CrediChain

A blockchain application for hiring documents

By: Luca Lo Nardo, Katie Connolly, Declan Townsend and Sebastian Munoz

Table of Contents

1.0 Current Market and Problem Identification

In today's world, hiring and credential verification is time-consuming, expensive and has many steps to them. Companies, universities, and third-party verification agencies all hold their own databases and methods for record storing. As a result, employers often spend significant time and money attempting to verify candidates' credentials, such as academic transcripts, certifications, reference letters, and criminal background information.
Right now, a large portion of employers use manual verification processes. Universities often require applicants or employers to request transcripts through third-party agencies, while courts and other institutions keep separate databases that are not interconnected. This causes inefficiencies, delays, and opportunities for fraud.

The major problems that exist within the current system include:

- Reference letters and resumes can be forged or manipulated.
- Applicants have to consistently resubmit the same sensitive documents to multiple employers.
- Employers must manually contact institutions for verification.
- Verification processes are slow and expensive.
- The use of different databases and systems causes inconsistencies.
- Sensitive data is vulnerable during repeated transfers between organisations.

These inefficiencies cause administrative problems for both employers and applicants, which could be avoided. In industries where trust and accuracy are critical, delays or fraudulent information can negatively impact hiring decisions.

Additionally, as hiring international people continues to become more common, the challenges become greater. Employers must often verify foreign degrees and legal documents from institutions that operate under different systems and laws. As a result, this increases the likelihood of delays and fraud.

Furthermore, the current hiring environment lacks a single, secure and trustworthy platform that allows credentials to be verified instantly and reliably.

2.0 Proposed Solution

CrediChain is a blockchain-based credential verification platform that is designed to simplify and secure the hiring document verification process.

The platform will use blockchain technology and smart contracts to create a decentralised and tamper-proof system where people can store and share their verified credentials.

The main idea behind CrediChain is to give institutions that are trusted, such as colleges, verification agencies and employers, the ability to issue verified credentials directly onto the blockchain. Individuals will still maintain ownership and control over access to their records, whilst employers can instantly verify the authenticity of the documents. Rather than people having to repeatedly email their transcripts, recommendation letters and other certificates to their employers, users can simply share a secured link that gives the employer permission to their records.

The proposed system has multiple improvements over of the current verification systems:

- Instant verification of documents.
- Minimal fraud through tamper-proof blockchain records.
- The removal of manual verification steps.
- Improved privacy and security through encrypted storage.
- Users have control over who can access their credentials.
- Faster hiring decisions.
- Reduction in administrative costs.

Using blockchain will allow us to move the document verification from a manual trust-based process into an automated, instantaneous trust system.

Current databases rely on centralised control, where records can be altered and manipulated. On the contrary, blockchain creates a distributed ledger where documents are tamper-proof once they are verified and uploaded.

CrediChain's goal is to create a user-friendly platform where:

- Institutions upload verified credentials.
- Users are able to store and manage their credentials.
- Employers have to request access to records.
- Smart contracts automatically verify authenticity.
- Verification only takes a few seconds rather than days or weeks.

The primary goal is to create a tamper-proof, trusted platform for hiring documents that will significantly improve the efficiency, transparency, and security of the process.

3.0 Key Activities

There are several operational activities that are required for CrediChain to be developed and scaled successfully.

College and Institutional Partnerships

Initially, our thought process led us to believe that directly partnering with colleges would be the most successful primary growth strategy. However, after receiving our presentation feedback, it became apparent that convincing a large number of universities to immediately adopt CrediChain may not be realistic for an early-stage startup.

Therefore, a more practical implementation strategy would be to first partner with existing credential verification agencies and other smaller certification organisations. Since these organizations already operate within the verification industry, they are more likely to be willing to bear adoption costs in order to improve efficiency and reduce fraud. This new approach would allow CrediChain to build credibility, demonstrate proof of concept and gradually scale toward larger institutional partnerships over time. Long term, colleges would still be important partners once the platform demonstrates adoption and reliability.

Blockchain Development and Maintenance

The technical infrastructure of the blockchain platform will be continuously developed, monitored, and improved.

This includes:

- Developing smart contracts.
- Maintaining secure blockchain infrastructure.
- Preventing exploitation and any vulnerabilities.
- Updating its security protocols.
- Improving its scalability and efficiency.

This is important as the platform must remain reliable and secure, as it will hold sensitive hiring documentation.

