself. It does not have access to external data unless the data are already added to a blockchain. The smart contract needs to be activated by either an external user or an oracle [49]. An oracle is essentially a bridge between the blockchain and the real world. It allows external data to be entered into the blockchain through an external transaction, as depicted in Figure 3.

Oracles play a crucial role in enabling smart contracts to interact with external data sources and systems. They can be used to access databases of different government agencies and push these data into the smart contract. There are different types of oracles, such as input oracles that deliver data onto the blockchain and output oracles that trigger the execution of specific actions [56].

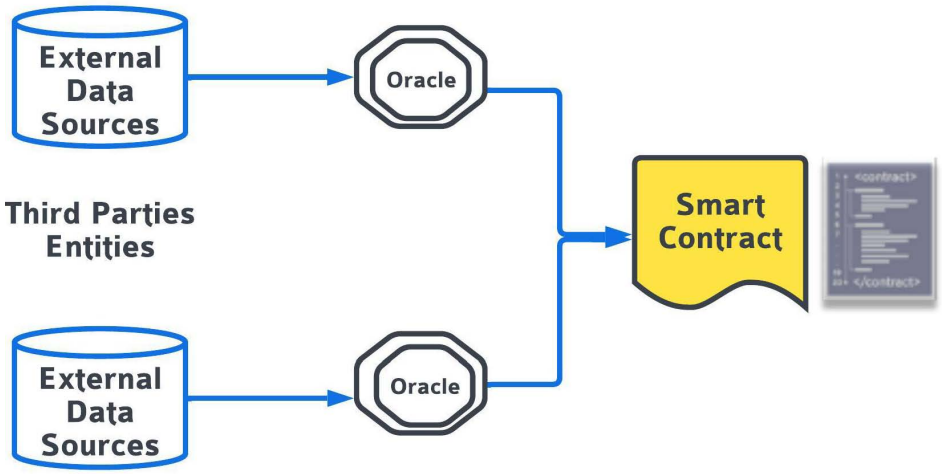

Figure 3. Oracle.

In the context of blockchain implementation for airport operations, oracles can facilitate interactions with various stakeholders and data sources, as depicted in the stakeholder map shown in Figure 4. These oracles can enable the smart contracts to access and validate data from government agencies, airlines, airport authorities, and other relevant entities, ensuring the accuracy and trustworthiness of the information used within the blockchain ecosystem.

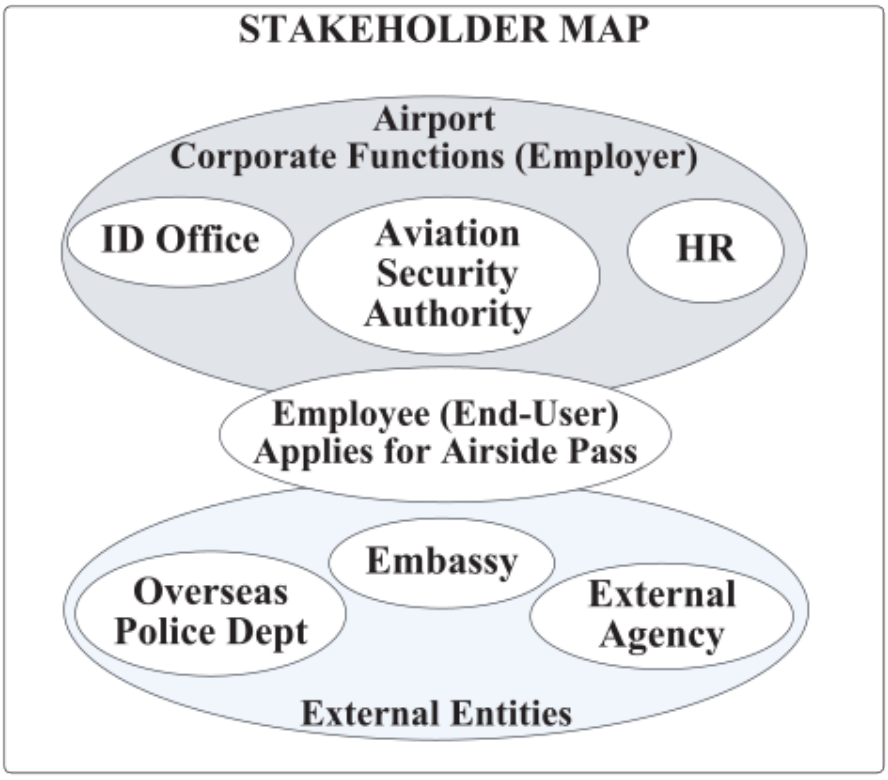

Figure 4. Stakeholder map.

Additionally, oracles can play a critical role in automating processes related to airport security, employee credentialing, and other operations, as illustrated in Figure 5. By securely connecting the blockchain to external data sources, oracles help ensure the integrity and efficiency of these processes within the airport environment.

