CrossCert: A Privacy-Preserving Cross-Chain System for Educational Credential Verification Using Zero-Knowledge Proof

Tuan-Dung Tran[1(✉)], Phong Khuu Minh[1], Trang Le Tran Thuy[1], Phan The Duy[2], Nguyen Tan Cam[2], and Van-Hau Pham[2]

[1] Faculty of Computer Networks and Communications, University of Information Technology, Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam
dungtran@uit.edu.vn, {20521742,20520323}@gm.uit.edu.vn

[2] Information Security Laboratory, University of Information Technology, Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam
{duypt,camnt,haupv}@uit.edu.vn

Abstract. Across various industries, credential verification stands as a critical requirement, yet traditional approaches face limitations in security, privacy, and interoperability. Although recent blockchain innovations promise decentralization, deploying them independently in institutions creates data isolation. While there are theoretical frameworks, lack of practical studies achieving a balance between credential mobility and privacy is noteworthy. This paper introduces CrossCert, a privacy-focused cross-chain system for verifying credentials between educational and employer blockchains. By incorporating zero-knowledge proofs, CrossCert facilitates anonymous checks without disclosing user details. Extensive experiments have consistently demonstrated CrossCert's real-time performance, even within blockchain limitations. Its security features, including cryptographic proofs and on-chain data management, demonstrate strong resilience against typical attacks and web vulnerabilities. CrossCert pioneers bridging the research gap between education, employment, and privacy, striving to achieve a balanced balance of credential accessibility and ethical information practices with its innovative cross-chain architecture. The system hence merits further research as a feasible solution to streamline decentralized credential validation across diverse stakeholders.

Keywords: Blockchain · Cross-chain · Credential Verification · Privacy-Preserving · Zero-Knowledge Proof

1 Introduction

As underscored in the study on secure credential verification by Kaneriya [1], the process of credential verification is pivotal in recruitment and employment

N.-S. Vo et al. (Eds.): INISCOM 2024, LNICST 595, pp. 256–271, 2024.
https://doi.org/10.1007/978-3-031-67357-3_18

across diverse industries and organizations. However, longstanding reliance on paper-based systems has precipitated manifold limitations. Physical credentials engender inconveniences in access, counterfeiting risks sans reliable verification, and a lack of interoperability between siloed issuer-verifier systems. Furthermore, data stored in traditional database systems can be easily modified by a group of administrators or high-privileged users. From there, the integrity, transparency, and irrefutability of the data will not be guaranteed [2].

Within the domain of contemporary technological progress, there have been remarkable and exponential strides made in the field of distributed ledger technologies, prominently exemplified by the advent of blockchain. These advancements hold great promise in terms of providing decentralized solutions that enable the seamless digitization of credentials [3]. Blockchain's characteristics of transparency, tamper-proofing, decentralization, and anonymously serve as key enablers for secure credential issuance, storage, and verification while preserving privacy as emphasized in the study by Monrat and his team [4]. In the realm of technological advancement, it is evident that the conceptualization of blockchain technology has outpaced its practical implementation. Regrettably, the prevailing trend of isolated blockchain deployment within various institutions has inadvertently given rise to a landscape characterized by fragmented data islands [5].

Cross-chain refers to systems that enable interoperability and communication between multiple blockchain networks [6]. The need for cross-chain technologies stems from the isolated development of independent blockchains, with limited ability to share data or exchange value between chains. Previous research exploring blockchain-based credentials has shed light on persistent challenges related to cross-chain interoperability and privacy preservation, as evidenced by various studies [7–9]. While blockchain-based credentials have been the subject of prior investigations, significant obstacles remain in achieving cross-chain interoperability. Additionally, the importance of preserving privacy cannot be overstated, especially in the context of credential verification systems to prevent the exposure of sensitive personal information. It's worth noting that while NoviChain [10] and Wu et al. [11] employed zero-knowledge proofs for location verification and COVID certificates, both solutions lacked cross-chain integration. Other applications predominantly centered on single blockchain designs, lacking robust privacy safeguards, as exemplified in studies [12–14].

Existing works that applied blockchain and zero-knowledge proofs mainly focused on single blockchain solutions without cross-system integration or sufficient safeguarding of individual privacy. At present, a salient research gap persists at the intersection of education, employment and privacy domains in developing cross-chain credential solutions that aim to balance verifiability and ethical information management while preserving user privacy. This paper pioneers an effort to address this lacuna by proposing CrossCert, an innovative cross-chain system integrating zero-knowledge proofs to facilitate decentralized, anonymous, and interoperable credential verification across both educational and employer blockchains.

