A Blockchain Base Decentralized Identity Verification Platform

Team IdentiChain.Ai

Md Arafin Alam Al Bariul

Mobashshir Shahriar Arnob

Md Borhan Uddin Ashik

Asifa Afrin Api

Humaira Nahar Shochona

TABLE OF CONTENTS

Abstract

ChainID represents a paradigm shift in digital identity management, leveraging blockchain technology to create a decentralized, secure, and user-controlled identity verification ecosystem. Our solution addresses the critical challenges of identity fraud, data breaches, and lack of user control over personal information that plague traditional centralized identity systems.

In the digital age, identity verification is essential for accessing services across banking, education, government, and healthcare. Traditional systems rely heavily on centralized databases controlled by third parties, leading to growing concerns over privacy, data breaches, and user autonomy.

Decentralized Identity Verification System (DID) powered by blockchain technology, enabling individuals to control, share, and verify their identity data without relying on centralized authorities. Through the implementation of Self-Sovereign Identity (SSI), blockchain security, and smart contracts, the system ensures secure, transparent, and verifiable identity management.

Problem Analysis

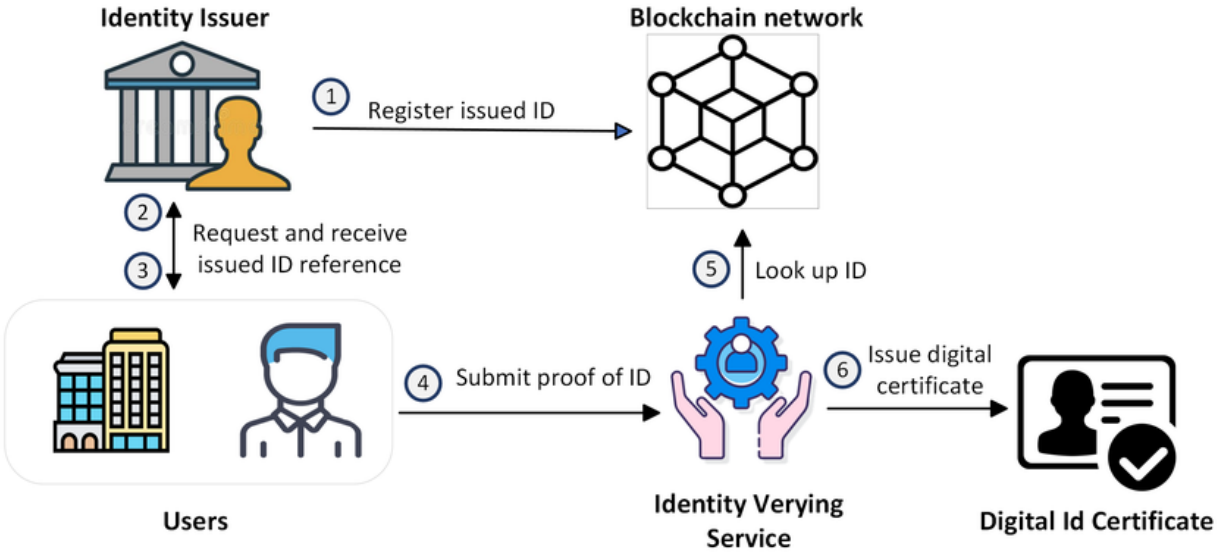
In today's digital world, identity verification is central to accessing essential services like banking, healthcare, education, and government programs. However, most current identity systems are centralized, meaning personal data is stored in large, siloed databases managed by third-party institutions. Users have very little control over their personal information once it is shared — they cannot monitor, revoke, or manage access effectively.

1. **Centralized Data Breaches:** Most identity systems store sensitive personal information in centralized databases. If a hacker breaches that system, millions of user records can be stolen in a single attack.

