IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 September 2023, accepted 28 September 2023, date of publication 5 October 2023, date of current version 11 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3322359

RESEARCH ARTICLE

Trustworthy Healthcare Professional Credential Verification Using Blockchain Technology

AYSHA ALNUAIMI[1], DIANA HAWASHIN[2], RAJA JAYARAMAN[1], KHALED SALAH[2], (Senior Member, IEEE), AND MOHAMMED OMAR[1]

[1]Department of Industrial and Systems Engineering, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates
[2]Department of Electrical Engineering and Computer Science, Khalifa University of Science and Technology, Abu Dhabi, United Arab Emirates

Corresponding author: Raja Jayaraman (raja.jayaraman@ku.ac.ae)

This work was supported by the Khalifa University of Science and Technology under Award CIRA-2019-001.

ABSTRACT Healthcare credentialing plays a vital role in ensuring the competence and integrity of healthcare professionals. However, the current credentials verification process suffers from time-consuming procedures due to the large number of intermediaries, limited information access, data fragmentation and the persistent risk of fraudulent credentials, leading to delayed hiring, increased administrative burden, and loss of trust and reputation in the healthcare system. In this paper, we utilize blockchain technology to enhance the credentialing process by streamlining the verification steps, improving data security, and providing stakeholders with confidence through secure storage of credentials. In addition, we utilize advanced security techniques, such as proxy re-encryption and cryptographic algorithms, to ensure the protection of sensitive data, facilitate secure communication, and prevent unauthorized access. We develop smart contracts which eliminate the need for intermediaries, automate the verification process, and enhance transparency and data integrity. We present system architecture, sequence diagrams, entity relationship diagrams, and the underlying algorithms of our blockchain-based solution. We discuss how our proposed solution attains the objectives outlined in the paper. We conduct cost evaluation and security analysis to validate the effectiveness of our solution. Additionally, we compare our proposed system with existing blockchain-based solutions, highlighting its novelty. The code of our smart contracts is made publicly available on GitHub.

INDEX TERMS Blockchain, Ethereum, credentialing, healthcare, smart contracts.

I. INTRODUCTION

The significance of credentialing has grown considerably in recent years, exerting a profound influence on the healthcare sector. It has become essential for healthcare workers to possess the appropriate qualifications and relevant medical experience before being granted access to healthcare facilities. Professional credentialing assumes a paramount role as healthcare facilities undertake a critical evaluation of healthcare providers, including physicians, dentists, and allied healthcare professionals, to ascertain their professional qualifications, training, and licensure prior to integrating them into their network. This vital safety measure ensures that these providers are authorized to administer patient treatment, contingent upon the submission of verifiable evidence substantiating their requisite degrees, certifications, and licenses [1], [2], [3].

Moreover, the importance of medical credentialing has grown significantly as healthcare organizations actively seek avenues to enhance patient safety, reduce costs, and protect their institutions from potential harm. By diligently assessing and confirming the qualifications of healthcare professionals, organizations can safeguard themselves against various liabilities, such as financial losses, the presence of incompetent healthcare providers, compliance breaches, and the looming threat of legal action. Additionally, establishing awareness of a doctor's credentials can foster a stronger patient-provider relationship. Otherwise, patients may hesitate to place complete trust in their chosen healthcare providers. Therefore, credentialing plays an indispensable role in reassuring patients about the competence and expertise of their healthcare professionals, empowering them to place

The associate editor coordinating the review of this manuscript and approving it for publication was Binit Lukose.

their trust with confidence in the providers they have selected [4].

The healthcare sector has experienced significant difficulties in recent years when it comes to assuring the authenticity and trustworthiness of credential verification for healthcare workers. Traditional methods of authenticating credentials, which rely on centralized authorities and paper-based documentation, have proven to be time-consuming, inaccurate, and non-transparent [5]. As a result, incidences of credential fraud and unlicensed practice [6] have emerged as severe dangers, threatening patient safety and eroding healthcare service integrity.

The primary motivation behind this work is the necessity for a comprehensive solution that concentrates on enhancing efficiency and streamlining processes to save valuable time and resources. The utilization of blockchain-based healthcare credential verification systems serves to boost confidence, simplify procedures, and minimize the risks connected to counterfeit or invalid credentials. It is crucial for the solution to enhance trust, and transparency, and ensure traceability throughout every step of the credentialing process. Furthermore, improving data security is imperative to protect sensitive information and comply with regulations. Additionally, facilitating seamless communication channels internally and externally is essential for fostering easy collaboration among team members and stakeholders.

The healthcare industry has shown great interest in blockchain technology, recognizing its potential to enhance various aspects of medical services. Numerous articles, including those by [7], [8], [9], [10], and [11], have highlighted the potential advantages of blockchain in improving healthcare systems. Specifically, the verification of credentials is an area within healthcare that can greatly benefit from blockchain technology.

By utilizing blockchain, a secure and unchangeable platform can be created for storing and managing credentials, while also improving privacy and data security. The Media Lab at MIT has been conducting experiments with blockchain technology in relation to digital certificates. Through their initial experiments, they have gained several valuable insights, including addressing the challenges associated with today's credentials is not a straightforward task and does not have a simple solution [12]. Moreover, managing public and private keys for authentication purposes, both for the issuer and the recipient, proves to be a more complex endeavor. The issue of privacy and granting users control over who can access and review credentials within the network presents a significant challenge [9]. Furthermore, in [10], the authors suggest that Blockchain technology can be utilized to create a ''smart contract'' for credentials. This means having a single, constantly updated database where all credential information is stored. Instead of searching multiple repositories for this data, it can be easily accessed in real-time, saving time and costs associated with repetitive credentialing processes. However, there is no technical proposed solution with detailed implementation using smart contracts is demonstrated.

Despite the recognized potential of blockchain in enhancing credentials verification, there is a lack of a comprehensive technical solution that effectively integrates blockchain into traditional credentialing methods, particularly in healthcare. The specific steps and stakeholder interactions are also unclear, limiting understanding of the technical complexities involved. A Blockchain-based healthcare credential verification system shows promise in boosting confidence, streamlining procedures, and mitigating risks related to counterfeit or invalid credentials.

This paper presents a blockchain-based solution that aims to establish a transparent and trusted system for sharing, securing, and verifying healthcare professionals' credentials. Our research aims to address and provide insights into the following key research questions:

Q1: How can blockchain technology overcome the existing issues with the current solutions?

Q2: What are the system elements and actors that contribute to the successful implementation of blockchain-based credential verification systems, ensuring enhanced confidence and mitigating risks associated with counterfeit or invalid credentials?

Q3: What is the sequential flow of interactions between the key stakeholders and blockchain-based system during the validation of licenses and certifications?

Q4: What aspects of the credentialing system does the blockchain-based solution enhance, including the practical implications associated with its implementation?

The Design Science Research Methodology is applied to our proposed solution [13]. First, the issue is recognized where there is a need for a technical blockchain-based solution with its implementation details for verifying healthcare professionals' credentials. Second, the paper's primary objective is outlined which is designing and implementing a blockchain-based solution that can be used as a transparent and trusted system for sharing, securing, and verifying healthcare professionals' credentials. Then, the proposed solution's design is planned and produced. Next, the solution is developed and tested. Finally, the proposed solution is evaluated, and based on the evaluation results, the process is iterated. Our main contributions in this paper can be summarized as follows:

- We propose a solution for managing and tracing healthcare professionals' credentialing in a decentralized, automated, and trustworthy manner using private Ethereum blockchain.
- We present a comprehensive demonstration of the system architecture, illustrating the interaction and collaboration of key elements and actors within the proposed solution.
- We utilize Proxy Re-Encryption Network for preserving data privacy and protecting the confidentiality of credentials.

- We develop smart contracts that eliminate intermediaries, automate verification, and elevate transparency and data integrity, accompanied by detailed algorithms depicting the underlying logic.
- We evaluate the performance of our proposed solution and demonstrate the enhancement of process management, access control, accountability, and data integrity. We conduct security and cost analyses for our smart contracts, validating the effectiveness of our solution.

The remainder of the paper is organized as follows. The related work is described in Section II. Section III describes the proposed blockchain-based solution for managing healthcare professionals' credentialing. The proposed solution's implementation, testing, and validation are described in Sections IV and V. In Section VI, we evaluate the performance of our solution, and we conduct a security analysis of the developed smart contracts. The results, limitations, and concluding remarks are summarized in Section VII.

II. RELATED WORK

In this section, we present the traditional process flow of credentialing. Additionally, we provide a brief introduction to blockchain technology and its features. Furthermore, we present existing blockchain-based solutions proposed for credential verification and discuss recent studies on data privacy in healthcare. Lastly, we summarize the issues related to these existing solutions and the research gap that this paper aims to fill.

A. TYPICAL PROCESS FLOW OF CREDENTIALING

Credentialing is when a healthcare provider's credentials and license are checked and evaluated to ensure they are in good standing. Once an applicant starts a new credentialing application, it will go through multiple steps. Figure 1 shows a typical process flow of the traditional credentialing method followed in case a new applicant aims to join a healthcare facility. It starts when the healthcare professional applies to the healthcare facility and attaches all requested supporting documents such as board certification, education, ongoing training, hospital affiliation, Drug Enforcement Agency (DEA) license, and malpractice insurance [14]. Then the healthcare facility conducts a primary source verification after the completed application is received. Determining whether a physician can legally practice in a facility is necessary. In that stage, the healthcare facility contacts the primary sources of the submitted documents to verify their authenticity. Primary source verification (PSV) can be accomplished in different ways; some organizations manually carry out the process, requesting relevant documents and information mailed, faxed, or emailed to the primary source and awaiting responses. In addition, PSV is being completed electronically by organizations. In fact, according to a recent study, 83% of healthcare organizations have automated their PSV processes completely or partially [15]. After the PSV is done, the results are sent to the medical staff service department, where these results will be analyzed and discussed with medical staff leaders to prepare a green-lighted practitioner's file. Finally, it is sent to the final decision makers: the evaluation committees that consist of the credentialing committee, executive medical committee, and the hospital governing board. The evaluation committees review the submitted file to decide on the credentialing status of the applicant [16].

B. BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed, shared, and tamper-resistant timestamp ledger of blocks that are used to store and share data [21]. There are several key elements of blockchain that make it a powerful technology, such as distributed ledger, immutable records, and smart contracts. All participants in a network have access to the records of transactions in the distributed ledger. These records are immutable and recorded only once; however, if they include any errors, then a new transaction will be added to solve that error, and both transactions will be visible [22]. A smart contract is a computer-based exchange convention that puts an agreement's terms into effect. The basic goal of a contract is to prevent unintentional and malicious exceptions in payment conditions, integrity, liens, and enforcement [23]. Therefore, blockchain has many advantages, such as transparency, immutability, decentralization, and persistence [24]. Furthermore, blockchain technology can be categorized into two main types, public and private. In a public blockchain, anyone can participate in the consensus mechanism. The whole public blockchain system is visible and transparent, and each participant's identity is kept pseudo-anonymous. On the other hand, private blockchain can be accessed only by pre-approved participants. The combination of public and private advantages leads to a hybrid type called consortium blockchain [25]. Blockchain technology has demonstrated its capacity to revolutionize conventional industries, such as insurance [24], healthcare [26], and supply chain [27].

The authors in [13] proposed a blockchain-based architecture for decentralized Internet of Medical Things (IoMT) healthcare systems. The architecture combines blockchain with a distributed data storage system, ensuring low latency, high security, and privacy. It provides automated medical services and facilitates digital agreements among stakeholders, ensuring traceability and data privacy. Moreover, in [29], they implemented Fortified-Chain 2.0, a decentralized smart healthcare system that enhances security, privacy, and trust. The system includes a distributed Machine Learning module for real-time patient health monitoring, showing impressive performance in low latency and high throughput. Yet, the integration of a distributed machine learning module introduces challenges related to achieving and maintaining model consistency across decentralized healthcare nodes.

