Securing Immigrant Identity: A Survey of Blockchain Applications in Data Management

Tanvi Kamble[1], Yash Dubey[2], and Kushagri Nayak[3]

[1,2,3] *Smt. Indira Gandhi College of Eng., Navi Mumbai*

Abstract-The current immigrant data management systems in India are outdated and inefficient, heavily relying on a combination of paper-based documentation and fragmented digital records. Such old traditional systems harbour significant risks, including data integrity issues, security vulnerabilities, and delays in monitoring the status and movements of immigrants, particularly refugees who often lack formal travel documents. The paper tries to explore the potential of using blockchain technology for solving the above concerns. Using blockchain's decentralized and unadulterated aspect along with tracking technologies such as a system of QR codes, SIM card-based tracking, and GPS, this paper will address how blockchain can improve data security, document verification, and real-time immigrant tracking. This paper will also evaluate the use of cryptographic hashing, Web3.js for blockchain interactions, and smart contracts to automate processes and ensure the integrity of documents like passports and visas. This paper shall attempt to present a comprehensive review that speaks to the current advancement in secure data management systems, specifically calling attention to the growth potential of blockchain and decentralized storage solutions like IPFS with respect to simplifying complexity in immigrant data management.

Index words- Blockchain Technology, Immigrant Data Management, Document Verification, QR Code Systems, SIM Card Tracking, GPS Tracking, IPFS (Inter-Planetary File System), Biometric Data Storage, Cryptographic Hashing, SHA-256, RSA Algorithm, Smart Contracts, Digital Identity, Decentralized Storage, Ethereum Blockchain, Location Tracking, Real-Time Monitoring, REST APIs, Elliptic Curve Digital Signature Algorithm (ECDSA), Web3.js, Proof-of-Work (PoW), Decentralized Identifiers (DIDs), Public Key Cryptography, Legal Compliance, Government Records.

I. INTRODUCTION

Managing immigrant data has become a critical issue in today's global landscape, particularly in India, where the systems in place are outdated and inefficient. These systems rely heavily on a combination of paper documents and fragmented digital records, which creates security vulnerabilities, data integrity issues, and inefficiencies in tracking the movement and status of immigrants. The need for a unified, secure platform is especially pressing for refugees, who often lack formal documentation and require stringent reporting and tracking mechanisms to ensure compliance with legal processes.

A way forward to overcome these problems is indeed blockchain technology. Decentralized and immutable blockchain-based solutions ensure safe handling of sensitive data regarding immigrants, such as passports, visas, and biometric information. Platforms like Ethereum facilitate the creation of smart contracts, which can automate processes such as document verification, visa expiration alerts, and compliance monitoring, reducing the potential for human error and fraud. There is also transparency in how blockchain technology ensures data integrity while allowing authorized parties live access to critical information.

In conjunction with blockchain, decentralized storage includes Inter-Planetary File System (IPFS) to store large datasets in the form of biometric data and scanned documents. The files will be stored off-chain but referenced through blockchain records for data privacy allied with immutability. For example, dealing with blockchain platforms will not be difficult with technologies like Web3.js, while stakeholders will be able to acquire, update, and authenticate their immigrant data without loss of security.

Moreover, real-time tracking technologies like QR codes, SIM card-based systems, and GPS can be integrated with blockchain to monitor immigrant movements. For refugees, automated reporting systems that send alerts via blockchain-based smart contracts can ensure compliance with legal obligations. The problem of data management on the side of the refugee will, henceforth be efficiently addressed by blockchain technologies.

II. METHODOLOGY

Our survey was conducted with the objective of identifying and evaluating blockchain-based

technologies that can effectively address the challenges in managing immigrant data. According to our approach: a thorough and systematic review of academic literature, technical reports, and case studies, with special focus on application in blockchain, decentralized storage, and tracking systems within sectors including immigration, education, healthcare, and even based on compliance with the law.

The research process began with a targeted keyword search on leading academic databases, including ACM Digital Library, Google Scholar, Springer, and IEEE Xplore. Specific keywords were employed to refine the search, such as "blockchain for secure immigrant data storage," "blockchain for document verification in immigration," "QR code-based tracking using blockchain," "SIM card tracking for refugees," "IPFS for storing biometric data," and "cryptographic hashing for securing documents." The key purpose to identify papers and scholarly articles that offer solutions toward the safe storage of sensitive documents, including passports, visas, and biometric information via blockchain or decentralized systems like IPFS to ensure data safety, integrity, and privacy.

