**Concept Note on**

**Block Chain**

**Submitted to**



[**www.ernet.in**](http://www.ernet.in/)

An Autonomous Scientific Society under

Ministry of Electronics & Information Technology (MeitY), Govt. of India

Contents

1. **ERNET India Profile ..................................................................................................................................... 4**
2. **ADVANTAGES OF PARTNERING WITH ERNET India ................................................................................... 5**

**4.1 The current scenario ............................................................................................................................................... 7**

# 5 details of solution ......................................................................................................................................... 9

**5.1 Key Highlights ........................................................................................................................................................... 9**

**5.2 The proposed platform core processes.......................................................................................................... 10**

**5.3 Smart Contracts in Issuance ............................................................................................................................... 11**

**5.4 Smart Contracts in Verification ......................................................................................................................... 11**

**5.5 Solution Architecture with the required infrastructure details and description: ......................... 12**

**5.6 Key Stakeholders & Their Roles ....................................................................................................................... 15**

**5.7 Key Considerations for Digital Certificate Issuance .................................................................................. 16**

**5.8 Interactions Between System Components & Stakeholders .................................................................. 16**

# 6. features of solution ....................................................................................................................................... 18

**6.1 Salient Features ...................................................................................................................................................... 18**

**6.2 Ease of Use ................................................................................................................................................................ 19**

1. **benefits .......................................................................................................................................................... 20**

**7.1 Benefits to Stakeholders ...................................................................................................................................... 20**

**9 Standards of Delivery ............................................................................................................................... 23**

# 10 PREREQUISITES, ASSUMPTIONS AND EXCLUSIONS ....................................................................... 23

**10.1 UGC/ERNET: ............................................................................................................................................................. 23**

**10.2 Universities: ............................................................................................................................................................. 23**

# 11 EXCLUSIONS………………………………………………………………………………………………………………..24

|  |  |
| --- | --- |
| **1** | **EXECUTIVE SUMMARY** |

# EXECUTIVE SUMMARY

As India advances towards becoming a $4 trillion economy, Technology is going to be the big charger as its citizens gear up to be globally accepted members of the 5th largest economy of the world. This is nation building at its best with the largest young work force striving for a better future, thus ensuring a better future for the country. Students form a large diaspora of this movement as they enter the job market armed with their degrees and skills. They are already adept at working with advanced technology. While pursuing their graduation or post-graduation, they are creating content on the Internet, coding, gaming, and being part of communities learning and disseminating information. I

The Education System in India is a big catalyst for this growth. The Education Sector, through the government and policy bodies does an incredible job in preparing students as future citizens of the country. The Colleges and Universities imparting this education have adopted technology at every turn, be it conducting examinations and issuance of degrees and certificates. This document adds a dimension of verification of the said certificates and credentials.

While all of the above is with good intent, there are still cracks in the system that is being misused by miscreants which is brining disrepute to the University / College and the whole Education System. Technology is the only way to mitigate any malicious attempt to disrupt this system. These degrees are used to seek employment in various sectors of the Industry vide matching the skill set to the Degree. It has been found that a particular Degree Holder never went to the college (s)he has provided proof of. This is discovered by the Employer during a Background Verification ( BGV) Process when the Agency approaches a particular University / College about an Alumnus. There is thus a need of a technology that allows for a document issuance and verification, in this case a Degree or Educational Credentials that allows a temper proof, decentralised and distributed system. Blockchain based technology answers to these requirements. Leading global institutions like the Massachusetts Institute of Technology (MIT) issued digital certificates using Blockchain technology in 2022.

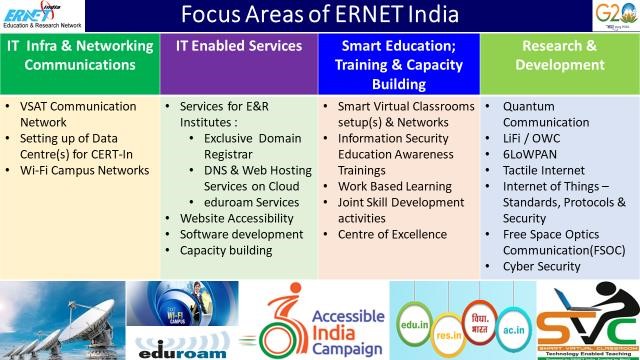
(Source: [https://www.hindustantimes.com/cities/pune-news/mit-issues-blockchain-powereddegree-certificates-to-2-212-students-101659030706105.html)](https://www.hindustantimes.com/cities/pune-news/mit-issues-blockchain-powered-degree-certificates-to-2-212-students-101659030706105.html)

|  |  |
| --- | --- |
| **2** | **ERNET INDIA PROFILE** |

ERNET India is a scientific autonomous organization under Ministry of Electronics and IT (MeitY) and its governing structure is as per guidelines of Govt. of India. Hon’ble MEIT is the chairman of its Governing Council and Secretary MeitY, is the chairman of its Executive Committee. Further, it implements the projects of central and States governments with the support of grant-in-aid.

