Article

Implementation of Global Academic Record and Verification System Against Credential Fraud

Juan Alamiro Berrios Moya and John Ayoade *

Posted Date: 8 November 2024

doi: 10.20944/preprints202411.0622.v1

Keywords: academic credential fraud; blockchain; interplanetary file systems; security; privacy

Article

Implementation of Global Academic Record and Verification System Against Credential Fraud

Juan Alamiro Berrios Moya and John Ayoade *

Victoria University, Crown Institute of Higher Education
* Correspondence: john.ayoade@cihe.edu.au

Abstract: Academic credential fraud poses a real challenge to the global academic and labour market. Fraudulent credentials devalue the legitimacy of bona fide certificates. The Global Academic Record and Verification based on Blockchain and Interplanetary File Systems (GARV-BI) framework was implemented and offers a holistic, privacy-preserving, immutable, secure, and interoperable system for managing academic records. Using advanced blockchain technology, it proposes zkEVM for smart contracts that enables verification of credentials without exposing the underlying data. It also integrates the use of Decentralized IDentifiers (DID) to standardize registration and identity management without relying on centralized entities. A key feature of GARV-BI is that it features a dual blockchain, which separates public and private information, allowing for greater efficiency and privacy of transactions. It also uses the interplanetary File System (IPFS), which allows for decentralized and secure storage of related documents. The result is an open-source solution that is easily integrated, as it uses a standardized Application Programming Interface (API). Extensive testing has shown that it can successfully manage transactions securely, privately, and at a lower cost than solutions based on Ethereum mainnet environments. GARV-BI is innovative in its combination of blockchain technologies, decentralized storage, and globally unique identifiers to achieve higher levels of interoperability, security, and privacy. GARV-BI will transform academic credential management with a platform that is accessible, adaptable, and robust for use by institutions around the world to maintain the integrity of academic qualifications and enable global student mobility.

Keywords: academic credential fraud; blockchain; interplanetary file systems; security; and privacy

1. Introduction

Globally, academic fraud through the fabrication of credentials is a widespread and lucrative industry that costs the world economy billions every year. The high cost of education and the international ease of access to these falsifications create an incentive that is difficult to regulate (Eaton and Carmichael, 2023). The very presence of this fraudulent system of acquiring academic titles leads the real ones to lose value and undermine the integrity and trust in the educational systems (Brown, 2006; Grolleau et al., 2016). Given that academic credential verifications become an integral part of society due to the increasing world demand for secure and verifiable credentials, the pressure to maintain the inventory of the educational records in a precise and reliable matter increases. All these challenges are exacerbated by the digital academic revolution, when academic institutions face not only academic credential fraud, but also data privacy issues and global interoperability.

In response to these challenges, there is greater focus on the use of emerging technologies, such as blockchain and smart contracts, to mitigate the damaging effects of fake qualifications. Research has suggested that such technologies can improve reliability and transparency while accelerating the process of verifying academic credentials, with blockchain cited as a key tool for ensuring the authenticity of academic records. (Michoulis et al 2020; Ghazaliand and Saleh 2018; Tang 2021) One of the major obstacles, however, has been the lack of standardisation frameworks to enhance interoperability. Current systems employed by institutions often have difficulties in integration or are unable to be implemented altogether because of differing infrastructures and technologies.

To solve these problems, GARV-BI is a framework that provides "a one-stop solution for academic credential management, while meeting security, privacy, and interoperability standards" by using blockchain technology operating in zkEVM environments. ZKPs can be used to prove the validity of academic credentials without revealing any information about adjacent data (Partala et al., 2020; Buterin, 2021). GARV-BI also uses decentralized identifiers (DIDs) for student identification, allowing for standardized identities and aiding international student mobility independent of centralized government systems (World Wide Web Consortium 2022). GARV-BI operates on two blockchains to further split data distribution, where sensitive data is stored on private servers, while academic credential data is published and verified on public servers, which not only improves transaction cost efficiency but also increases students' privacy and security for their academic records. Furthermore, the framework utilizes the InterPlanetary File System (IPFS), a decentralized p2p file storage system to ensure the integrity and security of academic documents in the distributed environment (Abed et al., 2024). Encryption of zk-SNARKs as modules in zkEVM ensures credential privacy by hiding private data from the verifier. GARV-BI is built on the Blockchain Academic Credential Interoperability Protocol (BACIP) framework, which provides an ethical and legal foundation, as well as establishing the fundamental principles that an academic credential management system should follow (Berrios Moya 2024). By combining all these features into a single system connected to each other through an API, GARV-BI enables higher education organizations to work together, regardless of their current infrastructure, language, and technology stack. The open-source nature of GARV-BI enables scalability and affordability of the system, this not only improves global interoperability, but also protects the privacy and security of academic records and ensures the integrity and immutability of academic records for a scalable, low-cost, high-performance distributed architecture for academic credential management and verification.