Throughout this survey, we focused on identifying methodologies and technologies that could be practically applied to our project. We were interested specifically in research papers discussing integration of decentralized storage solutions for large datasets together with biometric data into inherent blockchain capabilities for verification of document integrity. This review enables us to consider the possible application of these systems not only in immigration matters but also in the educational and healthcare sectors, wherein proper handling and verification of documents is a matter of utmost concern.

Our primary objective was to explore how blockchain could securely store sensitive documents and ensure real-time updates on immigrants' status and movements and legal compliance. As our project involves both legal migrants and refugees, we looked for studies that explored the use of QR codes, SIM card-based tracking, and GPS to enable real-time monitoring. Papers that proposed practical applications of these tracking methods in combination with blockchain systems were given priority, as they offered direct insight into how tracking could be integrated into our system. Conversely, we excluded papers that were purely theoretical or lacked clear real-world applications, as

our objective was to focus on solutions that could be realistically implemented.

We also considered how blockchain intrinsic properties, such as decentralization and immutability, could be leveraged to improve the verification process of documents and support automating processes, like sending alerts on visa expiration dates. Literature works that discussed approaches to data protection were considered, especially in terms of their capacity to ensure the authenticity and integrity of sensitive data. This was key in understanding how our project may leverage such approaches to keep migrant personal data safe without fully violating laws and regulations.

Our survey, except for purely conceptual papers, is focused on practical applications and thus provides a pragmatic view of how blockchain, along with its associated technologies, can be utilized to deal with the challenges surrounding management and governance of immigrant data. This structured methodology helped build a good foundation for the understanding of the current landscape of blockchain applications and paved the way for further evolution in this area.

III. LITERATURE REVIEW

Many studies have considered the future applications of blockchain technology in safe storage, authentic documents, and real-time mechanisms. There are various investigations on the adoption of blockchain technology across different industries, such as immigration sectors, education sectors, healthcare sectors, and legal systems with emphasis on better data security, transparency, and efficiency in operations.

Blockchain technology has been of extreme recognition that it can bring security, efficiency, and transparency to data management systems. In numerous sectors, blockchain's decentralized nature coupled with cryptographic algorithms and smart contracts have been considered as suitable solutions for storing sensitive data and automating key processes such as document verification and real-time tracking. The existing literature will provide a good basis in understanding how blockchain technology could be used to address challenges, especially in sectors such as immigration, health care, and education.

Document management and verification have

captivated much of the research studies. The immutable, tamper- proof ledger offered by blockchain has been exploited in several systems designed to store and verify sensitive documents like passports, visas, and educational certificates. [1] presents the idea of a B-Passport, thus introducing a blockchain-based passport system in order to guarantee safety and traceability of international travelling documents. This system uses smart contracts and decentralized consensus mechanisms to offer an open, transparent, and automated process for dealing with passport renewals and document verification. Similarly, a work presented in [29] looks into the application of blockchain for digital identity systems, focusing on vulnerable groups such as refugees. This research highlights the role of blockchain by giving users control over their personal data while keeping the latter safe yet accessible without intermediaries.

Several studies have also highlighted blockchain's role in academic document verification. [3] examines how blockchain can be used to issue and verify educational certificates for university admissions, ensuring that credentials are securely stored and protected from fraud. Such is in line with [15], which discusses the application of blockchain and IPFS in secure document verification. By keeping documents off-chain but referencing them to the record in the blockchain, sensitive data's integrity is maintained. This would eventually pave the way for the safer and scalable management of documents. [27] takes a broader perspective, discussing how blockchain can foster trust between governments and immigrants by providing a verifiable and immutable system for handling sensitive immigration documents.

In terms of decentralized storage, technologies like IPFS have been explored in depth. [5] and [17] discuss combining IPFS with the blockchain to embed large datasets, for example, medical images or immigration documents. These systems enable having off-chain storage for documents while keeping immutability and controlled access by the blockchain ledger. [28] further elaborates on the use of peer-to-peer networks in blockchain-based storage systems, providing an innovative solution for maintaining data integrity and privacy in decentralized environments.

Tracking mechanisms have been a crucial area of study in blockchain research, especially in some applications, for instance, it is needed in immigration management. [9] proposed a QR-code tracking system that would be provided to an individual, with a unique code pegged to his corresponding blockchain record, thereby monitoring movements in real-time. This system is transparent and secure and hence suitable for applications where people have to report their location periodically, such as in refugee management. [10] and [16] extend further from the one above, as they cover SIM card-based tracking systems based on mobile networks for the actual time-based location updates. They are dependent on blockchain so that the location data is immutable and thus allow tracing by the involved authorities.