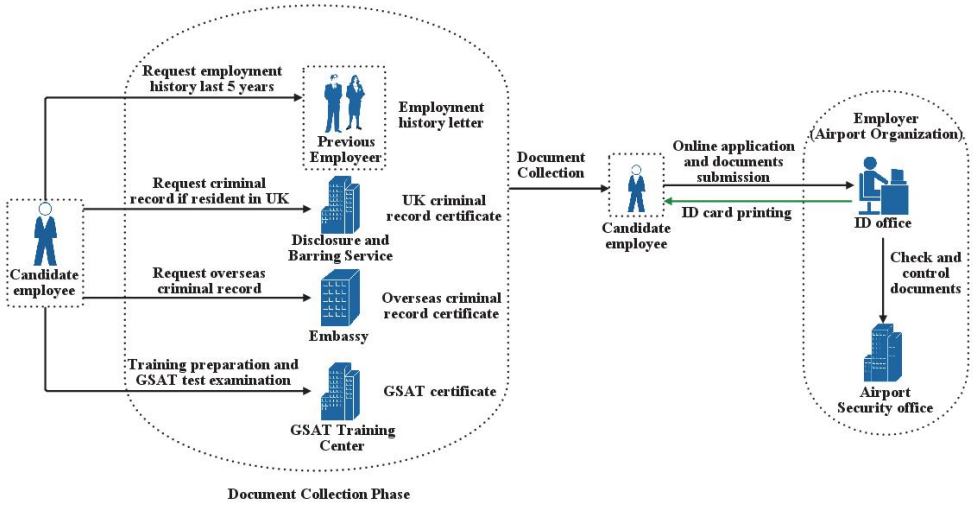

Figure 5. UK airside pass: existing process.

5. Use Case: Airside Pass

In this section, we present a comprehensive use case related to the issuance of the airside pass, incorporating data from official airport databases, publicly available records, and official documents from three major UK airports: Edinburgh [57], London Gatwick [58], and Manchester [59]. These airports provide explicit instructions on the application process for an airport ID and the associated background checks, outlined on their respective official websites.

For the implementation of this use case, a phased approach has been selected to ensure a methodical and well-structured deployment of the blockchain solution. The five phases include the following:

- **Phase 1: Problem Assessment:** Develop a clear vision and define business objectives through comprehensive assessments. The aim is to ensure that the blockchain solution addresses the specific use case and delivers results that optimize services and operational efficiency.
- **Phase 2: Organizational Readiness:** Engage blockchain subject matter experts to prepare the organization(s) for the blockchain solution. This phase involves setting up a project management office and establishing blockchain-tailored business, functional and technical requirements, and implementation plans.
- **Phase 3: Technology Selection:** Conduct a thorough investigation of various business considerations, such as the consensus mechanism, transaction costs, and on-chain/off-chain data requirements. Evaluate different types of blockchains, digital asset and distributed ledger technology (DLT) requirements, deployment models, and procurement options to create an optimal provider selection.
- **Phase 4: Blockchain Implementation:** Execute the implementation, customization, and configuration of the blockchain solution based on the chosen technology and requirements outlined in the previous phases.
- **Phase 5: Blockchain Integration:** Integrate the blockchain solution seamlessly into the infrastructure of the organization(s) involved, ensuring that it aligns with existing systems and processes.

Our objective is to construct a detailed workflow that encompasses all the activities and stakeholders involved in the airside pass issuance procedure, providing estimated timings for each activity based on the information obtained. Furthermore, we explore the potential of leveraging smart contracts using blockchain technology to streamline and expedite various steps in this process. The integration of smart contracts can significantly enhance the security, transparency, and efficiency of the overall airside pass issuance process.

5.1. UK Airports

In the UK, individuals cannot apply for an airside pass on their own behalf. Instead, applications must be submitted by sponsoring organizations with valid reasons for acquiring the pass. These sponsoring organizations must be registered with the airport's ID scheme and are responsible for gathering all required documents on behalf of their employees. To ensure compliance and document accuracy, many employers engage external vetting agencies. Regulations governing airside pass issuance are established by various authorities, including EU Regulation EC300 (2008), the Department for Transport (DFT), the Single Consolidated Direction (SCD) effective post-Brexit, and Local Airport Directives. Non-compliance or breaches of regulations can result in penalties under the Aviation Security Act 1982 and the Aviation and Maritime Security Act 1990.

The key information for constructing the process is categorized into three components: stakeholders, activities, and the time required.

The regulatory framework governing airside pass issuance comprises various authoritative sources, including:

- **(EU) Regulation EC300 (2008):** This European Union regulation lays out certain requirements and standards for airside pass issuance, ensuring a baseline of security across member states.
- **Department for Transport (DFT) Regulations:** The Department for Transport in the UK has its own set of regulations and guidelines concerning airside pass issuance and airport security.
- **Single Consolidated Direction (SCD):** This directive became effective on December 31st, 2021, as a consequence of the Brexit transition. It plays a crucial role in shaping the regulatory landscape for airside pass procedures.
- **Local Airport Directives:** In addition to national and international regulations, individual airports may have their own specific directives and procedures regarding airside pass issuance, tailored to their unique needs and security concerns.

Non-compliance with the established requirements to obtain an airside pass or any violations of these regulations can result in penalties, as stipulated under the Aviation Security Act 1982 and the Aviation and Maritime Security Act 1990. To construct a comprehensive understanding of the airside pass issuance process, we categorize the information into three vital components: stakeholders, activities, and the time required.

