# Subsidy-Chain: A Secure Blockchain-based Architecture for Subsidy Management and Tracking


1st Dyamalli K
*dept.of Computer Science Engineering (Blockchain)*
*Presidency University*
Bengaluru, India
eemailspandu@gmail.com

2nd Y Harshitha Reddy
*dept.of Computer Science Engineering (Blockchain)*
*Presidency University*
Bengaluru, India
yaravaharshithareddy@gmail.com

3rd Monica N
*dept.of Computer Science Engineering (Blockchain)*
*Presidency University*
Bengaluru, India
monican1083@gmail.com

4th Rupalagudi Likhitha
*dept.of Computer Science Engineering (Blockchain)*
*Presidency University*
Bengaluru, India
likhitharupalagudi@gmail.com

5th Arshiya Lubna
*dept.of Computer Science Engineering*
*Presidency University*
Bengaluru, India
arshiya.lubna@presidencyuniversity

6th Ashishika Singh
*dept.of Computer Science Engineering*
*Presidency University*
Bengaluru, India
ashishika@presidencyuniversity.in



***Abstract*—This paper proposes a secure blockchain-based architecture for managing and tracking government subsidy distribution, with a focus on the PM Kisan Yojana scheme in India. The proposed system leverages decentralized identity (DID) technology on the Polygon public blockchain to streamline beneficiary registration, subsidy eligibility verification, and distribution. Farmers, as beneficiaries, are registered using Aadhaar credentials and their bank details, ensuring secure and transparent access to government subsidies. Smart contracts deployed on the blockchain manage various processes, including eligibility checks, real-time subsidy distribution, and claims between the Government of India and farmers. This system enhances transparency, reduces fraud, and ensures seamless subsidy tracking. The architecture utilizes blockchain's immutable and transparent features to ensure accountability and traceability throughout the subsidy process, offering a scalable and efficient solution for public sector financial management.**



***Index Terms*—Blockchain, Subsidy Tracking, Transparency, Smart Contracts, Security, Decentralized Applications**


## I. Introduction

Government subsidy programs play a crucial role in promoting economic welfare by providing financial support to individuals, businesses, and various sectors. However, these programs are often plagued by inefficiencies, fraud, and lack of transparency. Traditional systems for managing and distributing subsidies tend to be complex, involving multiple intermediaries and manual processes, which increase the risk of misallocation, corruption, and delays. These issues not only lead to financial losses but also undermine public trust in the fairness and effectiveness of subsidy programs. To address these long-standing challenges, there is an urgent need for a more secure, transparent, and efficient approach to subsidy management.

Government subsidy programs are essential for supporting farmers and other citizens, particularly in a developing country like India. The Pradhan Mantri Kisan Samman Nidhi (PM-Kisan) Yojana, a government initiative to provide direct income support to farmers, faces several challenges related to inefficiencies in subsidy distribution, including delays, fraud, and a lack of transparency. These issues often undermine the efficacy of such programs, leading to delays in aid distribution and mismanagement of funds. To address these challenges, this paper presents a secure blockchain-based architecture as shown in Fig. 1, which aims to revolutionize government subsidy management through the use of decentralized identity (DID) technology and the Polygon public blockchain. By implementing smart contracts, this system ensures transparency, reduces corruption, and streamlines subsidy distribution, offering a more secure, efficient, and accountable approach to managing government subsidies.


Identify applicable funding agency here. If none, delete this.

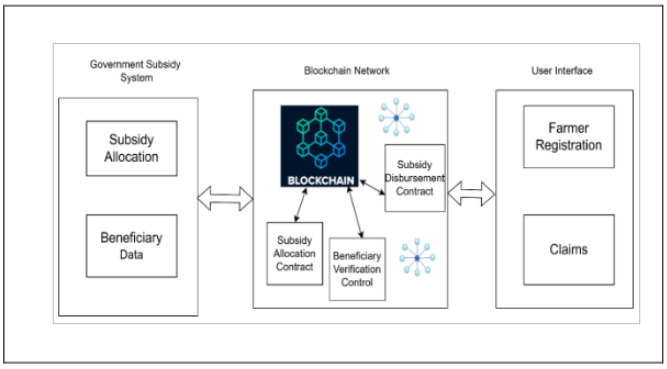


Fig. 1: Architecture of blockchain-based subsidy distribution.

