SECUREBLOCKCERT: ENHANCING THE SECURITY, PRIVACY, AND SCALABILITY OF EDUCATIONAL DIGITAL CREDENTIALS THROUGH BLOCKCHAIN

OMAR SAAD SALEH

DOCTOR OF PHILOSOPHY
UNIVERSITI UTARA MALAYSIA
2024

Awang Had Salleh
Graduate School
of Arts And Sciences

Universiti Utara Malaysia

PERAKUAN KERJA TESIS / DISERTASI
(Certification of thesis / dissertation)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

OMAR SAAD SALLEH

calon untuk Ijazah **PhD**
(candidate for the degree of)

telah mengemukakan tesis / disertasi yang bertajuk:
(has presented his/her thesis / dissertation of the following title):

"SECUREBBLOCKCERT: ENHANCING THE SECURITY, PRIVACY, AND SCALABILITY OF EDUCATIONAL DIGITAL CREDENTIALS THROUGH BLOCKCHAIN"

seperti yang tercatat di muka surat tajuk dan kulit tesis / disertasi.
(as it appears on the title page and front cover of the thesis / dissertation).

Bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan, sebagaimana yang ditunjukkan oleh calon dalam ujian lisan yang diadakan pada : **15 Ogos 2024.**
That the said thesis/dissertation is acceptable in form and content and displays a satisfactory knowledge of the field of study as demonstrated by the candidate through an oral examination held on: ***15 August 2024.***

Pengerusi Viva: *(Chairman for VIVA)*	**Prof. Dr. Huda Haji Ibrahim**	Tandatangan *(Signature)* Huda
Pemeriksa Luar: *(External Examiner)*	**Prof. Ts. Dr. Salman Yussof**	Tandatangan *(Signature)*
Pemeriksa Dalam: *(Internal Examiner)*	**Prof. Ts. Dr. Suhaidi Hassan**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Prof. Dr. Osman Ghazali**	Tandatangan *(Signature)*
Nama Penyelia/Penyelia-penyelia: *(Name of Supervisor/Supervisors)*	**Prof. Dato' Dr. Norbik Bashah Idris**	Tandatangan *(Signature)*

Tarikh:
(Date) ***15 August 2024***

Permission to Use

In presenting this thesis in fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

Abstrak

Dalam era digital masa kini, memastikan keaslian dan integriti sijil pendidikan menjadi keutamaan untuk mengatasi isu pemalsuan dan meningkatkan kepercayaan masyarakat. Walaupun teknologi blockchain menawarkan ciri tidak boleh diubah dan ketelusan yang sesuai untuk tujuan ini, sistem sijil digital semasa yang menggunakan blockchain masih menghadapi cabaran besar dalam mencapai keseimbangan antara keselamatan, privasi, dan skalabiliti. Kajian ini memperkenalkan SecureBlockCert, sebuah rangka kerja baharu berasaskan blockchain yang dirancang khusus untuk meningkatkan keselamatan dan privasi sijil digital sambil menangani isu skalabiliti. Menggunakan platform Hyperledger Fabric, SecureBlockCert memanfaatkan teknik kriptografi canggih seperti Kriptografi Lengkung Elips (Elliptic Curve Cryptography - ECC), EdDSA untuk tandatangan selamat, dan penyulitan homomorfik sepenuhnya bersama SHA-256, bagi melindungi data daripada akses tidak sah dan penyalagunaan. Tambahan pula, rangka kerja ini mengintegrasikan kontrak pintar (smart contracts), Pengenal Terdesentralisasi (Decentralized Identifiers - DIDs), dan Sijil Boleh Disahkan (Verifiable Credentials - VCs) untuk menyokong proses pengeluaran dan pengesahan sijil secara cekap dalam ekosistem blockchain. Pembangunan SecureBlockCert dijalankan secara berperingkat, termasuk pemodelan konsep, reka bentuk rangka kerja, pengesahan oleh pakar, dan penilaian prestasi yang teliti. Analisis keselamatan formal dilakukan menggunakan Tamarin Prover, manakala penilaian prestasi dilakukan dengan Hyperledger Caliper. Hasil eksperimen menunjukkan keupayaan SecureBlockCert untuk mencapai kadar transaksi dan latensi yang jauh lebih baik berbanding sistem sedia ada, dengan purata kadar bacaan melebihi 140 transaksi sesaat (TPS) dan latensi yang sangat minimum, sekali gus menonjolkan skalabiliti dan kecekapan rangka kerja ini. Dengan gabungan mekanisme keselamatan, privasi, dan skalabiliti, SecureBlockCert menawarkan penyelesaian inovatif untuk pengurusan sijil pendidikan. Ia juga berpotensi untuk diterapkan dalam pelbagai sektor lain yang memerlukan proses pengesahan sijil. Rangka kerja ini menyediakan asas untuk membangunkan ekosistem digital yang dipercayai, sambil menetapkan piawaian baharu dalam pengurusan sijil digital yang selamat dan menjaga privasi.

Kata Kunci: Blockchain, Sijil Digital, Keselamatan Data, Privasi Data, Skalabiliti.

Abstract

In the modern digital era, ensuring the authenticity and integrity of educational credentials is critical to countering credential forgery and fostering trust. While blockchain technology offers immutability and transparency that make it ideal for this purpose, current digital credential systems on the blockchain face significant limitations in effectively balancing security, privacy, and scalability. This study introduces SecureBlockCert, a novel blockchain-based framework designed to enhance the security and privacy of digital credentials while addressing scalability challenges. Built on Hyperledger Fabric, SecureBlockCert integrates advanced cryptographic techniques such as Elliptic Curve Cryptography (ECC), EdDSA for secure signatures, and fully homomorphic encryption, along with SHA-256 for data privacy, fortifying credential systems against unauthorized access and misuse. Additionally, the framework leverages smart contracts, Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs) to streamline credential issuance and verification. The framework's development follows a phased methodology, including conceptual modeling, framework design, expert validation, and rigorous performance assessment. Formal security analysis is conducted using the Tamarin Prover, while system performance is evaluated with Hyperledger Caliper. Experimental results demonstrate SecureBlockCert's capability, achieving significant improvements in transaction throughput and latency compared to existing systems. It achieved an average read throughput exceeding 140 transactions per second (TPS) with minimal latency, underscoring its scalability and effectiveness. SecureBlockCert offers a foundation for trusted digital ecosystems, setting a new standard for secure, privacy-preserving credential management. Its scalability and effectiveness position it as an innovative solution for educational credentialing, with potential applications across sectors reliant on credential verification.

Keywords: Blockchain, Digital Credentials, Data Security, Data Privacy, Scalability.

Acknowledgment

In the name of ALLAH, Most Gracious, Most Merciful:
"Work; so Allah will see your work and (so will) His Messenger and the believers;"
_____(The Holy Quran - AtTawbah 9:105)

I would like to express my deepest gratitude to my supervisors, **Prof. Dr. Osman Ghazali** (School of Computing, Universiti Utara Malaysia) and **Dato' Prof. Dr. Norbik Bashah Bin Idris** (Kulliyyah of Information and Communication Technology, International Islamic University Malaysia). Their tireless encouragement, wisdom, and experience were instrumental in guiding me through my research journey. Prof. Dr. Osman Ghazali provided me with constant guidance and constructive criticism throughout all stages of my research. I am forever grateful for his patience, input, and suggestions. I must also extend my thanks and gratitude to my co-supervisor Prof. Dr. Norbik for his guidance and continuous support. His extensive knowledge of research, and serious attitude toward research have been a great source of encouragement and inspiration for me to accomplish this research. He generously shared his experience and research ideas, both practical and theoretical, and motivated me during my most critical moments to complete my PhD journey. I am honored and grateful to have had the privilege of studying under their supervision, and without their valuable support, my thesis would not have been possible.

I would like to acknowledge the support and understanding of my wife Samar Hazim Mohammad and my children Mohammad and Lara, whose unwavering support, encouragement, and understanding have enabled me to devote myself to my thesis activities.

My grateful thanks also go to the Dean of Awang Had Salleh Prof. Dr. Norhafezah Yusof and Deputy Dean Dr. Siti Nazuar Sailin, whose support and assistance have been invaluable to me throughout my studies. Their prompt responses to my inquiries have been of great help.

Lastly, I would like to extend my gratitude to my beloved Universiti Utara Malaysia for entrusting me with the opportunity to pursue and complete my PhD journey. It has been an unforgettable and enriching experience that has contributed significantly to my personal and professional growth.

Table of Contents

List of Tables

List of Figures

List of Appendices

List of Abbreviations

VC	Verifiable Credential
DID	Decentralized Identifiers
IPFS	InterPlanetary File System
EdDSA	Edwards-curve Digital Signature Algorithm
SHA	Secure Hash Algorithms
GDPR	General Data Protection Regulation
CA	Certificate Authority
POC	Proof of Concept
KYC	Know Your Customer
PoA	Proof of Authority
EARs	Electronic Academic Records
SDK	Software Development Kit
HEIs	Higher Education Institutions
BTC	Bitcoin
JSON-RPC	JavaScript Object Notation - Remote Procedure Call
eDIS	Electronic Diploma Integrity Service
TVS	Trusted Verification Scheme
PKI-CA	Public key infrastructure
DApp	Decentralized Application
TPS	Transaction Per Second
DCVPC	Decentralized Certification Verification Privacy Control
W3C	World Wide Web Consortium
APIs	Application Programming Interfaces
JSON-LD	JavaScript Object Notation for Linked Data
DLT	Distributed Ledger Technology
MSP	Membership Service Provider

Org	Organization
EARs	Electronic Academic Records

CHAPTER ONE
INTRODUCTION

1.1 Research Background

In the digital era, digital credentials have become pivotal in both academic and professional domains. These credentials, which include degrees, diplomas, certificates, and transcripts, signify the completion of courses, mastery of skills, or acquisition of knowledge in various subjects [1]. Such electronic records are crucial for verifying educational achievements, often serving as prerequisites for employment, further education, or professional certifications. Traditionally, academic credentials were issued as physical documents with qualities such as authenticity and durability. However, these paper-based credentials have several limitations, including susceptibility to loss, challenges in verification, and high costs associated with printing and distribution. Furthermore, the verification process of physical credentials is often time-consuming and environmentally taxing [2]. In response, digital certificates, or e-certificates, have emerged as an innovative solution to overcome these limitations, offering efficiency and enhanced access to educational records [3].

Digital credential systems typically involve three primary roles: the issuer (educational institutions), the recipient (students), and the verifier (employers or educational institutions) [4]. While these systems streamline the issuance and verification of credentials, they still face challenges, particularly concerning privacy, security, and scalability. The increasing prevalence of fraudulent academic credentials exacerbates the need for secure, tamper-proof systems that can protect the integrity of the credentialing process [5].

Blockchain technology has emerged as a promising solution to these challenges, offering decentralization, immutability, and transparency [6]. However, the application of blockchain in digital credentialing presents several complexities. Most

blockchain systems, such as Blockcerts, have proven to be secure and transparent, yet they face critical limitations. These include performance bottlenecks during high transaction volumes, privacy risks associated with publicly accessible data, and insufficient control over credential data shared with verifiers [7]. Privacy, in particular, is a significant concern, as blockchain's transparency can expose sensitive personal information [8]. Existing blockchain-based systems like Blockcerts have addressed privacy through pseudonymity, but re-identification risks remain due to correlation attacks [9]. Additionally, current blockchain frameworks struggle to scale effectively when processing a large number of credentials, leading to delays and inefficiencies [10].

To address these challenges, this research proposes the SecureBlockCert Blockchain framework, which integrates advanced cryptographic techniques and decentralized technologies to provide a more secure, privacy-preserving, and scalable solution for digital credential systems. SecureBlockCert incorporates asymmetric cryptography for robust authentication and communication, ensuring that credentials are securely issued and verified without risk of tampering or unauthorized access. Homomorphic encryption is employed to protect user privacy, allowing computations on encrypted data without revealing the underlying information, a key advancement over existing systems that do not offer such privacy guarantees [11].

In addition, SecureBlockCert employs smart contracts to automate the issuance, verification, and revocation of digital credentials, reducing human error and operational costs while ensuring a transparent audit trail. Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) provide self-sovereign identities for users, empowering them with greater control over their credential data and ensuring compliance with GDPR and other privacy regulations [12].

By integrating these technologies within the Hyperledger Fabric platform, SecureBlockCert overcomes the scalability challenges seen in permissionless blockchains like Blockcerts. Hyperledger Fabric's modular architecture allows for private channels, ensuring that credential transactions are processed efficiently and securely, even as the system scales to accommodate a growing number of users and transactions [13].

In conclusion, SecureBlockCert Blockchain sets a new standard for secure, scalable, and privacy-preserving digital credential management. It provides an integrated framework that addresses the limitations of existing blockchain systems by combining advanced cryptographic techniques, decentralized identity management, and privacy-preserving technologies, making it a compelling solution for educational institutions and other credentialing bodies seeking to secure their credentialing processes in the digital age.

1.2 Problem Statement

Digital credential systems, such as those used to issue diplomas and certificates, have become increasingly essential for educational institutions and students [14]. These systems offer significant advantages by streamlining the authentication and verification of academic achievements in a digital format, improving efficiency, and accessibility, and reducing administrative overhead associated with traditional paper-based credentials [15, 16]. However, despite these benefits, digital credential systems still face substantial challenges, particularly in maintaining the security, privacy, and integrity of sensitive personal data [8].

Many of the existing digital credential platforms rely on centralized models, most commonly using Certificate Authorities (CAs) to manage the issuance and verification of credentials [17, 18]. While CAs play a crucial role in traditional public key

infrastructures, their centralized nature introduces significant vulnerabilities. Centralized CAs act as single points of failure and are prone to security breaches that can compromise the entire credential system [17]. In contrast, decentralized systems like Blockcerts provide a transparent and tamper-resistant method for issuing and verifying credentials, addressing some of these concerns [19]. However, Blockcerts has faced privacy challenges, as its reliance on public blockchains risks exposing sensitive personal data to re-identification through correlation attacks, and its scalability remains limited when handling large volumes of credentials during peak periods [7]. These vulnerabilities highlight the need for a more decentralized and resilient infrastructure that mitigates risks associated with centralized control while addressing privacy and scalability challenges.

While blockchain technology has emerged as a promising solution to address the decentralization problem, several critical issues remain unresolved, particularly in terms of privacy and scalability [20, 21]. One of the primary challenges of using public blockchains for credentialing systems is the potential exposure of sensitive personal data [8, 22]. Blockchains, by design, are transparent and immutable, meaning that all transactions are visible to every participant on the network. This poses a significant risk to the privacy of students, as their educational records, if not properly secured, can be viewed by unauthorized parties. Although some blockchain implementations, like Blockcerts, utilize pseudonymity to mask identities, this does not fully address the privacy concerns, as data can often be re-identified through advanced analytics or correlation attacks [23]. Furthermore, public blockchains do not inherently provide mechanisms for selective data sharing, leaving users with limited control over which information is disclosed and to whom [21]. This lack of granular privacy controls is a

major barrier to adoption, especially in jurisdictions with stringent data protection laws like the General Data Protection Regulation (GDPR) [8].

In addition to privacy concerns, ensuring the integrity of credentials on blockchain-based systems remains a significant challenge [9]. While blockchain's immutability ensures that records cannot be altered once written, ensuring the tamper-resistance of credentials during their lifecycle from issuance to verification requires robust cryptographic mechanisms. However, many existing systems fail to implement sufficient safeguards to protect against unauthorized modifications or revocations [24]. As a result, there are potential security gaps in ensuring that credentials remain both accurate and authentic throughout their usage.

Another critical issue is scalability [25]. Current blockchain-based digital credential systems, including Blockcerts, struggle to efficiently manage the large volumes of credentials generated by educational institutions [26]. Blockchains typically face performance bottlenecks as the number of transactions increases, leading to higher processing times and reduced throughput, especially during peak periods of credential issuance and verification. These scalability limitations not only affect the user experience but also compromise the system's ability to maintain robust security and privacy protections under high demand. This problem is exacerbated in permissionless blockchains, where consensus mechanisms like proof-of-work can introduce significant latency .

While blockchain offers potential solutions to the challenges faced by digital credential systems, current implementations, such as Blockcerts, fail to adequately address the intertwined issues of security, privacy, and scalability. A decentralized, privacy-preserving solution that enhances both the protection of personal data and the system's capacity to scale is urgently needed to ensure the integrity and confidentiality of digital

credentials. This research proposes to develop SecureBlockCert, a framework leveraging advanced cryptographic techniques like homomorphic encryption and decentralized technologies such as elliptic curve cryptography and smart contracts, to create a more secure, scalable, and privacy-preserving digital credential system for the educational sector.

1.3 Research Questions

The main research question is how can the SecureBlockCert framework be designed and implemented to enhance security (through authentication and data integrity mechanisms) and privacy (by ensuring confidentiality and data protection) in blockchain-based digital credential systems, specifically within the environment of educational institutions using permissioned blockchain networks?

a) How can the authentication mechanism, specifically through cryptographic key exchange protocols and identity verification schemes, be enhanced within the SecureBlockCert framework to strengthen protection against unauthorized access during entity registration?
b) What are the privacy-preserving techniques that can be applied within the SecureBlockCert framework to ensure the confidentiality and protection of credential data, while maintaining data utility and compliance with privacy regulations?
c) How can the issuance and verification processes within the SecureBlockCert framework be optimized to reduce latency, improve transparency, and ensure the immutability and accuracy of digital credentials?
d) How does the SecureBlockCert framework perform in terms of throughput, latency, and resistance to security attacks?

1.4 Research Objectives

The main objective of this research is to develop and evaluate the SecureBlockCert Blockchain framework to enhance security (through improved authentication and data integrity) and privacy (through confidentiality of credential data) in blockchain-based digital credential systems. Sub-objectives are:

a) To develop a security mechanism within the SecureBlockCert framework that enhances authentication during entity registration, using cryptographic schemes to improve data integrity and protect against unauthorized access.
b) To design a privacy-preserving mechanism within the SecureBlockCert framework using homomorphic encryption and access control algorithms to safeguard sensitive data during credential issuance and verification.
c) To construct an efficient issuance and verification mechanism within the SecureBlockCert framework using smart contracts to address issues of transparency, latency, and immutability in digital credential systems.
d) To evaluate the performance and security of the SecureBlockCert Blockchain framework using metrics, including throughput, latency, and resistance to attacks.

1.5 Research Scope

This research focuses on the design, implementation, and evaluation of the SecureBlockCert Blockchain framework within the Hyperledger Fabric platform. Hyperledger Fabric has been selected for its modular and permissioned architecture, which supports strong privacy and confidentiality, aligning with the security requirements of digital credential systems. The scope includes the development of cryptographic protocols based on asymmetric cryptography and digital signatures. These methods ensure that participant identities are securely verified and that each

transaction on the blockchain is both authentic and non-repudiable, providing a robust foundation for a secure credential system. The integration of homomorphic encryption forms a crucial aspect of the privacy-preserving measures within our framework. Homomorphic encryption enables computations on encrypted data without revealing the underlying information, ensuring compliance with stringent data protection standards. This technique will be explored within the context of digital certificates, focusing on how privacy can be maintained even during credential verification.

Our research also encompasses the development and implementation of access control mechanisms. These mechanisms will ensure that only authorized entities, such as credential issuers and verifiers, can interact with the digital credentials. By leveraging Hyperledger Fabric's fine-grained permissioning capabilities, we will design and enforce sophisticated access controls to maintain system security and data integrity.

Additionally, smart contracts (or chain code in Hyperledger Fabric terminology) will be a core component of the SecureBlockCert Blockchain framework. These self-executing programs will automate the lifecycle management of digital certificates, handling processes such as issuance, verification, revocation, and expiration. Smart contracts will ensure that business logic is enforced without requiring human intervention, facilitating trustless interactions between participants. A key feature of the framework is the incorporation of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). DIDs will serve as unique identifiers for entities, enabling verifiable and self-sovereign identities on the blockchain. VCs will allow for the verification of qualifications and attributes without exposing personal data, thus enhancing privacy while ensuring trust and interoperability. The research will also explore the practical application of this framework within academic and professional settings, addressing the architectural and operational challenges involved in real-world

deployments. However, the study will not delve into optimizing the performance of Hyperledger Fabric or exploring sectors outside of credential management. By focusing on these aspects, the SecureBlockCert Blockchain framework aims to significantly improve the security, privacy, and efficiency of digital credential systems.

1.6 Research Contributions

This research makes significant contributions to both the theoretical and practical domains of blockchain applications for digital certificate systems. The key contributions are as follows:

a) **Development of the SecureBlockCert Blockchain Framework**: This research introduces the SecureBlockCert Blockchain framework, a new approach that integrates advanced security and privacy features tailored specifically for digital credential systems. Unlike existing solutions, this framework combines asymmetric cryptography, homomorphic encryption, and smart contracts to deliver a comprehensive security solution. It directly addresses the gaps in authentication, privacy, and scalability that have persisted in previous blockchain-based credential systems.

b) **Exploration and Integration of Cryptographic Techniques**: The research offers an in-depth exploration of advanced cryptographic techniques such as homomorphic encryption and digital signatures within a blockchain framework. By demonstrating their practical implementation, this work shows how these cryptographic methods can enhance both security and privacy in digital credential systems, providing new insights into the use of homomorphic encryption for privacy-preserving computations and digital signatures for secure, verifiable transactions.

c) **Blockchain Application in Digital Credential Systems**: This work extends the application of Hyperledger Fabric beyond traditional cryptocurrency contexts by demonstrating its suitability for secure and private digital credential management. Through practical implementation, this research highlights the adaptability of Hyperledger Fabric's modular architecture for educational credential systems, offering a blueprint for decentralized, permissioned blockchain networks designed to meet the security and privacy needs of academic and professional sectors.

d) **New Security Evaluation Methodology**: A significant contribution of this thesis is the introduction of a tailored set of security performance metrics for blockchain-based certificate systems. This includes metrics for evaluating authentication mechanisms, privacy-preserving techniques, data integrity, and system scalability. These evaluation techniques provide a structured methodology for assessing the effectiveness of the security and privacy features integrated into blockchain-based credentialing systems, filling a critical gap in the current literature.

e) **Prototype Development and Proof of Concept:** The creation of a functional prototype of the SecureBlockCert Blockchain framework serves as a proof of concept, demonstrating the operational viability of the proposed system.

This prototype is a valuable resource for future researchers and developers working on blockchain-based credential systems, offering a practical reference model for the deployment of secure and scalable digital credentials.

f) **Identification of Research Gaps and New Avenues:** Through an exhaustive literature review, this research identifies key gaps in existing blockchain implementations for digital credentials, specifically in areas such as privacy, authentication, and scalability. The work suggests new research avenues by proposing novel solutions, such as the integration of homomorphic encryption for privacy-preserving credential verification and decentralized identifiers for self-sovereign digital identities.

g) **Expert Review and Interdisciplinary Collaboration:** This research incorporates an expert review phase to align the development of the SecureBlockCert Blockchain framework with industry standards and practical needs. Feedback from experts in cryptography, blockchain technology, and educational credentialing has been integrated into the design, ensuring the framework meets both theoretical and practical expectations, while emphasizing the importance of interdisciplinary collaboration for addressing real-world challenges in digital credential systems.

1.7 Significance of Study

The SecureBlockCert framework holds significant potential in improving the security and privacy of digital credential systems by leveraging the decentralized, immutable nature of blockchain technology. In today's digital landscape, where credential fraud and privacy breaches are prevalent, the SecureBlockCert framework addresses critical gaps in current digital credential systems, which often rely on centralized models that are prone to security vulnerabilities. Key contributions of this framework include enhanced security through asymmetric cryptography for secure authentication and the use of blockchain to ensure the immutability of credential records.

Unlike traditional digital credential systems that rely on central authorities (e.g., Certificate Authorities) and can be subject to single points of failure, SecureBlockCert introduces a distributed trust model, where credentials are verified through decentralized consensus, reducing the risk of forgery and tampering.

In terms of privacy, the framework employs advanced privacy-preserving techniques such as homomorphic encryption. This enables sensitive data to remain confidential even during computations, which is not a standard feature in most current blockchain-based systems. By integrating privacy measures that protect both data and identity, SecureBlockCert enhances the confidentiality of student information while maintaining transparency and verifiability. Furthermore, SecureBlockCert stands out by embedding smart contracts into the credential issuance and verification processes, automating these procedures with minimal human intervention. This automation leads to operational efficiencies by reducing administrative overhead, minimizing the risk of human error, and speeding up the verification process.

While traditional systems often face delays and high costs related to manual processing and verification, SecureBlockCert offers a streamlined and cost-efficient solution that can scale easily as institutions adopt digital credentials more widely.

The real-world impact of SecureBlockCert extends to several key stakeholders:

a) For educational institutions, it provides a reliable and secure way to issue, store, and verify credentials, ensuring the integrity of their academic records.
b) For students, it offers a tamper-proof, privacy-preserving record of their achievements, enhancing their control over personal information.
c) For employers and verifiers, it allows for fast and trustworthy verification of qualifications, reducing time and costs associated with traditional verification methods.

By comparing blockchain-based digital credential systems with and without the SecureBlockCert framework, the differences become clear. Without SecureBlockCert, current systems are more vulnerable to attacks on central authorities, have weaker privacy protections, and require more manual intervention. With SecureBlockCert, the system benefits from decentralized trust, stronger privacy measures, and improved efficiency, making it a more secure and scalable solution for digital credentialing. In conclusion, SecureBlockCert aims to significantly transform the academic and employment sectors by promoting a culture of trust, transparency, and privacy in the digital credentialing process. Its contribution lies not just in the technical implementation of blockchain and cryptography, but in its ability to redefine how digital credentials are managed and verified securely and efficiently in the modern world.

1.8 Thesis Organization

This thesis is organized into six chapters, each building upon the foundation set by the introductory material and progressively delving into the research.

a) **Chapter One** introduces the study by outlining the motivation, defining the research questions, objectives, scope, and highlighting the study's significance and contributions.

b) **Chapter Two** provides a comprehensive review of relevant literature to establish a theoretical background and identify gaps that this research seeks to address.

c) **Chapter Three** describes the research methodology, detailing the conceptual model, verification process, and performance metrics for security and privacy.

d) **Chapter Four** introduces both the initial design and the refined architecture of the SecureBlockCert Blockchain framework, incorporating expert-reviewed enhancements and outlining the technical specifications necessary for achieving robust security and privacy. This chapter also details the proposed mechanisms designed to preserve security, privacy, and scalability, thereby addressing the key challenges in digital credential management.

e) **Chapter Five** focuses on the implementation and evaluation of the SecureBlockCert framework, showcasing experimental results, and providing a comparative analysis of the framework's security and privacy aspects.

f) **Chapter Six** concludes the thesis by summarizing key findings, discussing contributions and limitations, and proposing avenues for future work to enhance the security and privacy of digital certificate systems.

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

The digitization of educational credentials has transformed how academic achievements are recorded, verified, and shared, but it also introduces challenges, particularly in security, privacy, and scalability. This chapter reviews the current landscape of digital credential systems, focusing on the potential of blockchain technology to address the limitations of traditional methods.

We begin by examining the concept of educational digital credentials and the critical security and privacy requirements for these systems, especially under regulations like GDPR. The chapter then explores blockchain technology, its core principles, and its application in digital credential management, including an analysis of different blockchain platforms and their operational steps.

The review assesses existing blockchain-based credential systems, highlighting their strengths and identifying significant gaps, particularly in security, privacy, and scalability. These gaps underscore the need for more robust solutions, which this chapter aims to address through the introduction of a conceptual framework designed to enhance current systems.

In summary, this literature review sets the foundation for developing a more secure, private, and scalable blockchain-based digital credential system, guiding the proposed solution presented in the following chapters.

2.2 Educational Digital Credential System

Educational digital credentials, often referred to as digital certificates, are formal documents issued by educational institutions to signify a student's completion of a

degree program or other educational training [27]. These credentials typically include details such as the student's name, the issuing institution, the type of degree or training received, the completion date, and other information. The significance of digital credentials lies not only in their role in verifying academic achievements but also in their widespread use for employment, further education, and other professional purposes.

Despite the advantages of digital credentials, traditional systems of issuing and verifying these certificates face significant challenges, particularly in terms of security, privacy, and efficiency [28]. Traditional methods often involve direct communication with educational institutions or third-party service providers for credential verification, which can be time-consuming, vulnerable to fraud, and difficult to scale. These limitations underscore the need for more secure and efficient solutions, such as blockchain technology, which offers enhanced security, transparency, and data integrity [29].

Digital credentials serve as the digital representations of traditional paper-based credentials and have been integral to the digitization of educational processes over the past few decades. Recent regulatory frameworks, such as the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA) in the USA, have further emphasized the importance of data privacy, user consent, and control over personal information in digital credential systems [28, 30].

A typical digital education credential system comprises several key components: the issuer, the recipient, the verifier, and the digital credential itself. The issuer, usually an educational institution, is responsible for providing the certificate to the recipient, who could be a student, graduate, or professional. The verifier, such as an employer or another educational institution, authenticates the credential by verifying the issuer's

records and the recipient's identity. The digital credential is an electronic representation of the recipient's educational achievements, qualifications, or competencies, typically stored in a digital format.

Several methodologies exist for issuing and authenticating digital educational credentials [31]. The traditional approach involves direct communication with the issuing institution, where individuals request certificates and verify their authenticity through the institution. While straightforward, this method can be cumbersome and raises concerns about data control and security. Alternatively, institutions may use third-party service providers to streamline certificate issuance and verification, offering additional services such as secure storage and digital delivery. However, this approach introduces potential data privacy concerns due to reliance on external entities.

To address these challenges, blockchain technology has emerged as a robust solution for academic certificate issuance and verification [32]. Blockchain-based systems utilize decentralized, tamper-proof digital ledgers to securely store certificate information [33]. By employing cryptographic techniques and distributed consensus, these systems ensure enhanced security, transparency, and auditability. In such a system, the issuer records the academic certificate on the blockchain, allowing the verifier to retrieve and confirm its authenticity. Successful verification results in the approval of the certificate, thereby maintaining data integrity and authenticity, as illustrated in Figure 2.1.

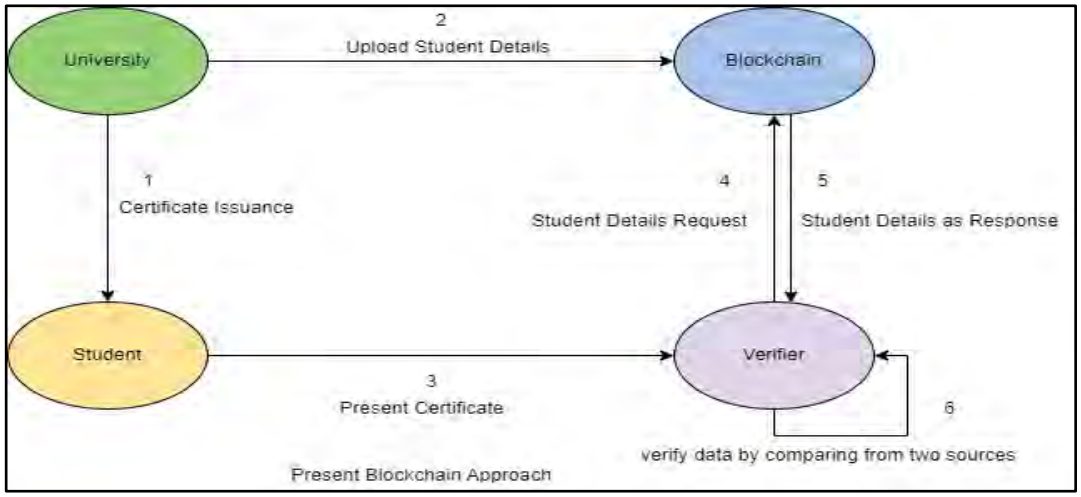

Figure 2.1 Blockchain-based Approach for Educational Digital Credential

2.3 Security and Privacy Requirements in Educational Digital Credential Systems

The digitization of educational credentials offers significant benefits, including increased efficiency and accessibility. However, it also introduces critical challenges, particularly concerning security, privacy, and scalability. As educational institutions transition from traditional paper-based credentials to digital systems, ensuring the authenticity, integrity, confidentiality, and scalability of these digital credentials has become paramount.ome paramount.

2.3.1 Security Requirements

A comprehensive framework for the security and privacy requirements in digital credential systems is essential. As articulated by A. Mühle, K. Assaf, D. Köhler, and C. Meinel [3], security measures must focus on several key aspects:

a) **Tamper Evidence**: Digital credentials must be resistant to tampering, ensuring that any unauthorized alterations are immediately detectable.

b) **Data Protection**: Strong data protection protocols are necessary to safeguard the sensitive information embedded within digital credentials, preventing unauthorized access and ensuring confidentiality.

c) **Elimination of Single Points of Failure**: The system architecture must avoid relying on centralized entities that could become targets for attacks, thus improving resilience and reliability.

d) **Verification Processes**: Robust verification mechanisms are needed to authenticate the identities of both learners and credential issuers, thereby preserving the integrity and trustworthiness of the credentials.

2.3.2 Privacy Requirements

Privacy requirements are critical in protecting individuals' personal information in digital credential systems. These include:

a) **Pseudonymity**: Protecting user identities by allowing interactions that do not reveal personal information unless explicitly required.

b) **No-Tracing**: Ensuring that user activities within the credential system cannot be tracked or monitored, thus protecting privacy.

c) **Data Minimization**: Limiting the amount of personal data collected and processed to only what is necessary for the credentialing process.

d) **Selective Disclosure**: Empower learners to control who has access to their personal information by allowing them to disclose only the necessary data for a specific verification purpose.

The integration of these security and privacy requirements is not just a technical challenge but also a compliance necessity, especially with the introduction of stringent data protection regulations like GDPR in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These regulations emphasize the importance of user consent, data protection, and the right to be forgotten issues that are particularly challenging to address in the context of immutable blockchain systems.

Tang [8] effectively addresses these challenges by identifying critical security and privacy requirements in digitized diploma management systems. The study presents a comprehensive framework that caters to both functional and non-functional requirements, such as safeguarding against the issuance of fake diplomas, preventing forgery, and mitigating the risks of issuer fraud. Additionally, the framework emphasizes the need to protect against potential corruption among diploma issuers and users, prevent the compromise of intermediary platforms, and ensure the confidentiality and integrity of diploma data.

However, while Tang [8] provides a solid foundation for addressing security and privacy concerns, it relies primarily on traditional cryptographic techniques, such as digital signatures and hash functions. Although these methods are proven and reliable, the study does not explore more advanced cryptographic techniques, such as zero-knowledge proofs or homomorphic encryption, which could offer enhanced privacy and scalability.

In contrast, Mühle et al. [3] offer a broader conceptual framework that not only focuses on security and privacy but also incorporates scalability, recognizing it as a critical factor for the effective deployment of digital credential systems. This framework emphasizes the importance of controllability, where users can manage their credentials, including issuance consent and sharing restrictions. It also introduces the concept of trust, extending beyond the technical verification of credentials to include the organizational trust needed to establish the credibility of issuers and verifiers.

When comparing these studies, it becomes evident that while Tang [8] provides the necessary technical underpinnings for security and privacy, Mühle et al. [3] offer a more comprehensive framework that includes additional considerations such as usability, trust, and scalability. Both studies highlight the importance of developing

frameworks that balance these critical aspects, but there remains a gap in integrating advanced techniques that can simultaneously address security, privacy, and scalability in large-scale, decentralized environments.

The limitations of traditional digital credential systems underscore the need for more robust, decentralized approaches, such as blockchain technology, which offers inherent features like immutability, distributed consensus, and enhanced cryptographic security. In the subsequent section, we will delve into the fundamentals of blockchain technology and explore how its characteristics align with the security and privacy requirements outlined here. This analysis will pave the way for understanding how blockchain can be effectively leveraged to overcome the limitations of traditional systems in managing educational digital credentials.

2.4 Blockchain Technology: Fundamentals and Concepts

Blockchain technology, originally conceptualized for cryptocurrency transactions, has since evolved into a powerful tool for secure data storage, management, and transfer across various sectors, including the verification of academic credentials. Its decentralized, peer-to-peer architecture eliminates the need for centralized intermediaries, thereby enhancing the reliability and security of digital systems [34].

At its core, a blockchain is a distributed ledger where each transaction is cryptographically linked to the preceding one, forming an immutable and tamper-resistant chain of records [35]. This structure not only ensures the integrity of the data but also supports transparent data sharing and secure peer-to-peer interactions through robust consensus mechanisms. One of the most significant features of blockchain technology is the use of smart contracts self-executing codes that automatically enforce predefined conditions, thereby reducing the need for intermediaries and streamlining processes [36].

2.4.1 Blockchain Architecture

Blockchain architecture comprises multiple layers, each performing distinct functions critical to the operation and security of blockchain systems. Figure 2.2 illustrates the layered architecture, which is based on the conceptual framework presented by Wang et al. [37].

a) **Application Layer**

The application layer is the topmost level where user-facing applications are developed. This layer includes smart contracts and application programming interfaces (APIs), which enable users to interact with the blockchain and implement various industry-specific solutions.

b) **Smart Contract Layer**

This layer hosts smart contracts, which are self-executing scripts that automate processes within the blockchain. These contracts follow predefined rules, ensuring tasks are carried out without the need for manual intervention.

c) **Incentive Layer**

The incentive layer is responsible for rewarding participants, such as miners, who contribute to maintaining the blockchain network. These rewards, often in the form of cryptocurrency, motivate continued participation and help secure the network.

d) **Consensus Layer**

At the consensus layer, protocols such as Proof of Work (PoW) and Proof of Stake (PoS) are employed to ensure agreement among network participants regarding the validity of transactions. This consensus is crucial for maintaining the integrity and trustworthiness of the blockchain.

e) **Network Layer**

The network layer facilitates communication between nodes in the blockchain network. It ensures that all participants have synchronized access to data and can effectively validate new blocks.

f) **Data Layer**

The data layer is the foundation of the blockchain, responsible for securely storing transaction data. This layer utilizes cryptographic techniques, such as hash functions and Merkle trees, to protect the integrity and security of the distributed ledger. Understanding these foundational principles of blockchain technology is essential for appreciating its potential as a transformative tool in the management of digital credentials. However, it is important to recognize that blockchain is not a universal solution; different types of blockchain platforms offer varying features and capabilities. The following section will explore the different types of blockchain platforms, laying the groundwork for selecting the most suitable technology to support secure and scalable digital credential systems.