ERNET India serves the mandate of Govt. of India to serve the academic and research institutions for captive use. It focuses on fulfilling the ICT requirements of academic and research institutions by providing consultancy, project management, training and other value added services such as domain registration, video conferencing as a service, CUG services, etc. ERNET India is serving more than a thousand of institutions in various sectors namely health, agriculture, higher education, schools and science & technology.

**ERNET India Services Portfolio**



|  |  |
| --- | --- |
| **3** | **ADVANTAGES OF PARTNERING WITH ERNET INDIA** |

▪ ERNET India status of being a not-for profit central government organization under the direct administrative control of Ministry of Electronics & IT, Government of India.

▪ ERNET India has the vast experience and domain Knowledge to cater to ICT needs of education community

▪ ERNET India is pioneer in providing IT/ICT solution to educational institutions across India and successfully delivered various project.

▪ ERNET India is exclusive registrar of the domain (ac.in, edu.in, res.in) and registered more than **17800 domains** to **educational institutes**. Under the domain services ERNET India is also providing the DNS Webhosting and VAS Services viz. **Website as service (WaaS)** and **Learning Management System as service (LMaaS).**

▪ ERNET India has more **than 6.5 Lakhs man-hours** of strong experience of establishing & operating **Smart Virtual Classroom (SVC) solution in 3279 schools and 54 DIETs** across the **09 states** of Assam, Sikkim, Tamil Nadu, Andhra Pradesh, Gujarat, Rajasthan, Haryana, Himachal Pradesh & Tripura.

▪ ERNET India ssuccessfully established and commissioned the **Smart Virtual Classroom in 75 schools and 4 DIETs of Sikkim and Assam** with the funding support of North Eastern Council (NEC).

▪ ERNET India successfully established **advanced Digital ICT infrastructure in 40 Schools of 8 North Eastern States (i.e. 5 schools in each North Eastern State)** by creating ecosystem for personalized adaptive learning using tools & techniques.

▪ ERNET India successfully established **WiFi-enabled campus network in North-Eastern Hill University (NEHU) at Shillong.**

▪ Successfully established and commissioned e-classroom Infrastructure in **6 Govt. Medical College of North East Region under National Medical College Network (NMCN).**

▪ ERNET India has successfully made **698 websites of 23 States/UTs of the country, accessible to Divyangjan as per WCAG 2.0 and GIGW**.

▪ ERNET India successfully **connected 13 colleges/universities with eduroam facility** exclusively provided by ERNET India to faculty, students/researchers so as to enable them roaming across various colleges/universities in India which are registered with ERNET for eduroam.

▪ With wide and varied past experience in executing different ICT projects, ERNET India has acquired necessary expertise, strength and technical resources to implement and manage large ICT based projects involving hardware/software integration for any service delivery on turnkey basis.

▪ ERNET India follows the GFR processes for achieving the nominal rates of services/solutions and focus on efficiency by prioritizing the completion of tasks within a timeframe and budget leading to quicker delivery of products or services.

|  |  |
| --- | --- |
| **4** | **CHALLENGES AND NEED OF SOLUTION** |
|  |  |
| 4.1 | THE CURRENT SCENARIO |

There are many of Government and Private Universities in India imparting higher education. These Universities are either run by Government or are by private education bodies / Trusts, though the accreditation as per Govt norms. All of these Institutions, deemed, private or government come under the purview of the policy guidelines issued by Government of India/UGC/state government higher education bodies. These universities cater to a huge demand of imparting higher education to a large young population of India. While it is a good sign that the centers for imparting higher education have increased in our country, it has alongside raised concerns over the veracity of the certificates being issued to candidates. . A bigger concern is the grades and marks in the certificates being issued. There is sometimes no correlation between the certificate a student is holding vis a vis the skill set(s) he possesses. Industry has discovered many times that a B.Tech certificate in Computer Science does not necessitate skills in Software Development or Computer Science.

There are various measures being undertaken by the government to ensure that the basic benchmarks are ensured but this issue is unresolved.. There is a demand from industry/employers as well that the authenticity of education and the certification be assured to avoid verification and cross checking. .

This scenario has produced a 2 fold challenge

* Issuance of Certificates based on marks and grades a Student has genuinely achieved.

* Authenticity of the Certificate should be verified through the working life of the certified.

As India embarks on digitization and the “Digital India’ program is taking strength, it is only imperative that the Educational Certificates be totally digitized and any reproduction in paper is restricted only by the authorised persons. This will further aid agencies who can digitally verify the certificates without physical verifications and emails.

Moreover, as a student moves out of a University armed with a degree, (s)he joins a company and embarks on a professional career spanning a few decades, the candidate will change jobs and places. (S)he will submit the educational credentials to his / her employer every time upon joining. These credentials are verified through various background verification agencies who either send an email or a person to visit the particular College / University to verify the authenticity of the student and the certificate, marks , specialization other such attributes.