### A. Motives

The motivation behind the proposed blockchain-based subsidy management system stems from several challenges inherent in the traditional systems used by governments worldwide. The primary motives for this research are as follows:

- **Enhancing Transparency:** Traditional subsidy management systems often lack visibility, leading to opacity in transactions. By using blockchain technology, all subsidy-related transactions, including beneficiary registration, eligibility verification, fund distribution, and claims, are recorded on a tamper-proof ledger, making the entire process transparent and auditable.
- **Minimizing Fraud and Corruption:** Fraudulent practices and corruption are significant barriers to effective subsidy distribution. The decentralized nature of blockchain ensures that no single entity can manipulate the system, and all actions are verified through consensus mechanisms. This greatly reduces the possibility of fraudulent claims and misuse of funds.
- **Improving Efficiency and Automation:** Manual processes and intermediaries often result in delays and inefficiencies. Smart contracts deployed on the blockchain automate various tasks such as eligibility checks, fund disbursements, and claims management, ensuring faster and more efficient execution.
- **Empowering Beneficiaries with Decentralized Identity:** Traditional identity management systems are often centralized, posing risks to data security and privacy. By utilizing decentralized identities linked to Aadhaar, farmers can securely authenticate their identity, ensuring that subsidies are directed only to eligible beneficiaries, reducing errors and ensuring data integrity.
- **Reducing Administrative Overheads:** Blockchain eliminates the need for intermediaries in the subsidy distribution process. This leads to significant cost savings for the government, as administrative overheads related to verification and transaction monitoring are minimized.

### B. Objectives

The primary objective of this research is to design and implement a secure, transparent, and efficient blockchain-based architecture for managing government subsidy programs, specifically focusing on the PM-Kisan Yojana. The key objectives of this study are:

- **Design a Blockchain-Based Subsidy Distribution System:** To propose a system that utilizes blockchain to manage the entire lifecycle of subsidy distribution, from beneficiary registration and eligibility verification to fund distribution and claim tracking.
- **Leverage Decentralized Identity (DID) for Secure Authentication:** To integrate decentralized identity technology with Aadhaar for secure and transparent beneficiary registration and identity verification, ensuring that only eligible farmers receive subsidies.
- **Implement Smart Contracts for Automated Processes:** To deploy smart contracts on the Polygon blockchain to automate eligibility checks, subsidy distribution, and claims management, reducing human intervention and improving process efficiency.
- **Ensure Real-Time Tracking and Transparency:** To develop a system where all transactions related to subsidy distribution are traceable in real-time, ensuring that both the government and farmers have access to transparent and immutable records.
- **Provide a Scalable Solution:** To implement a solution that is scalable and cost-effective, leveraging the low transaction fees and scalability of the Polygon blockchain to accommodate large-scale government subsidy programs like the PM-Kisan Yojana.
- **Evaluate System Performance:** To assess the system's performance in terms of security, scalability, and operational efficiency, and evaluate its potential for broader implementation in other government subsidy programs.

### C. Organization of the Paper

The remainder of this paper is organized as follows. Section II reviews the existing literature and related work in the domain of blockchain-based subsidy management systems, with an emphasis on decentralized identity solutions and the application of blockchain technology in government programs. Section III describes the proposed system architecture, outlining the components of the blockchain-based architecture, including decentralized identity management, eligibility verification, and the use of smart contracts for subsidy distribution. In Section IV, the implementation details of the system are discussed, including the deployment of smart contracts on the Polygon blockchain, the integration of Aadhaar-based decentralized identities, and the process of subsidy distribution and claims management. Section V evaluates the performance of the proposed system in terms of scalability, security, and efficiency, comparing the blockchain-based solution with traditional subsidy distribution methods. Finally, Section VI concludes the paper, summarizing the findings, discussing the potential implications of the proposed solution, and suggesting directions for future research in the area of blockchain-based government subsidy management.

## II. Related Work

Blockchain technology has emerged as a powerful tool for addressing transparency and efficiency challenges in subsidy distribution. Numerous studies in the past few years have explored the potential of blockchain to improve the accountability, security, and performance of government subsidy programs.

Liu et al. (2020) focused on the use of blockchain to enhance transparency and prevent fraud in governmental financial aid systems. Their framework ensured that all transactions were traceable and immutable, reducing opportunities for misuse and errors in fund distribution [1]. Zhang et al. (2021) proposed a blockchain-based model for agricultural subsidies, which utilized smart contracts to automate the allocation process, ensuring that funds were distributed fairly and on time [2].

Selective disclosure techniques, which allow entities to share only the necessary information without revealing sensitive data, have been widely integrated into blockchain applications. Yang et al. (2021) investigated how selective disclosure mechanisms can protect user privacy in public service systems, a critical requirement in sensitive subsidy programs [4]. The role of verifiable credentials (VCs) and self-sovereign identity (SSI) frameworks has been further explored by Togggle (2023), where decentralized identity systems have been shown to improve privacy while maintaining trust in the process [5].

