Blockchain Based Certificate Issuance and Verification System SmartCertify

Sufiyan Ahmad[1], Anuj Kumar[2], Shalini Singh[3]

[1,2,3]Department of Information Technology, Babasaheb Bhimrao Ambedkar Central University, Lucknow, India

DOI: https://doi.org/10.51584/IJRIAS.2026.11050093

Received: 15 May 2026; Accepted: 20 May 2026; Published: 02 June 2026

ABSTRACT

Modern digital era passing out very tough time due to cybercriminal activity, fraud etc. In this situation financial, reputation, and time losses is common concern. According to time of India news in case of the Manav Bharti University of Himachal Pradesh, where 36,000 fake degrees were sold, & the 2026 Prayagraj Pharmacy Scam incidents such as these have suffers free trust. So, this issue demanded to protect sensitive information and their secure management. Currently block chain is in prevalence for security due to its characteristic that have capability to reduce cybercriminal activity and effective management. In reality, our traditional education system is currently is facing of a big problem like increasing difficulty to verify the authenticity of academic degrees. Main reason behind problem is the education database systems which is in centralize based and all data is stored in the single location. So, this make possibility to hacking, and these systems also incline to be quite slow. So, to fight this situation in this paper present a block chain-based solution named "SmartCertify". It controls by smart contracts to eliminate any scope for fake activity. Basically, in this includes a "Rules-Based Governance" model, where regulatory bodies such as the UGC pre-configure seat limits directly onto the blockchain. If university attempts to fraud even single certificate beyond its allocated limit, the block chain will immediately block the transaction. For system security used cryptographic chaining tool, where every new certificate will cryptographically link to previous one. If anyone try to attempt to tamper with past records using tools like photoshop, complete chain will be broken, and fraud be instantly detected. This entire process operates on local "Ganache" blockchain, confirms complete transparency and security.

Keywords—Blockchain, Immutability, SmartCertify, Smart Contracts, Seat Limit Enforcement, SHA-256.

INTRODUCTION

Today's digital era, demanded the trade in fake marksheets and degrees is spreading with equal speed and proper security of confidential Information. Because regularly news indicates how individuals buying "Doctor/Engineer" degrees instantly. Some big cases like Manav Bharti University and Prayagraj pharmacy scam, where 36,000 fraudulent degrees were sold. This situation is like to milkman diluting pure milk with water. That becomes impossible for you to distinguish between the genuine thing and the fake. SmartCertify is a digital platform that forces Blockchain technology to confirm that once a degree is issued, it can neither be altered nor deleted by anyone. Under the current system, companies are often forced to make repeated visits universities for verification purposes a process that can take weeks, whereas this system renders entire verification process instantaneous. Its most distinctive feature is its "Rules-Based Governance" Imagine, for instance, a college with an intake capacity of only 100 seats. This software would simply prevent the issuance of a 101st degree. It well binds university's hands, certifying that they cannot issues degrees beyond their allowed capacity. This system employs cryptographic chaining, each new degree issues is digitally linked to the previous one, forming a nonstop digital chain. If user try to attempt to modify even a single name within an old record using software like photoshop, or other editing tools, whole chain will break, and act of fake will be detected immediately. Simply put, this technology to serves as digital guardian, within education sector, easily integrating both transparency and security. The rest of the paper follows a sequence of: Section II reviews

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

related work, Section III describes the methodology as need for study, Section IV proposed work, Section V system design, VI for the results and discussion, Section VII for results & conclusion and, Section VIII lists the overall paper.