5.2. Conceptual Existing Process

The process for acquiring an airside pass at a UK airport comprises several steps. This existing process involves multiple stakeholders and often requires a significant amount of time due to the need for document verification and validation. The key stakeholders involved in this process include:

1. **External Agencies:** Many employers engage external vetting agencies to assist in the airside pass application process. These agencies receive and review documents, verify information, and request additional information if necessary.
2. **Employers:** The sponsoring organization, typically an employer, plays a central role in the process. Employers are responsible for providing employment history for the past years and applying for overseas criminal records on behalf of their employees.
3. **ID Office:** The ID office at the airport is responsible for several critical tasks, including checking the correctness of the submitted documents, submitting documents to the security audit team, and ultimately issuing the airside pass.
4. **Aviation Security Authority:** This authority is responsible for verifying the documents and conducting security audits. Their involvement is crucial for ensuring the security and integrity of the airside pass issuance process.

The primary goal in improving this process is to automate it to the extent that the involvement of these stakeholders is either minimized or eliminated entirely. This can be achieved through the integration of blockchain-based smart contracts, which offer transparency, security, and automation.

One of the primary challenges in the current process is trust. When employees submit documents, there is no way to guarantee that these documents have not been tampered with or falsified. However, if documents are directly requested from the issuing authorities, encrypted, and sent to a blockchain-based smart contract, this issue of trust can be mitigated.

Introducing smart contracts into the process ensures automatic execution once all predefined conditions are met, streamlining the process and reducing the need for manual intervention. To maximize efficiency and flexibility, the functionality can be divided into multiple smaller smart contracts, allowing for incremental adoption of blockchain technology.

5.3. Proposed Smart Contract Process

The proposed system design takes into consideration the stakeholders involved in the airside pass issuance and leverages blockchain-based smart contracts to enhance the security, immutability, and transparent execution of the issuance process. Figure 6 provides a visual representation of the steps involved in airside pass issuance using blockchain smart contracts and oracles.

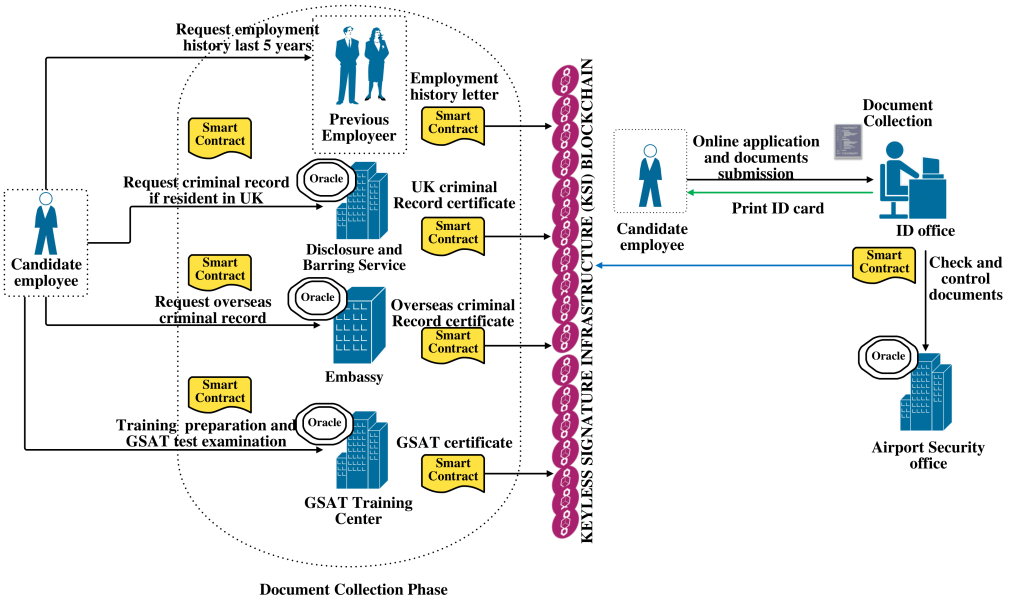

Figure 6. UK airside pass: process with smart contract.

The proposed process consists of seven key steps:

1. **Online Application:** The process begins with the employee filling out an online application on the airport ID platform, which is linked to the UK airport authority. This application is powered by blockchain technology. Since the UK airport ID office does not allow individuals to apply in person, a confirmation email is automatically sent to the employer if the employment information matches the email domain name. Upon confirmation by the employer, the smart contract automatically initiates the next step of the application.
2. **Employee Identification:** The employee submits their identification, which is verified using built-in Face-Match or similar technology. This technology compares the document submitted with an instant photo taken by a webcam or smartphone, ensuring identity verification.

3. **UK Criminal Record Check:** The employee submits a request for a criminal record check in the UK through the platform. By providing consent, the employee agrees to share the check results with the ID platform. An oracle is used to request data from the Disclosure and Barring Service, which is then pushed onto the smart contract. To ensure data privacy and integrity, the information is hashed using one-way cryptographic hash functions, and only the hash is stored on the KSI Blockchain.
4. **Overseas Criminal Record Check:** If required, the employee applies for an overseas criminal record check through the platform. If the country in question permits this, the record check is conducted online. However, if not, the employee can request the check in person and upload the results onto the platform. In this case, an oracle is utilized to request document verification from the issuing country. Once the results are received, they are pushed onto the smart contract. Similar to the local check, the information about overseas criminal records is added to the smart contract through an oracle, triggering an automatic response. To comply with EU data privacy rules, only a hash, or digital fingerprint, of the document is stored on the blockchain.
5. **GSAT Certificate Submission:** The employee submits their GSAT (Ground Security Awareness Training) certificate, a critical requirement for airside pass issuance.
6. **5-Year Employment Records:** The employee submits records of their 5-year employment history. These records are subject to verification. An automatic email confirmation is initiated to the employer mentioned in the application. If conditions such as the employer's email address matching the domain name and being publicly listed are met, verification proceeds.
7. **Airside Pass Issuance:** Once all the predefined conditions are met, the smart contract triggers the issuance of an airside pass for the employee. A command is sent to the ID office printer to produce the ID pass, and a notification is sent to the employee to collect the pass.