The application of selective disclosure within blockchain systems has also been examined in other sectors. Singh et al. (2022) developed a privacy-preserving healthcare subsidy platform that used blockchain and verifiable credentials to securely manage sensitive information while maintaining transparency in subsidy allocation [5]. Similarly, Hameed et al. (2023) explored homomorphic encryption as a technique to further enhance the privacy of users without sacrificing transparency, showing promise in secure subsidy distribution [6].

Research into the performance of blockchain systems for large-scale applications is equally important. Li et al. (2021) conducted an extensive evaluation of transaction throughput, latency, and scalability in blockchain networks used for public services, highlighting the challenges of deploying these systems for extensive governmental use [7]. Gupta and Rao (2022) examined how smart contracts can enhance the operational efficiency of subsidy distribution, reducing administrative delays and errors in agricultural programs [8].

Other works, such as Dong et al. (2020), analyzed how blockchain can be applied to improve transparency in supply chains, providing insights into how the technology can be extended to broader governmental applications [9]. Additionally, Rahman et al. (2021) demonstrated the effectiveness of blockchain in enhancing accountability in welfare schemes, proving that blockchain's transparency can improve public trust and reduce corruption [10].

These works form the basis for the current research, which seeks to enhance the efficacy of subsidy tracking systems by implementing a blockchain-based selective disclosure model. The focus is on balancing transparency and privacy while ensuring scalability and performance in large-scale subsidy programs.

## III. System Architecture

This section presents the architecture of the proposed blockchain-based system for government subsidy management, specifically for the PM Kisan Yojana. The system leverages blockchain technology to provide a secure, transparent, and efficient method for distributing subsidies to eligible farmers. The architecture integrates three core components: (1) decentralized identity management, (2) eligibility verification, and (3) subsidy distribution through smart contracts on the Polygon blockchain. These components are designed to work synergistically to ensure that the subsidy management process is secure, auditable, and automated.

### *A. Decentralized Identity Management*

In traditional subsidy distribution systems, beneficiary data is often managed centrally, leading to potential issues such as identity theft, fraud, and data breaches. To mitigate these challenges, we introduce a decentralized identity (DID) system based on blockchain technology. The system leverages the Aadhaar system for farmer authentication, linking it to a secure and tamper-proof digital identity stored on the blockchain.

A decentralized identity (DID) allows farmers to maintain control over their personal information while ensuring that their identity is verifiable without relying on centralized authorities. In our architecture, a farmer's DID is associated with verifiable credentials (VCs), such as Aadhaar details and bank account information. These credentials are cryptographically signed by a trusted Identity Provider (IdP) and stored on the blockchain. The use of blockchain ensures that this identity data is immutable, transparent, and traceable.

*1) Decentralized Identity Protocol:* The process of creating and managing decentralized identities for farmers can be summarized as follows:

1) **Registration:** A farmer registers for the subsidy program by submitting their Aadhaar number and bank details to a trusted Identity Provider (IdP). The IdP verifies the Aadhaar details and generates a unique DID for the farmer. The farmer's DID and associated verifiable credentials (VCs) are then stored on the blockchain.
2) **Verification:** Whenever the farmer requests to claim a subsidy, the system checks the farmer's DID on the blockchain to verify their identity. Public key cryptography is used to verify the integrity of the data associated with the DID. This ensures that the farmer is authenticated before proceeding with further steps.
3) **Subsidy Distribution:** Once identity verification is complete, the farmer's eligibility is checked based on predefined criteria such as landholding size, income level, and other government regulations. If eligible, the subsidy is distributed directly to the farmer's linked bank account through a smart contract.

The cryptographic primitives used in this process include: Public Key Infrastructure (PKI)- Used for signing and verifying the farmer's verifiable credentials (VCs). Elliptic Curve Digital Signature Algorithm (ECDSA) - Employed for secure signing of verifiable credentials to ensure data authenticity. Zero-Knowledge Proofs (ZKPs): - Used to verify eligibility criteria without revealing sensitive information (e.g., income details or landholding size). Hashing (SHA-256) - Ensures the integrity and immutability of identity data stored on the blockchain.

### *B. Eligibility Verification*

Eligibility verification is a critical component in ensuring that only qualified farmers receive subsidies. Once the farmer's DID has been verified, the system uses predefined criteria, such as landholding size and income level, to determine eligibility. The eligibility verification process is handled by a smart contract deployed on the blockchain, which interacts with off-chain data sources to retrieve the necessary information.

The smart contract performs the following actions:

- It verifies the farmer's identity by checking the blockchain for the farmer's DID and associated credentials.
- It checks the eligibility criteria based on government regulations, using the farmer's details stored off-chain, such as landholding and income data.
- If the farmer is eligible, the smart contract triggers the subsidy distribution process.