C. BLOCKCHAIN-BASED SOLUTIONS PROPOSED FOR CREDENTIAL VERIFICATION

The article in [30] explores the potential of blockchain, specifically the Ethereum blockchain, in transforming the verification process of educational credentials. With

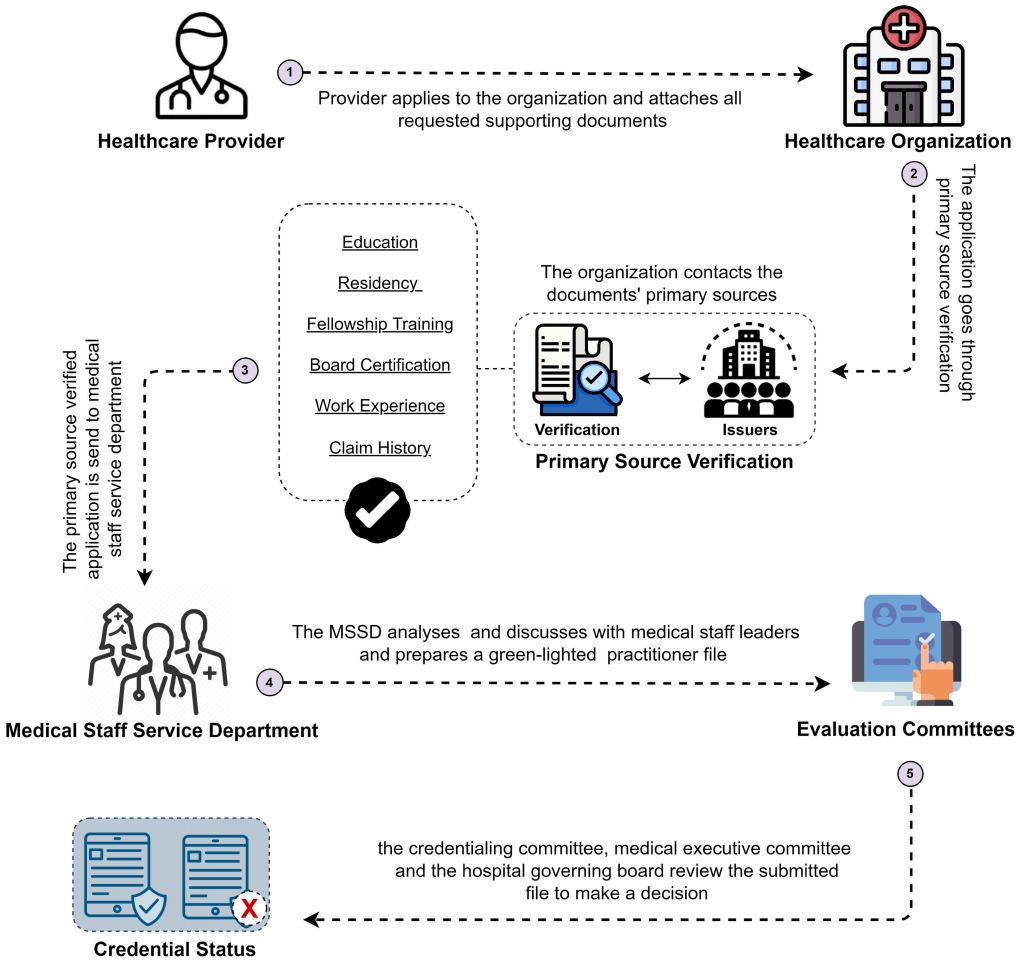

FIGURE 1. Typical process flow of healthcare professional credentialing.

approximately 10% of applicants falsifying their educational backgrounds, the authors propose a solution that leverages blockchain's decentralized nature to securely store academic credentials on users' personal devices. The immutable nature of the blockchain ledger ensures document integrity, making tampering impossible. This innovative approach holds great promise in enhancing trust and authenticity in credential verification. Nevertheless, since this method relies on the scanning of QR codes, there exists a chance of QR code spoofing.

Moreover, in [31], the authors focused on the implementation of blockchain technology, specifically hyperledger fabric, to address the complex processes of degree attestation verification and traceability between the Higher Education Commission (HEC) and universities. The proposed architecture provides a detailed design for degree attestation verification and a traceable direct channel between the HEC and universities. However, Fabric's permissioned nature limits transparency in Hyperledger projects [32]. Despite that the adoption of this system eliminates the need for manual verifications and physical submission, streamlining the verification process between the HEC and universities, there is a potential concern regarding data authenticity in this approach due to the direct uploading of files to IPFS. Additionally, the intricate architecture of this solution, when contrasted with Ethereum-based alternatives, introduces complexity to its adoption process [33].

In [20], the authors proposed a Blockchain-based solution, CredenceLedger, which is a system that saves compact data proofs of digital academic credentials in Blockchain ledger that are easy to be verified by education stakeholders and interested third-party organizations. This software platform is built on Multichain with the inclusion of the CredenceLedger mobile application, giving students the option of getting a valid digital version of their credentials in addition to the paper-based versions. The digital credentials are protected by Blockchain's built-in security features, which means that interested third parties will only have access to limited information (compact data proofs). Other information is encrypted and will be made available only upon request and with the recipient's consent. However, this study exhibited limited elaboration on design details and implementations.

The authors in [34] present a blockchain-based learning credential verification system in which a credential recipient can regulate the quantity of credential-related information revealed throughout the verification process. Using a Merkle tree, the suggested approach encodes the causal link between the credential's constituent bits of information. The abstract data model constructed on top of the binary Merkle tree has been developed so that a receiver can choose to reveal a portion of the credential information, including the recipient profile. This approach might require substantial resources and time due to its intricate nature.

In [37], the authors proposed a blockchain-based approach for IoT-enabled healthcare systems based on Mobile Application (MA) to create a privacy-preserving environment. The suggested approach promotes preventing unauthorized access to medical certificates and maintenance. Furthermore, it expedites the verification of a physical certificate and prohibits illegal access to birth, death, and sick leave information. Reference [38] presented CredChain, a blockchain-based decentralized application (DApp) that facilitates the issuance and storage of digital credentials. A user can redact information from a shared credential to protect their privacy without affecting the credential's use. Further, the verifier's access may be restricted by setting a time restriction for each sharing instance. Nonetheless, a notable challenge arises from the possibility of elevated storage costs, attributed to the storage of all files on the blockchain. The authors in [39] manage identities with the help of smart contracts and Ethereum accounts. Credentials are hashed and stored on the Ethereum blockchain.

The authors in [40] proposed a blockchain-based credential verification system to address the shortcomings of the traditional paper-based credential and certification system. The concept is to implement a decentralized blockchain network that provides a verification interface for the storage and processing of digital certificates. In this system, as the issuer holds the responsibility for generating and uploading credentials directly to a decentralized storage system, it might raise concerns regarding data privacy, conformity, and even potential security vulnerabilities. Despite these considerations, the proposed solution offers noteworthy advantages, including high transaction throughputs, low costs, and resource efficiency.

In [41], the authors proposed a decentralized accreditation system that includes digital certificate issuance, verification, and validation utilizing blockchain technology. The certified document provided by the student to employers includes a QR code and a unique number, which respective authorities would use to verify the certificate. However, it does not take into consideration the storage limitations of blockchain. While it proves that the certificate is signed by the university, it does not verify that the employee interacting with the employer is the actual certificate holder. Additionally, the implementation of the proposed system is missing, and therefore, the visibility and limitations are not adequately evaluated.

The authors in [42] introduced a permissionless blockchain ecosystem primarily built upon Ethereum. This solution doesn't primarily focus on the credentialing process; instead, its primary purpose is to enable Higher Education Institutions (HEI) to register the certificates they issue on the blockchain. This is achieved through the use of Consortium and HEI smart contracts, complemented by three applications: two intended for Higher Education Institutions and one for recruiters. The HEI client registers certificates, the Recruiting App verifies them via HEI's smart contract, and the Consortium App enables interaction and voting among consortium members. However, clients upload files directly to IPFS, and there is unrestricted access to the returned hash by anyone connected to the IPFS network, leading to potential access control issues.

D. PRIVACY IN HEALTHCARE SECTOR

Several methodologies have been proposed to address the privacy and security concerns in the healthcare industry.

In [44] the authors have presented a solution to the challenge of privacy by introducing a practical privacy-preserving single-layer perceptron scheme, called PSLP, which is based on the Paillier homomorphic cryptosystem. The proposed Protocol (PSLP) involves the outsourcing of confidential medical data by a hospital to the cloud in encrypted form. Subsequently, the cloud can perform privacy neural network training to derive the disease model.

The authors of [45] investigate the feasibility of utilizing identity-based and attribute-based cryptosystems in cloud computing for secure data sharing, re-encryption, broadcasting to multiple users, and similarity matching over cipher-texts. This study proposes an effective mobile health (mHealth) application that utilizes a well-suited set of schemes. The application enables secure sharing of patients' health records among healthcare providers and patients. Additionally, the application facilitates the identification of friends who are experiencing similar symptoms through the use of private data matching methods. The proposed system ensures data integrity and privacy preservation.

In [46], a secure, privacy-preserving, bidirectional access control scheme with fine granularity (PBAC-FG) is proposed. The PBAC-FG leverages fine-grained access control and matchmaking encryption technologies to ensure that both participants (e.g., patients and healthcare providers) can specify their respective fine-grained access control over the encrypted health data, so that only authorized counterparts can access the health data efficiently.

E. EXISTING CHALLENGES IN CREDENTIALING PROCESS AND RESEARCH GAP

The existing typical approach shown in Figure 1 is expensive and time-consuming, often requiring between four and six months to complete [14]. This lengthy procedure is prolonged even further when done manually since errors are more likely to occur, which may further reduce the

TABLE 1. A summary of the existing proposed solutions.

Related Work	Proposed Solution	Sector	Main Features	Platform	Code Implemtaion	Main Challenges\Limitations
[29]	Decentralized Smart Healthcare System	Healthcare	Privacy, Security, Traceability, Low Latency	Hyperledger Fabric	Yes	Model consistency challenge, Lack of data authenticity
[30]	Education and Employment Verification	Education	Trust, Authenticity	Ethereum	No	Possibility of QR code spoofing, Lack of research implementation
[31]	Degree Attestation and Verification Traceability for Higher Education Commission	Education	Privacy, Security, Traceability, Authenticity	Hyperledger Fabric	Yes	Lack of data access control, Missing stages from credentialing process
[20]	Verifiable Academic Credentials	Education	Access control, Security, Centralized databases	NA	No	Lack of research implementation, Limited design details
[34]	Credential Verification System	Education	Access control, Privacy	Ethereum	No	Intensive and time-consuming, Lack of research implementation
[36]	Accreditation and Degree Verification System	Education	Resilience, Authenticity, Privacy	Ethereum	No	Possibility of QR code spoofing, Lack of access control
[37]	Medical Certificate Generation and Verification	Healthcare	Privacy, Security, Tracking	Ethereum	Yes	Lack of data authenticity
[38]	Verifiable Credentials	Education	Security, Traceability	Ethereum	Yes	High storage cost, Data consistency challenge
[39]	Secure Sharing of Students Credentials	Education	Security	Ethereum	Yes	Lack of applicant data privacy, Limited design details
[40]	Educational credential verification	Education	Traceability, Scalability	Ethereum	Yes	Lack of data privacy and conventionality, Limited design details
[42]	Verifiable Qualifications	Education	Authenticity, Integrity	Ethereum	Yes	Lack of data access control

healthcare organization's productivity and efficiency [17]. In addition, it may cause significant delays in filling critically important healthcare positions and in the ability of healthcare workers to begin work [18] and offer their services to patients. In addition, organizations that manually process their data may experience an error rate of up to 85% due to human oversights. Simple details such as names, dates, and locations may be incorrect or absent, resulting in significant consequences. These mistakes and errors can negatively affect the accuracy of credentialing, leading to the inclusion of unqualified providers in the network, which can negatively affect the esteem and reputation of an organization.