The proposed process streamlines the airside pass issuance, enhances security, and ensures transparency throughout the process. By leveraging blockchain technology and smart contracts, the need for manual intervention and the associated delays is significantly reduced.

6. Implementation

The practical realization of a decentralized tracking system on the Ethereum platform necessitates the utilization of an array of tools and technologies. These essential components include smart contracts, web3.js, Truffle, and Remix.

6.1. Front-End Interface

The airside system represents a typical example of a decentralized spplication (Dapp) operating within a blockchain network. The system architecture includes a front-end interface, comprising elements like a web browser, HTML, and CSS, designed to offer a user-friendly interaction platform for individuals engaging with the system.

The front-end interface empowers the airport ID office by facilitating access for various stakeholders, including employees, employers, agents, embassies, and law enforcement, to submit and review their requisite documents efficiently. Access to the blockchain network is made possible through the utilization of any cryptocurrency wallet application. For the implementation of the airside system, Metamask wallet was employed.

6.2. Hosting and Back-End

The front-end interface of airside seamlessly integrates with a robust back-end system. In this implementation, we harnessed the power of the Web3 JavaScript library, which serves as a vital conduit for interfacing with the Ethereum virtual machine (EVM) through JSON RPC. This interaction enables the smooth flow of data and transactions within the system, ensuring its decentralized and secure operation (refer to Figure 7 for an illustrative overview of the airside Dapp).

To make the airside system accessible to users, we have hosted the website on an Apache web server, while a MySQL database complements the back-end operations. This comprehensive setup ensures the effective functioning of airside, providing a robust and secure platform for managing airside pass issuance efficiently.

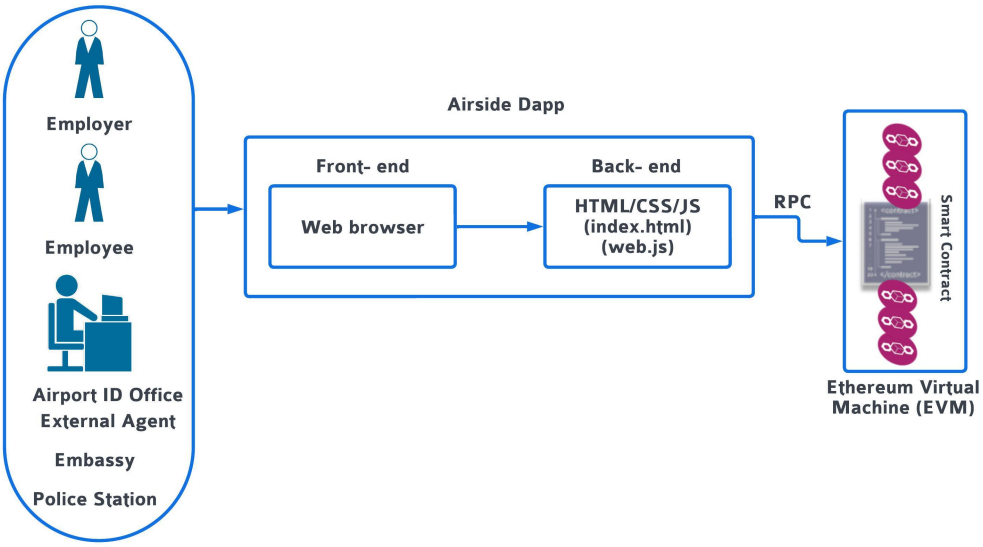

Figure 7. Airside Dapp.

6.3. Smart Contract

Creating a smart contract for the airside system entails a meticulous process that ensures its robustness and effectiveness:

- **Define the Functions and Variables:** The initial phase involves precisely defining the functions and variables that will govern the smart contract's behavior and interactions.
- **Coding:** Next, we delve into coding using Solidity, a language designed for writing secure and immutable smart contracts. This step demands stringent attention to detail as the code must guarantee the contract's security, prevent tampering, and execute the intended functions seamlessly, as illustrated in Figure 7.
- **Test and Debug:** Rigorous testing and debugging follow the coding phase to weed out any errors or vulnerabilities. This meticulous process ensures the smart contract's functionality and integrity.
- **Deploy on the Ethereum Network:** In the final stage, the smart contract is deployed onto the Ethereum public network. This deployment empowers the contract to execute its functions while securely storing airside ID card data on the Ethereum network.

The development of the smart contract stands as a pivotal milestone in the airside system's implementation on the Ethereum platform. It serves as the linchpin for data security, integrity, and transparent document tracking, making the entire system efficient and trustworthy.