2. Literature Review

2.1. BACIP

Blockchain Academic Credential Interoperability Protocol (BACIP) was introduced by Berrios Moya (2024). Due to the ease of obtaining fake credentials, several institutions are investing in technologies that allow them to distribute their academic credentials in a secure and immutable way to ensure a reliable method of verifying their authenticity. However, due to the diversity of approaches in the integration development of this technology, introducing the concept globally is a significant challenge, as there are not enough mechanisms to aid system interoperability. The idea of BACIP is to serve as a standard baseline platform for the development of blockchain that allows the issuance, storage, and verification of academic credentials, taking advantage of concepts such as immutability and decentralization that blockchain offers. This increases trust in the educational system due to the security features that blockchain is known for, especially in situations where students need to prove their qualifications in a foreign country.

In the development of BACIP, two main objectives were established: defining BACIP's fundamental principles, and considering ethical and viability aspects.

2.2. Blockchain

The blockchain technology was created by Nakamoto (2008), where he presented a model of information distribution that allows decentralized, secure, and transparent way of making transactions. This technology works on nodes in a network, that verifies and validates the authenticity of the information saved based on ledgers organized in blocks with a cryptographic link that form an immutable chain. This system was used initially in bitcoin and is widely used in other environments today such as finance, supply chains, and education, among others, being distributed in both private and public networks.

doi:10.20944/preprints202411.0622.v1

2.3. Public Blockchain

Bitcoin is one of the examples of blockchain running in a public network, this is a completely decentralized network that does not depend on entities to govern it. Here each participant can validate transactions. It uses a system called validation consensus, for example, Proof of Work or Proof of Shake among others that secure the network, where a validator node verifies their work. It is an excellent decentralized security system to operate transactions. However, it has disadvantages when it comes to scaling it, besides its high costs due to the number of participants that need to validate transactions (Buterin, 2014). However, for those systems where security and immutability of the data are vital, this system promises to be the most effective, due to its high degree of trust in its structure.

2.4. Private Blockchain

Unlike a blockchain system running in a public network, it is possible to implement a private network that works with the same system. However, being private, it loses its decentralization characteristic since the one who implements the system is in control. Therefore, despite being equally a secure and immutable system, it is usually implemented at an enterprise level where decentralization is not the focus, but rather to take advantage of data security. In this type of blockchain, only a selected group of participants are empowered to make transactions and validations of data. One of the benefits of a private network is that it does not require gas costs like one running on Ethereum publicly, for example, it is only the implementation costs which the administrator will be expected to bear (Strehle, 2020).

2.5. Zero-Knowledge EVM (ZKEVM)

The zkEVM (Zero-Knowledge Ethereum Virtual Machine) is a technology that combines zero-knowledge proofs (zk-SNARKs or zk-STARKs) with the execution of smart contracts on networks compatible with the Ethereum Virtual Machine (EVM). This approach allows the validity of transactions to be verified without revealing sensitive data, which considerably improves privacy in blockchain networks.

The zkEVM can be implemented in both public and private networks. In public networks like Ethereum, zkEVM is used to ensure transaction privacy without compromising network security. In private networks, zkEVM offers a scalable and private solution for business environments that need confidentiality in their transactions. According to Partala et al. (2020), zero-knowledge proofs are fundamental to ensuring privacy in blockchain applications, allowing verification without revealing sensitive data. Furthermore, recent research has shown that zkEVM is compatible with smart contracts written in Solidity, which facilitates its integration into both public and private networks, providing additional security and scalability (Partala et al., 2020; Buterin, 2021).

2.6. Decentralized Storage IPFS

The Inter Planetary File System (IPFS) is a way of storing files that does not rely on a central server, with the same goal as blockchain, but focused on large volumes of data such as files, which are broken into parts and sent to different parts of the computer network, which are called nodes. The files are stored in multiple parts at the same time, which allows that if a service goes down, these files are still available. The way the file is searched is different from regular storage, as it is not searched by the name but by a fingerprint that is stored in the code, so if the file is modified, this code will change, and it will be evident that the file has been tampered with. This allows detecting and removing this corrupted file from the node network, keeping the non-corrupted files (Abed et al., 2024). A good combination occurs when working together with blockchain as a system can be integrated and stores information based on transactions and verifications like blockchain does, and on the other hand, integrates a file storage system that can be related to the blockchain of greater weight and in an unstructured way that requires the same level of attention but with a structure more appropriate for each component (Abed et al., 2024).

2.7. Decentralized Identifiers (DIDS)

The Decentralized Identifiers (DIDs) were created to solve various problems faced by systems for registering and identifying individuals. For example, the centralization of these registries in the hands of governments or other traditional systems of individual registration contributed to the situation where individuals do not have full control over the management of the information after registration. Individual registered information could be vulnerable to attacks and breaches of personal data. In addition to this security concern is the portability issues where names may have different formats in different countries, different or even null identity numbers in some countries. Verifying an identity in environments outside the government that manages them is a complicated task, requiring an understanding of the registration structure of each country. In 2017, the World Wide Web Consortium formed the DID Working Group to develop the DIDs standard that would solve traditional registration and identity management problems in a decentralized way, launching in 2020 as DID v1.0, having the attributes of Decentralization, Control, Privacy, Security, Proof-based, Discoverability, Interoperability, Portability, Simplicity, and Extensibility (World Wide Web Consortium 2022).