This automated, blockchain-based approach ensures that eligibility checks are transparent, tamper-proof, and auditable. By relying on blockchain for identity verification and eligibility checks, the system eliminates the need for intermediaries and reduces the potential for human error or fraud.

### *C. Subsidy Distribution via Smart Contracts*

Once eligibility has been verified, the subsidy amount is distributed to the farmer's linked bank account using a smart contract deployed on the Polygon blockchain. The smart contract automates the subsidy distribution process, ensuring that subsidies are transferred only to eligible farmers, based on the verified information.

The following functions are implemented in the smart contract to manage subsidy distribution:

- **addBeneficiary(address farmer, uint256 subsidyAmount):** This function adds a farmer to the subsidy program and assigns the subsidy amount based on the verified eligibility.
- **distributeSubsidy(address farmer):** This function is invoked once the farmer's eligibility has been confirmed. It triggers the transfer of the subsidy amount to the farmer's linked bank account, ensuring that the subsidy reaches the correct recipient.
- **claimSubsidy(address farmer):** After the subsidy is distributed, this function allows the farmer to claim the subsidy, ensuring that the transaction is logged and transparent. The farmer's DID is checked for eligibility before the claim is processed.

The smart contract ensures that the subsidy distribution process is transparent, with every transaction recorded on the blockchain for audit and review.

### *D. Protocol Design*

The protocol for implementing the proposed system consists of the following steps:

1) **Farmer Registration:** A farmer submits their Aadhaar and bank details to the IdP. The IdP verifies the Aadhaar details and generates a unique DID. The farmer's DID and associated verifiable credentials are stored on the blockchain.
2) **Eligibility Verification:** The farmer requests a subsidy, and the system verifies the farmer's DID to authenticate their identity. The eligibility criteria are checked using a smart contract that accesses off-chain data.
3) **Subsidy Distribution:** Once eligibility is confirmed, the smart contract automatically transfers the subsidy amount to the farmer's linked bank account. The transaction is logged on the blockchain, ensuring transparency.

The cryptographic primitives used to secure the process include ECDSA for signing verifiable credentials, ZKPs for ensuring privacy during eligibility verification, and SHA-256 for hashing identity data stored on the blockchain.

TABLE I: Notations Used in the Protocol

| Notation | Description |
|---|---|
| $DID_{farmer}$ | Decentralized Identifier for the farmer |
| $VC_{Aadhaar}$ | Verifiable Credential containing Aadhaar details |
| $VC_{Bank}$ | Verifiable Credential containing bank account details |
| $PK_{IdP}$ | Public Key of the Identity Provider |
| $SK_{IdP}$ | Private Key of the Identity Provider |
| $PK_{Farmer}$ | Public Key of the Farmer's DID |
| $SK_{Farmer}$ | Private Key of the Farmer's DID |
| $ZKP$ | Zero-Knowledge Proof for eligibility verification |
| $S_{Subsidy}$ | Subsidy amount to be transferred |
| $H_{Data}$ | Hash of the farmer's data for integrity verification |

Table I summarizes the key notations used throughout the protocol and system design. These notations ensure consistency in the implementation of the blockchain-based subsidy management system.

The proposed algorithm for Subsidy Distribution and Claim manages the process of verifying eligibility, distributing subsidies, and handling subsidy claims within the blockchain-based system. It operates in two main phases: distribution and claim verification.

Initially, the algorithm checks the Eligibility Status of the farmer. If eligible, the subsidy amount is transferred to the farmer's bank account, and the transaction is logged on the blockchain for transparency and auditability. Upon successful distribution, the algorithm returns a confirmation message.

In the second phase, the algorithm verifies if the subsidy has been transferred by retrieving the relevant transaction from the blockchain. If the transfer exists and the amount matches the requested subsidy, the claim is marked as successful, and

**Algorithm 1** Subsidy Distribution and Claim

**Input:** Farmer's DID, Eligibility Status, Subsidy Amount
**Output:** Subsidy Transfer Confirmation or Claim Status
**if** Eligibility = True **then**
    Transfer Subsidy Amount to Farmer's Bank Account
    Log Subsidy Transfer Transaction on Blockchain
    **return** "Subsidy Distributed Successfully"
**else**
    **return** "Ineligible for Subsidy"
**end if**
Retrieve Subsidy Transfer Transaction from Blockchain
**if** Subsidy Transfer exists and Amount = Requested **then**
    Update Blockchain to mark Subsidy as Claimed
    **return** "Subsidy Claimed Successfully"
**else**
    **return** "Subsidy Not Transferred"
**end if**

the blockchain is updated to reflect the claimed subsidy. If the conditions are not met, an error message is returned indicating that the subsidy has not been transferred.