6.4. Ethereum Network

The airside pass implementation is currently built upon a private Ethereum network, serving as the foundational infrastructure for the system. This Ethereum network operates as a decentralized network under a consensus algorithm, guaranteeing the secure and transparent storage of all transactions and data within the network. It is important to note that this network is distinct from the main Ethereum network, established to facilitate the management and oversight of the testbed environment.

This dedicated Ethereum network operates through the use of the Ganache tool, providing a personal blockchain environment. This private network allows for the deploy-

ment and rigorous testing of systems within a confined and controlled network, ensuring a reliable and secure testing environment for the airside pass implementation.

6.5. Deployment of the Smart Contract

To deploy the smart contract, you have two options: using the Truffle tool or the Remix Solidity compiler. Ensure that you have completed all the necessary prerequisites before proceeding with this step. In the case of airside, we opted for the Remix Solidity compiler. After deploying the smart contract, you will need to insert the smart contract's address into the JavaScript code, which connects to the Ethereum node.

The implementation process of the system has been executed successfully, and rigorous testing has been conducted on a local Ethereum network employing the Ganache tool. The test results affirm the system's functionality and efficiency.

The primary objective of the airside system is to offer a secure and transparent means of storing vaccination records on the blockchain. The results conclusively demonstrate the system's ability to securely store documents on the Ethereum network, ensuring that records are exclusively accessible to authorized individuals and the Airport ID issuance office.

6.6. Performance Analysis

The performance evaluation of the airside system was conducted, taking into consideration several critical metrics, namely, time, memory, gas consumption, and overall system efficiency. Here are the findings of the performance analysis:

- **Memory Usage:** To assess memory usage in airside transactions, we utilized the v8 module provided by Node.js, which grants access to low-level performance metrics, including memory consumption. The employee registration transaction, a crucial transaction within the system, was examined. It was observed that the employee registration transaction consumed 787,412 bytes of memory. This indicates that this transaction demands a significant amount of memory during execution. When compared to the memory usage of other transactions in the system, it becomes apparent that the employee registration transaction is more memory-intensive.
- **Time Duration:** In addition to memory usage, we measured the time taken for transactions to complete. The duration was calculated from the initiation of the transaction with *eth_estimateGas* until its execution with *eth_sendTransaction*. The registration transaction, due to its complexity and the substantial amount of data to be stored on the blockchain, took approximately 5.892 s to complete. While this transaction takes longer compared to simpler transactions, the time duration falls within acceptable limits for a single transaction.
- **Gas Usage:** Gas is a measure of the computational effort required to execute a transaction in the Ethereum network. To evaluate gas usage in the airside system's employee registration transaction, we employed the *eth_estimateGas* method provided by the Web3.js library, which estimates the required gas before sending the transaction to the network. The measured gas usage for the user registration transaction was 563,328 Wei. Although higher than the gas usage of some simpler transactions, this amount is still within acceptable limits for a transaction of its complexity. It is important to note that gas usage can impact the cost of executing a transaction in the Ethereum network. It is crucial to consider that actual gas usage in the Ethereum main network may differ due to network congestion and gas price fluctuations.

The performance evaluation results indicate that the airside system performs well in terms of time and memory usage, with transactions being efficiently confirmed and added to the blockchain. However, gas consumption is relatively high, suggesting potential opportunities for optimization. Overall, the airside system effectively achieves its specified goals and objectives, and its performance is deemed satisfactory.

7. Discussion

This study delved into the potential impact and efficiency of integrating blockchain smart contracts within Airport Security Operations. Our analysis, showcased in Table 1, sheds light on how these innovations can be instrumental in revolutionizing airport security procedures, ultimately leading to a more agile and secure airside pass issuance process.

Table 1. Activities time for the issuance of full airside pass in UK.

Stakeholders	Activities	Duration without Smart Contract	Duration with Smart Contract
Employee	a. Provide employment history for the past years b. Apply for overseas criminal records	15 days on average	5 days
Employer	a. Provide employment history for the past years b. Apply for overseas criminal records	3–5 weeks	1 week
External Agency	a. Receive documents b. Verify information c. Request more information if required	3–5 weeks	1 week
ID Office	a. Check the correctness of the documents b. Submit documents to the security audit team c. Issues the ID pass	4–5 weeks	1 week
Aviation Security Audit	Verification of the documents	4–5 weeks	1 week
Embassy	a. Request a criminal record check b. Provide a clearance certificate to the employee	10–15 days	5 days
Overseas Police Department	a. Check person name through the criminal record database b. Provide a police certificate clearance to the employee	1–15 days	5 days

The key takeaways from our analysis are as follows:

- **Enhanced Efficiency:** The implementation of blockchain smart contracts has the potential to significantly expedite various critical activities within the airside pass issuance process. Notably, it can reduce the time required for employees, employers, external agencies, ID offices, aviation security audits, embassies, and overseas police departments to complete their respective tasks.
- **Reduction in Processing Time:** By automating and streamlining document verification, background checks, and other key steps, the processing time for airside pass issuance can be considerably shortened. This reduction in processing time directly contributes to quicker issuance and reduced delays associated with manual processes.
- **Data Integrity and Security:** Smart contracts, complemented by one-way cryptographic hash functions and blockchain technology, ensure the privacy and integrity of sensitive data, such as criminal record checks. This approach aligns with data privacy regulations while providing a secure and immutable record of the verification process.
- **Streamlined Verification:** Automation plays a pivotal role in streamlining the verification process. Smart contracts and oracles handle verification tasks efficiently, significantly reducing the need for manual intervention. This results in a more efficient and error-resistant system.