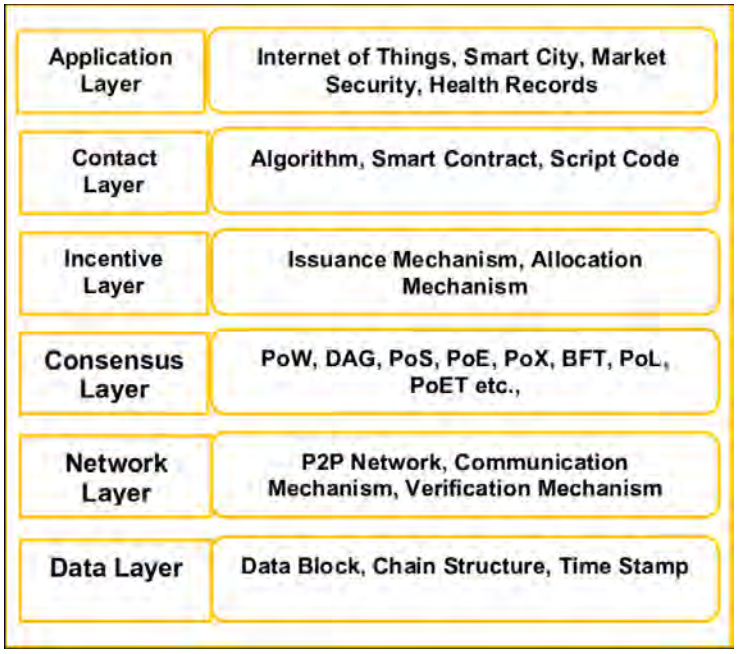

Figure 2.2 Layers of Blockchain Architecture

2.5 Types of Blockchain Platforms

Blockchain platforms can be broadly categorized into public, private, and hybrid types, each distinguished by varying levels of accessibility, control, and governance. These platforms also differ in their consensus mechanisms, approaches to distributed computing, immutability, and authentication protocols, making the choice of platform crucial for digital credential systems that must balance security, privacy, scalability, and accessibility [38].

2.5.1 Public Blockchain

Public blockchains, such as Bitcoin and Ethereum, are open to anyone without the need for prior authorization [39]. These platforms are characterized by their transparency and immutability, features that are advantageous in environments where trust and openness are paramount. In the context of digital credential systems, public blockchains ensure that credentials are universally accessible and verifiable, providing an immutable and transparent record of qualifications. However, the open nature of public blockchains may raise significant concerns regarding privacy and scalability, particularly when managing sensitive academic data.

2.5.2 Private Blockchain

Private blockchains, exemplified by platforms like Hyperledger Fabric and Corda, operate with restricted access, allowing participation only by selected entities [40, 41]. These networks emphasize data confidentiality through encryption and controlled access, making them particularly suitable for academic settings where sensitive information must be protected from unauthorized access. In digital credential systems, private blockchains ensure that only authorized institutions and stakeholders can issue,

verify, and access credentials, thereby maintaining privacy and enabling secure transactions between trusted parties.

2.5.3 Hybrid Blockchain

Hybrid blockchains, which combine elements of both public and private systems, offer a controlled yet partially decentralized platform [42]. This type of blockchain is ideal for scenarios requiring selective transparency across multiple organizations. In digital credential systems, hybrid blockchains can strike a balance between transparency and privacy, enabling universities to issue credentials that are publicly verifiable while keeping the underlying personal data private and accessible only to authorized entities.

A comparative analysis by D. Boughaci and O. Boughaci [43] of three prominent blockchain platforms Bitcoin, Ethereum, and Hyperledger illustrates the diverse attributes these platforms offer for digital credential systems. Bitcoin, renowned for its robust security and widespread adoption, may be less suitable due to its limited scripting capabilities and high transaction costs. Ethereum, with its support for smart contracts, facilitates complex credential verification processes, making it a strong candidate for systems requiring programmable logic and public accessibility. Conversely, Hyperledger, with its emphasis on privacy and permissioned networks, is particularly suited for scenarios where academic institutions need to manage credentials within a controlled environment, ensuring privacy and compliance with data protection regulations.

Each type of blockchain platform whether public, private, or hybrid presents unique advantages and challenges. Selecting the appropriate platform is critical for achieving the security, privacy, and usability objectives of digital credential systems. Building on this understanding, the next section will critically examine various security and

privacy frameworks, including those incorporating blockchain, as they have been proposed and implemented in the field of educational credentialing. This analysis will highlight the strengths and limitations of these frameworks, paving the way for the development of a more comprehensive and effective solution.

2.6 Hyperledger Fabric: A Permissioned Blockchain Platform

Hyperledger Fabric stands out as a permissioned blockchain platform, distinct from conventional public blockchains like Bitcoin and Ethereum. Designed for enterprise-level applications, Hyperledger Fabric supports a higher degree of privacy, confidentiality, and scalability [40]. Unlike public blockchains, which allow open participation and rely on resource-intensive consensus mechanisms like proof-of-work, Hyperledger Fabric restricts access to authorized participants within a permissioned network, making it an ideal solution for environments that handle sensitive data, such as educational credential systems. The platform's modular architecture enables customization of key components, including consensus mechanisms and membership services, allowing the implementation of different consensus protocols based on application needs. This flexibility, combined with its use of private channels and data collections, enhances privacy by enabling confidential transactions among designated subsets of participants. This feature is particularly valuable in educational settings where institutions need to exchange sensitive information while ensuring compliance with privacy regulations such as the GDPR.

Hyperledger Fabric also utilizes chaincode, a form of smart contract, to automate processes within the permissioned network [13]. This feature facilitates the efficient and secure issuance and verification of digital credentials, reducing the need for manual intervention and enhancing operational efficiency.

By supporting private channels, providing granular access control, and ensuring that only authorized entities can view or modify specific data, Hyperledger Fabric safeguards the integrity and confidentiality of digital credentials. These features, along with its scalable and efficient architecture, make Hyperledger Fabric a robust platform for managing and verifying academic credentials in a secure, privacy-preserving, and adaptable manner, aligning seamlessly with the goals of the privacy and security framework.

2.7 Blockchain Operational Processes in Digital Credential Systems

A thorough understanding of the fundamental processes within blockchain technology is essential for effectively leveraging this technology in digital credential systems. These foundational steps establish the security, consensus, and data integrity critical to the functioning of blockchain-based platforms, whether they operate as public, private, or hybrid systems [44].

2.7.1 Transaction Initiation

Blockchain begins when a user initiates a transaction, such as issuing or verifying an academic certificate. The transaction is digitally signed using the user's private key, ensuring authentication and traceability, which is vital for maintaining the integrity of the credentialing process.

2.7.2 Transaction Grouping

Transactions are then grouped into a block, allowing for efficient processing and validation. This batching of credential-related activities reduces the frequency of consensus operations, optimizing system resources.

2.7.3 Consensus Mechanism

The block is validated across the network through a consensus mechanism, such as (PoW) or (PoS). The choice of mechanism affects the system's performance, with

PoW offering high security but slower processing, while PoS provides faster, more scalable operations.

2.7.4 Block Validation and Addition

Upon achieving consensus, the block is added to the blockchain, creating an immutable record. This ensures that once credential transactions are recorded, they cannot be altered, preserving their authenticity.

2.7.5 Distributed Ledger Update

Finally, the distributed ledger is updated across all network nodes, ensuring transparency and that all participants have access to the same verified records. Having explored the operational steps of blockchain, it's important to consider how these processes are applied in current digital credential systems. The following section will analyze existing blockchain-based digital credential systems, evaluating their effectiveness and identifying areas where further improvement is needed.

2.8 Analysis of the Current Blockchain-Based Digital Credentials Systems

The proposed e-certificate system [45] offers a robust framework for issuing, verifying, and managing digital diplomas using blockchain technology, specifically Hyperledger Fabric. The framework effectively addresses key challenges in digital credentialing, such as ensuring the authenticity of diplomas and preventing fraudulent claims. By leveraging both RSA and ECC cryptographic methods, alongside facial recognition, the system ensures that diplomas are securely issued and verified, with all transactions immutably recorded on the blockchain.

From a privacy perspective, while the system effectively ensures that diploma data is protected, the use of facial recognition stored on the blockchain raises concerns. Although the blockchain is permissioned, any compromise of the facial recognition data could lead to significant privacy violations. Additionally, the approach of storing

facial recognition models on the blockchain, even in a hashed form, might not fully align with stringent privacy regulations like GDPR, which have specific requirements for biometric data handling.

Taufiq et al. [46] explore the implementation of crypto-governance using blockchain technology at Muhammadiyah Tangerang University (UMT) in Indonesia. The system aims to enhance the security and traceability of graduates' data, including diplomas, transcripts, and diploma supplements. The blockchain framework, implemented with Hyperledger Fabric, enables decentralized governance, ensuring that only authorized personnel can validate and approve academic records.

The study effectively demonstrates how blockchain can secure academic records and streamline the validation process within a university setting. The use of blockchain enhances data integrity, traceability, and security, ensuring that academic credentials are protected from tampering. However, the study primarily focuses on the technical aspects of blockchain implementation and lacks a thorough exploration of potential challenges, such as user adoption, scalability, and privacy concerns. Additionally, while the system's design is robust, its reliance on a private blockchain might limit transparency and trust among external stakeholders.

While the study showcases a promising application of blockchain in higher education, it could benefit from addressing broader concerns, including the scalability of the system as the number of participants grows and the potential privacy implications of storing academic records on a blockchain. Future work should also explore how the system can be integrated with national or international educational frameworks to enhance interoperability and trust.

Karamachoski [47] focuses on utilizing blockchain technology for certificate storage, emphasizing the decentralized, tamper-proof nature of blockchain as a secure solution

for managing academic credentials. The proposed system leverages the inherent properties of blockchain, such as immutability, redundancy, and non-repudiation, to ensure the integrity of stored records. The study details the use of elliptic-curve cryptography (ECC) and various consensus algorithms to secure transactions and maintain the reliability of the distributed ledger. The application, designed specifically for university diploma certification, is built using Ethereum's smart contracts and the InterPlanetary File System (IPFS) for decentralized storage.

The study presents a robust approach to digital certificate management by harnessing the blockchain's decentralized structure, which effectively addresses key issues like data tampering and unauthorized access. The implementation of ECC and smart contracts ensures that certificates are securely issued, stored, and verified, making the system highly reliable and resistant to fraud. Moreover, by integrating IPFS for decentralized storage, the system further enhances data accessibility and resilience against cyberattacks.

However, the reliance on blockchain and IPFS introduces certain challenges, particularly regarding scalability and the complexity of managing encryption keys. The system's dependence on consensus algorithms like (PoW) or (PoS) may lead to performance bottlenecks, especially as the number of transactions increases. Additionally, the management of encryption keys and user credentials could pose significant security risks if not handled properly, as any compromise could lead to unauthorized access to sensitive data.

While the proposed blockchain-based certificate storage system offers significant advantages in terms of security and transparency, its scalability and the potential challenges in key management need to be carefully addressed. Future work could explore more efficient consensus mechanisms and advanced key management

strategies to enhance the system's scalability and security, ensuring that it remains robust and practical for widespread adoption.

Badr et al. [41] present an end-to-end blockchain solution for the transmission and verification of academic records, leveraging Hyperledger Fabric and a web application interface. The system facilitates secure and efficient transcript requests, transfers, and validations between academic institutions, ensuring the integrity of academic credentials through hashing and permissioned access controls.

The proposed solution by Badr et al. [41] effectively addresses the need for a secure, scalable system for academic record management. By using a permissioned blockchain, the system ensures faster processing times and robust access control, making it well-suited for large-scale deployments in educational settings. However, the study identifies potential challenges related to data privacy, particularly in the context of long-term data retention on the blockchain. Additionally, while the system's scalability is supported by the permissioned blockchain architecture, the reliance on Hyperledger Fabric could limit flexibility in adapting to future technological advancements.

The study offers a strong foundation for blockchain-based academic record management, but it should consider the implications of data retention policies and the need for flexible integration with other educational systems. Addressing these concerns could further enhance the system's applicability and adoption across diverse educational contexts.

Smith et al. [48] introduce the Educational Certificate Blockchain (ECBC), a system designed to revolutionize educational data management by integrating schools, regulators, students, and employers into a peer-to-peer network. The ECBC employs a hybrid MPT-Chain structure, combining Patricia and Merkle trees to enhance query

efficiency and data integrity. While the system achieves high transaction throughput and low latency, the resource demands and intricacies of the MPT chain could impact performance, especially in resource-constrained environments.

ECBC offers significant advantages in data privacy, query efficiency, and blockchain scalability. However, the increased demands of the MPT-Chain, particularly regarding storage, could pose challenges for widespread adoption, especially in technologically less advanced settings. Exploring alternative, more resource-efficient indexing methods could help balance performance with system demands, potentially making the system more accessible.

While the innovative use of the MPT-Chain enhances blockchain performance, the complexity of the system may limit its broader implementation. Future research should investigate simpler solutions that maintain efficiency while reducing resource consumption, thereby making the platform more accessible across diverse educational environments.

Novak et al. [49] present EduCTX, a blockchain platform for managing higher education credits, modeled after the European Credit Transfer and Accumulation System (ECTS). EduCTX prioritizes student anonymity and employs a 2-2 multi-signature protocol for security. However, this approach introduces operational challenges, such as the risk of private key loss and the limitations of non-transferable ECTX tokens, which could affect the platform's usability.

EduCTX's focus on privacy and security is commendable, but its reliance on multi-signature protocols and restricted token transfers could complicate practical implementation. The platform's consortium blockchain model offers governance advantages, yet the initial limited node participation raises security concerns.

Moreover, the manual processes for key recovery may hinder user experience and scalability.

While EduCTX introduces important privacy-preserving measures, the platform's design choices, particularly regarding token transfer restrictions and key management, could limit its flexibility and adoption. Further exploration of more user-friendly and resilient solutions is necessary to ensure that EduCTX can effectively scale and operate in diverse educational contexts.

Baldi et al. [7] introduce Blockcerts, a blockchain-based decentralized notary system developed by MIT Media Lab and Learning Machine. Blockcerts integrates the Open Badges framework with blockchain to ensure tamper evidence, ownership, and versatile sharing of certificates. The system allows issuers to generate, sign, and verify certificates through a hash digest stored on the blockchain, with verification facilitated by the Blockcerts Universal Verifier platform.

While Blockcerts offers robust features like tamper resistance and decentralized certificate management, study by Santos [50] highlights a significant vulnerability: the lack of issuer identity verification. This flaw enables malicious actors to create fake certificates, undermining the trust and security that blockchain is meant to provide. Additionally, study by Han et al. [51] identify critical issues related to centralized control over certificate revocation, verification dependency on issuer infrastructure, and risks associated with centralized storage. These weaknesses contradict the decentralized ethos of blockchain, potentially compromising the system's reliability and security.

To enhance Blockcerts, implementing decentralized verification mechanisms and distributed storage, as proposed by the Hypercerts solution, could address these vulnerabilities. By leveraging smart contracts for automated revocation and using IPFS

for distributed storage, Hypercerts offers a more resilient and trustworthy system. This approach mitigates the risks posed by centralized control and storage, aligning more closely with the principles of blockchain technology.

Han et al. [51] propose using blockchain technology to create a decentralized system for securing and verifying educational records. They highlight the advantages of blockchain, such as the elimination of central authorities and the use of cryptographic techniques like SHA-256 and digital signatures to ensure the integrity and authenticity of educational data. However, despite these strengths, the study raises significant concerns. The reliance on smart contracts, while innovative, introduces potential security vulnerabilities, as flaws in contract code could lead to unauthorized access or manipulation of records. Additionally, the decentralized nature of the system, though beneficial for trustless transactions, presents challenges in governance and maintaining consistent security standards across all nodes. Privacy concerns are also notable, particularly regarding compliance with regulations like the GDPR. The immutable nature of blockchain records could conflict with legal requirements for data erasure, and the use of Resource URLs for accessing external documents might expose sensitive information if not adequately secured. Furthermore, the study does not fully address scalability issues, particularly the inefficiencies associated with traditional consensus mechanisms like (PoW). While the proposed system offers benefits such as enhanced collaboration among educational institutions and greater control for users over their records, these advantages may be undermined by the unresolved security, privacy, and scalability challenges. Addressing these issues through the integration of advanced cryptographic techniques and alternative consensus mechanisms would be essential for the successful implementation of a blockchain-based educational record system.

Gresch et al. [52] at the University of Zurich introduce a blockchain-based system for managing and verifying educational diplomas, leveraging the Ethereum blockchain and SHA-3 hash functions to ensure the authenticity and immutability of records. While the system's integration with existing legacy systems is innovative, it also introduces significant complexities and potential vulnerabilities. Specifically, the reliance on secure communication protocols and the need for effective data exchange mechanisms present risks that could undermine the security of sensitive student information. Additionally, while the use of smart contracts to automate verification processes is a strong feature, the study does not fully address the challenges of ensuring compliance with privacy regulations such as the GDPR, particularly regarding the right to be forgotten and data minimization. The risk of unauthorized access or manipulation of educational records remains a concern, especially given the lack of comprehensive strategies to manage these risks in decentralized environments. Therefore, while Xu et al. [48] offer a promising approach to diploma management, but it is crucial to develop more robust mechanisms to safeguard against security and privacy issues, particularly as the system scales to handle larger volumes of data and users.

Cheng et al. [53] explore the verification and storage of electronic certificates using blockchain technology. The system starts with user registration, where users upload certificates and personal IDs. These documents are verified against institutional records, and upon successful validation, the certificate serial numbers and ID card numbers are stored immutably on the blockchain.

A QR code is generated for the user, encapsulating the verified data, which is used during job applications. Employers can verify the authenticity of the credentials by referencing the QR code and serial number against the blockchain. The system employs blockchain hashing and asymmetric encryption to ensure data security and

integrity. While the blockchain provides transparency and immutability, concerns arise around data centralization, scalability, and privacy. The use of a single node for data storage contradicts the decentralized nature of blockchain, potentially creating a single point of failure. Additionally, the system's scalability must be considered, as increasing data volumes could impact performance.

The study's reliance on asymmetric encryption for key management is sound, but secure private key management is essential to prevent security breaches. Moreover, the system must ensure compliance with privacy regulations, particularly regarding the handling of personal data.

Arenas and Fernandez [54] present CredenceLedger, a permissioned blockchain platform designed for the decentralized verification of academic credentials. Developed on the Multichain framework, CredenceLedger integrates a mobile application, enabling students to manage and share digital versions of their credentials securely. The platform emphasizes privacy by encrypting sensitive data, with only essential information, referred to as "compact data proofs," accessible to third parties for verification purposes.

Key Features of CredenceLedger include a structured permission system that categorizes user actions into low, medium, and high-risk levels, each managed through transaction metadata. The use of blockchain "streams" allows for the secure handling of transactions without the need for cryptocurrency, supporting the system's scalability. Additionally, the platform employs a "mining diversity" scheme to prevent monopolization and ensure secure, decentralized validation.

Despite these strengths, critical considerations remain. While the permissioned blockchain enhances security and privacy, the risk of unauthorized access and potential privacy breaches necessitates robust authentication and encryption measures.

Furthermore, the permissioned nature of the blockchain introduces elements of centralization, potentially leading to control risks. Finally, although CredenceLedger is designed for scalability, its long-term performance in handling increasing data volumes warrants careful monitoring.

The studies by Huynh et al. [55] and Mthethwa et al. [56] explore blockchain-based solutions for enhancing the integrity and verification of digital certificates and hardcopy documents, respectively. Huynh et al. [55] present UniCert, which uses the UniCoin blockchain to store hashed certificates via a Merkle tree hash algorithm, ensuring tamper-resistance. Mthethwa et al. [56] focus on verifying hardcopy documents by integrating blockchain with OCR and barcodes, storing essential metadata on the blockchain for decentralized verification.

Both studies highlight blockchain's effectiveness in securing data and ensuring transparent verification. UniCert's approach in [offers strong tamper-resistance, but it raises privacy concerns due to the potential exposure of transaction metadata on the blockchain. Similarly, Mthethwa et al. [56] address document verification challenges by simplifying the use of barcodes linked to blockchain-stored metadata. However, it also faces privacy issues stemming from blockchain's inherent transparency.

While both studies effectively utilize blockchain's security features, they underscore the need for better privacy measures. Huynh et al. [55] could benefit from incorporating privacy-preserving techniques like zero-knowledge proofs to mitigate the exposure of sensitive data.

Gresch et al. [57] explore a blockchain-based system designed to meet the specific requirements of the University of Zurich (UZH) for issuing and verifying diplomas. The system is structured to ensure that only authorized departments can issue diplomas, maintaining confidentiality and scalability. The digital diplomas are hashed

and stored in a smart contract on the Ethereum blockchain, allowing companies to verify their authenticity autonomously without direct contact with the university.

The system proposed by Gresch et al. [57] effectively address key requirements such as authorized issuance, privacy, and ease of use, particularly in automating the verification process. However, the system's reliance on hashing for confidentiality raises concerns about the potential exposure of transaction metadata on the blockchain, which might reveal sensitive information. Additionally, while the system's design allows for scalability and batch processing, it could benefit from exploring more advanced privacy-preserving techniques to further protect student data.

While the study demonstrates a robust framework for diploma verification, it underestimates the challenges associated with blockchain transparency. Future iterations of the system should consider integrating more sophisticated cryptographic techniques, such as homomorphic encryption, to mitigate privacy risks while maintaining transparency and trust in the verification process.

Castro-Iragorri et al. [58] introduce the Blockchain-based Educational Records Repository (BcER2), a consortium blockchain system using the Hyperledger Composer framework. BcER2 allows authorized entities to create and manage educational records while ensuring that anyone can verify their authenticity. The system's business network model defines assets, transactions, and participants, enabling secure and decentralized management of educational records.

BcER2's use of a consortium blockchain effectively balances the need for restricted access to record creation with the openness required for verification. This semi-private approach ensures data integrity and authenticity while maintaining control over who can alter the records. However, the implementation of access control rules via Hyperledger's framework introduces potential complexities in managing permissions

across different participants. Additionally, while the system is designed for scalability and secure access, the reliance on a single framework may limit flexibility and adaptability to future technological advancements.

The study offers a promising approach to managing educational records, but it should address the potential limitations of using a single blockchain framework. To enhance the system's resilience and adaptability, future developments could consider incorporating multi-chain interoperability or alternative consensus mechanisms that allow for more flexible and scalable solutions.

Daraghmi et al. [59], introduced UniChain, a blockchain-based system designed to manage and secure academic records (EARs) within university databases. UniChain integrates blockchain technology with existing university systems, allowing universities to maintain and manage student records while granting students access rights. The system utilizes SHA-256 hashing, advanced encryption techniques, and smart contracts to ensure the integrity and security of academic records. Additionally, UniChain employs a Proof of Authority (PoA) consensus algorithm and a unique incentive mechanism for block creation and validation. UniChain's approach effectively enhances the security, integrity, and transparency of academic records by leveraging blockchain technology. The system's integration with existing university databases allows for a practical and seamless implementation without requiring a complete overhaul of current infrastructures. However, the reliance on a permissioned blockchain and centralized control by universities may limit the system's scalability and flexibility. The complexity of managing encryption and smart contracts, along with the requirement for universities to control access, could present challenges, particularly for institutions with limited technological resources.

While UniChain offers a strong framework for securing academic records, its reliance on a permissioned blockchain and centralized control could hinder broader adoption. Simplifying the system's architecture and exploring more decentralized models could improve scalability and accessibility, making the system more adaptable for a diverse range of educational institutions.

Leka and Selimi [60] present a solution for verifying and distributing digital certificates using Ethereum blockchain-based smart contracts. The system, called BCert, is designed to provide a secure and decentralized platform for managing academic credentials. The architecture employs Solidity for coding smart contracts, which are then deployed on the Ethereum blockchain. The system involves key roles, including issuers (universities or training centers), users (students, employers, or academic institutions), and accreditation bodies, ensuring that certificates added to the blockchain are immutable and verifiable.

BCert's use of the Ethereum blockchain for managing academic credentials presents a robust framework for ensuring the authenticity and integrity of digital certificates. The system's reliance on blockchain's decentralized nature enhances security, making it difficult for unauthorized entities to tamper with or forge certificates. Additionally, the use of AES encryption before hashing further protects sensitive data, ensuring confidentiality alongside blockchain's inherent transparency.

However, the system's reliance on encryption keys raises potential vulnerabilities. If a key is compromised, the associated certificate's security could be jeopardized, necessitating a complex process of re-encryption and re-issuance. Moreover, the need for private servers to store encryption keys and logs introduces a degree of centralization, which could undermine the blockchain's decentralized advantages. The architecture also imposes significant resource requirements, such as the costs

associated with Ethereum transactions, which may limit scalability and adoption, particularly in resource-constrained environments.

While BCert offers significant advancements in securing and verifying academic credentials, the challenges associated with key management and the costs of blockchain transactions need to be carefully addressed. Future enhancements could focus on developing more efficient key management protocols and exploring cost-effective blockchain alternatives to ensure that the system remains scalable and accessible to a broader range of institutions.

Litoussi et al. [61] present the current digital certification process at Moroccan universities, utilizing BarideSign for secure digital signatures with RSA-2048 encryption and SHA-256 hashing. The system requires students to manually request certificates, and each university creates separate academic accounts for students, leading to inefficiencies and fragmented records.

While the existing system offers a degree of security, it is limited by its centralized structure and manual processes, which can lead to delays and administrative burdens. The reliance on a single Certificate Authority (BarideSign) also introduces a potential single point of failure. Additionally, the fragmented nature of student records across different universities undermines the potential for a unified, streamlined certification process.

To address these challenges, the study proposes a Blockchain Smart Contract-based Model (BCSC-DApp), leveraging IPFS for distributed storage and Ethereum smart contracts for automated certification. This model offers significant improvements in security, efficiency, and transparency. By automating the issuance of certificates and using blockchain for immutability, the model reduces the risk of fraud and ensures that records are consistently available and verifiable across institutions.

The authors advocate for the adoption of the BCSC-DApp model, highlighting its potential to revolutionize the digital certification landscape by overcoming the limitations of the current system. They emphasize the benefits of decentralization, which would eliminate the reliance on a single authority and enhance the overall resilience and scalability of the certification process. However, the authors also acknowledge that implementing this model would require significant changes in infrastructure and administrative processes, which could be a barrier to widespread adoption.

Haveri et al. [62] explore the development of a blockchain-based system to securely store, share, and verify documents using (IPFS) and Ethereum private blockchain. The proposed methodology involves uploading documents to IPFS, generating a hash (Q-hash), and storing this hash in the blockchain. Transactions are managed through smart contracts that facilitate interactions between issuers, users, and requesters.

The proposed system effectively leverages blockchain's immutability and IPFS's decentralized storage to create a robust, secure platform for document management. The use of SHA-256 hashing ensures that any alteration to a document would produce a different hash, making unauthorized changes easily detectable. Additionally, by storing the document off-chain and the hash on-chain, the system overcomes the limitations of blockchain storage capacities. However, the reliance on Ethereum's (PoW) consensus mechanism may introduce latency and scalability issues, as PoW is computationally intensive and slow. The study acknowledges this by comparing PoW with Proof of Authority (PoA), highlighting PoA's efficiency in private networks where validators are trusted entities.

The system’s design effectively addresses key security concerns by ensuring that any unauthorized changes to documents result in hash mismatches, thereby maintaining

the integrity of the blockchain. The consensus mechanism further secures the network, although the study suggests that PoA may offer better performance in a private blockchain setting.

The authors advocate for a transition from PoW to PoA, particularly for private blockchains, where trust among participants can be established. They argue that PoA offers a more scalable solution with lower latency, making it a preferable choice for the proposed document management system. The study emphasizes the importance of using a decentralized approach to enhance security and reduce reliance on centralized systems, which are more vulnerable to attacks.

Nguyen, Dao, and Do [33] propose the VECefblock system, designed to enhance the trust and transparency of educational management systems in schools and universities through blockchain technology. The VECefblock system introduces a four-phase architecture (input-write-validate-seal), improving upon the traditional two-phase approach (input-write). The proposed system writes data to both a local database and a blockchain, validates the data, and seals it into a blockchain block, ensuring data integrity and immutability.

The VECefblock system effectively addresses the limitations of traditional educational data management by incorporating blockchain's immutable and transparent properties. The system’s architecture, which involves writing to both a local database and blockchain, adds an extra layer of security by ensuring that any modification to data is recorded and traceable. This dual-recording approach is particularly beneficial for educational institutions, where data integrity is paramount.

The use of a permissioned blockchain network, specifically Hyperledger Fabric, aligns with the needs of educational institutions in Vietnam, where data security and regulatory compliance are critical. The choice of a permissioned network, combined

with a consensus model like Practical Byzantine Fault Tolerance (PBFT), ensures that only authorized participants can access or modify the blockchain, thereby reducing the risk of unauthorized access or data tampering. Additionally, the system's design to use national IDs or hashed values for unique learner identification further enhances data security and reduces the risk of data duplication or inconsistency.

The authors advocate for the use of permissioned blockchain networks in educational settings, particularly in countries like Vietnam, where state agencies play a significant role in educational certification. They emphasize the importance of secure, traceable data management systems in educational institutions and propose VECefblock as a solution that not only meets these security requirements but also improves the transparency and trustworthiness of the educational certification process.

The authors also highlight the system's flexibility, noting that VECefblock can be deployed on various blockchain platforms, though they recommend Hyperledger Fabric for its security features and compatibility with Vietnamese regulations. They suggest that this system could significantly improve the reliability of educational certificates, making them more resistant to fraud and easier to verify.

Castro-Iragorri, Lopez-Gomez, and Giraldo [63] present a proposed system that integrates Blockchain and a Web-application to provide a secure, fast, and reliable network for verifying certificates using Optical Character Recognition (OCR) technology. The system allows users to upload certificates in various formats, such as JPEG, PNG, and PDF, either through a web application or via email. The uploaded documents are processed by an OCR module, which extracts text data and hashes it using a hashing algorithm. The hashed data is then queried on the Ethereum Blockchain to verify the authenticity of the certificate.

The proposed system effectively leverages blockchain's immutable and transparent nature to enhance the security of certificate verification processes. By integrating OCR technology, the system automates the extraction of data from certificates, which is then hashed and stored on the blockchain. This approach not only ensures that the certificate data is secure and tamper-proof but also simplifies the verification process for users.

The system's architecture, which includes a Blockchain Module, OCR Module, Webapp Module, and Email Module, is well-designed to handle various user interactions and automate the verification process. The use of Ethereum's Rinkeby test network for storing transactions ensures that the system can be tested and refined without incurring real costs. Additionally, the system's ability to handle bulk verifications, either through multiple file uploads or Excel sheets, demonstrates its scalability and practicality for large-scale use.

One of the system's strengths is its flexibility in user interaction. It offers multiple ways for users to verify certificates, either through a web interface or via email, making it accessible to a broad range of users. The inclusion of an email-based verification process, supported by Gmail API and Google Cloud's Pub/Sub service, is particularly noteworthy for its user-friendliness and accessibility.

However, the system's reliance on OCR for data extraction could be a potential limitation, as OCR accuracy can vary depending on the quality and format of the input documents. Additionally, while the use of a test network is beneficial for development, transitioning to a mainnet might introduce challenges related to transaction costs and network scalability.

The authors advocate for the use of blockchain technology in certificate verification, emphasizing the benefits of immutability, security, and transparency that blockchain provides. They highlight the importance of automating the verification process to

reduce the chances of human error and to increase the efficiency of the system. The authors also emphasize the system's ability to handle bulk data, making it suitable for use in educational institutions or organizations that manage large volumes of certificates.

The proposed system is seen as a high-end product that addresses the limitations of traditional verification methods, offering a more secure and reliable solution. The authors' approach is pragmatic, focusing on the integration of existing technologies (OCR, blockchain, and web applications) to create a system that is both innovative and practical

Mukta et al. [64] present a proposed solution for secure and privacy-preserving credential sharing using a Self-Sovereign Identity (SSI) framework and blockchain technology. The study outlines a scenario in which a student, Jane, needs to share her academic credentials with a foreign university while ensuring her privacy. The proposed system allows users to share only the necessary information, such as grades, while keeping other personal data, like birth dates, private. This selective disclosure is managed through a redactable signature technique, enabling the recipient to share specific attributes of a credential without needing re-signing or involving a third party. The study effectively addresses the challenges associated with secure credential sharing, particularly the balance between transparency and privacy. The proposed system uses SSI principles supported by blockchain technology to establish verifiable identities and facilitate secure, selective disclosure of credentials. The use of Decentralized Identifiers (DIDs) ensures that users maintain control over their personal data while interacting with verifiers, which is crucial for protecting privacy in a digital age.

One of the strengths of the proposed system is the adoption of redactable signature techniques. This approach allows for flexible and efficient selective disclosure, where multiple claims can be generated from a single credential without the need for re-signing by the issuer. This reduces the number of interactions between the issuer and recipient, enhancing privacy by preventing issuers from tracking the recipient's credential-sharing activities. The system's ability to handle selective disclosure at the attribute level, rather than bit-level granularity, addresses potential inaccuracies and inefficiencies, making it a more practical solution.

The architecture, termed "CredChain," integrates SSI with a decentralized application layer, offering a comprehensive framework for credential management. The service-based design of the platform allows for the incorporation of various selective disclosure schemes, adding to its flexibility and adaptability. The workflow for credential issuance, redaction, and verification is well-structured, ensuring that the system can operate efficiently in real-world scenarios.

The authors advocate for a privacy-focused approach to credential sharing, emphasizing the importance of giving users control over their data through selective disclosure. They highlight the limitations of existing credential-sharing systems, such as the risk of oversharing and lack of user privacy, and propose their system as a solution that addresses these issues by leveraging blockchain and SSI technologies. The authors also stress the system's scalability and flexibility, making it applicable to various types of credential-sharing scenarios beyond academic settings.

The authors demonstrate a strong understanding of the technical challenges and propose a well-thought-out solution that integrates modern cryptographic techniques with emerging technologies like blockchain and SSI. They anticipate potential issues, such as the need for attribute-level granularity in redaction and the importance of

minimizing issuer-recipient interactions to preserve privacy, and address these within their proposed framework.

Brunner et al. [65] introduce SPROOF, a decentralized, permissionless, and transparent platform designed for issuing, storing, and verifying digital documents using blockchain technology. The study outlines the building blocks of SPROOF, which include public storage via blockchain, key management in Hierarchical Deterministic (HD) wallets, and the processes for managing issuers, receivers, and verifiers within the system. The platform aims to ensure the integrity, privacy, and trustworthiness of digital documents by leveraging cryptographic techniques and decentralized storage.

The study presents a robust framework for a decentralized document management system that addresses several key challenges in digital verification, including scalability, storage costs, privacy, and traceability. By utilizing a public blockchain (such as Bitcoin or Ethereum) and a Distributed Hash Table (DHT), SPROOF ensures that documents are stored in a decentralized manner, which enhances security and transparency. The use of a blockchain allows SPROOF to maintain an immutable and verifiable global state of ordered data, while the DHT provides a scalable solution for storing the actual document data, with only the hash references stored on the blockchain.

One of the strengths of SPROOF is its innovative use of HD wallets for key management. This approach allows the generation of multiple pseudonyms from a single seed, enabling receivers to maintain privacy by using different pseudonyms for different documents. The ability to derive sub-keys from a master key also introduces the concept of "forced completeness" where documents that are related (e.g., a series of educational certificates) are verifiably linked, ensuring that no documents are

hidden. This feature is particularly valuable in educational settings, where a complete and accurate record of a student's achievements is essential.

The study also addresses potential vulnerabilities in the system, such as the risk of malicious issuers creating fake profiles or receivers sharing pseudonyms to fraudulently collect documents. The proposed solutions, including the use of identity claims and evidence events, as well as the Web of Trust (WoT) for issuer verification, provide a decentralized method for establishing trust and preventing fraud. The system's reliance on cryptographic hash functions and hierarchical deterministic key generation further enhances security and privacy.

The authors emphasize the importance of decentralization and transparency in digital document management. They argue that traditional, centralized systems are prone to issues such as data manipulation, lack of privacy, and the need for trusted intermediaries. SPROOF is presented as a solution that overcomes these limitations by leveraging blockchain technology and decentralized storage to create a trustless environment where documents can be securely issued, stored, and verified without relying on a single authority.

The authors also highlight the flexibility and scalability of SPROOF, noting that it can be used for a wide range of applications beyond educational certificates, including professional certifications, legal documents, and other forms of digital credentials. The ability to add identity claims and evidence events to strengthen the trustworthiness of issuers, along with the use of HD wallets for privacy-preserving pseudonym management, positions SPROOF as a versatile and secure platform for digital document management.

Abreu et al. [66] present a reference architecture and a proposed solution for utilizing blockchain technology to securely manage and validate higher education certificates.

The study outlines the architectural components necessary for creating a blockchain-based system that enhances security, privacy, and scalability in managing educational data. The proposed architecture aims to provide a credible environment for publishing and validating certificate information, reducing the risks of data loss and certificate falsification. The study effectively introduces a comprehensive blockchain-based reference architecture designed to address the specific needs of educational institutions in managing student certificates. By viewing blockchain as a software component, the study emphasizes the unique properties and limitations of blockchain technology, including its complexity, scalability challenges, and the need for network-based software components.

The architecture is divided into three main layers: the Application layer (Educ-Dapp), the API layer, and the Blockchain layer. Each layer plays a crucial role in ensuring the security, availability, and integrity of the educational data stored on the blockchain. The Educ-Dapp serves as the interface between external entities (such as students, educational institutions, and companies) and the blockchain, while the API layer facilitates communication between the front-end and the blockchain. The Blockchain layer stores the educational data and smart contracts, ensuring that the data remains secure and tamper-proof.

One of the key strengths of the proposed architecture is its ability to leverage blockchain's unalterable nature and data verifiability to prevent certificate forgery. The inclusion of a consensus algorithm and network layers further strengthens the architecture by ensuring that all nodes in the network participate in the consensus process, thereby maintaining the integrity of the blockchain.

The study also provides a proof of concept using the Ethereum platform, demonstrating the practical implementation of the proposed architecture. The use of

smart contracts, the Ethereum Virtual Machine (EVM), and various Ethereum-related technologies (such as Solidity, Web3 API, and Metamask) highlights the feasibility of the architecture in real-world applications. The validation scenario, involving experienced higher education professionals, adds credibility to the proposed solution by showing its effectiveness in a simulated environment.

The proposed blockchain-based reference architecture for securely managing and validating educational certificates presents a promising solution to enhancing security and trust in higher education systems. However, several critical issues warrant consideration. The reliance on public blockchain networks like Ethereum raises concerns about scalability, as performance bottlenecks and rising costs could pose significant challenges as the system expands to accommodate more certificates and users. Additionally, while the architecture aims to enhance data security, the use of public blockchains introduces potential privacy risks, particularly if the hash functions are compromised or if legal challenges arise regarding data transparency and protection. The implementation complexity, due to the dependence on advanced blockchain technologies such as Solidity and Web3 API, could also limit adoption to institutions with sufficient technical expertise, leaving less technologically advanced institutions at a disadvantage. Furthermore, the reliance on public blockchain infrastructure introduces dependencies on external factors beyond institutional control, such as changes in transaction fees or network protocols, potentially affecting the system's long-term viability. Lastly, the study does not fully address how the proposed solution aligns with existing legal and regulatory frameworks, particularly data protection laws like the GDPR, which could present significant barriers to implementation in regions with stringent privacy regulations. Therefore, while the architecture is innovative, its success will depend on addressing these scalability,

privacy, complexity, and legal compliance challenges to ensure its viability and adaptability across diverse educational institutions.