Furthermore, using fake documents has been a problem for many years, as many candidates embellish their qualifications to make their resumes more attractive to potential employers. According to a study, more than a third of job applicants admit to falsifying or ''boosting'' their qualifications for a job application [19]. Forging 'paper-based' documents to produce replicas of the authentic or official copies can be done in just a couple of hours. At worst, in the absence of a security mechanism in place, fraudulent copies of 'digital-based' credentials can be fabricated at enormous speed. While it is easy to counterfeit credentials almost instantaneously, verification of authenticity is more challenging [20]. Moreover, background checks are one of the most critical aspects of the credentialing process. They ensure that each candidate complies with national licensing standards. Organizations must ensure that all information about prospective candidates and applicants is secure, private, and confidential. The organization may be subject to hefty fines and sanctions in the event of misinformation [17].

Table [1] summarizes the existing proposed solutions, including their respective sectors, main features, challenges/limitations, and whether they have been implemented with code. The existing contributions centered around blockchain technology highlight its potential for enhancing credentials verification process, particularly in the education sector. However, it is important to note that most of these contributions lack code implementation. Specifically, there is a noticeable absence of a detailed technical solution that effectively incorporates blockchain into traditional methods of establishing credentials, particularly within the healthcare sector, as well as the lack of clarity regarding the specific steps and interactions among key stakeholders involved, which limits the understanding of the technical complexities involved in implementing blockchain technology.

Moreover, the healthcare sector presents unique challenges and complexities, particularly when it comes to privacy and confidentiality concerns surrounding credentials data. As a result, there is a research gap in understanding how to effectively incorporate off-chain storage, proxy re-encryption, and digital signatures within the healthcare context. While blockchain technology has been explored in other sectors like education, its application and adaptation to address the specific needs of healthcare credentialing and data security are less explored. This research aims to fill the gap by investigating and developing a solution that leverages off-chain storage, proxy re-encryption, digital signatures, and blockchain technology in conjunction to enhance privacy and security in healthcare credentialing processes, ultimately ensuring the integrity and confidentiality of credentialing information.

In light of the identified research gap, the main objectives of this paper are to propose a technical solution that effectively incorporates blockchain technology into healthcare credentialing, integrating off-chain storage, proxy re-encryption, and digital signatures, and to provide a clear understanding of the steps and interactions among key stakeholders involved, thus addressing the technical complexities and privacy concerns in the healthcare sector.

III. SYSTEM DESIGN

In this section, we introduce a blockchain-based solution for managing and tracing healthcare professionals' credentialing in a decentralized, automated, and trustworthy manner. The system is built on a private Ethereum blockchain that only authorized entities can access.

Figure 2 illustrates the high-level system architecture of our proposed blockchain-based solution. The developed system will help verify healthcare professionals' credentials to ensure they are qualified to practice medicine. The signature feature will make primary source verification much easier and faster. Our system consists of two smart contracts that authorized actors can access through frontend Decentralized Applications (DApps). The registration smart contract can be deployed by the regulatory authority to register the authorized entities. The data validation smart

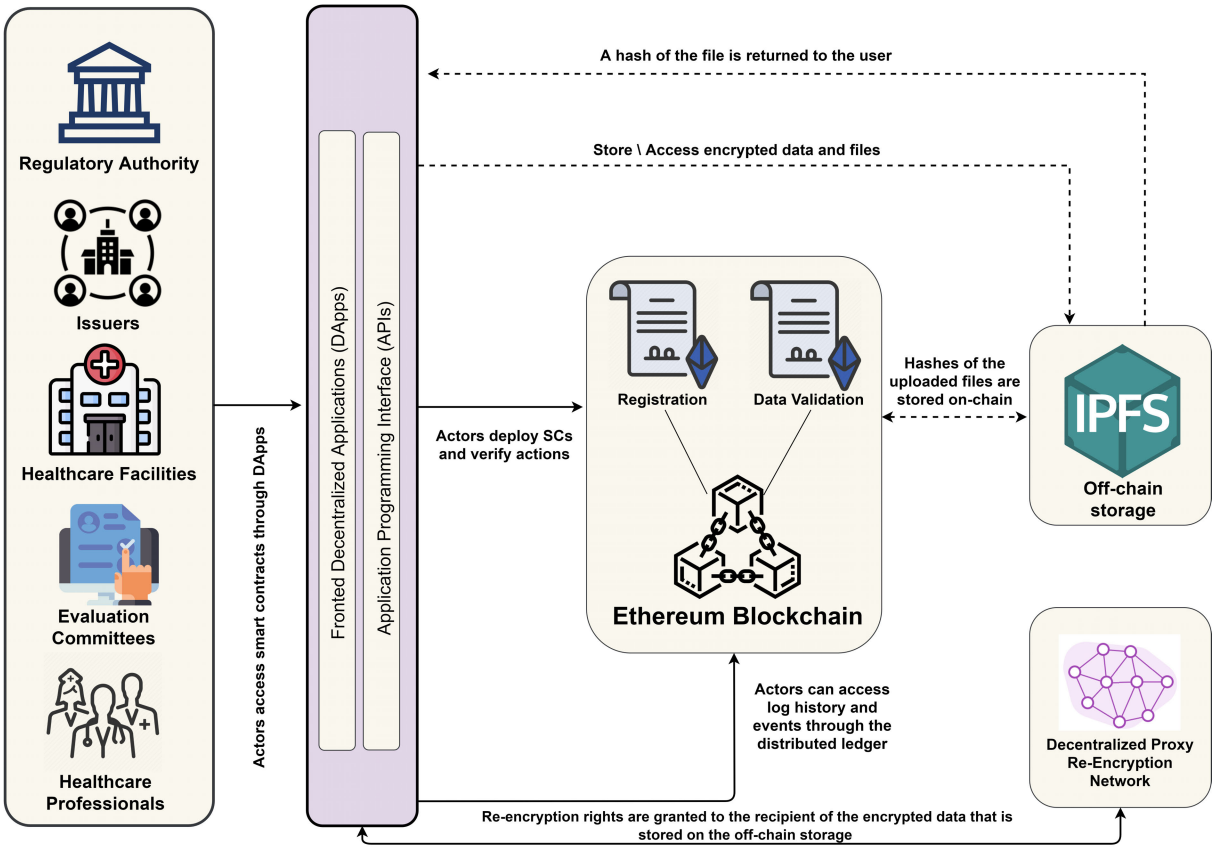

FIGURE 2. High-level system architecture of the credentialing healthcare professionals using Ethereum smart contracts.

contract will include the three phases of credentialing; the application, primary verification, and final evaluation. Moreover, it has RPC and Web3 as application programming interfaces (API). These APIs can connect the two smart contracts to the software devices that can access them (Dapps). Applicants also use IPFS, an off-chain storage system, to store large-size documents. The components of the proposed solution are described below:

- **Actors:** The main stakeholders of the system are the regulatory authority, healthcare professionals, healthcare facilities, and evaluation committees. Each of these actors will conduct their corresponding functions in the smart contracts and will have access to the information stored on/off-chain.
- **Decentralized Storage Systems:** The proposed solution is integrated with off-chain storage, Interplanetary File System, where stakeholders can store large-size files in low-cost storage rather than directly on the blockchain. The applicant can upload and store all requested documents for credentialing on the IPFS, where a unique cryptographic hash is created for the uploaded file, which is stored on the blockchain and accessed via the smart contract. If any of the uploaded files are altered in any way, the corresponding hash will change to reflect the change.
- **Ethereum Distributed Ledger:** The Ethereum Blockchain is the distributed ledger that permanently stores all transaction logs and events. These transactions are recorded in a tamper-proof manner. Thus, it ensures transparency, traceability, and accountability in the credentialing validation process. In addition, limiting public access to transactions and data using private permissioned blockchain will add more security, privacy, and confidentiality to the system.
- **Ethereum Smart Contracts:** We develop two smart contracts: registration and data validation. The registration smart contract is deployed by the regulatory authority, responsible for registering all entities to give them permission to access the system. While the data validation smart contract is responsible for the three phases of credentialing; credentialing application, primary source verification, and final evaluation.
- **Decentralized Proxy Re-Encryption Network (DPRN):** The principle of proxy re-encryption is to permit private and secure data exchange between multiple parties. It enables data owners to offer access to particular entities without sharing the decryption key, since a third-party proxy can transfer encrypted data from one encryption key to another without revealing the original data.

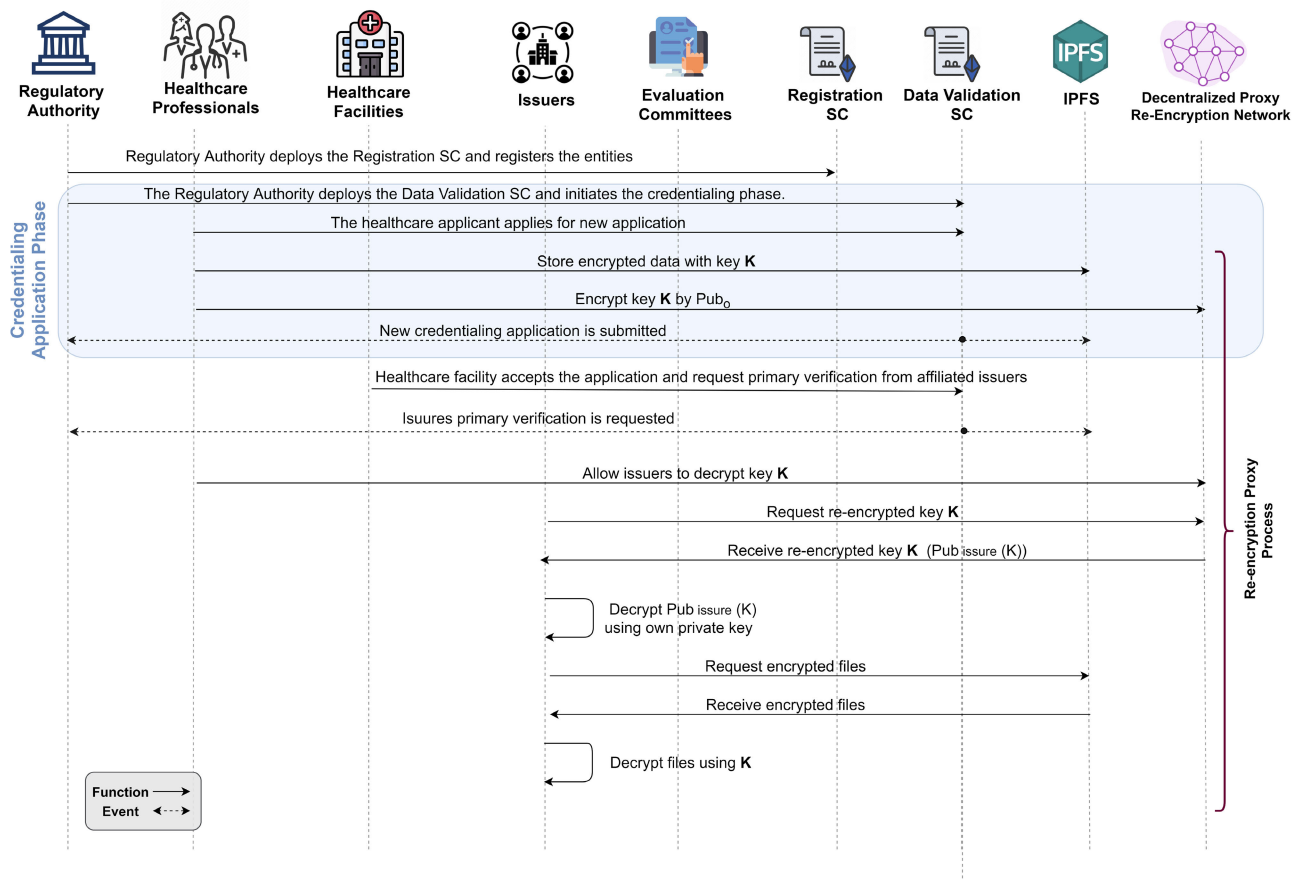

FIGURE 3. Sequence diagram stakeholder interactions in the credentialing phase and re-encryption proxy process.