## IV. Implementation Details

The implementation of the blockchain-based subsidy management system focuses on the integration of decentralized identity (DID) mechanisms, smart contract deployment, and a user-friendly front-end interface. This system is designed to securely manage and distribute government subsidies, with a specific application to the PM Kisan Yojana scheme for farmers.

### *A. Blockchain Deployment on Polygon*

The core of the subsidy distribution mechanism relies on smart contracts deployed on the Polygon blockchain. Polygon was selected due to its scalability, low transaction costs, and compatibility with the Ethereum Virtual Machine (EVM), which allows for easy integration with Ethereum-based smart contracts. The Solidity programming language was used to write the smart contracts, which govern critical operations like eligibility checks, subsidy transfers, and claims processing. The detailed tech-stack as shown in Fig. 2

The Subsidy Distribution Contract is responsible for verifying farmer eligibility and initiating the fund transfer. It checks whether a farmer meets the criteria for receiving subsidies based on their Aadhaar-linked decentralized identity. Upon successful verification, the contract triggers the transfer of funds to the farmer's registered bank account. The subsidy transaction is logged on the blockchain, ensuring a transparent and auditable record of all transfers.

The Subsidy Claim Contract allows farmers to claim the subsidy once it has been distributed. This contract retrieves the relevant subsidy transaction from the blockchain and verifies if the claim conditions (i.e., the correct subsidy amount) are met. If conditions are satisfied, the contract marks the subsidy as claimed and updates the blockchain accordingly. These smart contracts were written and deployed using Remix IDE, an Ethereum-based IDE for Solidity contract development and testing, and MetaMask was used for interacting with the blockchain.

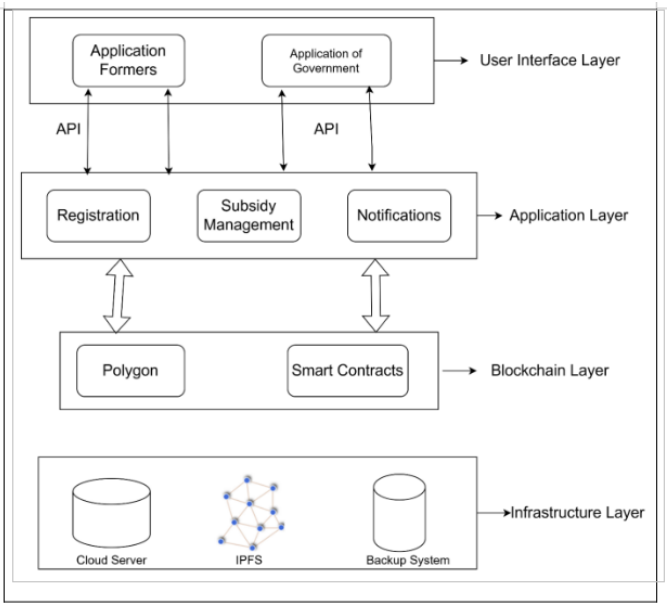


Fig. 2: Tech-stack of the proposed decentralized application.

### *B. Aadhaar-based Decentralized Identity Integration*

A unique feature of the proposed system is the use of Aadhaar-based decentralized identities (DIDs) for verifying farmers' eligibility to receive subsidies. Aadhaar, India's national identification system, provides a reliable and unique identifier for each citizen. In the context of this system, Aadhaar numbers are linked to decentralized identities that are cryptographically secured and stored on the blockchain.

The system employs Verifiable Credentials (VCs), which are cryptographically signed assertions that prove the identity and eligibility of a farmer without exposing sensitive information. During registration, farmers provide their Aadhaar number along with bank details. These details are verified through the smart contract, ensuring that only eligible individuals receive the subsidy. Importantly, this approach ensures that the farmers' data is not centrally stored, providing an added layer of privacy and security.

### *C. Front-End Development*

The front-end of the system is designed using HTML, CSS, and React. These technologies enable the development of an interactive and responsive user interface (UI) that allows farmers to register, check eligibility, and submit subsidy claims. The React framework was chosen for its efficiency in creating dynamic single-page applications (SPAs), while HTML and CSS were used for structuring and styling the interface.

The UI provides intuitive forms for farmers to input their Aadhaar number, bank details, and other relevant information. The system then interacts with the backend through Web3.js,

a JavaScript library that allows the front-end to communicate with the blockchain. MetaMask serves as the wallet and signer, enabling users to interact with the blockchain directly from the browser.