GARV-BI Framework incorporated DIDs as one of its components to leverage their qualities that align with BACIP principles, helping with system interoperability by allowing the management of a single standardized identification system for users globally. This way, it is possible to verify the ownership of credentials without relying on centralized systems. Additionally, it allows compliance with international standards like GDPR for data security and privacy.

3. Related Work

Some complex frameworks have been developed following an approach similar to GARV-BI, however, many are still in the theoretical stage and do not have a fully functional prototype. For example, CredenceLedger is a theoretical study proposing a permissioned blockchain system for secure academic credential verification. While it outlines the framework, no prototype has been developed or tested (Arenas and Fernandez, 2018). Similarly, Badr et al. (2019) proposed a permissioned blockchain-based system using Hyperledger to automate and secure the verification and transfer of academic records between institutions. While the paper outlines the system architecture, it remains theoretical, and no prototype has been developed or tested. Gaikwad et al. (2021) also proposed a blockchain-based verification system for academic certificates that uses Ethereum, OCR, and smart contracts to automate the process of verifying academic credentials. The foundations for implementation are well established, but they did not materialize into a functional development.

On the other hand, some systems have already been successfully implemented, allowing current use. For example, Nadeem et al. (2023) developed a system called Hybrid Blockchain-based Academic Credential Verification System (B-ACVS), which complies with GDPR regulations using a public blockchain based on Ethereum. In addition to the development, they implemented a functional system that was tested and validated. MIT Media Lab (2016) developed Blockcert, which was officially released in 2016 and distributed under the Open-Source License, allowing contributions and free use of the code. This system was based on Ethereum as a public network and aimed to comply with GDPR rules, incorporating IPFS for file management. On the other hand, Sony Global Education (2017) created a framework for credential registration and accreditation, but this time not using a public platform like Ethereum. Instead, it used a private network supported by Hyperledger Fabric deployed using IBM Cloud. This was because it did not need to be a decentralized system, but rather this is a system designed to manage foreign students arriving in Japan, with a variety of languages and learning paths. In this way, they can have an unforgeable academic verification system. Even though this system is fully developed and functionally active, its source codes are not openly available, in fact, it is a system that operates only privately in Japan. Learning Machine who collaborated with MIT Media Lab in the creation of Blockcert was acquired by Hyland Credentials, who using Blockcert as a base created a paid version of this system by changing some components and offering more support and infrastructure for the integration of the system, allowing institutions to delegate responsibilities, but this system is not open source. This platform does not have IPFS integrated, as it was integrated into Blockcert after the collaboration with Learning Machine, however, Hyland adds Decentralized Identifiers (Ledger Insights, 2020).

4. Methodology

The process of developing and evaluating the GARV-BI framework was divided into four distinct phases: design, comparison, implementation and evaluation. The goal was to set up a secure decentralised system for credential management, while still ensuring that the system is interoperable and compliant with global standards.

4.1. Phase 1: System Design and Architecture

The design and architecture of the GARV-BI framework provided a secure decentralised environment to store the academic credentials in a privacy-preserving manner and make the credentials interoperable with other systems adhering to the standards outlined in the Blockchain Academic Credential Interoperability Protocol (BACIP). The full-stack architecture of the system is based on four key modules:

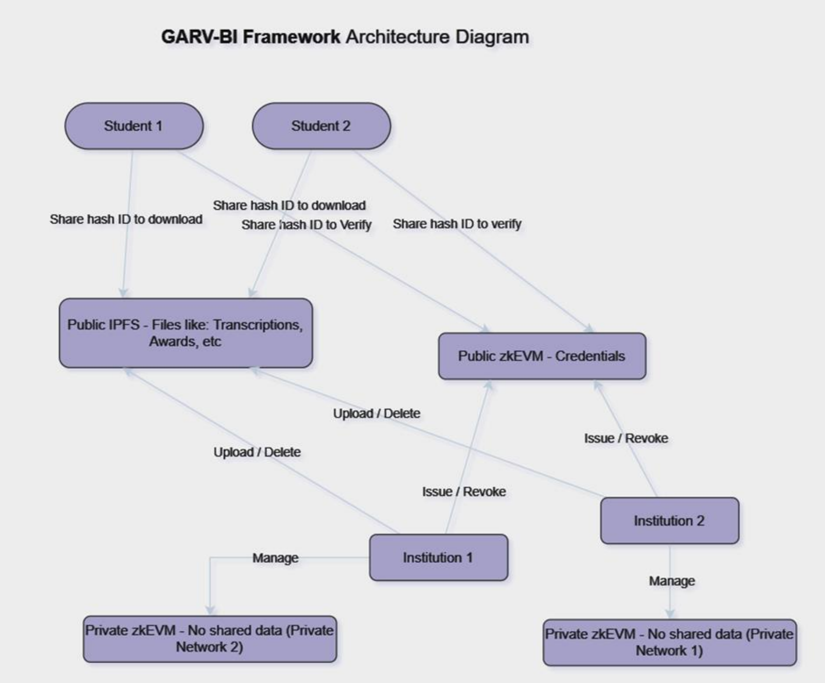
1. A public zkEVM blockchain that hosts the academic credential data, where the academic credential data is provided as an input and is verified by Zero-Knowledge Proofs (zk-SNARKs).