- **Overall Operational Efficiency:** The combination of these benefits translates into an overall enhancement of operational efficiency within airport security operations. Faster processing times, reduced reliance on external agencies, and improved data security together create a more agile and secure airside pass issuance procedure.

In conclusion, the integration of blockchain smart contracts offers a transformative potential for airport security operations, especially in the context of airside pass issuance. The automation of critical processes, the reduction in processing times, and enhanced data security collectively pave the way for a more efficient, secure, and reliable system.

As these innovations continue to evolve, it is imperative for airport authorities to consider their adoption, bearing in mind the tangible benefits they bring to the table. While challenges may exist in transitioning to such advanced systems, the potential rewards in terms of operational efficiency and security far outweigh the initial hurdles.

This study serves as a stepping stone towards understanding the promise of blockchain smart contracts in revolutionizing airport security operations, and we hope it inspires further research and implementation in this field.

8. Conclusions and Future Work

In the airline industry, expediency is often paramount, especially when it comes to processes like granting new employees access to the external, airside areas of airports. Unfortunately, such processes have been hindered by prolonged timelines, making swift access approvals a challenge. Based on an analysis of publicly available information from three prominent UK airports, our study unveiled that the issuance of airside passes frequently takes weeks, as summarized in Table 1.

To address this inefficiency, we propose a groundbreaking solution involving the integration of blockchain technology, specifically smart contracts. Smart contracts are autonomous computer programs designed to execute actions based on predefined conditions. In our novel application, we advocate for the incorporation of smart contracts into the airside pass issuance process, with the primary objective of significantly reducing the time required for successful completion.

This study pioneers the use of smart contracts within the airline industry, heralding a new era of efficiency and responsiveness in critical processes. Preliminary assessments suggest that the introduction of smart contracts could expedite processing times by nearly threefold.

As we conclude this phase of our research, it is important to highlight avenues for future studies and acknowledge the limitations of the current research. For future work, a comprehensive original survey could be conducted to validate and expand upon the findings of this study, providing a more comprehensive understanding of the implications of blockchain integration in airport security. Furthermore, it is essential to recognize the limitations and constraints of the current research, which include the focus on a specific set of UK airports and the reliance on publicly available data. Acknowledging these limitations contributes to a more transparent and comprehensive interpretation of the results, providing valuable insights for further research in this area.

