Null Card: Blockchain-Powered Single-Card KYC Solution using Web3

Dr. T. N. R. Kumar
Associate Professor
Dept. of Computer Science and Engineering
M. S. Ramaiah Institute of Technology
Bengaluru, Karnataka, India
tnrkumar@msrit.edu

Gurupreeth N.
Dept. of Computer Science and Engineering
M. S. Ramaiah Institute of Technology
Bengaluru, Karnataka, India
1ms22cs056@msrit.edu

Prajwal Paladugu
Dept. of Computer Science and Engineering
M. S. Ramaiah Institute of Technology
Bengaluru, Karnataka, India
1ms22cs103@msrit.edu

Harsh Kumar
Dept. of Computer Science and Engineering
M. S. Ramaiah Institute of Technology
Bengaluru, Karnataka, India
1ms22cs058@msrit.edu

Gulshan Lal
Dept. of Computer Science and Engineering
M. S. Ramaiah Institute of Technology
Bengaluru, Karnataka, India
1ms22cs055@msrit.edu

***Abstract*—Traditional Know Your Customer (KYC) processes are often slow, redundant, and vulnerable to privacy breaches due to their reliance on centralized data repositories. This paper presents *Null Card*, a blockchain-powered, single-card KYC platform leveraging Web3 technologies to realize the vision of "Verify Once, Trusted Forever." Null Card consolidates verified user credentials into a persistent, reusable digital identity secured by blockchain immutability and zero-knowledge cryptographic proofs. The platform streamlines onboarding procedures for financial institutions, governmental bodies, and digital service providers by eliminating repetitive document submissions and enabling privacy-preserving identity validation. Its modular architecture comprises containerized microservices, smart contract-based document validation, decentralized storage via IPFS, and user-friendly interfaces built with Next.js. Institutional APIs enable seamless and secure credential verification through encrypted, token-based access. A structured project management plan using Agile with Scrum ensures iterative development, continuous testing, and stakeholder feedback. Risk mitigation strategies address smart contract vulnerabilities, privacy compliance (e.g., DPDP Act 2023), and blockchain integration complexities. Implementation utilizes Hardhat, Solidity, Express.js, and Tesseract OCR, with mock APIs simulating real-world identity verification. Testing confirms system reliability, transaction immutability, and user-centric design. Future enhancements include biometric authentication, cross-chain interoperability, AI-driven fraud detection, and real-time integration with regulatory APIs. Null Card sets a new benchmark in decentralized identity management by balancing transparency, security, and user control—redefining KYC in the Web3 era.**

***Index Terms*—Blockchain, KYC, Digital Identity, Web3, Smart Contracts, Privacy, Zero-Knowledge Proofs, Decentralized Applications**

I. Introduction

The rapid digitalization of financial services, e-governance platforms, and decentralized applications (dApps) has made secure, efficient, and privacy-centric identity verification a cornerstone of modern digital infrastructure. Know Your Customer (KYC) processes, mandated by regulatory frameworks to curb financial fraud and ensure compliance with anti-money laundering (AML) policies, remain essential for onboarding users across industries. However, traditional KYC mechanisms are riddled with inefficiencies, such as repeated document submissions, fragmented storage systems, lack of standardization, and increased susceptibility to breaches due to centralized architectures.

These centralized systems store sensitive user information in silos, making them attractive targets for cyberattacks and unauthorized access. Furthermore, institutional redundancy in verification workflows results in high operational costs and poor user experience. Users are often required to submit the same set of identity proofs (e.g., Aadhaar, PAN, voter ID) across different platforms, increasing friction and decreasing trust.

Blockchain technology presents a viable alternative by enabling tamper-proof, transparent, and decentralized data handling. With its inherent immutability and consensus mechanisms, blockchain offers a trustless environment for managing identity credentials. When combined with smart contracts and zero-knowledge proofs (ZKPs), it becomes possible to automate document verification while preserving privacy and data minimization.

This paper introduces *Null Card*, a blockchain-powered, single-card KYC platform designed to enable "Verify Once, Trusted Forever." Null Card transforms traditional KYC workflows by issuing users a persistent, cryptographically verifiable digital identity. This identity can be reused securely across multiple institutions without re-submitting original documents, thereby reducing operational overhead and enhancing user autonomy. The system integrates a modular, containerized architecture comprising blockchain-based smart contracts, a

RESTful backend, a responsive web frontend, and optional decentralized storage using IPFS. The platform is designed to comply with contemporary data protection regulations such as the Indian DPDP Act 2023 and GDPR principles, ensuring user privacy without compromising verification authenticity.