2. **Lack of User Control:** Users can't manage or revoke access once their data is shared. They don't know who uses it or why, leading to privacy loss.
3. **Identity Fraud:** Stolen or fake IDs allow criminals to impersonate others. Centralized systems are easy targets for document forgery and duplicate identities.
4. **Lack of User Control:** Individuals have no control over how their identity data is stored, shared, or monetized

Solution

The problems identified above give rise to the demand for a secure multi-stakeholder digital environment which produces scope to automate solutions resulting in huge improvements in efficiency and reduced costs. In the new system, the user will have full control over his data, and can dictate who he/she reveals this information to along with what portion of the information he would like to reveal. Thus ensuring security of data and enabling easy verification by various stakeholders.



ChainID offers a revolutionary shift from centralized identity systems by empowering users to **own, control, and manage** their digital identities using blockchain technology. Here's how ChainID solves the core problems:

Centralized Data Breaches → Immutable, Distributed Ledger

ChainID eliminates central databases by storing identity credentials securely on a blockchain, where data is cryptographically hashed and distributed across a decentralized network. This design removes single points of failure — even if one node is attacked, the overall system remains secure, minimizing the risk of mass breaches.

Lack of User Control → Self-Sovereign Identity (SSI)

With ChainID, individuals create and manage their own Decentralized Identifiers (DIDs). These are private, verifiable identities that allow users to grant, monitor, and revoke access to their data at any time. Users can also selectively disclose information — for example, proving they are over 18 without revealing their exact date of birth.

Identity Fraud → Tamper-Proof, Verifiable Credentials

ChainID combats fraud through verifiable credentials signed by trusted issuers (e.g., schools, governments). These credentials are digitally signed and impossible to forge. Verifiers can instantly check authenticity without relying on paper documents or easily faked digital copies.

No Oversight on Data Usage → Transparent, Consent-Based Access

All data transactions and access requests in ChainID are recorded via smart contracts on the blockchain. This creates an auditable, transparent system where users are notified every time their identity is requested. No data is stored or monetized without the user's explicit consent.

Is Blockchain the right approach?

Traditional identity systems fail because they rely on centralized authorities that create single points of failure, control user data, and cannot provide interoperability across different systems. Blockchain technology is uniquely suited to solve these problems because:

1. **Immutability:** Once identity credentials are verified and recorded, they cannot be altered or falsified

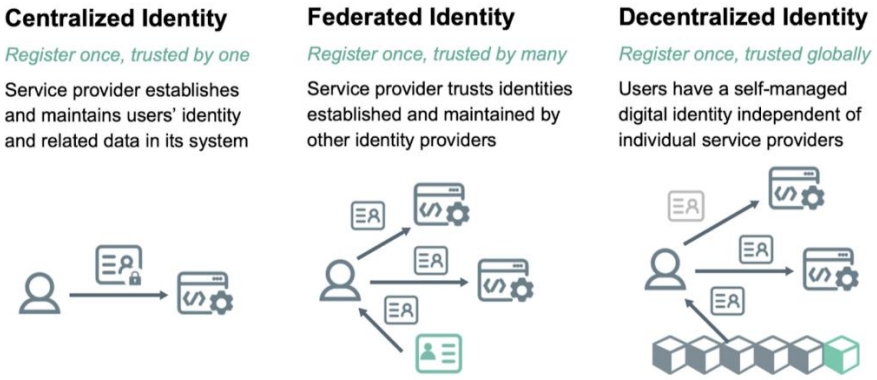
2. **Decentralization:** No single entity controls the identity data, eliminating single points of failure

3. **Cryptographic Security:** Advanced encryption ensures data integrity and user privacy

4. **Interoperability:** Blockchain-based identities work across different platforms and jurisdictions

5. **User Sovereignty:** Users maintain complete control over their identity data and sharing permissions

Our solution employs zero-knowledge proofs to enable identity verification without revealing personal information, ensuring privacy while maintaining security and trust.