Chaniago et al. [67] present a decentralized application (DApp) system integrated with the Ethereum blockchain to securely store, manage, and verify electronic diplomas and transcripts. The proposed system leverages smart contracts to create a tamper-proof record of these documents, ensuring their authenticity through cryptographic hashing and blockchain technology.

One of the key strengths of this system is its use of the SHA-256 algorithm to generate unique fingerprints (hashes) for each document, which are then recorded on the Ethereum blockchain. This ensures that any alteration to the document would result in a different hash, making it easy to detect tampering. Additionally, the system's decentralized nature provides strong security against hacking attempts, as the blockchain's inherent structure prevents the deletion or alteration of stored transactions.

However, while the system effectively secures the integrity of diplomas and transcripts, there are several critical considerations. First, the reliance on the Ethereum blockchain, while offering high security, also introduces potential scalability issues. As the blockchain grows, the costs associated with storing and verifying documents may increase, particularly due to the need for gas fees in the Ethereum network. This could limit the system's accessibility for institutions with limited financial resources.

Moreover, the system's design assumes that all stakeholders, including universities and employers, are familiar with blockchain technology and willing to engage with it. In practice, this might not be the case, as the technical complexity and need for specialized knowledge could act as barriers to adoption. The user interface, while

described as accessible, still requires interaction with blockchain transactions, which might be intimidating for non-technical users.

From a privacy perspective, the system focuses on document authenticity but does not deeply address the privacy of the individuals involved. Although the system does not store personal data directly on the blockchain, the process of managing and verifying documents still involves handling sensitive information. Ensuring that this information is adequately protected throughout the process is crucial, particularly in light of stringent data protection regulations like the GDPR.

Rani et al. [68] propose the EduCert-Chain, a blockchain-based framework designed to enhance the management and verification of educational certificates. This framework is structured to address prevalent issues in traditional Educational Certificate Management Systems (ECMS), particularly credential fraud, by leveraging the decentralized and immutable nature of blockchain technology. The framework integrates various components such as full nodes (Higher Education Institutions or HEIs), light nodes (students and employer organizations), smart contracts, and a peer-to-peer network, all governed by the Raft consensus mechanism.

One of the strengths of the EduCert-Chain is its comprehensive approach to certificate management, covering the entire lifecycle from issuance to verification. The framework ensures that only authorized entities, such as HEIs and employer organizations, can join the network, which is crucial for maintaining the integrity and trustworthiness of the system. By using (ECC) for key generation and the SHA-256 algorithm for hashing, the system offers a robust security model that protects against unauthorized access and tampering. However, the framework also presents some challenges and limitations that need to be critically examined. While the use of blockchain technology provides enhanced security and transparency, it also introduces

complexity and potential scalability issues. The reliance on a decentralized network with multiple nodes means that the system's performance could be impacted by the computational power and storage capacity of these nodes. The study acknowledges this by discussing throughput and latency as performance indicators, but further exploration is needed to assess the system's scalability, especially in large-scale implementations involving numerous HEIs and students.

Additionally, the adoption of such a blockchain-based system requires a significant shift in the technological infrastructure of educational institutions and employer organizations. The need for technical expertise to manage and interact with the blockchain network could pose a barrier to adoption, particularly for smaller institutions with limited resources. The study mentions the challenges associated with the technical workforce and the cost of adaptation, but it does not delve deeply into potential solutions or strategies to mitigate these issues.

From a user perspective, the system's reliance on a blockchain-based API and smart contracts for operations like certificate issuance and verification may require a steep learning curve for non-technical users. Ensuring that the system is user-friendly and accessible to all stakeholders, including students and employers with varying levels of technical proficiency, is essential for its widespread adoption. Having conducted a comprehensive analysis of various blockchain-based digital credential systems, it is evident that while these solutions offer significant improvements in security, transparency, and efficiency, they also present distinct challenges, particularly in the realms of scalability, usability, and privacy. As we move forward, the focus will narrow to critically examining solutions that are specifically designed to enhance the security and privacy of digital certificates on the blockchain.

In the next section, we will delve deeper into these specialized systems, exploring how they address critical issues such as data protection, encryption, access control, and compliance with privacy regulations like the GDPR. The analysis will also cover the innovative techniques employed to ensure that sensitive information is safeguarded while maintaining the integrity and trustworthiness of the digital certificates.

2.9 Security and Privacy-Focused Solutions for Digital Certificates on Blockchain

Kaneriya and Patel [27] present a comprehensive model for managing educational credentials through blockchain technology, with a focus on privacy, security, and automation. The framework utilizes smart contracts to automate key processes such as credential issuance, consent management, and verification, while storing encrypted data off-chain in IPFS. The model offers several advantages, such as enhanced privacy through selective disclosure and the use of cryptographic services to secure data exchanges. However, the study also highlights challenges related to scalability, as the reliance on Ethereum for smart contract execution can result in high gas costs and potential delays in transaction processing. Moreover, while the use of off-chain storage like IPFS is innovative, it introduces potential security vulnerabilities, particularly in the management of encryption keys and data retrieval processes.

From an implementation perspective, the model demonstrates feasibility in a controlled environment, yet real-world application could be hindered by the complexities involved in ensuring secure and efficient inter-contract communication. Additionally, the focus on decentralization and end-to-end encryption is commendable, but it may also limit the system's accessibility for smaller institutions that lack the technical infrastructure to manage such a sophisticated setup.

Tang [8] presents a blockchain-facilitated solution for managing diplomas with a focus on security and privacy. The solution introduces a diploma format that organizes

attributes in a binary tree structure, allowing for selective disclosure and enhanced privacy protection. Each attribute is hashed with a salt value, and the entire structure is signed by both the diploma issuer and the user to prevent fraud and ensure integrity. This approach addresses key challenges in diploma management, such as issuer fraud, diploma forgery, and the need for high availability and cyber-threat resilience.

The proposed system integrates blockchain technology to provide time-stamping services, facilitate interoperability between different diploma management systems, and simplify interactions between diploma issuers and verifiers. By using smart contracts, the solution enables secure storage, retrieval, and verification of diplomas, minimizing the amount of data stored on the blockchain and ensuring that the system remains scalable and efficient.

However, the reliance on blockchain introduces complexities, particularly in the management of public key certificates and the need for regular auditing to maintain trust. The system's design assumes that the blockchain platform remains neutral and that its operations are not influenced by the diploma issuer or users, which may be challenging to guarantee in practice. The study also highlights the potential risks associated with different types of blockchain platforms, suggesting that a consortium blockchain might be preferable due to its privacy-friendly nature and controlled access.

The solution's emphasis on privacy is notable, with mechanisms in place to protect user, issuer, and verifier information. The use of salt values and the organization of diploma attributes in a tree structure help to obscure sensitive data from unauthorized access. However, the system's effectiveness depends on the security of the cryptographic primitives used, such as the hash function and digital signature schemes, and the proper management of keys and certificates.

In terms of performance, the study provides a preliminary evaluation of the computational efficiency of the proposed solution, focusing on the cryptographic algorithms and smart contract execution. While the system shows promise in terms of security and privacy, the implementation of the full-fledged solution is expected to be complex and time-consuming. Additionally, the cost and efficiency of operating on a blockchain platform, particularly a permissionless one, remain concerns that need to be carefully managed.

Mishra et al. [69] introduce a two-phase architecture designed to securely and privately manage the sharing of students' credentials using blockchain technology. The first phase emphasizes security, trust, and scalability by recording interactions as immutable transactions on the blockchain while utilizing off-chain storage to handle large data. This approach ensures that credentials are securely stored and efficiently managed, with smart contracts automating critical processes. The second phase enhances privacy by encrypting credentials and controlling access through public-private key pairs, ensuring that personal information is accessible only to authorized entities.

The architecture’s strengths lie in its clear definition of stakeholder roles—such as government bodies, schools, students, companies, and professors each with distinct responsibilities that contribute to the system's overall efficiency. The use of blockchain provides a robust security framework, ensuring that all interactions are tamper-proof, while off-chain storage helps address scalability issues by keeping large data off the blockchain. However, the architecture’s complexity, especially in the privacy integration phase, may pose challenges for non-technical users, potentially limiting its widespread adoption. Additionally, while off-chain storage improves scalability, it introduces vulnerabilities that could be exploited if not adequately secured. The

temporary upload feature, designed to allow students to grant access to their credentials, also carries the risk of being misused for fraudulent purposes, despite the implementation of hash comparisons as a safeguard. Moreover, the reliance on a centralized government body for identity management and fund administration introduces a level of centralization that somewhat contradicts the decentralized ethos of blockchain technology.

Molina et al. [28] propose a GDPR-compliant, blockchain-based system for managing and verifying digital certificates. The system design carefully maps the roles of various actors (Data Controller, Data Processor, Data Owner, and Receiver) to institutions and individuals, ensuring that personal data, such as university certificates, are handled securely. The certificates themselves are stored off-chain, with only their hash values recorded on the blockchain to facilitate verification. This approach is aligned with privacy regulations, as it limits access to the verification process and requires user consent, particularly in compliance with the ruling from the Uruguayan Data Protection Agency.

The study's strengths lie in its rigorous approach to privacy and security. By storing sensitive data off-chain and using blockchain only for verification, the system minimizes the exposure of personal data. The threat modeling process, conducted using the Microsoft Threat Modeling Tool, identifies a comprehensive set of risks, particularly related to unauthorized access, data integrity, and system availability. The system's adherence to GDPR is another significant advantage, as it ensures compliance with strict data protection regulations.

However, the study also reveals several challenges. The reliance on off-chain storage and the need for a centralized authority to manage access control and consent introduce potential vulnerabilities. The system’s design places significant trust in the School

Registry Offices and the central gateway, which could become single points of failure or targets for attacks. Additionally, the study identifies a number of threats that remain unmitigated, including Denial of Service (DoS) attacks, which could disrupt the availability of the certificate verification system.

From a critical perspective, while the system is well-designed to meet the GDPR requirements, its complexity and reliance on centralized components may undermine the decentralized advantages typically associated with blockchain technology. The need for ongoing threat monitoring and mitigation is also a concern, particularly given the rapid evolution of cybersecurity threats. Furthermore, the system's approach to privacy, while robust, could be challenged by new interpretations of data protection laws or by advances in data re-identification techniques. To enhance the system's resilience, future work should explore decentralized solutions for access control and consent management, as well as more advanced mechanisms for protecting against DoS attacks and other emerging threats.

Delgado-von-Eitzen et al. [26] propose a model that effectively addresses key challenges in using blockchain for educational purposes, focusing on GDPR compliance and the shortcomings of previous initiatives.. It introduces a scalable system for issuing, storing, and verifying various types of academic information, using a multi-blockchain approach to balance scalability and privacy. The model ensures that academic institutions can maintain control over their data while providing solutions for orphan records if an institution closes. The integration of GDPR principles, including data portability, consent, and the right to erasure, is a strong point, ensuring that data subjects retain control over their personal information.

The proposed model offers a well-structured approach to leveraging blockchain technology in education, ensuring GDPR compliance while addressing previous

limitations. It provides a scalable and secure solution for issuing, storing, and verifying academic information, appearing robust and comprehensive. However, its feasibility in real-world applications requires careful consideration. The multi-blockchain approach, though innovative, adds complexity in coordinating across institutions, potentially leading to synchronization challenges. While the model's focus on GDPR compliance is commendable, reliance on off-chain storage poses risks, particularly if institutions fail to maintain secure databases, threatening the long-term viability of stored data. Additionally, the model's security, though bolstered by blockchain's immutability and encryption, hinges on effective key management and secure node operation, with any lapses potentially compromising the system's overall integrity.

Dewangan et al. [70] present an innovative approach to managing student identities and certificates using blockchain technology, with a strong emphasis on privacy preservation, security, and efficient data management. The system leverages the Ed25519 digital signature algorithm and IPFS for off-chain storage to ensure the security and privacy of student data, while also enabling secure transactions of certificates and other academic records. One of the system's key strengths lies in its ability to decentralize data management through blockchain and IPFS, reducing reliance on centralized databases and enhancing data integrity and tamper resistance. Additionally, the method for generating unique student identities based on random numbers and timestamps is particularly noteworthy, as it enhances security and reduces the likelihood of identity theft.

However, the system also faces several challenges that may limit its practical applicability. The complexity of implementing and managing a system that relies on multiple advanced technologies could be daunting, especially for institutions with limited technical resources. Scalability is another concern, as the increasing number of

transactions and participating nodes could strain the blockchain network and introduce latency issues in IPFS data retrieval. Furthermore, despite the system's focus on privacy, the public availability of certain data on the blockchain could still pose risks, potentially allowing adversaries to piece together private information. The system's dependence on the secure operation of IPFS and the robustness of the blockchain network also introduces potential points of failure that could compromise its overall effectiveness.

From a critical perspective, while the proposed system represents a significant advancement in the use of blockchain technology for educational purposes, its complexity and technical demands may hinder widespread adoption, particularly among smaller institutions or in regions with less technological infrastructure. Future research should aim to simplify the system's architecture, enhance its scalability, and address any remaining privacy concerns to ensure that it can be effectively implemented and utilized across a diverse range of educational settings.

Rani and Priya [71] propose a decentralized system for digital certificate management using blockchain, IPFS, and the Proof of Continuous Work (PoCW) consensus algorithm. This approach effectively addresses key issues like authenticity, fraud prevention, and reliable certificate storage by leveraging decentralized storage and immutable blockchain records. The inclusion of a decentralized chameleon hash function adds traceability while maintaining data integrity, which is particularly useful for academic records.

However, the system's complexity and potential scalability challenges raise concerns. While PoCW aims to optimize resource use, the growing size of the blockchain and the increasing number of transactions could lead to performance bottlenecks. The system’s intricate design, combining blockchain, IPFS, and custom algorithms, may

also pose adoption challenges, especially for educational institutions with limited technical expertise.

Security and privacy, although emphasized, present potential vulnerabilities, particularly in the implementation of the chameleon hash function and the management of encrypted data on IPFS. Furthermore, the study lacks a thorough examination of regulatory compliance, particularly regarding data protection laws like the GDPR, which could be crucial for the system's acceptance in educational settings. While the studies discussed in this section have made considerable advancements in enhancing security and privacy in blockchain-based digital credential systems, a closer examination reveals that there are still significant challenges related to privacy and GDPR compliance that need to be addressed.

One of the central issues is the management of personal data in a way that aligns with GDPR principles. GDPR mandates strict controls over how personal data is collected, processed, and stored, with specific rights granted to individuals regarding their data [72]. In the context of blockchain-based credential systems, ensuring that these rights are upheld is complex, particularly due to the immutable nature of blockchain records. Kaneriya and Patel [27] offer enhanced privacy through selective disclosure and encrypted data storage in their study on a secure and privacy-preserving student credential verification system using blockchain technology. However, the framework does not fully explore how it would handle GDPR-specific requirements such as the right to erasure ("right to be forgotten"), given that data recorded on a blockchain is typically immutable. This highlights a critical gap that must be addressed to ensure that such systems can be legally and ethically deployed within GDPR-regulated regions.

Similarly, the framework presented by Tang [8], while innovative in its approach to privacy through cryptographic techniques like hashing and digital signatures, does not provide a comprehensive strategy for GDPR compliance. Issues such as how to handle data portability, user consent management, and the secure processing of personal data need more detailed consideration. Without these elements, the framework may struggle to meet the stringent privacy requirements imposed by GDPR.

Moreover, Mishra et al. [69] introduce a two-phase architecture that includes encryption and access controls, which are essential for privacy protection. However, the off-chain storage used in this framework presents potential risks if the off-chain data is not adequately protected. GDPR compliance would require rigorous measures to ensure that any personal data stored off-chain is secure, that user consent is obtained for all data processing activities, and that individuals can exercise their rights over their data.

Finally, Molina et al. [28] explicitly focus on developing a GDPR-compliant system, which is a strong step towards aligning blockchain-based credential systems with legal requirements. Nonetheless, even in this study, challenges remain regarding the practical implementation of GDPR principles, particularly in decentralized environments where data governance can be complex.

2.10 Discussion of Existing Security and Privacy-Focused Solutions and Identified Gaps

The current landscape of blockchain-based digital credential solutions demonstrates significant advancements in security and privacy; however, critical gaps remain that need to be addressed to achieve robust, scalable, and privacy-preserving systems. Below, we analyze these gaps by examining existing solutions and their limitations.

2.10.1 Inadequate Advanced Cryptographic Techniques

In many blockchain-based credentialing solutions, security measures are primarily based on basic cryptographic techniques like hashing and digital signatures. For instance, Kaneriya and Patel [27] present a blockchain model that employs selective disclosure and cryptographic services for secure data exchanges. However, the framework does not integrate homomorphic encryption or advanced encryption algorithms that allow secure operations on encrypted data. This limitation makes such solutions vulnerable to unauthorized access, as they do not fully secure sensitive data throughout its lifecycle.

This highlights a significant gap in the use of advanced encryption techniques, such as homomorphic encryption, which are essential for ensuring data security and privacy in scenarios requiring cross-institutional data sharing. The lack of these techniques leaves blockchain-based credentialing systems susceptible to data exposure and unauthorized access.

2.10.2 GDPR Compliance and Right to Erasure

Several solutions do not fully address GDPR requirements, particularly the right to erasure and data portability. Kaneriya and Patel [27] emphasize privacy but do not provide mechanisms for data deletion, which is critical under GDPR's "right to be forgotten." Similarly, Tang [8] introduces privacy protection through hashing and digital signatures but lacks strategies for user consent management and detailed data protection mechanisms that comply with GDPR.

This reveals a significant challenge in reconciling the immutable nature of blockchain records with GDPR's requirements for data modification and deletion. The inability to erase or modify personal data in many blockchain-based solutions limits their applicability in jurisdictions with strict data privacy laws.

2.10.3 Limited Privacy-Preserving Verification Mechanisms

Current solutions often lack robust privacy-preserving methods for credential verification. Tang [8] uses selective disclosure and hashing to protect user data, but does not address dynamic consent management or user-controlled data access for granular privacy control. Tang [28] emphasiz privacy compliance by storing only hash values on the blockchain, which limits exposure but still relies on centralized control. This highlights a critical limitation in existing solutions, as they fail to provide fine-grained controls that allow users to manage access to their credentials. This inadequacy increases the risk of unauthorized data exposure. Moreover, the reliance on public keys for verification can inadvertently reveal sensitive information to unauthorized parties.

2.10.4 Insufficient Key Management and Access Control

The reviewed studies reveal gaps in key management and access control, essential components for secure credentialing. Mishra et al. [69] introduce public-private key pairs for access control but lack robust mechanisms to handle potential vulnerabilities in key management. In solutions where the security relies heavily on private keys, lost or compromised keys can lead to unauthorized access or denial of service.

These limitations in key management significantly increase the risk of unauthorized access and reduce users' ability to securely control their credentials. Furthermore, the absence of multi-layered access control mechanisms leaves these systems vulnerable to insider threats, undermining their overall security.

2.10.5 Scalability Issues in High-Volume Environments

Solutions relying on consensus mechanisms like Proof of Work (PoW) struggle to scale effectively, especially when handling high transaction volumes. For instance, Kaneriya and Patel [27] employ Ethereum’s PoW-based smart contracts, leading to

high gas costs and potential delays. Similarly, Tang [8] encounters performance bottlenecks due to transaction processing delays associated with PoW.

The high computational demands of PoW introduce inefficiencies and significant scalability challenges. These limitations are particularly problematic in educational settings, where real-time data management and inter-institutional coordination are critical for effective credentialing solutions.

2.10.6 Centralized Components Compromising Decentralization

Although blockchain is inherently decentralized, some solutions still depend on centralized elements for identity and access control. For example, Mishra et al. [69] and Molina et al.[28] rely on centralized authorities for identity management, which introduces potential single points of failure. This reliance contradicts the decentralized ethos of blockchain, limiting the system's resilience and transparency.

The dependence on centralized entities for core functionalities significantly undermines the security and privacy benefits that blockchain is designed to offer. This reliance not only makes the system vulnerable to manipulation or failure but also diminishes the trust and transparency associated with decentralized systems.

Table 2. 1 Comparative Analysis of Security and Privacy-Focused Solutions for Digital Certificates on Blockchain

Reference	Goal	Techniques Used	Blockchain Platform	Proposed Solution	Experimental Results	Evaluation
Security-Aware and Privacy-Preserving Blockchain Chameleon Hash Functions for Education System [71]	To overcome privacy violation issues in the Education credential system	Chameleon Hash Function, Proof of Continuous Work (PoCW), Smart contracts, IPFS for information storage	N.A	System Architecture	Maximum of 1500 queries per second to retrieve data from IPFS. Approximately 17% faster speed compared to traditional blockchain systems.	Theoretical analysis based on the used techniques.
A Privacy and Security-Aware Blockchain-Based Design for a Digital Certificate System [28]	To address privacy aspects of digital certificate systems		N.A	System Architecture incorporating privacy protection mechanisms	N.A	Methodology for security and privacy threat modeling based on Microsoft's STRIDE methodology
Privacy Protected Blockchain-Based Architecture and Implementation for Sharing of Students' Credentials [69]	To ensure the authenticity and privacy of students' credentials	Hash-based approach, IPFS, Smart contracts	Ethereum	Architecture with privacy protection	Execution time for credential upload requests by the school (average 16.00337 s), Execution time to send access requests and grant access right (without privacy 31.09165 s, with privacy 34.74195 s), Scalability test: requests sent asynchronously (20 transactions/second)	Security analysis.

Towards Using Blockchain Technology to Prevent Diploma Fraud [8]	To preserve the security and privacy of diplomas	Hash-based approach, Smart contracts	Ethereum	System Architecture with a focus on computational costs	Security and privacy analysis based on the techniques used.	Theoretical analysis
Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information [26]	To preserve the privacy of academic information	Hash-based approach, Smart contracts	Hyperledger Fabric	Framework compliant with GDPR	N.A	Security and privacy analysis based on the techniques used.
A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology [27]	To propose a Secure and Privacy-Preserving Student Credential Verification System	Smart contracts, RSA algorithm (2048-bit key), IPFS	Ethereum	System Architecture	Execution time for uploading a credential (16.00337 s), Execution time for access request processing (34.74195 s), Scalability (average time for asynchronous requests up to 1000)	Security analysis of smart contracts using open-source tool, MyThril.
Enhanced Privacy-Preserving in Student Certificate Management in Blockchain and Interplanetary File System [70]	Enhanced privacy-preserving in student certificate management	IPFS, EdDSA (Elliptic-curve Digital Signature Algorithm), SHA-256	PHP blockchain	System Architecture	Number of bits for data upload on IPFS (512 bits), Signature time (300 ms), Verification time (600 ms), Transaction speed (17 transactions per second), Single transaction time (60 ms)	Security analysis and privacy auditing based on the techniques used.

2.11 Current Frameworks for Digital Certificates Management on the Blockchain

Building on the security and privacy considerations discussed in the previous section, this section delves into the current frameworks that are being employed for digital certificates management on the blockchain. These frameworks represent the practical implementation of blockchain-based systems, incorporating various technological innovations to enhance the issuance, storage, and verification of digital credentials. In this section, we will examine the existing frameworks, assess their effectiveness, and explore their role in the broader context of blockchain-based digital certificates management

2.11.1 Educational Credit Transfer Framework

Srivastava et al. [73] introduce a consortium blockchain framework that balances public verification and privacy through a distributed consensus protocol based on (PoW). While this approach ensures data integrity and security, it also introduces inefficiencies due to high computational demands and potential delays in transaction processing. This highlights the need for more scalable and resource-efficient consensus mechanisms, such as Proof of Stake (PoS).

The framework effectively uses hash functions and Merkle trees for data integrity but lacks advanced encryption techniques and comprehensive access control, leaving room for improvement in protecting sensitive academic data. Integrating more robust security measures, like homomorphic encryption or advanced access control, could significantly enhance privacy and security.

Scalability is a concern, as PoW's resource intensity may cause performance bottlenecks, particularly in cross-institutional coordination. Addressing these issues

with more efficient consensus mechanisms and improved synchronization across institutions could enhance the framework's effectiveness.

While the use of multi-signature protocols for transactions adds security, the framework's adaptability may be limited by its reliance on specific cryptographic methods. Greater flexibility and customization options could broaden its applicability. Regulatory compliance, particularly with GDPR, is not explicitly addressed, which is crucial for institutions in jurisdictions with strict data privacy laws. Incorporating features like automated consent management and data anonymization would ensure legal robustness.

2.11.2 DegChain: A Permissioned Blockchain for Educational Verification

The DegChain framework, as outlined by Musti et al. [74], offers a promising blockchain-based solution for managing educational credentials, emphasizing privacy and security through the use of Hyperledger Fabric. This system allows candidates to control access to their degree certificates using private keys, ensuring that only authorized verifications occur. However, the framework faces several challenges that may impact its scalability, security, and overall usability. The reliance on secure private key management presents potential security vulnerabilities, as compromised or lost keys could lead to unauthorized access or denial of service. Additionally, the sequential approval process required for certificate generation across multiple departments could introduce delays, particularly in larger institutions, highlighting the need for more efficient consensus mechanisms or parallel processing. While the private blockchain setup ensures privacy, it also limits interoperability with other educational platforms, potentially hindering broader adoption. This could be addressed by integrating decentralized identity solutions or cross-chain interoperability. Furthermore, the requirement for candidates to manually approve each verification

request may become cumbersome, suggesting a need for automated access controls or predefined consent policies to improve user experience. Lastly, although DegChain prioritizes privacy, it does not explicitly address compliance with regulations such as GDPR, which is crucial for broader acceptance. Incorporating compliance mechanisms, such as automated data retention and right-to-erasure features, could enhance its regulatory alignment.

2.11.3 Framework for Digital Transfer of Educational Records

Hsu Mon Kyi, Ei Shwe Sin, and Thinn Thu Naing [75] propose a blockchain-based educational certification framework, introducing a comprehensive architecture designed to enhance the security, transparency, and reliability of managing student records. The framework is structured into four distinct layers: the front-end service layer, blockchain service layer, data storage service layer, and infrastructure service layer. Each layer contributes to the system's overall functionality, from managing student data and facilitating user interactions to securing transactions and maintaining the blockchain network's integrity.

One of the key strengths of this framework lies in its use of smart contracts to automate the validation and storage of educational records, thereby reducing the reliance on manual processes and enhancing the efficiency of academic certification. The inclusion of cryptographic services and distributed ledger technology ensures that student records are securely stored and immutable, addressing concerns about data integrity and tamper resistance. The auditing services, which leverage the proof-of-work consensus mechanism, further reinforce the system's security by ensuring that only authorized users can create and confirm transactions.

However, the framework also presents several challenges, particularly in terms of scalability and interoperability. The reliance on a decentralized peer-to-peer network,

while beneficial for transparency and security, may lead to performance bottlenecks as the number of transactions increases. This is especially relevant in the context of real-time data management, where the system's ability to handle large volumes of data efficiently could be strained. Additionally, while the framework allows for data sharing across different institutions and employers, the process of granting access through transaction IDs may become cumbersome for students, highlighting a potential area for further refinements, such as the introduction of more user-friendly access control mechanisms.

From a privacy perspective, the framework's design ensures that students retain control over who can access their records, aligning with GDPR principles. However, the effectiveness of this privacy control is contingent upon the secure management of private keys and the robustness of the cryptographic algorithms employed. Any vulnerabilities in these areas could compromise the system's overall security.

2.11.4 Framework for Secure Student Record Management

Alam [1] introduces a blockchain-based framework designed to enhance the management and verification of digital credentials in education. The framework leverages the capabilities of blockchain technology to address the inefficiencies and vulnerabilities associated with traditional paper-based and digital certificates. By integrating academic records into a blockchain network, the proposed system ensures that student credentials are securely stored, tamper-proof, and easily verifiable by external entities, such as employers and government officials.

A notable feature of the framework is its use of smart contracts to automate the verification process, thereby reducing the time and effort required for manual checks. When a student completes a course or module, their grades are recorded on the blockchain, and once all academic requirements are met, the system automatically

issues a digital transcript and diploma. These credentials are assigned a unique identifier, such as a Uniform Resource Identifier (URI), allowing for straightforward verification by third parties. The study also highlights several key issues with digital certificates, particularly the proliferation of counterfeit credentials and the difficulties associated with verifying and exchanging academic records. The blockchain-based solution addresses these challenges by providing a decentralized, immutable ledger that ensures the authenticity and integrity of academic credentials. Once recorded on the blockchain, these records are permanent and require no additional notarization, making the verification process more efficient and reliable.

However, the framework does present some challenges. The implementation of such a system requires significant technical infrastructure and expertise, which could be a barrier for smaller educational institutions. Additionally, while blockchain offers enhanced security and transparency, the system's success depends on the adoption of this technology across various sectors, including education and employment.

2.11.5 Blockchain Framework for Educational Record Management

Masood and Faridi [76] propose a framework that leverages blockchain technology to manage and verify educational credentials, focusing on digital signatures, smart contracts, and decentralized storage. While it effectively uses cryptographic techniques to ensure data integrity and security, there are gaps in its implementation of advanced privacy measures like homomorphic encryption and access control. The framework's approach to privacy, though innovative, relies heavily on public keys, raising potential concerns about data exposure.

Scalability is addressed through decentralized data management, but the framework does not explicitly tackle how it will manage large transaction volumes or prevent performance degradation over time. Its adaptability to various educational contexts is

promising, yet its flexibility in integrating new security features or evolving educational needs remains unclear.

Although the framework implies a focus on privacy, it does not specifically address compliance with regulations such as GDPR, potentially leaving gaps in data protection and user consent. Furthermore, the complexity of blockchain and smart contract management may pose challenges for institutional adoption, especially in regions with limited technical infrastructure.

To consolidate the key aspects discussed in this section, Table 2.2 provides a comprehensive summary of the current frameworks for digital certificate management on the blockchain, highlighting the privacy and security techniques employed across these solutions.

Although current frameworks for managing digital certificates on the blockchain provide robust structures for credentialing, they also reveal certain limitations and areas for improvement. These gaps highlight the need for further research and innovation. The following section will identify and discuss these research gaps, setting the stage for the development of more advanced and effective blockchain-based credentialing systems. Table 2.2 summarizes the solutions of Blockchain-Based Frameworks for Educational Digital Certificates.

Table 2. 2 Comparative Analysis of Blockchain-Based Frameworks for Educational Digital Certificates

Framework	Main Goal	Core Components	Techniques Used	Strengths	Weaknesses
Educational Credit Transfer Framework	Balance public verification with privacy in educational credit transfers.	Distributed consensus protocol, PoW, hash functions, Merkle trees, multisignature protocols.	PoW, hashing, multisignature protocols	Strong data integrity, public verification, and security through distributed consensus.	Security: Lacks advanced encryption techniques. Privacy: Inadequate protection of sensitive data. Scalability: High computational demands lead to performance bottlenecks.
DegChain: Permissioned Blockchain for Verification	Manage and verify educational credentials securely in a private blockchain.	Hyperledger Fabric, smart contracts, private key management, sequential approval process.	Smart contracts, private blockchain	Strong privacy controls, candidate-controlled certificate access, and a secure private blockchain environment.	Security: Vulnerabilities in private key management. Privacy: Limited user privacy in the approval process. Scalability: Delays due to sequential approval.
Digital Transfer of Educational Records Framework	Secure and transparent management of student records across institutions.	Multi-layer architecture: front-end, blockchain service, data storage, and infrastructure layers.	Smart contracts, cryptographic services, distributed ledger, proof-of-work consensus	Enhanced data integrity, transparency, and automation through smart contracts and cryptographic services.	Security: Dependence on robust cryptographic algorithms. Privacy: Potential key management issues. Scalability: Performance bottlenecks in decentralized networks.
Secure Student Record	Enhance the management and verification of	Blockchain network, smart contracts, unique	Smart contracts, blockchain,	Efficient verification process, tamper-proof records, and	Security: Vulnerability to centralized control if not widely adopted. Privacy: Risk of

Management Framework	digital credentials in education.	identifiers (URIs), decentralized storage.	digital transcript, and diploma issuance	automatic credential issuance.	exposing identifiers. Scalability: Requires significant infrastructure for broad implementation.
Blockchain Framework for Record Management	Manage and verify educational credentials with a focus on security and privacy.	Digital signatures, smart contracts, decentralized storage, public-private key pairs, portals for certificate verification.	Digital signatures, smart contracts, blockchain, certificate retrieval system	Strong data integrity and privacy through digital signatures and decentralized storage.	Security: Limited advanced privacy measures like homomorphic encryption. Privacy: Potential data exposure via public keys. Scalability: Unclear strategies for handling large transaction volumes.

2.12 Research Gaps in Current Blockchain-Based Frameworks for Educational Digital Certificates

This section outlines critical gaps in existing blockchain-based digital credential systems, focusing on security, privacy, and scalability. Addressing these deficiencies is essential for enhancing the robustness, user trust, and broader adoption of these systems.

2.12.1 Security Gaps

Despite the inherent security benefits of blockchain technology such as immutability and cryptographic safeguards current digital credential frameworks exhibit several security limitations. While some frameworks incorporate basic security features, they often lack advanced mechanisms, such as homomorphic encryption, which could further protect data even during processing. Additionally, inadequate key management practices leave these systems susceptible to unauthorized access and data breaches. Another major shortcoming is the absence of comprehensive protocols to counter insider threats, which increases the risk of data manipulation by internal actors with access privileges. Furthermore, many frameworks rely on basic cryptographic methods without integrating enhanced encryption techniques and robust access control mechanisms. This limited approach compromises the security posture of these systems, particularly when handling sensitive educational records across multiple institutions. Given the importance of safeguarding these records, it is clear that current frameworks lack the necessary layers of security to protect against sophisticated threats. These security gaps underscore a critical area for future development to enhance protection against unauthorized access, data tampering, and other potential security vulnerabilities.

2.12.2 Privacy Gaps

Privacy protection is another significant concern in blockchain-based credential systems, with many frameworks failing to address privacy comprehensively. Although public key cryptography is commonly employed, it does not fully mitigate privacy risks, especially when user data could be exposed if not managed correctly. Existing frameworks often lack mechanisms for data anonymization, which is essential for compliance with privacy regulations like the General Data Protection Regulation (GDPR).

Moreover, insufficient provision for user-controlled data access limits user autonomy over personal data. Many frameworks do not enable fine-grained control, preventing users from dynamically managing who can view or access their credentials. This absence of privacy-preserving features risks unauthorized data exposure and weakens user trust an essential factor for the success and acceptance of digital credential systems. Additionally, the reliance on public keys for credential search and verification introduces potential privacy risks, as it could permit unauthorized entities to access sensitive information. The lack of sophisticated privacy controls and consent management tools exacerbates this vulnerability, underscoring the need for more comprehensive privacy-preserving techniques within blockchain-based credential systems.

2.12.3 Scalability Issues

Scalability remains a critical barrier to the widespread adoption of blockchain-based digital credential systems. Many of the frameworks reviewed struggle to efficiently process high transaction volumes, particularly when using resource-intensive consensus mechanisms like Proof of Work (PoW).

These approaches can create performance bottlenecks, resulting in delays in transaction processing and difficulties in maintaining system performance as the network expands. Scalability challenges are particularly evident in frameworks designed to operate across multiple institutions or educational systems. The absence of effective synchronization and data management mechanisms across diverse environments restricts the ability of these systems to scale effectively, thus reducing their feasibility in real-world educational contexts. Moreover, many frameworks lack the flexibility to expand without significant performance degradation, which is a substantial concern in environments that demand real-time processing of educational records. Failures or delays in processing within these systems could have serious consequences for students and institutions. These scalability limitations highlight the need for more efficient and adaptable blockchain-based solutions capable of supporting widespread implementation across diverse and growing educational environments.

2.13 Conceptual Framework for SecureBlockcert

In response to the identified security, privacy, and scalability gaps within current digital credential systems, this section introduces a conceptual framework designed to address these challenges comprehensively. The proposed solution (SecureBlockcert) integrates advanced cryptographic techniques, privacy-preserving measures, and scalable architectures to enhance the overall robustness and adaptability of blockchain-based digital credential systems.

Hyperledger Fabric plays a central role in this framework by providing a permissioned environment that supports secure, private transactions. The platform's use of private channels and data collection allows for the controlled sharing of sensitive academic records, ensuring that only authorized participants can access specific data. This

approach directly addresses the privacy gaps identified earlier, where existing systems often fail to offer sufficient data anonymization and user-controlled access.

Furthermore, Hyperledger Fabric's modular consensus mechanisms enable the framework to scale effectively, accommodating large transaction volumes without compromising performance. The platform's flexible architecture also allows for the implementation of advanced cryptographic techniques, such as (ECC) and homomorphic encryption, which are crucial for enhancing security and ensuring data integrity.

By integrating Hyperledger Fabric into the proposed solution, the framework not only addresses the identified gaps in security, privacy, and scalability but also ensures compliance with regulatory requirements like the GDPR. This makes it a comprehensive and forward-looking approach to managing digital credentials in educational settings.

2.13.1 Core Components

This section outlines the fundamental components that form the backbone of the SecureBlockCert Framework, detailing their roles and applications in addressing security, privacy, and scalability challenges. Table 2.3 presents the key components and their respective applications within the framework.

Table 2. 3 Key Components and Their Applications in SecureBlockCert Framework

Component	Explanation	Application
Elliptic Curve Cryptography (ECC) and Edwards-curve Digital Signature Algorithm (EdDSA)	A public-key cryptography method offering strong security with smaller key sizes, suitable for resource-limited environments. EdDSA is a high-performance variant used for digital signatures.	Secures node authentication during registration, ensuring only legitimate entities can join the network.

Homomorphic Encryption	Enables computations on encrypted data without decryption, ensuring confidentiality during data processing.	Protects sensitive academic data (e.g., grades, certificates) by allowing secure processing without data exposure.
Hashing and Data Integrity	Hash functions create a fixed-size output from data, ensuring that any data alterations are easily detectable.	Ensures that certificate data remains tamper-proof, detecting any unauthorized modifications.
Access Control Mechanisms	Regulates who can view or interact with specific data, protecting sensitive information through controlled access.	Allows users to manage who can access their digital credentials, enhancing privacy and compliance with regulations.
Privacy Measures in Hyperledger Fabric	Advanced privacy features, including private data collections and channels, for confidential transactions.	Utilizes private channels to restrict access to sensitive data, ensuring it's only accessible to authorized parties.
Smart Contracts	Self-executing contracts that automate processes within the blockchain, enhancing efficiency and scalability.	Automates the issuance and verification of digital credentials, supporting scalability and reducing manual intervention.

