**Computer Science, Engineering and Technology**

**Vol: 3(2), June 2025**

**REST Publisher; ISSN: 2583-9179**

**Website: https://restpublisher.com/journals/cset/**

**DOI: https://doi.org/10.46632/cset/3/2/18**


# Smart Contract-Based Authentication Mechanism for Issuing Privilege Passes Using a Permissioned Blockchain for Indian Inter-State Travel

***Ramya V, Shivani R**

*Shri Krishnaswamy College for Women, Chennai, Tamil Nadu, India.*

*Corresponding author Email: ranjanlnmi4u@gmail.com

***Abstract:*** *India's dynamic socio-economic landscape and vast geography necessitate efficient and equitable public service delivery mechanisms, especially in areas like inter-state travel for citizens eligible for complimentary or concessional passes. Traditional systems used for issuing such privilege passes suffer from inefficiencies, fraud vulnerabilities, and inconsistent verification standards across states. This paper proposes a novel smart contract- based authentication mechanism built on a permissioned blockchain architecture to automate and secure the issuance of privilege passes for inter-state travel within India. By integrating Aadhaar-based digital identity verification and leveraging the immutability and transparency of blockchain, this approach enables real-time, verifiable, and tamper-proof pass issuance, while minimizing administrative overhead. The proposed system operates through a consortium-led blockchain network composed of central and state transport authorities and public sector technology partners. Smart contracts deployed on this network enforce eligibility rules automatically by interacting with off-chain data sources—referred to as oracles—that provide income, age, or employment status of applicants. Once eligibility is validated, a digital privilege pass is issued, cryptographically linked to the citizen's identity and stored on-chain. These digital passes can be presented through QR codes and verified instantly by transport officials using mobile applications. Key features of this system include tamper-resistant records, zero-knowledge proof support for privacy preservation, and revocation capabilities for dynamic eligibility management. Aadhaar e-KYC ensures that only legitimate individuals are granted benefits, while the use of hashed identifiers on-chain preserves personal privacy. Furthermore, the permissioned nature of the blockchain network ensures compliance with national data protection laws while allowing rapid consensus and controlled access. By introducing automation, auditability, and interoperability into the travel concession ecosystem, this framework significantly reduces the risk of misuse, streamlines citizen experience, and enhances governance efficiency. The solution supports pan-India applicability and is adaptable to the varied policy rules across different states. Its modular design also enables future expansion to other welfare services, such as subsidized healthcare or education benefits. This paper outlines the technical architecture, smart contract workflow, governance model, and potential challenges in implementing such a system. The integration of decentralized technologies in public service infrastructure marks a progressive step toward a transparent, efficient, and citizen-centric Digital India.*

***Keywords:*** *Blockchain, Smart Contracts, Aadhaar, Inter-State Travel, Identity Verification, Permissioned Blockchain, Digital Governance, Privilege Passes.*

## 1. INTRODUCTION

India's federal structure, vast geography, and socio-economic diversity present unique challenges when it comes to delivering public services uniformly across states. One such area of concern is the management and distribution of inter-state travel privileges for specific categories of citizens—such as senior citizens, students, persons with disabilities, government employees, and frontline healthcare workers. These privileges may include toll fee waivers,