Through agile development methodologies, privacy-preserving cryptography, and a scalable Web3 stack, Null Card establishes a future-ready KYC ecosystem that enhances trust, streamlines onboarding, and redefines digital identity management in the decentralized era.

II. Problem Statement

The existing Know Your Customer (KYC) frameworks are outdated and inefficient, creating significant bottlenecks for both users and service providers. These frameworks are inherently fragmented and suffer from multiple technical and operational shortcomings that hinder secure and streamlined user onboarding across platforms:

- **Redundancy:** Users are repeatedly required to submit the same documents (e.g., Aadhaar, PAN, voter ID) to multiple institutions. This results in a frustrating user experience and slows down the onboarding pipeline for financial and digital services.
- **Centralized Vulnerabilities:** Current KYC architectures rely heavily on centralized databases, which serve as single points of failure. These repositories are highly attractive targets for cyberattacks and data breaches, as evidenced by numerous real-world incidents involving sensitive user data leaks.
- **Lack of Interoperability:** Institutions operate in isolated silos, using disparate verification systems and standards. This fragmentation makes it difficult to securely share verified credentials or enable cross-platform verification, often forcing users to restart the KYC process from scratch.
- **High Operational Costs:** Manual document verification, coupled with repetitive administrative overhead, leads to significant resource consumption. Financial institutions must invest heavily in compliance teams, storage infrastructure, and audit trails to meet regulatory demands.
- **User Privacy Risks:** Centralized storage of sensitive identity data increases the risk of unauthorized access, misuse, or surveillance. Moreover, users have limited visibility or control over how their personal information is stored or shared.

In addition to these challenges, regulatory pressures are mounting to improve data protection and privacy compliance, particularly under frameworks such as the European GDPR and India's Digital Personal Data Protection (DPDP) Act 2023. These frameworks emphasize the principles of data minimization, purpose limitation, and user consent, all of which are difficult to guarantee using conventional KYC systems.

Null Card addresses these systemic issues through a decentralized architecture that eliminates the need for repeated document submission and centralized data custody. The proposed platform allows users to maintain control over their identity data while enabling authorized institutions to access cryptographically verified credential proofs using smart contracts and blockchain-based immutability. By embedding privacy-by-design principles and leveraging zero-knowledge proofs, the system enforces selective disclosure, thereby aligning with evolving privacy regulations and setting a foundation for scalable, secure, and user-centric digital identity management.

III. Objectives and Scope

The primary goal of the *Null Card* platform is to address the limitations of traditional KYC systems by developing a decentralized, privacy-preserving, and user-centric digital identity verification solution. This project aims to reimagine KYC workflows by leveraging blockchain's immutability, smart contracts, and advanced cryptographic techniques within a modular and scalable Web3 architecture.

The specific objectives of this project are as follows:

1) **Develop a decentralized KYC platform using blockchain technology:** Establish a tamper-proof distributed ledger for recording KYC verification events, ensuring data integrity, transparency, and resilience to centralized failures.
2) **Implement smart contracts for automated document validation:** Design and deploy Solidity-based smart contracts to encode verification logic and enforce business rules for document approval (e.g., Aadhaar, PAN) with minimal human intervention.
3) **Provide users with a persistent digital identity:** Assign each user a unique, reusable, and cryptographically verifiable digital ID linked to their validated documents, facilitating seamless cross-platform interoperability without repeated document submission.
4) **Ensure privacy and data minimization through cryptographic methods:** Integrate zero-knowledge proof (ZKP) techniques and encryption protocols to enable selective disclosure, ensuring sensitive personal data is not stored or exposed unnecessarily.
5) **Design a user-friendly interface for secure identity management:** Develop a web-based dashboard using Next.js that allows users to upload documents, monitor verification status, manage private keys, and share digital identities with external platforms.
6) **Enable scalable and modular deployment:** Use containerization (Docker) and orchestration (Kubernetes) to build an architecture that supports incremental feature addition, parallel service scaling, and maintainability across varied deployment environments.

