



VOIS Innovation Marathon 2.0

EkMat: Secure & Private Blockchain Voting



Team No. 34



**MIT ADT University,Loni
Kalbhor, Pune, Maharashtra**

**Team Lead, Ayush
Chougula, CSE**



**Shubham Singh,
CSE**



**Atharv Gaikwad,
CSE**

Problem Statement

- **Eroded Trust:** Systemic irregularities and opaque data disclosure undermine public confidence in traditional voting.
- **High Operational Costs:** Managing elections involves immense manpower (1+ crore staff) and financial expenditure (over ₹4,000 crore).
- **Low Youth Participation:** Less than 40% of eligible 18–19 year-olds register to vote due to complex processes and accessibility issues.



Broken Trust & Inefficiency

Lack of transparency, high costs and low youth participation plague India's elections.



Decentralised Solution

EkMat combines blockchain, zero-knowledge proofs and IPFS with an AI assistant to deliver secure, anonymous and accessible voting.



Transformational Impact

By digitising the process, we can cut costs by ~50% and raise participation by up to 3x.

Need of Project

- **The Solution:** A decentralized "Zero-Knowledge" voting ecosystem called EkMat.
- **Restoring Confidence:** Replaces centralized trust with cryptographic verifiability, ensuring results are tamper-proof and immutable.
- **Resource Efficiency:** Automates eligibility and counting to reduce manpower by 70% and operational costs by up to 60%.
- **Inclusivity:** Empowers citizens with a digital-first approach, removing physical barriers to boost participation by up to 3x.

Proposed Solution

- **Core Concept:** A "Zero-Knowledge" Blockchain Voting system designed to redefine democratic processes by providing absolute privacy and tamper-proof security.
- **Privacy-First Architecture:** Utilizes Groth16 zk-SNARKs to prove a voter is eligible without ever revealing their identity or who they voted for.
- **Trust Through Transparency:** Replaces a centralized "black box" system with an on-chain ledger where every step is publicly auditable and verifiable.
- **Integrity Measures:** Incorporates nullifier hashing and Merkle tree eligibility checks to cryptographically ensure that double voting is impossible.
- **Cost & Labor Efficiency:** Designed to automate the verification and counting process, aiming to reduce election costs by 60% and manpower requirements by 70%.

Solution Overview

- **Decentralized Infrastructure:** Built on the Ethereum blockchain (Sepolia Testnet) to ensure that election logic and results are permanent and immutable.
- **The Voting Flow:**
 - Registration:** Voters are verified against an eligibility database.
 - Proof Generation:** SnarkJS allows voters to generate cryptographic proofs directly on their own device, keeping sensitive data private.
 - On-Chain Validation:** The smart contract (Verifier.sol) checks the proof and records the vote only if it passes all cryptographic hurdles.
 - Censorship-Resistant Storage:** Uses IPFS and Pinata to store election manifests and metadata, ensuring that no single authority can delete or alter data.
- **EkSaathi AI Assistant:** A multilingual GenAI guide (powered by Llama 3) that helps voters navigate the portal in their native language to reduce participation barriers.
- **Live Auditability:** Includes a dedicated Results Dashboard for transparent, real-time tracking of election progress.

Technology used

1

Blockchain: Ethereum, Solidity (EkMatVoting.sol), and Ethers.js.

2

AI (EkSaathi): Powered by Llama 3/3.2 and Langflow for multilingual support.

3

Storage: IPFS and Pinata for censorship-resistant metadata storage.

4

UI/UX: Built with React and TypeScript for a robust, secure interface.

EkMat: Secure & Private Blockchain Voting

Technology Used



Blockchain &
Smart Contracts



Privacy & Cryptography
(Zero-Knowledge)



Agentic AI & GenAI
(EkSaathi)