Another approach to tracking is the use of GPS technology, which is explored in papers like [14] and [19]. These studies demonstrate how blockchain can be used to securely log GPS coordinates, providing a transparent and immutable record of an individual's location. This application is particularly relevant for ensuring compliance with immigration and legal requirements, where real-time updates are essential for monitoring the movements of refugees and migrants. In this context, [26] presents a recent development in blockchain-based geo-fencing. Movement is monitored by low-power sensors. This methodology has been applied in sensitive areas, like places of worship, ensuring physical security and also preserving an untampered log of activities.

Data security remains a central theme in blockchain research, particularly when it comes to protecting sensitive information like documents and biometric data. [2] and [6] discuss further cryptographic hashing methods applied to protect documents that are archived on the blockchain by utilization of RSA digital signatures and SHA-3. The techniques above can detect any document tampering; thus, it is safe enough to ensure integrity on data. Further discussion of other topics regarding cryptographic hashing can also be viewed in [5], which shows that the use of SHA-256 on PDF files preserves their integrity regardless of what networks they are being distributed through.

The integration of biometric data into blockchain systems has been explored in several papers, with a focus on enhancing security and privacy in identity verification. In [8], a scheme is presented whereby fingerprint data is safely held within a blockchain network, providing the possibility of authenticating individuals' identities without reliance on central supervision. Similarly, [20] offers a scheme in the

biometric world for generating a private key from a fingerprint, by which users may use their biometric traits to access secure blockchain- based services. The proposed solution promises strong identity verification, especially for illegal migrants who lack any sort of identification material.

Much discussions are available in literature stating that smart contracts can automate legal and administrative processes. [12] and [23] highlight the role of smart contracts in automating tasks such as visa expiration alerts and document verification. These contracts can be programmed to trigger specific actions based on predefined conditions, reducing the need for manual intervention and ensuring compliance with legal requirements. Following this, [30] considers the prospect of deploying blockchain for providing evidence over identity documents in refugee management scenarios to be tamper-evident but still accessible rapidly in international legal proceedings.

The potential for cross-border data sharing is another important area of blockchain research. [13] and [27] explain how the use of blockchain technology for the safe transfer of sensitive information across borders respects privacy and ensures integrity of data even in untrusted environments. These papers present applications of blockchain to immigration record management so governments and international organizations can share information in an independent, decentralized fashion without reliance on central infrastructure.

Healthcare data management is another key area where blockchain has shown promise [25] suggests the use of smart contracts to validate and manage patient records such that sensitive health data remains secure but accessible only to the right people. This aligns with [4], which explores using blockchain for securely storing large medical datasets, such as diagnostic images, in a decentralized system.

Finally, various studies suggest that blockchain is an important solution to the challenges that affect refugees.

[29] explores how blockchain-based digital identity systems can provide refugees with secure control over their identification documents, ensuring that their rights are protected even in the absence of traditional state- issued documents. Building on this, [30] looks into the Rohingya Archive (R-Archive), utilizing Arweave's blockweave to archive refugee

documentation and land deeds so that these records become tamper-proof and accessible for the whole litigative and cultural preservation processes.

In conclusion, the existing body of literature provides a comprehensive view of how blockchain can be applied to securely manage documents, track movements, and verify identities. The research demonstrates that blockchain's decentralized architecture, coupled with technologies like IPFS, smart contracts, and cryptographic hashing, offers absolute solutions for ensuring data integrity, transparency, and real-time monitoring.

IV. DISCUSSION

In the current immigrant data management systems in India are confronted with significant issues related to security, efficiency, and transparency. The fragmented and centralized nature of such systems makes it rather challenging to effectively store and verify documents in a secure manner, track movement of migrants and refugees, and comply with legal reporting requirements. Indeed, blockchain technology has proved to offer a sustainable solution in addressing such problems because it provides a decentralized approach and immutable and transparent ways of handling sensitive data. The paper attempts at discussing the application of blockchain in managing immigrant data, focusing on document storage and authentication, tracking the location in real time, processing biometric information and supporting law enforcement. For each of the proposed solutions, there is an existing technology, adapted from other contexts-for example, health, education, and disaster management-which is fitted to the needs of immigrant populations.

1. Document Management and Verification Approaches

An overall theme of immigrant data management is the secure storage and verification of important documents such as passports, visas, and biometric data. Traditional methods of document storage are highly centralized, creating vulnerabilities to hacking, unauthorized access, and data loss. Blockchain technology, however presents a decentralized solution where each document receives an allocation of cryptographic hash which resides in the blockchain ledger, guaranteeing its immutability and integrity. This methodology effectively brings out the impossibility of tampering since changes

made to the document after unauthorized entry will change its hash, making it immediately detectable.