Current Scope

The present scope of the project encompasses the development of a functional prototype that simulates real-world KYC

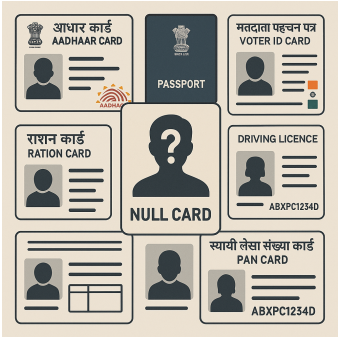

Fig. 1. Null Card Representation as a Universal Card

workflows under academic constraints. The core components include:

- Verification of Aadhaar, PAN, Voter ID, and Driving License using mock or sandbox APIs.
- Recording verification statuses as immutable blockchain transactions.
- Generation of persistent digital IDs with no centralized storage of sensitive data.
- Modular microservice architecture featuring a smart contract layer, Express.js backend, and a responsive Next.js frontend.
- Role-based user authentication with secure private key management.
- Implementation of privacy-by-design principles to align with regulatory best practices.

Future Scope

The project is intentionally designed to support extensibility and long-term adaptability. Potential enhancements include:

- **Integration of additional document types:** Support for passports, utility bills, and academic certificates.
- **Biometric verification:** Incorporation of facial recognition or fingerprint-based identity validation to strengthen user authentication.
- **Advanced cryptographic techniques:** Adoption of stronger zero-knowledge systems (e.g., zk-SNARKs or zk-STARKs) to improve scalability and efficiency.
- **Cross-chain interoperability:** Compatibility with multiple blockchain platforms such as Polygon, Hyperledger, or Solana.
- **AI-driven fraud detection:** Deployment of machine learning models to detect forged or tampered documents during the verification process.
- **Regulatory integration:** Direct API connectivity with governmental systems for real-time document validation and compliance reporting.
- **Mobile application development:** Release of a mobile interface to broaden user accessibility and facilitate remote verification.

Together, these objectives and scope considerations position *Null Card* as a forward-looking solution capable of evolving alongside digital identity and privacy standards in the Web3 era.

IV. Project Organization and Management

Given the dynamic and exploratory nature of blockchain and Web3 application development, the Agile software development methodology, specifically the Scrum framework, was selected to manage the *Null Card* project. Agile enables flexibility, rapid iteration, continuous feedback, and adaptive planning, making it well-suited for projects involving emerging technologies and evolving user requirements.

The project was divided into multiple time-boxed sprints, each typically lasting two to three weeks. Every sprint followed a structured cycle consisting of requirement gathering, architectural design, smart contract and API development, user interface implementation, system testing, and review. This iterative process facilitated early detection of integration issues, incremental delivery of core modules, and the incorporation of feedback from peers and faculty guides. Sprint reviews and daily stand-up meetings were employed to ensure transparency, accountability, and team coordination throughout the project lifecycle.

Role Distribution

To optimize productivity and leverage the diverse skill sets of team members, responsibilities were clearly defined and allocated across four specialized roles:

- **Blockchain Developer:** Responsible for designing and implementing Solidity smart contracts, managing blockchain environments using Hardhat, and ensuring the immutability and correctness of verification logic on the Ethereum-compatible network.
- **Security and Cryptography Engineer:** Focused on implementing privacy-preserving features using cryptographic primitives such as zero-knowledge proofs, handling secure key generation and management, and conducting threat assessments and basic smart contract audits.
- **Full-Stack Developer:** Developed the user-facing Next.js-based frontend and the Express.js backend. Responsibilities included document upload workflows, integration with smart contracts via Web3/Ethers.js, and ensuring a seamless user experience.
- **DevOps and Deployment Specialist:** Handled containerization of services using Docker, configured Kubernetes for orchestration, and established CI/CD pipelines for automated builds and deployments across test environments.

Collaborative Activities and General Contributions

In addition to role-specific tasks, all team members contributed to cross-functional activities including:

- **Literature Survey and Research:** Conducted reviews of blockchain-based KYC systems and cryptographic techniques to inform system design and justify technical decisions.
- **System Design and Architecture:** Collaboratively defined the modular architecture involving smart contracts, backend APIs, and frontend components, including system flowcharts and data models.
- **Testing and Debugging:** Participated in unit and integration testing using simulated user data and mock verification APIs to validate system functionality and robustness.
- **Documentation and Presentation:** Assisted in preparing project reports, technical documents, and presentations for academic evaluations such as the zeroth review, mid-semester review, and final demonstration.

By adopting a structured yet flexible project management methodology, the team was able to deliver a functional and extensible prototype within academic deadlines, while also incorporating best practices from professional software development.