Our main contributions are as follows:

- First, this paper proposes the CrossCert system, which aims to enhance cross-blockchain interoperability through a cross-chain decentralized application (DApp) within the context of integrating education and recruitment processes between enterprises. The motivation for developing the CrossCert system stems from the need to facilitate interactions between disparate blockchain networks
- Second, by incorporating Zero-Knowledge Proofs (ZKPs) through ZK-SNARKs libraries, we improve the privacy of cross-chain bridges. ZKP is applied to hide sensitive user data and transactions during the process of cross-chain communication and data sharing.
- Third, we implement and experiment with the CrossCert system, and then evaluate it through metrics such as execution time, cost, CPU usage, requests per second, and security. To assess the security of the CrossCert system, we conduct penetration testing to identify potential vulnerabilities. This evaluation includes an analysis of the CrossCert system's resilience against common security threats originating from web-based attacks and forged transactions. These comprehensive assessments collectively illustrate the robustness and effectiveness of our cross-chain solution.

The remainder of this paper is structured as follows: Sect. 2 examines the relevant literature pertaining to the topic at hand. Section 3 furnishes a comprehensive overview of our system, elucidating its principal components and elucidating its processing flow. Section 4 elucidates the implementation particulars and conducts an evaluation of our solution with regard to its performance and security. The final section, Sect. 5, encapsulates the core findings of the study while also accentuating potential avenues for future research.

2 Related Works

This section reviews relevant literature on blockchain applications and cross-chain technologies.

2.1 Blockchain Applications

Fundamentally, blockchain technology enables decentralized and tamper-proof transaction verification without intermediaries, with applications in various domains [15]. Its transparent transaction tracking can facilitate supply chain management [16,17]. Potential healthcare applications of blockchain include data sharing between parties, remote patient monitoring, and health analytics [18].

Several studies have explored using blockchain technology for certificate verification purposes [7,19]. A bibliometric analysis of publications from 2017 to 2021 indicates that the field of blockchain applications in education has grown considerably. Over the years, the use of blockchain to issue and verify academic

credentials has received more research focus compared to other educational uses of blockchain technology [20].

By serving as a decentralized ledger, blockchain could store learning records across institutions without a centralized authority. This innovative concept was investigated by Do et al. [12], Anwar et al. [13] who delved into the application of blockchain technology for distributing academic records and facilitating credential verification in their research. Their approaches capitalize on blockchain's ability to securely and transparently record credentials. However, as prior work notes, fully implementing such a system presents important challenges. There is a need for deeper exploration of blockchain interoperability and the protection of user privacy. In their work cited as BR et al. [21], a specific implementation of blockchain technology was proposed for educational credentialing through a web framework. Their system design incorporated functions like user registration, login, certificate issuance, verification, uploading marks data, and viewing certificates and marks lists. Nevertheless, the system has yet to fully realize cross-chain communication capabilities and preserve privacy to the desired extent.

There have been attempts to apply technological solutions to maintain privacy during authentication processes. Abid et al. [10] proposed a blockchain-based platform called Novidchain for privately issuing and verifying COVID-19 certificates using self-sovereign identity (SSI). Under SSI, individuals control their identity and data. However, managing private keys introduces responsibility as lost keys could mean lost identity. The system also did not integrate cross-chain protocols for inter-blockchain communication, despite progress in privacy-preserving identity solutions.

Prior scholarly works have sought to apply zero-knowledge proofs in other domains. For instance, Wu et al. [22] proposed a hybrid blockchain network with smart access points as the decentralized ledger to address centralization in location-proof architectures. The system supported location-based services with privacy using a zero-knowledge proof of location (zk-PoL) protocol. This allowed users to generate location proofs to access services while only disclosing necessary location metadata. Nevertheless, its limitation lay in the absence of cross-chain communication mechanisms, which hindered interoperability across different blockchain platforms.

Li et al. [23] proposed a privacy-preserving traffic management system using blockchain and zero-knowledge proof (ZKP). Within this framework, gateways validated vehicle attributes like location using zero-knowledge range proofs (ZKRPs), allowing validation without revealing values. This leveraged blockchain for distributed traffic while upholding privacy. However, it did not enable cross-chain communication or interoperability across distributed ledgers. The ZKP can enable privacy-preserving functionality by allowing verifiable claims without revealing private details [24]. Li et al. [25] proposed a private authorization system using blockchain and zk-SNARKs where users generate proofs to prove attribute satisfaction without revealing attributes. However, it's a common limitation in such systems that they often lack the capability for cross-chain communication.

2.2 Cross-Chain Approaches

In educational settings, the use of separate blockchains by individual institutions can lead to an "isolated islands" problem with limited ability to share data or exchange value between chains. Cross-chain technology serves as a solution to this problem by enabling interoperability between distinct blockchains. While communication within homogenous blockchains is straightforward, connecting heterogeneous chains presents challenges. To address these challenges, several prominent approaches have been developed:

Notary Scheme: This method utilizes a trusted third party (notary) to validate and confirm transactions across blockchains [26]. Executing actions on one chain in response to events on another, as performed by the notary node, raises concerns about security and decentralization due to its reliance on a single intermediary. A potential vulnerability is that the notary node could become compromised, calling into question the validity of any cross-chain transactions it has validated. Additionally, having a single point of control reduces the decentralized nature of blockchain networks [27].