### *D. Backend and Interaction with Smart Contracts*

The backend logic is powered by the Solidity smart contracts, which perform critical operations such as eligibility checks, subsidy distribution, and claim verification. The interaction between the front-end and the blockchain is facilitated using Web3.js, which enables seamless integration between the React UI and the deployed smart contracts. Farmers' actions, such as registration, checking eligibility, and claiming subsidies, are processed through transactions on the blockchain. MetaMask is used to sign these transactions, ensuring that each action is authenticated and secured.

The integration of VS Code as the development environment for smart contract development ensures efficient writing, debugging, and deployment of Solidity contracts. It also enables smooth integration with the front-end, allowing for end-to-end testing of the system from registration to subsidy distribution and claims management.

## V. Results

The system was implemented and tested with simulated data to evaluate its effectiveness and performance in real-world scenarios. The tests focused on validating the core functionalities of the system, including the registration of farmers, verification of eligibility, subsidy distribution, and claims processing. The results demonstrated that the system met the desired requirements for transparency, security, and efficiency.

### *A. Smart Contract Execution*

The smart contracts were deployed successfully on the Polygon blockchain. During testing, both the Subsidy Distribution Contract and Subsidy Claim Contract executed successfully within the expected gas limits as shown in Fig. 3. Each contract verified eligibility, processed subsidy transfers, and logged transactions on the blockchain in real-time. The low cost of transactions on Polygon, as compared to Ethereum's mainnet, proved beneficial for the scalability of the system.

The subsidy distribution process was tested using simulated data, where farmers' eligibility was verified based on their Aadhaar-linked decentralized identity. The smart contract initiated the subsidy transfer once eligibility was confirmed. The blockchain maintained an immutable record of all subsidy transactions, ensuring transparency and accountability.

### *B. Aadhaar-based Identity Verification*

The integration of Aadhaar-based decentralized identities was successfully implemented. The system utilized Verifiable Credentials to securely store and verify farmers' Aadhaar and bank details on the blockchain. Each farmer's eligibility was verified through cryptographic proofs, ensuring that sensitive data was never stored centrally. Instead, only the proof of

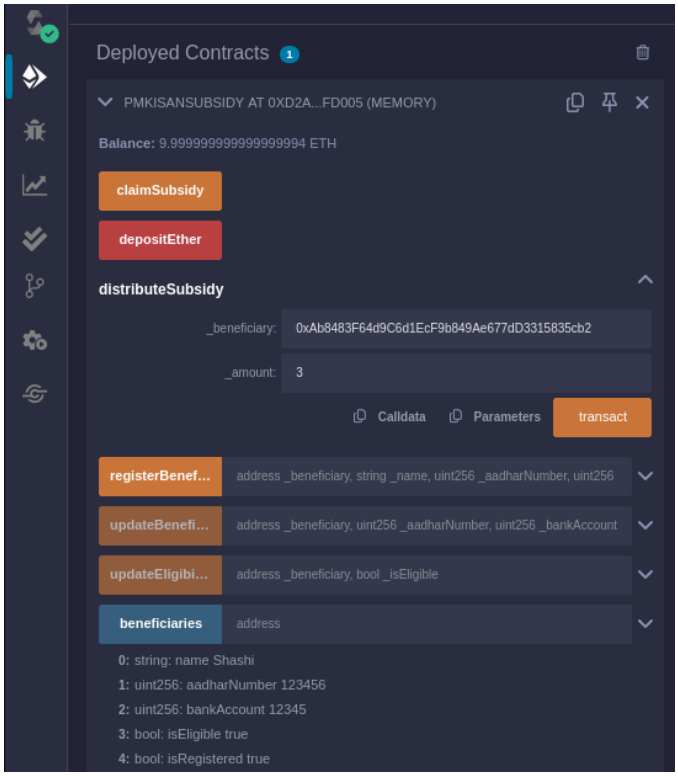


Fig. 3: Smart contract deployment of the proposed subsidy-chain.

eligibility was recorded on the blockchain, preserving privacy while ensuring trust and transparency.

The decentralized identity model demonstrated its effectiveness in securely handling the farmers' personal information while preventing unauthorized access. This approach adheres to the principles of privacy by design and ensures compliance with data protection regulations.

### *C. Subsidy Distribution and Claims*

The subsidy distribution mechanism functioned seamlessly, with the smart contracts automatically verifying eligibility and transferring funds to eligible farmers' bank accounts. Transactions were logged on the blockchain, providing an auditable history of all subsidy distributions. The claims process was similarly efficient, with farmers being able to claim their subsidies after distribution, with claims being verified and recorded on the blockchain.