2. A private zkEVM blockchain for the privacy of personal data and academic records in detail. This architecture ensures that the system meets the privacy-preserving requirement, and the same architecture is used as the public network for standardisation and interoperability.

3. Decentralised storage based on IPFS for the storage of the files like transcripts and award documents. To prevent the possibility of data tampering, cryptographic hashes recorded on the blockchain are used.

4. An HTTP-based standardised API was developed for communicating between the above modules, which ensures that the data is in a secure, private and interoperable manner without the need for an intermediate layer between the API and the smart contracts.

Figure 1 shows the architecture of GARV-BI Framework Architecture Diagram. A public blockchain based on zkEVM is developed for the management of academic credentials and an IPFS system for the management of related files, both shared by several academic institutions and students. Each institution also has a private blockchain system which is based on zkEVM and this manages sensitive data that do not require to be shared or verified by agents outside the institution.


GARV-BI Framework Architecture Diagram
Student 1
Student 2
Share hash ID to download
Share hash ID to download
Share hash ID to Verify
Share hash ID to verify
Public IPFS - Files like: Transcriptions, Awards, etc
Public zkEVM - Credentials
Upload / Delete
Upload / Delete
Issue / Revoke
Issue / Revoke
Institution 2
Institution 1
Manage
Manage
Private zkEVM - No shared data (Private Network 2)
Private zkEVM - No shared data (Private Network 1)

doi:10.20944/preprints202411.0622.v1

Figure 1. GARV-BI Framework Architecture Diagram.

4.2. Phase 2: Comparison of Components

GARV-BI framework was developed by selecting relevant blockchain-based scholarly credential management systems obtained from the reliable academic literatures, such as Blockcerts, Sony Global Education, or Hyland Credentials. GARV-BI system was compared with existing systems based on the following criteria: the selected type of blockchain (public, private and hybrid); applied privacy mechanisms (e.g., Zero-Knowledge Proofs); applied data management strategies (e.g., the use of IPFS for data decentralised storage); applied identity management strategies (e.g., Decentralised Identifiers); and applied data protection regulations (e.g., GDPR). This data was collected from documentation of the systems, academic papers and public reports. For each system, architecture, privacy, data management and legal compliance was analysed to enable a clear distinction between GARV-BI and other solutions in terms of architecture, technical features and legal compliance.

4.3. Phase 3: Development and Implementation

The development and implementation of GARV-BI followed an iterative approach. The system was set up in a way that it is functional, secure and interoperable. The core of the data structure was built using Solidity to develop smart contracts for issuance, verification and revocation of credentials, which were tested locally using Ganache and Truffle before deploying the contracts on the public zkEVM blockchain. The front-end, built using React.js, provided a user-friendly experience to the students and the institutions so that they could interact with the system, while the back-end, built using Node.js, handled the blockchain side and took care of storing data on IPFS. Communication and interaction between the front-end and back-end was ensured through the well-designed API. The front-end and the back-end of the system processed the interaction between the students and the institutions through the IPFS data structure to ensure that the integrity and the verifiability of the system were maintained. The IPFS layer was used to store huge academic documents so that they could be decentralised, and the integrity of the documents was maintained through cryptographic hashes recorded on various nodes on the blockchain. The system was tested and validated to ensure the smooth deployment and the operational efficiency of all the components.

4.4. Phase 4: Validation and Testing

Testing of the GARV-BI framework was conducted across several domains to ensure that the system could operate at scale under various conditions and within the constraints of security and compliance. The testing process was designed to capture important aspects of system scalability, security, integrity of data, functionality and cost.

Scalability Testing: This test was done to determine how the system performs with increasing numbers of concurrent credential issuance/verification requests. The test started with lower loads and incrementally increased the number of concurrent requests, measuring processing time, resource utilisation (CPU and memory), and response times to find a threshold. For instance, at which point we can expect the system to slow down in terms of performance. The test helped us determine the system's maximum capacity before a threshold is exceeded.

Data Integrity and Privacy Testing: The Data Integrity and Privacy Testing of academic credentials managed by the GARV-BI framework was carried out in a zkEVM environment. The process involved uploading a batch of academic documents to IPFS and generating their respective SHA-256 Cryptographic Hashes, which were then recorded in the zkEVM blockchain. In the first part of the testing, the documents were retrieved from IPFS and verified against the stored hashes. If any unauthorised changes were detected, it indicated that the system was able to prevent any tampering with documents. In the second part of the testing, the same batch of verifications was carried out, but this time using Zero-Knowledge Proofs (zk-SNARKs). Although the documents were verified, no adjacent data (including personal information) could be exposed in this part of the testing. The tests monitored both the system's ability to maintain document integrity, as well as its ability to keep the system private at the time of credential verification.