Hash Time-Locked Contracts (HTLCs): HTLCs employ cryptographic hashes and timelocks to facilitate conditional resource transfers between blockchains [28]. Users commit to exchanges via cryptographic proofs before configurable timeouts [29]. While removing intermediaries, HTLCs require simultaneous online participation. A limitation is that both counterparties need to be online at the same time to finalize the transaction within the timelock. If one party is offline when the timeout expires, the funds could be locked indefinitely.

Sidechains: Sidechains act as extensions of the primary blockchain or mainchain [30] that can two-way peg assets between the chains. As an extension, sidechains are separate blockchains that are linked to the mainchain through special transactions, allowing assets to move between the chains. This approach addresses interoperability while offloading some processing load from the mainchain to the extended sidechains [31].

Relay Chains: If a sidechain enables interoperability across multiple parent chains, it is referred to as a relay chain [32]. Projects like Polkadot and Cosmos have implemented relay chain architectures at scale. However, it's important to note that a relay chain introduces a single point of failure, as all interoperability flows through it. An issue with the relay chain could disrupt transactions across the connected blockchains, necessitating the incorporation of additional redundancy and fail-safes into relay chain architectures [33].

In general, current related approaches lack one or both of two critical factors: interoperability and privacy preservation. To the best of our knowledge, there has been limited scholarly research examining cross-blockchain data-sharing solutions in the context of educational credentials and employment verification while preserving individual privacy.

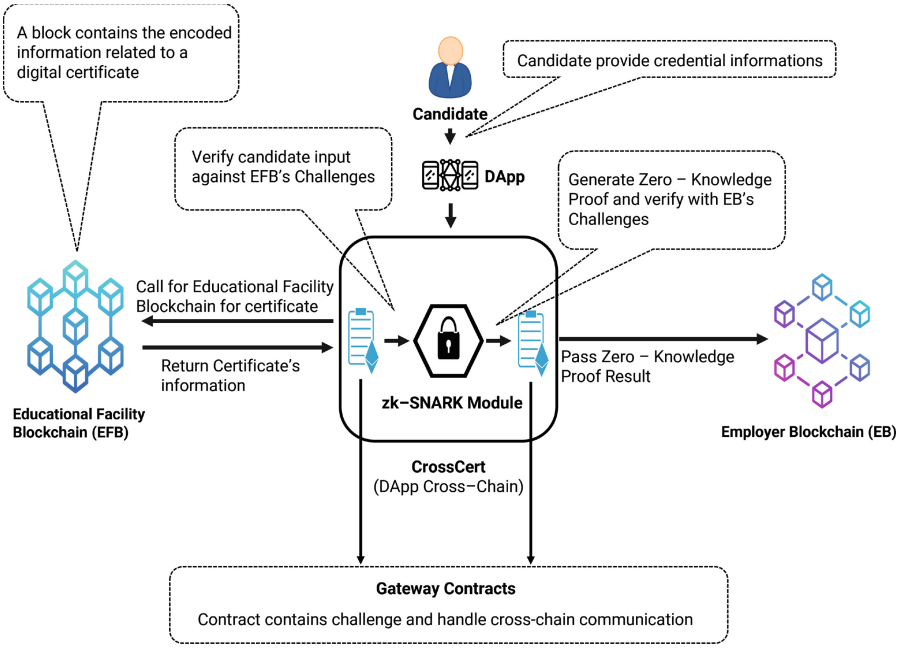

Fig. 1. The conceptual architecture of the CrossCert system

3 Proposed System

In this section, we propose CrossCert, a decentralized application-based (DApp-based) cross-chain bridge that enables the verifiable and privacy-preserving transfer of credentials across different blockchains.

3.1 System Architecture

The CrossCert system architecture comprises five core entities:

- Candidates: Individuals seeking to have their academic credentials verified for employment purposes.
- Educational Facility Blockchain (EFB): A permissioned blockchain deployed by educational institutions to immutably issue, store and manage student records and certificates in a decentralized manner.
- Employer Blockchain (EB): A separate permissioned blockchain operated by prospective employers to validate candidate qualifications while preserving sensitive personal details.
- CrossCert Application: Acts as a cross-system notary, interfacing the EFB and EB through an anonymization protocol. Key functions include retrieving certificate details from the EFB, performing zero-knowledge proofs to cryptographically verify claims, and transmitting validation results to the EB.

– zk-SNARK Module: An integral component of CrossCert leveraging zero-knowledge succinct non-interactive argument of knowledge proofs. This allows candidates to prove credential possession to the EFB without revealing private attributes. It also enables CrossCert to calculate cryptographic proofs from certificate attributes to verify against EB challenges in a privacy-preserving manner.