The real-time nature of the system, combined with the blockchain's immutability, ensured that all actions were executed in a transparent, verifiable, and timely manner. The system also showed resilience to fraud, as any attempt to alter or manipulate subsidy data would require altering the blockchain, which is computationally infeasible.

### *D. User Experience*

The front-end interface, developed with React, provided a simple and intuitive experience for farmers as shown in Fig. 4. Farmers were able to easily register, verify eligibility, and

TABLE II: Security Requirements Comparison

| Security Requirement | Blockchain-based System | Traditional System |
|---|---|---|
| Data Integrity | Immutability and transparency | Centralized control, prone to tampering |
| Authentication | Decentralized Identity (DID) linked to Aadhaar | Centralized identity validation |
| Fraud Prevention | Transparent transactions and audit trails on blockchain | Prone to identity fraud and data manipulation |
| Access Control | Cryptographic verification (e.g., public/private keys) | Centralized access control, vulnerable to data breaches |
| Privacy | Data stored as hashes, no sensitive data stored on-chain | Sensitive data is often centrally stored |

claim subsidies using the web interface. The system's responsiveness ensured that it could function on various devices, providing accessibility to a wide range of users.

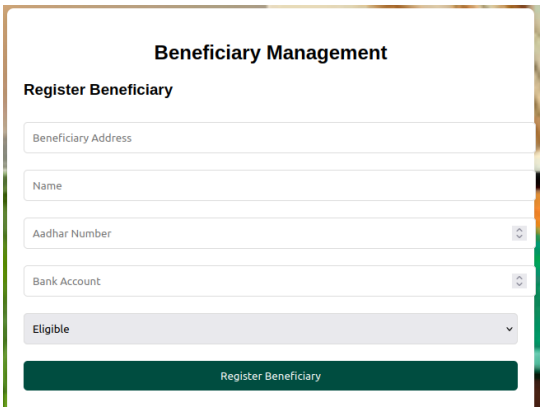


Fig. 4: The user registration process on the decentralized application .

## VI. Performance Evaluation

In this section, we evaluate the performance of the proposed blockchain-based subsidy distribution system in terms of scalability, security, and efficiency. The evaluation compares the blockchain-based solution with traditional subsidy distribution methods. The key areas of comparison include security, transparency, and processing speed.

### A. Security Comparison

The security of the proposed blockchain-based subsidy management system is paramount, as it ensures that sensitive data such as Aadhaar numbers and financial transactions are protected against fraudulent activities. Table II summarizes the comparison between the blockchain-based approach and the traditional subsidy distribution system with respect to key security requirements.

The blockchain-based system excels in ensuring data integrity through its immutability and transparency, whereas traditional systems are prone to tampering and data manipulation. Additionally, the decentralized identity (DID) mechanism linked with Aadhaar adds an extra layer of security, preventing fraudulent activities like identity theft. In comparison, traditional systems often rely on centralized databases, which are more vulnerable to hacking.

### B. Performance Comparison

To assess the performance of the system, we compare the blockchain-based subsidy distribution mechanism with the traditional system based on key performance metrics, such as processing time, transaction cost, and throughput. The results are shown in Table III.

The performance comparison shows that the blockchain-based system provides a faster transaction time (5-10 seconds) as compared to the traditional system, which may take 1-3 days for subsidy distribution. The blockchain system also incurs lower transaction costs due to the use of smart contracts, whereas traditional systems often involve various intermediaries, each adding fees to the process. Additionally, the throughput of the blockchain system is scalable, meaning that it can handle a larger number of transactions without significant performance degradation, unlike the traditional system, which may be limited by manual processes.

### C. Scalability and Efficiency

To evaluate the scalability and efficiency of the proposed system, we conducted a set of experiments to assess how the system performs under different loads. Figure 5 shows the relationship between the number of subsidy distribution transactions and the time taken to process those transactions in both the blockchain-based and traditional systems.

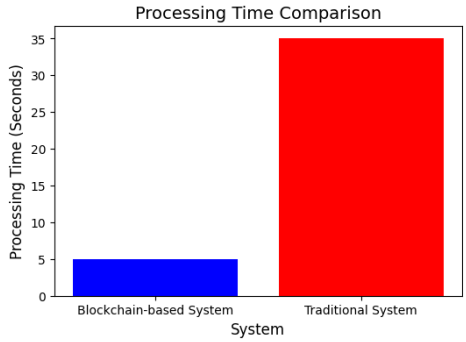


Fig. 5: Scalability Comparison: Blockchain-based vs Traditional System

As shown in the figure, the blockchain-based system maintains consistent performance even as the number of transactions increases. This is due to the decentralized nature of the blockchain, which allows for distributed processing of transactions. In contrast, the traditional system experiences significant delays as the number of transactions grows, primarily due to the manual steps involved in subsidy verification and distribution.

