MADHAV INSTITUTE OF TECH & SCIENCE
WORK IS WORSHIP

HACKORBIT

Digital Learning
Group

HackOrbit 2025

CODE MAVERICKS

Theme - Web3 and BLOCKCHAIN

Problem Statement -

Nowadays, certificates and credentials are widely shared online on LinkedIn, job portals and in resume. But this sharing leads to some major issues:

- Fake educational degrees are being sold online.
- Forgery and tampering of certificates is becoming too easy.
- Forged skill certifications are misleading recruiters
- Paper-based and PDF-based certificates are easy to edit using simple tools (even a non professional can do that using available online tools.)
- Institutions does not have any standard system to securely issue and verify the certificates.
- Verifiers (employers, colleges, govt) have to spend days for manual validity and authentication.

Key problems -

- Manual verification is slow, costly, and unreliable.
- Creates a lack of trust in institutions and hiring processes.
- The Genuine candidates are overshadowed by fake ones.
- Such a Fraud hiring affects performance and safety of company.
- No universal trusted platform for issuing / verifying certificates.
- Reputational damage of institution whose name is misused.

Our Innovative Solution : TrueStamp ✓

We propose **TrueStamp : a blockchain-powered certificate verification system** built to make certificates and credentials tamper-proof, publicly verifiable, and decentralized.

How It Works:

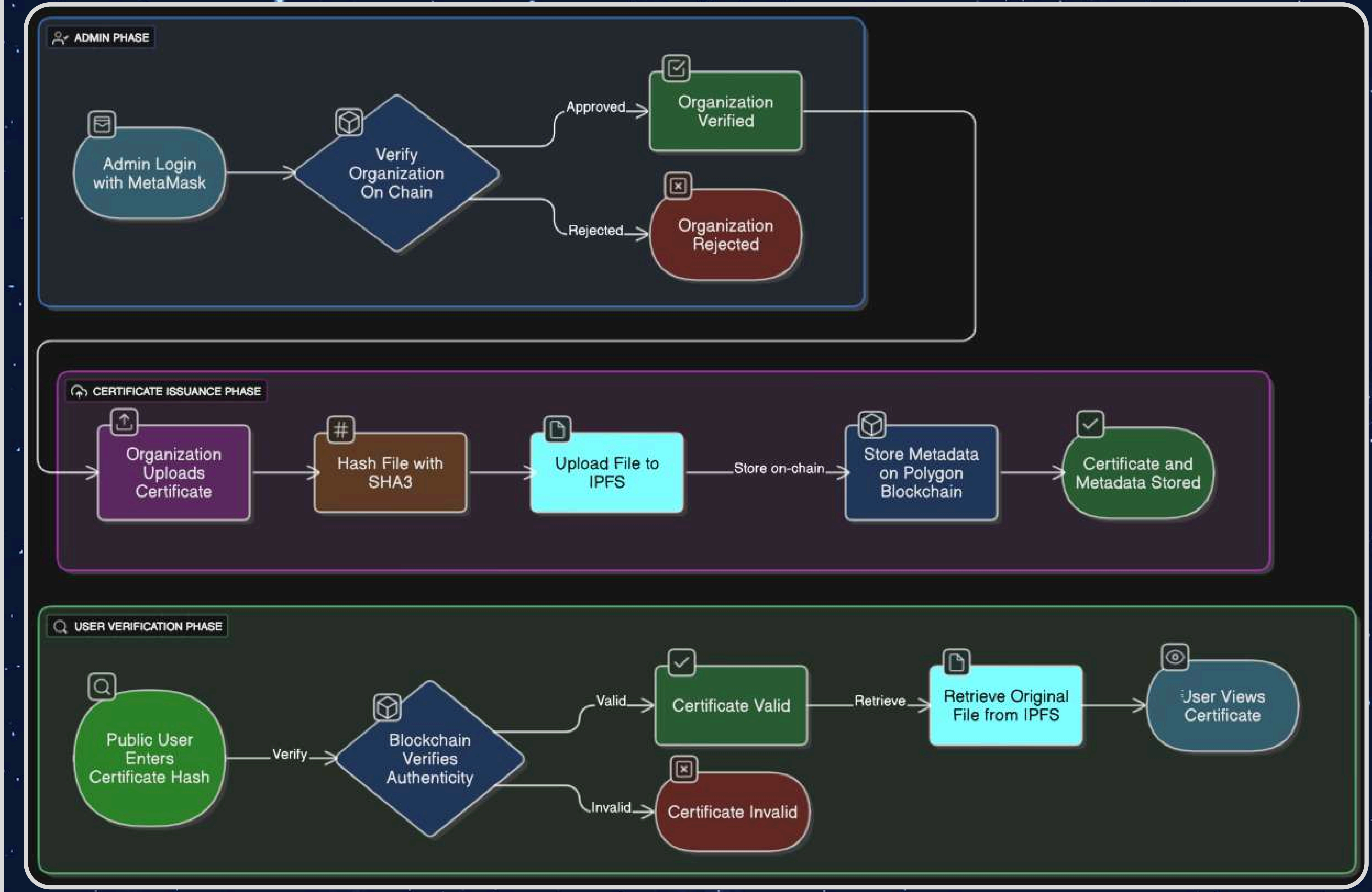
- Colleges or instructors can **issue digital certificates directly on the blockchain**. Allows the issuer to **generate unique hash** for each certificate.

  Certificate is:
- Hashed using SHA3 (unique digital fingerprint)
- Stored on IPFS (decentralized storage)
- Hash stored on blockchain

- Employers or anyone else can verify those certificates using a public search. Since each certificate is associated with a unique hash so **even a minor change will result in generation of completely different hash** which determines whether the **certificate is valid or not.**

- All records are publicly verifiable and tamper-proof — no paperwork required.
- As Anyone can verify the certificate using the hash — no need to trust a middleman.