subsidized transport passes, or special access to government facilities when traveling between Indian states. However, the current systems employed for issuing and verifying these privilege passes are largely manual, fragmented, and lack interoperability, making them inefficient and vulnerable to misuse. In the traditional model, state governments maintain their own databases and procedures to issue these passes, often involving paperwork, in-person verification, and limited cross-state recognition. A senior citizen traveling from Tamil Nadu to Maharashtra, for example, may not be able to avail of toll exemptions if their pass is not recognized outside their home state. Similarly, transport concessions issued by one state's public transportation department may not be honored by another. Such state-centric silos hinder the vision of a seamless and citizen-friendly public service framework and create bureaucratic overhead for both citizens and authorities. In this context, blockchain technology—particularly permissioned blockchains—offers a promising solution. Blockchain's fundamental strengths lie in immutability, decentralization, transparency, and trustless execution, all of which are essential attributes when handling citizen privileges across multiple jurisdictions. Permissioned blockchains, unlike public blockchains such as Ethereum or Bitcoin, allow only authorized participants (e.g., government nodes, verified stakeholders) to access and interact with the ledger. This design suits government use cases where data sensitivity and access control are paramount. Furthermore, the incorporation of smart contracts—self-executing code that runs on the blockchain—enables automated decision-making based on pre-defined eligibility rules, removing the need for manual processing or third-party validation. The proposed system automates the end-to-end process: from identity verification using Aadhar to eligibility checks and digital issuance of a privilege pass in the form of a non-fungible token (NFT) or a verifiable credential. The smart contract enforces strict rules—such as checking whether the citizen falls within the allowed quota, validating travel intent, or ensuring the pass hasn't been previously issued—before granting access to benefits. The citizen experience is also enhanced significantly. By using a simple mobile app or digital wallet interface, the individual can authenticate their identity through Aadhar OTP or biometric verification, after which the system automatically verifies eligibility and issues a digital pass. This pass can then be stored on the device, used offline via QR code, or presented at toll booths and government checkpoints for real-time validation. At the backend, the blockchain ensures that each transaction—from request to issuance to usage—is recorded immutably, ensuring auditability and preventing duplicate or fraudulent claims. In addition to improving user experience and reducing administrative burden, the proposed model also supports inter-state interoperability. By adopting a federated governance model, where each state functions as a node in the permissioned blockchain network, states can share information securely and recognize passes issued by other states. This paves the way for a unified, national-level privilege management system that preserves local autonomy while ensuring standardization and efficiency. From a policy standpoint, this system aligns with the Indian government's ongoing push for Digital India, e-Governance, and citizen-centric service delivery. It offers transparency in public expenditure, enables better monitoring and analytics of privilege usage, and lays the foundation for a tamper-proof, scalable public service infrastructure. Moreover, the use of cryptographic hashing and zero-knowledge proof techniques ensures that sensitive citizen data—such as Aadhar numbers—is never stored in plaintext, maintaining full compliance with India's Digital Personal Data Protection Act (DPDPA), 2023. Despite its promise, implementing such a system does come with challenges. These include technical complexities in integrating with legacy systems, ensuring adequate digital infrastructure at the point of use (e.g., toll booths, check-in desks), and managing change across bureaucratic and institutional layers. However, pilot implementations in select states or high-traffic inter-state corridors can help demonstrate feasibility, gather user feedback, and create a roadmap for nationwide deployment. In conclusion, this paper explores how a smart contract-based authentication mechanism on a permissioned blockchain can revolutionize the way Indian states issue and validate inter-state privilege passes. By combining technological innovation with public policy goals, the proposed framework represents a major step forward in delivering transparent, efficient, and citizen-friendly travel entitlements.

## 2. BACKGROUND AND MOTIVATION

A. **Challenges in the Current System:** The present system for issuing inter-state privilege passes in India faces multiple operational inefficiencies. Primarily, it is hindered by manual document verification, which demands significant administrative effort and introduces a high probability of human error. The absence of an automated identity verification mechanism has led to instances of fraudulent identity claims, thereby compromising the credibility of the process. Moreover, the lack of a unified national framework results in fragmented state-level systems, where each state may follow its own protocol for issuing and verifying travel permissions. This not only leads to inconsistency but also hinders interoperability among states. The processes remain opaque, offering minimal visibility to applicants and minimal auditability for authorities, resulting in delayed services and reduced public trust.

B. **Blockchain for Public Services:** To address these systemic inefficiencies, blockchain technology presents a viable solution for enhancing public service delivery. A blockchain-based system provides decentralized data verification, allowing multiple authorized parties to access and verify records without relying on a central authority. The inherent property of immutability ensures that once data is recorded, it cannot be tampered with, significantly reducing the risk of fraud. Furthermore, the use of smart contracts introduces automation into the verification process. These self-executing programs enforce predefined eligibility conditions and execute transactions automatically, without the need for manual intervention. This not only enhances operational efficiency but also ensures transparent and consistent governance. The integration of blockchain with privilege pass systems offers the potential to establish a trustworthy, interoperable, and transparent digital framework, thereby modernizing the governance process in a scalable and secure manner.

**TABLE 1.**

| Conventional Privilege Pass Issuance System | | Blockchain-based Privilege Pass Issuance System |
|---|---|---|
| • Manual document verification<br>• Fraudulent identity claims<br>• Fragmented state systems<br>• Opaque processes | » | • Decentralized verification<br>• Immutable records<br>• Transparent governance<br>• Smart contracts for eligibility |