  In the proposed system, zk-SNARKs are implemented using the G16 algorithm. A core component of the algorithm allows for verifying the validity of the assertion $C(pub, w) = true$, where pub represents a public input and w denotes a private input. Specifically, the algorithm enables proving that the statement C evaluates to true when given pub which is openly disclosed, along with w which is privately held. In the context of education and employment, a job posting by an employer may stipulate minimum grade point average (GPA) eligibility criteria that applicants must meet. For example, consider a posting that requires a certificate with a GPA^2 greater than 12. We define the following terms:
  - pub = the required GPA specified in the posting (12 in this case)
  - w = the GPA on the applicant's certificate
  - C = a statement that relates w and pub. We can write C as a proposition that relates the certificate GPA w and the required posting GPA pub. Specifically: $C(pub, w) = w^2 > pub$

  In more detail, the zk-SNARKs generation process first takes as input the circuit C, along with 12 as pub and w as GPA. It then generates a proof π, which is sent to the verifier. Separately, a verification key vk is generated, which consists of 5 elliptic curve points $(vk_\alpha, vk_\beta, vk_\gamma, vk_\delta, vk_{IC})$. The G16 algorithm constructs bilinear pairing $e : (G_1 * G_2) \longrightarrow G_T$ using the alt_bn128 curve. The verification procedure then uses both the proof π and verification key vk to confirm the statement's validity. Specifically, the verifier applies the bilinear pairing e to combinations of the vk components and elements of the proof π. If the result satisfies the circuit's output, the proof is deemed valid without revealing the GPA w.

As shown in Fig. 1, the EFB utilizes blockchain properties like transparency, security, and decentralization to issue credentials to students as blockchain tokens containing metadata like graduation year and GPA. Similarly, the EB stores validation records but not the full credentials themselves to preserve user privacy. The CrossCert DApp sits between these independent blockchains. It allows candidates to request anonymous credential checks with employers via its interface. Internally, it retrieves credential details from the EFB using zk-SNARK proofs to cryptographically verify claims without exposing private information. Validation results are then passed transparently to the EB for storage.

3.2 Interchain Credential Verification

Educational facilities (EFBs) and employers (EBs) must first register with the CrossCert validator platform by deploying dedicated smart contracts on their

respective blockchains and providing a network identifier. This allows CrossCert to collect the contract addresses and enable cross-chain communication between the different entities.

As part of the registration process, EFBs can input challenges representing the criteria that students must prove to demonstrate certificate authenticity. For example, an EFB may register a challenge requiring students to prove their completion of a specific course. Similarly, EBs can also register by inputting the criteria they require in order to validate a certificate's relevancy for a given job role. All challenges are stored securely on the deployed smart contracts, maintaining decentralization and transparency.

Algorithm 1. Certificate Verification Procedure

```
EFB ← get_contract_address(EFBNetworkID);
EFBChall ← get_challenges(EFB);
EB ← get_contract_address(EBNetworkID);
EBChall ← get_challenges(EB);
Proof ← zkp_generate_proof(EFBChall, CandidateInput);
IsEFBStudent ← zkp_verify(Proof);
if IsEFBStudent then
    CandidateKey ← extract_key(CandidateInput);
    CertificateData ← call_EFB_certificate(CandidateKey);
    Proof ← zkp_generate_proof(EBChall, ContractData);
    VerificationResult ← zkp_verify(Proof);
    if VerificationResult then
        notify_EB_and_candidate(SUCCESS);
        send_result_to_EB(Proof, VerificationResult);
    else
        notify_EB_and_candidate(FAIL);
        show_candidate_failed_requirement();
    end if
else
    raise_warning();
end if
```

After EFB and EB complete the registration process, whenever a candidate is requested to provide a certificate by an EB, they interact with the CrossCert verification platform. First, the candidate must input credentials to verify their student status against the EFB through ZKP challenges registered by the EFB. For example, the candidate may need to provide details of a specific course or lecturer to demonstrate they were enrolled as a student of the issuing EB. If the candidate successfully satisfies the ZKP checks, CrossCert requests the actual certificate data from the issuing EFB by calling a smart contract deployed on the EFB network. The EFB returns the certificate details to CrossCert. Secondly, CrossCert calculates proofs based on the certificate data and verifies their validity against challenges stored by the EB. If the proofs validate the certificate's

authenticity, CrossCert then communicates the verification outcome to the relevant parties on the EB network. CrossCert does this by invoking a smart contract that has been deployed previously on the EB blockchain. Specifically, CrossCert calls the appropriate functions within this smart contract to submit the verification result. Finally, CrossCert alerts both the candidate and employers that credential verification has been completed.