2.13.2 Addressing Identified Gaps

To bridge the gaps identified in existing blockchain-based credentialing solutions, this research proposes specific enhancements and mechanisms tailored to address security, privacy, and scalability challenges. These solutions are outlined below:

a) **Security Gaps:** The integration of ECC, EdDSA, and homomorphic encryption strengthens security by ensuring robust node authentication and secure data processing.

b) **Privacy Gaps:** Access control mechanisms and Hyperledger Fabric's privacy features address privacy concerns by giving users control over their data and ensuring compliance with the GDPR.

c) **Scalability Issues:** The use of smart contracts and Hyperledger Fabric's scalable architecture addresses scalability concerns, enabling efficient handling of large transaction volumes.

2.14 Conclusion

This chapter has examined the security, privacy, and scalability challenges in existing blockchain-based digital credential systems. While current solutions leverage blockchain's strengths in security and authenticity, significant gaps remain, particularly in advanced encryption, data privacy, and scalability.

To address these challenges, the proposed framework integrates robust components such as (ECC), EdDSA for secure authentication, homomorphic encryption for data confidentiality, and Hyperledger Fabric's privacy features. These measures not only enhance security and privacy but also ensure compliance with the GDPR and improve scalability through the use of smart contracts.

This review establishes the foundation for the proposed framework, which aims to overcome the identified gaps and create a more secure, private, and scalable system for managing educational credentials on the blockchain.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Introduction

The primary objective of this research is to develop a blockchain-based framework that enhances the security, privacy, and scalability of digital credential systems. The framework aims to fortify node security within the credentialing ecosystem, safeguard student data, and strengthen both the issuance and verification procedures for blockchain-based academic certificates. By addressing critical concerns in security and privacy, the research intends to overcome the existing limitations of digital credential systems and establish a more reliable and efficient platform. To achieve these goals, the proposed framework incorporates advanced cryptographic techniques, such as Elliptic Curve Cryptography (ECC) and homomorphic encryption, alongside mechanisms for privacy preservation and scalability enhancements using Hyperledger Fabric. This chapter outlines the comprehensive research methodology designed to meet the research objectives set out in the first chapter and elaborates on the systematic approach used to ensure the framework's successful development and evaluation.

3.2 Phases of Research

This research methodology is organized into several key phases, each of which plays a vital role in the development and validation of the blockchain-based digital credential framework. Figure 3.1 illustrates these research phases. Emphasis is placed on the integration of security, privacy, and scalability components throughout the framework's design, implementation, testing, and evaluation phases.

The research begins with the conceptualization and design of the framework. It then progresses through rigorous expert validation, practical implementation, and

comprehensive testing, culminating in an in-depth evaluation of the framework's overall performance. Each phase ensures that the framework not only meets theoretical objectives but is also capable of functioning effectively in real-world applications.

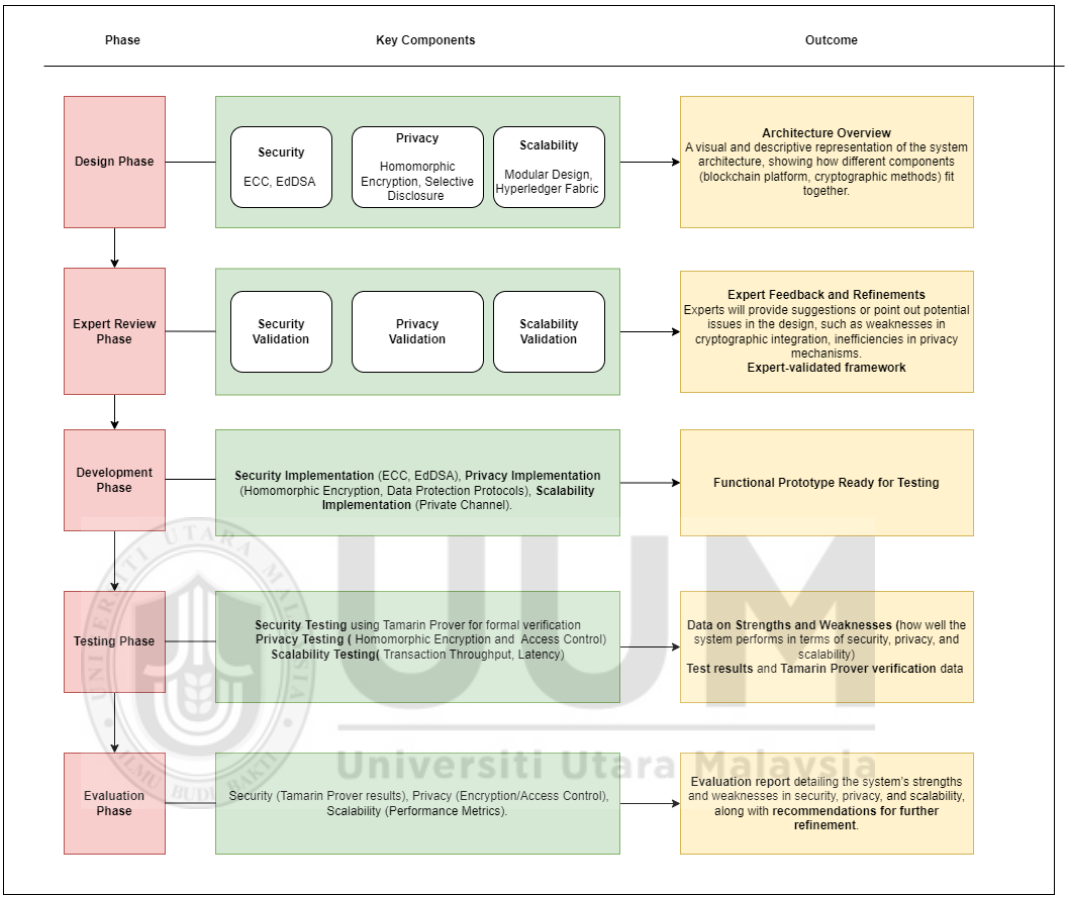

Figure 3.1 The Research Phases

3.2.1 Design Phase

The Design Phase serves as the cornerstone of the research methodology. During this phase, the conceptualization and architectural definition of the blockchain-based digital credential framework are established. It is critical to this process, as it lays the groundwork for integrating the essential components of security, privacy, and scalability key to addressing the deficiencies in existing digital credential systems.

3.2.1.1 Security Integration

Security is a primary concern for digital credential systems, as unauthorized access or data tampering can severely undermine the integrity and credibility of issued credentials. To mitigate these risks, Elliptic Curve Cryptography (ECC) and the Edwards-curve Digital Signature Algorithm (EdDSA) [77, 78] are incorporated into the framework. These cryptographic methods provide robust and efficient means for securing user authentication and ensuring transaction integrity.

The selection of ECC and EdDSA is driven by their strong cryptographic properties, which offer high levels of security with relatively low computational overhead compared to other algorithms. This makes them particularly well-suited for environments with limited resources or high transaction volumes.

In addition to these cryptographic algorithms, the framework includes role-based access control mechanisms to regulate data permissions. These mechanisms ensure that only authorized entities such as credential issuers, verifiers, and holders can access sensitive information. By doing so, the system prevents unauthorized access, ensures traceability, and makes credential-related actions auditable, thereby enhancing the overall security posture of the framework.

3.2.1.2 Privacy Integration

Protecting the privacy of credential holders is equally critical, particularly in educational and professional environments where sensitive personal data is involved. To safeguard user privacy, the framework integrates homomorphic encryption. This advanced cryptographic technique allows data to remain encrypted even while computations or verifications are performed, ensuring that no sensitive information is exposed during credential issuance or verification.

Furthermore, selective disclosure techniques are employed, granting users control over which specific data they choose to share with verifiers. This is especially useful in situations where verifiers require confirmation of specific attributes such as degree completion without needing access to the user's entire credential set. Through selective disclosure, the framework upholds user privacy while maintaining the integrity and reliability of the verification process.

3.2.1.3 Scalability Integration

As digital credential systems are expected to accommodate a growing number of institutions, users, and transactions, scalability becomes a crucial consideration during the design phase. The framework leverages Hyperledger Fabric, a modular and permissioned blockchain platform, to facilitate scalability. Hyperledger Fabric's flexible architecture allows for the seamless addition of new participants, channels, and nodes, all without negatively impacting system performance. This modularity ensures that the system can accommodate increasing transaction volumes as the number of users and credential transactions grows.

To further optimize scalability, the framework utilizes private channels within the blockchain network. These channels allow specific credential transactions to be processed privately between authorized participants, which reduces the computational burden on the main blockchain. Additionally, off-chain storage solutions are employed to manage large datasets, such as the actual content of digital credentials. Only essential transaction data such as hashes are stored on-chain, further minimizing the computational load and ensuring that the system can efficiently handle large volumes of credential issuance and verification.

At the conclusion of the design phase, a detailed blueprint is produced, outlining the system's architecture and its integrated components of security, privacy, and

scalability. This blueprint is a critical deliverable, as it will serve as the guiding document for the next stages of the research, particularly the Expert Review Phase and the Implementation Phase. By clearly defining the structure and functionality of the framework, the design phase ensures that the framework is ready for expert validation and practical implementation.

3.2.2 Expert Review Phase

The Expert Review Phase is a crucial step in the validation of the conceptual framework developed during the design phase [79, 80]. This phase focuses on gathering feedback from domain experts in the fields of security, privacy, and scalability to ensure the framework is both theoretically sound and practical for real-world deployment. Expert evaluations provide valuable insights into the framework's strengths and reveal areas for improvement, enabling necessary refinements before moving forward to the implementation phase. The expert review process follows established methodologies for security verification, privacy assessment, and scalability testing.

Expert reviews are widely recognized as a critical method for validating research frameworks, particularly in emerging fields like blockchain-based digital credential systems. The structured approach in this study ensures comprehensive feedback and rigorous validation, allowing the framework to be thoroughly examined.

3.2.2.1 Selection of Experts

The first step in this phase involves identifying suitable experts from academia. Experts were selected based on the following criteria:

a) A record of active engagement in fields relevant to blockchain security, cryptography, and privacy.

b) Possession of a doctoral degree in related fields.

c) Faculty positions at reputable universities with a proven record of scholarly publications in blockchain and security.
d) At least five years of relevant experience to ensure their feedback is both credible and valuable.

3.2.2.2 Establishment of Verification Criteria

To facilitate a structured review process, verification criteria were established, focusing on the following key areas:

a) Authentication
b) Authorization
c) Confidentiality
d) Integrity
e) Privacy

These criteria form the foundation for expert evaluations. Comprehensive checklists were developed and distributed to the experts, covering specific aspects of the framework that required assessment. These checklists ensured that no critical component was overlooked. For further details, refer to Appendices A and B in this study.

3.2.2.3 Gathering and Interpreting Feedback

Once the experts completed their evaluations, the feedback was carefully collected, reviewed, and synthesized to identify common themes and areas for further development. This process was instrumental in identifying vulnerabilities, weaknesses, and potential improvements related to the framework's security protocols, privacy mechanisms, and scalability solutions. After this analysis, critical refinements were made to enhance the framework's robustness and credibility.

The following sections detail how expert feedback was applied to each of these critical areas, leading to a comprehensive validation of the framework.

3.2.2.4 Security Validation

Security is one of the foundational elements of the digital credential framework. In this phase, experts in blockchain security and cryptography are consulted to assess the robustness of the cryptographic protocols integrated into the framework, such as Elliptic Curve Cryptography (ECC) and the Edwards-curve Digital Signature Algorithm (EdDSA).Formal verification of these protocols is conducted using tools like the Tamarin Prover [81], which allows for detailed modeling of adversarial conditions.

To further illustrate this process, Figure 3.2 shows Tamarin's Interactive Mode, which was used to model and verify the framework's cryptographic protocols under various potential attack vectors.

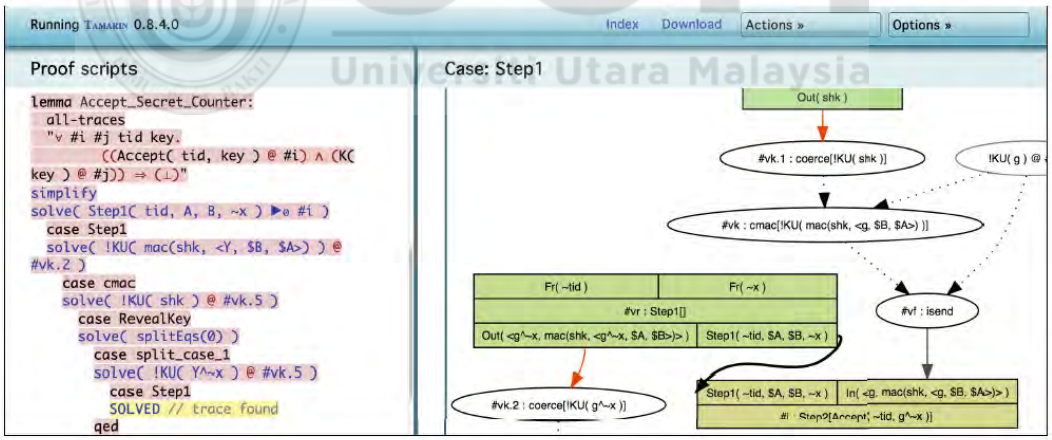

Figure 3.2 Tamarin's Interactive Mode

The interactive mode allows researchers to simulate complex cryptographic interactions and assess the resilience of the system against different types of threats, ensuring that the security components are robust and well-validated before implementation.

A panel of experts conducted an evaluation to assess the following aspects of the proposed framework: the effectiveness of ECC and EdDSA in ensuring secure user identification and preventing unauthorized access; the resilience of the framework against common attack vectors, such as man-in-the-middle (MITM) attacks, replay attacks, and unauthorized credential modification; and the strength of the access control mechanisms in regulating permissions and access to sensitive data within the credential system.

The methodology for security validation involves a combination of expert consultations, formal verification, and theoretical security proofs to rigorously evaluate and enhance the framework's cryptographic protocols.

a) **Expert Consultations**: Cryptography and blockchain security experts are provided with comprehensive details of the framework's security protocols and asked to identify potential risks and vulnerabilities.
b) **Formal Verification**: Tools such as the Tamarin Prover are employed to formally verify the cryptographic protocols, ensuring they are resilient to adversarial conditions. This includes modeling the system's cryptographic algorithms in a symbolic system.
c) **Security Proofs**: Theoretical security proofs are reviewed to ensure that the cryptographic elements of the framework (ECC, EdDSA) meet industry standards for confidentiality, integrity, and non-repudiation.

The feedback from the Security Validation phase helps refine the cryptographic measures in place, strengthening the framework's defense against potential security breaches.

3.2.2.5 Privacy Validation

In systems handling sensitive user data, privacy is of paramount importance. The Privacy Validation phase focuses on ensuring that the framework's privacy-preserving techniques such as homomorphic encryption [82] and selective disclosure [64, 83] mechanismsadequately protect user anonymity and data confidentiality, while still allowing for credential verification.

As part of this phase, experts assess the effectiveness of homomorphic encryption in ensuring that data remains encrypted during credential issuance and verification without exposing sensitive information. Additionally, they evaluate the applicability of selective disclosure techniques, which enable users to control which parts of their credential data are shared with verifiers. The evaluation ensures that these methods align with privacy regulations such as the General Data Protection Regulation (GDPR).

The privacy validation methodology employs a combination of theoretical analysis, simulation testing, and comparative benchmarking to rigorously evaluate the framework's privacy-preserving mechanisms.

a) **Theoretical Analysis**: Experts conduct a theoretical evaluation of the privacy mechanisms to ensure they meet legal and ethical standards for data protection.
b) **Simulation Testing**: Credential issuance and verification processes are simulated to assess how well the privacy mechanisms function under both normal and adversarial conditions. This includes verifying whether sensitive data remains protected throughout the process.
c) **Comparative Benchmarking**: The privacy-preserving features of the framework are compared against existing blockchain-based privacy solutions

to determine whether the framework offers advancements or requires improvements.

This validation ensures that the privacy mechanisms are robust enough to protect users' data and comply with relevant privacy regulations.

3.2.2.6 Scalability Validation

The scalability of the framework is essential to ensure that it can handle increasing transaction volumes and user growth without performance degradation. This phase involves simulations within the Hyperledger Fabric environment to evaluate system performance under different load conditions. Hyperledger Explorer was utilized during this validation phase to monitor real-time performance and identify bottlenecks as the system scales [100].

Figure 3.3 presents the Hyperledger Explorer Interface, offering insight into the real-time monitoring of the system's throughput and latency, which helps validate that the framework can manage increasing numbers of transactions without negatively affecting performance.

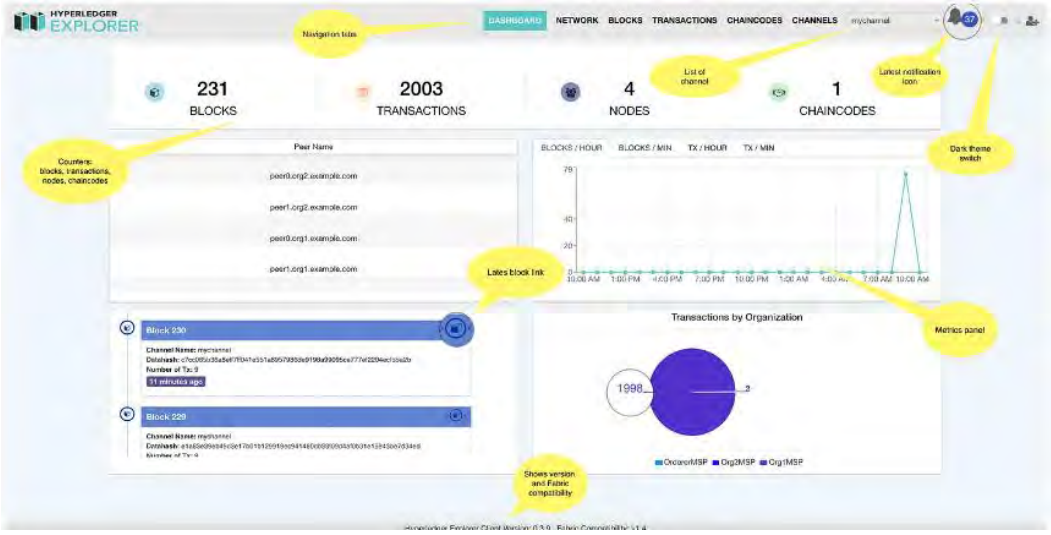

Figure 3.3 Hyperledger Explorer Interface

By using Hyperledger Explorer [84], [100], key performance metrics such as transaction throughput and latency were closely monitored, ensuring that the system is scalable enough to support large-scale credential issuance and verification across multiple institutions.

As part of this evaluation, experts assessed the design of the Hyperledger Fabric architecture, focusing particularly on the use of private channels to ensure efficient management of increasing numbers of participants and transactions. They also analyzed transaction throughput (measured in transactions per second) and latency (the time taken for a transaction to be confirmed and added to the blockchain), both of which are critical indicators of the framework's scalability.

The scalability validation methodology combines empirical analysis and performance metric evaluation to assess the framework's ability to handle high transaction volumes and meet the demands of large-scale credential issuance and verification.

a) **Empirical Analysis**: High transaction volumes are simulated within a Hyperledger Fabric environment to evaluate system performance under various conditions. This simulation tests the framework's capacity to handle growing credential issuance and verification demands.

b) **Performance Metrics**: Key metrics such as transaction throughput and latency are assessed to determine whether the framework can scale effectively. Transaction Throughput is defined as the number of transactions processed within a specific period of time [85], expressed as:

   Transaction Throughput = Number of Transactions Processed / Period of Time

   Latency refers to the time between the submission of a transaction and its addition to the blockchain [85], calculated as:

Latency = Time Between Transaction Submission and Addition to Blockchain

[85]

c) **Benchmarking**: The framework's scalability is compared with other blockchain platforms and digital credential management solutions to identify areas where improvements can be made.

The scalability validation helps confirm whether the framework can efficiently support large-scale operations and handle future growth

After the Expert Review Phase, the framework is refined based on the insights and recommendations provided by the experts. Any identified weaknesses, whether related to cryptographic security, privacy mechanisms, or scalability solutions, are addressed to ensure the framework meets the highest standards.

The final deliverable is an expert-validated framework that:

a) Has reinforced security protocols based on expert feedback and formal verification.

b) Demonstrates strong privacy-preserving features that comply with both technical standards and regulatory frameworks.

c) Confirms scalability through empirical testing, ensuring that the system can handle increased transaction volumes and users efficiently.

3.2.3 Development Phase

The development phase marks the transformation of the conceptual framework into a functional, real-world system. This phase involves both the construction and deployment of the blockchain-based digital credential system, integrating the security, privacy, and scalability components conceptualized during the design and expert review Phases. The focus of this phase is to turn the framework blueprint into an operational prototype, ready for rigorous testing in the subsequent phase.

The methodology for the Development Phase centers around four key activities:

a) Technical Setup and Configuration of the Blockchain Network
b) Integration of Security Mechanisms
c) Deployment of Privacy-Preserving Techniques
d) Ensuring Scalability through Blockchain Architecture

Each of these activities is essential for ensuring the framework operates securely, privately, and efficiently in a real-world environment.

3.2.3.1 Technical Setup and Configuration of the Blockchain Network

The first step in the Development Phase involves setting up the Hyperledger Fabric blockchain network, which serves as the foundation for the entire system. As Hyperledger Fabric is a permissioned blockchain, specific configurations are required to meet the framework's goals in terms of scalability, privacy, and security.

This phase begins with network initialization, which involves creating channels, and peer nodes, and configuring ordering services. Channels are critical for establishing isolated communication pathways between organizations, and ensuring confidential and auditable credential transactions. The next activity is the configuration of Membership Service Providers (MSPs), which manage identities within the Hyperledger Fabric network. This configuration ensures that all participating nodes, such as educational institutions and employers, are properly authenticated and authorized to access the blockchain. Finally, the ordering service is configured to determine how transactions are added to the blockchain ledger. Proper configuration of the ordering service guarantees that transactions are securely and efficiently ordered and added, supporting the scalability of the system.

The methodology for setting up the system begins with a systematic deployment of Hyperledger Fabric components in a staging environment. This initial deployment

allows for thorough testing and validation before transitioning to a production environment. After the setup, the network undergoes performance testing to evaluate its transaction throughput and latency. This testing ensures the network can handle anticipated workloads, such as processing multiple credential issuances and verifications, without experiencing performance degradation.

3.2.3.2 Integration of Security Mechanisms

Once the blockchain network is configured, the next step is the integration of the security mechanisms validated during the Expert Review Phase. This phase focuses on ensuring that the blockchain network is resistant to unauthorized access and data tampering. The first key activity involves the implementation of cryptographic protocols. The framework integrates Elliptic Curve Cryptography (ECC) and the Edwards-curve Digital Signature Algorithm (EdDSA) to secure transactions. Each credential issuance, verification, or modification within the blockchain is cryptographically signed and authenticated using these protocols. Another crucial activity is the setup of access controls. Role-Based Access Controls (RBAC) are implemented to regulate access to sensitive credential data. These controls are embedded within smart contracts, ensuring that only authorized participants, such as credential issuers, can issue, modify, or verify credentials.

The methodology for security integration encompasses two main approaches. First, cryptographic integration involves incorporating cryptographic libraries that implement ECC and EdDSA into the blockchain system, ensuring that all credential interactions are secure. Second, smart contract security is achieved by designing smart contracts with strict access controls. For example, credential issuers, such as universities, are authorized to issue credentials, while verifiers, such as employers, are restricted to viewing credentials without modification.

3.2.3.3 Deployment of Privacy-Preserving Techniques

Preserving privacy is a core objective of the blockchain-based digital credential system. This phase ensures the seamless integration of privacy-preserving techniques into the system to safeguard user data during credential issuance and verification processes.

A key activity in this phase involves the implementation of homomorphic encryption, which allows verifiers to perform calculations on encrypted data, such as validating a credential, without accessing the underlying raw data. This ensures that sensitive user information remains confidential, even during the verification process. Another critical activity is the incorporation of selective disclosure, a feature embedded in smart contracts that enables users to control which parts of their credential data are shared with verifiers. This mechanism allows users to disclose only the necessary information while keeping other details private.

The methodology for privacy integration includes two primary approaches. First, privacy testing is conducted by simulating credential transactions to rigorously evaluate the effectiveness of homomorphic encryption and selective disclosure under real-world conditions. This ensures that user data remains private throughout the process. Second, GDPR compliance is ensured by incorporating features such as the right to be forgotten and data minimization practices. These measures align the system with privacy regulations, ensuring that user data is protected in accordance with established legal standards.

3.2.3.4 Ensuring Scalability through Blockchain Architecture

The final activity of the development phase focuses on ensuring the system's scalability, a critical requirement for accommodating growing participants and

increasing transaction volumes. Hyperledger Fabric is designed to support such scalability, making it a foundational feature of the system.

One of the key activities in this phase is the implementation of private channels for credential transactions. These private channels isolate credential transactions between specific organizations, reducing network congestion and improving scalability. This configuration ensures that only relevant parties have access to the necessary transactions, thereby maintaining efficiency as the network expands.

The methodology for scalability integration involves two main approaches. First, load testing is conducted through simulations to evaluate the system under various transaction loads. During these tests, transaction throughput, latency, and network stability are continuously monitored to ensure that the system can scale without performance degradation. Second, the optimization of the consensus mechanism within Hyperledger Fabric is carried out. The pluggable consensus mechanism is fine-tuned to balance scalability with security, ensuring efficient transaction confirmations as the network grows.

At the conclusion of the development phase, the blockchain-based digital credential system is deployed as a functional prototype. This prototype integrates the security, privacy, and scalability components conceptualized during the previous phases. The system is now prepared for rigorous testing in the Testing Phase, where it will be operated in a controlled environment simulating real-world conditions to validate its ability to securely issue, verify, and manage digital credentials.

3.2.4. Testing Phase

The Testing Phase is a crucial part of the research methodology, where the blockchain-based digital credential framework undergoes rigorous testing to evaluate its performance across key areas: security, privacy, and scalability. The system is tested

under simulated real-world conditions using advanced tools such as Tamarin Prover, Hyperledger Caliper [86, 99], and Hyperledger Explorer [84] to assess its robustness, functionality, and overall performance.

The methodology for the Testing Phase is organized into three core testing areas:

a) Security Testing

b) Privacy Testing

c) Scalability Testing

These tests are essential for ensuring that the framework meets the specified goals of resilience, user privacy protection, and scalability.

3.2.4.1 Security Testing

The Security Testing phase is designed to evaluate the framework's resilience against various attack vectors, ensuring that its cryptographic protocols and authentication mechanisms provide robust protection.

A critical activity in this phase is penetration testing, which involves using tools such as Hyperledger Explorer to simulate external attacks, including man-in-the-middle (MITM) attacks, SQL injections, and brute force attacks. These simulations help identify vulnerabilities in the system's defenses. Another essential activity is formal security verification using the Tamarin Prover. This tool formally verifies cryptographic protocols, such as Elliptic Curve Cryptography (ECC) and Edwards-curve Digital Signature Algorithm (EdDSA). By modeling the protocols in a symbolic system, the Tamarin Prover validates their security properties under adversarial conditions, ensuring they meet standards for authentication, integrity, and non-repudiation.

The methodology for security testing incorporates two main approaches. First, penetration testing tools are employed to conduct simulated attacks, uncovering

potential vulnerabilities in the framework's security defenses. These tests assess the system's ability to prevent unauthorized access and data tampering. Second, formal verification with the Tamarin Prover is performed. The cryptographic protocols are modeled and tested in adversarial environments to validate their robustness and ensure that the framework's security properties withstand potential attacks.

3.2.4.2 Privacy Testing

The Privacy Testing phase evaluates the effectiveness of the framework's privacy-preserving mechanisms, ensuring that user data remains protected throughout the credential issuance, storage, and verification processes.

One of the key activities in this phase is the testing of homomorphic encryption. Simulated scenarios for credential issuance and verification are used to evaluate the system's ability to process encrypted data without revealing the underlying information, ensuring user data privacy during all stages of the transaction lifecycle. Additionally, the testing of selective disclosure is performed to verify the framework's ability to allow users to disclose only the necessary parts of their credentials while protecting other data from being accessed by verifiers.

The methodology for privacy testing includes three main approaches. First, simulated credential scenarios are used to test homomorphic encryption by issuing and verifying credentials in encrypted form, ensuring that the system processes encrypted data without exposing sensitive information. Second, selective disclosure simulations are conducted to confirm that the system allows users to share specific data points, such as degree completion, without revealing other personal information. Finally, privacy metrics are utilized to measure privacy protection. These metrics include data exposure risk, encryption performance (time and resource usage), and compliance with GDPR and other regulatory standards.

3.2.4.3 Scalability Testing

The Scalability Testing phase evaluates the framework's capacity to handle increasing transaction volumes and user growth without compromising performance. This phase ensures that the system maintains high throughput and low latency, even under stress. The first key activity in this phase is load testing, where the system is subjected to high volumes of credential issuance and verification requests using Hyperledger Caliper. This testing assesses how well the framework can scale to accommodate a growing number of transactions and participants. Next, transaction throughput measurement is performed to determine the number of transactions processed per second (TPS), ensuring the system maintains efficiency as demand increases. Finally, latency measurement involves monitoring the time taken for a transaction to be confirmed and added to the blockchain, a critical metric for real-time credential verification.

The tools and methodology for scalability testing involve two primary approaches. First, load testing with Hyperledger Caliper is conducted by running simulations to evaluate the system's performance under varying levels of demand. Key performance metrics are assessed, including transaction throughput, calculated as:

Transaction Throughput (TPS) = Number of Transactions Processed / Time Period.

and latency, calculated as:

Latency = Time Between Transaction Submission and Confirmation on Blockchain.

Second, performance monitoring with Hyperledger Explorer is used to track real-time performance. This tool enables testers to observe how transactions are processed under heavy loads and identify potential bottlenecks affecting scalability.

3.2.5 Evaluation Phase

The evaluation phase is critical to ensure that the blockchain-based digital credential framework performs well across all key dimensions. The goal of this phase is to assess

the framework's effectiveness in terms of security, privacy, and scalability, and to address any weaknesses identified during the Testing Phase. This phase also includes a comparative analysis of the framework against existing solutions, ensuring its readiness for real-world deployment.

The methodology for the Evaluation Phase focuses on the following areas:

a) Security Evaluation

b) Privacy Evaluation

c) Scalability Evaluation

d) Comparative Analysis and Refinement

3.2.5.1 Security Evaluation

The security evaluation phase focuses on analyzing the results obtained from the Tamarin Prover verification and penetration testing conducted during the Testing Phase. The primary objective is to ensure that the cryptographic protocols and security mechanisms are robust and meet established industry standards for security.

The methodology for security evaluation involves several critical steps. First, data compilation and review are undertaken to systematically analyze the results from the Tamarin Prover, penetration tests, and stress tests. This process identifies any existing security gaps or vulnerabilities in the framework's design. Next, a formal risk assessment is performed based on the test results, highlighting potential areas where additional security measures may be necessary. This step ensures that the framework's security mechanisms remain resilient against emerging threats. Finally, if vulnerabilities or weaknesses are identified, recommendations for further improvements are developed. These recommendations focus on enhancing cryptographic protocols, such as Elliptic Curve Cryptography (ECC) and Edwards-

curve Digital Signature Algorithm (EdDSA), and refining access control mechanisms to strengthen the overall security of the framework.

3.2.5.2 Privacy Evaluation

The privacy evaluation phase assesses the effectiveness of the framework's privacy-preserving mechanisms, particularly homomorphic encryption and selective disclosure. The objective is to ensure that these mechanisms comply with privacy standards, such as the General Data Protection Regulation (GDPR), while enabling secure and efficient credential verification.

The methodology for privacy evaluation involves a detailed analysis of privacy test results. Results from the privacy tests conducted during the Testing Phase, specifically those related to homomorphic encryption and selective disclosure, are thoroughly examined. This analysis evaluates whether the framework's privacy mechanisms align with established privacy regulations, ensuring that sensitive user data remains protected while supporting the operational requirements of credential verification.

3.2.5.3 Scalability Evaluation

The scalability evaluation phase assesses the framework's ability to handle increasing transaction volumes and user loads without experiencing performance degradation. This evaluation focuses on the system's efficiency in terms of transaction throughput, latency, and resource utilization, ensuring that the framework can scale to meet real-world demands.

The methodology for scalability evaluation involves two key approaches. First, a detailed performance metrics analysis is conducted using data obtained from Hyperledger Caliper. Key metrics, including transaction throughput and latency, are analyzed to assess the framework's scalability under stress. Transaction throughput is calculated as**:**

Transaction Throughput = Number of Transactions Processed / Time Period.

while latency is defined as:

Latency = Time Between Transaction Submission and Confirmation on Blockchain.

Second, comparative benchmarking is performed by comparing the scalability evaluation results against industry benchmarks for blockchain-based credential systems. This comparison highlights areas where the framework excels and identifies opportunities for improvement, ensuring the system is prepared to handle real-world scalability demands.

3.2.5.4 Comparative Analysis and Refinement

The comparative analysis phase evaluates how the framework performs relative to existing blockchain-based credential systems. This step is crucial for identifying areas where the framework demonstrates significant advantages and pinpointing opportunities for further refinement to ensure its competitiveness in the field.

The methodology for comparative analysis involves a rigorous benchmarking process. The framework's performance in key areas such as security, privacy, and scalability is compared against other established solutions. This comparison relies on industry-standard metrics and published performance data from similar systems, providing a clear perspective on the framework's strengths and areas for improvement.

3.3 Conclusion

The research methodology outlined in this chapter presents a systematic and rigorous approach to developing, validating, and evaluating a blockchain-based digital credential framework. Each phase design, expert review, implementation, testing, and evaluation was carefully structured to ensure the integration of essential security, privacy, and scalability components, addressing the identified gaps in existing digital

credential systems. In the design phase, the conceptual framework was developed by incorporating advanced cryptographic protocols such as ECC and EdDSA for security, homomorphic encryption for privacy, and Hyperledger Fabric for scalability. The Expert Review Phase provided a critical validation of this framework, refining it through feedback from domain experts specializing in blockchain security, privacy, and scalability. The Implementation Phase translated the theoretical design into a functional prototype, integrating the key components and ensuring that the system was built with robust security measures, privacy-preserving techniques, and scalable infrastructure. This phase also laid the foundation for real-world testing by deploying the framework in a controlled environment. During the Testing Phase, tools like Tamarin Prover, Hyperledger Caliper, and Hyperledger Explorer were used to evaluate the framework's performance. The results demonstrated its ability to handle real-world conditions securely, maintain user privacy, and scale efficiently under increasing loads. Each component was rigorously tested to ensure that the system met the defined security, privacy, and scalability objectives. Finally, the Evaluation Phase analyzed the testing outcomes to assess the framework's effectiveness. By reviewing performance metrics, comparing the system to existing solutions, and refining it based on expert feedback, the framework was confirmed to be a robust solution for managing digital credentials on the blockchain.

CHAPTER FOUR
SECUREBLOCKCERT FRAMEWORK DESIGN

4.1 Introduction

The emergence of digital credentials in educational institutions necessitates a robust framework to ensure their security, privacy, and scalability. This chapter presents SecureBlockCert, an innovative framework specifically engineered to elevate the security and privacy of entities and data within digital certificate systems on blockchain networks. The architecture of SecureBlockCert is meticulously crafted, comprising three integral modules: security enhancement, privacy preservation, and issuance and verification.

These modules are strategically designed to strengthen their corresponding dimensions of the digital certificate infrastructure, with a unified goal of reinforcing security protocols, ensuring data confidentiality, and nurturing systemic trust. At the heart of SecureBlockCert lies a commitment to maintaining the indisputable integrity of node registrations, protecting sensitive information against unauthorized access, and providing a streamlined workflow for the creation and validation of digital credentials. By focusing on these elements, SecureBlockCert aims to facilitate seamless and secure interactions among stakeholders, including educational institutions, students, and employers. The subsequent sections will explore the framework's architecture, its components, and the methodologies employed to safeguard sensitive data while ensuring the integrity and authenticity of credentials.

4.2 SecureBlockCert Framework

The SecureBlockcert framework is structured into multiple layers, each focusing on specific aspects such as blockchain infrastructure, cryptographic security, access control, privacy protection, and scalability. Each layer is designed to ensure that the

system meets the necessary requirements for managing digital credentials effectively. Figure 4.1 illustrates these layers within the SecureBlockCert framework.

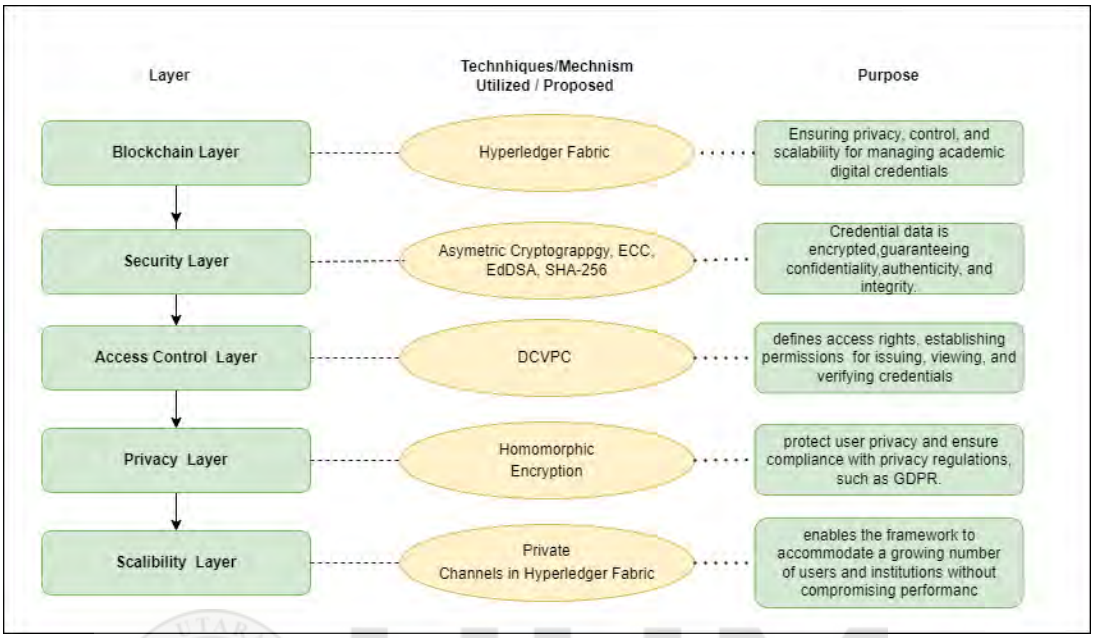

Figure 4.1 Layers of SecureBlockCert Framework

4.2.1 Blockchain Layer

The blockchain layer serves as the backbone of the proposed framework. Hyperledger Fabric is chosen as the underlying blockchain due to its permissioned nature, which allows for secure, private, and controlled access among credential stakeholders, including issuers, holders, and verifiers.

a) **Permissioned Access**: The permissioned structure of Hyperledger Fabric ensures that only authorized participants can join the network. This mitigates the risk of unauthorized access and potential data breaches, which are critical concerns in digital credentialing.

b) **Transaction Management**: The blockchain layer efficiently handles credential issuance, updates, and verifications through its transaction processing capabilities. The unique channel-based architecture of Hyperledger

Fabric enables institutions to create private communication channels for specific transactions, enhancing both privacy and performance.

c) **Immutable Ledger**: Every transaction is recorded on a tamper-resistant ledger, ensuring that the history of credential issuance and verification is transparent and auditable. This feature builds trust among stakeholders, as verifiers can confidently validate credentials against an unalterable record.

d) **Smart Contracts**: The incorporation of smart contracts automates the credential issuance and verification processes, minimizing human intervention and reducing the potential for errors. Smart contracts can define specific criteria that must be met before a credential can be issued or verified, further enhancing security.

