International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

ChainCred: Blockchain and AI-Driven Approaches for Credential Verification

AARCHA MALAVIKA, JERRY SANJU JOANES, JEZ THOMAS P KURIEN, JOE ABRAHAM K, MUHAMMED ILYAS H, SABEENA K, CHINCHU M PILLAI

Department of Computer Science, College of Engineering Chengannur, Kerala, India

aarchamalavika2306@gmail.com, jezthomaspkurien@gmail.com, jerrysanjujoanes000@gmail.com, joeabrahamk2004@gmail.com ilyashm@ceconline.edu, sabeenak@ceconline.edu, chinchumpillai@gmail.com

***Abstract*— Credential verification in education and recruitment faces increasing challenges due to fraud, unverifiable skill claims, and forged certificates. Blockchain and artificial intelligence (AI) technologies offer transformative opportunities to address these issues by enabling secure credential management, automated resume parsing, and authenticity checks for submissions such as code and projects. This paper presents a structured literature review of nine works in these domains. We analyze methodologies, datasets, and evaluation metrics, compare contributions and limitations, and synthesize implementable features for ChainCred, a decentralized credential verification platform. The results show that blockchain provides immutability and decentralized trust, while AI enhances automation and originality checks, creating a pathway for reliable credential ecosystems.**

***Index Terms*—Blockchain, Verifiable Credentials, Resume Parsing, AI Detection, Credential Verification**

I. Introduction

The global education and recruitment ecosystem has under- gone a paradigm shift with the rapid digitization of profes- sional credentials, academic transcripts, and resumes. While digital credentials make the sharing of qualifications seamless, they also increase the risks of manipulation and fraudulent claims. A 2022 industry report revealed that nearly 40% of employers encountered false claims in resumes, including inflated skillsets and counterfeit academic degrees. In higher education, forged certificates have caused reputational damage to institutions, while in recruitment, fraudulent hiring decisions have led to financial and productivity losses.

Traditional credential verification methods, such as man- ual document validation and background checks, are slow, resource-intensive, and often siloed across institutions. These systems lack interoperability, making cross-institution and cross-border verification particularly challenging. The emer- gence of generative AI has further complicated credential verification, as candidates may now use AI to fabricate project reports, essays, or even code submissions.

Blockchain technology offers a decentralized and tamper- proof infrastructure for issuing, storing, and validating digi- tal certificates. By design, blockchain introduces immutabil- ity, transparency, and decentralization, which are critical in preventing credential fraud. Complementarily, AI—especially natural language processing (NLP) and large language models (LLMs)—provides automation for parsing resumes, extracting relevant skills, and ranking candidates. AI-based detectors for code authenticity mitigate risks associated with AI-generated submissions in academic and hiring contexts.

This paper systematically reviews nine key works spanning blockchain-based certification systems, decentralized creden- tial management frameworks, AI-powered recruitment au- tomation, and AI-authenticity verification methods. The review is structured around methodologies, datasets, performance metrics, and contributions versus limitations, enabling a con- solidated roadmap of features for ChainCred, a proposed decentralized credential verification ecosystem.

This paper reviews existing work across blockchain-based credential systems, AI-powered recruitment tools, and AI- authenticity detection. The review is guided by the following research questions:

- RQ1: How have blockchain systems been applied to academic and professional credential verification?
- RQ2: What role does AI play in automating resume parsing and candidate screening?
- RQ3: How effective are AI-authenticity detectors in dis- tinguishing human- versus machine-generated content?
- RQ4: What gaps remain, and how can a system like ChainCred integrate these approaches into a unified framework?

II. Methodology and Dataset Analysis

A. Detailed Study

AI-authenticity studies have become an essential area of research in response to the rapid progress of large language

models (LLMs) and their increasing ability to generate code that is indistinguishable from human-written code. With ed- ucational institutions and recruiters expressing concern about academic dishonesty and skill misrepresentation, the field has moved quickly to address the growing challenge of detecting machine-generated code submissions.