V. Literature Survey

A. Blockchain for e-KYC

The increasing demand for secure, privacy-preserving digital identity systems has drawn substantial attention to the application of blockchain in electronic Know Your Customer (e-KYC) frameworks. Blockchain, as a decentralized and immutable ledger, offers several advantages over traditional centralized KYC infrastructures, particularly in terms of transparency, tamper resistance, auditability, and the potential for interoperability across institutions.

Several recent studies emphasize the use of smart contracts to automate document validation, thereby minimizing manual intervention and reducing turnaround time. AuthBridge, for instance, proposed a blockchain-driven KYC mechanism where encrypted user credentials are shared among authorized institutions through a permissioned network. Such systems allow seamless reuse of previously validated data while maintaining data provenance and regulatory compliance.

However, storing sensitive identity information directly on public blockchains is widely discouraged due to privacy and compliance concerns. Public ledgers, by design, expose transaction metadata to all network participants, making them unsuitable for handling confidential user data. To mitigate this, researchers advocate hybrid storage models that utilize off-chain decentralized storage systems such as the InterPlanetary File System (IPFS) or cloud-based encrypted repositories. In these designs, only cryptographic hashes or proof of verification are recorded on-chain, while the actual data resides off-chain, thereby ensuring both data integrity and confidentiality.

Moreover, permissioned or consortium blockchains are increasingly favored in KYC contexts, as they offer fine-grained access control and identity-aware consensus mechanisms suitable for regulated industries. These platforms support data governance policies and auditing requirements while leveraging blockchain's core strengths.

Despite these advancements, current research gaps remain in areas such as real-time integration with government verification APIs, user-centric privacy controls (e.g., zero-knowledge proofs), and cross-platform interoperability. These challenges underscore the need for practical, scalable solutions—such as the proposed *Null Card* system—that combine blockchain immutability with modern cryptographic techniques and decentralized identity standards.

B. Smart Contracts and Zero-Knowledge Proofs

Smart contracts, which are self-executing pieces of code deployed on the blockchain, play a pivotal role in automating core functions such as document verification, credential issuance, access authorization, and identity validation. By encoding predefined rules into immutable on-chain logic, smart contracts eliminate the need for manual oversight, reduce operational latency, and ensure tamper-resistant enforcement of verification protocols. This not only enhances the trustworthiness of the system but also provides an auditable trail of KYC interactions.

However, smart contracts alone do not inherently protect the confidentiality of user data. To address this, zero-knowledge proofs (ZKPs) have been introduced as a complementary cryptographic technique. ZKPs enable a user (the prover) to prove possession of valid credentials to a verifier without disclosing the underlying information. This approach significantly advances privacy preservation by enabling selective disclosure, a key requirement under data protection regulations such as the General Data Protection Regulation (GDPR) and India's DPDP Act. When integrated with smart contracts, ZKPs provide a verifiable yet privacy-preserving mechanism for digital identity validation, making them well-suited for modern KYC frameworks.

C. Self-Sovereign Identity and Decentralized Identifiers (DIDs)

The paradigm of Self-Sovereign Identity (SSI) represents a shift from centralized identity models toward decentralized frameworks that return control of identity data to the individual. Within the SSI architecture, users own and manage their identity attributes without relying on a central authority. This autonomy not only enhances user trust but also aligns with the principle of data minimization.

Decentralized Identifiers (DIDs), standardized by the W3C, are a core component of SSI. DIDs are unique, persistent identifiers that are not tied to any centralized registry but are instead resolvable via blockchain or other decentralized networks. They enable secure, verifiable interactions between users and service providers and form the foundation for interoperable digital identity systems. By integrating DIDs

with verifiable credentials and blockchain anchors, identity ecosystems can facilitate cross-platform authentication without compromising privacy or control.

D. Research Gaps

While existing blockchain-based e-KYC frameworks have made substantial progress in enhancing data integrity, transparency, and efficiency, several critical research and implementation gaps persist:

- **User-Centric Privacy Mechanisms:** Many implementations lack fine-grained privacy controls or fail to integrate advanced cryptographic schemes such as non-interactive ZKPs and homomorphic encryption, limiting user agency over data sharing.
- **Cross-Platform Interoperability:** The absence of standardized protocols and identity schemas hampers seamless integration between institutions, blockchains, and identity wallets.
- **Real-World API Integration:** Current systems often rely on mock or static datasets and fall short in connecting with real-time, government-issued identity verification APIs.
- **Modularity and Extensibility:** Monolithic architectures impede rapid upgrades, new feature inclusion, or regulatory adaptation.
- **Scalability and Accessibility:** Many frameworks do not address mobile compatibility or fail to incorporate adaptive identity formats suitable for emerging markets.