The blockchain layer guarantees security by ensuring immutability and controlled access, enhances privacy through the use of private channels for sensitive transactions, and contributes to scalability through efficient transaction processing and the potential for off-chain solutions.

4.2.2 Cryptographic Layer

This layer ensures secure interactions among participants through advanced cryptographic algorithms, with a focus on confidentiality, integrity, and authenticity.

a) **Elliptic Curve Cryptography (ECC)**: ECC is utilized for encryption due to its efficiency and strong security with relatively small key sizes. This is particularly important in a resource-constrained environment where computational efficiency is a priority.

b) **EdDSA for Digital Signatures**: The Edwards-Curve Digital Signature Algorithm (EdDSA) is employed to ensure that the credentials are securely

signed, guaranteeing their authenticity. EdDSA provides high security while being efficient in terms of performance.

c) **Secure Hash Function**: Hash functions such as SHA-256 are employed to maintain the integrity of credential data. Any modification to the credential can be detected by comparing the hash values, providing a layer of security against tampering.

The cryptographic layer enhances security by ensuring that data is encrypted, authenticated, and untampered. It supports scalability through the use of lightweight algorithms that do not compromise system performance, enabling efficient processing of numerous credential transactions.

4.2.3 Access Control Layer

The Access Control Layer implements a Role-Based Access Control (RBAC) mechanism to manage user roles and permissions, ensuring that only authorized entities can access or modify credential data.

a) **Role Definition and Management:** Roles are defined for various stakeholders—issuers, holders, verifiers, and administrators each with specific permissions tailored to their functions within the system. This structure allows for efficient management of user roles and ensures that security policies are enforced consistently

b) **Dynamic Access Policies:** Efficiently adapts access permissions as the network grows, ensuring scalability.

This layer strengthens security by enforcing strict access controls based on defined roles, enhances privacy by allowing credential holders to control who can access their data, and provides scalability by managing access permissions efficiently as the network grows.

4.2.4 Privacy Layer

The Privacy Layer is designed to protect sensitive information about credential holders while allowing verifiers to access necessary data for validation purposes. The integration of advanced privacy-preserving techniques ensures that user data remains confidential.

a) **Homomorphic Encryption**: This encryption method allows computations to be performed on encrypted data without requiring decryption. For example, verifiers can validate certain aspects of a credential (like its authenticity) without accessing the actual data, thereby preserving user privacy [87].

b) **Selective Disclosure**: Credential holders can choose to disclose only specific attributes of their credentials (e.g., completion of a course) without revealing additional sensitive information (like grades). This minimizes the risk of data exposure and aligns with privacy best practices.

c) **User-Controlled Consent**: The privacy layer incorporates mechanisms for user-controlled consent, allowing credential holders to grant or revoke access to their data as needed. This empowers users and enhances trust in the system.

The privacy layer directly addresses privacy concerns by ensuring sensitive data is not exposed during credential verification processes, while also supporting scalability by optimizing privacy-preserving operations and reducing data load.

4.2.5 Scalability Layer

To manage large datasets and accommodate a growing number of institutions, students, and verifiers, the framework incorporates solutions that ensure scalability and maintain high performance. Private Channels in Hyperledger Fabric: The use of private channels enables multiple private communication pathways within the

blockchain network. This allows for tailored interactions among specific parties, enhancing both privacy and efficiency in transactions.

This layer ensures scalability by optimizing data storage and communication methods. It supports privacy through the use of private channels and ensures that the framework can handle growing amounts of data and transactions without performance degradation.

To ensure interoperability and legal compliance, the framework aligns with several international standards and regulations:

a) **W3C Verifiable Credentials Standard**: Compliance with this standard ensures that digital credentials can be issued, stored, and verified across different systems, promoting interoperability among various stakeholders in the credentialing ecosystem.

b) **GDPR Compliance**: The framework's privacy measures, such as selective disclosure and data minimization, ensure that it adheres to the General Data Protection Regulation (GDPR) and other privacy regulations, thereby protecting user rights.

4.3 Initial Design of SecureBlockCert Framework

This section introduces the Initial Framework Design of SecureBlockCert, as illustrated in Figure 4.1. Developed from the findings in the literature review and inspired by successful solutions like Blockcert, the framework integrates three core components to achieve secure, privacy-respecting, and effective digital certificate management.

4.3.1 Stakeholder Inclusion:

The framework defines three primary stakeholders and their respective roles:

a) **Issuer**: Typically an educational institution responsible for issuing digital certificates, ensuring the authenticity and integrity of credentials.

b) **Student**: The certificate holder, who manages and controls their digital credentials and can decide what information to share with verifiers.

c) **Verifier**: Employers or institutions that assess the validity of the credentials presented by students, ensuring they meet required standards.

These roles are adapted from Blockcert's established structure, aligning with the framework's objectives.

4.3.2 Security Component

The Security Component focuses on strengthening authentication during node registration, drawing from but also enhancing existing solutions:

a) **Asymmetric Cryptography**: Uses public/private key pairs, as in Blockcert, to securely identify and communicate between participants. The public key is used for credential verification, while the private key is retained by the issuer for signing.

b) **Node Authentication**: Ensures that only authorized nodes join the network, addressing vulnerabilities found in current solutions.

c) By building on established security practices and introducing enhancements, this component provides robust protection against emerging threats.

4.3.3 Privacy Component:

This component enhances the protection of sensitive information contained in digital certificates. While Blockcert includes basic privacy features, SecureBlockCert incorporates advanced privacy-preserving techniques:

a) **Homomorphic Encryption**: Allows for computations on encrypted data without requiring decryption, thus preserving user privacy during verification and reducing the risk of data exposure.

b) **Data Privacy**: Keeps sensitive information encrypted throughout the verification process, offering enhanced protection that surpasses what existing solutions provide.

4.3.4 Issuance and Verification Enhancement:

The third component advances the issuance and verification process, building on Blockcert's issuance protocols with the following enhancements:

a) **Decentralized Identifiers (DIDs)**: Empowers users to manage their identities independently, enhancing control over personal data and addressing limitations in traditional systems.

b) **Verifiable Credentials (VCs)**: Uses cryptographically signed credentials issued by the issuer, ensuring authenticity and integrity. This approach reinforces the foundation for secure, privacy-conscious credentialing and aligns with Blockcert's principles.

Expert Review Feedback

As mentioned in the previous chapter, this initial framework was subjected to an expert review process. The feedback provided valuable insights that informed necessary enhancements to the design. Based on these suggestions, the framework has been revised and re-evaluated. The refined and verified framework, depicted in Figure 4.2, will be elaborated upon in the subsequent section.

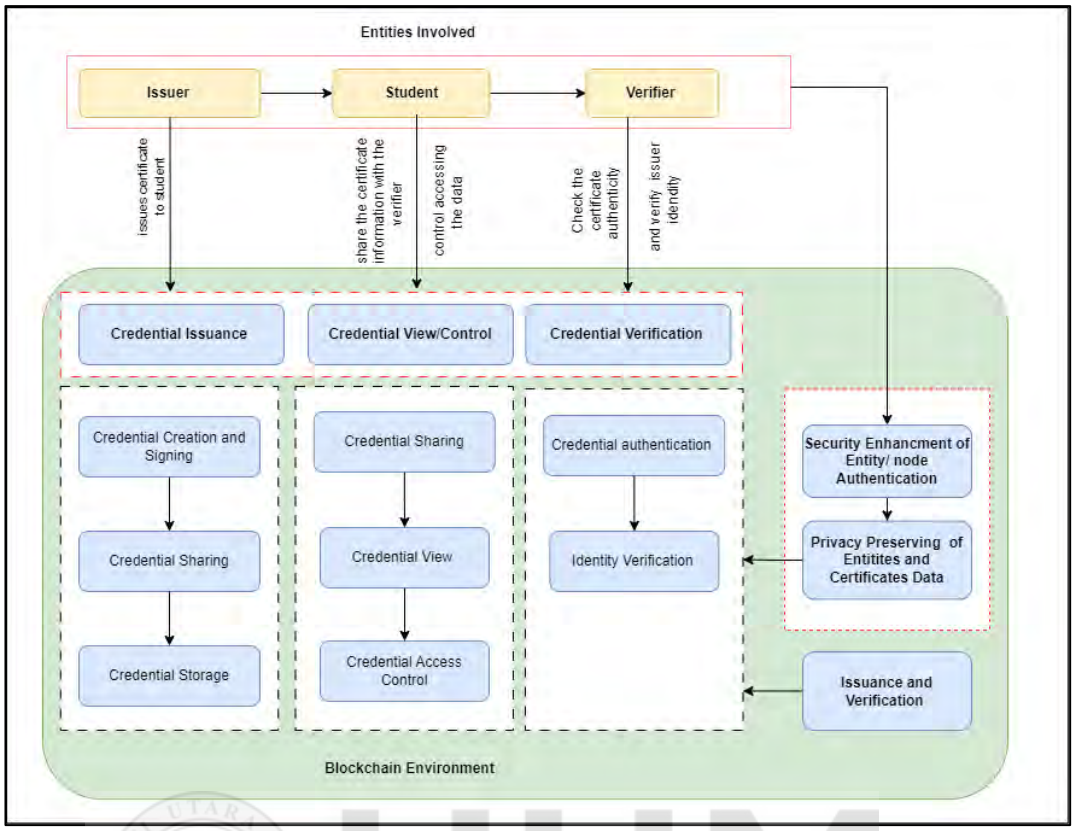

Figure 4.2 Initial Design of SecureBlockCert Framework

4.4 The Verified SecureBlockCert Framework: Enhancements in Security and Privacy

The verified SecureBlockCert framework, shown in Figure 4.3, enhances the initial design by incorporating several critical improvements aimed at bolstering security, privacy, and user engagement in digital credential management. Each enhancement is detailed below:

4.4.1 Stakeholder Roles and Responsibilities

The framework identifies three primary stakeholders: issuers, students, and verifiers. Each stakeholder has clearly defined roles, which enhances accountability and trust within the ecosystem.

a) **Issuer:** Typically an educational institution, the issuer is responsible for issuing digital certificates and ensuring their authenticity.

b) **Student:** Students manage their digital certificates and have the authority to decide what information to share with verifiers, empowering them with control over their credentials.

c) **Verifier:** This role, often filled by employers or other institutions, involves validating the credentials presented by students, allowing them to make informed decisions based on reliable information.

4.4.2 Public Key Infrastructure (PKI) Integration

The incorporation of PKI establishes a trusted Certificate Authority (CA) that validates the identities of nodes within the network. Each node must register with the CA to obtain a digital certificate, enhancing the trustworthiness of communications and transactions across the framework. This CA-based approach provides a structured method for establishing trust and mitigating the risks of impersonation and fraud.

4.4.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

The framework utilizes ECDSA for signing transactions and communications. ECDSA provides a high level of security with relatively small key sizes, improving efficiency and reducing computational overhead. This cryptographic technique helps ensure that only authorized entities can initiate transactions, thereby protecting against forgery and unauthorized access.

4.4.4 Blockchain-Specific Challenge-Response Protocol

The inclusion of a challenge-response protocol enhances ongoing node authentication. Nodes are periodically presented with cryptographic challenges that they must solve to prove their identity.

This mechanism ensures that even if a node's credentials are compromised, unauthorized access can be detected in real-time, maintaining the integrity of the network.

4.4.5 Advanced Cryptographic Techniques

a. **Asymmetric Cryptography Enhancements**

The use of public/private key pairs remains a cornerstone of the SecureBlockCert framework. Each participant generates a unique key pair, where the public key facilitates verification, and the private key is securely stored for signing transactions. This approach enhances authentication and secures communications between nodes while allowing for robust verification processes.

b. **Advanced Homomorphic Encryption Techniques**

To protect sensitive data within digital certificates, the framework incorporates an advanced homomorphic encryption algorithm. Unlike traditional methods that require decryption for data verification, homomorphic encryption allows computations to be performed on encrypted data without exposing the underlying information. This technique significantly enhances privacy and minimizes the risk of data exposure during verification processes.

4.4.6 Data Privacy Mechanism

The framework implements additional data privacy measures, ensuring that sensitive information within digital certificates remains encrypted throughout the verification process. By maintaining encryption during all interactions, the framework offers an added layer of protection, addressing concerns related to data breaches and unauthorized access.

4.4.7 Integration of Decentralized Identifiers (DIDs)

The incorporation of Decentralized Identifiers (DIDs) empowers users to manage their identities independently. Unlike traditional systems where identity management is centralized, DIDs allow users to control their personal data without relying on third-party entities. This feature enhances user autonomy and addresses privacy concerns associated with identity verification [88].

4.4.8 Verifiable Credentials (VCs) Implementation

The framework utilizes Verifiable Credentials (VCs), which are cryptographically signed by the issuer. VCs provide a tamper-evident proof of authenticity and integrity, ensuring that the credentials presented by students can be trusted by verifiers. This integration strengthens the overall certification process by fostering trust among stakeholders [89],[90].

4.4.9 Improved Issuance and Verification Processes

The issuance and verification processes are enhanced to create a more flexible and user-friendly system. By streamlining these processes, the framework improves the user experience for both students and verifiers, ensuring that digital credential management is efficient, secure, and accessible.

These comprehensive improvements collectively enhance the verified SecureBlockCert framework, reinforcing its security, privacy, and functionality. This advanced framework establishes a robust solution for managing digital credentials in a decentralized and secure manner, aligning with contemporary needs in digital identity and credential verification.

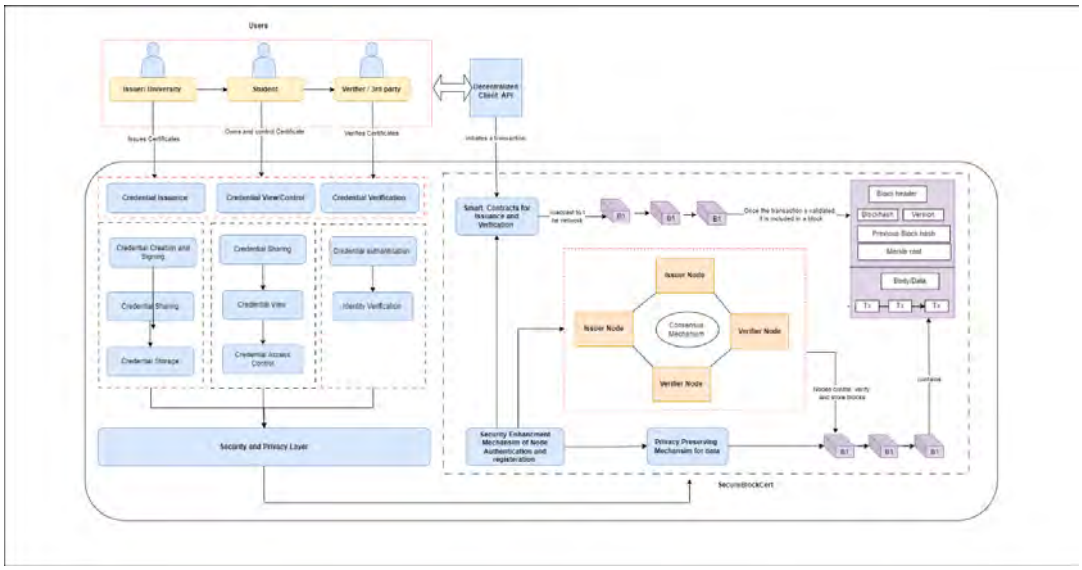

Figure 4.3 The Proposed Verified SecureBlockCert Framework

4.4.10 Security Enhancement Mechanism

In the SecureBlockCert framework, a secure and systematic mechanism is employed to generate cryptographic identities and enable confidential communication. This mechanism, outlined in Algorithm 1, ensures that every transaction and message exchanged within the network is private and verifiable. The steps in this process are designed to guarantee both the integrity and anonymity of peer-to-peer interactions, creating a tamper-resistant communication channel between peers. The detailed steps of the security enhancement component are shown in Figure 4.4.

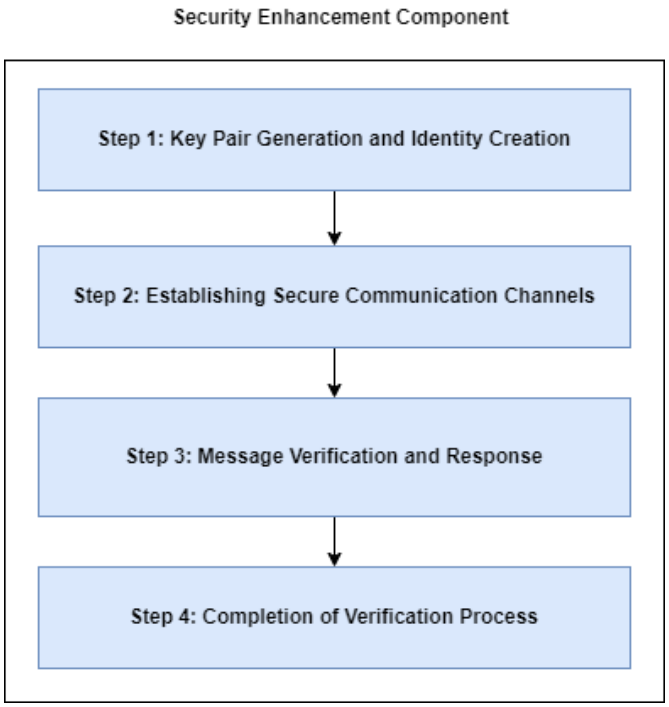

Figure 4.4 Steps in the Security Enhancement Component

Step 1: Key Pair Generation and Identity Creation

1.1 Peers generate key pairs using the Ed25519 cryptographic algorithm.

1.2 The Certificate Authority (CA) certifies the generated keys, which are stored in the peers' digital wallets.

1.3 A pseudo-identity for each peer is generated during the key creation process to enhance anonymity.

Step 2: Establishing Secure Communication Channels

2.1 Peers initiate a secure messaging channel for encrypted communication.

2.2 When a peer sends a message (Message 1), it is timestamped, and the potential time delay to reach the recipient is considered.

Step 3: Message Verification and Response

3.1 The receiving peer calculates the time delay and authenticates the signature of Message 1.

3.2 The receiving peer then sends back a signed response message (Message 2) with a new timestamp (Ti+1).

Step 4: Completion of Verification Process

4.1 The initial sender verifies the identity of the second peer by evaluating the time delay and signature on Message 2.

4.2 Both peers securely store the encrypted identities of each other in their digital wallets, laying the foundation for future secure interactions.

In blockchain-based credential systems, the secure registration and authentication of peers is essential to ensure that only verified entities can participate in the network. This is particularly important in the SecureBlockCert framework, where each peer must have a unique and protected identity to maintain privacy and security standards. The "Peer Information Registration and Authentication Algorithm" Algorithm (1) presented below outlines a step-by-step approach to achieving this goal by using pseudo-identities, encrypted communication, and mutual authentication protocols.

Algorithm (1) serves two main purposes: (1) it ensures that each peer is authenticated in a way that protects their privacy, and (2) it securely registers each peer, preventing unauthorized access or duplication. Through the use of nonces and timestamp-based message validation, the algorithm is designed to prevent replay attacks, ensuring that each authentication request is unique and cannot be maliciously repeated. Additionally, it aligns with Research Objective 1, which focuses on enhancing security measures in digital credential systems by developing a robust peer authentication protocol. The process begins with initializing essential components, including the Certification Authority (CA), peer identities, timestamps, and encryption functions.

The algorithm then checks for any existing registration, terminating if the peer is already registered to avoid redundancy.

For unregistered peers, a credential generation phase is conducted, assigning a pseudo-identity to each peer through the CA. This pseudo-identity serves as a unique identifier, enabling the peer to participate in the system securely.

Once credentials are generated, the authentication phase begins. Peers exchange authentication requests and responses in a time-sensitive manner, ensuring that only authorized entities can interact. Each peer calculates and verifies the time delay between message exchanges, which serves as an added security measure. Once authenticated, the peers securely store their identities, encrypted with private keys, to prevent unauthorized access.

Algorithm 1 below details the full peer registration and authentication process. The legend provided explains the symbols used, such as Pi for peers and CA for the Certification Authority, to clarify the notation within each step.

Legend:

- **Pi:** A peer in the network, denoted as Peer i.
- **CA:** Certification Authority responsible for certifying keys.
- **Ti:** A timestamp associated with Peer i's actions.
- **E(x):** The encryption of x using the framework's cryptographic methods.
- **PID(x):** The pseudo-identity generated for entity x to enhance anonymity.
- **ni:** A nonce associated with Peer i, used for ensuring the uniqueness of transactions.

Algorithm (1): Peer Information Registration and Authentication

Require: Peer information registration

Ensure: Authenticated peers with self-control on registration data

1. Initialize peers: Pi ← Peers
2. Initialize certification authority: CA ← Certification Authority
3. Initialize timestamps: Ti ← Time Stamps i
4. Define encryption function: E(x) ← Encryption of x
5. Define pseudo identity: PID(x) ← Pseudo Identity of x
6. Define nonce for each peer: ni ← Nonce for peer i
7. If Pi is already registered then
8. Process is terminated.
9. End If
10. Credential Generation
11. For i = 1 to Last Peer do
12. CA ← Pi(RegReq)
13. Pi ← CA(PID(Pi))
14. End For
15. Peer Authentication and Message Passing
16. Pi(PID(Pi)) ← AuthReq(Pj(PID(Pj)))
17. M1 = Pj(TiPID(Pj)) Signed(Pj), Ti
18. Pi ← M1
19. Pi calculates M2
20. M2 = Pi(T(i + 1)PID(Pi)) Signed(Pi), T(i + 1)
21. Pi compares time delay
22. δT = Ti - T(i + 1) for (M1, M2)
23. On verification of time delay, Pi accepts the public key of Pj and sends an acceptance message.
24. Store Identity in Registration
25. Store E(PIDi)PrivateKey(Pi) and Store E(PIDj)PrivateKey(Pj)

This algorithm provides a structured and secure approach to managing peer identities within a blockchain-based credentialing framework.

By ensuring the secure transmission and storage of authentication data, it mitigates risks of data tampering and unauthorized access. The pseudo-identities and encryption methods used are critical in upholding privacy standards and addressing the core challenges of digital credentialing in decentralized environments.

4.2.1 Privacy Preserving Enhancement

The privacy component of the SecureBlockCert Blockchain framework is designed to strengthen the security of digital certificates while preserving user privacy. The framework leverages a combination of advanced cryptographic techniques to ensure that only authorized entities can access sensitive data and that all verification processes protect user anonymity. The privacy preservation mechanisms are built on three key pillars: Homomorphic Encryption (HE), Access Control, and Hash Functions.

4.4.11.1 Privacy Preservation of Data and Transactions Using Homomorphic Encryption and Hashing

The protection of private information is a fundamental requirement in digital credentialing systems, especially in applications like SecureBlockCert where sensitive certificate data must be managed securely. Homomorphic encryption is employed to allow encrypted computations on data without requiring decryption, thereby preserving confidentiality. The "Homomorphic Encryption Algorithm" Algorithm (2) presented below is designed to apply fully homomorphic encryption (FHE) on certificate data, enabling secure, privacy-preserving operations on encrypted information. Algorithm (2) provides a method for securely handling certificate information by using homomorphic encryption to ensure that private information remains confidential throughout the transaction process.

The algorithm identifies private components within the certificate data and applies homomorphic encryption where needed, with final data securely uploaded to the blockchain as an encrypted hash. By integrating FHE, this approach ensures that computations on private data can occur without exposing the underlying information, aligning with Research Objective 2, which aims to enhance privacy preservation within the digital credential system.

The algorithm takes Certificate-Information as input and outputs a hashed, encrypted version of the data. If private information is detected within the data, fully homomorphic encryption is applied. Otherwise, the data is uploaded directly to the transaction layer. When private information is identified, a customized encryption process encrypts each component Di of the data, enabling secure operations without compromising privacy. During the homomorphic encryption process, a summation of encrypted data components is performed, ensuring that calculations on sensitive data do not reveal raw information. Additionally, if any part of the certificate information is numeric, further hashing and encryption are applied to maintain data confidentiality. The final output, a hash of the encrypted data, is uploaded to the blockchain, securing the information in an immutable and private form. Algorithm 2 below details the step-by-step procedure for applying homomorphic encryption to certificate data. Legends for each symbol used, such as E(x) for encryption and Hashfun for the hashing function, are provided to clarify notation.

Legend:

- **E(x):** The encryption of x using the framework's cryptographic methods.
- **Hashfunc(x):** The hashing function applied to x to ensure data integrity.
- **Di:** The component i of the certificate information.
- **FHE:** Fully Homomorphic Encryption, enabling computations on encrypted data.

Algorithm (2): Homomorphic Encryption Algorithm for Certificate Data Protection

Procedure: Homomorphic Encryption for Certificate Data

Input: Data(Certificate-Information)

Output: Hashfunc(E(Data(Certificate-Information)))

1. If private information is present then
   2. Check the Data(Certificate-Information)
   3. If Data(Certificate-Information) contains private information then
      4. Apply Fully Homomorphic Encryption (FHE)
   5. Else
      6. Upload data to transaction layer.
   7. End If
8. Else
   9. Apply FHE with monoalphabetic information
   10. For homomorphic encryption, use E(m1 + m2) = (E(m1) + E(m2) ∗ E(m2))
      11. For Data(Certificate-Information) represented as D1 + D2 + ... + Dn
         12. For i > 0
            13. Calculate E(Data) = ∑_(i=1)^n (E(Di) + E(D(i+1)) * E(D(i+1)))
            14. If Di is numeric then
               15. For i = j to m
                  16. Calculate E(Data_numeric) = Hashfunc(∑_(i=j)^m (E(Di) + E(D(i+1)) * E(D(i+1)))
               17. End For
            18. End If
         19. End For
20. End If
21. Upload the hashed encrypted data using Hashfunc(E(Data)).

This algorithm ensures that certificate data is encrypted and hashed before being stored, preventing unauthorized access while allowing operations on the data through fully homomorphic encryption.

By securing data at the component level and ensuring that any numeric values are doubly protected, this process guarantees confidentiality for sensitive information. This approach is critical in decentralized credentialing systems like SecureBlockCert, where privacy-preserving mechanisms must be maintained even as data is processed for issuance or verification.

4.4.11.2 Enhanced Access Control

Access control is implemented using attribute-based encryption (ABE) to create a role-based data access system [91]. In cases where information sensitivity varies across different user groups (e.g., administrative staff and external verifiers), Role-Based Information Release is employed.This mechanism ensures that only authorized users can retrieve necessary data, which is particularly important during legitimate verification processes or audits.

4.4.11.3 Hash Function for Data Integrity

A robust cryptographic hash function guarantees the system's data integrity by ensuring that any tampering is detectable. Binding and blinding techniques are applied to protect encrypted certificates, allowing them to be validated without revealing their contents. This ensures privacy is upheld and data is only unveiled when absolutely necessary.

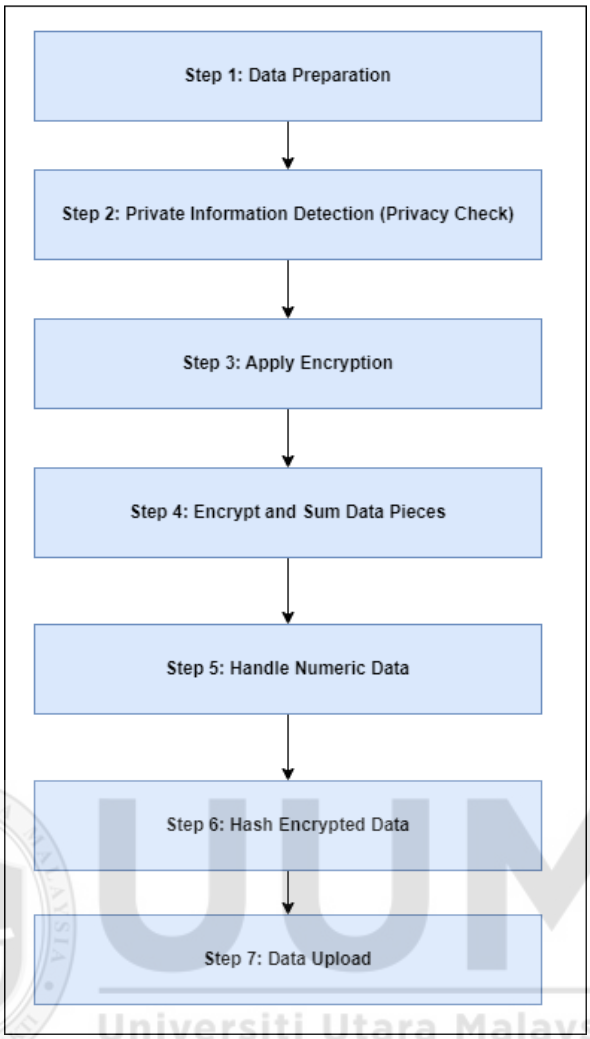

Figure 4.5 Steps in the Privacy Preserving Enhancement Component

This process guarantees that any portion of certificate information deemed private is encrypted using Fully Homomorphic Encryption (FHE) and hashed before being uploaded to the blockchain [92],[93]. The steps outlined ensure that sensitive data remains confidential while allowing computations to be performed on encrypted data.

4.4.11.4 Decentralized Certificate Verification and Credential Privacy (DCVPC) Protocol

The Decentralized Certificate Verification and Credential Privacy (DCVPC) Protocol is designed to securely manage and authenticate interactions between ministries, universities, and students in a blockchain-based credentialing framework. This

protocol, henceforth referred to as the DCVPC Protocol, outlines the process for creating a structured, decentralized ledger where credentials can be issued, verified, and managed with privacy-preserving measures.

The DCVPC Protocol defines clear relationships between entities, establishing a secure pathway from ministries to universities and, ultimately, to students. By leveraging decentralized peers and controlled data-sharing mechanisms, the protocol enhances the privacy and security of credentials. The implementation of the DCVPC Protocol is formalized through Algorithm (3): Ministry, University, and Student Interaction Framework, which details the hierarchical structure and interactions within this credential management framework. This algorithm provides a step-by-step approach for managing credentialing interactions in alignment with the DCVPC Protocol.

This protocol adopts a channel-based architecture that facilitates the creation of private domains for universities, enabling secure sharing of information. Only verified institutions and ministries can access the network, preventing unauthorized organizations from participating. The protocol ensures that nodes (e.g., universities) are acquainted with one another, promoting secure cooperation while minimizing the attack surface.

The DCVPC Protocol dictates a system where credentials are issued and verified with integrity. It regulates node admission, access controls, and secure communication while enabling a permissioned blockchain model. This ensures a trusted environment for managing academic credentials.

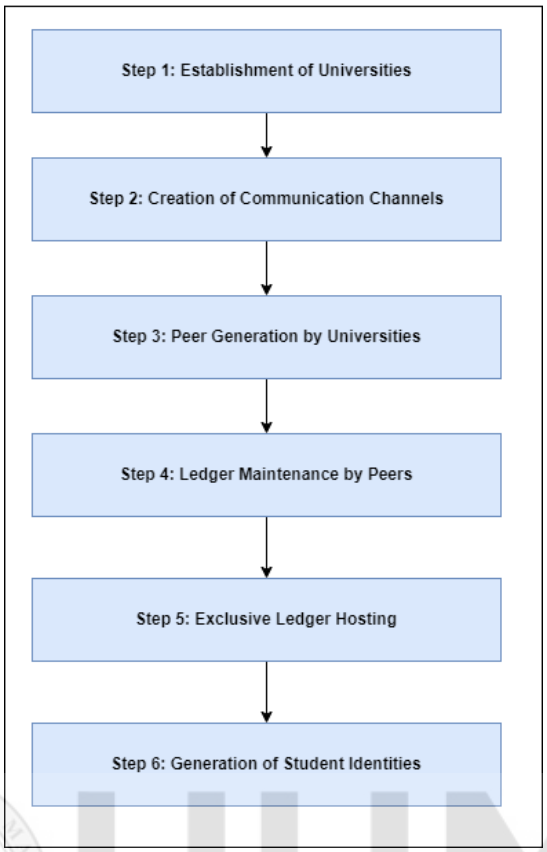

Figure 4.6 Steps for Securing and Preserving Identity Privacy within the Hyperledger Fabric Blockchain using the DCVPC Protocol

The DCVPC Protocol is designed to enable secure and privacy-focused verification of academic credentials within higher education. This protocol leverages decentralized processes, controlled access, and strong identity management to protect sensitive student data. Below are the key steps in the DCVPC Protocol for managing digital credentials.

a) **Ministry Authority Setup**: The ministry, as the primary governing authority, establishes organizational entities for each university within the network. This setup forms the foundation for a decentralized credential management system.

b) **Channel Establishment**: Each ministry creates a dedicated channel to connect universities, overseeing authentication across the network to ensure secure, authorized communication between institutions.

c) **University Peer Network Configuration:** Each university, functioning as an independent organization, configures and maintains its own network peers. This decentralized peer setup supports secure data handling and transaction validation without relying on a central administrator.

d) **Ledger Maintenance and Transaction Validation:** Peers within each organization maintain a local copy of the ledger, validating transactions before adding them to the distributed ledger. This approach enhances trust in the network by ensuring that only verified transactions are committed.

e) **Restricted Ledger Hosting:** Only universities are authorized to host the ledger, which restricts access to trusted academic entities and safeguards the integrity of sensitive credential data.

f) **Student Identity Generation:** Each university organization generates unique digital identities for students, enabling secure, individualized credential issuance and preventing unauthorized access or identity impersonation.

g) **Exclusive Certification Authority:** Each university's administrative entity is the only authority permitted to issue digital certificates. This exclusive control reduces the risk of unauthorized credential issuance.

h) **Certificate Hashing and Student Control:** Once issued, certificates are hashed, with control over each hashed certificate retained by the student. This process ensures data integrity and enables students to maintain ownership of their academic records.

i) **Student Access and Sharing:** Students are given secure access to their certificates, allowing them to view and share these credentials with third parties as needed. This step supports user autonomy and privacy.

j) **Third-Party Validation:** Third parties, such as employers or other institutions, need only the certificate ID to validate and authenticate credentials, ensuring a streamlined, privacy-preserving verification process.

k) **Controlled Authentication by Students:** Certificates can only be authenticated when explicitly shared by the student, ensuring that students control access to their credentials, thus upholding privacy throughout the verification process.

In a decentralized credentialing system, defining and managing roles and relationships among ministries, universities, and students is critical. This section presents an algorithm that establishes these hierarchical interactions, ensuring that credential data is managed securely and efficiently. The algorithm facilitates structured communication and data sharing, allowing ministries to oversee universities and universities to manage student identities and credentials. This approach aligns with the framework's goals of decentralized, privacy-preserving credential management.

Legend:

- **MinistryN:** Represents each ministry within a list of countries.
- **N:** The set of all ministries in the system.
- **n(Ministry) = x:** The constant number **x** of universities associated with each ministry.
- **University_i:** The ith university associated with a ministry.
- **ChannelM:** The communication channel assigned to each ministry.
- **M:** The ministry overseeing a set of universities.
- **Peer_i:** The unique peer assigned to each university for decentralized interaction.
- **Ledger {Peer_0, ..., Peer_i}:** The distributed ledger containing all peers in the system.

- **Universityadmin:** The administrator responsible for managing student identities and certificates.
- **Identity_s:** The unique identity assigned to each student.
- **Certificate_s:** The certificate issued to each student.
- **Students ⊆ s:** The set of all students in the system.
- **→:** Symbol representing an action or responsibility.
- **∈:** Symbol denoting set membership

Algorithm (3): Ministry, University, and Student Interaction Framework

Procedure: Ministry, University, and Student Interaction Framework

1. Define Ministries and Universities:
   - Let N be the set of ministries in a list of countries.
   - For each MinistryN ∈ N, define n(Ministry) = x.
   - Assign each MinistryN a set of universities { University1, University2, ..., Universityi }, where i > 0.
2. Establish Communication Channels:
   - Define a communication channel ChannelM for each MinistryN.
   - Each university UniversityMi communicates through ChannelM, governed by M = MinistryN.
3. Assign University Peers:
   - For each university UniversityMi, assign a unique peer Peer_i.
   - Define the ledger as { Peer_0, ..., Peer_i }.
4. Manage Identities and Certificates:
   - University administrators manage identities Identity_s and certificates Certificate_s for students s ∈ Students.
5. Enable Student Data Access:
   - Allow each student s ∈ Students to share or view their certificates.

4.5 Issuance and Verification Process in the SecureBlockCert Framework

The SecureBlockCert framework leverages blockchain technology, smart contracts, Decentralized Identifiers (DID), and Verifiable Credentials (VC) to ensure secure,

private, and efficient credential issuance and verification. This section explores the key components and steps involved in this process.

4.5.1 Overview of the Issuance and Verification Process

The issuance and verification process in the SecureBlockCert framework provides a structured approach to managing academic credentials. By implementing decentralized technologies, it ensures that credentials are issued, stored, and verified with minimal reliance on intermediaries. This setup enhances security, privacy, and user autonomy in handling academic records.

4.5.2 Role of Smart Contracts in Credential Issuance and Verification

Smart contracts are integral to the framework, automating and enforcing the rules for credential issuance and verification [94]. Within SecureBlockCert, smart contracts manage the entire lifecycle of a credential from creation by authorized universities to verification requests by third parties. This automation reduces administrative overhead, ensures integrity, and provides transparency throughout the process.

The SecureBlockCert framework leverages five essential smart contracts to manage the lifecycle of digital credentials securely and effectively. Each smart contract is designed to fulfill a unique role, ensuring the integrity, authenticity, and privacy of academic credentials within the blockchain network. These contracts are fundamental to the framework's operations, providing decentralized, automated management of credential issuance, sharing, and verification.