Employer Verification Services

CrediChain will also need to have systems that allow the employer to request and verify credentials quickly and efficiently.
Employers should be able to:

- Access requested credentials.
- Verify the authenticity instantly.
- Minimise manual administrative work.
- Improve hiring confidence.

Product Design and User Experience

The platform needs to be simple and user-friendly. Most employers, students, and institutions are not blockchain experts. Therefore, it is important that the platform's interface prioritises usability and accessibility.

Important design considerations include:

- Simple credential sharing.
- Easy permission control.
- Clear verification indicators.
- Mobile and desktop compatible.
- Secure login and identity management.

Scaling the Platform

Once CrediChain gains initial adoption, it can scaled by:

- Expanding partnerships to a higher institutional level.
- Integrating with HR software systems,
- Onboarding more employers.
- Creating verification standards
- Expanding internationally.

The network effects will become increasingly more valuable as more users and institutions adopt the platform.

4.0 Use Cases

CrediChain has multiple practical applications within the hiring and document verification industry.

Job Applications

The main use case involves employment verification. Applications can place and store their verified credentials on the blockchain and instantly provide employers access to these records. Employers can then verify the transcripts, documents and letters instantaneously without needing to go through a slow third-party agency. This will minimize hiring delays and fraudulent applications.

International Hiring

International hiring can be complicated as additional challenges occur because credentials must be verified across different countries and institutions. CrediChain will be able to simplify this by allowing internationally recognized institutions to upload their verified credentials directly onto the blockchain. This in return, creates a globally accessible verification system that decreases the challenges that come with cross-border hiring.

Certification Verification

Professional certifications will also be stored and verified through the platform. Major industries such as healthcare, finance, technology**,** and engineering commonly require verification of certificates before employment. CrediChain will allow employers to instantly confirm if the certificates are valid and up to date.

Background Verification

Courts and other authorised institutions will have the ability to upload verified legal records and background check data to the blockchain. Employers would then be able to request permission-based access to relevant information while protecting the users' privacy.

Academic Credential Storage

Students and graduates will be able to maintain a permanent digital record of their academic history. This will remove the need to repeatedly request transcripts from colleges while also reducing the administrative costs for them.

5.0 Implementation Plan

The implementation plan for CrediChain would be a multistage approach. After receiving feedback on the presentation, we needed to focus on making the implementation plan more realistic and achievable for a startup. Instead of trying to onboard major colleges nationwide, we would focus on smaller pilot partners and verification-focused organisations.

Phase 1: Build

Phase one would focus on building the core infrastructure. This would include:

- Creating the blockchain platform.
- Forming secure user identities.
- Building employer verification tools.
- Implementing smart contracts for access controls.
- Building document storage systems.

During this stage, the team would focus on security, scalability and functionality.

Phase 2: Launch

Phase two focuses on launching the system and beginning to find partnerships and onboarding users. This would include:

- Onboarding employers.
- Partnering with colleges.
- Establishing verification standards.
- Testing user experience.
- Refining platform functionality based on user feedback.

Pilot programs would allow CrediChain to evaluate the performance and identify areas that need improvement. The initial marketing strategy would focus on growth through relationship-building.

Possible strategies to acquire early customers:

- Partnering with a couple of local colleges that are willing to test the system.
- Working with verification agencies already serving employers.
- Offering pilot programs to medium-sized employers with high hiring volumes.
- Proving the reduced verification processing time and reduced fraud risk.
- Attending HR technology and recruiting conferences.
- Forming a partnership with HR software providers.

This strategy creates a more achievable path towards nationwide adoption.

Phase 3: Scale

Once the platform proves to be successful, CrediChain will then focus its efforts on scaling. This stage would include:

- Expanding partnerships across institutions.
- Integrating with HR and ATS systems.

- Increasing employer adoption.
- Moving CrediChain international.
- Improving network effects.

As the number of users increases, the value of the platform will also increase as more verified credentials become available within the platform.

6.0 Technology and System Architecture

CrediChain operates on a permissioned blockchain framework. Unlike open blockchain systems where anyone can access any information, a permissioned blockchain restricts credential issuance and verification to authorized entities only. This structure improves privacy, compliance, and security across all user types.

Smart contracts automate the core verification process. When an employer requests access to a candidate's credentials, the smart contract verifies the validity of the credential, the legitimacy of the issuing institution, the candidate's permission grant, and the integrity of the data — all without human intervention.

Every user is assigned a digital identity linked to their credentials, with access controlled through permissions and private keys. Institutions upload verified credentials directly onto the blockchain, creating a single trusted source of record.