A key aspect of this system is its integration with distributed storage technologies like Inter-Planetary File System (IPFS). IPFS enables an important form of off-chain file storage and allows for larger files to be stored, such as biometric data or digitized passports while simultaneously harnessing the security-related properties offered by blockchain technology. For these documents inside the blockchain ledger, only the cryptographic hash of those files is stored, ensuring that actual files are private and decentralized. This hybrid model safes documents, and also it does not have a problem with scalability because the blockchain is not cluttered with huge file size. This system benefits with processing massive amounts of immigrant data which would need to be managed in India as well because there are many migrants who depend heavily on secure systems for documentation purposes.

Furthermore, document verification becomes a streamlined process with blockchain. For the legally documented migrants with a passport and visa, blockchain would thus act as one central source of verifiable information allowing the immigration authorities, consulates, and border control agencies to verify these various documents in real time. The establishing of an immutable group record eliminates the need for intermediaries at the same time giving any interested party the same verified data. This significantly reduces the risk of fraud, document tampering, or delays in the verification process.

Blockchain technology will aid in verifying documentation of migrants crossing borders, an easier collaboration between various countries and agencies. It is more important for legal migrants, who have to seek verification through several government bodies or even consulates at different instances of travels or relocations. Transparency and immutability embedded in blockchain will enhance the degree of trust between governments and migrants, with more efficient migration processes and fewer bureaucratic inefficiencies.

2. Location Tracking Solutions

Effective immigrant data management requires not only the secure storage of documents but also real-time location tracking to ensure compliance with legal regulations, enhance security, and provide better oversight of both legal migrants and refugees.

Different blockchain-based tracking mechanisms have been proposed, each offering varying levels of accuracy, scalability, and feasibility depending on the specific context and needs of the immigrant population.

QR Code-Based Tracking: The least ambiguous techniques of tracking the movements of registered migrants are the QR code monitoring systems. Under this regime, every migrant is issued with a unique QR code marking his entry on the blockchain. At certain points of junctures such as airports or border crossings, the QR code is read, and the migrant's location is permanently recorded on the blockchain. This system strongly fulfils the role of monitoring migrants who frequently cross documented sites, and it would enable the authorities to create a profile of movement. However, the strength of the system depends very much on physical checks, which does, in a way, weaken its advantages when one crosses the same undocumented or isolated areas often.

SIM Card-Based Tracking: SIM Card-Based Tracking On the other hand, the tracking using the SIM card has the advantage of numerous mobile phones available to give a location report about a person in real-time. It is more flexible than tracking with QR codes since it does not rely on physical stations. The moment the user's mobile device registers to a cellular network, its position is entered into the blockchain which allows continuous tracking. Although this system is scalable in tracking the movement of people seeking refuge, who may not necessarily have formal documents but have phones, in general it has an added advantage of being feasible in the event of implementation in areas that may not have the comprehensive infrastructures available. This would make it an ideal choice for tracking refugee movements in remote or conflict-affected regions. It depends on the continued possession by individuals of mobile devices and access to mobile network connectivity, though this may be a limitation in particular geographic area

GPS-Based Tracking: Using GPS technology, one can accurately track people in real-time. Devices are usually made with built-in functionality of GPS-enabled ones; thus, the particular location of a migrant or refugee can be recorded in the blockchain, and hence, migrants are constantly kept under surveillance without being monitored through some human network. This system works best with those classified as high-risk, or in situations where there is

a strict movement restriction. However, the use of GPS tracking requires that the persons carrying them have GPS-enabled devices at all times, which is unrealistic for most refugees and migrants who lack access to these technologies. Moreover, GPS systems require more investment in resources compared to QR code or SIM card-based systems as they require significant hardware and infrastructure to support constant tracking.

Table 1: TRACKING METHODS FOR MIGRANTS AND REFUGEES

Tracking Method	Accuracy	Feasibility for Legal Migrants	Feasibility for Refugees	Blockchain Integration
QR Code-Based	Moderate	High (Documented locations)	Low (No checkpoints)	High
SIM Card-Based	Moderate	High (Mobile-enabled)	High (Mobile-enabled)	High
GPS-Based	High	High (Real-time tracking)	Moderate (Device-dependent)	High

The above table (TABLE 1) provides a comparison of the three tracking methods, focusing on their accuracy, feasibility for different migrant groups, scalability, and integration with blockchain.

In each of these models, there are benefits and some infrastructural and scalability limitations. A hybrid model can amend these challenges. For instance, the check-in system may ask migrants or refugees to prove their identity using biometrics or QR codes for every few days. Periodic updates are balanced by real-time tracking as it conducts constant location information without requiring constant monitoring.