4.5.2.1 Add Authority Contract

This smart contract establishes trusted governing entities, such as government bodies or educational accreditation boards, within the SecureBlockCert network. Authorities created through this contract are responsible for overseeing the subordinate institutions

within the network, maintaining the overall credibility and integrity of the system. By assigning administrative powers to these authorities, the contract ensures that only recognized, reputable entities have influence over the credentialing ecosystem.

4.5.2.2 Add University Contract

The Add University contract allows verified authorities to integrate educational institutions into the blockchain network. This process ensures that only accredited universities can participate in the credential issuance process, maintaining the trustworthiness and quality standards of the digital credentialing system. By permitting only authorized institutions to issue credentials, the contract upholds a high level of reliability within the network.

4.5.2.3 Issue Certificate Contract

Central to the framework, the Issue Certificate contract manages the creation of verifiable digital credentials. This contract automates the issuance process, ensuring that every certificate generated is accurate, authentic, and cryptographically signed by the issuing authority. The issued credential is then securely stored on the blockchain, enabling it to be verified by any third-party stakeholders while safeguarding its integrity and authenticity.

4.5.2.4 Share Certificate Contract

The Share Certificate contract grants students control over their digital credentials, allowing them to selectively share their achievements with employers, educational institutions, or other stakeholders. By providing a secure and controlled mechanism for credential dissemination, this contract upholds student privacy while ensuring that shared records remain verifiable and tamper-proof. It empowers students to manage and share their academic records autonomously and securely.

4.5.2.5 Verify Certificate Contract

Designed for external stakeholders, the Verify Certificate contract facilitates the authentication of digital credentials presented by students. Employers, educational institutions, and accreditation bodies can use this contract to confirm the legitimacy of credentials within the network efficiently. The verification process is streamlined and precise, reinforcing trust in the digital credentials and ensuring their authenticity without compromising student privacy.

In SecureBlockCert, each smart contract corresponds to a critical function for decentralized digital credential management. The algorithms presented above detail the logical structure and flow of these smart contracts, outlining how each function supports the creation, management, and verification of digital certificates while ensuring security, privacy, and user control. Each smart contract is crafted to address specific aspects of the credential lifecycle:

a) **Adding the Authority Member**

The function "addAuthorityMember" is designed to facilitate the addition of a new authority member to the system given in algorithm 4. It takes several parameters as input, including the authority member's identifier DaDa, unique identifier IDaIDa, additional details ββ, and status. The function begins by identifying the transaction initiator TeTe, ensuring that the initiator holds the status of an authority member within the system. Following this verification, the system checks whether the authority member with the specified identifier IDaIDa already exists. If the authority member does not exist, a new authority entity AA is created. This new authority is assigned the provided identifier, with the transaction initiator designated as its issuer. The status and additional details provided for the authority member are also assigned to the newly created entity. Once all details are set, the new authority entity AA is stored in the

system's authority registry under the identifier IDaIDa. Finally, the function returns the newly created authority entity AA as confirmation of the successful addition. If the specified authority member already exists in the system, the function returns a failure indication.

Algorithm (4): Add New Authority Member

```
1: function addAuthorityMember(Da, IDa, β, status)
2: Te ← Transaction initiator
3: Require that Te is an Authority member
4: if AuthorityNotExist(IDa) then
5: A ← newAuthority()
6: A.id ← IDa
7: A.issuer ← Te
8: A.status ← status
9: A.details ← β
10: Πa[IDa] ← A
11: return A
12: end if
13: return failure
14: end function
```


b) **Adding New University**

The function "CreateUniversity" serves the purpose of adding a new university entity to the system given in algorithm 5. It takes several parameters as input, including the university's name DuDu, unique identifier IDuIDu, additional details $\beta\beta$, and status. Similar to the previous algorithm, the function starts by identifying the transaction initiator TeTe, ensuring that the initiator holds the status of an authority member within the system. Following this verification, the system checks whether the university with the specified identifier IDuIDu already exists. If the university does not exist, a new university entity UU is created. This new university is assigned the provided identifier,

with the transaction initiator designated as its issuer. The status and additional details provided for the university are also assigned to the newly created entity. Once all details are set, the new university entity UU is stored in the system's university registry under the identifier IDuIDu. Finally, the function returns the newly created university entity UU as confirmation of the successful addition. If the specified university already exists in the system, the function returns a failure indication.

Algorithm (5): Add New University

```
1: function CreateUniversity(Du, IDu, β, status)
2: Te ← Transaction initiator
3: Require that Te is an Authority member
4: if UniversityNotExist(IDu) then
5: U ← newUniversity()
6: U.id ← IDu
7: U.issuer ← Te
8: U.status ← status
9: U.details ← β
10: Πu[IDu] ← U
11: return U
12: end if
13: return failure
14: end function
```


c) **Add New Certificate**

The function "CreateCertificate" is designed to facilitate the creation of a new certificate within the system given in algorithm 6. It takes several parameters as input, including the university's identifier $DuDu$, unique identifier $IDuIDu$, certificate identifier $IDsIDs$, additional details $\beta\beta$, and status. Similar to the previous algorithms, the function begins by identifying the transaction initiator $TeTe$ and ensuring that the initiator holds the status of a university administrator within the system. Following this

verification, the system checks whether the certificate with the specified identifier $IDaIDa$ already exists. If the certificate does not exist, a new certificate entity CC is created. This new certificate is assigned the provided identifiers, with the transaction initiator designated as the entity responsible for the file hash $C.fileHashC.fileHash$, student $C.studentC.student$, and issuer $C.issuerC.issuer$. The status and additional details provided for the certificate are also assigned to the newly created entity. Once all details are set, the new certificate entity CC is stored in the system's certificate registry under the identifier $IDcIDc$. Finally, the function returns the newly created certificate entity CC as confirmation of the successful addition. If the specified certificate already exists in the system, the function returns a failure indication.

Algorithm (6): Add new Certificate

```
1: function CreateCertificate(Du, IDu, , IDs, β, status)
2: Te ← Transaction initiator
3: Require that Te is an university admin
4: if certificateNotExist(IDa) then
5: C ← newCertif icate()
6: C.f ileHash ← Te
7: C.student ← Te
8: C.issuer ← α
9: C.status ← status
10: C.details ← β
11: Πc[IDc] ← C
12: return C
13: end if
14: return failure
15: end function
```

d) **Share Certificate**

The "ShareCertificate" function facilitates the sharing of a certificate with a verifier given in algorithm 7. It takes two parameters as input: the identifier of the certificate

to be shared $IDcert$IDcert and the identifier of the verifier IDvIDv. Similar to previous algorithms, the function starts by identifying the transaction initiator TeTe and verifying that the initiator is a student within the system. If the initiator is confirmed as the holder of the certificate specified by $IDcert$IDcert, the function proceeds to retrieve the certificate entity CC associated with the provided identifier $IDcert$IDcert. Subsequently, the verifier's identifier IDvIDv is added to the list of entities with whom the certificate is shared ($C.shareWithList$C.shareWithList). If the update of the certificate with the new shared status is successful, the function returns the updated certificate entity CC as confirmation of the successful sharing process. If any of the initial conditions are not met (such as the initiator not being the certificate holder or the certificate not existing), the function returns a failure indication.

Algorithm (7): Share Certificate

```
1: function ShareCertificate(IDcert, IDv)
2: Te ← Transaction initiator
3: Require that Te is an Student
4: if isCertificateHolderStudent(Te, IDcert) then
5: C ← GetCertif icate(IDcert)
6: C.shareWithList.P ushV erif ier(IDv)
7: if UpdateCertificate(C) then
8: return C
9: end if
10: end if
11: return failure
12: end function
```

e) **Verify Certificate**

The "VerifyCertificate" function is responsible for verifying the authenticity and validity of a certificate given in algorithm 8. It takes one parameter as input: the

identifier of the certificate to be verified, denoted as $IDcertIDcert$. The function begins by identifying the transaction initiator, represented by $TeTe$, and ensuring that the initiator is a member of the network authorized to perform certificate verification. Upon verification of the initiator's network membership, the function proceeds to retrieve the certificate entity associated with the provided identifier $IDcertIDcert$, denoted as cc.

Following this, the function checks if the transaction initiator is included in the list of entities with whom the certificate is shared, denoted as $c.shareWithListc.shareWithList$. If the initiator is found in the list of authorized verifiers, the function returns the certificate entity cc, confirming the successful verification process. However, if the initiator is not authorized to verify the certificate or if the certificate does not exist, the function returns a failure indication.

Algorithm (8): Verify Certificate

```
1: function VerifyCertificate(IDcert)
2: The ← Transactioninitiator
3: Require that Te is a member of the network
4: c ← GetCertificate (IDcert)
5: if c.shareWithList.IsExist(Te) then
6: return c
7: end if
8: return failure
9: end function
```

In the context of the smart contract descriptions, Table 4.1, Notations Used in Smart Contract Development, provides a comprehensive reference for the specific notations used throughout the algorithms. Each notation represents a key element, entity, or parameter involved in the smart contract operations, enabling a clearer understanding of the contract logic and flow. This table serves as a quick reference guide for

interpreting the roles and identifiers in the smart contract algorithms, ensuring consistent terminology across the explanations of each contract's function and process.

Table 4. 1 Notations Used In Smart Contract Development

Notation	Description
T_e	Transaction initiator
A	Authority
U	University
S Student	Student
C	Certificate
V	Verifier
ID_a	Authority identity
ID_u	University identity
ID_s	Student identity
ID_{cert}	Unique certificate id
ID_v	Verifier identity
Π_u	University list
Π_a	Authority member list
Π_c	Certificate list
λ	Certificate hash
D_{course}	Course details
D_{cert}	Certificate details
β	Other Details

4.5.3 Implementation of Decentralized Identifiers (DID) and Verifiable Credentials (VC)

The SecureBlockCert framework integrates Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) to reinforce security, privacy, and self-sovereignty in digital credential management.

4.5.3.1 Decentralized Identifiers (DIDs)

DIDs provide a decentralized mechanism for individuals to generate unique identifiers under their control, bypassing reliance on centralized authorities and mitigating risks of unauthorized access to personal data. Each DID is globally unique and coupled with a DID document, which contains essential metadata and cryptographic keys needed for secure exchanges, ensuring user-centric control.

4.5.3.2 Verifiable Credentials (VCs)

Verifiable Credentials (VCs) serve as tamper-evident digital attestations of an individual's qualifications or attributes. Within SecureBlockCert, VCs complement DIDs by verifying the authenticity and integrity of credentials, thus facilitating efficient, privacy-preserving verification. Together, DIDs and VCs form a cohesive digital identity framework, which upholds the privacy, security, and self-management goals of SecureBlockCert.

The implementation of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) in the SecureBlockCert framework utilizes the Ed25519 cryptographic signature scheme, ensuring robust security for identity verification and credential issuance.

4.5.3.3 Steps for Issuing Credentials

The credential issuance process in SecureBlockCert involves several steps, facilitated by smart contracts, DID, and VC:

a) **Student Registration:** Students are registered with a DID, which uniquely identifies them within the system.

b) **Credential Request:** The university generates a credential request, which is processed by the smart contract to ensure all required conditions are met.

c) **Credential Creation and Signing:** The credential is created as a Verifiable Credential (VC) and cryptographically signed by the issuing authority.

d) **Storage in Blockchain:** The credential is securely stored in the blockchain ledger, ensuring tamper-resistant records.

e) **Student Access**: The student is granted access to their credential, allowing them to share it with verifiers as needed.

4.5.3.4 Steps for Verifying Credentials

Verification in SecureBlockCert is a privacy-preserving process that upholds the integrity of shared credentials:

a) **Verifier Credential Request:** A third-party verifier submits a credential request to the student.

b) **Student Consent and Sharing:** The student provides consent by sharing a secure link or access to the credential.

c) **Smart Contract Authentication:** The smart contract authenticates the request, ensuring the verifier is authorized.

d) **Verification of VC:** The verifier checks the VC's digital signature and DID to confirm authenticity without accessing sensitive data.

e) **Result Delivery:** The verifier receives a validation response, confirming the credential's authenticity while protecting student privacy.

4.5.3.5 Security and Privacy Considerations

The SecureBlockCert framework prioritizes security and privacy throughout the issuance and verification process:

a) Data Integrity: Hashing and cryptographic signatures ensure that credentials cannot be tampered with.

b) User Privacy: By leveraging homomorphic encryption and selective disclosure, SecureBlockCert allows students to share only necessary credential details with verifiers.

c) Access Control: Smart contracts enforce role-based access, ensuring that only authorized entities can issue or verify credentials.

This research provides an example of a DID document designed for a specific use case, illustrated in Listing 1 and encoded in JSON-LD format. The DID document is uniquely identifiable by its "id: issuerID" property, which in this case is set to "1KoR4pzD59gfD2eUPvFp91KxCFy638EWhS" on line 3. Lines 2-3 define the DID method type, issuer identifier, and issuance timestamp. The subsequent lines, 4-9, describe the public key and its corresponding identifier, verification type, and key-value in multiple bases. Lines 10-20 specify the claims regarding the DID holder, including personal information and affiliations. The authentication method is defined in lines 25-28, outlining the method type, public key, and signature value. Lastly, lines 29-42 specify the proof method, which determines the verification type, creation timestamp, creator, verification method, and signature value used to sign the DID document. The example showcases how a DID document can be structured to include identifying information, personal information, and proof of authenticity. The JSON-LD format enables machine-readability and interoperability with other systems that use semantic web technologies.

1. {"context": "https://www.w3.org/ns/did/v1",
2. "issuer": {
3. "issuerID": "1KoR4pzD59gfD2eUPvFp91KxCFy638EWhS",
4. "publicKey": {
5. "type": "Ed25519VerificationKey",

```
"value":
"9d45579de90a05d9a91cabab4cd379b1c2ac3cf7771fd9555ae87eadc48a0
a81"
},
"issuanceDate": "2021-03-01 18:37:19"
},
"student": {
"studentID": "1BoBiew5dkyZmAJF5XQApHBrHfrkyCocJw",
"fullName": "Omar Saad Saleh",
"email": "omar@malayisa.ac.my",
"profileURL": [
"https://bob.org",
"https://linkedin.com/bob"
],
"affiliation": {
"institutionID": "1KUTTG5QSWjXydwyE4w1LP2nET8hvNnMs1",
"institution name": "Universiti of Utara Malaysia",
"department": "Department of Computer Science & Engineering",
"classRoll": "M2019200"
},
"personalInfo": {
"type": "Ed25519Encryption",
"phone": "############",
"address":
"############################################################"
},
"publicKey": {
"type": "Ed25519VerificationKey",
"value":
"75bfab0b5a43a1ab46370b97d49da713eaee19636c2ff847fe62efa81a6dd2
85"
}
},
"authentication": {
```

35. "type": "EdDSA",
36. "signature":
    "8b83c71c8c5a874e29bef72562d5a8d81b58cf8bceed97e04963bad3f37279dd5d0aed29de8f700b9fd86381eef961a3bcba9bc0770de484a37e311e4ae01b03"
37. },
38. "proof": {
39. "type": "EdDSA",
40. "signature":
    "0da7682f66822cf63c135f54241feed452b0abce2e4256b32a70f738df42bef1af0e762ead2df066fe258d31e12f366f97a5b5fcdb16f12198e5ac063bd98d09"
41. }
42. }

Listing 1. Design of a DID document schema in JSON-LD 1 format.

The design of DID in listing 1 is a JSON object containing a Digital Identity (DID) document for a student named Omar Saad Saleh. The document contains information about Omar, his institution, and his public key for authentication. Line 1 indicates that the document conforms to the W3C DID standard [95]. Lines 2-8 contain information about the issuer of the DID document, including the issuer's ID, public key, and issuance date. Lines 10-33 contain information about the student, including his ID, full name, email, profile URLs, affiliation with an institution, personal information such as phone number and address, and public key for verification. Lines 34-37 contain information about the authentication method used, including the type of authentication (EdDSA) and the signature generated using that method. Lines 38-41 contain information about the proof of the document, including the type of proof (EdDSA) and the signature generated using that method. This DID document provides a way to authenticate and verify Omar's identity using his public key and the authentication and proof signatures included in the document.

Listing 1 provides an example of a decentralized identifier (DID). Unlike a verifiable credential (VC), a DID consists of two signatures: one from the student and another from the issuer. To generate a DID, a student first obtains a JSON format DID form from their issuer. The student then fills out the form, generates a signature by signing their input information with their private key, and sends the form back to the issuer. Using the EdDSA scheme, the issuer verifies the student's signature using their public key. If the signature is valid, it confirms that the student authorized the information in the claim and ensures the data integrity of the student's information. Next, the issuer signs everything in the JSON file, except for the proof that contains the issuer's signature. If the signature is verified using the issuer's public key, it confirms that the claim was investigated and authenticated by the issuer and ensures the data integrity of the entire claim. In our case, the university controls the private key to prove ownership, and if the identifier and data are retrieved from other blockchains, the user can trust the data, identifier, and controller because of our operations. We verify and create the identity of the controller through a certificate authority (CA), only allowing authorized controllers to sign their data, and provide digital trails for all operations with a digital signature from the person performing the transaction.

Designing a verifiable credential (VC) schema in JSON-LD format involves utilizing the W3C Verifiable Credentials Data Model (VC Data Model) and the JSON-LD context [95]. The VC Data Model outlines the essential structure of a VC, which includes the subject, issuer, and claims. Meanwhile, the JSON-LD context maps the VC Data Model properties to JSON keys. A VC schema usually comprises several technical components, including:

a) @context: This field establishes the correlation between the terms employed in the document and their corresponding definitions.

b) id: This field specifies a unique identifier for the schema, such as a URL or URI.

c) type: This field defines the type of object described by the schema, like "VerifiableCredential" or "VerifiablePresentation."

d) issuer: This field identifies the entity or organization that issued the VC.

e) credentialSubject: This field describes the entity to whom the VC is issued, including relevant properties or characteristics.

f) proof: This field describes the cryptographic proof utilized to verify the authenticity and integrity of the VC, such as a digital signature.

g) claim: This field contains specific assertions or statements made by the issuer about the credential subject, such as their name, age, or qualifications.

h) Additionally, depending on the use case and other requirements, the schema may include other fields like expirationDate, credentialStatus, and revocation.

i) Moreover, it is worth noting that JSON-LD allows the utilization of reversed property, thereby offering flexibility in the structure for VC.

A verifiable claim pertains to a qualification, accomplishment, assertion, or fact regarding an entity that can be supported, such as a person's identification, education, or learning success [96]. A verified claim refers to a statement made by a third party affirming that the claim is factual. Claims often describe an entity's features that guarantee its singular existence, such as its name, amount, quality, and other details. However, a person, group, agency, or piece of equipment is limited in the kind of claims they can make. For instance, a student can assert that they earned a degree from a reputable institution, while an employer can assert that they have access to educational data for evaluating employment applications. The following is a JSON-LD verifiable credential schema for a certificate issued to a student by a university:

```
{
"@context": "https://www.w3.org/ns/did/v1",
"issuer": {
"issuerID": "1KUTTG5QSWjXydwyE4w1LP2nET8hvNnMs1",
"publicKey": {
"type": "Ed25519VerificationKey",
"value":
"a76f23be037469be7f6af21c4fcd25f0ae78407dc5c27835e2240adfdc906833"
},
"issuanceDate": "2022-12-11 18:37:19"
},
"subject": {
"certificateID": "7BCD-8D4C-9G3K-A62N",
"studentID": "1BoBiew5dkyZmAJF5XQApHBrHfrkyCocJw",
"fullName": "Omar Saad Saleh",
"degree": "MSc in Computer Science & Engineering",
"institutionName": "University Utara Malaysia",
"department": "Department of Computer Science & Engineering",
"roll": "M2019200",
"score": "4.48/4.50"
},
"proof": {
"type": "EdDSA",
"signature":
"cd3f919a2c9b15933c0c3ed33af4f1d2c8a4483f6c7eb8978f53e1ca63841aeab
b3ba968c1f7f98d83a52de700a9eb1c285343d377243302a24051e79466910e"
}
}
```

Listing 2**:** Example of JSON-LD verifiable credential schema for a certificate issued to a student by a university

This schema includes several key components:

a) The @context field defines the context of the JSON-LD document, which establishes the mapping between the terms used in the document and their corresponding definitions. In this case, the context is defined as the W3C DID specification.
b) The 'issuer' field identifies the entity or organization that issued the verifiable credential. It includes the issuer's unique identifier, public key, and issuance date.
c) The 'subject' field describes the entity to whom the verifiable credential is issued, including their personal information and relevant qualifications. In this case, it includes the certificate ID, student ID, full name, degree, institution name, department, roll, and score of the student.
d) The 'proof' field describes the cryptographic proof used to verify the authenticity and integrity of the verifiable credential. It includes the type of signature algorithm used and the signature value.

This schema follows the W3C Verifiable Credentials Data Model and uses the JSON-LD context to map the properties of the data model to JSON keys. It includes all the necessary fields to provide a comprehensive description of the verifiable credential, including the issuer, subject, and proof.

4.5.3.6 Cryptographic Implementation using Ed25519

The implementation of DIDs and VCs in SecureBlockCert employs Ed25519, an elliptic curve-based digital signature algorithm known for its security and efficiency. Ed25519 enables strong identity verification and credential issuance, making it suitable for blockchain systems. The generation of DIDs and VCs using Ed25519 follows these steps:

a) **Generating a Key Pair**: The user generates a unique Ed25519 key pair—consisting of a private key for signing and a public key for verification.

b) **Creating a DID**: The public key, prefixed with "did:example:", forms a unique identifier within the system.

c) **Creating a DID Document**: The DID document includes the DID, the public key, and other metadata. To demonstrate control, the individual signs this document using their private key.

To construct a VC with Ed25519:

a) **VC Creation**: The issuer, such as a university, generates a JSON-LD document with information about the individual's qualifications, such as name and degree.

b) **Signing the VC**: The issuer signs the VC with their Ed25519 private key, creating a verifiable signature that any party can check using the corresponding public key.

c) **Storing the VC**: The signed VC is then stored on the blockchain, making it accessible for verification by authorized verifiers.

By employing Ed25519, SecureBlockCert ensures authenticity, tamper-proofing, and public verifiability for DIDs and VCs, aligning with the W3C Verifiable Credentials Data Model and Decentralized Identifiers (DIDs) specifications.

4.5.3.7 Mathematical Basis of Ed25519

Ed25519 works on Edwards25519, which is a twisted version of the Edwards curve [97] . Equation (1) expresses the twisted Edwards curve over a prime field :

$$ax^2 + y^2 = 1 + dx^2y^2 \quad (4.1)$$

The curve used in this context is known as the Edwards curve, and it is of the untwisted variety. The twisted Edwards curve is a more general form of the Edwards curve.

When specific values of a and d are used, the resulting curve is known as Edwards25519, which can be represented mathematically as follows:

$$-x^2 + y^2 = 1 + dx^2y^2 \quad (4.2)$$

A public key can be created through elliptic curve point multiplication (ECPM), which involves multiplying a secret key by a base point, as expressed in equation (2). This base point is multiplied with the secret key to generate the public key. It is worth noting that ECPM is a standard technique used to generate public keys in elliptic curve cryptography (Islam et al., 2019) and can be defined as follows:

$$P_k = S_k P \quad (4.3)$$

Here, is a point on (2) and can be obtained by adding to itself times, such that (Bernstein et al., 2007):

$$P_k = \underbrace{P + P + \ldots + P}_{S_k - 1 \text{ times}} \quad (4.4)$$

If S_k can be represented as a power of two, P_k can be computed by doubling P on itself times, such that [3]:

$$P_k = \underbrace{\ldots 2(2(2(P)))}_{log_2 S_k \text{ times}} \quad (4.5)$$

The EdDSA (Edwards-Curve Digital Signature Algorithm) is a cryptographic signature scheme designed for secure and efficient message authentication. Algorithm 9 described below generates a digital signature using elliptic curve parameters and a private key. The EdDSA signature generation process is efficient and secure, making it suitable for applications requiring high levels of integrity and non-repudiation. This section details the steps involved in generating an EdDSA signature, using SHA-256 for hashing and elliptic curve arithmetic for key and signature calculations.

Legend:

- **P(x, y):** The base point on the elliptic curve.
- **a, d, p:** Curve parameters, where **p** is the prime order of the field.
- **n:** The order of the base point **P**.
- **Sk:** The private key.
- **M:** The message to be signed.
- **S:** The final signature output.
- **h:** The digest of the private key after applying SHA-512.
- **α, β:** The suffix and prefix derived from **h**.
- **γ:** The hash derived from the concatenation of **β** and **M**.
- **Pk(x, y):** The public key, computed as a multiple of the base point **P**.
- **r(x, y):** The randomized point, calculated during signature generation.
- **h′:** The hash of the concatenated values of **r**, **Pk**, and **M**.
- **s:** A part of the signature, computed using elliptic curve arithmetic.

Algorithm (9): EdDSA Signature Generation

Procedure: EdDSA Signature Generation

Input: Private key Sk, message M

Output: Signature S

1. Define Curve Parameters:
   - P(x, y), a, d, p, order n
2. Compute Digest of Private Key:
   - Apply SHA-512 to Sk to compute h.
3. Extract Suffix and Prefix from Digest:
   - Extract the first 32 bytes of h as suffix α.
   - Extract the next 32 bytes of h as prefix β.
4. Hash the Message:
   - Compute γ as the SHA-512 hash of β concatenated with M.

5. Convert to Integers:
   - Convert α and γ to integers in little-endian form.
6. Generate Public Key:
   - Compute public key Pk(x, y) as α multiplied by base point P.
   - Encode Pk as a byte string.
7. Calculate Point r(x, y):
   - Compute r(x, y) as γ multiplied by base point P.
   - Encode r as a byte string.
8. Compute Hash h′:
   - Compute h′ as the SHA-512 hash of r concatenated with Pk and M.
   - Convert h′ to an integer in little-endian form.
9. Compute Signature Part s:
   - Calculate s as ($\gamma + h' \times \alpha$) mod n.
10. Form the Signature:
   - Concatenate r and s to form the signature S.
11. Return Signature:
   - Return the final signature S for message M.

The EdDSA (Edwards-Curve Digital Signature Algorithm) verification process is used to confirm the authenticity of a signature by ensuring that it was created with the correct private key, without requiring access to the private key itself. This verification process relies on elliptic curve parameters and the SHA-512 hashing function to validate the signature against the message and the public key. Algorithm 10 described below details the steps required to verify an EdDSA signature.

Legend:

- **S:** The signature being verified, consisting of two parts, **r** and **s**.
- **M:** The message that was originally signed.
- **Pk:** The public key associated with the private key used for signing.
- **h:** The hash value computed during the verification process.
- **r:** The first part of the signature, representing a point on the elliptic curve.

- **s:** The second part of the signature, used in verification calculations.
- **sP:** The resulting point from elliptic curve operations involving **s** and the base point **P**.
- **P(x, y):** The base point on the elliptic curve.
- **SHA-512:** The cryptographic hashing function used to ensure message integrity.

Algorithm (10): EdDSA Signature Verification

Procedure: EdDSA Signature Verification

Input: Signature S, message M, public key Pk

Output: Returns True if the signature is valid, False otherwise

1. Extract Signature Components:
   - Extract the first part of S as r.
   - Extract the second part of S as s.
2. Compute Hash for Verification:
   - Compute h using M, Pk, and r with the SHA-512 hash function.
3. Convert to Integer Representation:
   - Convert s and h to integers in little-endian form.
4. Decode Point r:
   - Decode r into x and y coordinates of a point on the elliptic curve P(x, y).
5. Compute Point sP:
   - Calculate sP as the sum of the decoded r value and the product of h and Pk.
6. Signature Verification:
   - If sP equals the point obtained by computing s times the base point minus r times Pk, then:
     - Return True.
   - Else:
     - Return False.

4.6 Operational Flow of SecureBlockCert Framework

The operational flow of the SecureBlockCert framework, as delineated in Figure 4.8, commences with the user onboarding process. This process is categorized into distinct

steps, each integral to establishing and maintaining a secure and private digital environment for academic credential management.

Step 1: Network Joining and Wallet Generation

1.1 Users begin by submitting a network joining request through a dedicated blockchain-based API or decentralized application (dApp).

1.2 During this initiation phase, users are required to generate a key pair using the Ed25519 cryptographic algorithm, as specified in Algorithm 11.

1.3 This key pair generation is facilitated by a Certificate Authority (CA), ensuring the creation of secure, authenticated identity credentials for each user.

1.4 The output includes the generation of a unique pseudo-identity and the key pair, both of which are securely stored within the user's blockchain wallet.

The Ed25519 signature algorithm is a high-performance elliptic curve signing algorithm based on the Curve25519 elliptic curve. It provides secure, efficient signature generation and verification processes, making it widely used in cryptographic applications. Algorithm 11 consists of three main stages: key generation, signature generation, and signature verification. Each stage uses the Curve25519 base point G and SHA-512 as the cryptographic hash function.

Legend:

- **s:** A 32-byte random seed used to generate the private key.
- **A:** The public key computed as the multiple of the private key and the base point **G**.
- **pk:** The encoded public key.
- **sk:** The encoded private key.
- **R:** A 32-byte random value used in the signature generation process.

- **H:** The cryptographic hash function **SHA-512**.
- **M:** The message to be signed.
- **S:** The final signature for the message **M**.
- **l:** The order of the base point **G**, which defines the size of the elliptic curve.
- **h:** The hash computed from the concatenation of **R**, **pk**, and **M**.
- **h':** The hash recomputed during the verification stage.
- **S':** An intermediate value used in the signature verification process to check the validity of **S**.

Algorithm (11): Ed25519 Signature Algorithm

1: Key Generation:
2: Generate a 32-byte random seed s
3: Compute A = aG, where a is the private key and G is the base point
4: Set pk to be the encoding of A
5: Set sk to be the encoding of a
6: Signature Generation:
7: Compute h = H(R||pk||M), where R is the 32-byte random value
8: Compute R = rG, where r is the result of SHA-512 applied to h and the private key
9: Compute S = (R + h · A) mod l, where l is the order of the base point
10: Signature Verification:
11: Compute h′ = H(R||pk||M)
12: Compute S′ = R + h′ · A
13: if S′ is equal to S then
14: return True (valid signature)
15: else
16: return False (invalid signature)
17: end if

Step 2: Access Control and Privacy Protocol Activation

The authorization verification protocol activates to ascertain the permissions of issuers within the framework. This includes establishing encrypted channels for secure message exchange between peers. The communication protocol incorporates algorithms that utilize timestamps, Ti and Ti+1, to appraise message delivery delays, validate peer signatures, and thereby affirm message authenticity. Secure channel establishment is imperative for preserving end-to-end communication privacy. On successful validation, peers securely archive each other's encrypted identities within their wallets for subsequent interactions.

Step 3: Wallet Verification and Block Generation

Upon successful generation of the wallet, the SecureBlockCert network's validators scrutinize the user's submitted details alongside the wallet's credentials. If validated, these details are recorded onto the blockchain, leading to the generation of a corresponding block. The user's dApp then conveys the wallet particulars back to them, marking the completion of the onboarding process.

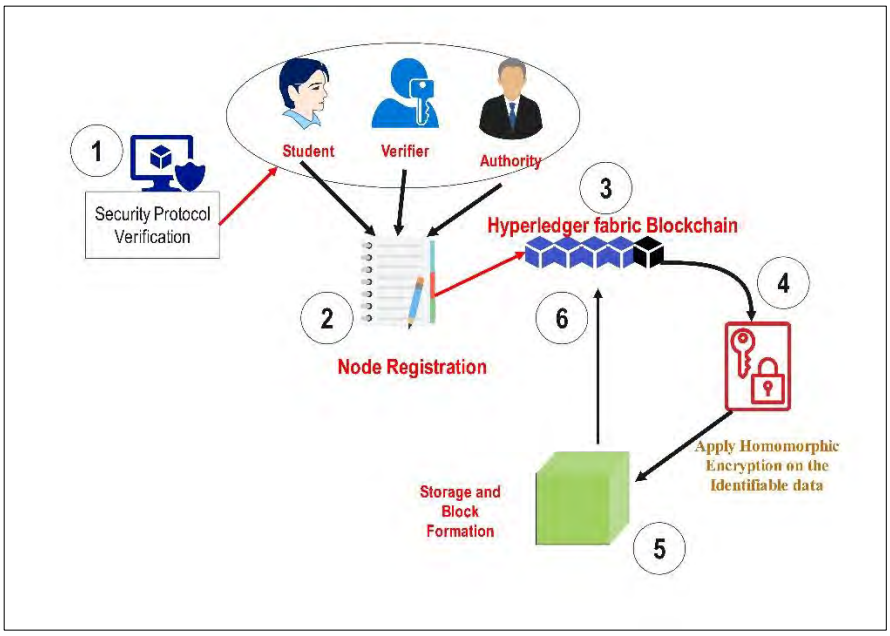

Figure 4.7 The Workflow of SecureBlockCert Framework

4.7 Implementation of SecureBlockCert on Hyperledger Fabric

The SecureBlockCert framework leverages the Hyperledger Fabric blockchain (HLF) to provide a robust and private infrastructure tailored to the needs of digital certificate issuance and verification. Unlike public blockchain networks such as Bitcoin and Ethereum, which are permissionless and use proof-of-work protocols for consensus, HLF is designed for permissioned environments where identity and trust are paramount [38],[86].

HLF's permissioned nature ensures that only identified and authorized participants can access the network, making it an optimal choice for SecureBlockCert's use case. Participants are verified and given certificates, creating a trusted ecosystem for managing digital identities. With HLF as its backbone, the SecureBlockCert framework operates within a controlled and secure environment supportive of regulatory compliance, such as GDPR, where identifiable information is handled with care. Notably, HLF's compatibility with popular programming languages like Java, Python, Go, and Node.js accelerates the development cycle by tapping into the existing skills of development teams. This versatility is crucial for SecureBlockCert as it allows for accessible and flexible smart contract development—a core component of the digital certification process.

HLF's consensus protocol, which is not tied to a one-size-fits-all approach like proof-of-work, is adaptable to diverse business needs. For SecureBlockCert, this means a consensus mechanism can be configured that balances speed, security, and fault tolerance tailored to the operations of digital credential verification. Although HLF does not require the use of a cryptocurrency, it presents an architecture capable of integrating custom token systems if needed, offering an avenue for potential incentives or transaction management within SecureBlockCert.

The architecture of HLF includes several key components that can be utilized effectively:

a) **Membership Service Provider**: Manages identities and authenticates participants within the network.

b) **Certificate Authority**: Issues and revokes certificates, aligning with the digital certificates managed by SecureBlockCert.

c) **Chaincode (smart contract)**: Encapsulates the business logic, providing SecureBlockCert with automated issuance and verification processes.

d) **Peers (endorsing, committing, and ordering nodes)**: Maintain the network and its integrity, ensuring the ledger's consistency across all nodes.

e) **Channels**: Enable private communications between specific network members, allowing SecureBlockCert to handle sensitive data securely and with confidentiality.

f) **Shared Ledger**: Records all transactions in a tamper-resistant and immutable manner, supporting the SecureBlockCert's need for a reliable audit trail of credential transactions.

g) **Gossip Network Protocol**: Facilitates efficient data dissemination and ledger synchronization across the network, ensuring all nodes in the SecureBlockCert framework have the latest state of the ledger.

The transaction flow within the HLF framework involves five high-level

a) User enrolment via the Membership Service Provider (MSP).

b) Submission of a transaction proposal to endorsing peers by the user.

c) Execution of the chain code by endorsing peers, followed by endorsement and return of the transaction to the client.

d) Submission of the endorsed transaction to the ordering service by the client.

e) Collection, verification, and addition of endorsed transactions to a new block by the ordering service, followed by validation and appending of the block to the blockchain by peers.

As shown in Figure 4.9, a Hyperledger Fabric network with multiple channels supports SecureBlockCert's approach to isolating interactions among participants. Each channel provides a distinct communication pathway, enabling secure and private exchanges of credential data between organizations. This channel-based design in Hyperledger Fabric allows the SecureBlockCert framework to ensure data privacy while maintaining efficient and secure credential management across different entities

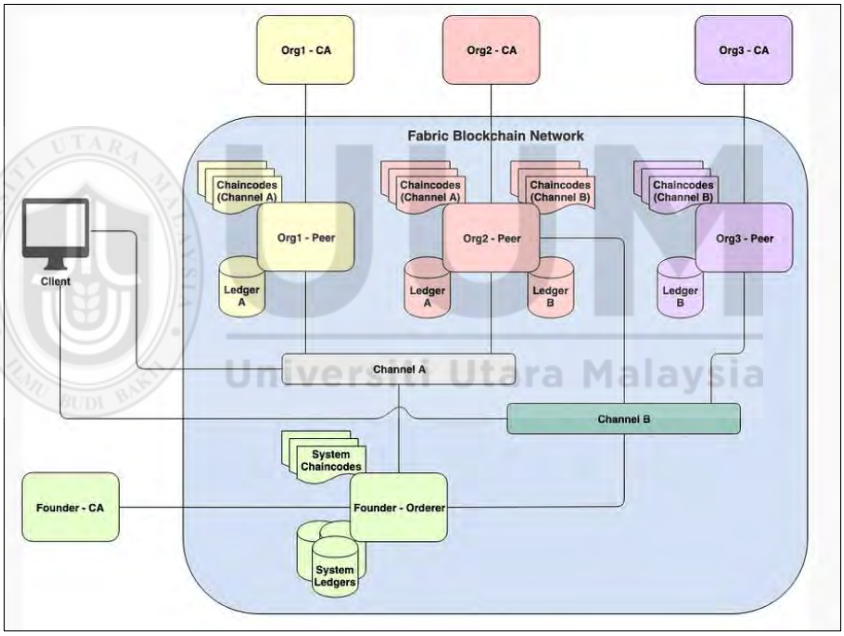

Figure 4.8 Fabric Network with Multiple Channels

This tailor-made approach in HLF allows SecureBlockCert to create a decentralized but controlled ecosystem conducive to the educational environment, where privacy, security, and trust are non-negotiable requirements. The HLF network's configurability is especially beneficial for SecureBlockCert, as it allows the framework to be finely tuned to meet the specific demands of credential issuance and verification.

Incorporating these HLF components, SecureBlockCert can deliver a solution that marries the benefits of blockchain technology transparency, security, and

immutabilitywith the needs of academia and professional entities for a more trusted and streamlined process for managing digital certificates. These enhancements to the SecureBlockCert framework, powered by Hyperledger Fabric, aim to provide not just an alternative, but a superior solution to the prevalent issues in digital certificate systems today. The SecureBlockCert's use of HLF embodies the cutting-edge of blockchain applications in educational and professional domains, setting a benchmark for future developments in this field [41],[98].

4.7.1 Certificate Authority in SecureBlockCert

Within the SecureBlockCert framework, the Certificate Authority plays a pivotal role in establishing the trust architecture of the digital certificate system. Its primary responsibility is to issue digital certificates that authenticate the identities of network participants, which include not only peers, clients, and administrators but also educational institutions and students. These digital certificates serve as the backbone of the framework, as they bind public keys with participant identities, ensuring that communications and transactions within the network are secure and verifiable.