Market and Partners

The global digital identity market is experiencing explosive growth:

- **Market Size:** $34.5 billion in 2023, projected to reach $83.2 billion by 2028
- **Growth Rate:** 19.2% CAGR driven by increasing digitalization and security concerns
- **Target Segments**:
  - Financial services (30% of market)
  - Healthcare (25% of market)
  - Government services (20% of market)
  - E-commerce and retail (15% of market)
  - Education and certification (10% of market)

Strategic Partnership Ecosystem

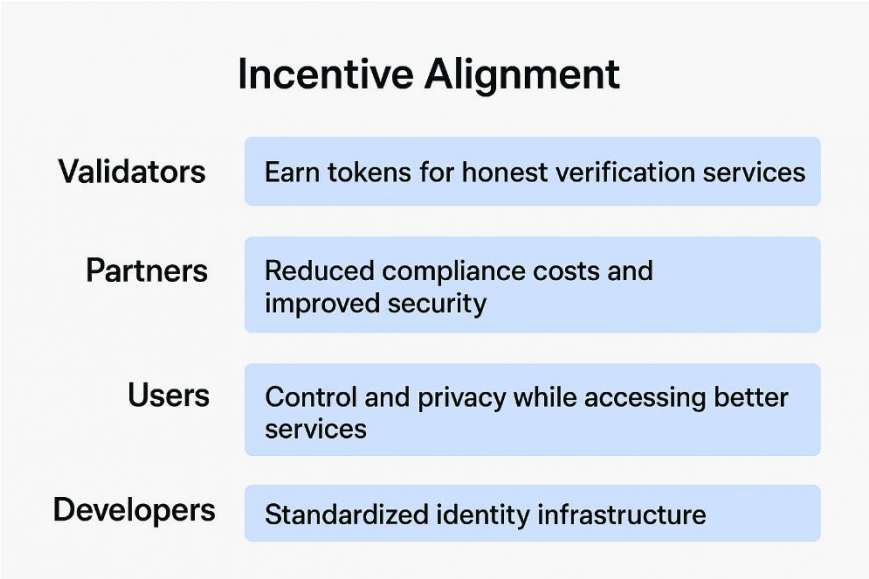
ChainID's success depends on strategic partnerships across multiple sectors:

Government Partners: Government partners such as National ID agencies, Regulatory bodies, and Digital transformation units play a vital role in verifying credentials, ensuring legal compliance, and integrating with citizen services.

Financial Institution Partners: such as Banks, Payment processors, and Insurance companies are crucial for enhancing trust and security.

Technology Partners: Cloud infrastructure providers (e.g., AWS, Azure, Google Cloud), Cybersecurity firms**,** and API integration platforms are essential for building a reliable and scalable identity system. They ensure secure data storage, advanced threat protection, and smooth connectivity across services.

Incentive Alignment: ensures that all participants in the ecosystem are rewarded for their contributions. **Validators** earn tokens for providing honest and accurate verification services. **Partners** benefit from reduced compliance costs and enhanced security. **Users** gain greater control over their personal data and enjoy improved privacy. Meanwhile, **developers** can build faster and more efficiently using a standardized, interoperable identity infrastructure.



Architecture

Technical Architecture

Our solution aims to decentralize and secure citizen data (such as National ID) using Hyperledger Fabric, a permissioned blockchain framework ideal for sensitive and high-trust environments. The system architecture consists of the following major components:

System Overview

Frontend: Developed using React.js with Tailwind CSS for a responsive and modern user interface.

Backend: Powered by Node.js, serving RESTful APIs for frontend communication and blockchain interaction.

Blockchain Layer: Hyperledger Fabric network with multiple government departments as validating nodes.

Database: MongoDB is used for storing encrypted citizen data off-chain.

Identity Management: Each citizen is assigned a Decentralized Identifier (DID) and issued verifiable credentials via blockchain-based identity management.

IPFS (Optional): For storing cryptographic proofs or large files if needed.

Data Flow

1. A citizen registers via the frontend.
2. Their personal data is encrypted and stored in **MongoDB.**
3. A hash of this data and metadata (timestamp, issuer, etc.) is stored **on-chain**.
4. **Smart contracts** handle:
    - Data access requests
    - Consent management
    - Audit trail logging
5. **Verifiable credentials** are issued via DID standards, allowing the citizen to share information securely.