The end-to-end workflow is as follows:

1. Institution uploads verified credential.
2. Candidate stores credential to their blockchain identity.
3. Employer requests credential access.
4. Candidate grants permission.
5. Smart contract validates credential instantly.
6. Employer receives verified result.

7.0 Target Markets

An essential change to be made based on the feedback provided was the specification of the customers for the platform.

While multiple stakeholders profit from using the platform, the main target audience of the first stage will be the employers and certificate verifiers, since these institutions have a much higher cost of operations due to the time-consuming nature of verification procedures.

For the long-term ecosystem, there will also be universities and certification organisations, but, at first, we will concentrate on those who already spend money on such services.

Employers

Companies are one of the major target markets as they frequently verify applicant credentials. Industries that the team would focus their attention on first are: finance, healthcare, technology, government, education, and consulting. These large employers have to process thousands of applications yearly and spend significant resources on background verification.

College and Educational Institutions

College institutions are another important target market. These institutions can use the platform to:

- Issue digital credentials.
- Decrease transcript processing costs.
- Improve student services.
- Strengthen security.

Certification Agencies

Professional certification agencies may utilize CrediChain for issuing and validating their certifications. This helps build credibility and prevents any fraudulent certification claims.

International Companies

Large multinational organisations gain from the standardisation of international credential verification. Foreign hiring processes become much simpler once employers can validate foreign credentials.

Government and Legal Institutions

Government agencies and courts can benefit from the secure digital verification system that CrediChain would supply. The potential applications could be:

- Identity verification.
- Licensing verification.
- Legal document verification.
- Professional background validation.

8.0 Revenue Stream and Economics

CrediChain plans to operate using a subscription and transaction-based revenue model to generate sustainable income during its early stages.

Employers would pay an annual subscription fee of $3000 to access the verification platform. Additionally, each of the credential verification requests would carry a $5 transaction fee. Revenue will also be generated from universities and institutions by requiring a small $0.50 fee per credential uploaded into the CrediChain platform. Based on these prices and pilot year assumptions, we estimate the following:

Source	Quantity	Price	Revenue
Employers	25	$3000	$75,000
Employer Transactions	10,000	$5	$50,000

Institution Uploads	50,000	$0.50	$25,000
		Total Gross Revenue	$150,000

The initial year of offering will involve substantial costs to develop the platform, establish strong security, ensure regulatory compliance, and incentivize university integration. In addition to start-up costs are recurring cloud and storage costs which we estimate will come to approximately $6000 annually. A summary of these cost categories and their respective estimates are:

Category	Estimated Cost
Platform Development	$40,000
Compliance/Security	$15,000
Cloud/Storage (annual)	$6,000
University Integration Pilots	$10,000
	$71,000

This yields a projected first-year net operating profit of $79,000. These figures suggest that CrediChain could reach operating profitability during its growth stages provided adoption targets are met. Given a predicted profit of $79,000, these estimates also provide flexibility and cushion in case estimated revenues prove to be overstated or estimated costs understated. In the following years, we intend for employers to renew their subscriptions and verification volume to grow, resulting in compound revenue and stable growth.

In terms of organization, we do not plan to introduce a token during the early phase of the platform. Our priority is the first build of a reliable and widely adopted ecosystem. To focus on this, we want to eliminate unnecessary complexity that could be caused by tokenization. However, future tokenization could be utilized to incentivize institutions to report accurate credentials, provide maintenance support, or become active CrediChain users.

9.0 Competition and Competitive Advantage.

Several companies are currently operating with the credential verification space including Appii, Workwolf, EveryCred, R-Block, and Dock. However, most of these competitors focus on only one aspect of verification. For example, Appii specializes in career history while Workwolf focuses on digital passports and Dock concentrates on credential issuance and validation.

CrediChain functions as a comprehensive all-in-one verification platform unlike the competitor companies that target a single credential type, CrediChains supports academic records, certifications recommendation letters, court records, and employment verification all within one system. Additional

advantages include faster verification, reduced fraud, decentralized trust, user control, security, encrypted storage, stability and lower administrative costs. The combination of blockchain immutability and smart contract automation creates a more effective and trustworthy system relative to any current market offerings.

10.0 Risks and Challenges

While CrediChain presents significant potential, several risks must be carefully managed across its development and growth stages.