The CA issues X.509 certificates, a standard format for public key certificates that provide robust security over internet connections, including TLS/SSL. In the context of SecureBlockCert, the CA's use of X.509 certificates becomes fundamental in managing the secure exchange of credentials and other sensitive information. By maintaining a stringent issuance and management process, the CA ensures that each certificate's integrity and authenticity are beyond reproach, which is critical for upholding trust among all stakeholders in the digital certification ecosystem.

The reliance on a CA within the SecureBlockCert framework ensures a high degree of trust, as each actor within the network—be it a student, an educational institution or a potential employer—is verified and thus accountable for their actions. This effectively

mitigates the risk of fraud and misrepresentation, reinforcing the credibility of the SecureBlockCert system.

4.7.2 Membership Service Provider in SecureBlockCert

In the context of the SecureBlockCert framework, the Membership Service Provider is the gatekeeper of the network, managing the identities and privileges of all participants involved in the digital certificate system. The MSP adheres to a set of predefined rules and policies that it enforces to determine the validity of participants based on their assigned roles and permissions within the infrastructure. This ensures that only verified and credentialed members have the authority to perform network functions such as issuing, endorsing, and validating academic certificates, as well as accessing secure ledger data.

The MSP works in tandem with the Certificate Authority to maintain and verify a list of members and their associated cryptographic credentials. The process is streamlined by utilizing the same digital certificates issued by the CA, which the MSP validates to authenticate each participant's identity. This guarantees that every transaction in the SecureBlockCert network is performed by legitimate entities, which is especially important in academic settings where the integrity of credentials is paramount.

Each participating educational institution within the SecureBlockCert ecosystem operates under its own MSP, which allows it to enforce identity and access controls tailored to its specific governance and policy requirements. This level of fine-grained control is fundamental for institutions that need to ensure the security and validity of their issuance processes.

By leveraging the combined functionalities of the CA and MSP, the SecureBlockCert framework creates a trusted environment where the integrity, security, and confidentiality of academic transactions are upheld. Such a robust system empowers

institutions to maintain high standards for credential verification, enhancing the reliability of educational certifications on a global scale.

4.7.3 Peer Nodes in SecureBlockCert

Within the SecureBlockCert framework, peer nodes serve as the cornerstone of the blockchain infrastructure. Their primary function is to facilitate the entire lifecycle of digital certificates within the Hyperledger Fabric network. Peers are responsible for validating transactions and maintaining an accurate and consistent state of the ledger, which in the case of SecureBlockCert, contains vital educational credentials and certification information.

In Hyperledger Fabric, peer nodes are categorized into endorsing peers and committing peers, both of which play an integral role within the SecureBlockCert system:

a) **Endorsing Peers**: These nodes examine transactions against specific endorsement policies and execute chaincode (smart contracts) to simulate transaction results. In the context of SecureBlockCert, endorsing peers are critical as they ensure the legitimacy and compliance of certificate issuance and verification requests before they get written to the ledger.

b) **Committing Peers**: After transactions are endorsed, committing peers are then responsible for appending them to the ledger. Within SecureBlockCert, these nodes maintain the most recent and accurate state of digital certificates issued and revoked, making them the guardians of the ledger's integrity.

These peer types are vital for the SecureBlockCert's efficient operation; the endorsing process validates the legitimacy of digital certificate transactions, while the committing peers maintain the trustworthiness of the information stored on the blockchain. Together, they ensure a secure, transparent, and immutable record-keeping system that upholds the authenticity of academic credentials.

4.7.4 Ordering Service in SecureBlockCert

For the SecureBlockCert framework, the ordering service within Hyperledger Fabric is critical as it establishes the definitive order of transactions and guarantees consistent updates to the ledger. This service is particularly crucial for the integrity of the digital certificate system as it ensures that the issuance, revocation, and verification of certificates are sequentially processed and permanently recorded.

Rather than being managed by a single central authority, the ordering service in SecureBlockCert can be distributed across different entities, reflecting a consortium model where no single participant holds unilateral control over the ledger. This distributed approach aligns well with educational environments where multiple institutions collaborate, yet also maintain their independence and governance standards. The ordering service is charged with the following tasks:

a) **Batching Transactions into Blocks**: The ordering service selects verified transactions from the endorsement phase and batches them into a block, ensuring that they are organized in a clear, chronological sequence. This step is vital in the SecureBlockCert context as it preserves the history of academic credentials, making them verifiable and traceable in a transparent manner.

b) **Signing and Distributing Blocks**: Once a block is formed, the ordering service digitally signs it to ensure its authenticity and then reliably distributes the block to all peers in the network for validation and commit. This is essential to maintaining a single source of truth that all network participants can trust.

The reliability of the ordering service in the SecureBlockCert ensures correctness and non-repudiation of records on the ledger, thereby preventing discrepancies or conflicts in certificate statuses. This system's structure fosters high trust among all network users and greatly contributes to the security of digital certifications. Thanks to the

ordering service, all parties involved can have confidence that the ledger reflects a true and unilateral sequence of all certificate-related transactions, upholding the framework's overall integrity and confidentiality.

4.7.5 Channels in SecureBlockCert

In the SecureBlockCert framework on Hyperledger Fabric, channels play a critical role in safeguarding the privacy and confidentiality of academic certificates. By establishing private "subnets" within the broader network, channels enable participants such as universities, accreditation bodies, and students to interact and transact in a secure environment distinct from the main blockchain network.

This private ledger feature of channels is key to the SecureBlockCert framework, as it allows:

a) **Sensitive Data Protection**: Academic credentials and personal student information are shared and stored securely, accessible only to authorized network members who have been granted explicit permission to view and manage such data.

b) **Smart Contract Deployment**: Channels allow the creation and execution of specialized chaincodes, which can manage the logic for specific educational transactions such as credential verifications, record updates, and access rights.

c) **Selective Membership**: Only participants who have been authenticated and authorized via their digital identities, managed by the Certificate Authority and Membership Service Provider, can create or be invited to join a channel.

d) **Transaction Privacy**: Transactions conducted within a channel are only visible to its members, thus ensuring that the confidential exchange of academic records and certifications remains private among involved parties.

Each channel within the SecureBlockCert framework acts as a silo designed to streamline interactions between members while reinforcing the security and integrity of the exchange. Digital signatures add to this privacy by verifying the identity of participants and ensuring only those with the right access can engage in channel transactions. By utilizing channels, the SecureBlockCert framework achieves a balance between the collaborative needs of educational institutions within a public network and the desire to keep certain interactions private, underpinning a secure and efficient digital certification process.

4.7.6 Chaincode in SecureBlockCert

Chaincode is the backbone of the SecureBlockCert's transaction management system within the Hyperledger Fabric network. It encapsulates the business logic that defines the operations associated with digital certificates, such as issuance, revocation, and verification. Within SecureBlockCert, chaincode functions as follows:

a) **Ledger State Management**: The primary purpose of chaincode is to manage the ledger state, which in the context of SecureBlockCert includes the detailed attributes of the digital certificates, the certification authority details, and the transaction records between participants.

b) **Invocations and Transactions**: Applications within SecureBlockCert invoke chaincode to perform functions. Every time an educational institution issues or a potential employer verifies a certificate, the corresponding chaincode is triggered to execute the transaction by reading from or writing to the ledger.

c) **Inter-Chaincode Communications**: SecureBlockCert can utilize one chaincode to interact with others, adding a layered functionality that supports complex operations. For example, one chaincode responsible for identity verification might interact with another managing certificate credentials.

d) **Built-in Functions**: Chaincodes in SecureBlockCert have access to a suite of built-in functions like GetState() to retrieve data from the ledger and PutState() to update or add new records. These functions are fundamental for maintaining an accurate and up-to-date ledger reflecting all certificate-related activities.

Programming languages such as Go, Java, or Node.js can be used to write chaincode, offering versatility and the power necessary to implement complex logic required for managing various certificate processes in the SecureBlockCert framework.

4.7.7 Shared Ledger in SecureBlockCert

In the SecureBlockCert initiative, powered by Hyperledger Fabric, the Shared Ledger is a digital compendium of every transaction conducted within the network. As each transaction related to digital certificates is verified and endorsed, it is immutably recorded in this ledger, creating a traceable record of all certificate issuances and validations. Key attributes of the Shared Ledger in SecureBlockCert include:

a) **Chronological Order**: Transactions are recorded in a time-stamped series of blocks, which provides a tamper-evident history of all certificate transactions, allowing any network participant to audit and verify past activities with ease.

b) **Data Privacy Through Channels**: SecureBlockCert leverages the multi-channel architecture of Hyperledger Fabric. Each channel represents a distinct ledger, enabling participating entities to transact privately, thus ensuring that sensitive academic records and transactions are shared only among authorized participants.

c) **Cryptographic Veracity**: Every transaction on the Shared Ledger is cryptographically signed, enhancing the security of the digital certificate platform. This cryptographic signature assures the authenticity and integrity of each transaction.

d) **Consensus Mechanism**: A consensus mechanism maintains the ledger's accuracy and consistency. SecureBlockCert can flexibly implement this by adopting an algorithm such as Proof of Authentication.

4.7.8 Gossip Network Protocol in SecureBlockCert

In the SecureBlockCert framework, the Gossip Network Protocol is a key mechanism for ensuring that all nodes in the network have consistent and updated information regarding the state of the ledger, particularly concerning digital certificates.

how the Gossip Network Protocol benefits SecureBlockCert is given below:

a) **Peer-to-Peer Communication**: This protocol allows SecureBlockCert nodes to effectively share ledger data amongst each other. When a peer node in the blockchain network updates its ledger with new transactions, such as the issuance or verification of digital certificates, this information is then gossiped to its neighbors.

b) **Efficient Data Dissemination**: Through gossiping, data is rapidly relayed from one node to the next, quickly reaching all corners of the network. This efficiency is paramount in SecureBlockCert to ensure near-real-time updates regarding certificate statuses, ensuring that all stakeholders have the latest information about credential validity.

c) **Scalability and Reliability**: As information disseminates in an overlapping and redundant manner, the Gossip Network Protocol leads to a scalable system capable of handling growth without compromising performance. Moreover, this redundancy contributes to the network's fault tolerance because even if some nodes fail or become disconnected, information can still propagate through alternative pathways.

d) **Maintaining Ledger Consistency**: To maintain the integrity of the SecureBlockCert framework, it's vital that all nodes agree on the state of the ledger. The Gossip Network Protocol assists in this by making sure that ledger updates reach every node, and consequently, every participant is synchronized with the latest state of the shared ledger.

Implementation of the Gossip Network Protocol in SecureBlockCert is essential for achieving a robust, trustworthy system for digital certificate exchange on the blockchain, enabling users to verify the accuracy and timeliness of academic credentials across the network.

4.8 Transaction Flow in SecureBlockCert Framework

The transaction flow within the SecureBlockCert framework, which utilizes the Hyperledger Fabric network, follows a structured sequence of steps to ensure secure transactions:

1.8.1 User Enrolment:

Initially, a participant (e.g., a university, student, or employer) must enroll with the SecureBlockCert network via the Membership Service Provider. The MSP manages digital identities and grants participants the credentials needed to interact with the blockchain.

1.8.2 Transaction Proposal:

Once enrolled and authenticated, the user can submit a transaction proposal. For SecureBlockCert, this could involve proposing a new digital certificate or requesting to verify the authenticity of a certificate.

1.8.3 Execution and Endorsement:

Proposals are sent to endorsing peers, which execute the relevant chaincode (smart contract) that encapsulates the logic for digital certificates. After executing the transaction, endorsing peers endorse the results and return them to the client (user).

1.8.4 Ordering of Transactions:

The client collects endorsements and submits the transaction to the ordering service, which aggregates transactions from throughout the network into blocks.

1.8.5 Validation and Commitment:

Finally, the ordering service delivers the blocks to all peers. The peers validate the transactions and once verified as correct and consistent, append the new block to their copy of the blockchain.

This process ensures the SecureBlockCert transactions are consistently ordered, validated, and recorded in an immutable and verifiable manner and reflects how blockchain technology enhances the security and privacy of digital certificate systems.

4.9 System Structure of SecureBlockCert

The system structure of SecureBlockCert, built on the Hyperledger Fabric platform, can be conceptualized in a four-layer hierarchy as shown in figure 4.10

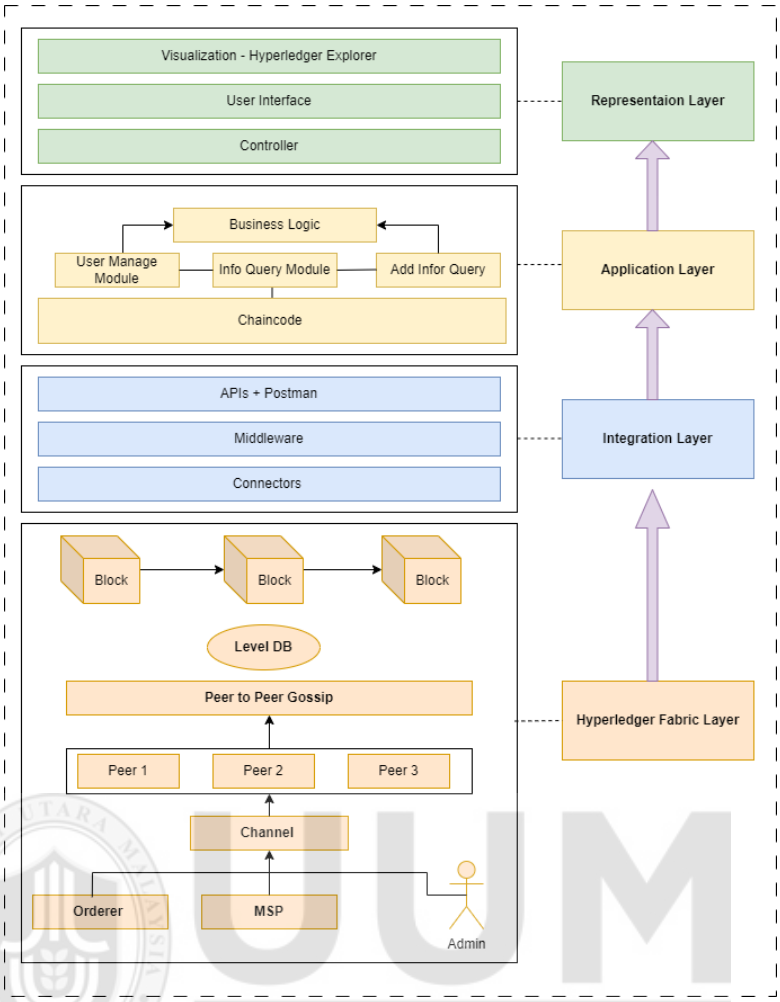

Figure 4.9 System Architecture of the SecureBlockCert Framework on Hyperledger Fabric

4.9.1 Hyperledger Fabric Layer:

This foundational layer leverages Hyperledger Fabric to provide a secure, permissioned blockchain infrastructure. Key components include:

a) **Organizations**: Represent authorized stakeholders within the network, such as academic institutions and verification entities, with distinct roles and permissions.

b) **Orderer Node**: Manages the ordering of transactions into blocks, ensuring their chronological sequencing and consistency across the network.

c) **Peer Nodes:** Store replicas of the blockchain, validate transactions, and are instrumental in upholding the decentralized network structure.

d) **Certificate Authority:** Issues and manages digital certificates for network participants, linking public keys to participant identities and facilitating secure interactions.

e) **Membership Service Provider:** Governs access through identity verification, enabling secure and authenticated participation within the network.

f) **Channels:** Provide private conduits for communication, allowing participants to transact confidentially and ensuring selective information sharing.

g) **Gossip Protocol:** Ensures the rapid and efficient dissemination of data, assisting peers in staying up-to-date with the latest state of the ledger.

h) **Storage Layer:** - LevelDB: Implements key-value store functionality, enabling efficient ledger data management through straightforward data insertion, retrieval, and deletion operations.

i) **Block Structure:** - Blocks: Act as the basic building blocks of the ledger, encapsulating batches of transactions that are immutably linked together to form the blockchain

4.9.2 Integration Layer in SecureBlockCert

The integration layer in SecureBlockCert plays an essential role in bridging the blockchain network with external applications and services. Key components of this layer include:

a) **APIs**: Provide a set of interfaces for SecureBlockCert, facilitating interaction and data exchange between the blockchain and external systems. The APIs enable various operations such as submitting certificate issuance requests, querying certificate validity, and more.

b) **Middleware**: Acts as an intermediary layer that translates requests and data formats between the blockchain network and third-party systems or services, ensuring seamless connectivity.

c) **Connectors**: Serve as the tools or adapters that enable communication between SecureBlockCert and external infrastructure, supporting a wide array of applications and databases.

This layer's successful operation is validated through tools like Postman, which test the robustness and reliability of APIs to handle network requests efficiently.

4.9.3 Application Layer in SecureBlockCert

The application layer hosts the user-facing components of SecureBlockCert, enabling interaction with the underlying blockchain:

a) **Business Applications**: These applications provide the interface through which users, such as educational institutions, students, or employers, can interact with the blockchain. They might include web interfaces or mobile apps that facilitate tasks such as accessing, issuing, or verifying academic certificates.

b) **Chaincode**: Developed using Java, a popular and versatile programming language chosen for its flexibility and widespread use. This ensures both the ease of chaincode development and its adaptability to future updates or changes in business logic.

c) **Functionalities**: The chaincode is designed to be secure and deterministic, enabling functions like issuing verifiable digital certificates, confirming their authenticity, and managing student achievements and records with accuracy and efficiency.

d) **Customization**: Given the specific needs of the academic sector, these functionalities are tailored to handle various academic credentialing requirements, supporting reliable issuance and verification processes essential for maintaining the integrity of educational certifications.

4.9.4 Representation Layer in SecureBlockCert

In SecureBlockCert, the representation layer is where users directly engage with the system. It includes several important components:

a) **Controller**: Serves as the conduit between the blockchain backend and the frontend, orchestrating the flow of data and requests to ensure that the application logic and user commands are in sync.

b) **User Interface**: Provides visual or command-line interfaces that allow users to carry out transactions, view ledger data, and interact with various other functionalities of SecureBlockCert. It is designed with an emphasis on intuitiveness to accommodate users with different levels of technical expertise.

c) **Hyperledger Explorer**: A visualization tool that reveals the activities within the blockchain network, including detailed views of blocks, transactions, and network participants. It is vital for stakeholders who need to audit or review the trail of activities on the blockchain.

4.10 Conclusion

In conclusion, SecureBlockCert exemplifies the substantial potential of blockchain technology in fortifying digital credential systems within educational contexts. This chapter outlined the systematic development and structure of the SecureBlockCert framework, detailing its strategic modules designed to enhance security, safeguard privacy, and optimize credential issuance and verification processes within blockchain networks. The security enhancement module fortifies the system against unauthorized

intrusions, reinforcing its resilience. The privacy preservation module ensures data confidentiality, protecting sensitive information from unauthorized access. Additionally, the issuance and verification module streamlines credential distribution and verification, fostering a trusted, efficient environment for stakeholders. The integration of these modules establishes a robust infrastructure that redefines how educational institutions issue, manage, and verify academic credentials. SecureBlockCert's design not only adheres to rigorous security standards but also prioritizes user data privacy, laying the foundation for a new era of trust and integrity in digital certifications.

CHAPTER FIVE
IMPLEMENTATION AND EVALUATION OF SECUREBLOCKCERT

5.1 Introduction

This chapter offers a detailed examination of the SecureBlockCert framework, a new blockchain-based approach designed to enhance security and privacy in digital credentialing systems. SecureBlockCert aspires to establish new standards within digital certification by integrating advanced security measures and privacy-preserving mechanisms. The chapter is structured to first outline the development and implementation of a prototype for SecureBlockCert, with particular emphasis on validating its security and privacy objectives. A systematic evaluation then follows, in which the framework's components are rigorously tested against both established benchmarks and practical scenarios. The aim of this evaluation is to gain a comprehensive understanding of SecureBlockCert's capabilities and limitations, particularly in terms of security, privacy, and operational efficiency. The insights derived from this analysis are essential to verify that SecureBlockCert meets, and potentially exceeds, the rigorous requirements expected of contemporary digital certification systems. By addressing these criteria, this framework aims to contribute a robust, secure, and scalable solution for managing digital credentials.

5.2 Prototype Implementation

The development of a Hyperledger Fabric-based prototype for digital certificate management represents a crucial phase in validating the SecureBlockCert framework. This section outlines a strategic approach to constructing the prototype, ensuring each phase adheres to high standards of security and privacy.

5.2.1 Hyperledger Fabric Network Setup

The foundation of SecureBlockCert is a distributed ledger infrastructure built using Hyperledger Fabric. Essential stakeholders such as educational institutions, verification bodies, and peer organizations are integrated into the network, facilitating secure, transparent record management. Strict access control policies are enforced to align with SecureBlockCert's privacy requirements, ensuring data integrity and confidentiality.

5.2.1 Smart Contract Development

Smart contracts, or "chain code" in Hyperledger Fabric, are developed to encode the business logic necessary for issuing, managing, and verifying digital certificates. These contracts are rigorously designed to meet stringent security and privacy standards, supporting the complex queries and transactions integral to credential management.

5.2.2 Client-Focused Application Design

User interfaces are developed to streamline interaction with the blockchain network and associated smart contracts. These client interfaces are tailored for distinct user roles, including certificate issuers, recipients, and third-party verifiers, ensuring efficient issuance, verification, and access to academic certificates.

5.2.3 Cryptographic Integration

To enhance data security, SecureBlockCert incorporates advanced cryptographic methods:

a) **Asymmetric Cryptography**: Manages secure communications and identity verification across network participants.

b) **Homomorphic Encryption**: Preserves data confidentiality during processing, enabling computations on encrypted data without decryption.

5.2.4 Testing Protocols

Rigorous transaction testing is applied to validate each component of the blockchain system. This includes stress-testing smart contracts under diverse scenarios and auditing cryptographic implementations to ensure resilience against unauthorized access and data breaches.

By methodically executing each phase, from network setup to comprehensive testing, the SecureBlockCert prototype aims to establish a new benchmark in secure, privacy-focused digital certificate management.

5.3 Experimental Environment

SecureBlockCert leverages Hyperledger Fabric to establish two private blockchain consortiums dedicated to digital certificate verification and management. This setup fosters secure collaboration among multiple organizations, with Hyperledger Fabric's permissioned framework enhancing security, privacy, and trust.

The architecture of Hyperledger Fabric, known for its open-source, permissioned nature, is well-suited for organizational applications requiring privacy, security, and scalability. Within SecureBlockCert, this architecture facilitates the secure and private exchange of digital certificates among verified entities. Key roles within this network include:

a) **Certificate Authorities (CAs):** Responsible for issuing and revoking digital certificates within the network.

b) **Peers**: Function as network nodes managed by participating organizations, processing transactions and maintaining the ledger's state.

c) **End-Users**: Access the blockchain via client applications to request digital certificates and verification services.

d) **Ordering Service**: Establishes transaction order and generates definitive blocks for the 3 ledger.

e) **Channels**: Create private subnets for communication, enabling confidential transactions and segregating traffic based on organizational affiliation.

Through Hyperledger Fabric, SecureBlockCert provides secure and private data sharing, fortifying the network infrastructure against cyber threats, enhancing data privacy, and establishing a trusted environment for digital certificate management.

5.3.1 Hardware Environment

The experiments are conducted using the system with the following hardware specifications:

a) 2 Core CPU (Intel (R) Core ™ i5-4570 CPU @ 3.20 GHz);

b) 8 GB RAM;

c) Ubuntu OS (version 22.04.1 (TS))

5.3.2 Software Environment

To facilitate a seamless and efficient development and testing process for the SecureBlockCert framework, the following software prerequisites were established. Figure 5.1 provides an overview of the necessary tools and environments for installing Hyperledger Fabric. Additionally, Table 5.1 details the installed Hyperledger Fabric components, which form the backbone of SecureBlockCert's blockchain functionality.

a) **Hyperledger Fabric v2.5**: As the foundation for SecureBlockCert, this version of Hyperledger Fabric provides the necessary platform and features for developing an enterprise-grade blockchain to handle digital certificates.

b) **cURL**: The latest version of cURL is used to communicate with web services and to facilitate the downloading of prerequisites and necessary files during setup and operation.

c) **Docker** (version 17.06.2-ce or greater): Docker containers encapsulate the SecureBlockCert components and allow for consistent deployment and scaling across various environments.

d) **Docker Compose** (version 1.14.0 or higher): This tool is utilized for defining and running multi-container Docker applications, streamlining the setup of the Fabric network and associated services.

e) **Golang** (version 1.11.x): The chain code, or smart contracts, for the SecureBlockCert are written in Golang, as it is the primary programming language supported by Hyperledger Fabric.

f) **Node.js** (version 8. x): Due to compatibility with the current version of Hyperledger Fabric, Node.js is used for developing client applications that interact with the blockchain.

g) **NPM** (version 5. x): Node.js packages, which are critical for the client application development, are managed using this package manager.

h) **Python** (version 2.7): Some scripts and applications within Hyperledger Fabric require Python 2.7; hence, it is included in the software environment.

i) **VS Code**: This Integrated Development Environment is recommended for writing chain code and client applications due to its robust support for Hyperledger Fabric development and its rich set of extensions.

j) **Hyperledger Caliper**: This benchmarking tool allows for performance testing of the SecureBlockCert, providing insights into transaction processing speeds, latency, and throughput under various conditions.

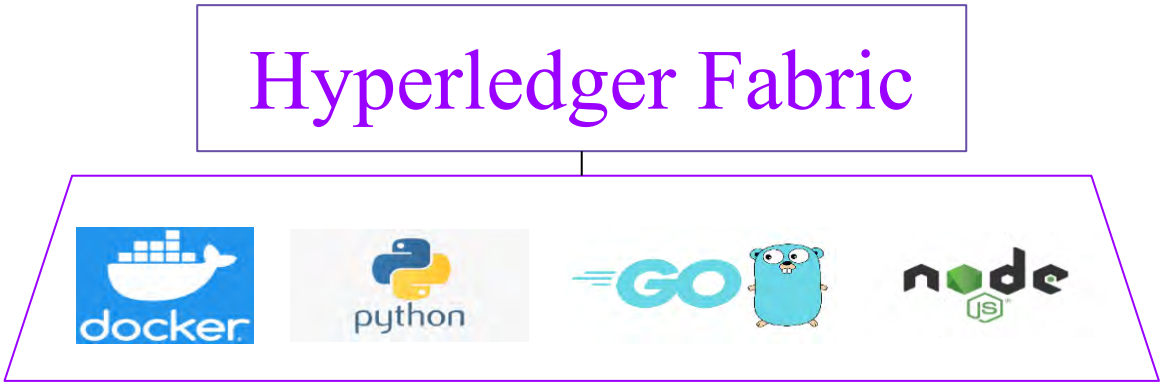

Figure 5. 1 Requirements for installing the Hyperledger Fabric Environment

Table 5. 1 Installed Hyperledger Fabric Components

Container ID	Image	Command	Ports	Names
3e3f0eaee48a	dev-peer0.org2.example.com-basic_1.0-a76471f5e7ff9dfcc5c9d8b2298aa41d2f5608956c8cbdc31018f938d87786eb-7675af52fe7a5d6de1c3a46a90584bd905e9b19a3a19869ee597b630e95342e6	docker-entrypoint.sh ...		dev-peer0.org2.example.com
7262edee80fc	dev-peer0.org1.example.com-basic_1.0-a76471f5e7ff9dfcc5c9d8b2298aa41d2f5608956c8cbdc31018f938d87786eb-9135f8c114e56ae21525a234907f2191577d4bc661bfaf91492ef8c7edba1b0c	docker-entrypoint.sh ...		dev-peer0.org1.example.com
ab5064c01294	hyperledger/fabric-tools:latest	/bin/bash		cli
50b959e09eb2	hyperledger/fabric-peer:latest	peer node start	0.0.0.0:9051->9051/tcp, :::9051->9051/tcp, 7051/tcp, 0.0.0.0:9445->9445/tcp, :::9445->9445/tcp	peer0.org2.example.com
64d9d41c00be	hyperledger/fabric-peer:latest	peer node start	0.0.0.0:7051->7051/tcp, :::7051->7051/tcp, 0.0.0.0:9444->9444/tcp, :::9444->9444/tcp	peer0.org1.example.com

ee6f6fc91761	couchdb:3.1.1	tini -- /docker-entrypoint.sh couchdb	4369/tcp, 9100/tcp, 0.0.0.0:7984->5984/tcp, :::7984->5984/tcp	couchdb1
e3d0e52ac603	hyperledger/fabric-orderer:latest	orderer	0.0.0.0:7050->7050/tcp, :::7050->7050/tcp, 0.0.0.0:9443->9443/tcp, :::9443->9443/tcp	orderer.example.com
487216193ef8	couchdb:3.1.1	tini -- /docker-entrypoint.sh couchdb	4369/tcp, 9100/tcp, 0.0.0.0:5984->5984/tcp, :::5984->5984/tcp	couchdb0
fad3249f0e83	hyperledger/fabric-ca:latest	sh -c 'fabric-ca-server start -b admin:admin pw -d'	0.0.0.0:8054->8054/tcp, :::8054->8054/tcp, 7054/tcp, 0.0.0.0:18054->18054/tcp, :::18054->18054/tcp	ca_org2
7e91d60e05a6	hyperledger/fabric-ca:latest	sh -c 'fabric-ca-server start -b admin:admin pw -d'	0.0.0.0:9054->9054/tcp, :::9054->9054/tcp, 7054/tcp, 0.0.0.0:19054->19054/tcp, :::19054->19054/tcp	ca_orderer
2063c567f9a1	hyperledger/fabric-ca:latest	sh -c 'fabric-ca-server start -b admin:admin pw -d'	0.0.0.0:7054->7054/tcp, :::7054->7054/tcp, 0.0.0.0:17054->17054/tcp, :::17054->17054/tcp	ca_org1

We installed the necessary prerequisites as outlined in the official Hyperledger documentation, utilizing Ubuntu 22.04.3 LTS on a Windows 10 system.

Figure 5.2 illustrates the core Fabric components of the proposed blockchain, providing the architectural foundation for the SecureBlockCert framework. This schematic offers insights into the interconnected elements of Hyperledger Fabric, forming a cohesive and secure blockchain network optimized for managing digital certificates.

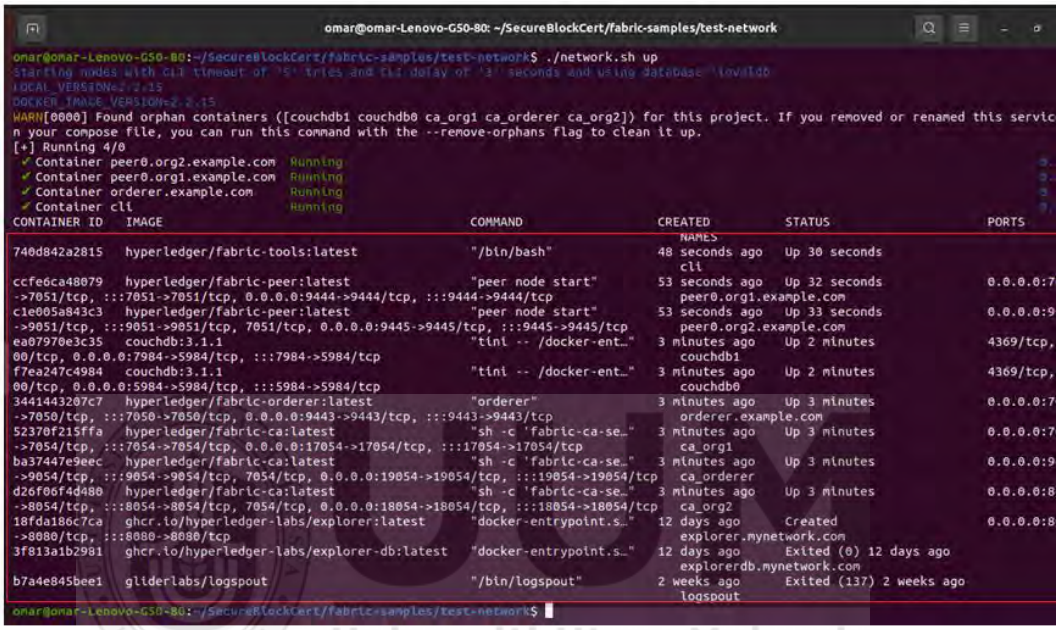

Figure 5. 2 Essential Components of the Hyperledger Fabric Network for the SecureBlockCert Framework

Moving on to the initiation process, Figure 5.3 captures the channel creation procedure, a crucial step where secure communication channels between different network participants are established. This ensures that all transactions involving digital credentials are conducted within a trusted and private environment.

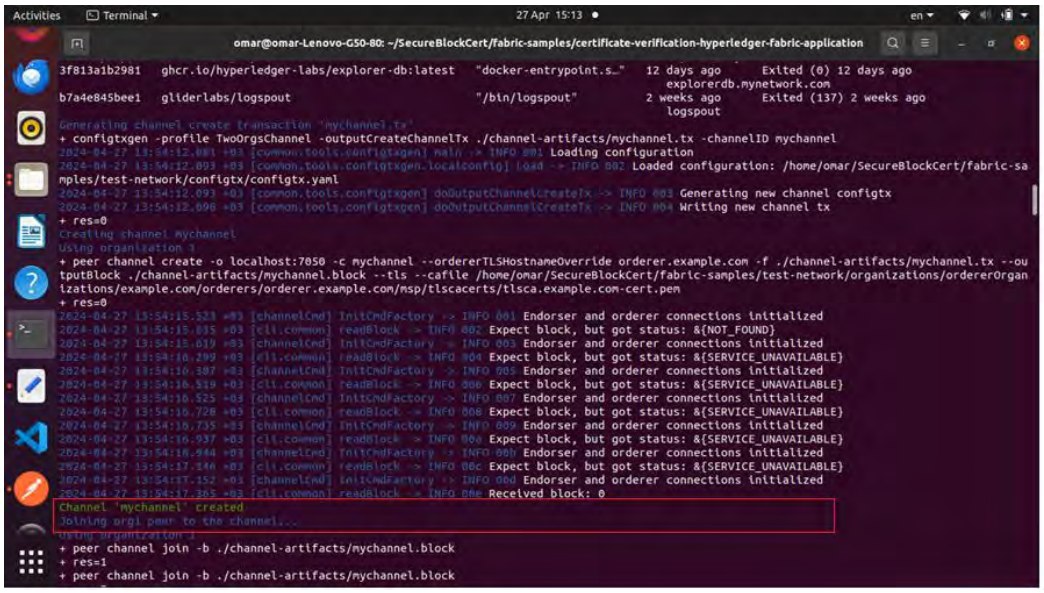

Figure 5. 3 Chanel Creation

In Figure 5.4, how the chain code is packaged is shown. This procedure packages the smart contracts that will dictate the rules and validations of the digital credentials, preparing them for deployment within the blockchain network.

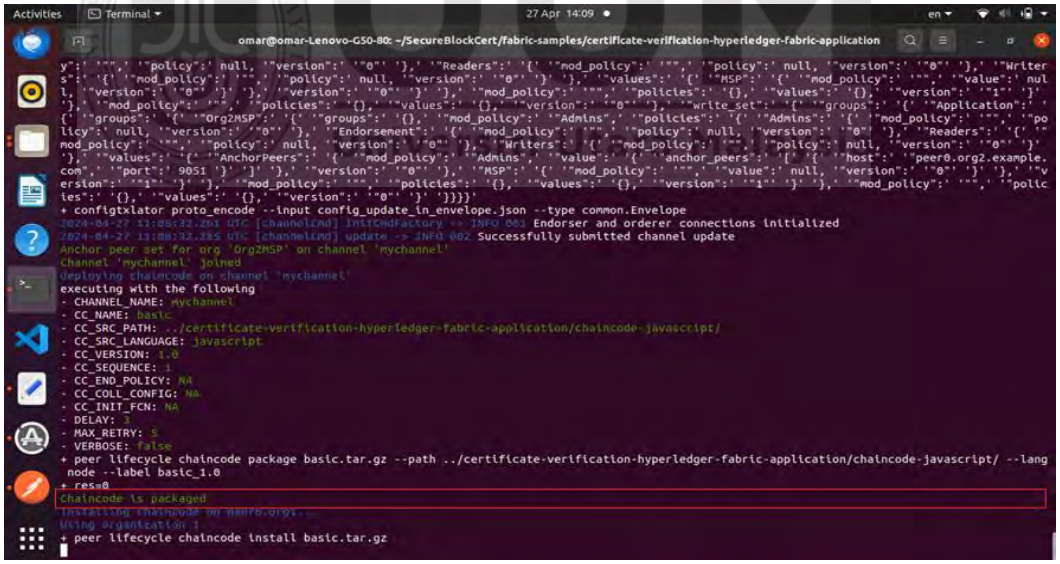

Figure 5. 4 Chaincode is Packaged

Figure 5.5 represents the next step with a visual of the chain-code installation. This is where the packaged smart contracts are installed on the network peers, integrating the logic that will automate and secure credential transactions.

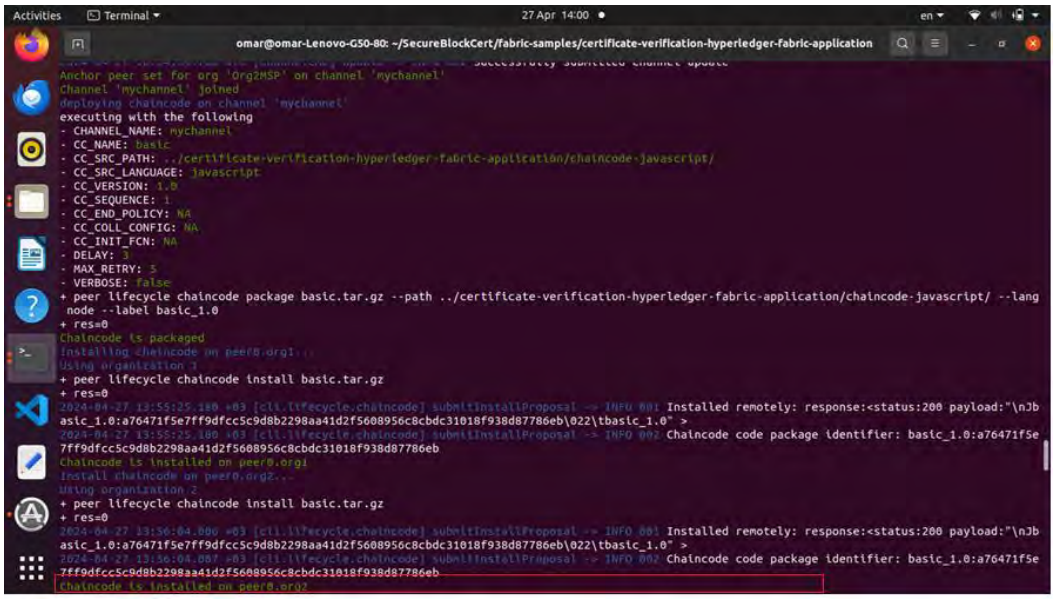

Figure 5. 5 Chain-code Installation

Subsequently, Figure 5.6 depicts the process where the chain code is approved. Approval from the requisite network participants is mandatory before the smart contracts become active, signifying a consensus-driven approach to maintain the network's integrity. Figure 5.7 demonstrates the Hyperledger fabric listening to APIs for Data Transactions. This interaction is instrumental in enabling real-time, secure communication and transactions within the network, reflecting the system's responsiveness. In Figure 5.8, we have a screenshot of the transaction history API tested in POSTMAN, confirming the successful initialization of the contract. This illustrates the practical application of the API and provides evidence of the system's functionality in a simulated environment.