This is also very flexible but may not be the best option every time. Each of these - QR codes, SIM cards, and GPS - has its pros and cons. QR codes are effective for tracking purposes, particularly in highly bounded areas like an airport or office, but SIM card tracking is definitely better since it offers full coverage except it has problems with privacy. GPS tracking is very accurate but best for situations involving high risk and constant monitoring.

3. Biometric Data Management

Biometric data management automatically becomes a must for refugees who lack most of their traditional documents but can be identified through their fingerprints, face, or iris features. In this regard, the use of blockchain technology will ensure a secure, immutable way for the storage and verification of biometric data due to its inability to facilitate possible manipulation or unauthorized entry.

Biometric information could be kept off-chain using decentralized storage solutions such as IPFS in a blockchain structure. However, the associated cryptographic hash will remain on the blockchain. This way, in essence, actual privacy of biometric information is maintained, and at the same time, integrity could be validated. When someone's biometrics is used for access authentication, the system validates if the recorded hash on the blockchain matches.

Biometric verification is one of the strong tools used in managing refugee identity, mostly in cases where they lack any conventional means of identification. Biometric data become a safe key, enabling them to use such basic services as health care and housing and education even when they lack physical means of identification. This reduces intimidation from fraudulent activities or identity theft.

In addition, biometric verification with blockchain technology will also facilitate smoothing out of the refugee application and asylum processes. Because refugee biometric information recorded on the blockchain securely cannot be changed or forged, it can offer a reliable, tamper-proof record of identity. Hence, asylum claim processing can be done much faster as biometric identity checks will no longer need the verification of physical documents.

4. Cryptographic Algorithms and Hashing Techniques

To secure sensitive immigrant data on the blockchain, cryptographic algorithms and hashing techniques play a key role in ensuring data confidentiality, authenticity, and integrity. These methods are crucial for handling immigration-related information like passports, visas, and biometric details. After reviewing various approaches, the most suitable algorithms for an immigration management system can be identified.

SHA-256 and SHA-3 Hash Functions

SHA-256 and SHA-3 are widely used cryptographic hash functions designed to ensure data integrity. SHA- 256 is part of the SHA-2 family and is known for its robustness against collision attacks, making it an ideal choice for many blockchain applications where even minor changes to the data result in a completely different hash. SHA-3 is a newer addition, offering enhanced resistance to specific cryptographic vulnerabilities, such as length-extension attacks.

In the context of immigration management, both SHA-256 and SHA-3 are suitable for hashing sensitive data such as biometric information, visas, and passports. These algorithms ensure that even minor alterations to the document data produce a drastically different hash, making tampering easily detectable. SHA-256 is widely supported and may be preferable in systems that use established blockchain platforms like Ethereum, while SHA-3 could be adopted where higher security is needed.

RSA Digital Signatures

The RSA algorithm is a public-key cryptography system that is widely used for digital signatures, which are critical for authenticating the origin and integrity of documents. RSA signatures allow immigration authorities to digitally sign documents, such as legal agreements or passports, ensuring that only authorized parties can validate and alter these records.

In an immigration management context, RSA digital signatures can be employed to establish trust across different stakeholders, such as government entities and international organizations. By signing documents before storing them on the blockchain, these signatures guarantee that no unauthorized alterations are made, ensuring that document verification is secure, transparent, and easily auditable.

Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA is a more efficient digital signature algorithm compared to RSA, offering the same security level with smaller key sizes, making it ideal for environments with resource constraints, such as mobile applications. ECDSA is commonly used in blockchain systems like Ethereum for signing transactions and verifying identities, given its reduced computational load compared to RSA.

In immigration management systems that use mobile platforms for real-time updates and verification, ECDSA is particularly well-suited. Its ability to minimize computational demands while maintaining secure transactions makes it ideal for mobile-based solutions like SIM card tracking, where the device's processing power is limited.

Chameleon Hashing

Chameleon hashing allows controlled modifications to data while ensuring that the system remains secure. This technique is valuable in scenarios where documents, such as visas, need updates without invalidating previous records. By allowing specific authorized changes while maintaining the immutability of records, chameleon hashing provides flexibility in document management.

In immigration management, chameleon hashing can be used for scenarios where legal or immigration status changes are common, such as visa renewals. While it offers the flexibility needed to update records securely, this technique must be carefully managed to avoid creating potential vulnerabilities in the system.

Fingerprint-Based Cryptographic Keys

Biometric data such as fingerprints can be used to generate cryptographic keys. This method allows individuals without formal identification to securely access and manage their personal data on the blockchain. Fingerprint- based keys can be employed as a private key, providing a highly secure and tamper-proof identity verification mechanism.