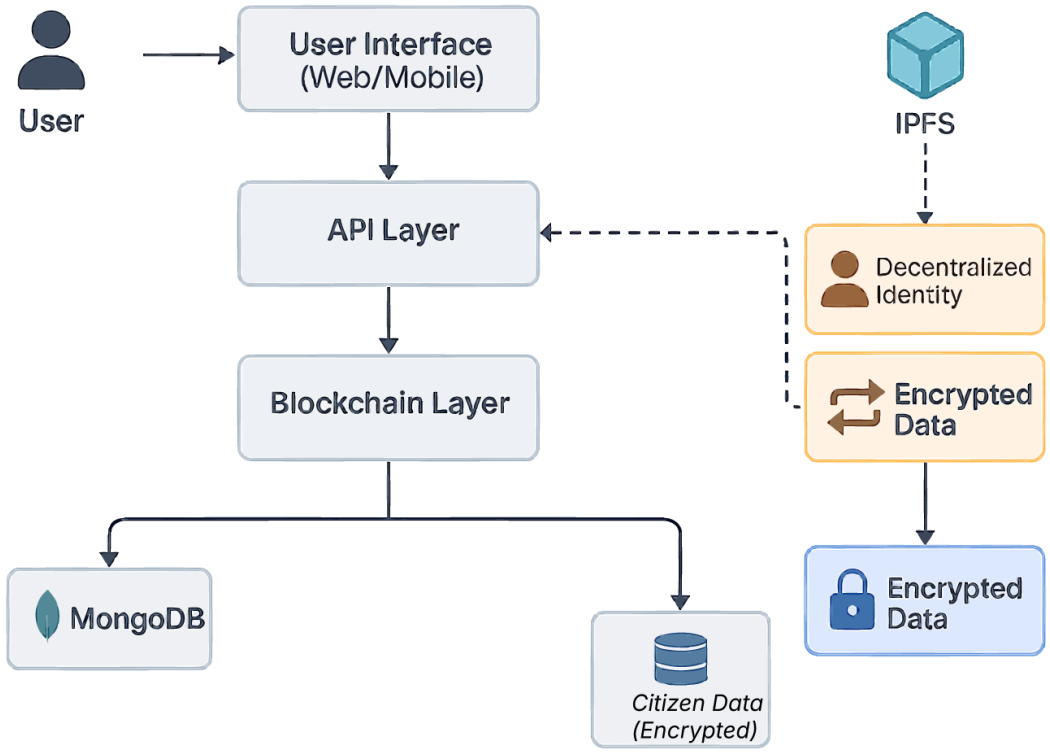
On-chain vs Off-chain Design

Data Type	Storage Location	Justification
Citizen personal data (NID, name, etc.)	Off-chain (MongoDB, Encrypted)	Privacy & storage constraints
Data Hash (for verification)	On-chain	Immutable verification
Access Logs / Audit Trails	On-chain	For accountability
Citizen DID & Credential Metadata	On-chain	For decentralized identity

Smart Contracts Design

Smart contracts in the Fabric chain code are responsible for:

- Data Access Control: Ensures only authorized institutions can request access.
- Consent Enforcement: Citizens must approve access requests via their DID interface.
- Audit Trail: Logs every access or modification attempt.
- Credential Management: Handles issuance and revocation of identity credentials.



Governance

Governance Structure

Governance is divided into **three layers** as per blockchain best practices:

1. Network Membership Governance

- Node Members: Government agencies (e.g., NID Authority, Passport Office) operate Fabric peers.
- Access Rules: Permissioned access controlled via Fabric's MSP and ACL.
- Onboarding/Offboarding: Done through admin proposals and multi-signature voting.

2. Business Network Governance

- A central business charter defines each agency's role.
- Citizen onboarding, data verification and credential issuance workflows are standardized.
- Service-Level Agreements (SLAs) for uptime, support, and regulatory compliance are defined.

3. Technology Infrastructure Governance

- Fabric Chaincode Upgrades: Managed by versioned releases and peer consensus.
- Data Privacy & Compliance: Handled via encryption, access logs, and regulatory reviews.
- Disaster Recovery: Regular backup of off-chain data; chain snapshots for restoration.
- Interoperability: APIs exposed for integration with existing legacy systems in ministries.