A digital platform will facilitate online verification of these certificates almost instantly and will totally eliminate physical visits or visiting the institute.

The platform can be an end to end Certificate Issuance and Verification Engine for all students.

A Blockchain based system is ideally suited to provide a solution for the above. Blockchain as a technology works on

* Distributed Ledger Technology – All participants on the chain are working on a Distributed Ledger and its immutable record of transactions. With this shared ledger, transactions are recorded or issued only once, thus eliminating duplication. Any updation or change to the transaction will be done on consensus and all the stakeholders get notified of the same.

* Immutable Records – No participant can change or tamper with a document or a transaction without keeping the others informed. Any change must be recorded in the ledger and both transactions will be visible to all the participants

* Smart Contracts – In order to lay down certain rules or policies that everyone can follow and to increase speed, a set of rules called ‘ Smart Contracts ‘ is stored on the blockchain and run automatically. A smart contract can define the issuance of Certificates based on certain conditions being met like passing of exam and meeting the minimum criteria. These can be immutable once issued and will be the same for a particular student for the course of his life.

|  |  |
| --- | --- |
| **5** | **DETAILS OF SOLUTION** |

The Blockchain-Based Certificate Issuance & Verification Platform is a secure, template-driven system designed to issue certificates while ensuring authenticity and ownership through blockchain technology. Each certificate includes a **No-Touch QR Code**, enabling instant verification by scanning. The platform is designed to be extendable, opening the way for integration with third-party platforms like Digilocker. This will enable candidates to access their certificates seamlessly while maintaining full ownership and control over their data. The platform does not store raw data; instead, it retrieves information from issuing institutes on demand, making it a decentralized, trustdriven solution for academic credential verification.

|  |  |
| --- | --- |
| 5.1 | KEY HIGHLIGHTS |

* **1. SECURE & TAMPER-PROOF CERTIFICATE ISSUANCE**

The platform enables universities and educational institutions to issue certificates using a template-driven approach. Each certificate undergoes cryptographic hashing before being released to owners, ensuring that it remains unalterable and verifiable. By eliminating the possibility of forgery, the system guarantees the security and authenticity of all issued certificates.

* **2. BLOCKCHAIN-BACKED PROOF OF AUTHENTICITY**

To establish proof-of-authenticity and proof-of-ownership, the platform records the cryptographic hash of each certificate on the blockchain using smart contracts. This immutable ledger ensures that certificates cannot be tampered with and allows verification at any time without relying on a central authority.

* **3. INSTANT VERIFICATION WITH QR CODE & SMART CONTRACTS**

Each certificate is embedded with a No-Touch QR Code, which contains student identifiers, blockchain references, and a verification URL. When scanned, the platform retrieves the blockchain-registered certificate hash, recomputes the document hash, and instantly validates its authenticity. This trustless verification process ensures fast and secure credential validation without institutional involvement.

* **4. FRAUD PREVENTION & IMMUTABLE RECORD-KEEPING**

By leveraging blockchain’s immutability and transparency, the platform prevents fake or duplicated certificates. Since cryptographic proofs are permanently recorded, any tampering attempts are instantly detectable, preserving the credibility and integrity of issued credentials.

* **7. SCALABLE & AUTOMATED DIGITAL INFRASTRUCTURE**

With smart contract automation, the platform reduces manual intervention in both certificate issuance and verification. Its scalable architecture supports multiple institutions, ensuring efficient and standardized certificate management across diverse educational organizations.

This decentralized, trust-driven platform redefines how academic credentials are issued, verified, and managed— ensuring a secure, transparent, and candidate-controlled future for digital certification.

|  |  |
| --- | --- |
| 5.2 | THE PROPOSED PLATFORM CORE PROCESSES |

■ **1. ISSUANCE PROCESS**

The proposed platform will enable educational institutions to issue certificates through a template-driven system, ensuring consistency, security, and automation. Institutions will provide student-data via a secure API, which the platform will use to generate PDF certificates. Each certificate will undergo cryptographic hashing, with the resulting hash recorded on the blockchain via smart contracts to establish proof-of-authenticity.

Once the cryptographic proof is secured:

* The certificate will be issued to the candidate.
* The certificate hash and its identifiers will be stored on the blockchain. ● The candidate will be notified of certificate availability.

This blockchain-backed issuance process ensures that certificates are tamper-proof, verifiable, and owned solely by the candidate, reducing fraudulent claims and administrative inefficiencies.

■ **2. VERIFICATION PROCESS**

The platform will support instant and trustless verification using No-Touch QR Codes embedded within each certificate. These QR codes will contain student identifiers, blockchain references, and a verification URL, allowing verifiers (e.g., employers, universities, or government agencies) to quickly validate the certificate.

The verification process will function as follows:

* Upon scanning the QR code, the platform will retrieve the blockchain-registered certificate hash via a smart contract.
* The system will recompute the hash of the presented certificate and compare it with the stored hash.
* If the hashes match, the certificate is confirmed as authentic and unaltered.
* If the hashes do not match, the document is flagged as potentially tampered with, and additional verification steps may be triggered.