## 3. SYSTEM ARCHITECTURE

**A. Components:** The proposed system leverages a permissioned blockchain network, such as Hyperledger Fabric or Quorum, to ensure secure and authorized participation by recognized stakeholders. Unlike public blockchains, permissioned networks provide controlled access, enhanced privacy, and high throughput, making them ideal for government-led service delivery systems. At the core of the architecture are smart contracts, which define and enforce the rules for privilege pass issuance, verification, and revocation. These contracts execute automatically based on predefined logic, thereby minimizing manual intervention and ensuring policy compliance. Aadhaar, India's unique biometric identity system, serves as the primary authentication mechanism, linking each citizen's digital identity with their application. This ensures that only eligible individuals can apply for and receive privilege passes, thereby eliminating impersonation and fraud. The system includes two types of front-end interfaces: Citizen and Admin Portals. Citizens can apply for privilege passes, track application status, and view usage history through a secure and user-friendly interface. The Admin Portal allows authorities to monitor applications, verify eligibility, and audit transactions in real-time**.**

**B. Stakeholders:** The platform brings together multiple stakeholders. Citizens are the primary users who request inter- state travel passes. State and Central Transport Authorities are responsible for verifying eligibility and issuing permissions. A Consortium Governance Body, comprising representatives from key state and central agencies, oversees the operation and ensures compliance with legal and administrative frameworks. Together, this architecture promotes security, transparency, and scalability, offering a robust digital infrastructure for inter-state privilege pass management across India.

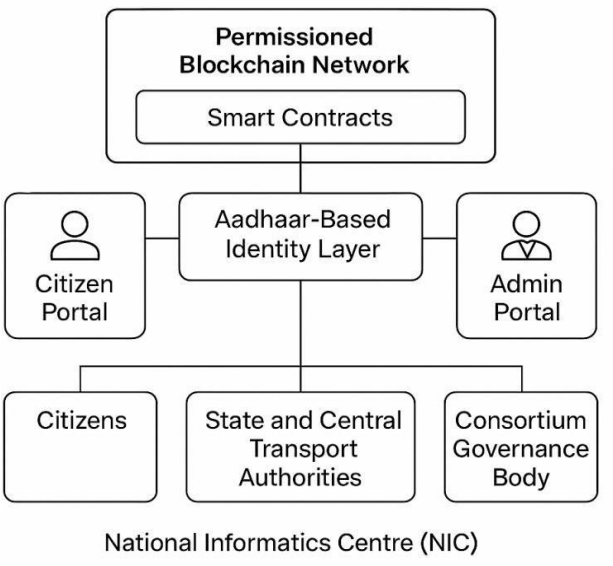


**FIGURE 1.**

## 4. AUTHENTICATION WORKFLOW

**Identity Verification via Aadhaar:** The authentication workflow begins with robust identity verification using India's Aadhaar infrastructure. Citizens authenticate themselves through either biometric (fingerprint or iris) or OTP-based authentication, leveraging the Unique Identification Authority of India (UIDAI)'s e- KYC APIs. This ensures that only legitimate individuals can initiate the privilege pass application process. Upon successful authentication, the system performs a one-way cryptographic hash of the Aadhaar UID and maps it to a unique blockchain wallet address. This approach ensures that no personally identifiable information (PII) is stored directly on-chain, thereby safeguarding citizen privacy while maintaining a secure link to their identity in a verifiable format.

**Smart Contract Logic:** Smart contracts, deployed on the permissioned blockchain, automate the issuance, verification, and revocation of privilege passes. The three main functions are: verifyEligibility(): This function evaluates whether an applicant qualifies for a privilege pass based on age, income status, and employment category. Data is fetched using off-chain oracles, which securely retrieve records from trusted government databases or APIs. The logic is deterministic and enforces pre-defined eligibility rules without human bias or delay. issuePass(): Upon passing the eligibility check, a digital privilege pass is generated and immutably recorded on the blockchain. The pass is cryptographically linked to the citizen's wallet address, ensuring secure access and traceability. revokePass(): This function allows designated authorities to revoke a privilege pass under predefined circumstances, such as misuse, expiration, or regulatory violations. Every revocation event is logged on-chain, providing a tamper-proof audit trail.

**Privacy Considerations:** To protect citizen data while preserving transparency, the system integrates advanced privacy-preserving techniques: Zero-Knowledge Proofs (ZKPs) are employed to allow eligibility validation without revealing sensitive user attributes. This ensures trust without compromising confidentiality. Personal information is stored off-chain in secure, encrypted storage systems that comply with data protection guidelines. Only cryptographic hashes and minimal metadata are recorded on-chain, referencing the off-chain data without exposing actual personal details. This architecture ensures that the authentication and verification processes are secure, transparent, and privacy-conscious, aligning with best practices in e-governance and digital identity management.