Security & Privacy Considerations

- All sensitive data is encrypted using AES-256 before off-chain storage.
- Role-based access is enforced via smart contracts and application layer authentication.
- DID ensures that citizens control their own identity.
- Zero Knowledge Proof (ZKP) techniques may be incorporated for selective data disclosure.

By leveraging Hyperledger Fabric, MongoDB, and DID standards, this architecture ensures:

- Privacy-preserving data management
- Transparent auditability
- Scalable governance
- Citizen empowerment in controlling personal data

This architecture is well-suited to mitigate risks of centralized data leaks and aligns with modern decentralized digital infrastructure ideals.

Competition

Currently in Bangladesh, there are no direct competitors that are focusing on developing a unifying framework for certificates on a publicly accessible blockchain platform.

However, there are some direct & indirect competitors which we can categorize into 3 parts:

Local Software Companies: Local companies such as Datasoft, Revesoft, Lead Soft, Southtech, Tiger IT etc. could provide non-blockchain softwares & solutions in the similar markets we want to target. These companies are the major portion of the current market.

Private Blockchain-as-a-Service (BaaS) Providers: Cloud-based solution that enables developers, entrepreneurs, and enterprises to develop, test, and deploy blockchain applications and smart contracts that will be hosted on a BaaS platform. Provides all the necessary infrastructure and operational support to ensure that the blockchain applications run smoothly. E.g. Azure, IBM, AWS, SAP etc. These companies cannot support government blockchain needs due to restrictions in the Digital Security act of Bangladesh. However the government could use our software, while storing the data in the national fourth tier data center.

Open Public Blockchain Platforms: Open-source community-driven public blockchain platforms where anyone can build blockchain applications. E.g. Ethereum, Neo, Wanchain, Eos etc. These platforms cannot operate in Bangladesh due to the ban on cryptocurrencies.

Existing Competitors

Worldcoin relies on biometric-based identification but faces significant privacy concerns. Civic and uPort were early pioneers in decentralized identity, yet their adoption and scalability remain limited. Sovrin and Evernym have strong enterprise-focused solutions, but they are not designed for direct end-user control or mass-market integration.

Our Competitive Advantage

Our system offers a privacy-first design using advanced cryptographic proofs, ensuring maximum data protection. Users enjoy full control through simple, intuitive interfaces, supported by a flexible architecture that can adapt to both local and global identity systems. With cross-industry compatibility, low partner onboarding barriers, and a compliance-first approach, our platform is built for secure, scalable, and regulatory-ready adoption.

Risk & Mitigation

Category: Technical Risk

Risk	Mitigation
Scalability Challenges	Implement Layer-2 scaling solutions and sharing.
Key Management Failures	Use secure multi-signature wallets and recovery mechanisms.
Quantum Computing Threats	Adopt quantum-resistant cryptographic algorithms.

Category: Business Risk

Risk	Mitigation
Regulatory Uncertainty	Engage proactively with regulatory bodies and adopt compliance frameworks.
Low User Adoption	Provide education programs and seamless onboarding experiences.
Partner Integration Issues	Design flexible APIs and maintain dedicated integration support teams.

Category: Market Risk

Risk	Mitigation
Economic Downturns	Focus on cost-saving value propositions for enterprises.
Rapid Technology Shifts	Maintain an agile development approach and invest in continuous innovation.
High Competition	Build a strong intellectual property portfolio and leverage first-mover advantages.

Category: Operational Risk

Risk	Mitigation
System Downtime & Outages	Use redundant infrastructure, automated failover, and 24/7 monitoring.
Data Breaches & Insider Threats	Enforce zero-trust security, regular security audits, and role-based access control.