LITERATURE REVIEW

The SmartCertify starts with a serious look on the current educational site, which is currently facing a huge trust issue, because real world evidence suggests that the traditional way of issuing and verifying certificates is no longer secure. Huge no of scams, such as the Manav Bharti University [1] case where 36,000 fake degrees were sold, and the recent encounter of an association in Delhi issuing over 5,000 forged documents [2], show that our current systems are easily hacked or misused and this problem isn't controlled to general degrees, even the healthcare sector has been hit, as seen in the Prayagraj racket case, where 7,000 and above fake B-Pharma certificates were put into circulation [3]. These activities happen because universities currently run in a black box where there is no transparency regarding their actual student capacity against the number of certificates they actually print. This is where the technical development of Blockchain comes into play on the basis of our system built on the peer-to-peer principles first introduced by Satoshi Nakamoto (2008) [23][25] and the architectural bases clear by Zheng et al. (2017) [26], which claim that decentralization is the only way for reach true immutability. And nowadays moving from concept to practical, researchers [5][7] similar as Rahmah et al. (2026) [4][6][9] have already been mixing smart contracts for digital certification in vocational higher education to confirm validity [8][10]. Similarly, Shaikh et al. (2026) [15][16][17] strategic of tamper proof decentralized framework just for educational documents to break illegal data changes. But, even with these improvements, an important research gap remains. Most traditional models, as well as the European EBSI standards/TRON based structures [12][14] discovered by Andrade and Amate (2025) [11][13], focus totally on making the document secure after it allotted and the regularly ignorance the source cause, the lack of control over the number of issuances, while current literature discusses, how to verify, it stays silent on how to prevent extra issuance.

Need For Study

Nowadays, the market suffers with fake degrees, causing public trust issues in the education system. For instance, the Manav Bharti University scam involved the sale of over 36,000 fake degrees. Our current system has 'centralized' means all data is stored in a single location making it extremely easy to hack or alter through internal collusion. The most significant problem that universities often surreptitiously issue degrees far beyond their actual capacity operating as 'black box' without anybody on the outside presence any wisher.

Furthermore, when a company attempts to verify an individual's degree, it faces wait of several weeks due to the sluggish nature of the verification process.

So, we require a system like SmartCertify that operates on the principles of 'rules-based governance.' Such system would not only defence data but also completely remove the root problem of the degree over-issuance.

Table 1: Existing vs Proposed System

Feature	**Traditional System**	**SmartCertify (Proposed)**
Data Security	Centralized Database (Low security, vulnerable to hacking)	Blockchain-based Ledger (High security, immutable records)
Verification Speed	Manual process involving third parties (Takes days/weeks)	Automated and Decentralized (Instant verification in seconds)
Administrative Control	No real-time seat or issuance control	Rules-Based Governance (Strict seat limits via Smart Contracts)

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Transparency	Closed system with limited access to audit logs	Publicly verifiable audit trail for every transaction
Operational Cost	High (Due to manual labour and third-party verification)	Low (Automated process with no intermediaries)

Proposed Work

The primary objective of paper is to completely remove fraud and manual delays over a use blockchain technology. Where, employed cryptographic chaining method where every certificate possesses its own unique digital fingerprint or hash.

Interestingly, each new block securely embeds the hash of the preceding block within itself, thereby forming a strong chain. Should anyone will attempt to tamper to historical record using photoshop or any other tool, then the entire chain will be immediately register as broken.