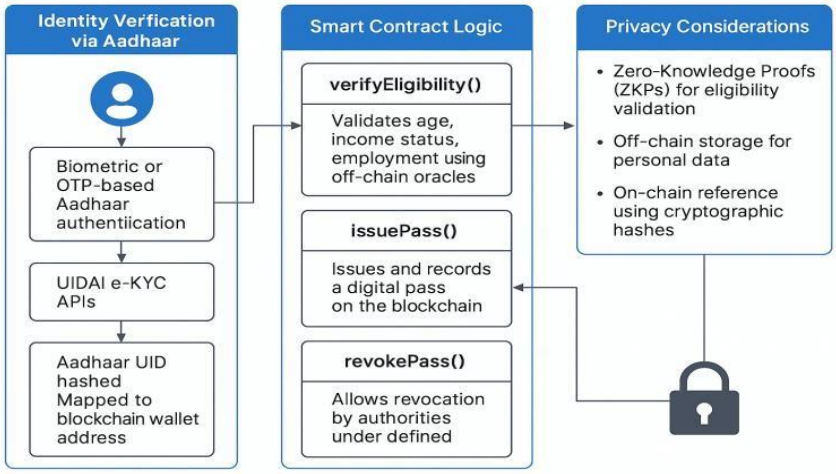


**FIGURE 2.**

## 5. TECHNICAL FRAMEWORK

The proposed authentication mechanism for issuing complimentary privilege passes relies on a well- structured technical framework that integrates several advanced technologies to ensure secure, scalable, and efficient operations. Below is an overview of the technologies used at each layer of the system.

**Blockchain:** Hyperledger Fabric / Quorum: At the core of the system lies the blockchain layer, which is built on Hyperledger Fabric or Quorum, two popular permissioned blockchain platforms. Hyperledger Fabric offers a modular architecture, enabling flexibility in the choice of consensus mechanisms and privacy features. Its permissioned nature ensures that only authorized participants can interact with the network. On the other hand, Quorum is a permissioned version of Ethereum, providing support for private transactions and high throughput, making it suitable for use in governmental applications like issuing inter-state privilege passes.

**Smart Contracts:** Go/Chain code (Fabric), Solidity (Quorum): For Hyperledger Fabric, Go is typically used to write Chaincode, the smart contract logic. Chain code allows for the definition of rules for issuing, updating, and validating the privilege passes, ensuring seamless interaction within the blockchain. This Ethereum compatible language ensures that the system benefits from existing development standards and tools available in the Ethereum ecosystem.

**Identity:** Aadhaar e-KYC APIs: The identity verification layer leverages Aadhaar e-KYC APIs, which are part of India's unique identification system. Aadhaar, the world's largest biometric database, is used for verifying the identity of Indian citizens. The integration of e-KYC allows for real-time, secure identity verification, ensuring that only authorized citizens can access the privilege pass system. This integration also streamlines the process of issuing passes and ensures that the system remains compliant with India's privacy and data protection regulations.

**Frontend:** React / Flutter The frontend layer, which interacts with the blockchain backend, uses React for web applications and Flutter for mobile applications. React is chosen for its component-based architecture, which makes it easy to develop a dynamic and responsive user interface for web platforms. Flutter, on the other hand, allows for building cross-platform mobile applications with a single codebase, ensuring that users can access the privilege pass system on both Android and iOS devices.

**Oracles:** Chainlink / Custom REST APIs Chainlink serves as a decentralized oracle network, ensuring that the system can securely access off chain data. In cases where custom data is required, Custom REST APIs can be used to integrate data from trusted external sources, such as state transport departments or transit authorities.

**Storage:** IPFS / NIC Databases Data storage is handled by IPFS (InterPlanetary File System) for storing large files such as identity documents and privilege passes securely in a decentralized manner. NIC Databases, managed by the National Informatics Centre, are also used for storing non-sensitive information in a centralized manner for efficient

querying and processing. This layered approach ensures that the system is secure, scalable, and capable of handling large volumes of transactions while maintaining privacy and compliance with regulatory standards.