When acting upon a request to verify a certificate claim, CrossCert follows a standardized verification procedure that can be conceptualized through the pseudocode of Algorithm 1. Figure 2 provides a visual overview of this 9-step verification process utilizing blockchains, zero-knowledge proof, and a cross-chain architecture.

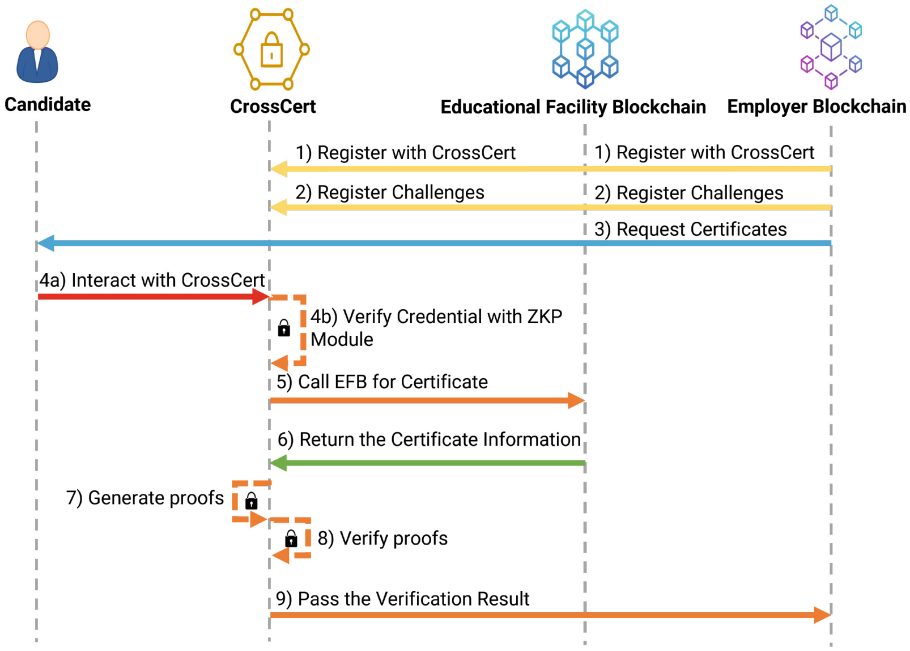

Fig. 2. The sequence diagram of the CrossCert system

4 Experiments and Results

4.1 Experimental Setup

In order to simulate a cross-chain application scenario resembling real-world conditions, we set up a test network comprising three virtual machines (VM1, VM2, and VM3), each equipped with the following specifications:

- Each VM has 4 GB of RAM, 16 GB of SSD storage, and a 2-core CPU.
- VM1 and VM2 hosted different blockchains to simulate the connection between Ethereum and ConsenSys Quorum. VM1 ran an Ethereum Blockchain connected to VM2 ran a ConsenSys Quorum Blockchain. This was to model an application where one blockchain (Ethereum) stores certificates and the other (ConsenSys Quorum) stores candidate credentials.
- VM3 hosted the DApp interface using an Apache web server.

On VM1 and VM2, we installed Node.js version 16.16, used the Axelar Local Development Framework and Quorum Developer to deploy Ethereum Virtual Machines (EVMs) and generate Genesis blocks for the test networks. The system configuration details are summarized in Table 1. Our implementation of the CrossCert framework can be found on GitHub[1].

Table 1. Experimental environment

Virtual machine	CPU	RAM	Hard drive	OS	Deputation
VM1	2-core	4 GB	16 GB	Ubuntu 22.04	Ethereum
VM2	2-core	4 GB	16 GB	Ubuntu 22.04	Quorum
VM3	2-core	4 GB	16 GB	Ubuntu 22.04	Hosting

4.2 Performance Evaluation

To evaluate transaction throughput, we developed a simple smart contract that allowed recording timestamped transactions to the blockchains. Subsequently, we built a front-end interface on VM3 to submit transactions. The analysis revealed an average execution time of approximately 12 s for individual transactions within the CrossCert decentralized credential verification system. This overall transaction speed was found to be acceptable given that transactions on the underlying Ethereum blockchain currently range from 15 s to 5 min to reach finality. The transaction times can be broken down into the constituent operations as follows:

- Registration of a verification challenge, which generates a transaction on the Ethereum blockchain, took approximately 3 s on average to complete. Querying for an existing credential from the large pool of certificates stored within the system required 6–7 s.
- Verification of credential proofs via an arithmetic circuit incurs no meaningful time cost, with a maximum observed execution time of just 0.5 s. This operation leverages hardware optimizations to efficiently implement zero-knowledge proofs.

[1] https://github.com/phongkhuu115/CrossCert.

– Finally, passing data between chains, such as calling another smart contract on a separate blockchain and generating a cross-chain transaction, took an average of 5 s. This step necessarily interacts with multiple blockchains and thus incurs confirmation delay overhead.

