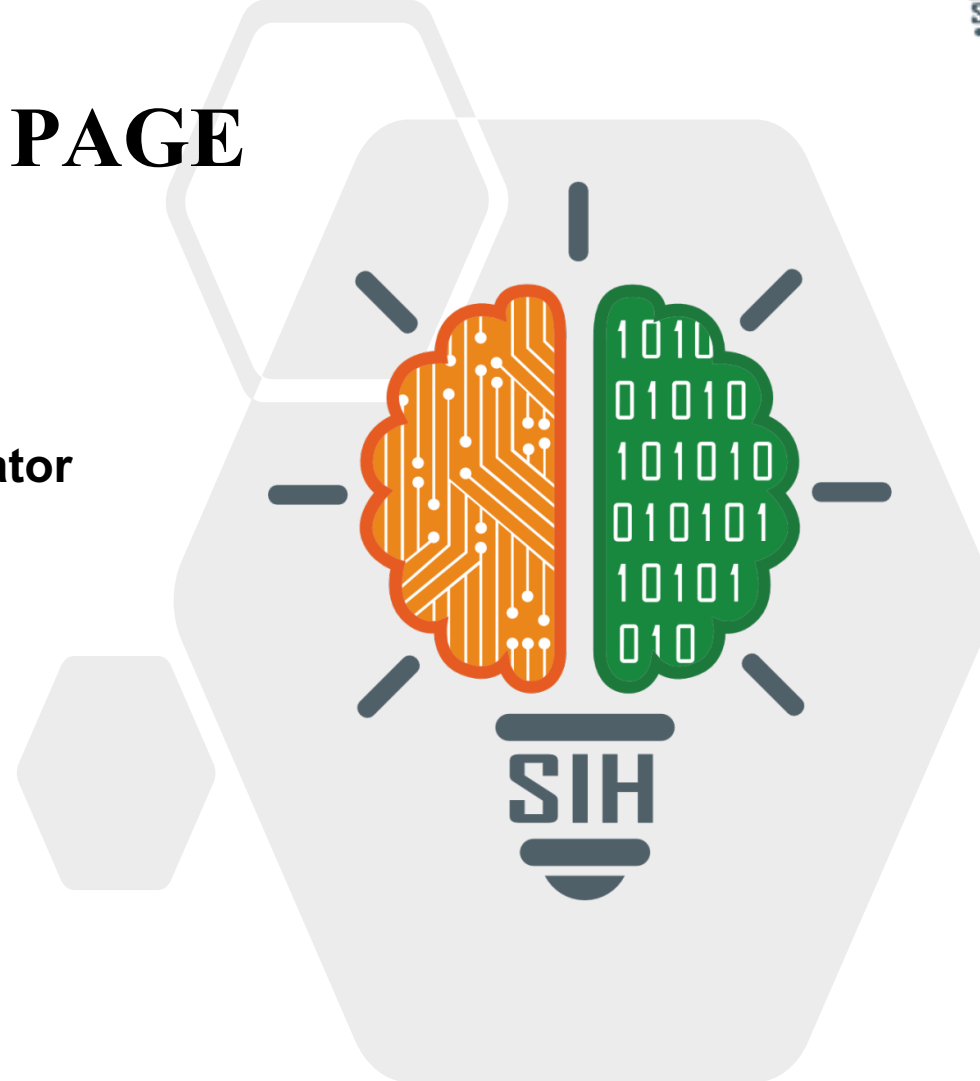# SMART INDIA HACKATHON 2025

TITLE PAGE

- Problem Statement ID –25029

- Problem Statement Title- Authenticity Validator for Academia

- Theme- Smart Education

- PS Category- Software

- Team ID-Bug Bengers

- Team Name - Bug Bengers

Bug
Bengers

- **End-to-end digital verification** – Ensures authenticity of both legacy and new certificates using OCR, AI, and blockchain.

- **Central + decentralized registry cross-verification** – Matches uploaded certificates against verified institutional databases.

- **Intelligent forgery detection** – Detects tampering in seals, photos, grades, and duplicate entries.

- **Scalable, secure platform** – Provides dashboards, alerts, and strict access controls for state-wide rollout.

- **Adaptable across institutions** – Works with diverse formats, ensuring inclusivity and affordability.

TECHNICAL APPROACH

Technologies to be Used:
- Python (AI/ML, OCR)
- Tesseract / Google Vision (OCR)
- Blockchain (Hashing & QR validation)
- MySQL / PostgreSQL (Database)

Methodology:
1. Upload certificate (PDF/scan)
2. OCR + AI → extract & validate details
3. Cross-check with university database
4. Blockchain hash verification
5. Output: Authentic / Fake / Suspicious

FEASIBILITY AND VIABILITY

- Integration with DigiLocker & UGC systems makes adoption realistic as universities are already digitizing records.

- Use of open-source tools like Blockcerts reduces development cost and enables quick prototyping.
- Challenges: Different university ERPs, adoption resistance, and compliance with India's DPDP Act (Data Protection Law).
- Strategy: Begin with pilot projects in select universities, demonstrate success, then scale statewide.
- Using a permissioned blockchain (Hyperledger) ensures scalability, low cost, and faster certificate validation.
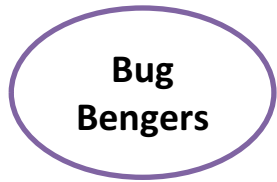
IMPACT AND BENEFITS

- Ensures academic integrity by eliminating fake degrees and certificates.

- Reduces verification time from weeks to seconds via blockchain + QR validation.

- Builds trust among universities, employers, and government bodies.

- Saves administrative costs and minimizes manual paperwork.

- Scalable solution aligned with Digital India and Smart Education initiatives.

RESEARCH AND REFERENCES

- **National Academic Depository (NAD)** – Govt. of India digital repository of academic awards
  DigiLocker NAD

- **DigiLocker** – Secure platform for storing and verifying academic certificates
  DigiLocker

- **Verifi-Chain**: Credential Verification using Blockchain & IPFS
  https://arxiv.org/abs/2307.05797

- Consortium Blockchain for Academic Certificate Verification (Hyperledger)
  https://link.springer.com/chapter/10.1007/978-981-16-8062-5_23

WORKFLOW

Certificate Issuance	Blockchain Storage	Verification Request	Validation Engine	Result & Reporting

The academic institution issues a student's certificate, which is digitally signed and converted into a secure hash. This ensures that the certificate's core data, such as student details and academic records, cannot be altered once generated.

The hash of the certificate is stored on a blockchain ledger along with essential metadata like institution name, course, and year of completion. This immutable storage guarantees that no unauthorized modifications can be made.

When an employer, university, or third party wants to validate a certificate, they upload or scan the document. The system extracts the details, recalculates the hash, and prepares it for comparison against blockchain records.

The verification engine cross-checks the certificate hash with the blockchain entry. If both match, the certificate is marked authentic. If discrepancies are found, the system flags the certificate as fake or tampered.

Finally, the system generates a real-time authenticity report. Verified certificates are instantly approved, while fraudulent attempts trigger alerts and can be logged for further investigation.