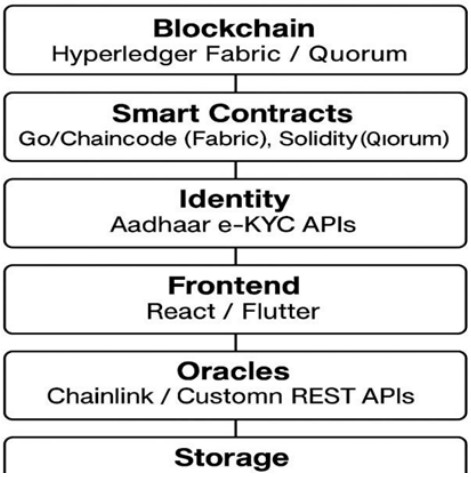


**FIGURE 2.** Flow chart

## 6. GOVERNANCE AND INTEROPERABILITY

**Consortium Model Governance**: In the context of an inter-state privilege pass system built on a permissioned blockchain, governance is a crucial factor in ensuring the efficiency, security, and adaptability of the system. The Consortium Model provides an optimal structure for managing the governance of the blockchain network, particularly when multiple stakeholders are involved, such as central and state government agencies. The consortium model involves a group of trusted entities—both public and private—that jointly govern and operate the blockchain network. In this case, these entities would include central government ministries, state transport departments, law enforcement agencies, and public service departments. Each of these bodies has a vested interest in ensuring that the blockchain system functions effectively, while adhering to the legal, policy, and procedural requirements specific to their jurisdiction. A key advantage of the consortium model is shared validation of transactions across multiple nodes, which ensures that no single entity has control over the system. In the context of issuing inter-state privilege passes, the blockchain network can ensure that every transaction, such as the issuance of passes or updates to the system, is validated by multiple stakeholders. This increases the transparency and security of the system. Moreover, the shared governance structure allows for collaborative decision-making when it comes to upgrading or modifying smart contract protocols. These smart contracts, which automate the issuance of privilege passes, can be upgraded with consensus from the consortium. This feature allows the system to remain adaptable to changing regulations, emerging technologies, and policy needs at both the central and state levels. The governance of the blockchain network would include provisions for auditing and monitoring smart contracts and transactions, ensuring accountability and compliance with government policies. Consensus protocols, such as proof of authority (PoA) or practical Byzantine fault tolerance (PBFT), can be used to validate transactions, ensuring that all participating parties have a say in decision-making and preventing misuse or fraud within the system. Thus, the consortium model governance provides a scalable, transparent, and flexible framework for managing the blockchain network, enabling cooperation between various government stakeholders and fostering a collaborative approach to the implementation and maintenance of the inter- state privilege pass system.

**Inter-State Compatibility:** A significant challenge in implementing a system for inter-state privilege passes lies in ensuring compatibility across different states, each with its own policies, regulations, and legal frameworks. The permissioned blockchain network offers an ideal solution for addressing this challenge through the use of unified smart contracts that are configurable to meet the varying requirements of each state. These smart contracts can be configured with specific parameters tailored to each state's policies, such as eligibility criteria, the duration of pass validity, and the limits on the number of passes that can be issued. This flexibility allows a single smart contract to handle transactions across multiple states, ensuring consistency in the overall system. while accommodating state-specific requirements. For instance, different states may have different rules regarding eligibility for privilege passes,

based on factors such as the purpose of travel or the traveler's demographic characteristics. Smart contracts can be programmed to account for these variations, enabling each state to apply its own policies while maintaining uniformity in the system. This flexibility ensures that the system remains adaptable to the diverse regulatory environments in India, without requiring separate smart contracts for each jurisdiction. Furthermore, the interoperability of the blockchain network is critical for ensuring that a privilege pass issued in one state can be recognized and accepted in another state. Blockchain interoperability protocols can facilitate seamless communication between states, ensuring that all participants in the network have access to real-time data regarding the validity and authenticity of privilege passes. This approach eliminates the need for travelers to apply for separate passes when crossing state borders, streamlining the process and enhancing the user experience. By adopting configurable and interoperable smart contracts, the blockchain system can provide cross-state compatibility, ensuring compliance with local regulations while promoting seamless travel across state boundaries. This enables the broader goal of creating an efficient and effective framework for inter-state travel, benefiting both government agencies and citizens.

# 7. BENEFITS

The implementation of a blockchain-based inter- state privilege pass system offers several key advantages, primarily revolving around enhanced security, efficiency, and transparency. The following sections outline the primary benefits:

**Fraud Mitigation via Biometric Checks and Immutable Records:** One of the main advantages of adopting blockchain technology in the privilege pass system is the significant reduction in fraud risks. Biometric authentication can be employed to verify the identity of individuals, ensuring that only eligible users are issued privilege passes. Each transaction related to the pass issuance is securely recorded on the blockchain, creating a permanent, transparent, and verifiable ledger. This immutable record provides a strong defense against fraud, such as the creation of fake passes or unauthorized alterations.