In systems designed for refugee management, fingerprint-based cryptographic keys offer a way to ensure that those without traditional identification documents can still securely authenticate their identity. Using biometric data for verification strengthens security and simplifies the process of accessing and updating personal records without the need for conventional identification documents.\

The comparison below (TABLE 2) highlights the suitability of each cryptographic algorithm for different use cases in immigration management. SHA-256 and RSA are ideal for hashing and document verification due to their proven security and widespread adoption. ECDSA offers efficiency for mobile-based solutions, while fingerprint-based cryptographic keys are well-suited for refugee management systems that require secure and accessible biometric verification. Chameleon

hashing provides controlled flexibility, allowing for

necessary updates without sacrificing security.

TABLE 2 CRYPTOGRAPHIC ALGORITHMS FORIMM IGRATION SYSTEMS

Algorithm	Use Case	Efficiency	Feasibility in Immigration Systems
SHA-256	Hashing documents (passports, visas)	High	High (widely supported)
SHA-3	Hashing documents (more secure)	Moderate	Moderate (newer, more secure)
RSA Digital Signatures	Document authentication	Moderate	High (widely used)
ECDSA	Mobile-based verification	Very High	High (efficient for mobile platforms)
Chameleon Hashing	Controlled updates to records	Moderate	Moderate (requires careful management)
Fingerprint-Based Keys	Biometric verification for refugees	High (Biometric)	High (secure for identity management)

5. Immigration laws and regulations compliance is part of essential managing of immigrant data. With the use of blockchain technology, most especially with smart contracts, there can be very efficient automation of many legal compliance activities in transparent manners. For example, smart contracts will enable the automatic execution of specified pre-programmed actions whenever certain conditions are met, thus almost totally minimizing reliance on human intervention. For instance, smart contracts may automatically send distinct notifications of the expiring immigrant visa or failure to check-in in case a refugee. The contracts shall be kept on the blockchain ledger where every single activity performed becomes irrevocable and all the legal compliance met is clear. One can track easily still it puts responsibility upon people as everyone has the same verified information. Smart contracts can encourage synergies between institutions that cross borders among governments and immigration officers. For instance, when a migrant or refugee crosses an international border, the blockchain ledger can promptly inform the authorities in the two countries that the individual's movement is registered in both countries while at the same time avoiding migrants and refugees contravening immigration laws in the two countries. This mitigates the risk of oversight and enables real-time monitoring of migrants and refugees as they travel across borders.

6. Challenges and Future Directions Although the blockchain technology encompasses various benefits, several issues need to be addressed before it can be applied widely in managing the data of immigrants. The prime one among them is the privacy of the data, particularly of the biometric data.

Blockchain provides a sound and unalterable structure; however, it has to adhere to the regulations related to privacy like GDPR. Encryption and zero-knowledge proofs, techniques 9 that concern the preservation of privacy, will embrace data security in terms of integrity and blockchain transparency. Integrating diverse tracking technologies with blockchain creates unique logistical complexities. While each of the tracking methodologies considered-the QR code, SIM card, and GPS tracking-has its drawbacks, future systems are unlikely to work across large areas without a hybrid strategy that would integrate multiple techniques in order to be at once scalable and accurate. This approach might involve supplementing static check-ins with dynamic, real-time tracking and making adjustments according to what is needed by the various cohorts of migrant or refugee flows. Lastly, scalability is the final challenge facing blockchain-based systems. The more people that are being followed, the more resource-intensive the consensus mechanisms of the blockchain will be especially at larger scales. Such an application may adopt another consensus mechanism by adopting PoS thereby lowering the environmental impact as well as operational expenses associated with running a large scale blockchain system.

V.CONCLUSION

This survey paper has explored the revolutionary capabilities of blockchain technology in addressing pressing concerns regarding managing immigrant data. Through a comprehensive review of the literature, multiple applications of blockchain for document storage, verification processes, and real-time tracking have been identified in the paper as it

highlights its capacity towards enhancing data integrity and transparency. Advanced ideas of managing confidential information are delivered through solutions like decentralized storage systems, for example, Inter-Planetary File System (IPFS) and cryptographic hashing methods, among others. Such solutions are crucial for vulnerable segments, for example, refugees, who are usually not found with proper identification. The added value of handling biometric data along with geolocation tracking abilities provides an advanced framework that ensures compliance with legal requirements while at the same time enhancing the general security of immigrant documents.

As the landscape of immigration continues to evolve, the adoption of blockchain has much promise to enhance the effectiveness and reliability of any systems working with immigrant data. Such advancements only fortify the verification process of authentic immigrants while, at the same time, giving refugees an opportunity to use alternative forms of identity verification in cases where formal documents are inaccessible. However, a challenge such as data confidentiality exists, infrastructural demands and the desire for compliance with the need of each cure, hence advanced strategy tailored to the respective need of different migratory communities must be devised.