■ **3. OWNERSHIP AND DATA SOURCING**

The proposed platform is designed in such a way that the platform will not store raw certificate data. Instead, it will rely on a secure API-driven approach to retrieve required information on demand from the issuing institution.

For each issuer/institution there will be an “Issuer Client ” .Details of this can be found in section 5.5.3.

The ownership and data sourcing process includes:

* **Cryptographic Proofs on Blockchain** – Only certificate hashes and its identifiers will be recorded on the blockchain, ensuring privacy and security.
* **On-Demand Data Retrieval** – When a verifier requires additional certificate details, the platform will request explicit candidate consent before retrieving data from the issuing institution.
* **Decentralized Verification** – Verifiers can authenticate certificates without direct interaction with the issuing institution, relying on immutable blockchain records for instant trust.

By ensuring that candidates control access to their certificates, the platform promotes a privacy-first, decentralized verification system while maintaining the integrity and authenticity of issued documents.

|  |  |
| --- | --- |
| 5.3 | SMART CONTRACTS IN ISSUANCE |

In the proposed platform, smart contracts will play a crucial role in ensuring secure, transparent, and automated certificate issuance. The following steps outline their involvement:

* **1. CERTIFICATE HASHING & SMART CONTRACT INVOCATION**
* Once a certificate is generated using the template-driven approach, the platform will compute a cryptographic hash of the data in the document (e.g., using SHA-256).
* This hash, along with its identifiers, will be sent to a smart contract deployed on the blockchain.
* **2. SMART CONTRACT EXECUTION & BLOCKCHAIN ANCHORING**
* The smart contract will validate the incoming data and store the certificate hash on the blockchain.
* The contract will ensure that duplicate or tampered certificates cannot be registered, enforcing integrity.
* Each transaction (certificate issuance) will be logged immutably, ensuring proof-of-existence and proofof-authenticity.
* **3. ISSUANCE CONFIRMATION & CANDIDATE NOTIFICATION**
* Once the hash is stored on the blockchain, the smart contract will generate a unique blockchain transaction ID .
* The platform will be updated with the transaction ID and the certificate record to generate a No-Touch QR Code, embedding blockchain reference details.
* The smart contract can also trigger an event notification, signaling the successful issuance of the certificate with a timestamp.

|  |  |
| --- | --- |
| 5.4 | SMART CONTRACTS IN VERIFICATION |

The proposed platform will leverage smart contracts to provide decentralized, tamper-proof, and privacypreserving certificate verification. Smart contracts will ensure that certificates can be authenticated without direct involvement from the issuing institution, except in cases where additional data validation is required.

* **VERIFICATION FLOW USING SMART CONTRACTS**

1. **QR Code-Based Initial Verification** 
   * When a verifier (e.g., employer or university) scans the No-Touch QR Code embedded in the certificate, the platform extracts the blockchain transaction ID.
   * The platform queries the smart contract to retrieve the original certificate hash and its identifiers and compares it with currently generated certificate hash.
   * If the hashes match, the platform confirms the existence of the certificate.
2. **Dynamic Data Sourcing for Full Verification** *(Requires Candidate Consent)*

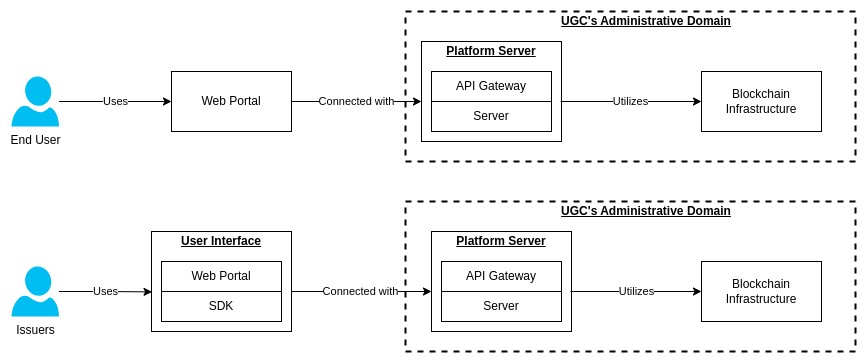
* If the verifier requires full certificate details (e.g., student name, grades, or program duration), the platform will request explicit candidate consent before proceeding.
* Upon candidate approval, the platform will securely retrieve the certificate details from the issuing institution via a secure API.
* The retrieved data will then be used to recompute the expected hash and confirm authenticity.
* Once verified, the full details will be displayed to the verifier.

**3. Fraud Detection & Alerting**

* + If the presented certificate’s computed hash does not match the blockchain-stored hash, the platform will flag the document as potentially tampered with.
  + If further validation is needed, the platform can alert the issuing institution and request manual verification.

|  |  |
| --- | --- |
| 5.5 | SOLUTION ARCHITECTURE WITH THE REQUIRED INFRASTRUCTURE DETAILS AND DESCRIPTION: |

The proposed platform is designed to securely issue, store, and verify academic and professional certificates using blockchain technology. The architecture is structured to ensure seamless integration with issuing institutions, candidate-centric ownership, and decentralized verification.