A. SYSTEM ELEMENTS INTERACTIONS

The interactions among the stakeholders, smart contracts, and storage systems are represented in this subsection.

The sequence of all interactions in the proposed system is shown in Figure 3 and Figure 4. The process starts with deploying the registration smart contract by the regulatory authority to register the authorized healthcare facilities, authorized documents' issuers, and assigned evaluation committees. Then the data validation smart contract is also deployed by the regulatory authority to initiate the credentialing phase, and the healthcare applicant creates an account to start a new application. Once the account is created, the applicant submits the new application. A symmetric key is utilized to encrypt the healthcare applicant files and data before it is stored on IPFS where both the key and the encrypted data are kept, however, the symmetric key is also encrypted before storing it on the IPFS. The smart contract stores the hash of the encrypted data on-chain. Once the application is submitted and accepted by the healthcare facility, they initiate a request to the issuers for primary source verification. This request is transmitted as an event, notifying all relevant issuers to commence their respective tasks. However, the data owner, a healthcare professional, creates a new key using own private key and issuer's public key. The proxy network receives this new key for the re-encryption process. When issuers need access to the IPFS file content, they interact with the re-encryption proxy network by requesting and receiving the re-encrypted key. Finally, the issuers can decrypt the received Key using their own private key to get the Key which is used to decrypt the needed files. The privacy and security of the data being transported are ensured by utilizing this technique since the proxy can re-encrypt the message without having access to its content. Moreover, this proxy re-encryption utilizes the unidirectional scheme. This scheme is commonly applied in scenarios where a sender delegates the secure forwarding of messages to a recipient, and its full implementation details are explained in [47].

The healthcare facility sends an off-chain request to the issuers to sign a message confirming the issuance of the documents. Thus, if the issuers signed and approved the distribution of the documents within the time window, the signatures are successfully stored on the chain, and an event is sent. Otherwise, if the issuers fail to sign the message within the time window, the signatures fail to be stored, and an event is emitted. Then, the primary verification results are either accepted or rejected depending on the number of signatures received; if all documents are verified by the issuers, then

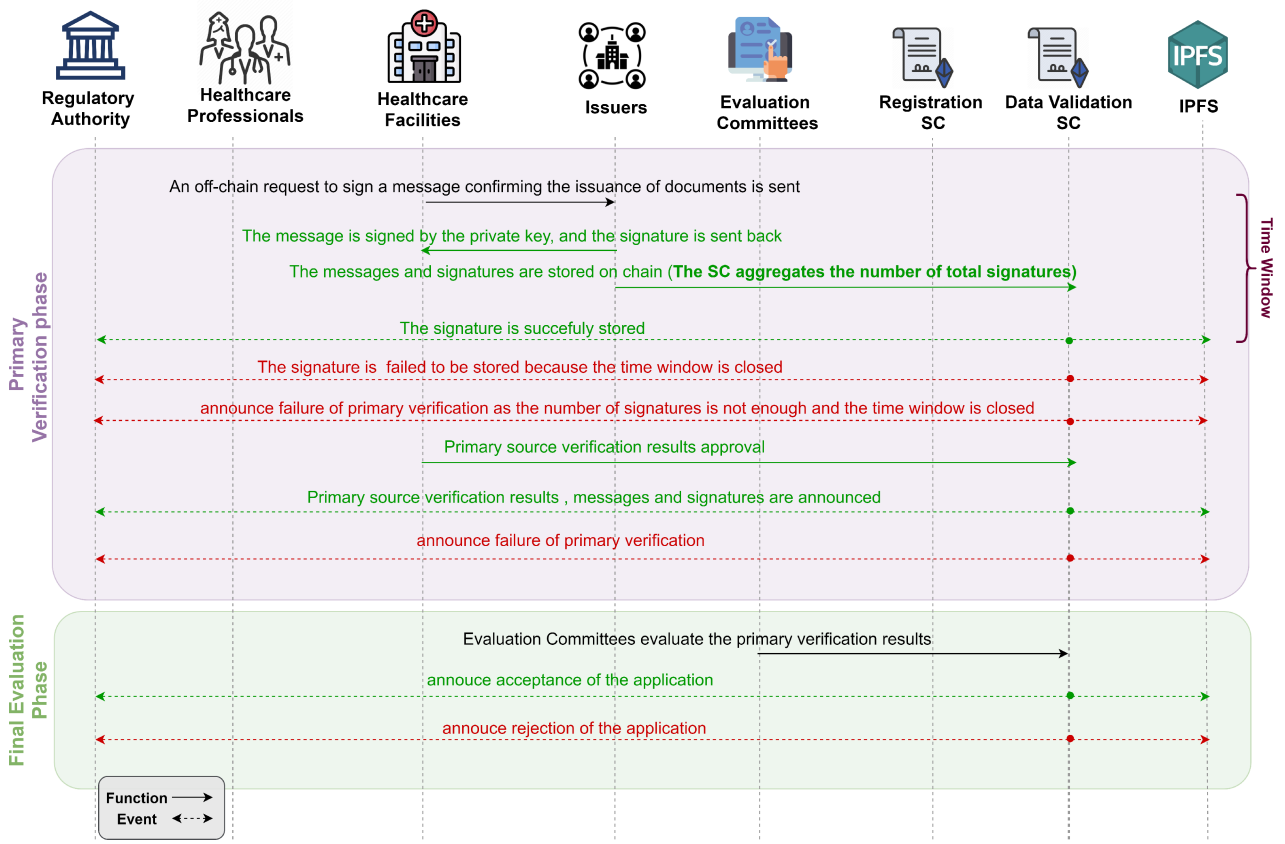

FIGURE 4. Sequence diagram stakeholder interactions in the primary verification and final evaluation phases.

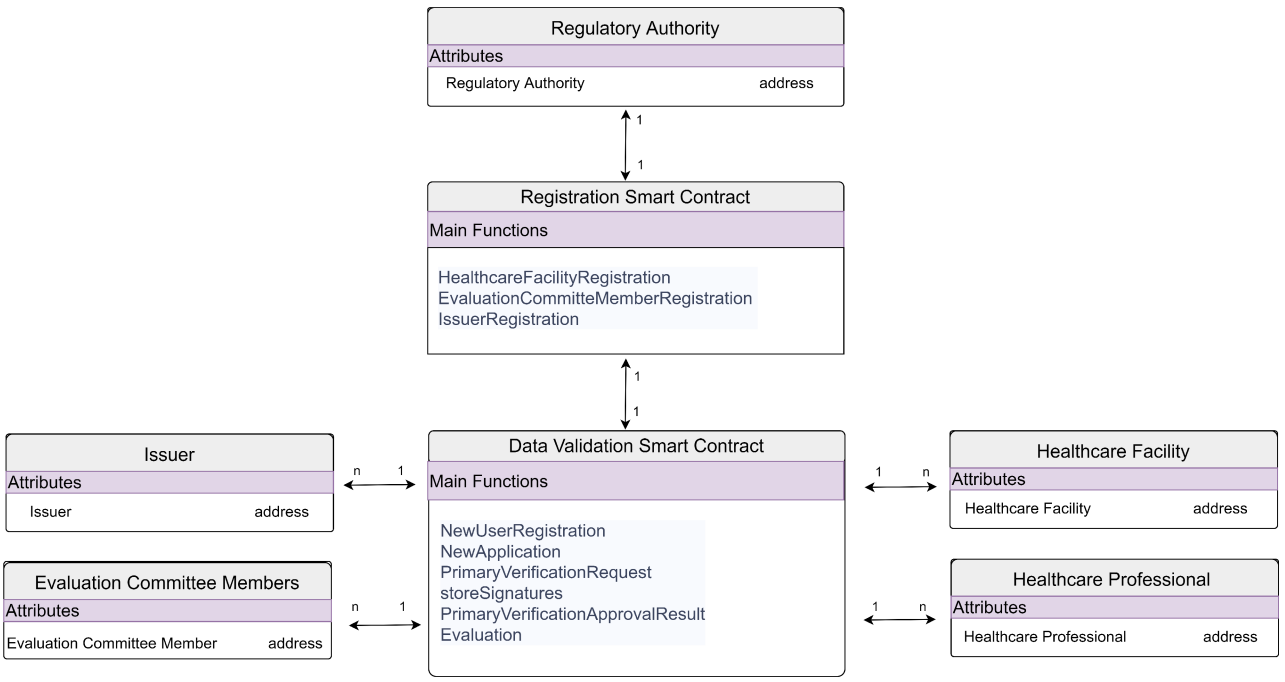

FIGURE 5. Entity-relation diagram of smart contacts and participants.

Algorithm 1 Registration

Input: *UserEA*

UserEA: The Ethereum address of a new entity, either a new Issuer, a new healthcare facility, or a new evaluation committee member
if *caller* == *regulatory_authority* ∧ *(HealthcareFacility[UserEA] = false)* **then**
    HealthcareFacility[*UserEA*] = True
else
    Revert contract state
end
if *caller* == *regulatory_authority* ∧ *(EvaluationCommitteMember[UserEA] = false)* **then**
    EvaluationCommitteMember[*UserEA*] = True
else
    Revert contract state
end
if *caller* == *regulatory_authority* ∧ *(Issuer[UserEA] = false)* **then**
    Issuer[*UserEA*] = True
else
    Revert contract state
end

Algorithm 2 New Application

Input: *IPFShash*, *ApplicantID*, *UserEA*

IPFShash: Is the generated hash that is returned to the user after uploading a document to the IPFS
ApplicantID: Is the identity document of the applicant
UserEA: Is the Ethereum Address of a user
ApplicantApplicationNumberMapping: Is a key-value pair that links the *ApplicantID* to the *ApplicationNumber*
ApplicationInfoMapping: Is a key-value pair that links the *ApplicationInfo* to the *ApplicationNumber*
if *healthcareprofessional[UserEA] = false* **then**
    healthcareprofessional[*UserEA*] = true
else
    Revert contract state
end
`/* A new healthcare professional is registered */`
if *caller* == *RegisteredHealthcareProfessional* **then**
    Increase *ApplicationNumber* by 1
    Update *ApplicantApplicationNumberMapping*
    Update *ApplicationInfoMapping*
    Update *ApplicationStatus* to Pending
    Emit an event announcing that new application is submitted
else
    Revert contract state
end
`/* A new application is submitted */`

it's approved and eligible for the final evaluation phase. Otherwise, it is rejected, and events are emitted. Finally, the application is evaluated by the authorized evaluation committees for the final decision, and events are sent to announce the approval or rejection of the application.

IV. IMPLEMENTATION DETAILS

This section presents the solution, and the detailed algorithms to explain the logic of each smart contract. The proposed solution is built on a private Ethereum blockchain, thus, the smart contracts' functions can be executed only by authorized entities.