Revenue and Distribution

Realistic Revenue Model

Primary Revenue Sources:

1. Government Service Fees:

- $0.02 per identity verification for government agencies
- Target: 50,000 verifications/month in Year 1 = $1,000 monthly revenue
- Gradual scaling to 200,000 verifications/month by Year 3 = $4,000 monthly revenue

2. SaaS Licensing for Government Departments:

- Basic tier: $2,000-$5,000 annually per government department
- Enterprise tier: $10,000-$25,000 annually for larger ministries
- Target: 5 departments in Year 1, scaling to 15 departments by Year 3

3. Integration & Consulting Services:

- $50-$150 per hour for system integration support
- Fixed-price implementation projects: $15,000-$50,000 per agency
- Maintenance contracts: $5,000-$15,000 annually per implementation

4. Premium Citizen Services (Long-term):

- Digital identity wallet premium features: $2-$5/month
- Express verification services: $1 per expedited verification
- Only viable after achieving significant user adoption (Year 2+)

Conservative Revenue Projections:

- Year 1: $50,000-$75,000 (pilot implementations, 3-5 government partners)
- Year 2: $200,000-$300,000 (broader adoption, 8-12 government partners)
- Year 3: $500,000-$750,000 (regional expansion, private sector integration)
- Year 4: $1.2M-$1.8M (national scale, premium services launch)
- Year 5: $2.5M-$4M (mature market, cross-border services)

Pragmatic Go-to-Market Strategy

Phase 1: Proof of Concept (Months 1-8):

The project will partner with 1–2 government departments—such as the National ID Authority and a key ministry like Education—to run a pilot program. The goal is to register 1,000–5,000 citizens, focusing on proving the system's technical feasibility and demonstrating its value to stakeholders.

Phase 2: Limited Production (Months 9-18):

The initiative will expand to 3–5 government departments and introduce a basic citizen-facing mobile application. The target is to register 25,000–50,000 citizens while establishing robust operational processes and collecting valuable user feedback to refine the system.

Phase 3: Regional Scaling (Months 19-30):

The project will scale to 8–12 government departments nationwide, introduce premium features, and form partnerships with the private sector. The aim is to register 150,000–300,000 citizens, ensuring operational sustainability and securing strong market validation.

Phase 4: Market Maturity (Months 31-48):

The project will launch cross-border pilot programs with neighboring countries and fully integrate with private sector players such as banks, telecoms, and healthcare providers. The goal is to surpass 500,000 registered citizens, solidifying market leadership and preparing for large-scale international expansion.

Distribution & Partnership Strategy

Government Partnerships (Primary Focus):

- Start with National ID Authority as anchor partner
- Leverage existing relationships between government departments
- Focus on demonstrating cost savings and efficiency improvements
- Utilize government procurement processes and tender opportunities

Technology Integration Partners:

Collaborate with government IT contractors, system integrators, cloud providers, and cyber security firms to ensure robust, secure, and scalable implementation.

Market Entry Approach:

- Begin with free pilot programs to demonstrate value
- Focus on solving specific pain points (e.g., passport renewal, voter registration)
- Emphasize compliance and security benefits over technological innovation

Value Proposition (Realistic Benefits)

For Government Agencies:

- Cost reduction: 20-30% savings in identity verification processes
- Processing time: 40-50% faster citizen service delivery
- Fraud reduction: 60-70% decrease in identity-related fraud cases
- Audit compliance: Automated reporting and transparent audit trails

For Citizens:

- Convenience: Single digital identity for multiple government services
- Privacy: Greater control over personal data sharing
- Speed: Faster processing of government applications and renewals
- Security: Reduced risk of identity theft and document forgery

For Private Sector (Long-term):

- KYC efficiency: 30-40% reduction in customer onboarding time
- Compliance cost: 25-35% savings in regulatory compliance expenses
- User experience: Seamless identity verification across services

Funding & Sustainability Strategy

Bootstrap Phase (Year 1):

- Minimal viable product development with internal resources
- Government grants and innovation funds ($100,000-$250,000)
- Focus on proving concept and securing first government partnerships

Growth Phase (Year 2-3):

- Angel investment or seed funding ($300,000-$500,000)
- Revenue from government contracts and consulting services
- Reinvest in product development and team expansion