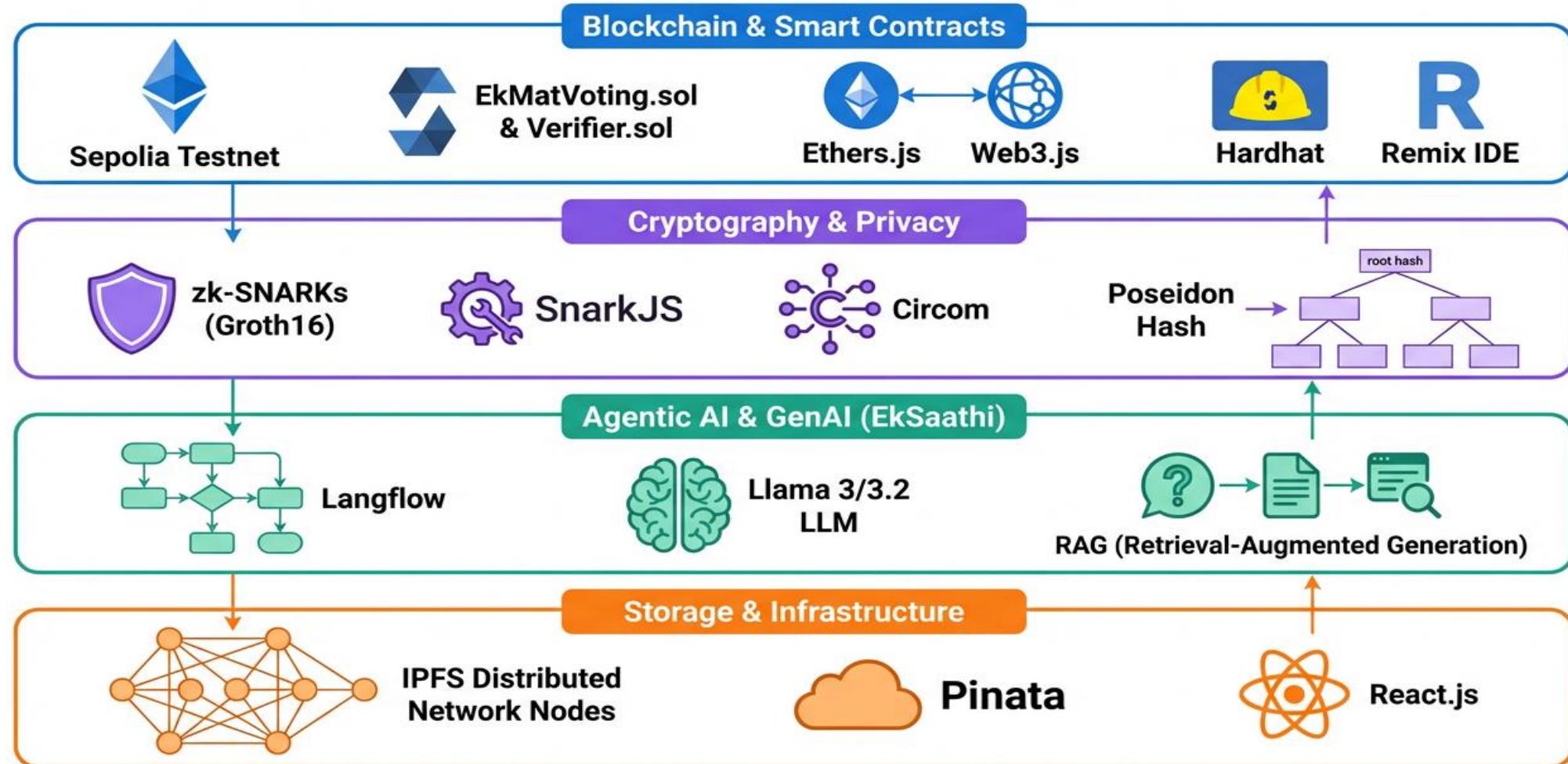
Decentralized
Infrastructure

- Ethereum (Sepolia Testnet Groth16 zk-SNARKs [🔗](#))
- Solidity
- Web3.js / Ethers.js
- SnarkJS
- Merkle Tree & Nullifier Hashing [🔗](#)