Figure 5 illustrates the entity-relationship diagram between the actors and the two smart contracts. First, the regulatory authority interacts with the registration smart contract to register the main actors by executing the three main functions shown in the diagram. There is only one regulatory authority that is declared as an address. However, other entities are declared as mapped, meaning multiple healthcare facilities, issuers, and evaluation committees exist. The regulatory authority is the only one who deploys and interacts with the registration smart contract; thus, the relationship is 1 to 1. The data validation smart contract's main functions are listed in the figure, and the relationship between the actors and the smart contract is n to 1 as multiple actors are interacting with the smart contract. Different enumerating variables in data validation smart contract describes the different status of credentialing phases, such as Application State that shows the five states of the application; "Not Submitted", "Pending", "In Progress", "Approved" and "Rejected". Another enumerating variable is Primary Verification Approval State, which can be "Pending," "Approved," or "Rejected."

The regulatory authority deploys the registration smart contract, and all authorized entities are registered by executing their respective functions. The registered entity will eventually be allowed to perform its tasks in the Data validation smart contract.

A. ALGORITHMS

Algorithm 1 illustrates the registration of new issuers, healthcare facilities, and evaluation committee members. If the caller is the regulatory authority and the entity is not registered, then the Ethereum address will be added to the authorized entities. However, the registration of a new healthcare professional is described in Algorithm 2. The healthcare professional executes the function *NewUserRegistration* to create an account to submit a new credentialing application. After the registration step, the healthcare professional executes *NewApplication* function and enters the IPFS hash and the Applicant ID as inputs, then the counter *ApplicationNuber* is increased by 1, the *ApplicantApplicationNumberMapping* and *ApplicationInfoMapping* are updated. In addition, the *ApplicationStatus* is updated to be "Pending," and an event

Algorithm 3 Primary Verification Request

Input: *ApplicantID*, *durationtime*, *NeededsignaturesNumbers*

ApplicantID: Is the identity document of the applicant
durationtime: Is the time duration available for issuers to sign and verify the documents
NeededsignaturesNumbers: Is the minimum number of needed signatures that must be stored to approve the primary verification
if *(caller == RegisteredHealthcareFacility)* ∧ *(durationtime > 0)* ∧ *(NeededsignaturesNumbers > 0)* ∧ *(PrimaryVerificationApprovalStatus = Not Requested)* **then**
    Set *EndOfDurationtime = block.timestamp +* (*durationtime* * 1 days)
    Update *ApplicationStatus* to In Progress
    Update *PrimaryVerificationApprovalStatus* to Pending
    Emit an event announcing that new primary verifications are requested
else
    Revert contract state
end
`/* A New primary verification is requested */`

is emitted to announce that a new application has been submitted.

Once the credentialing application is submitted, it goes through the primary verification phase as it is illustrated in Algorithm 3. Where the *PrimaryVerficationRequest* function is executed by the registered healthcare facility and it is required that the *durationtime* and the *NeededsignaturesNumber* be >0. Moreover, to execute this function the *PrimaryVerificationApprovalStatus* should be ''Not Requested''. Thus, if the requirements are met, then the *ApplicationStatus* is updated to be ''In Progress'' and the *PrimaryVerificationApprovalStatus* is updated to be ''Pending'', and an event is emitted to announce that new primary verification is requested.

Algorithm 4 shows the issuer verification stage, where the issuer signs an off-chain message to confirm the issuance of a document and stores the signature on-chain. The *StoreSignatures* function is executed by the healthcare facility. In addition, it illustrates the message signing and verification process, in which the message is first hashed using the Keccak256 hashing algorithm. Then, The message hash is encrypted using the issuer' s private key, producing a unique hash. After that, the signature is sent to the healthcare facility to store the message and the issuer' s signature as confirmation of issuance, where recipients can use the sender's public key to confirm the authenticity of the provided signature [48]. The function that stores the message and signature runs a validity check to verify that the signature relates to the issuer. The verification process

Algorithm 4 Issuers Verifications

Input: *ApplicationNumber*, *Message*, *Signature*

ApplicationNumber: Is a unique number given to any new application
Message: Is a text message that the Issuer has to sign to verify a document
Signature: Is the induced outcome from signing a message
ThesignatureOwner: Is a key-value pair that links the *Signature* which is linked to the issuer EA to the *ApplicationNumber*
isApplcationIDSignedBy: Is a key-value pair, where the value is true if the application number is signed by a specific issuer, otherwise, the value is false
Apply keccak256(*Message*) to produce *hashA*
Encrypt *hashA* with the *RegisteredIssuer* private key to produce a unique *Signature*
Send the *Signature* and *message* to the *RegisteredHealthcareFacility*
if *(caller == RegisteredHealthcareFacility)* **then**
    if *(block.timestamp < EndofDurationtime)* ∧ *(signaturesCount < NeededsignaturesNumbers)* **then**
        Apply keccak256(*Message*) to produce *hashA*
        Decrypt the *Signature* using the *RegisteredIssuer* public key to produce *hashB*
        if *hashA == hashB* **then**
            Set the *signature* of *RegisteredIssuer* as valid **Increase** *signaturesCount* by 1
            Update *ThesignatureOwner*
            Update *isApplcationIDSignedBy*
            Emit an event declaring the stored signature details
        else
            Revert contract state
        end
    else
        Emit an event declaring that the signature was failed to be Stored
        Update *PrimaryVerificationApprovalStatus* to Rejected
        Emit an event declaring that primary verification is rejected
    end
else
    Revert contract state
end

involves applying the same hashing algorithm (Keccak256) to the message, where the issuerś public key is used to decrypt the signature. If both hashes are the same, the signature is considered valid and is stored on the blockchain. Otherwise, it is reversed and an event is emitted. Therefore, the *PrimaryVerificationApprovalStatus* is updated to R̈ejected..

Algorithm 5 Primary Verification Results and Final Evaluation

Input: *ApplicationNumber*

ApplicationNumber: Is a unique number given to any new application
if *(caller == RegisteredHealthcareFacility)* **then**
  if *signaturesCount = NeededsignaturesNumbers* **then**
    Update *PrimaryVerificationApprovalStatus* to Approved
    Emit an event declaring that primary verification approval result is Approved
  else
    Update *PrimaryVerificationApprovalStatus* to Rejected
    Emit an event declaring that primary verification approval result is Rejected
  end
else
  Revert contract state
end
if *(caller == RegisteredEvaluationCommitteeMember)* $\wedge$ *(signaturesCount = NeededsignaturesNumbers)* **then**
  if *PrimaryVerificationApprovalStatus = Approved* **then**
    Update *ApplicationStatus* to Approved
    Emit an event declaring that the application is Approved
  else
    Update *ApplicationStatus* to Rejected
    Emit an event declaring that the application is Rejected
  end
else
  Revert contract state
end

Finally, Algorithm 4 shows the final phase of credentialing, where the primary verification results are evaluated by the evaluation committee members. It is approved by the healthcare facility if the *signaturesCount = NeededSignaturesNumber*, otherwise, it is rejected and events are emitted to declare either the approval or the rejection. Then, it goes through the final evaluation phase, where the evaluation committee member executes the *Evaluation* function. The *ApplicationStatus* is updated to "Approved" if the *signaturesCount = NeededSignaturesNumber* and the *PrimaryVerficationApprovalStatus* is "Approved", otherwise, it is rejected and events are emitted.

V. TESTING AND VALIDATION

In this section, the functionality of the two smart contracts is tested and validated. The smart contracts are written in Solidity language and are tested and validated using Remix IDE. Table 1 shows the actors and their corresponding Ethereum addresses that were used in the test. The registration smart contract and the data validation smart contract are deployed at "0xd9145CCE52D386f254917e481eB44e9943F39138" and "0×358AA13c52544ECCEF6B0ADD0f801012ADAD5eE3", respectively. The Ethereum addresses of actors that are used in testing are presented in Table 1. Also, for testing purposes, the inputÂ data is assumed and the time window for primary source verification was in seconds. However, it may take days and weeks. The smart contract code is made publicly available at GitHub,[1] and the transactions and logs of the tested functions are shown below.

TABLE 2. The Ethereum addresses of participants in testing scenario.

	Ethereum Address
Regulatory Authority	0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
Healthcare Facility	0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
EvaluationCommitteMember	0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db
Issuer 1	0x78731D3Ca6b7E34aC0F824c42a7cC18A495cabaB
Issuer 2	0x617F2E2fD72FD9D5503197092aC168c91465E7f2
Issuer 3	0x17F6AD8Ef982297579C203069C1DbfFE4348c372
Applicant 1	0x5c6B0f7Bf3E7ce046039Bd8FABdfD3f9F5021678
Applicant 2	0x03C6FcED478cBbC9a4FAB34eF9f40767739D1Ff7
RegistrationSCaddress	0xd9145CCE52D386f254917e481eB44e9943F39138
DataValidationSCaddress	0x358AA13c52544ECCEF6B0ADD0f801012ADAD5eE3

FIGURE 6. Logs showing a successful registration of healthcare facility.

1) HEALTHCARE FACILITY REGISTRATION:

The registration functions are executed by the regulatory authority where Ethereum addresses of authorized entities

[1] https://github.com/InsuranceMangment/credentialing/blob/main/code.sol

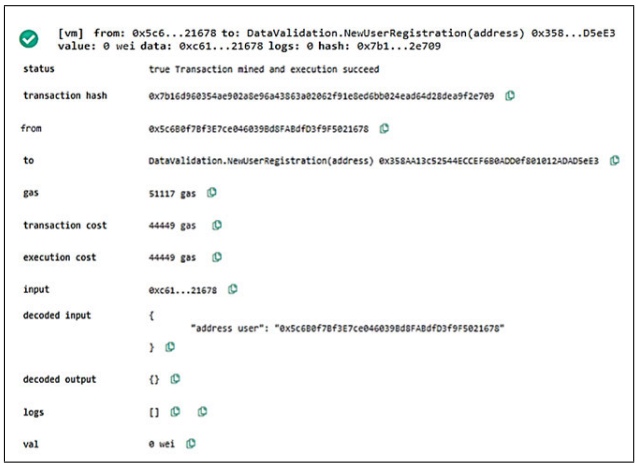

FIGURE 7. Logs showing a successful execution of new user registration.

FIGURE 8. Logs showing a successful execution of new application function.

are added. A Successful healthcare facility registration, along with associated events and logs, are depicted in Figure 6.

2) NEW USER REGISTRATION:

The new applicants or the healthcare professionals should register before starting a new credentialing application by executing the *NewUserRegistration* function. Figure 7 displays a successful execution of the function and its related events and logs.

3) NEW APPLICATION:

once the healthcare professionals register, they can submit their credentialing application by uploading all requested documents to the off-chain storage and using the returned IPFS hash as inputs while executing the *NewApplication* function. Figure 8 shows a successful execution of a New application submission.

FIGURE 9. Logs showing a successful execution of primary verification request function.

4) PRIMARY VERIFICATION REQUEST:

After submitting the credentialing application, the healthcare facility executes the *PrimaryVerificationRequest* function to verify the authenticity of the submitted documents. For testing purposes, we set the duration to be in seconds, however, in real-life scenarios it can take days or weeks. Figure 9 shows a successful primary verification request.

5) STORE SIGNATURES:

The issuer signs an off-chain message to confirm the issuance of a document and then executes the *StoreSignatures* function to store the signatures on-chain. Figure 10 shows a successful execution of the function where the signature is stored successfully on the blockchain. However, if the time window is closed the signature will not be stored. Figure 11 shows a failed execution of the function where the issuer tried to sign and store the signature after the time window was closed.

6) EVALUATION:

The final evaluation function is executed by the evaluation committee member to either approve or reject the credentialing application. Figure 12 displays a successful execution of the function and its related events and logs.

VI. DISCUSSION AND EVALUATION

In this section, we thoroughly examine the deployment of the proposed solution. We focus on security, analyzing its resilience to threats, vulnerabilities, and smart contract flaws. We also evaluate the performance and cost and compare our approach with existing blockchain-based approaches. Lastly, we address the challenges and limitations of implementing the solution.