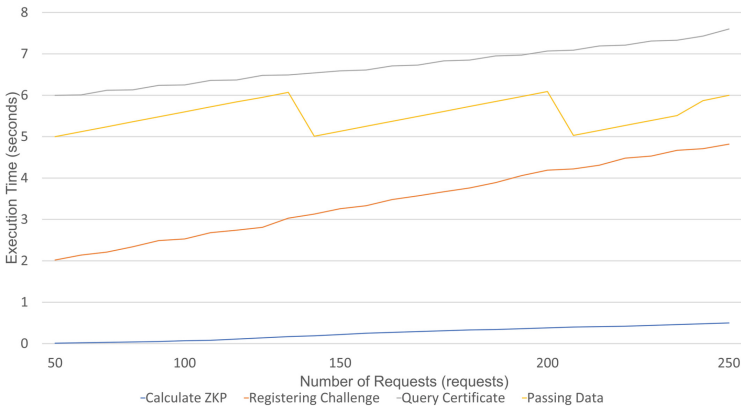

Fig. 3. Variation of Execution Time with Number of Requests

Through leveraging asynchronous programming paradigms, our system architecture was able to concurrently execute multiple transactions in parallel. We conducted performance benchmarking to quantify the maximum requests per second (RPS) that our test network infrastructure could sustain under load. By implementing an asynchronous transaction processing model, we observed a throughput of over 250 RPS for the Verify Proof Action operation. This result signifies that an asynchronous programming approach allowed the system to service a significantly higher volume of concurrent requests compared to a synchronous model by overlapping I/O wait times and avoiding blocking on individual operations. Further optimization may yield even higher scalability through continued exploitation of asynchronous processing techniques to achieve non-blocking parallelism.

However, it should be noted that the RPS does not guarantee the completion of all requests within a second, as the throughput is ultimately limited by the capacity of the blockchain. At present, the Ethereum mainnet can support approximately 10–15 transactions per second. Empirical evidence indicates a positive correlation between transaction execution time and CPU usage. As the duration of a transaction increases, there is a corresponding increase in the percentage of CPU resources utilized. Notably, the transaction involving a certificate query with the longest observed execution time of 7.6 s exhibited the highest CPU utilization at 50.24%. This observation suggests that longer-running queries impose greater demands on processing power, as more CPU cycles are required to execute transactions that take a longer time to complete. The relationship

between the number of requests, CPU usage, and program execution time is depicted in Fig. 4 and Fig. 3, providing visual insights into these associations.

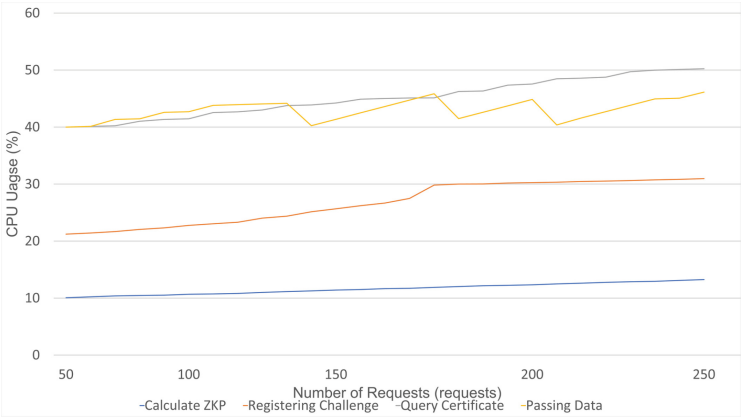

Fig. 4. CPU Usage on number of requests

In other words, the profiled execution times, RPS indicates the CrossCert system can achieve real-time verification performance while relying on underlying blockchain infrastructures still in early development and deployment stages. The prospect of further optimizations holds promise for even greater cost reductions. Each transaction or smart contract function call on our test network incurred only the basic gas fees required by the underlying blockchains, with no extra charges imposed by our system. Therefore, transaction costs would be comparable to operating directly on the magnets. As shown in Table 2, quantitative data on system performance was collected and summarized.

Table 2. The average execution time and gas fee of operation

Object	Transaction	Request per second	Gas per Request	USD
Blockchain Entities	Register Challenges	157	26.361	3.95
CrossCert	Query Certificate	68	778.565	116.78
	Pass Verification Proof	92	46.249	6.94
zk-SNARK	Generate Proof	246	0	0
	Verify Proof	238	0	0

4.3 Security Analysis

An extensive security analysis of the CrossCert cross-chain framework was conducted, with a focus on evaluating the inherent blockchain trilemma tradeoffs between security, decentralization, and scalability. Additionally, the privacy

preservation capabilities were analyzed. While CrossCert aims to bolster security and privacy for cross-chain transactions, the fundamental security properties of the involved blockchains remain contingent on their individual designs. However, our experiments offer valuable insights into CrossCert's security model.