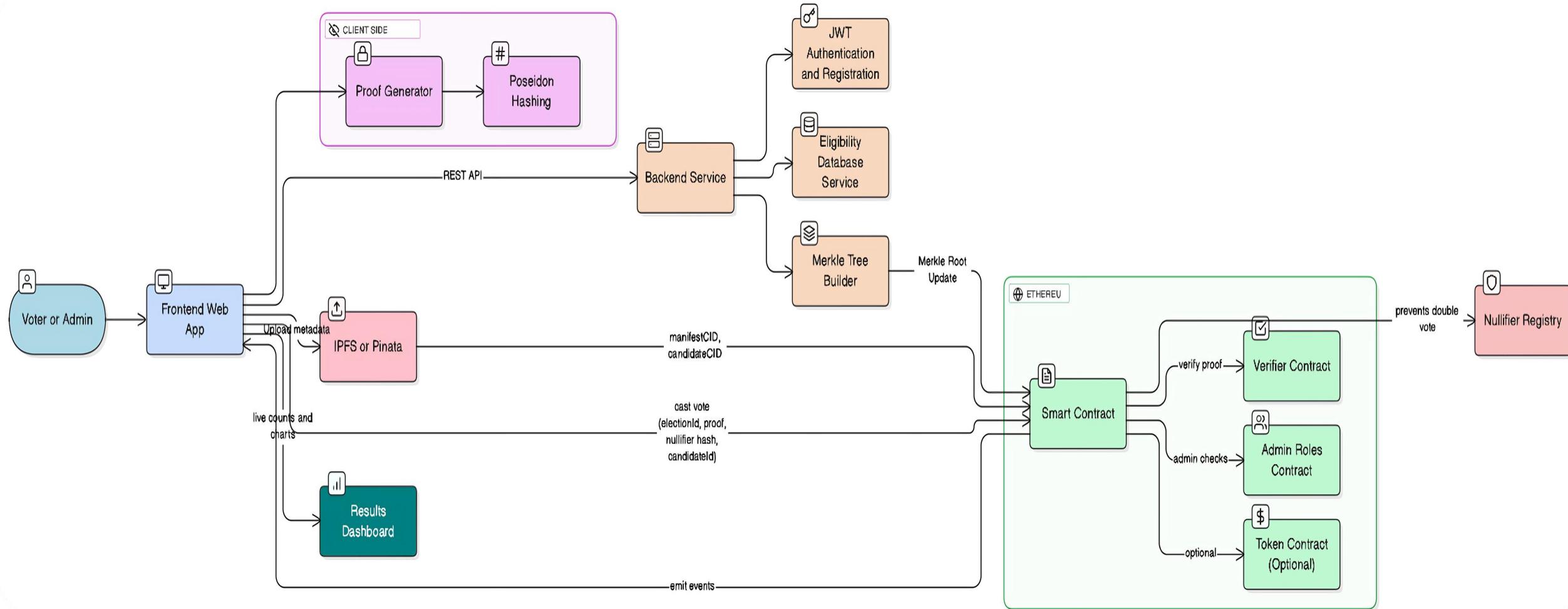
- Langflow Platform
- Llama 3 / 3.2 Models
- Retrieval-Augmented Generation (RAG)
- IPPS InterPlatntanal [🔗](#) & Fisiem [🔗](#)
- Pinata
- React & Tysschipte