One noteworthy approach is the MAGECODE study, which introduced a specialized LLM-based model designed to detect AI-generated code samples. This model combined multiple advanced metric-based techniques and leveraged deep learning to analyze not only structural features and syntax patterns but also subtle stylistic nuances that differentiate AI-written code from human-produced solutions. MAGECODE was evaluated on a variety of benchmarks, including code samples from di- verse programming tasks and educational contexts, showcasing high accuracy in recognizing text generated by state-of-the-art LLMs.

In parallel, other benchmarking studies have compared the performances of several detection models using large and diverse datasets. For example, the MultiAIGCD dataset covers more than 120,000 AI-generated and over 30,000 human- written code snippets across Java, Python, and Go, using six leading LLMs and multiple prompt strategies. These studies test detectors such as OpenAI's Ada embeddings, Salesforce's CodeT5+, and CodeBERTa, each evaluated on scenarios including generating code from problem definitions, fixing runtime errors, and correcting outputs. Results consis- tently show strong performance in detecting straightforward, problem-definition-generated code but substantially reduced accuracy when the AI is used to fix or modify existing human code. Furthermore, models experience significant drops in performance when subjected to cross-language tasks (e.g., trained on Java and tested on Python), raising questions about generalization.

TABLE I
METHODOLOGIES AND DATASET CHARACTERISTICS

Paper	Methodology	Dataset/Source
Kourtzanidis (2020)	Blockchain for academic self-sovereignty	University academic records
Blockchain Certification	Distributed ledger for diploma verification	Sample digital diplomas
EduChain	Gas-optimized blockchain framework	Simulated certificate transactions
Safe Credential Checking	Blockchain-based hiring validation	Candidate resumes, hiring data
Decentralized Credential Status	Revocation and status registries	Credential lifecycle datasets
Resume Parsing (Gemini API)	Custom pattern-matching skill extraction	Resume corpus with labeled skills
NLP Resume Screening	NLP ranking and shortlisting	Resume sets + job postings
MAGECODE	LLM-based detection of AI code	AI vs human code samples
AI Detector Benchmarking	Comparative detector evaluation	Student assignments + benchmarks

B. Comparative Table: Methodologies and Datasets

Blockchain research for credential verification mainly uses prototype datasets—such as simulated certificate records and university academic data—to test smart contract and authen- tication functionalities. However, these prototypes often lack the complexity and volume found in national or global cre- dentialing systems. NLP-based resume screening and parsing studies employ real resumes and job postings, but face issues like limited dataset diversity and the risk of biased results, especially when training data is not representative of a broad population. AI code detection methods often rely on synthetic benchmarks created by generating code with various LLMs, sometimes mixing in human-written samples. While these artificial datasets enable rigorous model comparisons, they may not reflect the complexity of real-world scenarios where human and AI code can blend, and where efforts to evade detection are increasing. Overall, these methodological differ- ences highlight the important trade-offs between experimental control and real-world applicability across blockchain, NLP, and AI-authenticity studies.

TABLE II
PERFORMANCE METRICS SUMMARY

Paper	Metrics Used	Performance Highlights
Kourtzanidis (2020)	Integrity, Transparency	Enabled self-sovereign academic identity
Blockchain Certification	Fraud resistance, Trust	Secure diploma verification across nodes
EduChain	Scalability, Gas cost	Reduced transaction cost by ~25%
Safe Credential Checking	Tamper-resistance, Reliability	Verified recruitment credentials in real-time
Decentralized Credential Status	Revocation latency	Credential status updated within seconds
Resume Parsing (Gemini)	Precision, Recall	Skill extraction accuracy above 85%
NLP Resume Screening	Ranking accuracy	Improved shortlisting efficiency by ~30%
MAGECODE	Detection accuracy	LLM detection accuracy above 90%
AI Detector Benchmarking	Precision, Recall, F1	Inconsistent; F1 scores ranged 60–80%

III. PERFORMANCE AND METRICS EVALUATION

A. Detailed Study

Blockchain-based credential verification systems are typi- cally assessed using a variety of key performance metrics that reflect real-world applicability and scalability. Among these, gas efficiency, transaction throughput, and revocation latency stand out as critical indicators. For instance, EduChain demon- strated an impressive reduction in gas costs by approximately 25