FLOWCHART & METHODOLOGY


ADMIN PHASE
Admin Login with MetaMask
Verify Organization On Chain
Approved
Organization Verified
Rejected
Organization Rejected
CERTIFICATE ISSUANCE PHASE
Organization Uploads Certificate
Hash File with SHA3
Upload File to IPFS
Store on-chain
Store Metadata on Polygon Blockchain
Certificate and Metadata Stored
USER VERIFICATION PHASE
Public User Enters Certificate Hash
Verify
Blockchain Verifies Authenticity
Valid
Certificate Valid
Invalid
Certificate Invalid
Retrieve
Retrieve Original File from IPFS
User Views Certificate

1.User Connects Wallet:
Admins or issuers connect via MetaMask to access the dashboard securely.

2. Certificate Generation:
Certificate details are entered and converted into a unique SHA3 hash.

3. IPFS Upload:
The certificate file is uploaded to IPFS using Web3.Storage for decentralized storage.

4. Blockchain Recording:
Certificate hash and metadata (recipient, issuer, course, date) are stored on a smart contract on the Polygon network.

5. Public Verification:
Anyone can verify a certificate by entering its hash. If valid, the file is retrieved from IPFS.

This flowchart illustrates the entire lifecycle of certificate verification using blockchain and IPFS:

1.Start

User (admin or issuer) opens the CertiChain Dashboard.

2. Connect Wallet

MetaMask prompts the user to connect a Web3 wallet.

3. Fill Certificate Details

The issuer enters certificate details like name, course, date, etc.

4. Generate Hash

A unique SHA3 hash of the certificate data is generated to ensure tamper-proof integrity.

5. Upload to IPFS

The original certificate file is uploaded to IPFS (via Web3.Storage), giving a decentralized file URL.

6. Store on Blockchain

The hash + metadata + IPFS link are sent to a smart contract deployed on the Polygon network.

7. Verification Request

A verifier enters the hash in the Verify section.

8. Smart Contract Lookup

The contract checks if the hash exists and returns the matching IPFS file and details.

9. Verify Output

If valid, certificate info is shown and file is downloadable from IPFS.

10. End

Tech Stack :

Layer	Tools/Tech
Frontend	Express/React, TailwindCSS, React Router
Web3 Integration	Ethers.js, MetaMask
Blockchain	Polygon Amoy Testnet, Solidity Smart Contract
Storage	IPFS via Web3.Storage
Hashing	js-sha3 (SHA3 hashing algorithm)
Authentication	MetaMask wallet login
Build Tools	Vite, npm

Features & Novelty

Key Features :

- **Blockchain-based Verification** – It Ensures certificates are tamper-proof and publicly verifiable.
- **MetaMask Integration** – Secure and decentralized login for the authorized issuers.
- **IPFS Storage** – Certificates are stored on decentralized web for permanent access.
- **Easy Hash-Based Search** – Just enter a certificate hash to verify instantly.
- **User-Friendly Dashboard** – Simple interface for Admins, Issuers, and Public Verifiers.

What Makes It Novel ?

- **TrueStamp** does not rely on centralized storage or approval like other traditional platforms (e.g., DigiLocker), .
- It Uses Web3 technology end-to-end: Smart Contracts, IPFS, Wallets.
- No server dependency – Everything is peer-to-peer, verifiable, and forever accessible.
- Open for any institution – It Can be extended beyond government use, like private universities, online courses, or hackathon certificates.

Real-Life Use Cases :

- **University Certificates** – Helps in Issuing and verifying degrees securely.
- **Hackathon & Workshop Certs** – Can Publish and verify participation or achievement.
- **Govt or NGO Skill Certifications** – Provides trustable proof of skills without middlemen.
- **Employment Background Checks** – Fast, trusted, and direct certificate validation.

Drawbacks & Future Scope

1.Requires MetaMask Login

Currently, users need to install MetaMask to access blockchain features.

Plan: Integrating WalletConnect or social logins for a broader accessibility.

2. No Certificate Editor or Preview

Organizations can't preview or edit certificate details before upload.

Plan: To Add a certificate builder UI for real-time editing and preview.

3. No Mobile-Friendly UI

The interface is mainly optimized for desktop use right now.

Plan: To Use responsive design and test on mobile browsers.

4. No Certificate List View

There's no dashboard to view previously uploaded certificates.

Plan: Adding an admin/user dashboard to view and manage all uploaded records.

5. Manual Hash Input for Verification

Users must copy-paste hash to verify — not yet QR or scan-based.

Plan: To Add QR code generation and scanning for easier access.

Competitors, USP & Revenue Generation

Competitors :

- DigiLocker – Government platform for digital documents.
- TrueCert (private tools) – Blockchain-based certs but costly & limited to premium clients.
- Manual Processes – Still used by many institutions, prone to fraud and delays.

What Makes Us Different ?

- Fully decentralized using Web3 & Blockchain.
- Open to any verified organization, not just big players.
- Certificate data is stored using IPFS, making it tamper-proof and transparent.

Revenue Generation :

- Freemium Model: Free for small orgs; premium for extra features like dashboards, analytics.
- Onboarding Fees: Institutions pay once to register and verify.
- Storage Upsell: Extra charges for additional IPFS storage beyond free limit.
- API Access: Offer paid APIs for third-party integration (e.g. universities, job platforms).
- Digital Verification Service: Charge companies to verify candidate certificates quickly.

CODE MAVERICKS

EVENLY DISTRIBUTED

MILIND GARG : +91 9875248985
POORVI KULSHRESTHA : +91 8770613319
POOJA WANJARE : +91 9770083248
UTSAV KUMAWAT : +91 6267085737

Thank you