Technical flow diagram -

EkMatVoting Decentralized Voting System - Professional Technical Architecture

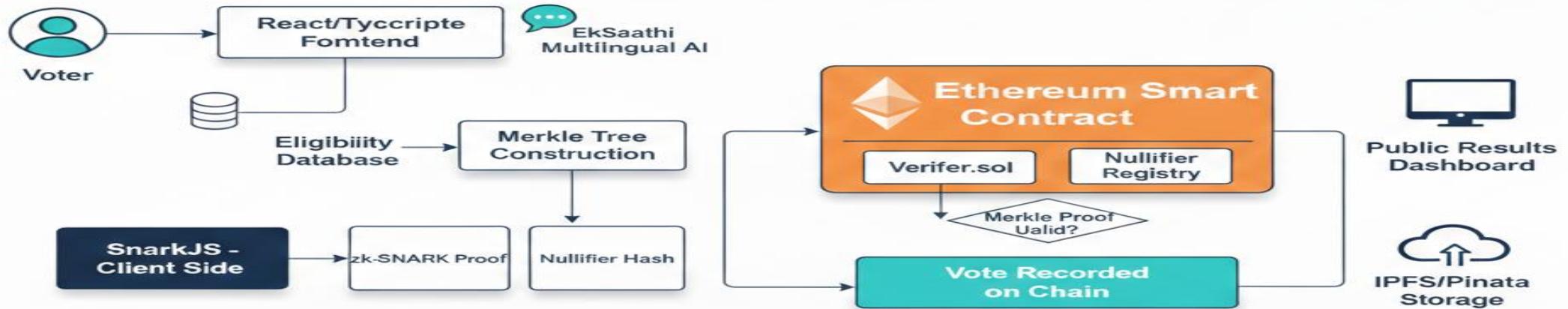


Architecture Blueprint



Workflow diagram

EkMat: Secure & Private Blockchain Voting



Screen shots of your project -

The screenshot shows the homepage of the EkMat Pilot Election Portal. At the top, there is a navigation bar with the logo "EkMat PILOT ELECTION PORTAL" on the left, followed by links for Home, Vote, Results, Audit, Admin, and Support. To the right of these are buttons for "Network: Testnet" and "Connect Wallet". Below the navigation bar, a green button indicates "MAINNET READY". The main title "EkMat" is prominently displayed in large blue letters. Below the title, a subtitle reads "Secure, verifiable and privacy-preserving elections on blockchain.". A large blue "Get Started" button is centered below the subtitle. At the bottom of the page, there is a section titled "How It Works" with three numbered steps (1, 2, 3) and a blue speech bubble icon.

EkMat PILOT ELECTION PORTAL

Home Vote Results Audit Admin Support

Network: Testnet Connect Wallet

MAINNET READY

EkMat

Secure, verifiable and privacy-preserving elections on blockchain.

Get Started

How It Works

1 2 3

Connect Wallet

Screen shots of your project -

The screenshot shows the EkMat Pilot Election Portal. At the top, there is a navigation bar with the logo "EkMat PILOT ELECTION PORTAL" and links for Home, Vote, Results, Audit, Admin, Support, Network: Testnet, and Connect Wallet. The main content area is divided into several sections:

- Election Overview:** Displays the message "Viewing real-time results from the ledger." and a dropdown menu showing "No elections found".
- Vote Distribution:** A large empty rectangular area with a dashed border.
- Total Turnout:** Shows "0" in large blue text, followed by "Votes Cast" in smaller text.
- Transparency Resources:** Includes a link to "View Election Manifest (IPFS)" with a small IPFS icon.

At the bottom left, there is a URL: <https://ekmat-deploy-frontend.vercel.app/results>. On the right side, there is a blue circular button with a white square icon.

Screen shots of your project -

The screenshot shows the EkMat Support Center page. At the top, there is a navigation bar with links for Home, Vote, Results, Audit, Admin, and Support. The Support link is currently active, indicated by a blue background. To the right of the navigation bar, it says "Network: Testnet" and there is a "Connect Wallet" button. The main content area has a title "Support Center" and a subtitle "Resources and assistance for the EkMat secure voting ecosystem." Below this, there are two main sections: "HELP & FAQS" and "SYSTEM HEALTH".

HELP & FAQS

Common questions from voters & admins

Identity & Verification Voting Process Technical Security

What should I do if my ID verification fails?

First, double-check that your details match your government-issued ID exactly. If the issue persists, you can submit a support request through the secure form on this page, selecting "ID Issue" as the category.

Where is my personal identity data stored?

Contact support

Name Email
Optional you@example.org

SYSTEM HEALTH

Network Status

All systems operational

Blockchain: Connected (Sepolia Testnet)
IPFS Gateway: Online
ZKP Verifier: Ready

End-to-End Verifiable

Quick help

For urgent issues impacting an active election, contact your election administrator through the official offline channels in addition to filing a report here.

Screen shots of your project -

The screenshot displays the EkMat Pilot Election Portal's user interface. At the top, there is a navigation bar with links for Home, Vote, Results, Audit, Admin, Support, Network: Testnet, and Connect Wallet. Below the navigation bar, the main content area features a title "How It Works" followed by four numbered steps: 1. Verify ID (Government issued identity verification), 2. Prove Eligibility (Generate Zero-Knowledge Proof), 3. Vote Anonymously (Cast your vote on-chain), and 4. Verify Vote (Check via Manifest & Merkle Root). To the right of the steps is a dark-themed support chat window titled "EkSaathi" which states: "EkSaathi will never ask for your private keys, seed phrase, biometric data, or ZKP nullifiers." It also says "Ask EkSaathi anything about ID verification, ZK proofs, or casting your vote." The chat window includes input fields for "Type your question..." and "Send", and buttons for "How to verify ID?", "Is my vote anonymous?", and "Track my vote". A blue speech bubble icon is located at the bottom right of the chat window.