**Auditability through On-Chain Logs:** Blockchain's inherent structure provides full auditability through on-chain logs. Every action in the system, including the issuance, renewal, and validation of privilege passes, is recorded on the blockchain, ensuring complete transparency and traceability. Authorized officials or auditors can access these logs at any time to verify the authenticity of transactions and ensure compliance with regulatory requirements. The audit trail provided by on-chain logs allows for continuous monitoring of the system. It also facilitates the investigation and resolution of any issues or disputes that may arise. This transparency not only enhances trust in the system but also provides a robust mechanism for ensuring accountability.

**Automation Reduces Administrative Burden**: The use of smart contracts significantly enhances the efficiency of the system by automating processes. Smart contracts are self-executing agreements that automatically trigger actions when predefined conditions are met, eliminating the need for manual intervention. In the case of the privilege pass system, smart contracts can automatically verify eligibility, issue passes, and even renew them without human input. This automation reduces the administrative burden, speeds up the processing time, and ensures that errors related to manual data entry or approval are minimized. By decreasing the reliance on administrative staff, the system can operate more efficiently, offering a smoother experience for both citizens and government authorities.

**Interoperability Across States:** The interoperability of blockchain technology is another key advantage in the context of the inter- state privilege pass system. Since each state in India has its own policies and regulations regarding eligibility for privilege passes, the system must accommodate these differences while maintaining consistency across the network. Blockchain's configurable smart contracts provide a solution by allowing each state to define its own criteria for issuing passes, such as eligibility rules or validity periods. The decentralized nature of the blockchain ensures that the system operates seamlessly across state boundaries, enabling the privilege pass issued in one state to be valid in another. This cross-state interoperability reduces the complexity of the system by eliminating the need for multiple passes or applications, enhancing the user experience and promoting efficiency in inter-state travel. By leveraging the unique capabilities of blockchain technology, including fraud mitigation, auditability, automation, and interoperability, the blockchain-based inter-state privilege pass system offers an advanced, efficient, and secure solution. These features work together to provide a streamlined process that benefits

both users and government authorities, ensuring a transparent and efficient means of issuing and validating privilege passes.

## 8. CHALLENGES

While the blockchain-based inter-state privilege pass system offers numerous advantages, it also faces several challenges that must be addressed to ensure successful implementation. The primary challenges are outlined below:

**Integration with Legacy Systems:** A significant challenge when implementing a blockchain-based solution for inter-state privilege passes is the integration with legacy systems currently in use by government departments and other stakeholders. Many existing systems may rely on outdated technology or non-standardized data formats, making it difficult to seamlessly integrate them with a modern blockchain platform. The interoperability between blockchain and legacy systems requires careful planning, including the development of middleware or application programming interfaces (APIs) to facilitate data exchange. Without efficient integration, there is a risk of operational inefficiency, data inconsistency, or disruptions in service. Ensuring that the blockchain system can work harmoniously with existing infrastructure is critical to the smooth transition and adoption of the new system.

**Digital Literacy and Accessibility Gaps**: Another challenge is the digital literacy and accessibility gaps that may exist among certain segments of the population, particularly in rural areas. While blockchain technology promises efficiency and security, not all citizens are familiar with digital tools and online services. This can hinder the adoption of the system, especially for individuals who may lack the skills to navigate digital platforms or access the internet. To address this, the government would need to implement extensive digital literacy programs and provide offline solutions for people who have limited access to technology. It is essential that the system is designed with user-friendliness in mind, ensuring that individuals with varying levels of digital competency can easily access and use the privilege pass system.

**Legal Compliance with Aadhaar and Data Protection Laws:** The integration of biometric data for identity verification raises significant concerns related to legal compliance, particularly with respect to Aadhaar and data protection laws in India. The use of Aadhaar for authentication must comply with the legal requirements set forth by the Aadhaar Act and other privacy regulations, including the Personal Data Protection Bill. Blockchain's immutable nature poses a challenge to data protection principles, such as the right to be forgotten, which is critical under data protection laws. Furthermore, using Aadhaar for authentication purposes requires strict safeguards to prevent unauthorized access, misuse of personal data, and breaches of privacy. The system must therefore ensure compliance with these laws by employing appropriate encryption techniques and data management practices that safeguard user privacy while enabling the secure issuance of privilege passes.