Author Contributions: Conceptualization, I.K., M.P., K.A.-H. and A.K.; Data Curation, I.K., M.P., K.A.-H. and A.K.; Writing—Original Draft, I.K., M.P., K.A.-H. and A.K.; Methodology, I.K., M.P., K.A.-H. and A.K.; Review and Editing, I.K., M.P., K.A.-H. and A.K.; Supervision, I.K., M.P., K.A.-H. and A.K. These authors contributed equally to this work. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported in part by the DSO-RIT Dubai Research Fund (2023-24-1004) from Rochester Institute of Technology—Dubai (RIT-Dubai).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Pereira, A.; Lohmann, G.; Houghton, L. Innovation and value creation in the context of aviation: A systematic literature review. *J. Air Transp. Manag.* **2021**, *94*, 102076. [CrossRef]
2. Lopes, P.; Rita, P.; Treiblmaier, H. The impact of blockchain on the aviation industry: Findings from a qualitative study. *Res. Transp. Bus. Manag.* **2021**, *41*, 100669.
3. Baykov, F. Digital Transformation of the world market of aviation services. *E-Management* **2020**, *3*, 70–76. [CrossRef]
4. Ahmad, R.; Salah, K.; Jayaraman, R.; Hasan, H.; Yaqoob, I.; Omar, M. The Role of Blockchain Technology in Aviation Industry. *IEEE Aerosp. Electron. Syst. Mag.* **2021**, *36*, 4–15. [CrossRef]
5. Vonitsanos, G.; Panagiotakopoulos, T.; Kanavos, A.; Tsakalidis, A.K. Forecasting Air Flight Delays and Enabling Smart Airport Services in Apache Spark. In Proceedings of the Artificial Intelligence Applications and Innovations, AIAI, Hersonissos, Greece, 25–27 June 2021; Springer: Cham, Switzerland, 2021; Volume 628, pp. 407–417.
6. Han, J.; Susilo, W.; Mu, Y.; Zhou, J.; Au, M.H.A. Improving Privacy and Security in Decentralized Ciphertext-Policy Attribute-Based Encryption. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 665–678. [CrossRef]
7. Hu, J.; Zhu, P.; Qi, Y.; Zhu, Q.; Li, X. A patent registration and trading system based on blockchain. *Expert Syst. Appl.* **2022**, *201*, 117094. [CrossRef]
8. Qiu, J.; Lo, F.P.W.; Gu, X.; Jobarteh, M.L.; Jia, W.; Baranowski, T.; Steiner-Asiedu, M.; Anderson, A.K.; Mccrory, M.A.; Sazonov, E.; et al. Egocentric Image Captioning for Privacy-Preserved Passive Dietary Intake Monitoring. *IEEE Trans. Cybern.* **2023**, 1–14. [CrossRef] [PubMed]
9. Vonitsanos, G.; Panagiotakopoulos, T.; Kanavos, A.; Maragoudakis, M.; Mylonas, P. Issues and Challenges associated with Blockchain in Smart Cities. In Proceedings of the 16th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP), Corfu, Greece, 4–5 November 2021; pp. 1–5.
10. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using Blockchain Technology to Enhance the Traceability of Original Achievements. *IEEE Trans. Eng. Manag.* **2023**, *70*, 1693–1707. [CrossRef]
11. Kanavos, A.; Kounelis, F.; Iliadis, L.; Makris, C. Deep learning models for forecasting aviation demand time series. *Neural Comput. Appl.* **2021**, *33*, 16329–16343. [CrossRef]
12. Price, J.; Forest, J. *Practical Aviation Industry*, 2nd ed.; Elsevier: Amsterdam, The Netherlands, 2013.
13. Cunha, D. Making sense of airport security in small and medium-sized airports. In *The Air Transportation Industry*; Macario, R., Voorde, E.v.d., Eds.; Elsevier: Amsterdam, The Netherlands, 2022; pp. 247–272.
14. ICAO. About ICAO. 2022. Available online: https://www.icao.int/about-icao/Pages/default.aspx (accessed on 12 February 2023).
15. EASA. The Agency. 2022. Available online: https://www.easa.europa.eu/the-agency/the-agency (accessed on 10 January 2023).
16. FAA. A Brief History of FAA. 2022. Available online: https://www.faa.gov/about/history/brief_history#birth (accessed on 8 November 2022).
17. AviationAct1990. Aviation and Maritime Security Act 1990. 1990. Available online: https://www.congress.gov/101/statute/STATUTE-104/STATUTE-104-Pg3066.pdf (accessed on 8 November 2022).
18. Al-Othman, H. 300 Heathrow Staff Have Passes Suspended Amid Security Scam Probe. 2016. Available online: https://www.standard.co.uk/news/crime/investigation-launched-into-security-pass-scam-at-heathrow-airport-a3317371.html (accessed on 17 March 2022).
19. Suri, M. Man arrested at Indian Airport for Impersonating Lufthansa Pilot, 2019. Available online: https://edition.cnn.com/travel/article/india-fake-lufthansa-pilot-arrest/index.html (accessed on 17 March 2022).
20. Szyliowicz, S.J. Aviation Security: Promise or Reality? In *Homeland Security and Terrorism*; Howard, J.R., Moore, J., Eds.; McGraw-Hill Education: New York, NY, USA, 2017; pp. 127–146.
21. Poole, R. The case of risk-based aviation security. *World Cust. J.* **2009**, *3*, 3–16.
22. King, P.; Malnic, E. From the Archives: Crash of a Pacific Southwest Airlines Jetliner Centers on Fired Employee. 1987. Available online: https://www.latimes.com/la-me-pacific-southwest-airlines-crash-archive-19871209-story.html (accessed on 8 October 2022).
23. Commission, E. COMMISSION IMPLEMENTING REGULATION (EU) 2019/103. 2019. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0103&from=IT (accessed on 23 July 2022).
24. ECA. Enhanced Pilot Background Checks to Feature Intelligence Information. 2019. Available online: https://www.eurocockpit.be/news/enhanced-pilot-background-checks-feature-intelligence-information (accessed on 23 July 2022).
25. Shahaab, A.; Maude, R.; Hewage, C.; Khan, I. Blockchain: A Panacea for Trust Challenges In Public Services? A Socio-technical Perspective. *J. Br. Blockchain Assoc.* **2020**, *3*, 1–11. [CrossRef] [PubMed]
26. Cilluffo, F.; Pattak, B. Cyber Threats: Ten Issues to Consider. In *Homeland Security and Terrorism*; Howard, J.R., Moore, J., Eds.; McGraw-Hill Education: New York, NY, USA, 2017; pp. 186–194.
27. GAO. Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges. 2021. Available online: https://www.gao.gov/assets/gao-21-288.pdf (accessed on 23 February 2023).
28. Allessie, D.; Sobolewski, M.; Vaccari, L. Blockchain for Digital Government. In *Blockchain for Government and Public Services: Realizing the Potential*; Pignatelli, F., Ed.; Publications Office of the European Union: Luxembourg, 2019; pp. 57–66.
29. Olnes, S.; Ubacht, J.; Janssen, M. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Gov. Inf. Q.* **2017**, *34*, 355–365. [CrossRef]