EkMat PILOT ELECTION PORTAL

Home Vote Results Audit Admin Support Network: Testnet Connect Wallet

How It Works

- 1 Verify ID
Government issued identity verification
- 2 Prove Eligibility
Generate Zero-Knowledge Proof
- 3 Vote Anonymously
Cast your vote on-chain
- 4 Verify Vote
Check via Manifest & Merkle Root

EkSaathi
Secure, multilingual support assistant · EN हिं मरा
English

EkSaathi will never ask for your private keys, seed phrase, biometric data, or ZKP nullifiers.

Ask EkSaathi anything about ID verification, ZK proofs, or casting your vote.

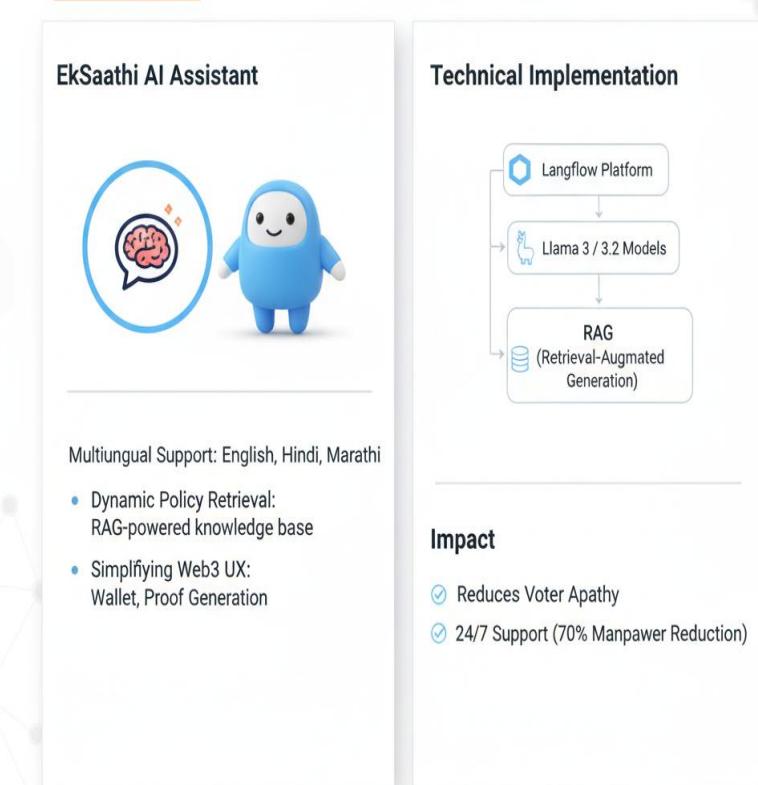
Type your question...

✉

Whv FkMat?

Role of Agentic AI and Gen AI in the solution

- Multilingual Support:** Uses GenAI to provide real-time assistance in English, Hindi, and Marathi, ensuring the portal is inclusive for diverse demographics.
- Dynamic Policy Retrieval:** Utilizes RAG (Retrieval-Augmented Generation) to fetch and explain election rules, voting procedures, and candidate information without human intervention.
- Simplifying Web3 UX:** Acting as an "Agentic Guide," the AI helps users navigate technical steps—such as wallet connection or cryptographic proof generation—through natural language dialogue.



Novelty and Uniqueness

1

Absolute Privacy with **ZK-SNARKs** EkMat is a pioneering platform that merges **Groth16 zk-SNARKs**

2

Client-Side Security Model
Unlike **centralized digital systems**, EkMat uses SnarkJS

3

AI-Driven Multilingual Inclusion The integration of **EkSaathi**

4

End-to-End Auditability
Despite total privacy, every step of the election is recorded on the **Ethereum blockchain**.

Git Hub Link

1. **Public Repository URL:** <https://github.com/ayushcody/vois>

2. **Repository Status:** Public (Enabled "Add README" button)

3. **Mandatory Files Uploaded:**

- **app.py:** The core application logic and backend integration for the EkMat platform.
- **EkMat_ProblemStatement.pdf:** Detailed documentation of "The Ailing Ballot Box" and the crisis of trust in modern elections.
- **EkMat_Presentation.pptx:** The final version of this project presentation for the VOIS Marathon 2.0.