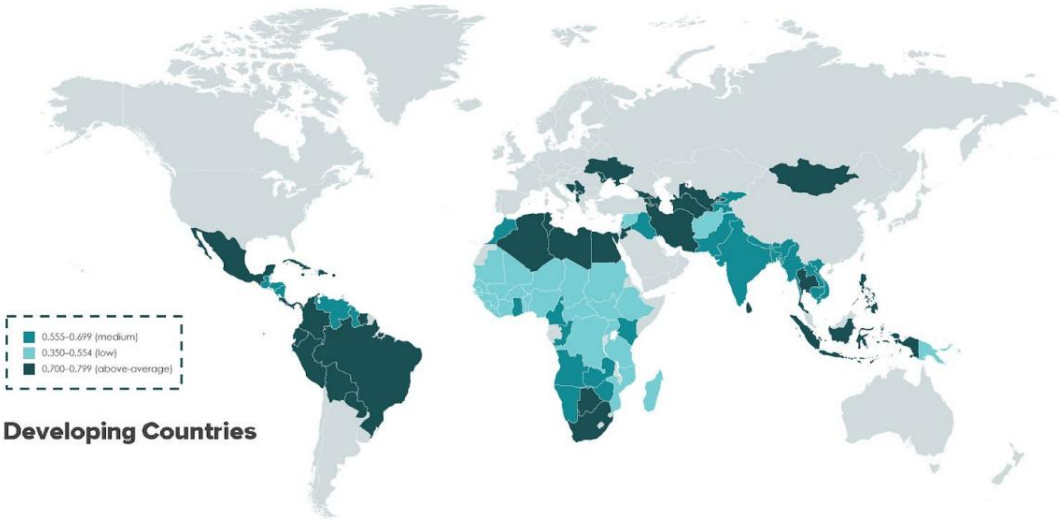
Scale Phase (Year 4-5):

- Series A funding if market validates scalability ($1M-$3M)
- Revenue diversification through private sector partnerships
- Potential for acquisition by larger identity or government technology companies

Impact

The proposed decentralized identity verification system is poised to revolutionize the way individuals interact with digital services across multiple sectors. By placing ownership and control of personal data back into the hands of users, it addresses long-standing issues of privacy, surveillance, and data misuse. The system will reduce institutional burdens related to identity fraud and repetitive verification, lowering operational costs and boosting trust. In developing nations, where millions remain excluded from digital ecosystems due to lack of verifiable identity, this system can play a transformative role in promoting financial and social inclusion. Moreover, it aligns with global efforts toward ethical digital identity frameworks, empowering individuals while enabling secure, efficient, and privacy-preserving service delivery.

Moving Forward



We have a dream to expand beyond our own borders. In the next couple of years, many underdeveloped or developing countries will be seeking new ways to digitize or upgrade their current paper-based certificate systems. By expanding our operations to those countries, we want to assist them into taking a leapfrog to our blockchain-based platform instead of any conventional digital solution.

Appendix

1. Technical Specifications

This section outlines the foundational technologies behind the system, including DID methods, verifiable credentials, smart contracts, and zero-knowledge proofs. For an in-depth overview, see the W3C's Decentralized Identifiers specification:
Source: W3C Decentralized Identifiers (DIDs)

2. Compliance Documentation

Describes how the system aligns with global privacy laws such as GDPR and eIDAS, ensuring user data protection and rights management. For detailed legal frameworks, refer to:
Source: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910 and https://gdpr.eu/

3. Flow Diagrams & Process Maps

Visual representations clarify credential lifecycle and governance workflows. For examples of verifiable credential flows and diagrams, consult:
Source: https://sovrin.org/wp-content/uploads/Sovrin-Whitepaper.pdf

4. Sample Use Cases

Showcases practical applications like banking KYC, academic verification, and healthcare data sharing. For real-world decentralized identity use cases, visit:
Source: https://www.hyperledger.org/use

5. Glossary

Defines core terms related to decentralized identity and blockchain technology. For a comprehensive glossary, check:
Source: https://digitalbazaar.com/glossary/