Well-established cross-chain attack techniques, such as transaction forgery and double spending, were implemented to assess CrossCert's resilience. Leveraging zero-knowledge proofs cryptographically, CrossCert maintains the privacy of transaction contents and verification challenges within the system. Through deploying exemplar smart contracts and calculating ZKPs utilizing existing frameworks, we found it computationally infeasible to generate falsified proofs due to the cryptographic properties of ZKPs. Specifically, CrossCert's unique ZKP configuration prevents the reuse of stolen challenges or proofs in our verification module. Moreover, we tested the decentralized application's web interface for cross-site scripting and input validation vulnerabilities by submitting malicious inputs to smart contracts. The application employs input sanitization and language security features to mitigate such risks, enhancing the overall security posture.

Regarding decentralization, CrossCert functions as a verification node between chains without persisting data long-term. The certificate's data is utilized instantly for zero-knowledge proof calculation. While a single CrossCert node can hypothetically introduce centralization per the notary scheme's nature, deploying multiple nodes maintains the decentralization of the whole cross-chain system. With respect to interoperability and scalability, CrossCert can interact with diverse blockchains by deploying necessary smart contracts and configuring network identifiers. This extensible design aims to facilitate cross-chain interactions at scale across varying blockchain architectures.

By harnessing zk-SNARKs, individuals can establish ownership of specific information within their credentials without revealing their complete portfolio. This is achieved without requiring direct interaction between the candidate and the potential employer. Furthermore, by directly inputting the credential contents into the ZKP module for proof generation, CrossCert ensures the user's data is not retained or stored by CrossCert or any blockchain networks, except the originating blockchain where the credential information is provided. Consequently, this approach effectively safeguards user privacy, aligning with the intended objective.

5 Conclusions and Future Work

This work introduces CrossCert, a decentralized application-based cross-chain framework designed for privacy-preserving educational credential verification. The architecture of CrossCert serves as a decentralized application that leverages cross-chain technologies, facilitating interoperability among blockchains. This innovative approach addresses the issue of "isolated islands" by enabling the sharing of academic certificate data across different blockchains that traditionally operated independently. Moreover, CrossCert integrates the use of

zero-knowledge proofs, ensuring that candidates' qualifications can be verified without compromising their personal information or necessitating direct interaction with employers during the verification process. This robust privacy protection mechanism was successfully validated through experimental results, which demonstrated CrossCert's ability to achieve real-time verification performance while maintaining acceptable levels of transaction processing times and costs. Through an overall security assessment, our findings indicate that the system effectively ensures the balance between the properties in the trilemma blockchain while protecting the privacy of user data.

However, there is potential for further optimizations to minimize computational overhead. Looking ahead, the focus will shift towards expanding the scope of applications beyond certificate verification to encompass other domains within the education and employment sectors. As an example, extending the framework could allow candidates to prove qualification equivalence without disclosing their complete certificates. Notably, collaborations with industry partners will play a pivotal role in evaluating usability and addressing adoption challenges in real-world contexts.

Acknowledgment. This research is funded by the University of Information Technology - Vietnam National University Ho Chi Minh City under grant number D1-2024-02.

References

1. Kaneriya, J., Patel, H.: A secure and privacy-preserving student credential verification system using blockchain technology. Int. J. Inf. Educ. Technol. **13**(8) (2023)
2. Christa, S., Mittal, T.: Blockchain enabled marksheets and degree certificates. In: AITC-2023 and CSSP-2023, p. 122 (2023)
3. Lohit, A., Makode, P.: Blockchain application in the elimination of scholarship-based manipulation. Int. J. Appl. Sci. Eng. **10**, 2289–2296 (2022)
4. Monrat, A., Schel'en, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
5. Han, P., Yan, Z., Ding, W., Fei, S., Wan, Z.: A survey on cross-chain technologies. Distrib. Ledger Technol. **2**(2), 1–30 (2023)
6. Hardjono, T.: Blockchain gateways, bridges and delegated hash-locks. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LNCS, vol. 12605, pp. 71–86 (2021)
7. Sharma, N., Afzal, M., Dixit, A.: Blockchain-blockcerts based birth/death certificate registration and validation. Int. J. Inf. Technol. (IJIT) **6**(2) (2020)
8. Kamil, M., Sunarya, P., Muhtadi, Y., Adianita, I., Anggraeni, M.: BlockCert higher education with public key infrastructure in Indonesia. In: 2021 9th International Conference on Cyber and IT Service Management (CITSM), pp. 1–6. IEEE (2021)
9. Gayathiri, A., Jayachitra, J., Matilda, S.: Certificate validation using blockchain. In: 2020 7th International Conference on Smart Structures and Systems (ICSSS), pp. 1–4. IEEE (2020)
10. Abid, A., Cheikhrouhou, S., Kallel, S., Jmaiel, M.: Novidchain: blockchain based privacy-preserving platform for Covid-19 test/vaccine certificates. Softw. Pract. Exper. **52**(4), 841–867 (2022)