30. Airports, A. Guidelines Full Airside ID Pass. 2017. Available online: https://www.glasgowairport.com/media/1692/check-airside-pass.pdf (accessed on 23 April 2022).
31. Airport, C.N. Instruction—How to Apply for a Background Check, 2022. Available online: https://luftfartstilsynet.no/globalassets/dokumenter/bakgrunnssjekk/instruction---how-to-apply-for--background-check---english.pdf (accessed on 23 April 2022).
32. Martinovic, L.K.I.; Sluganovic, I. Blockchains for Governmental Services: Design Principles, Applications, and Case Studies. *Cent. Technol. Glob. Aff.* **2017**, *7*. Available online: https://www.ctga.ox.ac.uk/article/blockchains-governmental-services-design-principles-applications-and-case-studies (accessed on 23 April 2022).
33. IATA. Future of the Airline Industry 2035. 2018. Available online: https://www.iata.org/contentassets/690df4ddf39b47b5a075bb5dff30e1d8/iata-future-airline-industry-pdf.pdf (accessed on 12 May 2022).
34. McLaughlin, B. Are We Heading into the Teenage Years of Blockchain? Available online: https://www.sita.aero/pressroom/blog/are-we-heading-into-the-teenage-years-of-blockchain/ (accessed on 22 January 2023).
35. Izmaylov, M.; Anderson, P.; Lemble, A.; Vysoky, J. A Practical Application of Blockchain for the Travel Industry. 2018. Available online: https://static1.squarespace.com/static.pdf (accessed on 22 March 2023).
36. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org, 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 22 March 2023).
37. Treiblmaier, H. Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies. *Front. Blockchain* **2009**, *2*. [CrossRef]
38. IATA. Blockchain in Aviation Exploring the Fundamentals, Use Cases, and Industry Initiatives. 2018. Available online: https://www.iata.org/contentassets/blockchain-in-aviation-white-paper.pdf (accessed on 12 May 2022).
39. AirCanada. Air Canada Partners with Winding Tree on a Blockchain-Based Travel Distribution Platform. 2018. Available online: https://aircanada.mediaroom.com/2018-10-24-Air-Canada-Partners-with-Winding-Tree-on-a-Blockchain-based-Travel-Distribution-Platform (accessed on 12 May 2023).
40. AirFrance-KLM. AirFrance-KLM partners with Winding Tree to Strengthen Innovation in the Travel Industry Using Blockchain Technology. 2018. Available online: https://www.airfranceklm.com/en/air-france-klm-partners-winding-tree-strengthen-innovation-travel-industry-using-blockchain (accessed on 10 January 2023).
41. Schwabe, L. Generating More Transparency in Aviation with Blockchain Technology. 2022. Available online: https://www.lufthansa-industry-solutions.com/de-en/solutions-products/aviation/generating-more-transparency-in-aviation-with-blockchain-technology (accessed on 12 January 2022).
42. Airlines, S. KrisFlyer Launches Innovative Miles-Based Digital Wallet, KrisPay. 2018 Available online: https://www.singaporeair.com/en_UK/sg/media-centre/press-release/article/?q=en_UK/2018/July-September/ne2518-180724&affc=ebefbc33-8d3d-406c-8d34-d4da90e35cee (accessed on 12 November 2021).
43. Das, K.V. Blockchain and Its Use Cases in the Airline Industry. 2020. Available online: https://www.blockchain-council.org/blockchain/blockchain-and-its-use-cases-in-the-airline-industry/ (accessed on 13 August 2022).
44. Kshetri, N. Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [CrossRef]
45. Irvin, C.; Sullivan, J. Using Blockchain to Streamline Airline Finance. 2018. Available online: https://www2.deloitte.com/us/en/pages/consulting/articles/airlines-blockchain-finance.html?nc=1 (accessed on 23 September 2022).
46. Buterin, V. Ethereum: A Next Generation Smart Contract and Decentralized Application Platform, 2014. Available online: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf (accessed on 23 September 2022).
47. Schär, F. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Fed. Reserve Bank St. Louis Rev.* **2021**, *2*, 153–174. [CrossRef]
48. Szabo, N. Samrt Contracts: Building Block for Digital Markets. 1996. Available online: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (accessed on 18 March 2022).
49. Bambara, J.; Allen, P. *Blockchain: A Practical Guide to Develop Business, Law, and Technology Solutions*, 1st ed.; McGraw-Hill Education: Cambridge, MA, USA, 2018.
50. Iansiti, M.; Lakhani, K. The Truth About Blockchain. *Harv. Bus. Rev.* **2017**, *2*, 118–127.
51. Castaños, V. *Case Study Report: E-Estonia*; Publications Office of the European Union: Luxembourg, 2018.
52. Guardtime. About Guardtime. 2022. Available online: https://www.//guardtime.com/about (accessed on 20 March 2022).
53. E-estonia. KSI Blockchain Stack: Zero Trust Applications. 2022. Available online: https://www.digiexpo.e-estonia.com/Solutions/guardtime-ksi-blockchain-stack/html (accessed on 20 March 2022).
54. PwC. Estonia—The Digital Republic Secured by Blockchain. 2019. Available online: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf (accessed on 24 March 2022).
55. Meyer, R. *Keys to Bitcoin: Learn How Bitcoin Really Works*, 1st ed.; Bowker: Chatham, NJ, USA, 2021.
56. Chainlink. What Is a Blockchain Oracle? 2021. Available online: https://chain.link/education/blockchain-oracles (accessed on 24 April 2022).
57. Airport, E. Airport ID Pass Scheme Standards, 2021. Available online: https://assets.ctfassets.net/2hwzhse7szu0/2u7h6oMjbe9TR0FEd1T02w/265d93121f9ba0873862dd42083fdd16/ID_Pass_Application_Standard_V9.pdf (accessed on 24 April 2022).

58. Airport, G. IDC Pass Regulations September 2019. 2019. Available online: https://business.gatwickairport.com/globalassets/company/id-centre/id-pass-regulations.pdf (accessed on 17 December 2022).
59. Airport, M. MAG Standard/SIDS/29.07.2015. 2015. Available online: http://mag-umbraco-media-live.s3.amazonaws.com/1004/magpluspassplusinstructions.pdf (accessed on 10 October 2022).