Data Privacy and Storage Architecture

The most critical challenge is determining what information belongs on the blockchain versus in secure off-chain systems. Storing sensitive documents such as transcripts or criminal records directly on a ledger creates notable regulatory and privacy risks. As further detailed in Section 14, CrediChain mitigates this through a hybrid storage model in which only cryptographic hashes, issuer addresses, timestamps, and access permissions are written on-chain. All sensitive document content remains in encrypted off-chain databases, which are only accessible through candidate-controlled permissions. This approach satisfies GDPR's right to erasure and FERPA's consent requirements while preserving the verification benefits of blockchain.

Smart Contract Vulnerabilities

Bugs or logical flaws in smart contract code can result in unauthorized access, incorrect permission grants, or permanent data corruption. Unlike traditional software, deployed smart contracts cannot simply be patched when mistakes are realized. To mitigate this risk, CrediChain will conduct third-party security audits. The contract will also undergo a minimum 90-day testing period on a test network before handling real credential data, with ongoing automated monitoring to flag suspicious activity.

Adoption Risk

Universities, employers, and certification bodies may be hesitant to transition away from established verification systems due to integration costs, limited blockchain familiarity, or strong relationships with existing third parties. CrediChain addresses this by targeting existing credential verification agencies as its first partners rather than approaching institutions directly. These agencies already operate within the verification industry, have established institutional relationships, and have a direct financial incentive to reduce manual verification costs.

Regulatory Compliance

CrediChain must comply with FERPA in the United States, GDPR in Europe, and various state and international data privacy laws. Additionally, blockchain-based identity systems remain a relatively new legal frontier, with ongoing uncertainty around digital identity standards, credential liability, and cross-border data ownership. CrediChain will address this through dedicated legal consultation beginning

in Phase 1 and will maintain a permissioned blockchain architecture to limit regulatory exposure relative to fully public systems.

Scalability

As verification volume grows, the platform must be able to handle increasing numbers of credential records, access requests, and employer transactions. It must do this without losing performance quality or experiencing radical cost jumps. CrediChain will manage this through its smart contract design and horizontally scalable cloud infrastructure that grows with demand.

11. Regulation and Compliance

CrediChain will be in charge of sensitive educational and personal information, and therefore regulatory compliance is a major priority. In the United States, educational records are protected under FERPA, meaning the platform has to have student consent, secure storage, and restricted access to credentials. For international users, GDPR regulations would also require strong privacy protection and transparency regarding how the user's data is being stored and shared.

To decrease the privacy risks, sensitive documents will not be stored directly on the blockchain. Instead, the blockchain will store encrypted verification documents, while the real documents remain securely stored off the chain.

Due to the new nature of the blockchain-based credential systems, the legal standards surrounding digital identity, international verification, and data ownership are continuing to evolve. As a result of this, CredChain would require continuous legal review and compliance monitoring throughout the development process.

12.0 Reflection and Feedback Incorporation

The feedback received during the presentation phase meaningfully improved the quality and realism of this project across several areas.

First, our original partnership strategy centered on direct university relationships at scale. Following feedback that this approach is not realistic for an early-stage startup, we shifted focus toward credential verification agencies and smaller certification organizations as our primary Year 1 partners. These organizations already operate within the verification industry, making adoption more achievable and the value proposition more immediate. Universities remain part of the long-term vision once the platform has demonstrated reliability and market traction.

Second, feedback stated privacy as a significant concern that our original presentation did not address with sufficient depth. In response, we developed the hybrid storage architecture detailed in Sections 13 and 14, clarifying precisely what data lives on-chain versus off-chain and explaining how this design satisfies FERPA and GDPR requirements. This architectural decision is now central to CrediChain's technical identity rather than a footnote.

Third, feedback pushed us to sharpen our target customer definition and develop a more concrete go-to-market strategy. The revised report identifies credential verification agencies as the anchor customer in Year 1, with employers as the primary direct customer from Year 2 onward. The implementation plan now includes a specific three-step acquisition sequence rather than a general list of marketing activities.

13.0 Execution Plan and Coding

The execution plan for CrediChain focuses on building a functional credential verification system using Solidity smart contracts on the Ethereum network. Development follows the three phases outlined in Section 5: building core contract infrastructure, integrating institutional and employer workflows, and scaling toward HR system compatibility.

The smart contract is built around a `Credential` struct that stores a hash of the underlying document rather than the document itself, keeping sensitive data off-chain while enabling tamper-proof on-chain verification. Access permissions are candidate-controlled, meaning no employer can view a record without an explicit grant from the candidate.