Functional Testing: This was functional testing, where we ensured that the system functioned as a whole, meaning from end-to-end. We tested credential issuance, verification and revocation, and how the front-end (user interface) interacted with the back-end (blockchain interactions) and IPFS. The functional testing verified that smart contracts executed as expected and that the data handling functions functioned as intended so the system would work as expected under normal usage.

Cost Efficiency Analysis: The Cost Efficiency Analysis analysed the cost effectiveness of issuing, verifying and revoking credentials on the public zkEVM network. It tracked gas fees and other transaction costs as part of the system's operation in the zkEVM. It also compared the costs of deploying GARV-BI in the zkEVM to deploying the system on Bitcoin and Ethereum. These simulations allowed us to gauge the performance of the zkEVM relative to other blockchain networks. We identified optimisations that would minimise transaction costs for the system while keeping it economically viable for academic institutions.

5. Results

5.1. Comparison of Components of GARV-BI with Other Systems

Analyzing the current systems that have a practical implementation of a framework for the management of academic credentials using blockchain, as we can see in Figure 1, GARV-BI Framework, which is based on the distribution of credentials through a public zkEVM network but also integrates a private zkEVM for managing data that does not need to be shared. In this way, GARV-BI is the only one to propose a dual system that also uses the same EVM technology. Unlike other systems that decide to use one or the other platform, this allows GARV-BI to efficiently distribute data by sharing only the strictly necessary ones on the public network. GARV-BI, along with Hyland Credential, are the only ones that have integrated the Decentralized Identity system, allowing for the standardization of identity management on a global scale, in addition to increasing students' control over the verification of their personal data. An IPFS system that allows for storing files as unstructured data in a secure and decentralized manner, such as certificates documents, passports pictures, or others, in various formats like PDFs, images, etc., has been adopted by GARV-BI, Blockcert, and Sony Global Education. Regarding complying with GDPR standards, all these systems stated that they follow these rules in their frameworks.

Figure 2 shows the presence of various operational components based on blockchain support the management of academic credentials. Figure 2 shows how GARV-BI integrates most components such as IPFS, Decentralisation, public Blockchain, GDPR, and private blockchain.

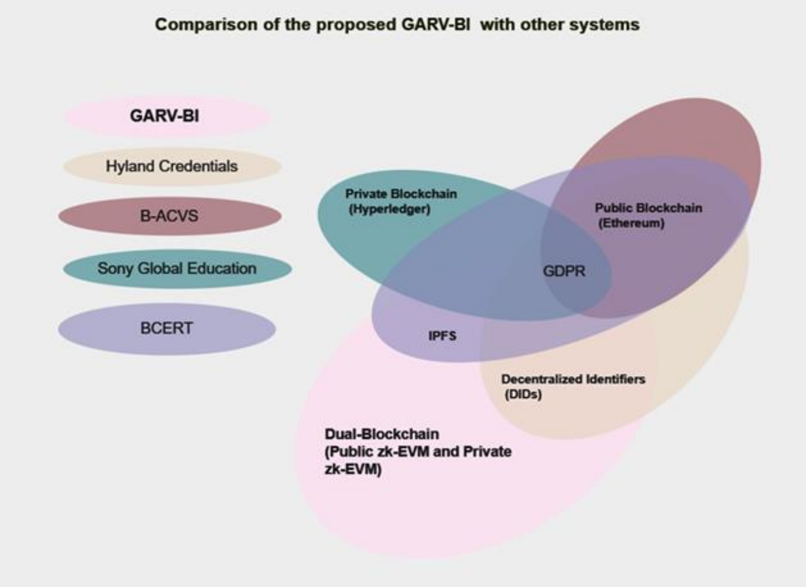

Comparison of the proposed GARV-BI with other systems
GARV-BI
Hyland Credentials
B-ACVS
Sony Global Education
BCERT
Private Blockchain (Hyperledger)
Public Blockchain (Ethereum)
GDPR
IPFS
Decentralized Identifiers (DIDs)
Dual-Blockchain (Public zk-EVM and Private zk-EVM)

Figure 2. Comparison of the proposed GARV-BI with other systems.

5.2. Development and Implementation

The GARV-BI framework was successfully developed, resulting in a fully functional system for decentralized academic credential management. Key components such as smart contracts, APIs, and front-end/back-end integrations were implemented and thoroughly tested. The smart contracts, written in Solidity, handle essential tasks such as credential issuance, verification, and revocation on the public zkEVM blockchain, while sensitive data is securely managed on a private zkEVM network. Both networks were designed to ensure security, privacy, and interoperability.

A significant outcome of this phase was the release of the GARV-BI codebase and documentation under an open-source license. The repository, which includes the smart contracts, API documentation, installation instructions, and IPFS integration details, is available on github.com/portfoliojuanberrios/GARV-BI. The open-source license encourages collaboration and adoption, allowing academic institutions and developers to freely implement, modify, and improve the system. This approach promotes innovation while reducing the technical and financial barriers to decentralized credential management, aligning with the project's mission of global standardization and transparency.