FIGURE 10. Logs showing a successful execution of store signature function.

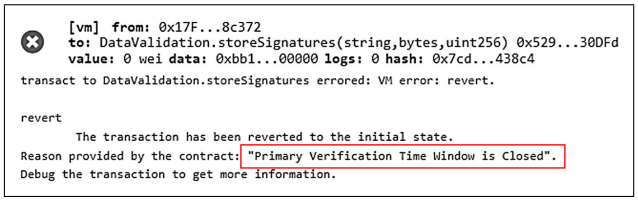

FIGURE 11. Logs showing a failed execution of store signature function.

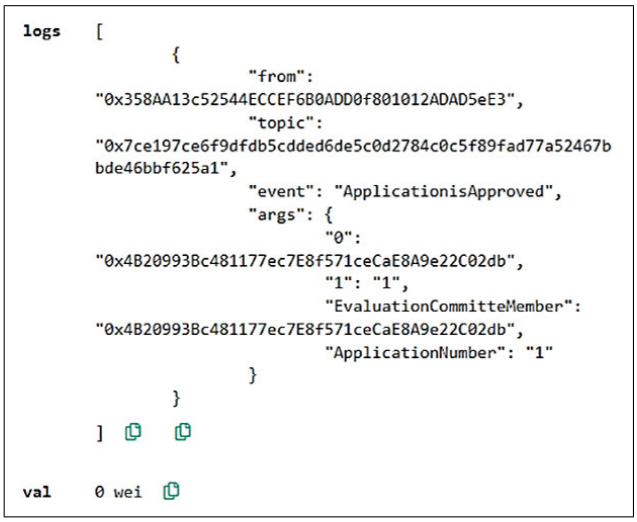

FIGURE 12. Logs showing a successful execution of evaluation function.

A. EVALUATION

Based on our implementation, we conduct a comprehensive assessment to determine the feasibility of our proposed solution. We evaluate how our proposed solution improved the performance of the healthcare credentialing system. The following are the key areas or aspects in which the involved stakeholders faced limitations and challenges.

1) DATA AND PROCESS MANAGEMENT

It is crucial to have an effective management of process and data when it comes to the blockchain-based verification of healthcare professionals' credentials. it is essential to establish a clear and standardized set of actions that streamline the verification process. This includes defining the steps for submitting credentials, requesting verification, and approving or rejecting credentials. As our proposed system and smart contracts have well-defined action requirements, it can minimize delays and ensure a more efficient verification process overall. Moreover, the management of data involved in our verification process employs robust data storage techniques and implements strong encryption measures to safeguard sensitive information. It restricts access to authorized individuals and mitigates the risk of unauthorized data breaches. Each stakeholder benefits in different ways. Healthcare facilities can inspect or verify the credentials of healthcare professionals with high confidence because they cannot be changed or manipulated. Also, it streamlines the verification process for healthcare professionals by accessing credentials in a decentralized way, eliminating the need for manual verification and reducing managerial loads. For healthcare professionals, they can be guaranteed that their credentials are securely and permanently stored on the blockchain. Moreover, it enhances portability among different organizations. The regulatory authority benefits from the ability to audit and monitor entities in real-time to ensure adherence to regulations.

2) SECURITY

In our proposed solution, smart contracts employ cryptographic algorithms for secure key management, encryption, and digital signatures. This can protect sensitive information from unauthorized access and ensure secure transmission between parties. In addition, smart contracts employ a gas mechanism to enhance security by preventing Denial-of-Service (DoS) Attacks. Smart contract security increases all stakeholders' trust and strengthens regulatory enforcement of healthcare credentialing standards through auditable records. Meanwhile, healthcare facilities benefit from secure smart contracts by streamlining the verification process and reducing administrative burdens. Lastly, secure smart contracts protect healthcare credentials from unauthorized access and tampering.

3) ACCESS CONTROL

In our healthcare credential verification blockchain solution, precise control over permissions and access rights is ensured. Proxy re-encryption enables precise control of data access, with owners assigning and adjusting rights using re-encryption keys. Smart contracts use a 'Modifier function' to enforce access control, allowing only authorized entities access to sensitive blockchain data. Specific requirements

must be met before running functions and accessing the data in these smart contracts. This system enables all stakeholders to ensure stringent access controls, preventing unauthorized access to sensitive information and prohibiting any actions that are not permitted.

4) PRIVACY AND CONFIDENTIALITY:

In the blockchain-based credential verification of healthcare professionals, we utilize a proxy decentralized re-encryption network which acts as a protective layer, ensuring that sensitive data remains encrypted and only accessible to authorized entities. Additionally, we include the adoption of an on-chain digital signature for verifying certifications and licenses. This involves attaching a unique digital signature, serving as a seal of authenticity. By verifying the signature on the blockchain, we can ensure that the qualifications of healthcare professionals are legitimate and trustworthy. By combining these measures, we establish a robust system that upholds both privacy and confidentiality in blockchain-based credential verification for healthcare professionals. This allows healthcare professionals to store and keep their information, certifications, and licenses securely. Additionally, it allows healthcare facilities to guarantee that the qualifications of these professionals are trustworthy.

5) ACCOUNTABILITY AND AUDIT TRAIL

This aspect ensures transparency, traceability, and the ability to conduct thorough reviews and audits throughout the entire verification process. This involves keeping a comprehensive record of all actions, decisions, and modifications made during the verification process. In our solution, the distributed ledger serves as a transparent and reliable historical account, capturing the sequence of all events emitted by the developed smart contract. The presence of events ensures traceability, allowing for the tracking of each step taken during the verification process. This benefits healthcare facilities by providing assurance against fraud and offering a clear and transparent history of healthcare professionals' credentialing process and actions. Additionally, it enables the regulatory authority to benefit from having an audit trail, ensuring precise and accurate documentation of all actions. This allows for easy detection of any illegal actions or discrepancies. Overall, by establishing accountability and maintaining events history we promote the integrity and credibility of the credential verification process.

6) DATA INTEGRITY

Blockchain's immutability feature provides robust security, guarding against unauthorized modifications or tampering. Once data is recorded, it becomes virtually impossible to alter it without detection. Any changes or additions to the data are registered as new transactions, creating a transparent and traceable history of the credential verification process. However, in a private blockchain setting, it is important to ensure that it is set up with a proper number of nodes to maintain this feature. We utilize IPFS integrated with the proxy re-encryption method to securely store healthcare professionals' credentials. This decentralized system distributes the data across multiple nodes. Each data piece is assigned a unique cryptographic hash, acting as its identifier. Retrieval from the IPFS network is based on this hash, ensuring data integrity and authenticity. Data integrity benefits healthcare professionals by providing a reliable and transparent record of their credentialing history, enhancing their trustworthiness and professional reputation. In addition to that, healthcare professionals and facilities can protect themselves against fraudulent activities.

Although our proposed solution manages to address these critical aspects, it still has limitations and challenges in terms of scalability, technical complexity, interoperability issues, and implementation cost.

B. CHALLENGES AND LIMITATIONS

Our proposed solution for credential verification for healthcare professionals using Blockchain, IPFS, and Proxy Re-Encryption Network presents an assuring approach, however, the following are some challenges and limitations that must be addressed. First, finding ways to scale the blockchain infrastructure while maintaining optimal performance is a significant consideration. Second, convincing healthcare professionals to embrace the blockchain-based credential verification system can be met with resistance and skepticism. Additionally, there is a need for a certain level of technical expertise to build our proposed system. Third, the cost related to implementing and sustaining the infrastructure of a blockchain network could potentially discourage organizations from embracing its adoption. Moreover, there is a challenge in achieving seamless data exchange and interoperability between different systems, ensuring the smooth operation of the system while ensuring compliance with relevant regulations and legal requirements.

Furthermore, in our proposed system, a limitation arises if a malicious issuer obtains the initial encryption key (key K) and shares it with unauthorized parties. To overcome this issue, a time-based access control sets specific timeframes when authorized users can access encrypted data. This minimizes the chances of misuse. Time-limited encryption includes an expiration period during encryption. Encrypted data becomes inaccessible when the time elapses. This prevents unauthorized key use, even if a malicious issuer obtains the key, as the limited decryption time restricts misuse opportunities. Lastly, integrating an intermediate entity like a re-encryption proxy into the credentialing process presents a significant challenge due to the security risks associated with introducing an additional software component. While meticulous security measures, constant monitoring, and adherence to industry best practices in software development and data protection can help address these risks, there may be other techniques available to overcome this issue.

TABLE 3. Cost analysis of the deployed smart contracts and executed functions.

Smart Contract	Function	Gas Usage	Execution Cost (Gwei)	Execution Cost (Ether)
Registration	Deployment	624659	39978176	0.039978176
	Registration	44449	2844736	0.002844736
DataValidation	Deployment	2562100	163974400	0.1639744
	New Application	208564	13348096	0.013348096
	Primary Verification Request	85500	5472000	0.005472
	Store Signatures	210170	13450880	0.01345088
	Primary Verification Result	43258	2768512	0.002768512
	Evaluation	43520	2785280	0.00278528

```
Compiled with solc
Number of lines: 269 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 2 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 0
Number of informational issues: 0
Number of low issues: 1
Number of medium issues: 0
Number of high issues: 0


+----------------+------------+------+-----------+--------------+-----------+
|      Name      | # functions | ERCS | ERC20 info | Complex code |  Features |
+----------------+------------+------+-----------+--------------+-----------+
|  Registration  |      4     |      |           |      No      |           |
| DataValidation |      8     |      |           |      Yes     | Ecrecover |
|                |            |      |           |              |  Assembly |
+----------------+------------+------+-----------+--------------+-----------+
```

FIGURE 13. Smart contracts vulnerability analysis.

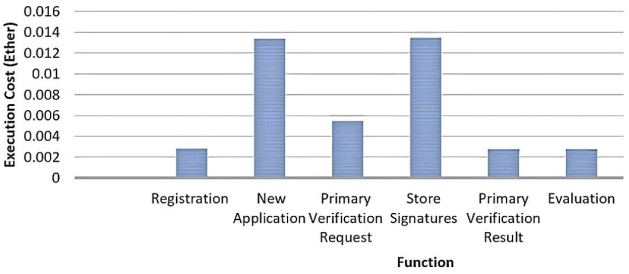

FIGURE 14. Comparison of the execution cost between the functions.

C. SECURITY ANALYSIS OF THE SMART CONTRACTS CODES

The security of smart contracts can be breached by a number of different types of faults and defects. Even though we deploy and test our Solidity smart contract code with Remix IDE, which checks for compilation and run-time errors automatically, we still need to conduct a security check to ensure that our code is not vulnerable to attacks and exploitation. Therefore, a security analysis using Slither is performed to confirm that our smart contract codes were secure. Slither is a Solidity static analysis framework developed in Python 3. It executes a collection of vulnerability detectors, publishes visual information on contract details, and provides an API for writing custom analyses with relative ease. It helps developers to detect vulnerabilities, and improve their code comprehension [49]. Figure 13 depicts a summary of the vulnerabilities that are detected by Slither in our smart contracts. There is one detected low issue that is mainly due to the usage of solidity blocktime.stamp for time comparison. The miners can alter the block validation time by a few seconds; however, in our situation, a delay of a few seconds does not affect the outcome because the end time is measured in days. Further information on the vulnerabilities detected in our smart contract is available online on GitHub. In general, our smart contract's flaws aren't particularly severe; further details on each may be found in [50].