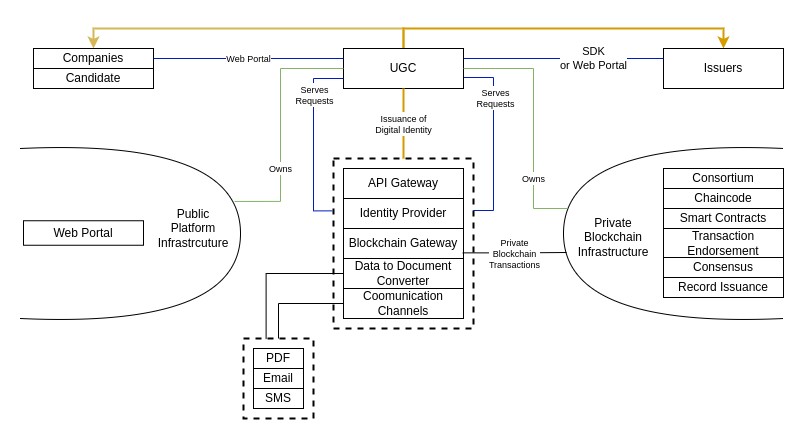


**Figure 1: Users using the platform**

■ **5.5.1. PUBLIC PORTAL (WEB & MOBILE APP)**

The Public Portal serves as the primary interface for candidates and verifiers to access, manage, and verify certificates.

* + **Candidate Access:** Allows students to view issued certificates, grant verification permissions, and manage document sharing.
  + **Verification Portal:** Enables third parties (employers, universities, government agencies) to scan and validate certificates instantly using blockchain-backed verification.
  + **Secure Authentication:** Implements identity verification mechanisms leveraging **Digital Identities** (e.g. user-id, password) to authenticate each request securely.
  + **Ease of Access:** Integrates a **No-Touch QR Code System** for effortless certificate retrieval and sharing.



**Figure - 3: System Diagram - All the components together**

■ **5.5.2. PLATFORM SERVER**

The Platform Server acts as the core processing unit, handling interactions between institutions, candidates, verifiers, and the blockchain infrastructure. It comprises several sub-components:

* + **5.5.2.1 API GATEWAY**
  + Central entry point for all system interactions.
  + Routes requests between the Public Portal, Issuer Client, and Blockchain Infrastructure.
  + Ensures secure communication through encryption and authentication.
  + **5.5.2.2 IDENTITY PROVIDER**
  + Manages user authentication and role-based access control (RBAC).
  + Supports multi-factor authentication (MFA) and OAuth-based authorization.
  + Leverages Digital Identities to verify and authenticate certificate issuers and recipients.
  + **5.5.2.3 BLOCKCHAIN GATEWAY**
  + Interfaces with the blockchain infrastructure for certificate issuance and verification.
  + Facilitates transaction endorsement, smart contract execution, and consensus processes. ● Ensures certificate authenticity by storing cryptographic proofs on the blockchain.
  + **5.5.2.4 DATA-TO-DOCUMENT CONVERTER**
  + Converts structured data received from institutions into PDF certificates.
  + Attaches a No-Touch QR Code for instant verification and seamless access.
  + Supports certificate template-based printing, ensuring consistent document generation.
  + **5.5.2.5 COMMUNICATION CHANNELS**
  + Notifies candidates of certificate issuance via email, SMS, and push notifications.
  + Sends alerts to institutions and verifiers regarding verification requests.
  + Uses secured communication channels to maintain data integrity and prevent unauthorized access.

■ **5.5.3 ISSUER PORTAL (ISSUER CLIENT)**

The Issuer Client is a web-based portal hosted within the environment of the issuing institution. It acts as a bridge between the institution and the Platform Server.

* + **Data Sourcing:** The Platform Server queries the Issuer Client to retrieve candidate and certificate data on demand.
  + **Request Processing:** Institutions can initiate certificate issuance and other processing activities.
  + **Access Control:** Ensures only authorized institutional personnel can manage certificate issuance.
  + **Secure Transactions:** Uses digital identities (public-private key infrastructure) to sign transactions (e.g.

http requests), ensuring authenticity.

■ **5.6.4 BLOCKCHAIN INFRASTRUCTURE**

The platform leverages a permissioned/private blockchain consortium to ensure the authenticity, integrity, and non-repudiation of issued certificates.