5.3. Validation and Testing

5.3.1. Scalability Testing

The Scalability Testing revealed that the GARV-BI framework was capable of efficiently managing up to 280 concurrent credential issuance and verification requests without significant performance issues. During this load, resource utilization, including CPU and memory usage, remained within acceptable limits, and response times were consistent. However, when the load surpassed 280 concurrent requests, there was a marked increase in processing time and resource consumption, leading to noticeable delays in response times. CPU usage peaked significantly, and the system began experiencing bottlenecks, indicating that its operational capacity had been reached. These results highlight the system's robustness at moderate traffic levels but suggest that optimizations are necessary to support higher volumes without performance degradation.

Figure 3 shows a graph with the relationship between the time required to process a certain number of simultaneous requests as well as marking the breaking point of the system's collapse.

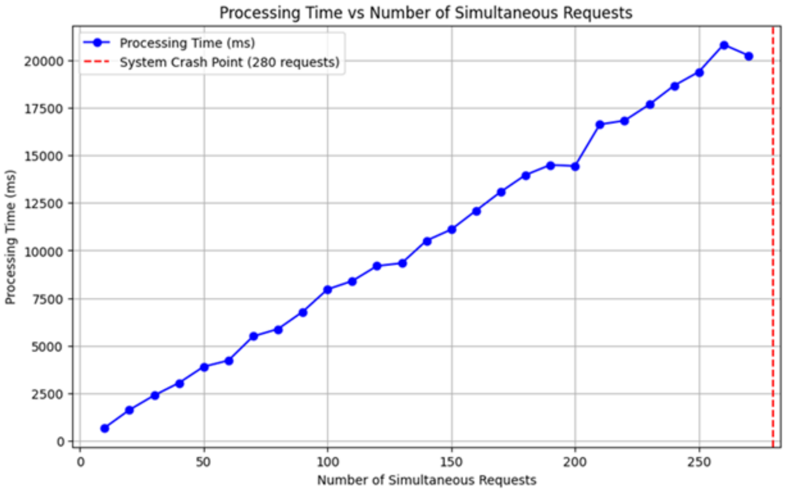


Figure 3. Processing Time vs Number of Simultaneous Requests.

5.3.2. Data Integrity and Privacy Testing

The Data Integrity and Privacy Testing on the zkEVM environment confirmed that the GARV-BI framework was still robust and uncompromised. The cryptographic hashes of the documents (stored on the zkEVM blockchain and linked via a hash to the data on IPFS) were tested for consistency. The system proved impervious to any kind of trickery in document updates, as all documents that were not changed produced matching hashes. Modifications to documents resulted in mismatched hashes, as did attempts to create hash collisions. All these malicious intent scenarios were blocked at their source. Privacy tests also confirmed that the zk-SNARKs implemented in the GARV-BI framework were doing their job and allowed the system to authenticate credentials (eg, university qualifications) without revealing other, adjacent personal data. The zkEVM network sent out only cryptographic proofs, and the data itself remained fully protected. This confirmed that GARV-BI does indeed offer a strong extra layer of privacy. The system is GDPR-compliant.

5.3.3. Functional Testing

The integration and interplay of all the elements of the GARV-BI framework for Functional Testing was successful. This included the front-end, back-end, smart contracts, and integration with external systems. The system worked smoothly when issuing credentials, verifying credentials, and for revoking credentials, all done correctly using the smart contracts in the zkEVM blockchain. The front-end was built in React.js for a smooth interaction experience for the students and institutions, and the back.js actively listens to requisite information from the front-end, communicates with the blockchain, and securely stores the documents on IPFS.

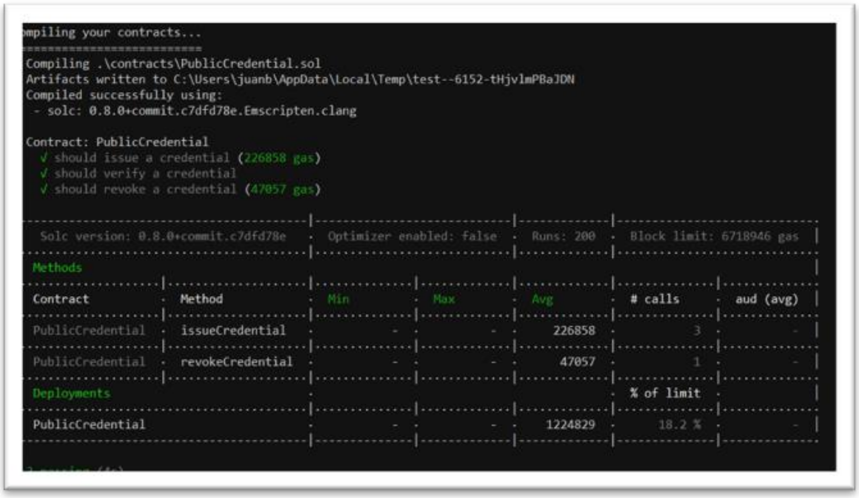
Sensitive data protection: positive result, sensitive information strictly protected for all transaction cycles. Unit tests (smart contracts and API): OK, no errors or security vulnerabilities identified. Web app: OK, all connections with external systems by API works, no errors. Functional tests: OK for all transactions, all step, all conditions. System works properly, no error or security vulnerabilities discovered. The system is ready for use. We can feed external systems with information, use the web app.