The proposed *Null Card* platform is designed to bridge these gaps by offering persistent digital identities through blockchain-based anchors, a secure wallet-like interface for credential management, and a modular architecture supporting microservices, containerization, and API extensibility. Through the adoption of privacy-by-design principles and emerging Web3 standards, Null Card contributes to the development of scalable and privacy-compliant digital identity systems that are ready for real-world deployment.

VI. Project Management Plan

The development of the *Null Card* platform adhered to a structured academic schedule, divided into sequential and iterative phases aligned with institutional deliverables and Agile Scrum practices. The project lifecycle was segmented into multiple milestones, including the initial synopsis submission, zeroth review, project planning with a Gantt chart, preparation of the Software Requirements Specification (SRS), literature survey, architectural design, mid-semester evaluation, phased implementation, system integration and testing, documentation, and final evaluation.

Agile project management principles were employed to foster adaptability and ensure continuous progress. Weekly sprints incorporated sprint planning, task estimation, implementation, review, and retrospectives. This approach enabled the team to incorporate feedback, mitigate evolving risks, and adapt to academic deadlines without compromising deliverable quality.

Risk Management

Risks were systematically identified and categorized across technical, managerial, resource, and compliance dimensions. To address these risks, buffer periods were embedded into the sprint schedule, and contingency strategies were formulated. Key risk categories included:

- **Technical Risks:** Integration challenges with blockchain platforms (e.g., Hardhat and Solidity environments), vulnerabilities in smart contracts due to logic flaws or reentrancy issues, and latency introduced by zero-knowledge proof (ZKP) operations.
- **Project Management Risks:** Strict academic deadlines, overlapping coursework, and team coordination complexities were mitigated through clear role allocation, shared calendars, and progress tracking via Git and Trello.
- **Resource Risks:** Limited access to production-grade identity verification APIs required the use of mock endpoints and testnets. Hardware constraints were addressed by containerizing services to run efficiently on low-spec development machines.
- **Regulatory and Ethical Risks:** The platform's handling of simulated identity data mandated attention to ethical considerations and privacy compliance. Although the current version used mock data, provisions were made for future alignment with India's DPDP Act 2023 and global privacy frameworks such as GDPR. Documentation of access policies and consent mechanisms was maintained to guide real-world deployment.

This structured, risk-aware project management methodology ensured that Null Card progressed smoothly through development, testing, and demonstration while maintaining alignment with academic and technical expectations.

VII. Software Requirement Specifications

A. Purpose and Scope

The Software Requirements Specification (SRS) document serves as a foundational blueprint for the design, implementation, and evaluation of the *Null Card* decentralized KYC system. It defines the scope, functionality, constraints, and performance expectations for the platform, offering a reference for developers, stakeholders, and academic evaluators.

The primary objective of the system is to enable users to perform identity verification once and reuse their verified credentials across multiple institutions using a blockchain-anchored persistent digital identity. By integrating smart contracts and cryptographic mechanisms, the system ensures that sensitive identity data remains under user control and is not exposed to unauthorized parties.

B. System Overview

The system comprises a user-facing web interface (developed using Next.js), a backend API layer (Node.js with Express.js), smart contracts (written in Solidity and deployed on a local Ethereum testnet using Hardhat), and an optional decentralized file storage layer (IPFS). Users upload identity documents, which are processed and hashed for integrity before being submitted for verification. Institutions can access verification status via cryptographically signed API calls, without gaining access to raw user data.

C. Functional Requirements

- User registration and login with secure key pair generation.
- Document upload for Aadhaar, PAN, voter ID, and driving license.
- Smart contract-based document hashing, submission, and verification.
- Issuance of a persistent, verifiable digital ID.
- Role-based access control for institutions.
- Viewing and managing verification status.

D. Non-Functional Requirements

- **Privacy and Security:** All identity data is hashed or encrypted before storage. ZKP mechanisms enable selective disclosure.
- **Scalability:** Modular microservices enable independent scaling of identity management, verification, and frontend systems.
- **Interoperability:** The platform is built to integrate with future government APIs and third-party services via RESTful endpoints.
- **Maintainability:** Docker and Kubernetes-based deployment ensures ease of maintenance, portability, and version control.
- **Usability:** User interfaces are responsive, intuitive, and accessible across devices.