D. COST ANALYSIS

Understanding the costs associated with executing functions is important for assessing the feasibility of implementing the proposed solution on Ethereum's mainnet. The gas consumption represents the computational effort required to execute transactions and smart contracts, closely mirroring the underlying resource consumption such as CPU, memory, and storage. Each action incurs transaction and gas usage, with each unit of gas having a cost.

Deploying a smart contract on a blockchain involves an initial communication cost that is determined by the size of the contract and gas prices set by the network. Ongoing interactions with the smart contract through transactions require constant communication between users and the blockchain network. The cost of these transactions depends on the gas consumed by the operations performed in the contract, execution cost, and any additional fees or gas costs required for the transaction. The computational cost of executing a Solidity smart contract depends on the complexity of the contract's logic and depends on the gas usage and price. Additionally, it can also be influenced by network congestion, reflecting the supply and demand for resources. In our testing case, there are no additional fees or gas costs associated with the transaction, apart from the computational resources consumed during the execution of the code. This implies that the total transaction cost can be equated to the corresponding execution cost, as the computational resources utilized constitute the primary contributing factor to the overall expense incurred. Table 2 summarizes the gas usage and associated costs in Ether for smart contract deployment and function executions. The calculations were based on an average gas price of 103 Gwei sourced from the ETH gas station on May 17, 2023. Looking at the table, it becomes evident that deploying smart contracts is the most expensive operation in the proposed solution. In addition to that, in Figure 15, we have compared the

TABLE 4. Comparison between our solution and existing blockchain-based solutions.

Features	[20]	[28]	[29]	[30]	[31]	[34]	[36]	[37]	[38]	[39]	[42]	Our Solution
Mode of Operation	Private	NA	Private	NA	Private	Public	Private	Public	Public	Private	Consortium	Private
Decentralized Storage	No	IPFS	IPFS	IPFS	IPFS	No	No	IPFS	NA	IPFS	IPFS	IPFS
Storage Pinning Cost	NA	0.0059$/GB	0.0059$/GB	0.0059$/GB	0.0059$/GB	NA	NA	0.0059$/GB	NA	0.0059$/GB	0.0059$/GB	0.0059$/GB
Gas Cost	None	NA	None	NA	None	High	None	High	High	None	None	None
Proxy Decentralized Re-encryption Network	No	No	No	No	No	No	No	No	No	No	No	Yes
Digital Signatures	Yes	Yes	No	No	No	No	No	No	No	No	Yes	Yes

execution costs of the functions in Ether. It is worth noting that the submitting of new candidate applications and store signatures functions tend to incur relatively high costs. Hence, besides ensuring data confidentiality where access to the data is restricted to those who are permitted, it is suitable to implement our solution on a private blockchain rather than a public blockchain to avoid the high gas costs.

E. COMPARISON WITH THE EXISTING SOLUTIONS

In order to highlight the contribution of our solution and how it is different from other existing blockchain solutions, a comparison was made in Table 4. Different features are taken into consideration such as the mode of operation, either public or private; offering off-chain storage for large-sized data files; storage cost, gas cost, credentials' security and the sector they are focusing on.

The existing blockchain solutions are proposed for either the education sector or the healthcare sector. The solutions in [20], [29], [31], [34], and [39] offered systems that are built on private Ethereum where gas cost is zero, however, according to the multiple functions and huge number of candidates, definitely the gas cost is high in other solutions. On the other hand, in [34], [37], and [38] the proposed solutions were built on public Ethereum blockchain where there is a gas cost. The approach in [36] where built on consortium, which is more secure, efficient and scalable than a public blockchain network and similar to the private blockchain where it has access controls. However, it is less transparent. If a member node is compromised, it can still be hacked, and the blockchain's own rules can render the network inoperable.

The credentials documents in [20], [34], and [36] are stored directly on blockchain which lead to a high storage cost. The storage costs in [13], [29], [30], [31], [37], [39], and [42], and our solution had lower costs compared to other solutions, as the credential documents are stored on decentralized storage, specifically using IPFS. IPFS incurs a storage pinning cost of 0.0059$/GB. The storage pinning in decentralized systems involves keeping specific data accessible and persistent. The cost varies based on factors like pinning duration, data size, and pricing model.

Furthermore, a digital signature is a powerful cryptographic tool that serves multiple purposes. Its primary function is to ensure that data is authentic, maintaining its integrity and preventing any repudiation. Only our solution, [13], [20], and [36] utilized the on-chain signatures, however, none of the existing blockchain solutions incorporates a proxy decentralized re-encryption network.

We offer a decentralized system that is resilient and secure against the problem of a single point of failure, which is very important for a healthcare system. Our solution is built on a private blockchain to ensure data confidentiality, where access to the data is restricted to those who are permitted. Additionally, as we mentioned, based on our cost analysis, it is suitable to implement our solution on a private blockchain rather than a public blockchain. Moreover, to avoid expensive on-chain storage of huge documents, our approach leverages decentralized storage while the credentials' security is maintained. In order to avoid the security vulnerabilities that can occur due to transferring data to the decentralized storage, we encrypted the data before storing it on the IPFS by using a symmetric encryption key.

Furthermore, our system architecture is superior because it incorporates Ethereum off-chain storage, proxy re-encryption, digital signatures, and blockchain technology in conjunction to enhance privacy and security in healthcare credentialing processes, ultimately ensuring the integrity and confidentiality of credentialing information. In this solution, we ensure that all components work harmoniously together, and we optimize our smart contract to reduce their gas consumption, adhering to industry standards and regulations while keeping data privacy intact. Moreover, to guarantee the authenticity of certificates and verify their issuance by registered entities, our smart contracts utilize on-chain digital signatures. This confirms that certificates cannot be tampered with and can be traced back to trustworthy sources.

F. GENERALIZATION

Our proposed solution processes healthcare professionals' credentials verification. It can include physicians, nurses, pharmacists, dental hygienists, and others. However, it can also be generalized and extended to other Industries. There

are many occupations that require some type of credentials in different industries such as education, legal, transportation, and community and social services. In order to accommodate a different industry, different actors may be added depending on the requirements. In addition, slight modifications can be made to the functionalities of smart contracts in order to accommodate various industries. All of these needs are easily adaptable to our proposed system, as it will follow the same procedure. In addition, distinct credentials will necessitate the storage of large files, hence the system will require off-chain storage. In addition, slight modifications must be made to the algorithms in order to accommodate various sectors.

VII. CONCLUSION

In this paper, we have proposed a blockchain-based solution for managing healthcare professionals' credentialing in a more credible, trusted, and decentralized manner when compared to today's solutions for credentialing. To avoid storing large files on the blockchain, we have proposed to use decentralized storage (IPFS) in our solution while maintaining data integrity. We presented the system architecture, sequence diagrams, and algorithms to illustrate the working principles behind our proposed approach. Furthermore, the code of the smart contract has been made publicly available on GitHub. We evaluated our proposed system, as well as, we performed a cost and security analysis which showed that our solution is free from known security bugs and vulnerabilities. Lastly, we demonstrated the challenges and limitations intrinsic to the implementation of our proposed solution.

Our blockchain-based solution enhances credentialing by streamlining verification, improving data security, and instilling stakeholder confidence through secure credential storage. Advanced security techniques like proxy re-encryption and cryptographic algorithms protect sensitive data, enable secure communication, and prevent unauthorized access. Our developed smart contracts eliminate intermediaries, automate verification, and enhance transparency and data integrity. In addition to that, the precise access control mechanisms enable stakeholders to enforce stringent permissions, preventing unauthorized access to sensitive information.

Furthermore, our solution promotes accountability and transparency through the use of distributed ledgers and comprehensive audit trails. The immutable nature of the blockchain ensures the integrity of the credential verification process, while integrating IPFS with proxy re-encryption provides secure storage and retrieval of credentials. These advancements enhance the trustworthiness of healthcare professionals' credentials. However, our proposed solution had some limitations, including scalability, technical complexity, interoperability issues, and implementation costs. These aspects need to be carefully considered during the implementation and adoption of the blockchain network infrastructure. Future efforts should prioritize addressing scalability, interoperability, regulatory frameworks, adoption barriers, and cost implications. For instance, testing the solution using scaling methods like Sharding and layer 2 scaling can assess their impact on scalability. Additionally, developing participant-specific front-end DApps for streamlined interaction with off-chain and on-chain data is crucial.

REFERENCES

[1] MDJ. *Protecting the Public in Action*. Alberta RN. Accessed: Nov. 25, 2022. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/29758142/
[2] S. D. Barnett, "Growing pains of credentialing research: Discussions from the institute of medicine workshop," *J. Continuing Educ. Nursing*, vol. 46, no. 2, p. 5355, 2015.
[3] M. H. Baumann, S. Q. Simpson, M. Stahl, S. Raoof, D. D. Marciniuk, and D. D. Gutterman, "First, do no harm: Less training ≠ quality care," *Amer. J. Crit. Care*, vol. 21, no. 4, 2012, Art. no. 227230.
[4] The Bogot Post. (Jun. 5, 2019). *10 Reasons Why Medical Credentialing Is Important*. Accessed: Nov. 25, 2022. [Online]. Available: https://thebogotapost.com/10-reasons-why-medical-credentialing-is-important/38590/
[5] S. Chen, T. Luo, W. Liu, and J. Song, "A framework for managing access of large-scale distributed resources in a collaborative platform," *Data Sci. J.*, vol. 7, Dec. 2008, Art. no. 137147.
[6] T. G. Legotlo and A. Mutezo, "Understanding the types of fraud in claims to south African medical schemes," *South Afr. Med. J.*, vol. 108, no. 4, p. 299, Mar. 2018.
[7] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018.
[8] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.
[9] D. J. Skiba, "The potential of blockchain in education and health care," *Nursing Educ. Perspect.*, vol. 38, no. 4, pp. 220–221, Aug. 2017.
[10] Q. Mamun, "Blockchain technology in the future of healthcare," *Smart Health*, vol. 23, Mar. 2022, Art. no. 100223.
[11] M. N. Kamel Boulos, J. T. Wilson, and K. A. Clauson, "Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare," *Int. J. Health Geographics*, vol. 17, no. 1, p. 25, Dec. 2018.
[12] MIT Media Lab. *What We Learned From Designing an Academic Certificates System on the Blockchain*. Medium. Accessed: May 23, 2023. [Online]. Available: https://l8.nu/sXEF
[13] A. Hevner and S. Chatterjee, "Design science research in information systems," in *Design Research in Information Systems: Theory and Practice*. New York, NY, USA: Springer, 2010, pp. 9–22.
[14] NursingCenter. *Is Blockchain the New Pathway to Credentialing?* Accessed: Nov. 25, 2022. [Online]. Available: https://www.nursingcenter.com/ncblog/march-2020/blockchain-credentialing
[15] Default. *Understanding Primary Source Verification*. Accessed: Nov. 25, 2022. [Online]. Available: https://veritystream.com/resources/details/blog/2021/09/07/understanding-primary-source-verification
[16] *The Provider Credentialing Process From Start to Finish—Symplr (ND)*. Accessed: Aug. 14, 2023. [Online]. Available: https://l8.nu/t43I
[17] S. Smith, Sep. 9, 2022, "Top 10 Challenges in Healthcare Credentialing," Tollanis Solutions Inc., Accessed: Nov. 15, 2022. [Online]. Available: https://tollanis.com/credentialing/top-challenges-healthcare-credentialing/
[18] *Verifiable Credential Use Cases: Healthcare Credentialing*. Accessed: Sep. 9, 2022. [Online]. Available: https://www.dock.io/case-study-healthcare
[19] I. Kim. *Lying on a Resume About Your Degree*. Accessed: 2021. [Online]. Available: https://www.monster.com/career-advice/article/lying-on-your-resume
[20] R. Arenas and P. Fernandez, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," in *Proc. IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC)*, Jun. 2018, pp. 1–6.
[21] L. Zhou, L. Wang, and Y. Sun, "MIStore: A blockchain-based medical insurance storage system," *J. Med. Syst.*, vol. 42, no. 8, p. 117, Aug. 2018, doi: 10.1007/S10916-018-0996-4.
[22] IBM Blockchain. *What is Blockchain Technology?* Accessed: Mar. 16, 2023. [Online]. Available: https://www.ibm.com/topics/blockchain

[23] M. Thenmozhi, R. Dhanalakshmi, S. Geetha, and R. Valli, "WITHDRAWN: Implementing blockchain technologies for health insurance claim processing in hospitals," *Mater. Today, Proc.*, Mar. 2021, doi: 10.1016/J.MATPR.2021.02.776.