* + **5.5.4.1 PERMISSIONED/PRIVATE BLOCKCHAIN**
  + Designed for controlled access, ensuring only approved institutions and verifiers can interact with the ledger.
  + Provides an immutable record of certificate issuance and verification transactions.
  + **5.5.4.2 CONSORTIUM MODEL**
  + A governance model that allows multiple educational institutions to participate in the blockchain network.
  + Ensures collective decision-making and decentralized trust.
  + **5.5.4.3 CHAINCODE & SMART CONTRACTS**
  + Defines the rules for certificate issuance, ownership transfer, and verification.
  + Automates trustless validation of certificates using cryptographic hashes.
  + Secures authentic data by ensuring only verified transactions are recorded.
  + **5.5.4.4 TRANSACTION ENDORSEMENT & CONSENSUS**
  + Uses endorsement policies to validate transactions before they are committed to the ledger.
  + Ensures consensus is achieved among participating institutions before certificate data is stored on-chain.
  + **5.5.4.5 DOCUMENT ISSUANCE PROCESS**
  + Generates a cryptographic hash of each certificate and records it on the blockchain.
  + Provides proof-of-authenticity, proof-of-existence, and proof-of-ownership.
  + Enables tamper-proof verification through blockchain-registered hashes.
  + Facilitates on-demand document retrieval via secure APIs, ensuring privacy and efficiency.

This architecture ensures a seamless, secure, and decentralized approach to certificate issuance and verification. By leveraging blockchain technology, the platform guarantees the integrity of academic credentials while enabling institutions to streamline their certification processes.

Additionally, the platform:

* + Provides **ease of access** through web portals, mobile apps, and QR-based verification.
  + Uses **digital identities** to authenticate transactions and ensure data integrity.
  + Implements **secured communication channels** for safe interactions.
  + Ensures **authentic data and document printing** via structured templates.

The inclusion of the Issuer Client ensures institutions retain control over data, while the Public Portal empowers candidates and verifiers with instant access to authentic records. The result is a trust-driven system that eliminates fraud, reduces administrative overhead, and enhances transparency.

|  |  |
| --- | --- |
| 5.6 | KEY STAKEHOLDERS & THEIR ROLES |

|  |  |
| --- | --- |
| Stakeholder | Key Role in the System |
| Educational Institutions (Issuers) | Issue certificates, manage student data, approve verification requests. |
| Candidates (Students, Alumni) | Receive certificates, share with verifiers, provide consent for data access. |
| Verifiers (Employers, Universities, Government Agencies) | Verify authenticity of certificates using blockchain-backed records. |
| Blockchain Network Participants | Maintain the distributed ledger, validate transactions, endorse certificate issuance. |

|  |  |
| --- | --- |
| 5.7 | KEY CONSIDERATIONS FOR DIGITAL CERTIFICATE ISSUANCE |

Figure-2 illustrates the relationship between physical entities (e.g., UGC, Universities, Candidates, Employers) and digital components (e.g., Web Portal, Blockchain, Digital Identity, Secure Communication). The figure highlights how the platform ensures seamless certificate issuance, verification, and access through interconnected digital and physical entities. It showcases how data flows securely between stakeholders, ensuring authenticity, ease of access, and trustless verification.

Key aspects represented in Figure-2:

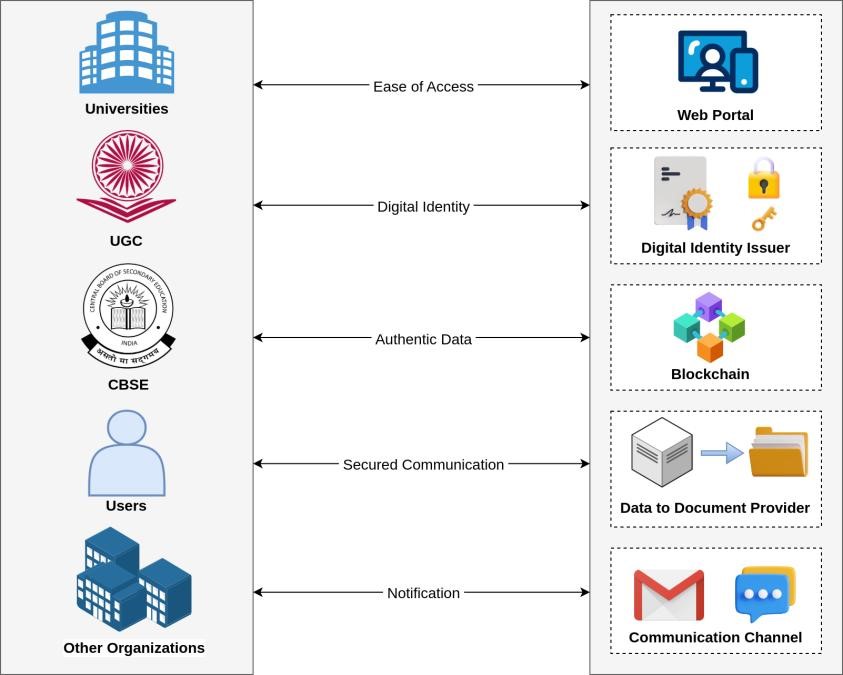
* + Web Portal & Mobile App: Acts as the primary interface for candidates and verifiers to interact with digital certificates.
  + Blockchain Infrastructure: Ensures certificate authenticity by securely storing cryptographic hashes.
  + Digital Identity Provider: Facilitates secure authentication for institutions, candidates, and verifiers.
  + Issuer Portal (Issuer Client): Enables institutions to issue and manage certificates while ensuring data privacy.
  + No-Touch QR Code System: Embeds blockchain references into certificates for instant verification.
  + Secured Communication Channels: Ensure data integrity when retrieving records from issuing institutions.