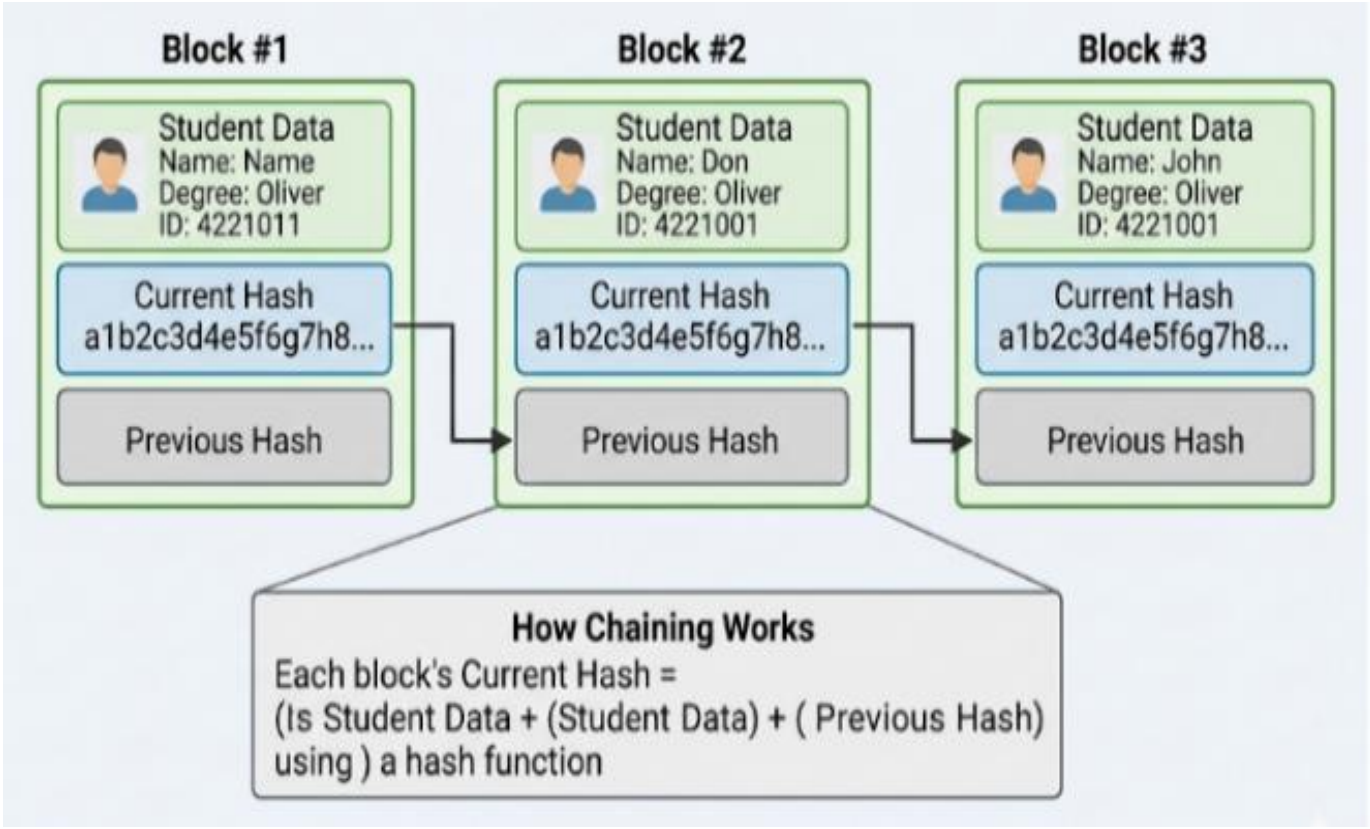
Additionally, we empowering to regulatory bodies, i.e. UGC, with authority that establish seat limits in system.

For instance, if specific course capacity of 100 seats, blockchain will simply refuse to authorize issuance of a 101st certificate.

This entire structure of system across 3 separate layers are following:

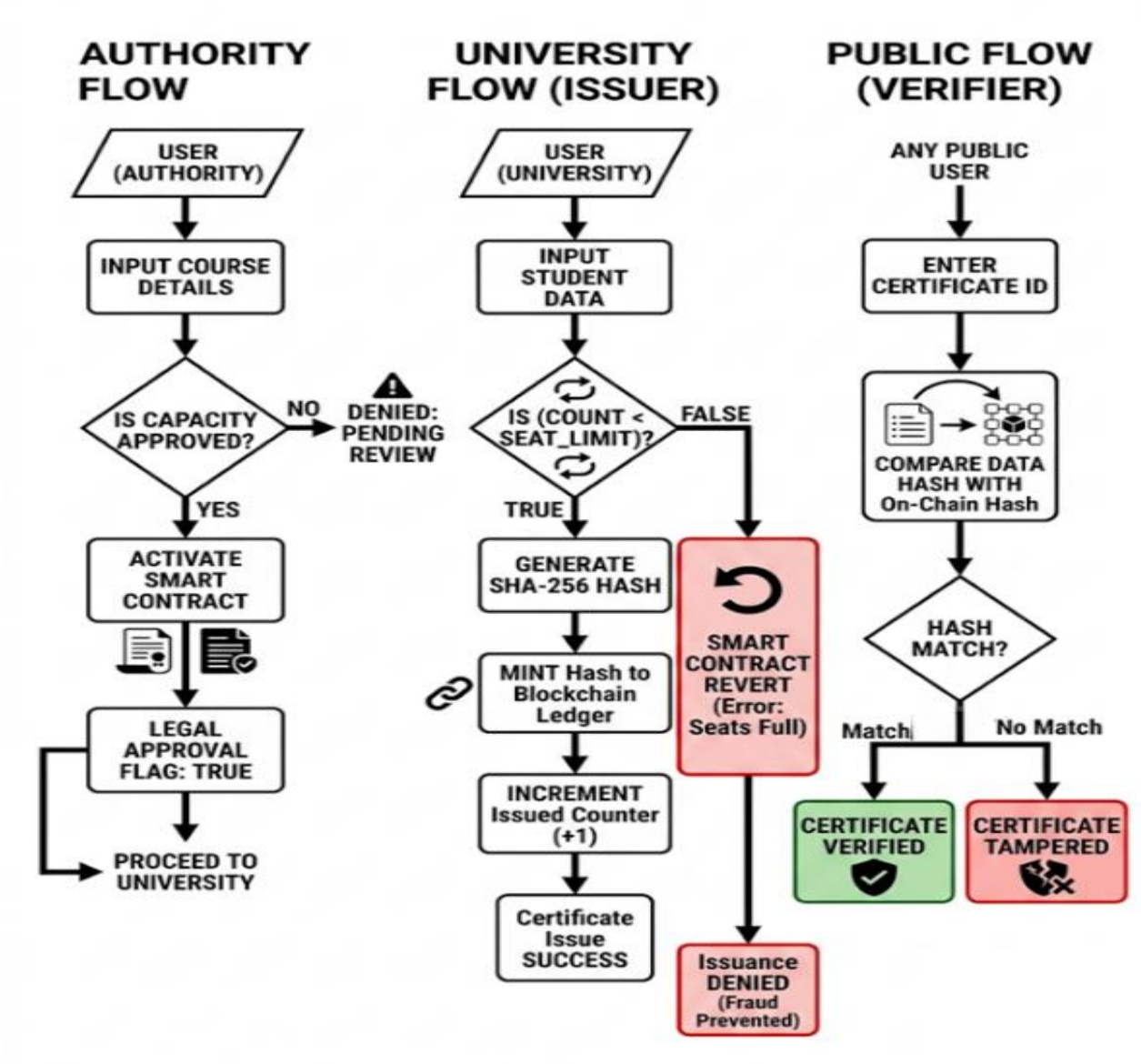
1. Python Tkinter for the frontend,
2. Solidity Smart Contracts for the underlying logic, and
3. The Ganache blockchain for data storage.

Figure 1: Link-by-Link Chaining



ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Figure 2: Logic Workflow Diagram



System Design

The technical architecture of SmartCertify is in very simple. We can imagine this with drawing an analogy to way of school or an office operates. Here, system divides in 3 main parts:

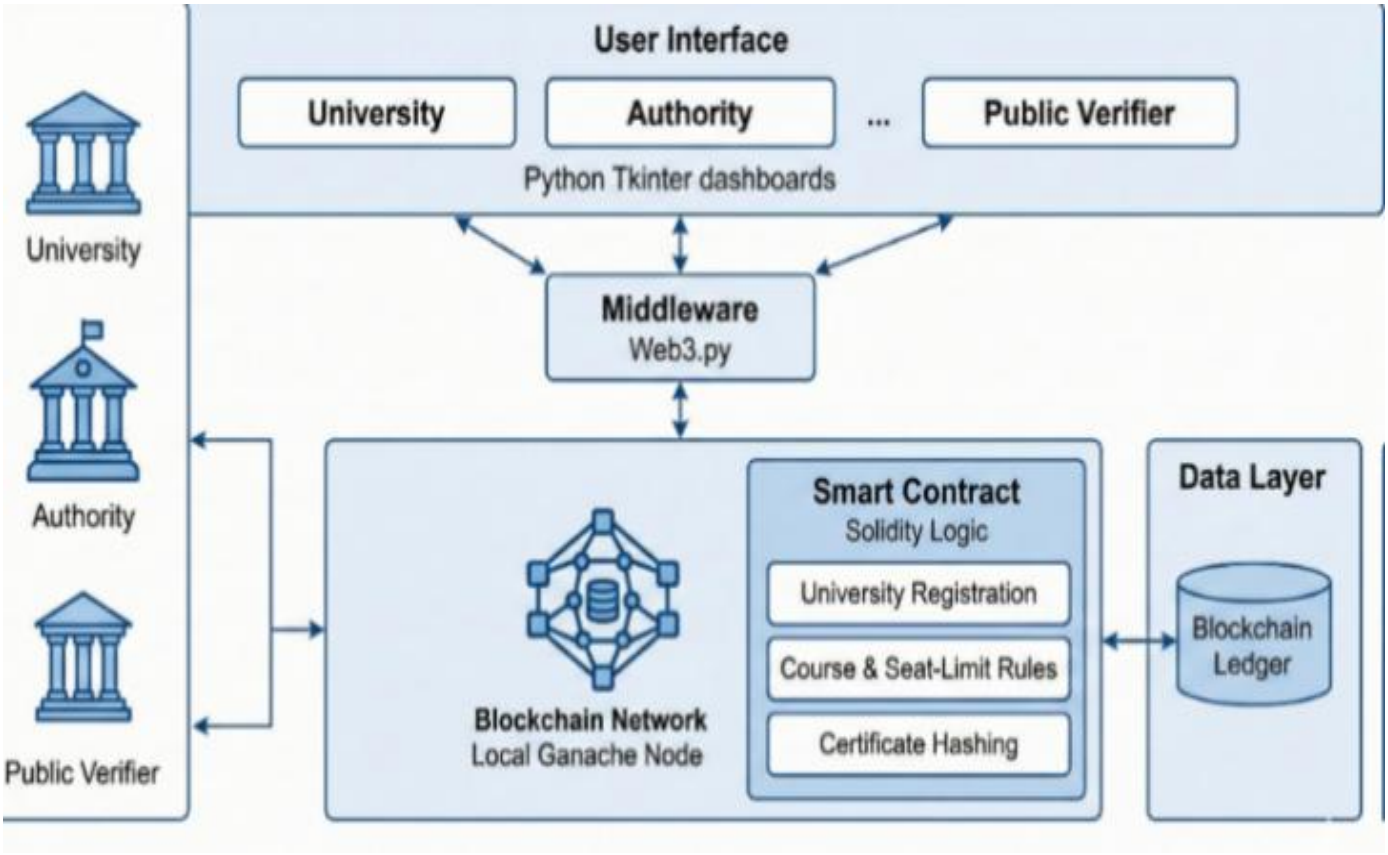
1. **Presentation Layer (Frontend):** This layer of the system, is used by user. It has built using Python & Tkinter. It is greatest advantage is that universities and administrators are do not need to study coding order to operate system. It provides a straightforward and user-friendly interface, allowing data entry and verification tasks to be performed without any technical 3problems.

2. **Logic Layer (Rule book):** This is to serves brain of whole system, making all critical decisions. It driven by smart contracts written in solidity programming language. This is layer which enforces specific rules, such as setting limits on number of certificates issued and is performing hashing of certificates. If any rule effected like for instance & issuing more certificates than prescribed limit, this layer immediately halts to operation.

3. **Data Layer (Storage):** In this layer all data and all transaction records are securely stored on the or for perpetuity. Ganache blockchain utilized for maintaining all permanent records, interpreting system hack-proof and immutable. Additionally, JSON files are of employed to facilitate quick and easy access to as a local data. This helps to maintains of the overall speed and efficiency of the system.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Figure 3: High level Architecture of SmartCertify



Draw the all these horizontal label arrows:

- University → Authority: Request Course & Seat-Limit Approval.
- Authority → Blockchain: Send Transaction: Approve Seats (e.g., 60).
- Blockchain → Authority: Confirm Rule Stored.
- University → Blockchain: Request Issuance (Student A, M.Sc IT).
- Blockchain → Blockchain (Self-check): Check Logic: Remaining Seats > 0?
- Blockchain → University: Confirm Issue: Return Trxn Hash & Block No.