[24] M. Raikwar, S. Mazumdar, S. Ruj, S. Sen Gupta, A. Chattopadhyay, and K.-Y. Lam, "A blockchain framework for insurance processes," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–4, doi: 10.1109/NTMS.2018.8328731.

[25] *What is Decentralization?* Accessed: Mar. 16, 2023. [Online]. Available: https://aws.amazon.com/blockchain/decentralization-in-blockchain/

[26] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proc. 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30, doi: 10.1109/obd.2016.11.

[27] M. Hader, A. Elmhamedi, and A. Abouabdellah, "Blockchain technology in supply chain management and loyalty programs: Toward blockchain implementation in retail market," in *Proc. IEEE 13th Int. Colloq. Logistics Supply Chain Manage. (LOGISTIQUA)*, Dec. 2020, pp. 1–6, doi: 10.1109/logistiqua49782.2020.9353879.

[28] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control," *IEEE Internet Things J.*, vol. 8, no. 14, pp. 11717–11731, Jul. 2021, doi: 10.1109/JIOT.2021.3058946.

[29] B. S. Egala, A. K. Pradhan, P. Dey, V. Badarla, and S. P. Mohanty, "Fortified-chain 2.0: Intelligent blockchain for decentralized smart healthcare system," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12308–12321, Jul. 2023, doi: 10.1109/JIOT.2023.3247452.

[30] R. Garg, "Blockchain ecosystem for education and employment verification," in *Proc. 13th Int. Conf. Netw. Commun. Secur.*, Toronto, ON, Canada, Sep. 2021, Art. no. 1001997.

[31] A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission," *Appl. Sci.*, vol. 11, no. 22, p. 10917, Nov. 2021, doi: 10.3390/app112210917.

[32] A. Davies. (Apr. 26, 2023). *Pros and Cons of Hyperledger Fabric for Blockchain Networks*. [Online]. Available: https://www.devteam.space/blog/pros-and-cons-of-hyperledger-fabric-for-blockchain-networks/

[33] SoluLab. (Jan. 29, 2020). *Hyperledger Fabric on Blockchain Technology: What are the Advantages and Disadvantages?*. Medium. [Online]. Available: https://solulab.medium.com/hyperledger-fabric-on-blockchain-technology-what-are-the-advantages-and-disadvantages-43fffc6a27fe

[34] A. M. San, N. Chotikakamthorn, and C. Sathitwiriyawong, "Blockchain-based learning credential verification system with recipient privacy control," in *Proc. IEEE Int. Conf. Eng., Technol. Educ. (TALE)*, Dec. 2019, pp. 1–5.

[35] W. Grther, S. Kolvenbach, R. Ruland, J. Schtte, C. Torres, and F. Wendland, "Blockchain for education: Lifelong learning passport," *Proc. 1st ERCIM Blockchain Work*, vol. 2, no. 10, 2018, pp. 1–10.

[36] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 4, pp. 1503–1514, Aug. 2023,.

[37] S. Namasudra, P. Sharma, R. G. Crespo, and V. Shanmuganathan, "Blockchain-based medical certificate generation and verification for IoT-based healthcare systems," *IEEE Consum. Electron. Mag.*, vol. 12, no. 2, pp. 83–93, Mar. 2023.

[38] R. Mukta, J. Martens, H.-y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-based verifiable credential sharing with selective disclosure," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 959–966.

[39] R. A. Mishra, A. Kalla, N. A. Singh, and M. Liyanage, "Implementation and analysis of blockchain based DApp for secure sharing of students' credentials," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2.

[40] S. K. Ambast and T. A. Sumesh, "A blockchain based credential verification system using IPFS," in *Proc. IEEE 19th India Council Int. Conf. (INDICON)*, Nov. 2022, pp. 1–5.

[41] P. P. Bokariya and D. Motwani, "Decentralization of credential verification system using blockchain," *Int. J. Innov. Technol. Exploring Eng.*, vol. 10, no. 11, pp. 113–117, Sep. 2021.

[42] D. Serranito, A. Vasconcelos, S. Guerreiro, and M. Correia, "Blockchain ecosystem for verifiable qualifications," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 192–199.

[43] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *Proc. Bus. Inf. Syst. Workshops*, 2019, pp. 185–196.

[44] G. Wang, R. Lu, and C. Huang, "PSLP: Privacy-preserving single-layer perceptron learning for e-Healthcare," in *Proc. 10th Int. Conf. Inf., Commun. Signal Process. (ICICS)*, Dec. 2015, pp. 1–5.

[45] P. K. Maganti and P. M. Chouragade, "Secure health record sharing for mobile healthcare in privacy preserving cloud environment," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Feb. 2019, pp. 1–4.

[46] J. Sun, Y. Yuan, M. Tang, X. Cheng, X. Nie, and M. U. Aftab, "Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare," *IEEE Trans. Ind. Informat.*, vol. 18, no. 9, pp. 6483–6493, Sep. 2022, doi: 10.1109/TII.2021.3133345.

[47] S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient unidirectional proxy re-encryption," in *Progress in Cryptology AFRICACRYPT 2010* (Lecture Notes in Computer Science), vol. 6055, D. J. Bernstein and T. Lange Eds. Berlin, Germany: Springer, doi: 10.1007/978-3-642-12678-9_19.

[48] S. R. Subramanya and B. K. Yi, "Digital signatures," *IEEE Potentials*, vol. 25, no. 2, pp. 5–8, Mar. 2006, doi: 10.1109/MP.2006.1649003.

[49] ImmuneBytes. *Slither: A Solidity Static Analyzer for Smart Contracts*. Accessed: Jun. 2, 2023. [Online]. Available: https://www.immunebytes.com/blog/slither-a-solidity-static-analyzer-for-smart-contracts/

[50] Crytic. *Crytic/Slither: Static Analyzer for Solidity*. GitHub. Accessed: Jun. 2, 2023. [Online]. Available: https://github.com/crytic/slither#bugs-and-optimizations-detection

AYSHA ALNUAIMI received the B.S. degree in electrical engineering from United Arab Emirates University, United Arab Emirates, in 2020. She is currently pursuing the degree in engineering systems and management program with Khalifa University, Abu Dhabi, United Arab Emirates. She is a Research and a Teaching Assistant with the Department of Industrial Systems Engineering, Khalifa University. Her research interest includes blockchain applications in healthcare.

DIANA HAWASHIN received the B.S. degree in electrical engineering from United Arab Emirates University, in 2020, and the M.S. degree in engineering systems and management from Khalifa University, in 2022. She is currently a Research Associate with the Department of Electrical and Computer Engineering, Khalifa University. Her research interests include blockchain, management, and supply chains.

RAJA JAYARAMAN received the bachelor's and master's degrees in mathematics from India, the M.Sc. degree in industrial engineering from New Mexico State University, and the Ph.D. degree in industrial engineering from Texas Tech University. He is currently an Associate Professor with the Department of Industrial and Systems Engineering, Khalifa University, Abu Dhabi, United Arab Emirates. His postdoctoral research was centered on technology adoption and implementation of innovative practices in the healthcare supply chains and service delivery. He has led several successful research projects and pilot implementations of supply chain data standards adoption in the U.S. healthcare systems. His research interests include application of blockchain technology, NFTs, the IoT, and process optimization techniques to characterize, model, and study complex systems with applications to supply chains, maintenance planning, and healthcare delivery.

KHALED SALAH (Senior Member, IEEE) received the B.S. degree in computer engineering with a minor in computer science from Iowa State University, USA, in 1990, and the M.S. degree in computer systems engineering and the Ph.D. degree in computer science from the Illinois Institute of Technology, USA, in 1994 and 2000, respectively. In August 2010, he joined Khalifa University, United Arab Emirates, where he is currently a Full Professor with the Department of Electrical and Computer Engineering, and is teaching graduate and undergraduate courses in the areas of cloud computing, computer and network security, computer networks, operating systems, and performance modeling and analysis. Prior to joining Khalifa University, he worked for ten years with the Department of Information and Computer Science, King Fahd University of Petroleum and Minerals (KFUPM), Saudi Arabia. He has more than 190 publications and three patents, has been giving a number of international keynote speeches, invited talks, tutorials, and research seminars on the subjects of blockchain, the IoT, fog and cloud computing, and cybersecurity. He is a member of the IEEE Blockchain Education Committee. He was a recipient of the Khalifa University Outstanding Research Award, in 2014 and 2015, the KFUPM University Excellence in Research Award, in 2008 and 2009, and the KFUPM Best Research Project Award, in 2009 and 2010, and the Departmental Awards for Distinguished Research and Teaching in prior years. He is the Track Chair of IEEE Globecom 2018 on Cloud Computing. He serves on the editorial boards of many WOS-listed journals, including *IET Communications*, *IET Networks*, *Journal of Network and Computer Applications* (Elsevier), *Security and Communication Networks* (Wiley), *International Journal of Network Management* (Wiley), *Journal of Universal Computer Science*, and *Arabian Journal for Science and Engineering*. He is an Associate Editor of IEEE BLOCKCHAIN NEWSLETTER.

MOHAMMED OMAR is currently a Full Professor and the founding Chair of the Department of Engineering Systems and Management (currently renamed Industrial and Systems Engineering), Khalifa University, Abu Dhabi, United Arab Emirates. Prior to joining the Masdar-Institute/KUST, he was an Associate Professor and a Graduate Coordinator with Clemson University, Clemson, SC, USA, and was part of the founding Faculty Cohort with Clemson University, Greenville, SC, USA. He also led an NSF I/UCRC Center and was part of the DoE GATE Center of Excellence in Sustainable Mobility Systems. His current laboratory with the Masdar City Campus includes capabilities in composite fabrication and manufacturing analytics. His research group did support two postdoctoral scholar's career planning to become an assistant professors with Texas A&M University at Qatar, in 2013, and the University of Sharjah, in 2015. He was named a Tennessee Valley Authority Fellow for two consecutive years during the Ph.D. studies, in addition to being a Toyota Manufacturing Fellow. His professional career includes a Postdoctoral Researcher with the Center for Robotics and Manufacturing Systems (CRMS) and a Visiting Scholar with the Toyota Instrumentation and Engineering Division, Toyota Motor Company, Japan. His group graduated seven Ph.D. dissertations and more than 35 M.Sc. theses; four of the Ph.D. students are currently on academic ranks in U.S. universities. He has more than 100 publications in the area of product lifecycle management, knowledge-based manufacturing, and automated testing systems, in addition to authoring several books and book chapters; he has been granted four U.S. and international patents. His work has been recognized by the U.S. Society of Manufacturing Engineers SME through its Richard L. Kegg Award and the SAE Foundation Award for Manufacturing Leadership. In addition, the College of Engineering, Clemson University, awarded the Murray Stokely Award. He currently serves as the Editor-in-Chief for the *Journal of Materials Science Research* (Part of the Canadian Research Center) and an Associate Editor for the *Soft Computing* (Springer), handling the area of decision science and knowledge-based systems; in addition to the membership on several editorial boards and conference organizations. He serves on the advisory board of the Strata PJSC (part of Mubadala Aerospace).