5.3.4. Cost Efficiency Analysis

The analysis, based on gas prices published on September 9, 2024 (Polygon, 2024; Etherscan, 2024), demonstrated that zkEVM Polygon consistently provided approximately 94% cost savings across all operations of Issuing a credential, Revoking a credential, and Contract deployment when compared to Ethereum Mainnet.

These findings underscore the substantial cost advantage of using zkEVM Polygon for the decentralized management of academic credentials. Figure 4 illustrates the gas consumption for the GARV-BI system, while Figure 5 visualizes the cost differences between both networks for credential-related transactions.

Moreover, by segregating sensitive data into a private network, GARV-BI minimizes public transaction costs, as only necessary credential issuance and verification data incur public network fees. This dual-network approach further enhances the system's cost efficiency.



```
mpiling your contracts...
=========================
Compiling .\contracts\PublicCredential.sol
Artifacts written to C:\Users\juanb\AppData\Local\Temp\test--6152-tHjvlmPBaJDN
Compiled successfully using:
 - solc: 0.8.0+commit.c7dfd78e.Emscripten.clang

Contract: PublicCredential
  ✓ should issue a credential (226858 gas)
  ✓ should verify a credential
  ✓ should revoke a credential (47057 gas)

------------------------------------------|---------------------------|-------------|----------------------------
  Solc version: 0.8.0+commit.c7dfd78e    ·  Optimizer enabled: false  ·  Runs: 200  ·  Block limit: 6718946 gas  │
·········································|···························|·············|····························
 Methods                                                                                                         │
····················|····················|·············|·············|·············|··············|·············
 Contract           ·  Method            ·  Min        ·  Max        ·  Avg        ·  # calls     ·  aud (avg)  │
····················|····················|·············|·············|·············|··············|·············
 PublicCredential   ·  issueCredential   ·          -  ·          -  ·     226858  ·           3  ·          -  │
····················|····················|·············|·············|·············|··············|·············
 PublicCredential   ·  revokeCredential  ·          -  ·          -  ·      47057  ·           1  ·          -  │
····················|····················|·············|·············|·············|··············|·············
 Deployments                             ·                                         ·  % of limit  ·             │
·········································|·············|·············|·············|··············|·············
 PublicCredential                        ·          -  ·          -  ·    1224829  ·      18.2 %  ·          -  │
-----------------------------------------|-------------|-------------|-------------|--------------|-------------
```

Figure 4. Gas calculation of smart contract PublicCredential.sol on GARV-BI System.

Figure 4 show gas used results for the PublicCredential.sol smart contract. Shown is the gas consumed to issue (226,858 gas), revoke (47,057 gas), and deployment (1,224,829 gas).

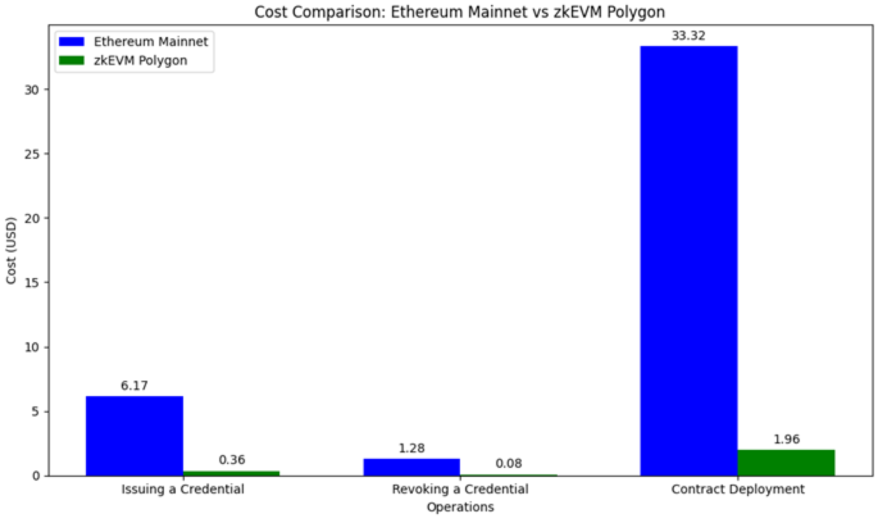


Figure 5. Cost comparison between Ethereum Mainnet and zkEVM Polygon for credential issuance, revocation, and contract deployment in the GARV-BI system.

This graph illustrates the cost efficiency differences between Ethereum Mainnet and zkEVM Polygon for issuing a credential, revoking a credential, and deploying the PublicCredential.sol smart contract. On average, zkEVM Polygon reduces transaction costs by approximately 94% compared to Ethereum Mainnet, as calculated based on gas prices and the operations related to academic credentials management.

6. Conclusion

The development and implementation of the GARV-BI framework mark a significant advancement in decentralized academic credential management. Leveraging the capabilities of both public and private zkEVM blockchains, GARV-BI ensures the integrity and privacy of academic records through robust cryptographic methods, including Zero-Knowledge Proofs (zk-SNARKs) and decentralized storage via IPFS. This dual-network architecture not only enhances data security and privacy but also achieves cost efficiency, as demonstrated by the approximately 94% reduction in operational costs when compared to Ethereum Mainnet.