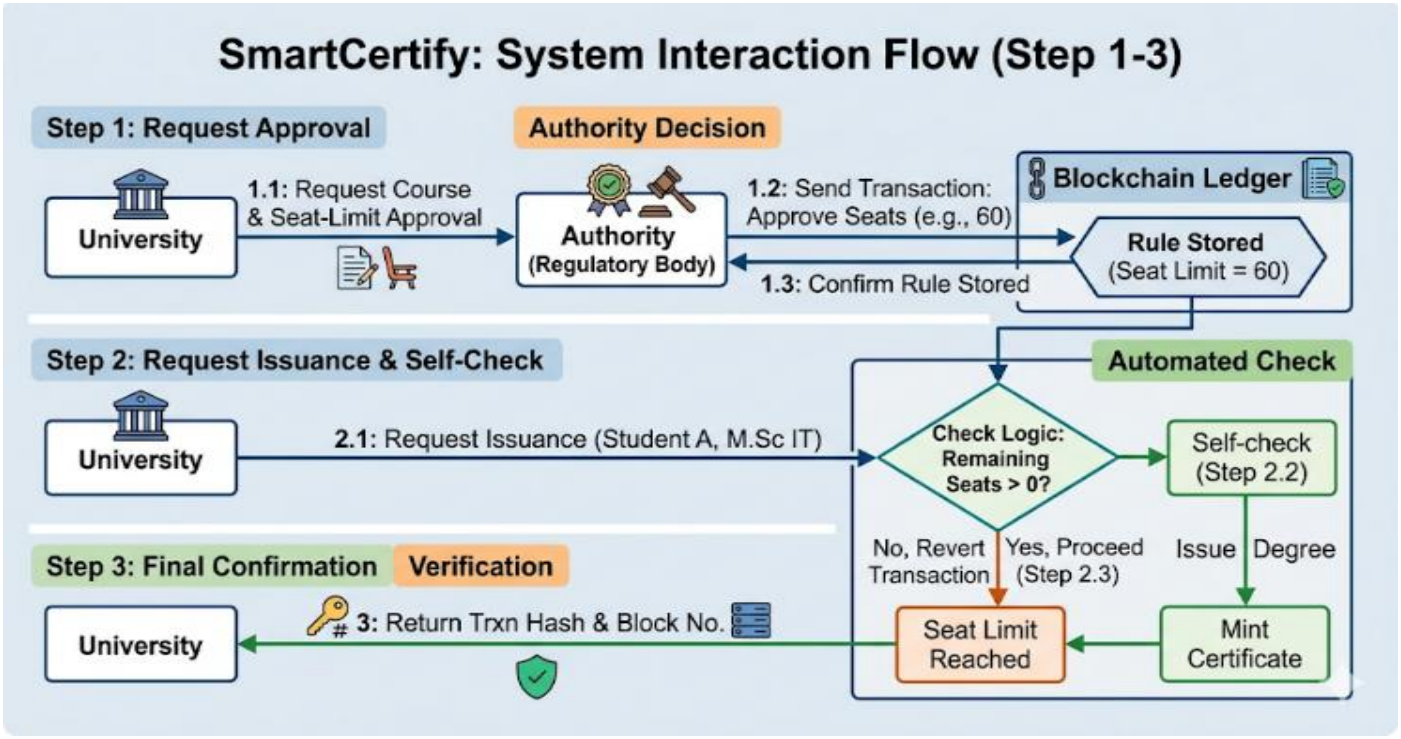
Module Description

This entire system is operated in 3 main parts:

1. Authority Module, which institutions are like UGC operate to register to universities and regulate according to their seat capacity.
2. University Module comes into play & once approval granted, then universities have permission to their limited no. of certificates issues, with system automatically tracks seat count.
3. Finally, Public Verification Module functioning their search tool feature. Here, if any student or company can simply enter their certificate ID to verify if exist then decide a degree authentic or not & then gives a popup alert.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue V May 2026

Figure 4: Module Workflow Diagram



RESULT AND DISCUSSION

To test all features & functions, we entered in system on local ganache node. Every transaction cleared under 2 seconds, which was great. We also fixed a quick security checked manually by changing one of candidate's name in records of local JSON file. The system caught that instantly flagging certificate as invalid because hash not match which is actually try to verifying on blockchain.

Table 2: System Performance Analysis

Feature	**Traditional System**	**SmartCertify**
Data Security	Low (Centralized)	High (Blockchain)
Verification Speed	Takes days/weeks	Instant (Seconds)
Seat Control	No real-time control	Strict Rules-Based

CONCLUSION

Protection of Sensitive information and their secure management is still lacking in tradition educational databased system and their management. And best salutation is SmartCertify. So, when use SmartCertify, it confirmed that it resolved the traditional issues because the blockchain is actual deal on keeping academic records safe & easy to verify and also making trust by using smart contract in education system. Furthermore, by using Rules-Based Governance, we are able to drain time consuming manual approvals of every single file, which speedup the education system. SmartCertify proof that decentralized technical structure is the way to go if they want to stop certificate scam and actually build trust in reference of security secure management etc. back into education system.