This SRS guides the entire project lifecycle and ensures alignment with the platform's goals of security, decentralization, and user empowerment.

E. Product Features

- Document verification for Aadhaar, PAN, voter ID, and driving license using mock APIs.
- Persistent digital ID for reuse across platforms.
- Immutable transaction records on blockchain.
- Privacy-preserving authentication using cryptography and ZKPs.
- Secure key management via wallet-like interface.

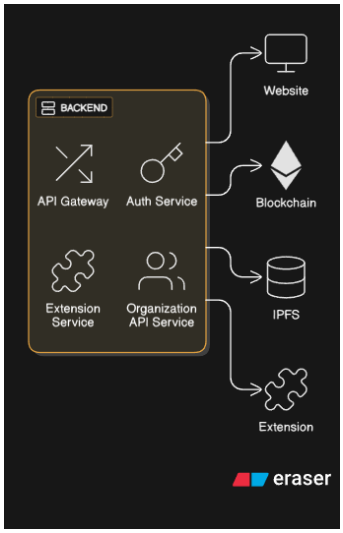

Fig. 2. System Architecture

- User-friendly dashboard for document upload and status tracking.
- Institutional API access for verification.
- Scalable, containerized deployment.

VIII. System Architecture and Design

A. Architecture Overview

The architecture of the *Null Card* system is designed as a modular, four-layer stack to ensure scalability, privacy, and interoperability. Each layer performs specialized functions that collectively support decentralized KYC verification:

- **User Layer:** Consists of a browser-based interface built with Next.js and a wallet-like browser extension that handles cryptographic key management and transaction signing. It facilitates document upload, status monitoring, and secure user authentication.
- **Application Layer:** Powered by an Express.js backend, this layer processes API requests, coordinates identity verification workflows, communicates with smart contracts, and enforces business logic for institutional queries.
- **Blockchain Layer:** Built on the Ethereum-compatible Hardhat testnet, this layer hosts Solidity-based smart contracts responsible for recording verification statuses and anchoring cryptographic proofs. OpenZeppelin templates were used to enforce secure contract design patterns.
- **Data Layer:** Incorporates mock API and sandbox datasets to simulate identity verification. Optionally, InterPlanetary File System (IPFS) is used to store off-chain metadata, ensuring privacy while maintaining document integrity via on-chain hashes.

The system ensures that personally identifiable information (PII) is never stored on-chain. Only verification hashes, digital ID references, and metadata pointers are recorded, satisfying the principle of data minimization and complying with privacy regulations such as the DPDP Act and GDPR.

B. User Interface Design

The frontend features a responsive and accessible dashboard that enables users to upload documents, track verification status, and manage digital identity credentials. A companion browser extension emulates a Web3 wallet, managing private keys, and enabling one-click authentication for third-party verification requests. UI components are styled using Tailwind CSS and adhere to accessibility standards for usability across devices.

C. Low-Level Design

The core workflows include:

- **Document Submission and Hashing:** Users upload documents that are parsed using OCR (Tesseract), hashed, and submitted for verification via smart contracts.
- **Verification and Credential Anchoring:** Admins validate documents through mock APIs and update the user's status on-chain. A unique digital ID is generated and anchored to verified metadata.
- **Verification Querying:** Authorized institutions can verify a user's status via secure RESTful APIs without accessing original documents, using token-based authentication and ZKP-backed disclosures.

Each module is encapsulated and interacts via well-defined interfaces to support maintainability and potential upgrades.

IX. Implementation

A. Tools and Technologies

The system was built using the following technologies:

- **Frontend:** Next.js, React, Tailwind CSS
- **Backend:** Node.js, Express.js, Ethers.js
- **Blockchain:** Solidity, Hardhat, OpenZeppelin Contracts
- **Storage:** IPFS (off-chain metadata)
- **DevOps:** Docker, Kubernetes, Jenkins, GitHub Actions
- **OCR:** Tesseract.js for document content extraction

B. Workflow Summary

The user initiates interaction by connecting their crypto wallet and uploading documents through the dashboard. The backend verifies these documents using sandbox APIs and updates smart contracts with the verification status. All document metadata is securely stored off-chain (IPFS). Institutions can query user status via APIs using the digital ID. Secure interactions are ensured via cryptographic key signatures and access tokens.