**Scalability and Smart Contract Limitations**: While blockchain technology offers numerous advantages, scalability remains a challenge, particularly for permissioned blockchain that require high levels of consensus among multiple stake holders. Additionally, smart contract limitations must be carefully considered. Although smart contracts automate the process of issuing and validating privilege passes, they are often constrained by the capabilities of the underlying blockchain platform. Issues such as limited contract execution speed, high transaction fees, and the complexity of maintaining and upgrading smart contracts must be addressed to ensure the system remains efficient and flexible. Developing a robust framework for managing these challenges will be crucial to the scalability and sustainability of the inter-state privilege pass system. The blockchain-based inter-state privilege pass system faces a variety of challenges, including integration with legacy systems, digital literacy and accessibility gaps, legal compliance, and scalability issues. Addressing these challenges will require a coordinated effort from all stakeholders involved, including government agencies, technology providers, and the public, to ensure the system's successful deployment and adoption.

## 9. FUTURE WORK

As the blockchain-based inter-state privilege pass system continues to evolve, several opportunities for enhancement and expansion are being explored. The future development of the system will focus on leveraging emerging

technologies, improving user experience, and extending the system's applicability to other areas. The following outlines the key areas of future work:

**AI Integration for Anomaly Detection:** One promising direction for future development is the integration of Artificial Intelligence (AI) for anomaly detection within the blockchain system. AI techniques, such as machine learning and pattern recognition, can be employed to identify unusual behaviors or fraudulent activities within the network. By analyzing transaction patterns and user behavior in real-time, AI systems can flag potential security threats, such as identity fraud or unauthorized access attempts. AI-driven anomaly detection will enhance the system's security by providing proactive alerts and automated responses to suspicious activities. This integration could significantly improve the overall fraud mitigation capabilities, making the system more robust and trustworthy, while reducing the need for manual oversight and intervention.

**Integration with DigiLocker and UPI Apps:** To further streamline the user experience, future work will focus on the integration of the inter-state privilege pass system with DigiLocker and Unified Payments Interface (UPI) applications. DigiLocker, a digital locker system for secure storage of documents, can serve as an ideal platform for storing and sharing the digital privilege pass. By integrating with DigiLocker, citizens could easily access and present their privilege passes from a single, secure digital location. Moreover, integration with UPI apps could enable seamless payment processing for any associated fees, such as for pass renewals or updates. UPI's widespread adoption across India offers the potential for faster and more secure transactions, simplifying the financial aspect of the privilege pass system. Users could make payments directly through their preferred UPI apps, enhancing convenience and reducing friction in the system.

**Public Feedback Systems On-Chain:** Another area for future enhancement is the implementation of a public feedback system directly on the blockchain. By leveraging blockchain's transparency and immutability, citizens can provide real-time feedback regarding their experience with the privilege pass system. This feedback could be recorded on the blockchain, ensuring that it is tamper-proof and publicly accessible. The inclusion of a public feedback mechanism will not only allow the government to monitor public sentiment but also encourage continuous improvement of the system. Stakeholders, including citizens and government officials, will be able to review feedback, identify areas for improvement, and take action accordingly.

**Expansion to Other Welfare Schemes:** Beyond the scope of inter-state privilege passes, the blockchain framework could be expanded to other welfare schemes, such as subsidies, healthcare benefits, or public distribution systems. By utilizing the same underlying technology, the blockchain could help streamline the administration and delivery of various government services. The flexibility of blockchain would allow different welfare schemes to be managed through configurable smart contracts, ensuring that eligibility, disbursements, and auditing processes are automated and transparent. Such an expansion could lead to a holistic digital welfare ecosystem, improving the efficiency, transparency, and accessibility of multiple public services. In conclusion, the future development of the inter- state privilege pass system will focus on AI integration, system integration with DigiLocker and UPI, public feedback systems, and expanding the system's scope to cover other welfare schemes. These advancements have the potential to not only improve the efficiency and security of the privilege pass system but also contribute to the broader goal of digitalizing and modernizing government services in India.

## 10. CONCLUSION

This paper has presented a secure, transparent, and efficient smart contract-based authentication mechanism for issuing privilege passes on a permissioned blockchain. The proposed system harnesses the unique capabilities of blockchain technology, including its immutability, transparency, and security, to address the current challenges associated with the issuance of inter- state privilege passes in India. By leveraging blockchain's decentralized nature and the power of smart contracts, the system not only ensures that the process is streamlined and efficient but also mitigates the risks associated with fraud, manipulation, and human error. A key feature of the system is its ability to enable fraud-proof access to inter-state travel benefits. The use of biometric authentication, coupled with immutable blockchain records, ensures that only eligible individuals are granted privilege passes. The combination of biometric verification with blockchain guarantees that the identity verification process is both highly accurate and secure, minimizing the possibility of fraudulent activities. Given the widespread concerns about identity theft, misrepresentation, and corruption in traditional systems, this mechanism offers a much-needed solution to combat