REFERENCES

1. Manav Bharti University (MBU) Scam (36,000 Fake Degrees): Integrity Asia Investigation Report, Feb 2021.

2. Delhi Police Busts Massive Syndicate (5,000+ Fake Degrees): ET Education, June 2025.
3. Prayagraj Police B-Pharma Racket (7,000+ Certificates): Medical Dialogues, April 2026.
4. Micro-Credentials & Smart Contracts: M. Rahmah et al., "Integrating Blockchain-Based Smart Contracts for Digital Certification," JITE, Vol. 9, No. 2, 2026.
5. Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. Applied Sciences, 9(12), 2400.
6. Awan, S. M., Azad, M. A., Arshad, J., Waheed, U., & Sharif, T. (2023). A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information (Switzerland), 14(2).
7. Dashkevich, N., Counsell, S., & Destefanis, G. (2024). Blockchain Financial Statements: Innovating Financial Reporting, Accounting, and Liquidity Management. Future Internet, 16(7).
8. Imelda Bandaso, T., Randa, F., & Arwinda Mongan, F. F. (2022). Blockchain Technology: Bagaimana Menghadapinya? –Dalam Perspektif Akuntansi. Accounting Profession Journal, 4(2), 97–115.
9. Paksi, A. B., Hafidhoh, N., & Bimonugroho, S. K. (2023). Perbandingan Model Pengembangan Perangkat Lunak Untuk Proye Tugas Akhir Program Vokasi. Jurnal Masyarakat Informatika, 14(1), 70–79.
10. Surucu-Balci, E., Iris, Ç., & Balci, G. (2024). Digital information in maritime supply chains with blockchain and cloud platforms: Supply chain capabilities, barriers, and research opportunities. Technological Forecasting and Social Change, 198, 122978.
11. Decentralized Academic Issuance (TRON Network): A. J. E. Andrade and F. C. Amate, International Journal of Computer Science & Information Technology (IJCSIT), Vol. 17, No. 6, 2025.
12. Greenfield, N. M. 2022. “The Many, Always Deleterious Faces of Credential Fraud.” UNESCO IIEP ETICO, October 27, 2022.
13. K. S.Mortensen, "How to Prevent Credential Fraud in 2023," Diplomasafe, 12 Sept. 2023.
14. A. Hayes,“Blockchain Facts: What Is It, How It Works, and How It Can Be Used,” Investopedia, updated Mar. 24, 2025. [Online].
15. Tamper-Proof Frameworks: N. N. Shaikh et al., "Blockchain-Based Tamper-Proof and Decentralized Framework for Educational Documents Verification," Spectrum of Engineering Sciences, Vol. 4, Issue 2, 2026.
16. C. Campbell and G. Pacheco, “What are the 4 different types of blockchain technology? Each blockchain network has distinct pluses and minuses that largely drive its ideal uses,” TechTarget, Aug. 7, 2024.
17. European Parliamentary Research Service, “EPRS STU (2020)641530_EN: ‘Blockchain and the general data protection regulation — Can distributed ledgers be squared with data protection?’”, European Parliament, June 2020.
18. European Standards (EBSI): E. Tan et al., "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI)," Big Data Cogn. Comput., Vol. 7, No. 79, 2023.
19. European Commission (EC). EBSI. 2021.
20. Janssen, D. Power Grid Operators Launch Blockchain for Home and Car Batteries. *Euractiv*. 1 May 2020.
21. Steiu, M.F. Blockchain in Education: Opportunities, Applications, and Challenges. 2020. First Monday.
22. Thakkar, P.; Nathan, S.; Viswanathan, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. 2018.
23. Blockchain Core Principles: Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System."
24. Dai,"b-money,"
25. A. Back, "Hashcash - a denial of service counter-measure,"
26. Architecture & Trends: Zheng, Z. et al. (2017). "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE.
27. Chaubey, P. K., & Singh, U. (2022). The impact of cyber-crime on the internet and system can prevent its spread around the world. International Journal of Research and Analytical Reviews (IJRAR).