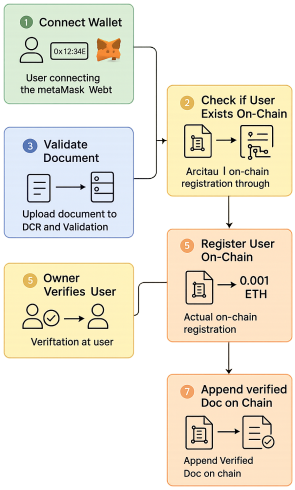

Fig. 3. Workflow Diagram

C. Module Overview

The following system modules were implemented and tested:

- **Wallet Connection Module:** Enables Ethereum wallet integration for user authentication and signature verification.
- **Smart Contract Layer:** Manages document hashes and verification statuses immutably on-chain.
- **Validation Engine:** Processes uploaded documents, integrates OCR, and interfaces with mock verification APIs.
- **IPFS Integration Module:** Handles metadata encryption, off-chain storage, and content-addressable referencing.
- **Admin Panel:** Allows KYC administrators to review submissions and update verification statuses.
- **Browser Extension:** Provides secure private key management and one-click digital ID sharing.
- **Institutional API Gateway:** Facilitates identity verification queries by service providers.
- **Monitoring and Testing Framework:** Integrates logging, smart contract unit tests, and container health checks.

X. Results and Discussion

The *Null Card* prototype successfully demonstrates the feasibility of decentralized, reusable KYC. The key outcome is the realization of the "verify once, trusted forever" paradigm. System-level testing confirmed that blockchain immutability and cryptographic credential sharing improve trust, reduce user friction, and decrease verification redundancy.

Quantitative performance evaluations showed:

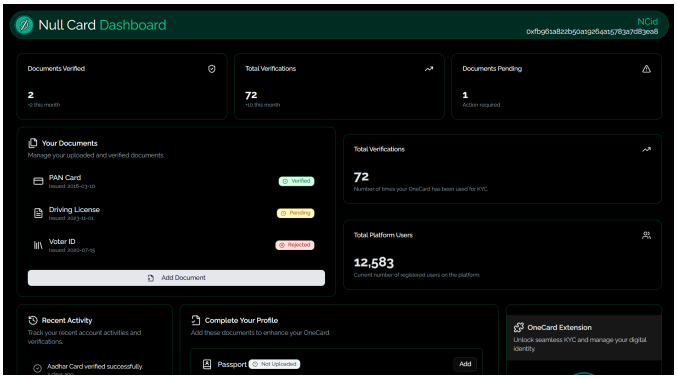

Fig. 4. Webpage Dashboard

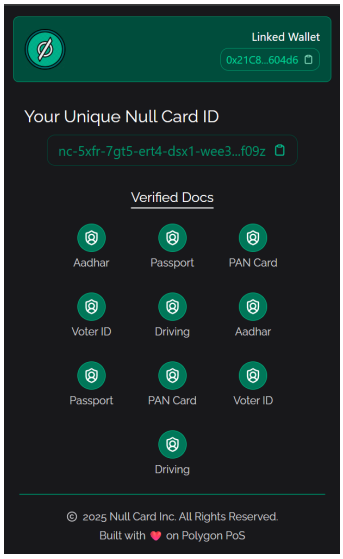

Fig. 5. Extension

- **Sub-second average API response times** for identity queries on the local server.
- **5 second transaction finality** for smart contract writes on the Ethereum testnet (Hardhat environment).
- **Zero critical vulnerabilities** in smart contract logic, verified using OpenZeppelin templates and manual audits.

The system's modular architecture supports scalability and future extensibility. Compared to centralized KYC workflows, Null Card shows clear improvements in operational efficiency, user privacy, and regulatory alignment.

XI. Conclusion and Future Work

This research presents *Null Card*, a blockchain-powered KYC platform that enables persistent digital identity through verifiable credentials, smart contract automation, and decentralized storage. The system successfully addresses core challenges in traditional KYC: inefficiency, centralization, and privacy compromise.

The project demonstrates how modern cryptographic techniques, decentralized protocols, and microservices can collectively improve digital identity management. The current prototype provides a solid foundation for real-world deployment in fintech, e-governance, and Web3 ecosystems.