In the domain of AI-driven recruitment tools, performance metrics emphasize both accuracy and efficiency. The Gemini API-based resume parser achieved over 85

AI-authenticity detection tools, focused on identifying machine-generated content such as code, have shown consid- erable promise but also present challenges regarding reliability and consistency. The MAGECODE system reported detection accuracies exceeding 90

Collectively, these evaluations indicate that while blockchain and AI technologies have advanced significantly in credential verification and authenticity detection, ongoing improvements in efficiency, scalability, and detection robustness are essential for their widespread adoption and real-world impact.fferent detectors, with F1 scores varying between 60–80%. These results underline the need for more robust and generalized AI-authenticity models.

IV. Innovations, Contributions, and Limitations

A. Detailed Study

Blockchain technology has contributed significantly to advancing credential verification through several innovative frameworks. One key contribution is the concept of self- sovereign academic identity, as explored by Kourtzanidis, which empowers individuals to own and control their aca- demic records securely on decentralized platforms. This model enhances privacy and ensures immutability, giving students and professionals greater trust and autonomy over their cre- dentials. Concurrently, blockchain-based fraud-proof diploma verification systems offer robust protection against forgery, enabling institutions to issue diplomas recorded immutably on distributed ledgers, as highlighted in the Blockchain Cer- tification framework. EduChain further advances the field by introducing cost-optimized certificate validation, reducing gas fees and making blockchain verification economically feasible for large-scale implementations. Meanwhile, Safe Credential Checking applies blockchain to recruitment pipelines, provid- ing real-time validation of candidate credentials and preventing fraudulent hiring decisions. Credential status registries com- plement these advances by enabling near-instant revocation of credentials, ensuring that invalid or compromised certificates cannot be misused, thereby maintaining continuous trust in the credential ecosystem.

Artificial intelligence has also made impactful contributions. Resume parsing systems leverage AI to extract structured skill information from unstructured resume texts, facilitating automated and scalable candidate screening processes. NLP- powered shortlisting algorithms improve human resources (HR) efficiency by ranking candidates more effectively and reducing manual workload. The MAGECODE system exem- plifies AI's role in authenticity verification by applying large language models (LLMs) to detect AI-generated programming submissions, a growing concern in academic and hiring con- texts. Benchmarking studies on AI detectors shed light on varying strengths and weaknesses, informing ongoing efforts to refine and standardize these tools.

Despite these advancements, limitations persist across do- mains. Blockchain systems, while promising in prototype phases, face significant challenges in achieving large-scale in- stitutional adoption. Barriers include scalability issues related to transaction throughput and gas costs, as well as difficul- ties integrating with legacy education systems and ensuring interoperability across diverse institutions and jurisdictions. NLP models for resume parsing and screening are often constrained by biases embedded in training datasets, which may inadvertently disadvantage minority or underrepresented groups, raising concerns about fairness and ethical AI use. AI- authenticity detection systems confront the complex problem of false positives and negatives, particularly when submitted code involves hybrid human–AI collaboration or deliberate attempts to mask AI generation, underscoring the ongoing need for improved, generalized detection methodologies.

In summary, while blockchain and AI technologies demon- strate transformative potential in credential verification and authenticity assurance, their practical deployment necessitates addressing scalability, interoperability, fairness, and reliabil- ity challenges to realize trustworthy, efficient, and equitable credential ecosystems at scale.

TABLE III
Summary of Core Contributions and Limitations

Paper	Contributions	Limitations
Kourtzanidis (2020)	Academic self-sovereignty	Limited adoption in practice
Blockchain Certification	Fraud-proof diplomas	Prototype, lacks scaling
EduChain	Gas-optimized framework	Simulation only, not deployed
Safe Credential Checking	Secure hiring verification	Privacy and adoption hurdles
Decentralized Credential Status	Real-time revocation	High complexity, scalability issues
Resume Parsing (Gemini)	Accurate skill extraction	Limited across formats
NLP Resume Screening	Improved shortlisting	Bias from training corpora
MAGECODE	AI code detection	Misclassifies hybrid code
AI Detector Benchmarking	Comparative benchmarks	Inconsistent accuracy

V. Final Discussion and Insights

The reviewed works highlight critical lessons for building an integrated credential verification ecosystem like ChainCred. The following nine key insights summarize the contributions of each paper:

.