Figure - 2: Solution Key-Consideration

* + Decentralized Trust Model: Ensures that verification does not require direct issuer involvement, reducing administrative overhead.

|  |  |
| --- | --- |
| 5.8 | INTERACTIONS BETWEEN SYSTEM COMPONENTS & STAKEHOLDERS |

The platform architecture ensures seamless interaction between key stakeholders (e.g., educational institutions, candidates, verifiers, employers) and digital components (e.g., Web Portal, Blockchain Infrastructure, Digital Identity Provider). These interactions are structured to ensure secure certificate issuance, verification, and management while maintaining trust, transparency, and efficiency.

* + **5.8.1 CERTIFICATE ISSUANCE PROCESS**

(Interaction: Issuer → Platform Server → Blockchain → Candidate)

* + The Issuer Client submits student data to the Platform Server via a secure API.
  + The Data-to-Document Converter generates a digitally signed PDF certificate.
  + The Blockchain Gateway computes the certificate’s cryptographic hash and records it on the Blockchain Infrastructure.
  + The Platform Server issues the certificate to the candidate via the Public Portal (Web & Mobile App). ● A notification is sent to the candidate.

Outcome: A tamper-proof, verifiable digital certificate is issued and made accessible to the candidate.

* + **5.8.2 CERTIFICATE VERIFICATION PROCESS**

(Interaction: Verifier → Public Portal → Blockchain → Candidate (if needed) → Issuer (if needed))

* + The Verifier scans the No-Touch QR Code embedded in the certificate.
  + The Public Portal retrieves the stored certificate hash from the Blockchain Infrastructure.
  + The system recomputes the certificate hash and compares it with the stored hash.
  + If the hashes match, the certificate is confirmed as authentic.
  + If a verifier requires additional details, the system requests candidate consent. ● Upon approval, the Issuer Client provides the required data securely via API.

Outcome: Instant, trustless verification without issuer intervention, unless additional consent-based verification is required.

* + **5.8.3 OWNERSHIP & CONSENT-BASED DATA ACCESS**

(Interaction: Candidate → Verifier → Public Portal → Issuer Client → Platform Server)

* + Candidates own their certificates and control access to additional data.
  + If a verifier requests more details, the Public Portal notifies the candidate.
  + The candidate grants or denies consent via the platform.
  + If approved, the Platform Server requests additional data from the Issuer Client. ● The Issuer Client fetches the data securely and provides it to the verifier.

Outcome: A privacy-first, candidate-controlled approach to verification, reducing the risk of unauthorized data access.

* + **5.8.4 SECURE COMMUNICATION & NOTIFICATIONS**

(Interaction: Platform Server → Candidates, Issuers, Verifiers, Third-Party Services)

* + The Communication Channels send real-time updates via SMS, email, and push notifications.
  + Candidates receive alerts when certificates are issued, accessed, or verified.
  + Issuers are notified when data access requests require their intervention.
  + Secure API-driven communication ensures that no sensitive data is exposed.

Outcome: Transparent, real-time updates for all stakeholders while ensuring data security.

**At a glance**

|  |  |  |  |
| --- | --- | --- | --- |
| **Interaction** | **Stakeholders Involved** | **System Components Involved** | **Outcome** |
| Certificate Issuance | Issuer → Candidate → Blockchain | Issuer Client, Platform  Server, Blockchain  Gateway, Public Portal | Authentic certificate issued to candidate, blockchain-proof stored. |
| Certificate Verification | Verifier → Blockchain → Candidate | Public Portal, Blockchain Gateway, Smart Contracts | Instant verification with tamper-proof records. |
| Consent-Based  Verification | Verifier → Candidate → Issuer | Public Portal, Issuer  Client, Platform Server | Privacy-centric, secure data retrieval only when approved. |
| Secure Notifications | Platform Server → Stakeholders | Communication Channels, Identity Provider | Real-time alerts and updates on issuance, verification, and access. |

**6. FEATURES OF SOLUTION**

○

Based on the need of a solution, technology is the answer. A digital platform that can provide a seamless, tamper proof and decentralised environment is best suited for issuing certificates and ensuring its authenticity because of the platform’s nature of immutability.

A decentralized Blockchain based PLatform specifically designed and developed for the Agency ( UGC / CBSE / ERNET) will have all the features to be perfect solution.

|  |  |
| --- | --- |
| 6.1 | SALIENT FEATURES |

***Issuance***

* Issuers can upload the certificate data or push the data to the platform using API. The list of credentials pushed are displayed on the UI for the Issuers. The cryptographic hash is created for every certificate and stored in the Blockchain layer.