11. Wu, W., Liu, E., Gong, X., Wang, R.: Blockchain based zero-knowledge proof of location in IoT. In: ICC 2020-2020 IEEE International Conference on Communications (ICC), pp. 1–7. IEEE (2020)
12. Do, B.-L., Nguyen, V.-T., Dinh, H.-N., Dao, T.-C., Nguyen, B.: Blockchain for education: verification and management of lifelong learning data. Comput. Syst. Sci. Eng. **43**(2) (2022)
13. Anwar, A.S., Rahardja, U., Prawiyogi, A.G., Santoso, N.P.L., Maulana, S.: Ilearning model approach in creating blockchain based higher education trust. Int. J. Artif. Intell. Res. **6**(1) (2022)
14. Kumar, A., Bindushree, T., Pasha, A., Chandana, M., Yashashwini, H.: Verification and validation of degree certificate using block chain. In: 2022 7th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 548–553 (2022)
15. Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019)
16. Rawat, R.: A systematic review of blockchain technology use in e-supply chain in internet of medical things (IoMT). Int. J. Comput. Inf. Manuf. (IJCIM) **2**(2) (2022)
17. Raja Santhi, A., Muthuswamy, P.: Influence of blockchain technology in manufacturing supply chain and logistics. Logistics **6**(1), 15 (2022)
18. Ghosh, P.K., Chakraborty, A., Hasan, M., Rashid, K., Siddique, A.H.: Blockchain application in healthcare systems: a review. Systems **11**(1), 38 (2023)
19. Gayathiri, A., Jayachitra, J., Matilda, S.: Certificate validation using blockchain. In: 2020 7th International Conference on Smart Structures and Systems (ICSSS), pp. 1–4 (2020)
20. Ocheja, P., Agbo, F.J., Oyelere, S.S., Flanagan, B., Ogata, H.: Blockchain in education: a systematic review and practical case studies. IEEE Access **10**, 99525–99540 (2022)
21. BR, A.K., Bindushree, T., Pasha, A., Chandana, M., Yashashwini, H.: Verification and validation of degree certificate using block chain
22. Wu, W., Liu, E., Gong, X., Wang, R.: Blockchain based zero-knowledge proof of location in IoT. In: ICC 2020 - 2020 IEEE International Conference on Communications (ICC), pp. 1–7 (2020)
23. Li, W., Guo, H., Nejad, M., Shen, C.-C.: Privacy-preserving traffic management: a blockchain and zero-knowledge proof inspired approach. IEEE Access **8**, 181733–181743 (2020)
24. Luong, D.A., Park, J.H.: Privacy-preserving blockchain-based healthcare system for IoT devices using ZK-snark. IEEE Access **10**, 55739–55752 (2022)
25. Li, Q., Xue, Z.: A privacy-protecting authorization system based on blockchain and ZK-snark. In: Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies, ser. CIAT 2020. Association for Computing Machinery, New York, pp. 439–444 (2021)
26. Kotey, S.D., Tchao, E.T., Ahmed, A.-R., et al.: Blockchain interoperability: the state of heterogenous blockchain-to-blockchain communication. IET Commun. **17**(8), 891–914 (2023)
27. Duan, L., Sun, Y., Ni, W., Ding, W., Liu, J., Wang, W.: Attacks against cross-chain systems and defense approaches: a contemporary survey. IEEE CAA J. Automatica Sinica **10**(8), 1647–1667 (2023)
28. Mao, H., Nie, T., Sun, H., Shen, D., Yu, G.: A survey on cross-chain technology: challenges, development, and prospect. IEEE Access **11**, 45527–45546 (2023)

29. Haugum, T., Hoff, B., Alsadi, M., Li, J.: Security and privacy challenges in blockchain interoperability - a multivocal literature review. In: Proceedings of the 26th International Conference on Evaluation and Assessment in Software Engineering, ser. EASE 2022, pp. 347–356. Association for Computing Machinery, Gothenburg (2022)
30. Wang, G., Wang, Q., Chen, S.: Exploring blockchains interoperability: a systematic survey. ACM Comput. Surv. **55**(13s), 1–38 (2023)
31. Ou, W., Huang, S., Zheng, J., Zhang, Q., Zeng, G., Han, W.: An overview on cross-chain: mechanism, platforms, challenges and advances. Comput. Netw. **218**, 109378 (2022)
32. Frauenthaler, P., Sigwart, M., Spanring, C., Schulte, S.: Leveraging blockchain relays for cross-chain token transfers. Gas **300**, 600 (2020)
33. Lv, Z., Wu, D., Yang, W., Duan, L.: Attack and protection schemes on fabric isomorphic crosschain systems. Int. J. Distrib. Sensor Netw. **18**(1), 15501477211059944 (2022)