1) From Kourtzanidis (2020): Self-sovereign identity through blockchain empowers individuals to manage their academic records while ensuring immutability and trust.
2) From Blockchain-Based Certification: Distributed ledger verification enhances trust across institutions, enabling fraud-proof diploma validation.
3) From EduChain: Gas optimization techniques reduce transaction costs, making blockchain-based credential verification scalable for large deployments.

4) From Blockchain for Safe Hiring: Integrating credential verification into recruitment pipelines prevents fraudu- lent hiring decisions by ensuring real-time validation.
5) From Decentralized Credential Status Management: Re- vocation registries provide dynamic trust by ensuring credentials can be invalidated immediately when com- promised.
6) From Resume Parsing (Gemini API): Custom pattern- matching algorithms significantly improve structured skill extraction from unstructured resumes.
7) From NLP-Powered Resume Screening: Automated ranking systems improve candidate shortlisting effi- ciency, reducing HR workload and increasing fairness.
8) From MAGECODE: LLM-based authenticity detection achieves high accuracy in identifying AI-generated code, ensuring integrity in programming submissions.
9) From AI Detector Benchmarking: Comparative evalu- ation of detectors reveals inconsistencies, underscoring the need for standardized, robust authenticity detection frameworks.

Together, these insights indicate that ChainCred should adopt a phased development roadmap: first establishing blockchain-based trust foundations, then integrating AI- powered recruitment automation, and finally incorporating advanced AI-authenticity verification to safeguard originality in submissions.

VI. Conclusion

This literature review analyzed nine works spanning blockchain, NLP, and AI-authenticity detection, examining their methodologies, datasets, metrics, contributions, and lim- itations. The findings highlight that blockchain provides im- mutable trust and decentralized credential management, while AI contributes automation in candidate evaluation and safe- guards against fabricated content. Although each approach shows promise, limitations such as scalability, interoperability, dataset bias, and inconsistent detection accuracy remain barri- ers to real-world adoption. Taken together, these insights point toward a roadmap for ChainCred: first establishing blockchain- based trust foundations, then enhancing recruitment with AI- driven parsing and ranking, and finally incorporating authen- ticity verification to protect originality in submissions. By combining the strengths of blockchain and AI, ChainCred can create a secure, efficient, and reliable credential verification ecosystem that addresses the shortcomings of traditional meth- ods.

References

[1] K. Kourtzanidis, K. Votis, D. Tzovaras, and L. Roumeliotis, “Academic self-sovereignty via blockchain,” in *ASE 2020*, 2020.
[2] A. Author, B. Author, and C. Author, “Blockchain-Based Certification System: The Prospect of Revolutionizing Credential Verification,” 2021. [Online]. Available: Uploaded PDF.
[3] A. Author, B. Author, and C. Author, “EduChain: A Blockchain-Based System for Efficient and Secure Certificate Verification,” 2022. [Online]. Available: Uploaded PDF.
[4] A. Author, B. Author, and C. Author, “Blockchain for Safe Credential Checking in Hiring,” 2023. [Online]. Available: Uploaded PDF.
[5] A. Author, B. Author, and C. Author, “Decentralized Credential Status Management: A Paradigm Shift in Digital Trust,” 2023. [Online]. Available: Uploaded PDF.
[6] A. Author, B. Author, and C. Author, “Resume Parsing and Skill Extraction using Custom Pattern Matching Algorithm and Gemini API,” 2023. [Online]. Available: Uploaded PDF.
[7] A. Author, B. Author, and C. Author, “NLP-Powered Resume Screening and Ranking System,” 2023. [Online]. Available: Uploaded PDF.
[8] A. Author, B. Author, and C. Author, “MAGECODE: Machine-Generated Code Detection Method Using Large Language Models,” 2023. [Online]. Available: Uploaded PDF.
[9] A. Author, B. Author, and C. Author, “Assessing AI Detectors in Identi- fying AI-Generated Code: Implications for Education,” 2023. [Online]. Available: Uploaded PDF.