Future research should prioritize developing pilot projects and real-world applications that involve these blockchain technologies in the system, thus providing crucial input for continuous improvement. The advantages of blockchain technology could then be leveraged by the stakeholders in building a safer, efficient system to equitably manage immigrant data. This, by its own merit, is likely going to result in further development of an immigration framework better suited to this diverse and ever-changing population, in which trust and accountability among stakeholders will be fostered. As we move forward, the continuous exploration and adaptation of blockchain solutions will prove pivotal in ensuring that those experiences by immigrants are treated with the dignity and respect that such experiences deserve.

VI. REFERENCES

[1] M. T. A. Tonoy, N. Munjal, R. A. Sinha, A. Paul and H. S. Lamkuche, "Unlocking Borderless Identity: B-Passport and the Blockchain Revolution," 2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE), Bangalore, India, 2024, pp. 109-116, doi: 10.1109/ICWITE59797.2024.10503329.

[2] B. Parıldar, D. Sayin, F. Z. Türkzeybek, O. Küçüköz and Y. M. Erten, "Help Chain: A Blockchain based Disaster Management System," 2023 4th International Informatics and Software Engineering Conference (IISEC), Ankara, Turkiye, 2023, pp. 1-5, doi: 10.1109/IISEC59749.2023.10391032.

[3] A. Jain, D. Desai and R. Sangole, "A Case Study on Use of Blockchain Technology as a Dominant Feature to Issue and Verify Documents Required for Admission to UG/PG Technical Programs in Maharashtra (India)," 2022 IEEE Pune Section International Conference (PuneCon), Pune, India, 2022, pp. 1-5, doi: 10.1109/PuneCon55413.2022.10014917.

[4] S. D. Ashwini, A. P. Patil and S. K. Shetty, "Moving Towards Blockchain-Based Solution for Ensuring Secure Storage of Medical Images," 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 2021, pp. 1-5, doi: 10.1109/INDICON52576.2021.9691516.

[5] A. Sharif, D. S. Ginting and A. D. Dias, "Securing the Integrity of PDF Files using RSA Digital Signature and SHA-3 Hash Function," 2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA), Medan, Indonesia, 2021, pp. 154-159, doi: 10.1109/DATABIA53375.2021.9650121.

[6] Acquah, Moses Arhinful, Na Chen, Jeng-Shyang Pan, Hong-Mei Yang, and Bin Yan, "Securing Fingerprint Template Using Blockchain and Distributed Storage System," Symmetry 12, no. 6: 951, 2020, https://doi.org/10.3390/sym12060951.

[7] Susanto H, Kemaluddin N, "Innovative Blockchain-Based Tracking Systems, A Technology Acceptance for Cross-Border Runners during and Post-Pandemic," Sustainability, 15(8):6519, 2023, https://doi.org/10.3390/su15086519.

[8] S. Sankhe, P. Malhotra, A. A. Siddiqui, A. R. Shaikh, R. Mulla and J. Khan, "A Blockchain based solution to manage vehicle documents using QR-Code," 2023 6th International

Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2023, pp. 7-12, doi: 10.1109/ICAST59062.2023.10454935.

[9] F. M. Enescu, C.-G. Nicolaescu, V. M. Ionescu, "Blockchain in Personal Document Archiving Services," 2024.

[10] S. Tandon, S. Singhal, S. Khan and M. P. Kumar, "GPS System based Tracking model for Mobile phone," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 814-821, doi: 10.1109/ICCES51350.2021.9488931.

[11] T. S. R. Rajeswari, S. K. Shareef, S. Khan, N. Venkatesh, A. Ali and V. S. Monika Devi, "Generating and Validating Certificates Using Blockchain," 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatre, India, 2021, pp. 1048-1052, doi: 10.1109/ICCES51350.2021.9489105.

[12] M. Shahriar Rahman, A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto and G. Wang, "Accountable Cross-Border Data Sharing Using Blockchain Under Relaxed Trust Assumption," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1476-1486, Nov. 2020, doi: 10.1109/TEM.2019.2960829.

[13] G. S. Praba Devi and J. C. Miraclin Joyce Pamila, "Accident Alert System Application Using a Privacy- Preserving Blockchain-Based Incentive Mechanism," 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 2019, pp. 390-394, doi: 10.1109/ICACCS.2019.8728507.