Through comprehensive testing—ranging from scalability and data integrity to functional performance and cost analysis—GARV-BI has proven to be a secure, scalable, and interoperable solution for academic institutions worldwide. By open-sourcing the framework, GARV-BI fosters global adoption and innovation, encouraging institutions to implement, modify, and improve the system. This aligns with the framework's mission of establishing a global standard for the secure and decentralized verification of academic credentials, adhering to legal and privacy standards like GDPR.

Ultimately, GARV-BI presents a future-proof solution to the challenges of credential fraud, data privacy, and interoperability, positioning itself as a leading framework in the realm of academic credential verification.

References

1. Abed, S.I., Albeltaji, O.S., and Alnabriss, H. (2024). Decentralized Storage Using Inter Planetary File System. Advances in Security Networks and Internet of Things, Springer Cham. https://doi.org/10.1007/978-3-031-49544-1_19

2. Arenas, R., and Fernandez, P. (2018). CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. IEEE International Conference on Engineering Technology and Innovation (ICE/ITMC), IEEE. https://doi.org/10.1109/ICE.2018.8436324
3. Badr, A., Rafferty, L., Mahmoud, Q.H., Elgazzar, K., and Hung, P.C.K. (2019). A Permissioned Blockchain-Based System for Verification of Academic Records. IEEE International Conference on Engineering Technology and Innovation (ICE/ITMC), IEEE. https://doi.org/10.1109/NTMS.2019.8763831
4. Berrios Moya, J.A. (2024). Blockchain Academic Credential Interoperability Protocol (BACIP): Enhancing Security, Privacy, and Interoperability in Verifying Academic Credentials. arXiv. https://doi.org/10.48550/arXiv.2406.15482
5. Brown, G.M., 2006. Degrees of doubt: legitimate, real, and fake qualifications in a global market. Journal of Higher Education Policy and Management, 28(1), pp.65-77. Available at: https://doi.org/10.1080/13600800500440789
6. Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper. https://ethereum.org/en/whitepaper
7. Capece, G., Ghiron, N.L., & Pasquale, F. (2020). Blockchain technology: Redefining trust for digital certificates. Sustainability, 12(21), 8952. https://doi.org/10.3390/su12218952
8. Eaton, S.E. and Carmichael, J.J., 2023. Are You for Real? Lessons for the Academy About Professors with Fake or Fraudulent Degrees. In Fake Degrees and Fraudulent Credentials in Higher Education. Springer. Available at: https://doi.org/10.1007/978-3-031-21796-8_12
9. Ghazaliand, O. and Saleh, O.S., 2018. A Graduation Certificate Verification Model via Utilization of the Blockchain Technology. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). Available at: https://jtec.utem.edu.my/jtec/article/view/4707
10. Grolleau, G., Lakhal, T. and Mzoughi, N., 2016. An introduction to the economics of fake degrees. Journal of Economic Issues, 50(2), pp.492-508. Available at: https://doi.org/10.1080/00213624.2008.11507173
11. Michoulis, G., Nousias, N., Basagiannis, S. and Petridou, S.G., 2020. Verification of Academic Qualifications through Ethereum Blockchain: An Introduction to VerDe. In: XIV Balkan Conference on Operational Research, Thessaloniki, Greece, September 2020, pp. 429-433. ISBN: 978-618-85079-0-6. Available at: https://www.researchgate.net/publication/344037052_Verification_of_Academic_Qualifications_through_Ethereum_Blockchain_An_Introduction_to_VerDe
12. MIT Media Lab (2016). Blockcerts and the Digital Certificates Project. MIT Digital Currency Initiative. https://dci.mit.edu/dci-news/digital-certificates-project
13. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
14. Nadeem, N., Hayat, M.F., Qureshi, M.A., Majid, M., Nadeem, M., & Janjua, J. (2023). Hybrid Blockchain-based Academic Credential Verification System (B-ACVS). Multimedia Tools and Applications, 82, 43991-44019. https://doi.org/10.1007/s11042-023-14944-7
15. Partala, J., Nguyen, T. H., & Pirttikangas, S. (2020). Non-Interactive Zero-Knowledge for Blockchain: A Survey. IEEE Access. DOI: 10.1109/ACCESS.2020.3046025
16. Preukschat, A., & Reed, D. (2021). Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. Manning Publications. Electronic ISBN:9781617296598
17. Strehle, E. (2020). Public vs. Private Blockchains. Blockchain Research Lab. https://www.blockchainresearchlab.org/wp-content/uploads/2020/05/BRL-Working-Paper-No-14-Public-vs-Private-Blockchains.pdf
18. Tang, Q. (2021). Towards Using Blockchain Technology to Prevent Diploma Fraud. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3137901
19. W3C (2022). Decentralized Identifiers (DIDs) v1.0. World Wide Web Consortium. https://www.w3.org/TR/did-core/#brief-architecture-overview-longdesc

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.