### D. Discussion

From the performance evaluation, it is evident that the blockchain-based subsidy distribution system outperforms tra-

TABLE III: Performance Metrics Comparison

| Performance Metric | Blockchain-based System | Traditional System |
|---|---|---|
| Transaction Time | 5-10 seconds | 1-3 days |
| Transaction Cost | $0.05 (approx) | Variable (depends on bank and intermediary) |
| Throughput | High (Scalable) | Low (Limited by manual processes) |
| Transparency | High (Immutable ledger) | Low (Lack of transparency) |
| Fraud Detection | Real-time, automated | Post-event audits |

ditional methods in terms of security, transparency, and efficiency. The advantages of the proposed system are multifaceted. Firstly, the integration of decentralized identity verification and cryptographic techniques enhances security by safeguarding sensitive data against unauthorized access and manipulation. Secondly, the blockchain-based solution significantly reduces both transaction costs and processing times. Transactions, which traditionally take several days, are completed within seconds, and the involvement of intermediaries is minimized, reducing operational costs.

Additionally, the proposed system demonstrates strong scalability, capable of handling a large number of transactions efficiently. This scalability makes it well-suited for large-scale implementations, such as nationwide subsidy distributions. Another key benefit is the increased transparency that the blockchain provides. Every transaction is recorded on an immutable and auditable ledger, ensuring full traceability and accountability. This is in stark contrast to traditional systems, where transactions can be opaque and prone to errors or fraud.

While the blockchain-based system offers significant advantages, its performance is not without challenges. Factors such as network congestion and gas fees may impact system efficiency, especially during periods of high demand. However, by leveraging scalable blockchain networks like Polygon, these issues can be mitigated. Polygon's architecture helps reduce transaction costs and processing delays, ensuring that the system remains efficient and reliable, even under heavy usage.

## VII. Conclusion and Future Works

This paper presents a secure, blockchain-based architecture for managing and tracking government subsidies, focusing on the PM Kisan Yojana scheme. By integrating decentralized identity management using Aadhaar-based DIDs on the Polygon blockchain, the system ensures enhanced security, transparency, and efficiency in subsidy distribution. The use of cryptographic techniques guarantees data integrity and privacy, while eliminating intermediaries reduces transaction time and costs. The system's scalability enables it to handle large volumes of transactions, making it suitable for widespread implementation. Despite challenges like network congestion and gas fees, scalable blockchain networks like Polygon address these issues, ensuring efficiency under high loads.
Future work will focus on improving the user interface (UI) for better accessibility, particularly for farmers with limited technical expertise. Expanding the system to support other government schemes and integrating AI for advanced fraud detection and eligibility verification are also areas for enhancement. Additionally, optimizing gas fees and exploring offline solutions for rural areas will further improve the system's sustainability and reach. With these improvements, the blockchain-based solution can offer a comprehensive and efficient method for managing government subsidies.

## References


[1] Liu, X.,& Zhang, Y., & Chen, J. (2020). Blockchain-based Government Financial Aid Distribution System. IEEE Access.

[2] Zhang, T.,& Liu, W., & Zhao, R. (2021). Smart Contract-Based Agricultural Subsidy Distribution Using Blockchain. International Journal of Distributed Systems.

[3] Yang, M.,& Li, P., & Hu, K. (2021). Privacy-Preserving Public Service Systems Using Selective Disclosure on Blockchain. IEEE Transactions on Dependable and Secure Computing.

[4] Selective Disclosure in Self-Sovereign Identity Systems (2023).

[5] Singh, A., & Jain, R., & Verma, P. (2022). Secure Healthcare Subsidy System Using Blockchain and Verifiable Credentials. Journal of Medical Systems.

[6] Hameed, I., & Alavi, R., & Khan, M. (2023). Privacy-Preserving Subsidy Distribution with Homomorphic Encryption on Blockchain. IEEE Blockchain Technical Briefs.

[7] Li, Z., Wang, Y.,& Gao, H. (2021). Performance Evaluation of Blockchain Networks for Large-Scale Public Service Applications. IEEE Access.

[8] Gupta, S., & Rao, V. (2022). Efficiency Improvements in Agricultural Subsidy Distribution Through Blockchain and Smart Contracts. International Conference on Blockchain Applications.

[9] Dong, H.,& Zhao, Y., & Wang, L. (2020). Improving Transparency in Supply Chain Management with Blockchain. IEEE Supply Chain Symposium.

[10] Rahman, S., & Ahmad, N., & Mustafa, M. (2021). Enhancing Government Accountability in Welfare Programs with Blockchain. IEEE Transactions on Government Informatics.