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

contract CrediChain {

    struct Credential {

        bytes32 credentialHash;  // SHA-256 hash of off-chain document

        string  credentialType;  // e.g. "Transcript", "Reference", "CriminalRecord"

        address issuedBy;        // Issuing institution's address

        bool    isValid;         // False if revoked

    }

    // Candidate address => list of credentials

    mapping(address => Credential[]) private credentials;

    // Candidate => Employer => authorized?

    mapping(address => mapping(address => bool)) private access;

    // Institution issues a verified credential to a candidate

    function issueCredential(address _candidate, bytes32 _hash, string memory _type) public {
```

```
        credentials[_candidate].push(Credential(_hash, _type, msg.sender, true));
    }
    // Candidate grants an employer permission to view their records
    function authorizeEmployer(address _employer) public {
        access[msg.sender][_employer] = true;
    }
    // Employer verifies a credential hash against what is stored on-chain
    function verifyCredential(address _candidate, bytes32 _hash) public view returns (bool) {
        require(access[_candidate][msg.sender], "Not authorized");
        for (uint i = 0; i < credentials[_candidate].length; i++) {
            if (credentials[_candidate][i].credentialHash == _hash &&
                credentials[_candidate][i].isValid) {
                return true;
            }
        }
        return false;
    }
    // Issuing institution revokes an outdated or incorrect credential
    function revokeCredential(address _candidate, uint _index) public {
        require(credentials[_candidate][_index].issuedBy == msg.sender, "Not the issuer");
        credentials[_candidate][_index].isValid = false;
    }
}
```

Each function maps directly to a step in the CrediChain workflow: institutions call `issueCredential()` to write verified records, candidates call `authorizeEmployer()` to grant

access, employers call `verifyCredential()` to confirm authenticity, and institutions call `revokeCredential()` to invalidate outdated records. Sensitive document content never touches the chain — only its SHA-256 hash is stored, which contains no personally identifiable information and satisfies the privacy architecture described in Section 14.

14.0 System Architecture and Privacy Design

CrediChain uses a hybrid storage model where the blockchain stores proof of credentials rather than the credentials themselves. Every sensitive document, transcripts, recommendation letters, criminal records, is stored in AES-256 encrypted off-chain databases. Only the document's SHA-256 hash, the issuing institution's address, a timestamp, validity status, and employer access permissions are written on-chain. Since a hash contains no personally identifiable information, a breach of either layer in isolation yields nothing exploitable.

Data	Storage	Reason
Credential hash	On-chain	Tamper-proof fingerprint; no personal data
Issuer address + timestamp	On-chain	Audit trail; no personal data
Validity + access permissions	On-chain	Required for real-time verification
Document content	Off-chain (encrypted)	FERPA/GDPR protected

When an employer is granted access via `authorizeEmployer()`, they receive a time-limited permissioned link to the off-chain document, not a permanent copy. Candidates retain full ownership at all times and can revoke access instantly. This design satisfies GDPR's right to erasure by allowing off-chain deletion and on-chain revocation without altering the immutable ledger, and satisfies FERPA's consent requirements through the smart contract's permission enforcement.

15.0 Conclusion

CrediChain addresses a genuine and costly inefficiency in the modern hiring process. By replacing slow, fragmented, and fraud-prone verification systems with a blockchain-based platform powered by smart contracts, CrediChain emerges as a superior alternative. It is designed to deliver faster hiring decisions, reduce administrative costs, and provide tamper-proof credential records for employers, candidates, and institutions.

The platform's hybrid storage architecture ensures that privacy and regulatory compliance are built into the system by design. By storing only cryptographic hashes on-chain while keeping sensitive documents

in encrypted off-chain databases, CrediChain satisfies FERPA and GDPR requirements while preserving the immutability and transparency that make blockchain valuable.

While challenges around adoption, smart contract security, and regulatory uncertainty remain, CrediChain's phased implementation strategy provides a structured and realistic approach. Beginning with credential verification agencies as anchor partners followed by scaling to direct institutional relationships, provides an achievable path to market. As the platform grows and network effects compound, CrediChain has strong long-term potential to meaningfully transform how credentials are verified across industries.

16.0 References

Appii. Career verification platform information.

Dock Labs. Blockchain credential verification services.

EveryCred. Digital credential issuance and verification platform.

Federal Educational Rights and Privacy Act (FERPA).

General Data Protection Regulation (GDPR).

R-Block. Blockchain hiring verification platform.

Workwolf. Digital work passport platform.

Class lecture materials and course discussions related to blockchain technology and smart contracts.