[14] Patel, D., Balakarthikeyan, Mistry, V., "Border Control and Immigration on Blockchain," in Blockchain – ICBC 2018, Lecture Notes in Computer Science, vol 10974, Springer, Cham, 2018, DOI: https://doi.org/10.1007/978-3-319-94478-4_12.

[15] K. Goswami, D. Vaithiyanathan, P. Verma and B. Kaur, "Document verification using Blockchain," 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India, 2024, pp. 1-7, doi: 10.1109/AMATHE61652.2024.10582173.

[16] Y. Qi, Y. Fu, T. Wang and H. Lv, "Pf,"tom: A Blockchain based on Fingerprint," 2020 Chinese Automation Congress (CAC), Shanghai, China, 2020, pp. 5338-5344, doi: 10.1109/CAC51589.2020.9326945.

[17] S. Panchamia and D. K. Byrappa, "Passport, VISA and Immigration Management Using Blockchain," 2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM), Bangalore, India, 2017, pp. 8-17, doi: 10.1109/ADCOM.2017.00009.

[18] Ranjith Kumar, M.V., Bhalaji, N., "Blockchain Based Chameleon Hashing Technique for Privacy Preservation in E-Governance System," Wireless Pers Commun 117, 987–1006, 2021, DOI: https://doi.org/10.1007/s11277-020-07907-w.

[19] Mohammad Reza Nosouhi, Shui Yu, Wanlei Zhou, Marthie Grobler, Habiba Keshtiar, "Blockchain for secure location verification," Journal of Parallel and Distributed Computing, Volume 136, 2020, Pages 40-51, ISSN 0743-7315, DOI: https://doi.org/10.1016/j.jpdc.2019.10.007.

[20] Tiwari, Meher & Anil Kumar, Kakelli, "Decentralization System Using Smart Blockchain with Secure Hash," SN Computer Science, vol. 4, 2023, DOI: 10.1007/s42979-023-02026-2.

[21] Priscilla, C. & Devasena, T., "Aadhaar Identity System using Blockchain Technology," International Journal of Computer Applications, vol. 174, pp. 27-32, 2021, DOI: 10.5120/ijca2021921188.

[22] Nema, Bashar & Jaafar, Ali. (2020). Geo Location of Mobile Device. 10.5772/intechopen.92154.

[23] Y. Sun, R. Zhang, X. Wang, K. Gao and L. Liu, "A Decentralizing Attribute-Based Signature for Healthcare Blockchain," 2018 27th International Conference on Computer Communication and Networks (ICCCN), Hangzhou, China, 2018, pp. 1-9, doi: 10.1109/ICCCN.2018.8487349.

[24] Páez, Rafael, Manuel Pérez, Gustavo Ramírez, Juan Montes, and Lucas Bouvarel, "An Architecture for Biometric Electronic Identification Document System Based on Blockchain," Future Internet, vol. 12, no. 1, 2020, DOI: https://doi.org/10.3390/fi12010010.

[25] M. Sharma, S. Singh, A. Deep, D. Garg and A. Kumar, "Blockchain's Frontier: Enhancing Data Security and Collaboration for Healthcare," 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2024, pp. 1-6, doi: 10.1109/ICRITO61523.2024.10522385.

[26] A. Vishnoi, T. Choudhury, J. C. Patni, A. Sar and H. F. Mahdi, "A Proposed Framework for Smart Geo-Fencing For Religious Places," 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), Istanbul, Turkiye, 2023, pp. 1-6, doi: 10.1109/ISAS60782.2023.10391370.

[27] Chun-Wei Chiang, Eber Betanzos, and Saiph Savage, "Exploring Blockchain for Trustful Collaborations between Immigrants and Governments," in Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18), Association for Computing Machinery, New York, NY, USA, Paper LBW531, 1–6, https://doi.org/10.1145/3170427.3188660.

[28] M. P. Jariwala, M. S. Obaidat, M. Wazid, A. K. Mishra and D. P. Singh, "Designing Blockchain-Based Decentralized Scheme for Secure File Storage System," 2024 International Conference on Computer, Information and Telecommunication Systems (CITS), Girona, Spain, 2024, pp. 1-7, doi: 10.1109/CITS61189.2024.10607985.

[29] R. Sharma and A. Kaur, "Digital Identity: An Attempt to Sustain the Refugees," 2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech), Banur, India, 2023,pp. 87-94, doi: 10.1109/ICACCTech61146.2023.00023.

[30] Sheikh, S., Gilliland, A.J., Kothe, P. and Lowry, J., "Distributed records in the Rohingya refugee diaspora: Arweave and the R-Archive", Journal of Documentation, Vol. 79 No. 4, pp. 813-829, 2023, https://doi.org/10.1108/JD-08-2022-0174.