4. **Additional Repository Contents:**

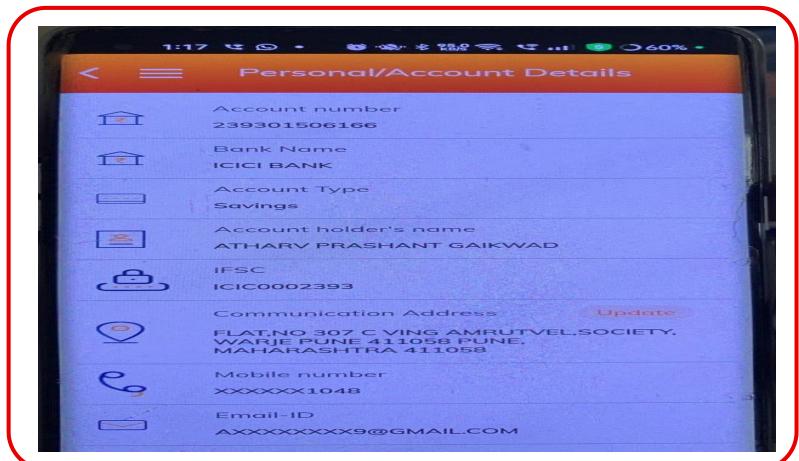
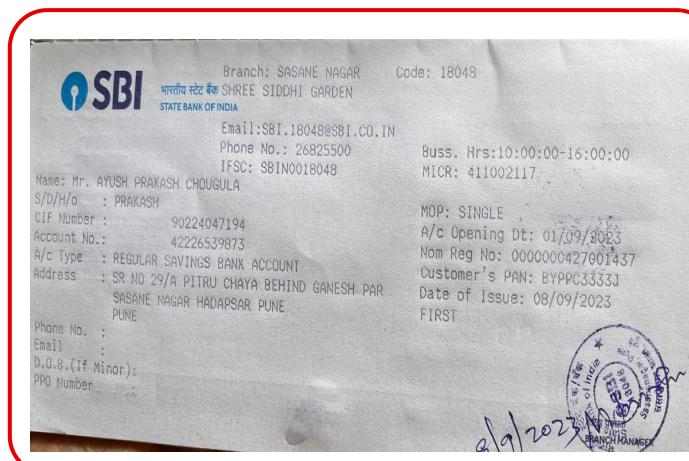
- **Smart Contracts:** Source code for EkMatVoting.sol and Verifier.sol.
- **ZKP Circuits:** The circom files used for generating zero-knowledge proofs.
- **AI Agent Logic:** Orchestration files for the EkSaathi multilingual assistant.
- **Comprehensive README:** Includes a project overview, technical architecture diagrams, and a step-by-step setup guide.

Future Scope

- **National ID Integration (Aadhaar):** Transition from manual verification to automated, cryptographically secure identity checks by integrating with the Aadhaar ecosystem. This will streamline the "Know Your Voter" (KYV) process while maintaining privacy through Zero-Knowledge identity bridging.
- **Layer 2 (L2) Scaling & Batching:** To handle the throughput required for national-level elections, the platform will leverage L2 Rollups (such as zkSync or Arbitrum). This allows for batching thousands of votes into a single on-chain transaction, drastically reducing gas costs and increasing speed.
- **Mobile-First & Offline Support:** Development of a dedicated mobile application designed for low-bandwidth environments. Future iterations will explore "offline-first" cryptographic voting, where votes are signed locally and synced once a connection is established, ensuring inclusivity for rural populations.
- **Decentralized Governance (DAO):** Establishing a Decentralized Autonomous Organization (DAO) to manage the platform's evolution. This ensures that future changes to voting protocols, candidate lists, and system updates are decided by the community rather than a single central authority.
- **Expanded AI Capabilities:** Enhancing EkSaathi to support more regional dialects and accessibility features (such as voice-to-vote for the visually impaired), making the democratic process truly barrier-free.

Bank Details

Full Name (as per bank records):	Bank Name	Branch Name	Account Number	Account Type (Savings / Current)	IFSC Code
Shubham Singh	State Bank Of India	NARELA DELHI,Code: 6812	41505814740	SAVINGS	SBIN0006812
Ayush Prakash Chougula	State Bank Of India	SASANE NAGAR, Code: 18048	42226539873	SAVINGS	SBIN0018048
Atharv Prashant Gaikwad	ICIC Bank	WARJE PUNE	239301506166	SAVINGS	ICIC0002393



Team Member 1

Team Member 2

Team Member 3

Thank You