these issues. The system's design is fully aligned with the objectives of Digital India, which aims to leverage technology to improve the delivery of public services, enhance citizen engagement, and promote transparency and efficiency in government operations. By incorporating cutting-edge technologies such as blockchain and biometrics, the proposed system addresses key challenges faced by public services, particularly in ensuring accessibility, security, and accountability. Furthermore, by automating the entire process through the use of smart contracts, the system removes much of the administrative burden from government agencies, leading to faster processing times, reduced costs, and more accurate records. A primary benefit of the blockchain-based approach is the auditability and transparency it offers. Every action, from the issuance to the renewal and validation of privilege passes, is securely recorded on the blockchain, creating a transparent and immutable audit trail. This not only strengthens accountability but also allows for ongoing monitoring and auditing of transactions. Government authorities, auditors, and stakeholders can access the on-chain logs to verify the legitimacy of transactions and ensure compliance with the regulations, further enhancing public trust in the system. Additionally, this system allows for inclusive access to inter-state travel benefits, catering to citizens from diverse backgrounds, including those from rural or underserved areas who may face difficulties accessing traditional service delivery methods. Given that digital literacy remains a challenge in certain regions, the system has been designed with accessibility in mind. Future work could involve offline solutions or simplified interfaces to ensure that individuals with limited digital literacy can still benefit from the system. As part of its broader societal impact, the inter-state privilege pass system has the potential to transform public service delivery across multiple domains. The blockchain infrastructure that powers this system could be extended to other welfare schemes, such as healthcare benefits, social security programs, and public distribution systems. By creating a unified and scalable framework, blockchain can facilitate the delivery of a wide range of government services in a manner that is more efficient, transparent, and secure. Moreover, this system could be a stepping stone toward a more integrated and interoperable digital governance model. Blockchain's decentralized nature, combined with its flexibility and configurability, allows it to easily integrate with other governmental and public-facing systems, ensuring smooth data exchanges across different domains. For example, integrating the privilege pass system with platforms like Digi Locker for document storage or UPI for payment processing could further streamline the process and enhance the user experience, making the system even more accessible and efficient. However, the successful implementation of the proposed blockchain system requires overcoming several challenges, such as integration with legacy systems, digital literacy gaps, legal compliance, and scalability. Despite these challenges, the future potential of the system remains significant. Ongoing advancements in AI, machine learning, and data protection laws will help mitigate existing hurdles, ensuring the system remains scalable, secure, and compliant with national regulations. In conclusion, the proposed blockchain-based inter-state privilege pass system represents a major step forward in the digitalization of government services in India. The system addresses key concerns of security, efficiency, and transparency, while supporting the Digital India initiative. By implementing blockchain and smart contracts, the system not only improves the administrative efficiency of public services but also enhances the citizen experience. The future potential for scaling this model to other welfare schemes highlights its capacity to transform public service delivery in India and can set a benchmark for future digital governance frameworks globally.

## REFERENCES


[1]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[2]. Corda, R. (2016). Corda: A distributed ledger. R3. Retrieved from https://www.r3.com/corda- platform/ Jain, S., & Patil, S. (2020). "Smart contract- based access control mechanisms for secure digital identity verification." International Journal of Advanced Research in Computer Science, 11(4), 76-82. https://doi.org/10.6029/ijarcs.v11i4.025

[3]. Rai, R., & Verma, A. (2021). "Permissioned blockchain and its applications in the Indian public service sector." Journal of Blockchain Technology and Applications, 3(2), 58-68. https://doi.org/10.1155/jbta.2021.028957

[4]. Zohar, M., & Levy, G. (2019). "A survey of blockchain consensus algorithms." Journal of Computer Science and Technology, 34(4), 907- 918. https://doi.org/10.1007/s11390-019-1947-5

[5]. Singh, R., & Kumar, P. (2020). "Digital identity management using blockchain: Challenges and future directions." International Journal of Digital Governance, 9(3), 112-123. https://doi.org/10.1007/s11320-020-00151-2

[6]. Kumar, V., & Dubey, S. (2022). "Smart contract-based solutions for public welfare services in India." International Journal of Blockchain and Distributed Ledger Technology, 1(2), 45-58. https://doi.org/10.1145/ijbdlt.2022.0010