Future enhancements will include:

- Integration of biometric verification (e.g., facial recognition, fingerprint scanning).
- Expansion of supported document types (e.g., passport, utility bills, academic credentials).
- Deployment on public blockchains such as Polygon or Ethereum Mainnet for real-world interoperability.
- Adoption of advanced cryptographic primitives such as zk-SNARKs for scalable, privacy-preserving proofs.
- Real-time integration with national APIs (e.g., UIDAI, DigiLocker) for live document verification.
- Transitioning to a SaaS-based model for global financial institutions.

These directions position Null Card as a forward-compatible digital identity solution capable of driving compliance and trust in decentralized digital ecosystems.

Acknowledgment

We thank the Management and Dr. N.V.R Naidu, Principal, and Dr R China Appala Naidu, HOD, CSE, MSRIT, for their support. Special thanks to our guide Dr.TNR Kumar for his guidance and encouragement throughout this project.

References

[1] S. Mamatha, R. Kumar, and P. Sharma, "Blockchain-based KYC verification system for financial institutions," *Journal of Financial Technology*, vol. 15, no. 3, pp. 45–62, Mar. 2023.
[2] AuthBridge Consortium, "Decentralized identity verification using blockchain technology," Technical Report, AuthBridge Foundation, 2023.
[3] L. Wang, Y. Zhang, and M. Chen, "Smart contract-based identity verification: A comprehensive survey," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2845–2860, 2021.
[4] J. Gao, H. Liu, and S. Kumar, "Privacy-preserving KYC using zero-knowledge proofs on blockchain," *ACM Transactions on Privacy and Security*, vol. 24, no. 2, pp. 1–28, Apr. 2021.
[5] AppInventiv Technologies, "Blockchain KYC: Applications and benefits in digital identity verification," Technical White Paper, AppInventiv Research, 2025.
[6] KYCChain Foundation, "Interoperable digital identity solutions using blockchain technology," in *Proceedings of the International Conference on Blockchain Technology*, 2024, pp. 112–127.
[7] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 459–474.
[8] W3C Working Group, "Decentralized identifiers (DIDs) v1.0," W3C Recommendation, World Wide Web Consortium, Jul. 2022.
[9] M. Sporny, G. Noble, D. Longley, D. Burnett, and B. Zundel, "Verifiable credentials data model 1.0," W3C Recommendation, World Wide Web Consortium, Nov. 2019.
[10] European Union, "General Data Protection Regulation (GDPR)," *Official Journal of the European Union*, L 119/1, May 2016.
[11] Government of India, "Digital Personal Data Protection Act 2023," Ministry of Electronics and Information Technology, New Delhi, Aug. 2023.
[12] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, 2014.

[13] OpenZeppelin Team, “OpenZeppelin contracts: Secure smart contract library,” GitHub Repository, OpenZeppelin, 2023. [Online]. Available: https://github.com/OpenZeppelin/openzeppelin-contracts
[14] J. Benet, “IPFS - Content addressed, versioned, P2P file system,” *arXiv preprint arXiv:1407.3561*, 2014.
[15] R. Smith, “An overview of the Tesseract OCR engine,” in *Proceedings of the Ninth International Conference on Document Analysis and Recognition*, vol. 2, 2007, pp. 629–633.
[16] K. Schwaber and J. Sutherland, “The Scrum Guide: The definitive guide to Scrum,” Scrum.org, Nov. 2020.
[17] V. Buterin, “Ethereum: A next-generation smart contract and decentralized application platform,” Ethereum White Paper, 2013.
[18] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Bitcoin White Paper, 2008.
[19] Hyperledger Foundation, “Hyperledger Fabric: A distributed ledger framework for enterprise solutions,” Linux Foundation Collaborative Projects, 2023.
[20] A. Chiesa and E. Tromer, “Proof-carrying data and hearsay arguments from signature cards,” in *Proceedings of the 1st Symposium on Innovations in Computer Science*, 2010, pp. 310–331.
[21] C. Allen, “The path to self-sovereign identity,” *Life With Alacrity Blog*, Apr. 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[22] M. Swan, “Blockchain: Blueprint for a new economy,” O’Reilly Media, Inc., 2015.
[23] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts,” in *2016 IEEE Symposium on Security and Privacy*, 2016, pp. 839–858.
[24] J. Groth, “On the size of pairing-based non-interactive arguments,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2016, pp. 305–326.
[25] D. Birch, “Identity is the new money,” London Publishing Partnership, 2014.