* Once uploaded the candidates can claim the certificates on the Platform as they have digital proof of existence of their certificate details using blockchain technology.

* The generated proof of the certificate is immutable.

***Verification***

* Verifiers can verify a certificate as a Guest User or as a Permissioned User. As a Guest User or a permissioned user, a restricted view is available and every time a verification is requested by a consent OTP is sent to the document owner. The platform is GDPR compliant.

* Admin Panel for UGC/Universities to onboard issuers (Universities & Colleges).

* Platform has a secure mechanism to connect with APIs.

* A fee may also be charged for every verification by incorporating a payment gateway (If this feature is required we can do it).

|  |  |
| --- | --- |
| 6.2 | EASE OF USE |

* Certificate sharing is as simple as sharing a URL.

* GDPR Compliant

* Consent of the Certificate Owner is obtained

* There is no need to print out any certificates

* API Integration with Digilocker can also be provided as per need.

|  |  |
| --- | --- |
| **7** | **BENEFITS** |
|  |  |
| 7.1 | BENEFITS TO STAKEHOLDERS |

The innovative project once implemented shall be used by all the involved stakeholders starting from UGC/CBSE to candidates. The envisaged usages/benefits to the end user(s) are described as under:

# UGC/ERNET

* End to end visibility on the Certificate issuance process.
* Ability to address any malpractices in the system.
* Complete transparency of the process and authenticity of the certificates are guaranteed.

creating a trusted network of universities, colleges and candidates.

# Universities

* Eliminate the need to issue paper certificates.
* Verification of certificates is done instantly via the link shared by certificate recipient.
* Impossible to produce counterfeit certificates.

# ERNET

* Can collaborate and jointly publish credentials on the shared data layer to ensure authenticity.
* Eliminate the need to issue paper certificates.
* Impossible to produce counterfeit certificates.

# CANDIDATES

* Certificate sharing is as simple as sharing a URL Data stored on a shared data layer is encrypted, hence only the certificate holders can see and share this data as they wish.
* The solution is GDPR compliant.

# VERIFICATION COMPANIES

* Companies are sure that the certificates are genuine, without the hassles of spending many hours and money validating all the prospective employees’ diplomas and their work experiences.
* Digitally issued certificates are stored on a public (or private) shared data layer, hence there is a guarantee that data stored is immutable and cannot be tampered with. Also, since it’s decentralised, there is no signle point of failure

|  |  |
| --- | --- |
| **8** | **BILL OF MATERIAL** |

The following table provides the list of command-and-control center infrastructure elements including hardware and software at the Command-and-control Center, location will be identified in consultation with the University.

|  |  |
| --- | --- |
|  | **Infrastructure Requirement** |
| **A** | **Bandwidth** |
| 1 | Cloud Infrastructure |
| **B** | **Permissioned/Private Blockchain Network Infrastructure** |
| 1 | VM for Development Environment |
| 2 | VM for QA, UAT Environment |
| 3 | VM For Production Environment |
| 4 | Kubernetes |
| **C** | **Web Portal, Identity Provider, Data to Document Converter** |
| 1 | VM for Development Env |
| 2 | VM for QA, UAT Env |
| 3 | VM For Production Environment |
| 4 | SMTP |
| 9 | SMS Gateway |
| **D** | **Development** |
| 1 | Git Repository |
| 2 | CI/CD Pipelines |

1. **STANDARDS OF DELIVERY**

The platform will follow Agile methodology to enable iterative development, continuous feedback, and adaptability. Built on a cloud-based infrastructure, it will integrate hardware and software configurations to ensure scalability, security, and performance. Security and compliance will be maintained through encryption, authentication mechanisms, and blockchain-based validation to protect data integrity and trust. This approach will support reliability, performance, and a smooth user experience while allowing flexibility for future improvements.

1. **PREREQUISITES, ASSUMPTIONS AND EXCLUSIONS**

**Prerequisites:**

|  |  |
| --- | --- |
| 10.1 | UGC/ERNET: |

* + To recommend the Universities with whom a PoC implementation can be done
  + To provide space for hosting the platform
  + To set out the success criteria of the PoC
  + Coordination with Universities and affiliated colleges.
  + Nomination of a SPOC with complete understanding of the Business logic **●** To conduct acceptance testing of the implemented solution.

|  |  |
| --- | --- |
| 10.2 | UNIVERSITIES: |

* + To provide us an understanding of the existing process for certificate issuance and verification
  + To provide the data points for building the APIs.
  + To provide support in installing and placing the compatible hardware and software required
  + To conduct acceptance testing of the implemented solution.

1. **EXCLUSIONS:** 
   * The concept note does not include hardware software sizing. This will be based on the design of the platform and the number of certificates being issues, the number of VM instances etc.
   * The Concept note does not cover any commercials, the same can be provided based on the sizing and number of certificates issued / verified. A POC can be conducted to ascertain the same.

- ------------------------------------------------- xxxxx-------------------------------------------------------