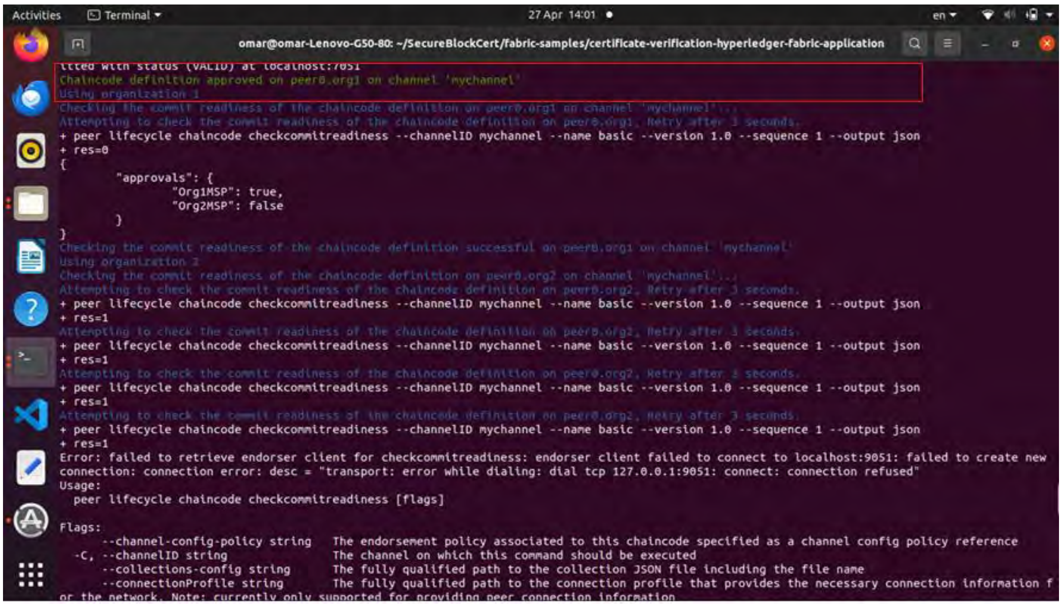

Figure 5. 6 Chain-code is approved

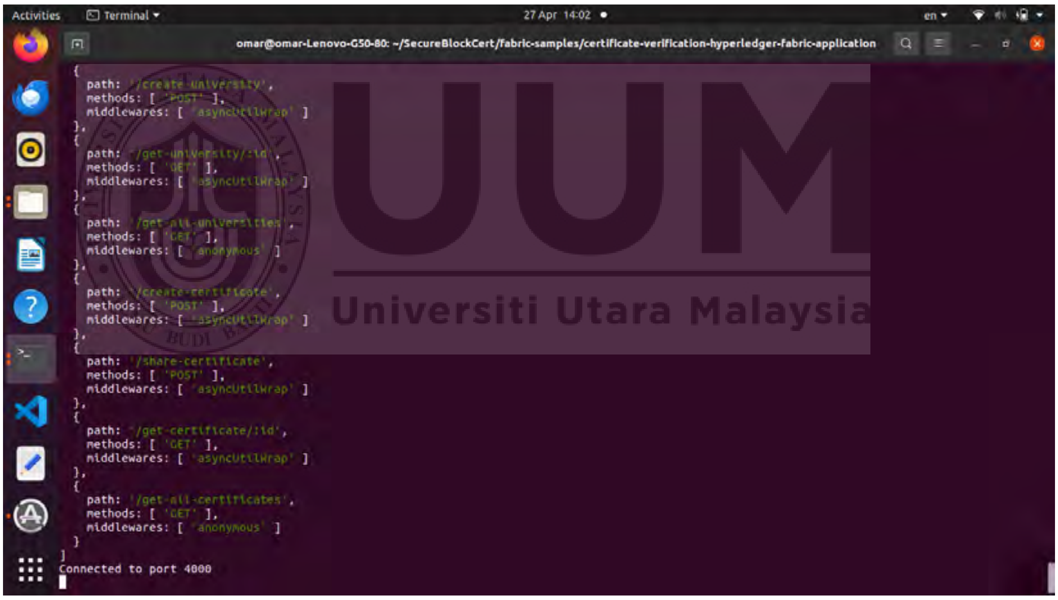

Figure 5. 7 Hyperledger Fabric is listing to APIs for Data Transaction

Finally, Figure 5.9 showcases a Screenshot of a successful Transaction History API as tested in Hyperledger Fabric, triggered by a Ministry. This transaction exemplifies a real-use case scenario, verifying the efficacy of SecureBlockCert in an operational setting and signaling a successful interaction with the blockchain.

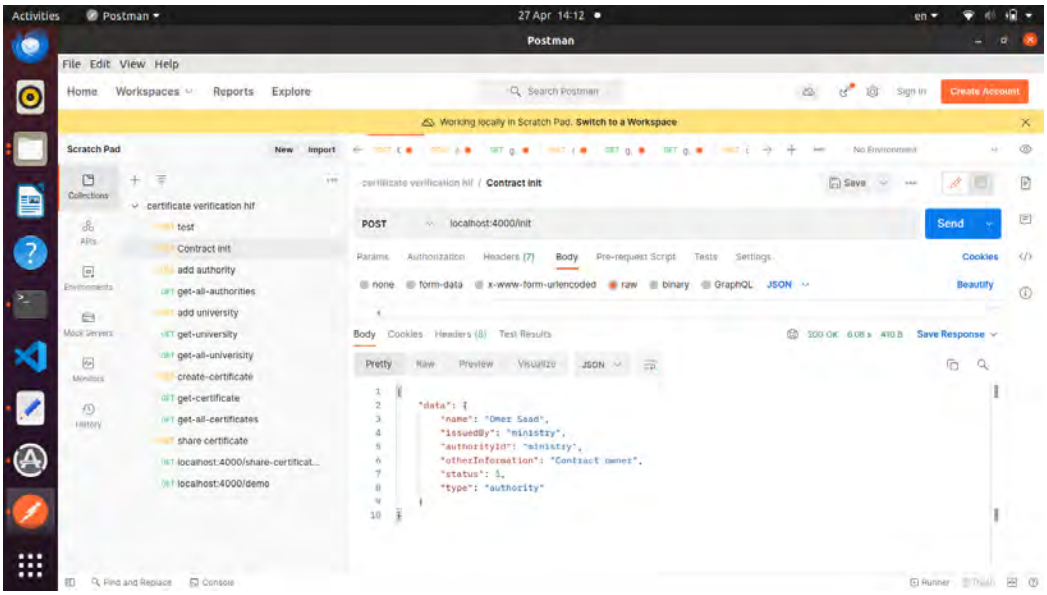

Figure 5. 8 Screenshot of the Transaction History API tested in POSTMAN

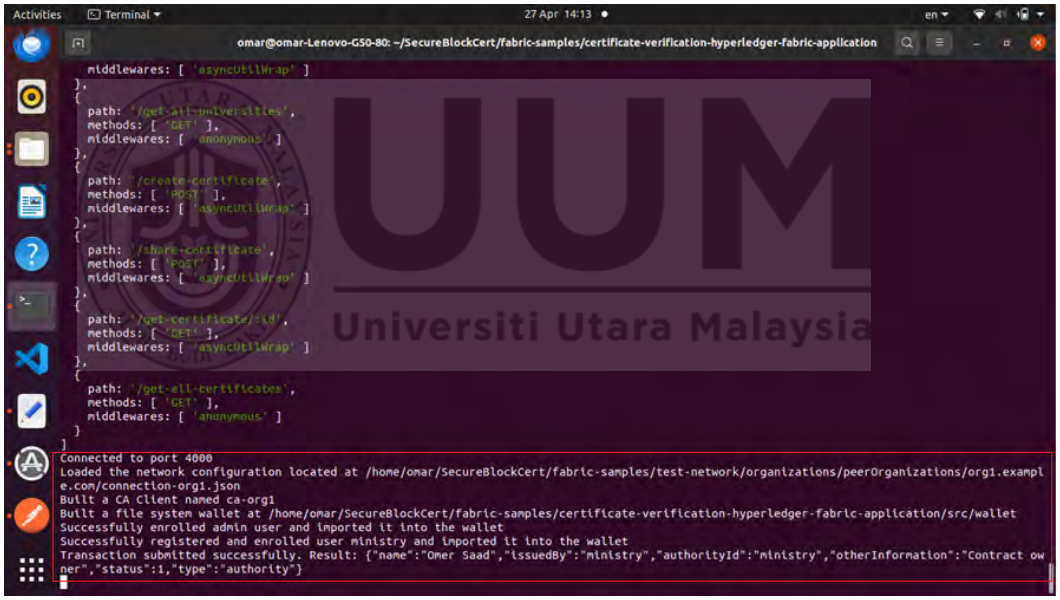

Figure 5. 9 Screenshot A successful Transaction History API tested in

5.4 Evaluation of SecureBlockCert Framework

This section presents the evaluation and deployment of the SecureBlockCert framework, using the methodologies outlined in Chapter 3. The evaluation includes expert reviews, security verification, privacy auditing, integration testing, and performance analysis to assess the framework's capabilities.

a) **Expert Review Evaluation**: Blockchain experts specializing in security and privacy reviewed SecureBlockCert's design, protocols, and privacy features. Their feedback was instrumental in refining the framework and enhancing its resilience against potential vulnerabilities.

b) **Security Verification**: The Tamarin Prover, a tool for protocol verification, was employed to formally verify the security protocols within SecureBlockCert, confirming their robustness against various threats.

c) **Privacy Auditing**: A privacy audit assessed SecureBlockCert's ability to maintain confidentiality, data integrity, and regulatory compliance throughout the certificate lifecycle.

d) **Hyperledger Fabric Integration**: Implementing SecureBlockCert within Hyperledger Fabric enabled a proof-of-concept prototype, showcasing the framework's capabilities in a controlled environment.

e) **Performance Analysis**: Key performance metrics, such as latency and throughput, were analyzed to establish a benchmark for scalability and efficiency under varying load conditions.

5.4.1 Verification through Expert Reviews

The primary aim of the verification process in this study is to ensure the SecureBlockCert framework's security and privacy features function as intended. Experts with extensive experience in blockchain technology, security protocols, and privacy measures were carefully selected based on criteria outlined in previous research [89],[103]. These criteria, discussed in detail in Chapter 3, were instrumental in identifying the most qualified individuals to assess our framework.

Out of thirteen experts initially contacted, six agreed to participate in the verification process for SecureBlockCert. Online and face-to-face meetings were arranged, with

all six experts attending the review sessions. Table 5.2 provides a summary of the experts' backgrounds.

The review sessions involved the following activities:

a) **Overview of the Study**: The researcher provided an overview of the study, including the steps involved in the verification of the SecureBlockCert framework.

b) **Framework Analysis**: Experts, leveraging their specialized knowledge in blockchain, security, and privacy, examined the security and privacy techniques integrated into the SecureBlockCert framework. The researcher was available to provide clarifications as required.

c) **Expert Feedback**: Each expert offered feedback on the accuracy and robustness of the security and privacy techniques within the SecureBlockCert framework, providing insights and observations based on their expertise.

d) **Framework Revisions**: Following the review, the researcher incorporated the experts' recommendations into the SecureBlockCert framework, enhancing its compliance with security and privacy requirements based on the constructive feedback received.

Feedback from the experts affirmed the SecureBlockCert framework's potential to enhance digital credential security and privacy. The framework's approach to cryptography, verification, and ease of use received positive responses. Table 5.3 summarizes the results of Results for the SecurBlockcert Verification.

Table 5. 2 Experts' Background

ID	Qualifications	Expertise	Years of Experience	Institutions
Expert A	Ph.D.	Blockchain, Privacy Preservation	22	Asia Pacific University of Technology and Innovation (APU), Malaysia

Expert B	Ph.D.	Blockchain , Data Science Machine learning, Software reliability	30	Galgotias University- India
Expert C	Ph.D.	Cryptography, Data Security, Cloud Computing, Image Encryption	25	University of Technology- Iraq
Expert D	Ph.D.	Information Security, Cloud Computing	15	University of Technology- Iraq
Expert E	Ph.D.	Blockchain, Information Security	25	School of Information Technology and Engineering, Vellore Institute of Technology, Vellore
Expert F	Ph.D.	Blockchain, Cybersecurity, Reverse Engineering, Malware Analysis	20	Princess Sumaya University for Technology, Jordan

Table 5. 3 Results for the SecurBlockcert Verification

Steps	**Expert A**	**Expert B**	**Expert C**	**Expert D**	**Expert E**	**Expert F**
The framework's objectives and methodologies are articulated clearly and unambiguously.	Agree	Agree	Agree	Agree	Agree	Agree
The framework accurately addresses the security and privacy concerns of the digital certificate	Agree	Agree	Agree	Agree	Agree	Agree

system on the block chain.						
The framework is logically structured and easy to navigate.	Agree	Agree	Agree	Agree	Agree	Agree
The framework introduces novel approaches to enhancing the security and privacy of block chain-based digital certificates.	Agree	Agree	Agree	Agree	Agree	Agree

Table 5. 4 Overall Comments of The Experts Regarding the Proposed Framework

Overall Comments
Expert A: The framework clearly outlines the objectives (enhancing security and privacy of digital credentials on the block chain) and proposes methodologies (ECC for authentication, HE for privacy, and access control). It is well-organized and easy to follow. The framework addresses security concerns through authentication and access control mechanisms. It tackles privacy concerns through homomorphic encryption.

Expert B: You have pinpointed digital credential issues and privacy concerns as key elements to secure the ledger, which is of paramount importance in the context of emerging technological fields. To address these challenges, You proposed the use of elliptic curve cryptography, which is well-suited for enhancing security within the narrow constraints of block chain technology.

The Tamarin prover, recognized for its utility in security protocol verification, will be employed to rigorously assess the integrity of the security enhancements we have introduced into the blockchain framework. Its application is indeed timely and aligns with contemporary needs for robust security verification tools.

Expert C: SecureBlockCert effectively utilizes blockchain technology to provide a secure and transparent solution for verifying academic credentials. The platform's focus on authenticity and tamper-proof records is commendable and addresses a significant need in the academic and professional communities

Expert D: The proposed framework appears clear and comprehensive, addressing security and privacy concerns in the blockchain-based digital certificates system. Its logical organization facilitates easy navigation

Expert E: SecureBlockCert's implementation of robust homomorphic encryption and access control mechanisms is pivotal in ensuring data security and integrity. By employing granular access controls and authentication protocols, the platform limits access to authorized users only, reducing the risk of unauthorized data manipulation or breaches.

Expert F: the proposed framework proposes ambitious and technologically advanced approaches to secure digital credentials on the block chain.

5.4.2 Formal Security Analysis

To verify that SecureBlockCert's security protocols are robust against potential vulnerabilities, the Tamarin Prover was used for formal verification. Tamarin is a specialized tool for analyzing and verifying security protocols within a symbolic model, allowing rigorous testing of protocol resilience against various threats. This section details the process of modeling and verifying the security properties of SecureBlockCert using Tamarin Prover, including protocol representation, lemma definition, and verification results.

5.4.2.1 Protocol Modelling and Representation

In Tamarin, security protocols are represented as multiset rewriting rules that define the interactions between entities and the conditions under which these interactions occur. Each rule specifies an initial state (preconditions), an observable action, and a resulting state (post conditions) after the action is executed. The SecureBlockCert protocol involves multiple key steps, such as nonce generation, key exchange, and digital certificate issuance, which are essential for ensuring secure communications.

For example, the key exchange process between an initiator (e.g., student) and responder (e.g., verifier) can be represented by rules as follows:

a) **Initiation**: The initiator sends a nonce N to the responder to request a secure session:

$$Initiate\_I \rightarrow Sent\_I(N)$$

b) **Acknowledgment**: The responder acknowledges with a response, potentially including a session key K for secure communication:

$$Sent\_I(N) \rightarrow Acknowledged\_R(N, K)$$

5.4.2.2 Security Properties as Lemmas

To formally verify the security properties of the protocol, key attributes such as Nonce Secrecy and Injective Agreement are defined and validated as lemmas. These properties ensure confidentiality, integrity, and resistance to replay attacks, forming the foundational security guarantees of the framework.

a) **Nonce Secrecy**: Ensures that any nonce N generated within the protocol remains confidential and cannot be accessed by unauthorized entities. The secrecy lemma is defined as follows:

$$\forall N: Nonces(N) \Rightarrow \neg(Reveal(N) \wedge Attacker(N))$$

This lemma guarantees that the nonce N cannot be observed by an attacker, preserving the confidentiality of each session.

b) **Injective Agreement:** Ensures that both the initiator and responder agree on the data exchanged (e.g., nonce N and session key K), confirming that the interaction is uniquely associated with a specific protocol instance:

$$\forall N, K: Agreed(I, R, N, K) \Rightarrow Fresh(N)$$

This property ensures that nonce N is unique and fresh, mitigating replay attacks and preserving the integrity of the key exchange.

5.4.2.3 Temporal Properties for Authentication

Authentication properties are critical to ensure that the protocol steps occur in a specific sequence. Using temporal logic, we ensure that each message is exchanged in the correct order. For instance, the initiator should only accept a response from the responder after sending the initial request. This property is represented as:

$$\forall I, R, M: Sent(I, M) \Rightarrow \Diamond Received(R, M)$$

The temporal operator (◇) specifies that if the initiator sends a message M, there must exist a future state where the responder receives it, preserving the protocol's intended flow.

5.4.2.4 Verification Process and Results

Each protocol rule and lemma was encoded in Tamarin using a .spthy file, which defines the symbolic model for SecureBlockCert. Tamarin's verification process explores all possible protocol traces, checking whether each trace satisfies the specified safety properties.

a) **Verified Properties:** For each lemma, Tamarin confirmed that the SecureBlockCert protocol adheres to the defined security properties, such as nonce secrecy and injective agreement.

b) **Counter examples and Protocol Refinement:** During testing, Tamarin identified areas for refinement in the initial protocol design. By addressing these counterexamples, we enhanced the protocol's resilience against potential attack vectors.

The successful verification demonstrates that the SecureBlockCert protocol meets its security objectives, ensuring robust protection against unauthorized access, replay attacks, and confidentiality breaches. This formally verified protocol can now be confidently integrated into the blockchain-based framework, supporting a secure and private infrastructure for managing digital credentials. Figure 5.10 illustrates the steps involved in the Tamarin Prover setup and verification process.

1. **Initialize Public Key Infrastructure:**
   - Generate a long-term key-pair for each participant $(ltk_A, pk(ltk_A))$.
   - Register public keys $(pk(ltk_A))$ to a public directory.
2. **Initiator (I) Starts Protocol:**
   - Generate a fresh nonce (ni).
   - Encrypt a message $('1', ni, I)$ with the responder's public key (pk_R).
   - Send the encrypted message $(m1)$ to the responder.
   - Enter state St_I_1.
3. **Responder (R) Receives Message:**
   - Decrypt $m1$ using their long-term key (ltk_R).
   - Generate a fresh nonce (nr).
   - Encrypt a message $('2', ni, nr)$ with the initiator's public key (pk_I).
   - Send the encrypted message $(m2)$ to the initiator.
   - Enter state St_R_1.
4. **Initiator (I) Receives Message:**
   - Decrypt $m2$ using their long-term key (ltk_I).
   - Encrypt a message $('3', nr)$ with the responder's public key (pk_R).
   - Send the encrypted message $(m3)$ to the responder.
   - Establish shared secrets (ni, nr) with the responder.
5. **Responder (R) Receives Message:**
   - Decrypt $m3$ using their long-term key (ltk_R).
   - Establish shared secrets (ni, nr) with the initiator.

Figure 5. 10 Steps of Tamarin Prover

The results generated from the security protocol are given in Figure 5.11.

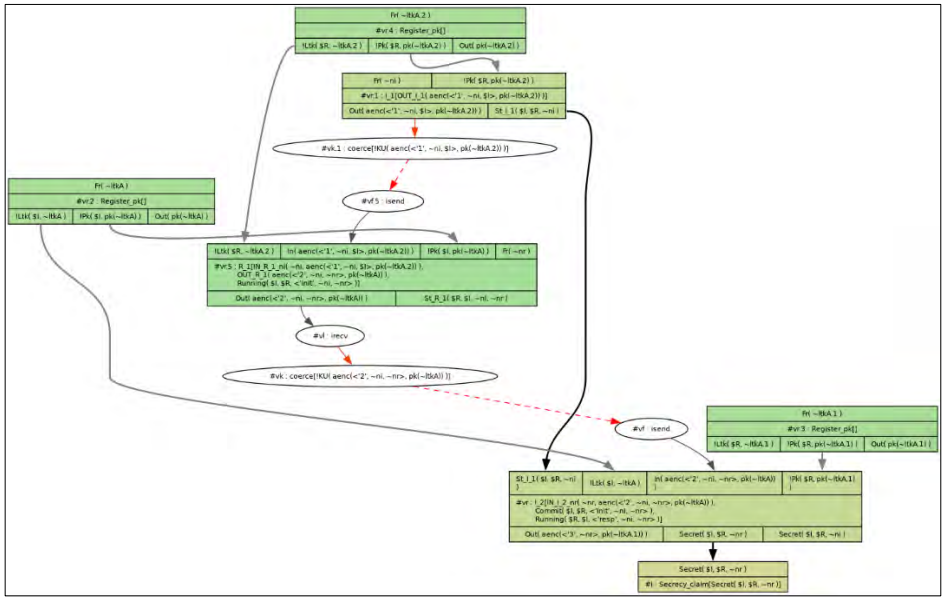

Figure 5. 11 Generated results of Security protocol by Tamarin Prover

The visualization produced by the Tamarin Prover is intuitively structured, presenting a bifurcated graph that uses green and red arrows for clear differentiation. Green arrows represent successfully executed protocol steps, indicating compliance with designated security properties. These paths highlight sequences within the protocol that conform to expected security standards, demonstrating secure and verified transactions or exchanges. In contrast, red arrows identify potential vulnerabilities or breaches in security properties, signaling instances where the protocol deviates from the ideal. These paths reveal areas of weakness, indicating conditions under which the security measures may fail or could be exploited. This color-coded graph enables security analysts to quickly detect and diagnose areas of concern. The distinct segmentation allows for focused analysis green paths confirm functional adequacy, while red paths spotlight vulnerabilities that warrant further investigation and rectification. The delineation of successful and problematic pathways provided by the Tamarin Prover graph is instrumental in refining the security protocol. This efficient and comprehensive assessment ensures that robustness and reliability are integral to the finalized protocol design.

5.5 Experimental Results and Performance Analysis of SecureBlockCert

This section presents a comprehensive evaluation of the SecureBlockCert prototype's performance in managing the issuance, sharing, and verification of educational credential certificates. Focusing on two key performance metrics throughput and latency we assess the framework’s responsiveness and scalability across various transaction loads and operational scenarios. This analysis provides insights into SecureBlockCert's practical application in real-world settings.

To simulate typical demands in the digital credential lifecycle, we established test scenarios that include generating new certificates, sharing certificates between entities,

and processing real-time verification requests. These scenarios mirror common system usage, such as handling large transaction volumes during peak certificate issuance events or processing verification requests from third-party organizations. Each scenario was tested to evaluate the framework's ability to manage concurrent operations effectively.

5.5.1 Experimental Setup and Methodology

The experiments were conducted using Hyperledger Caliper as the benchmarking tool. Hyperledger Caliper enables realistic simulation by generating representative transaction loads for SecureBlockCert's blockchain network. Transactions were submitted by a distributed set of independent workers, ensuring an unbiased and realistic transaction distribution.

To account for potential variances due to environmental or network factors, each test was run four times, and the results were averaged to establish a consistent baseline for performance evaluation. This approach aligns with best practices in benchmarking blockchain systems, as detailed by previous studies [104].

5.5.2 Performance Metrics

The performance analysis focused on two critical metrics:

a) **Throughput**: This metric quantifies the number of transactions SecureBlockCert can process within a given timeframe. Throughput is particularly crucial in high-volume scenarios, such as during large-scale certificate issuance after graduation ceremonies or during peak enrollment periods [104].

b) **Latency**: Latency represents the time taken for a single transaction to complete. Low latency is essential for real-time certificate verification, where

immediate response times are expected by end users, particularly in environments that demand quick credential validation [56].

5.5.3 Results and Discussion

The following analysis examines SecureBlockCert's performance under varied conditions, demonstrating its capability to support digital credential management's operational demands effectively. The results highlight the system's responsiveness and scalability, confirming its suitability for large-scale, real-world applications.

a) **Throughput Analysis**: The throughput results indicate that SecureBlockCert can efficiently handle high transaction volumes, even during peak periods. This performance is consistent with expectations for blockchain-based credential management systems that must accommodate large-scale issuance and verification demands.

b) **Latency Analysis:** The latency results demonstrate the system's responsiveness, with transaction completion times within acceptable limits for real-time verification. This confirms that SecureBlockCert meets the necessary criteria for prompt, efficient verification processes in high-demand educational settings.

The findings from these experiments collectively validate the SecureBlockCert framework as a robust and scalable solution for digital credential management, effectively balancing throughput and latency to support extensive usage in educational institutions.

5.6 Comparative Analysis with Related Studies

This section evaluates the performance of the SecureBlockCert Framework in comparison to related studies that utilize Hyperledger Fabric for network latency and

throughput assessments under varying transaction loads. By analyzing these benchmarks, we position SecureBlockCert within the broader context of blockchain-based credential management.

5.6.1 Benchmark Configurations

Four studies are considered for comparison, with transaction rate configurations as follows:

a) Litoussi et al. [61]: Conducted experiments at transaction loads of 100, 200, 500, and 1000 transactions per second (tps).

b) Leka and Selimi [60]: Tested network performance at higher rates, including 2000, 4000, 6000, and 8000 tps.

c) Rama Reddy et al. [2]: Examined network behavior under lower transaction loads of 10, 30, and 50 tps.

d) Chaniago et al. [67]: Explored intermediate rates of 50, 100, 200, 300, 400, and 500 tps.

To enable a direct comparative analysis, the SecureBlockCert Framework was tested using these same transaction rate configurations in both reading and writing modes, providing consistency and validity for performance evaluation.

5.6.2 Performance Metrics

The analysis focuses on two key metrics:

a) **Throughput**: Defined as the number of successful transactions processed per second, throughput is critical for evaluating the framework's efficiency under high-demand conditions.

b) **Latency**: Defined as the time elapsed from transaction submission to confirmation, latency provides insights into the system's responsiveness, particularly at higher transaction rates.

These metrics are critical for assessing the scalability and efficiency of SecureBlockCert in handling real-world educational credentialing scenarios.Table 5.5 presents the experimental parameter configuration for all tests conducted in this study, ensuring consistency with the transaction rate configurations observed in related studies.

Table 5. 5 Experimental Parameter Configuration

Experiment	Configuration	Workers	Test Duration (sec)	Rounds	Transaction Load per Round	Transactions Mode	Network Size	Varied Factor
Experiment 1	Configuration 1	1	60	4	100 , 200 , 500 , 1000	Read	1 channel, 2 organizations, 2 peers/organization , 1 orderer, 1 CA/organization.	Block time
	Configuration 2	1	60	4	100 , 200 , 500 , 1000	write	1 channel, 2 organizations, 2 peers/organization , 1 orderer, 1 CA/organization.	Block time
Experiment 2	Configuration 1	1	60	4	2000 , 4000, 6000 , 8000	Read	1 channel, 2 organizations, 2 peers/organization , 1 orderer, 1 CA/organization.	Block time
	Configuration 2	1	60	4	2000 , 4000, 6000 , 8000	write	1 channel, 2 organizations, 2 peers/organization , 1 orderer, 1 CA/organization.	Block time

Table 5.5 continued.

	Configuration 1	1	60	4	10 , 30 , 50	Read	1 channel, 2 organizations, 2 peers/organization, 1 orderer, 1 CA/organization.	Block time
Experiment 3								
	Configuration 2	1	60	4	10 , 30 , 50	write	1 channel, 2 organizations, 2 peers/organization, 1 orderer, 1 CA/organization.	Block time
	Configuration 1	1	60	4	50 , 100 , 200 , 300 , 400 , 500	write	1 channel, 2 organizations, 2 peers/organization, 1 orderer, 1 CA/organization.	Block time
Experiment 4								
	Configuration 2	1	60	4	50 , 100 , 200 , 300 , 400 , 500	write	1 channel, 2 organizations, 2 peers/organization, 1 orderer, 1 CA/organization.	Block time

5.6.3 Results and Discussion

Experiment 1: Fixed Rate Reading and Writing Performance on [100, 200, 500, and 1000]

The principal objective of this experiment is to quantify the reading and writing performance of the SecureBlockCert Blockchain framework at predetermined transaction rates. This evaluation intends to provide an understanding of how the system handles consistent operational loads, reflecting capacity and scalability. The fixed rates chosen for this experiment 100, 200, 500, and 1000 transactions per second (tps) are identical to the transaction rates applied in the study, facilitating direct performance comparisons. The experiment is conducted in two distinct modes to comprehensively assess the framework's capabilities:

a) **Reading Mode:** we measure the performance of the SecureBlockCert when retrieving credentials from the ledger. This simulates scenarios such as verification requests from employers or educational institutions seeking to confirm the validity of presented certificates.

b) **Writing Mode:** In this mode, the focus is on the SecureBlockCert Blockchain's throughput in terms of recording new credentials or updates to existing ones. This is indicative of the system's capacity to manage batch processing of credentials, akin to the end-of-term graduation certification process. A comprehensive summary of the results of this experiment can be found in Table 5.6 and 5.7.

Table 5. 6 Summary of the Results for SecureBlockCert Blockchain Reading Mode on Fixed Send Rates [100, 200, 500, 1000]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
100	6001	0	100	0.36	0.01	0.02	100
200	8871	0	147.9	0.41	0.01	0.02	147.8
500	8987	0	149.8	0.45	0.01	0.02	149.8
1000	9037	0	150.6	0.47	0.01	0.02	150.6

Reading Mode Performance Analysis of Experiment 1

The performance of the SecureBlockCert Blockchain was assessed across varying fixed send rates (100, 200, 500, and 1000 transactions per second (TPS)), providing insights into its throughput and latency behavior. The results, summarized in Table 5.6 and depicted in Figures 5.12 and 5.13, highlight both the strengths and limitations of the system under different transaction loads.

Throughput Analysis

As shown in Figure 5.12, throughput scales linearly with the send rate up to a point. At lower send rates (100 and 200 TPS), the throughput closely matches the send rate, reaching 100 TPS at a send rate of 100 TPS and approximately 148 TPS at a send rate of 200 TPS. However, as the transaction rate increases to 500 and 1000 TPS, the throughput plateaus around 150 TPS, signaling a performance cap in the system's ability to handle higher transaction loads. This throughput limit suggests a bottleneck, likely due to either processing limitations or resource constraints within the blockchain framework.

This plateaued throughput at higher send rates implies that the SecureBlockCert Blockchain can efficiently handle moderate transaction volumes but may require further optimization or scaling mechanisms to sustain performance under heavy loads.

Latency Analysis

The latency trends, as depicted in Figure 5.13, further illustrate the system's stability and efficiency:

Maximum Latency: As the send rate increases from 100 to 1000 TPS, the maximum latency grows modestly from 0.36 seconds to 0.47 seconds. This slight increase indicates that while the system is impacted by higher loads, it maintains a reasonable maximum latency, preventing excessive delays even at peak transaction rates.

Minimum Latency: The minimum latency remains consistently low at 0.01 seconds across all send rates, highlighting the system's capability for near-instantaneous responses in certain scenarios. This stability in minimum latency is crucial for applications requiring real-time or low-latency responses.

Average Latency: The average latency remains steady at 0.02 seconds regardless of the transaction rate. This consistency demonstrates the framework's efficient processing capability and ensures a stable user experience under varying loads.

The SecureBlockCert Blockchain exhibits reliable performance at lower to moderate transaction loads, with stable average latency and minimal delay increases as transaction rates rise. However, the plateau in throughput at higher send rates (500 and 1000 TPS) suggests that the system may require additional scalability improvements to accommodate higher transaction volumes. Despite this limitation, the low and stable average latency across all tested rates demonstrates efficient read operations, which is critical for real-time applications in credential verification or educational platforms.

Overall, the performance evaluation indicates that SecureBlockCert Blockchain is well-suited for environments with moderate transaction loads, maintaining a consistent and low-latency experience. However, to address scalability needs in high-volume

scenarios, further optimization may be necessary to improve throughput beyond the observed 150 TPS threshold.

Table 5. 7 Summary of the Results for SecureBlockCert Blockchain Writing Mode on Fixed Send Rates [100, 200, 500, 1000]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
100	6001	0	100	0.6	0.01	0.04	100
200	7999	0	133.3	0.62	0.02	0.04	133.3
500	8056	0	134.3	0.83	0.02	0.05	134.2
1000	8025	0	133.8	0.75	0.02	0.05	133.7

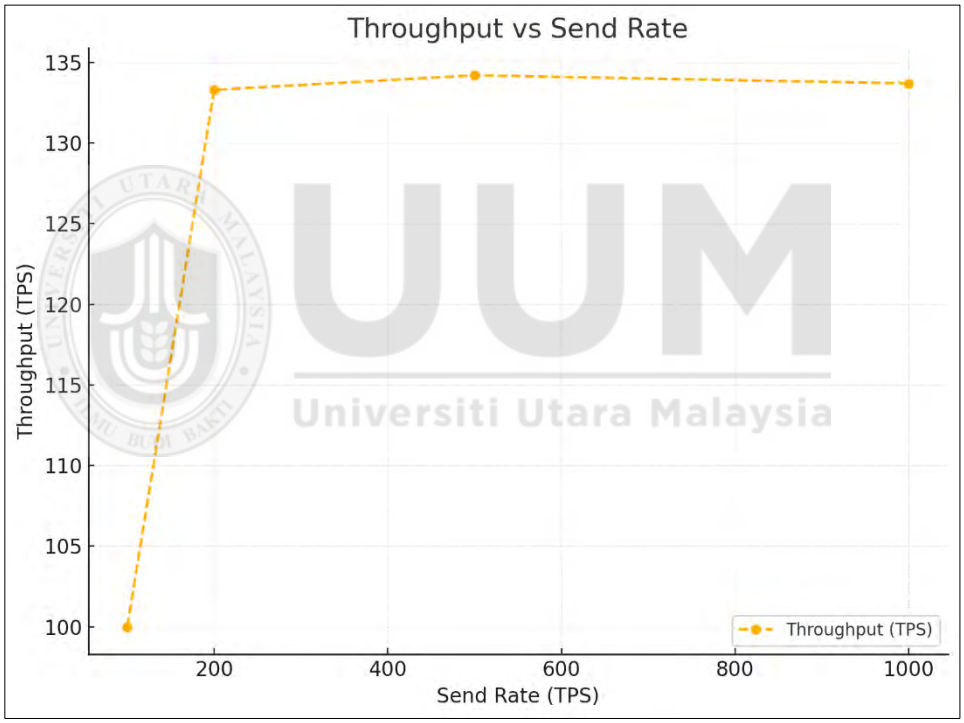

Figure 5. 12 Throughput vs. Send Rate at Reading Mode of Experiment 1

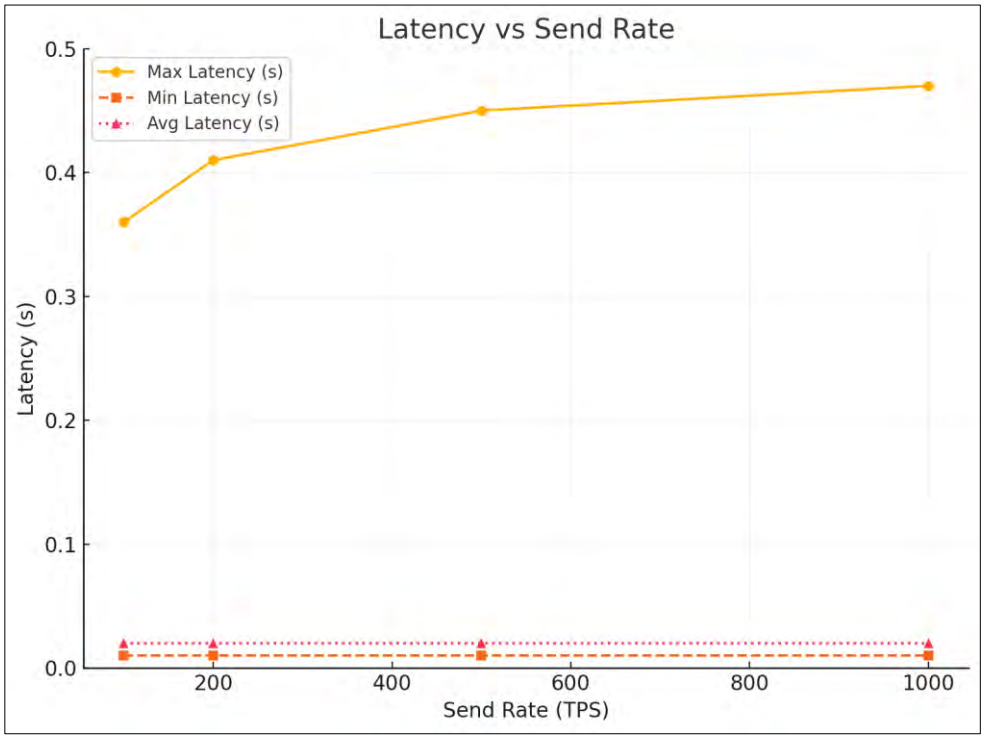

Figure 5. 13 Latency vs send rate at Reading Mode of Experiment 1

Writing Mode Performance Analysis of Experiment 1

The performance of the SecureBlockCert Blockchain in writing mode was evaluated under varying fixed send rates (100, 200, 500, and 1000 transactions per second (TPS)), as summarized in Table 5.7 and illustrated in Figures 5.14 and 5.15. These results offer insights into how the system handles different transaction loads in writing operations.

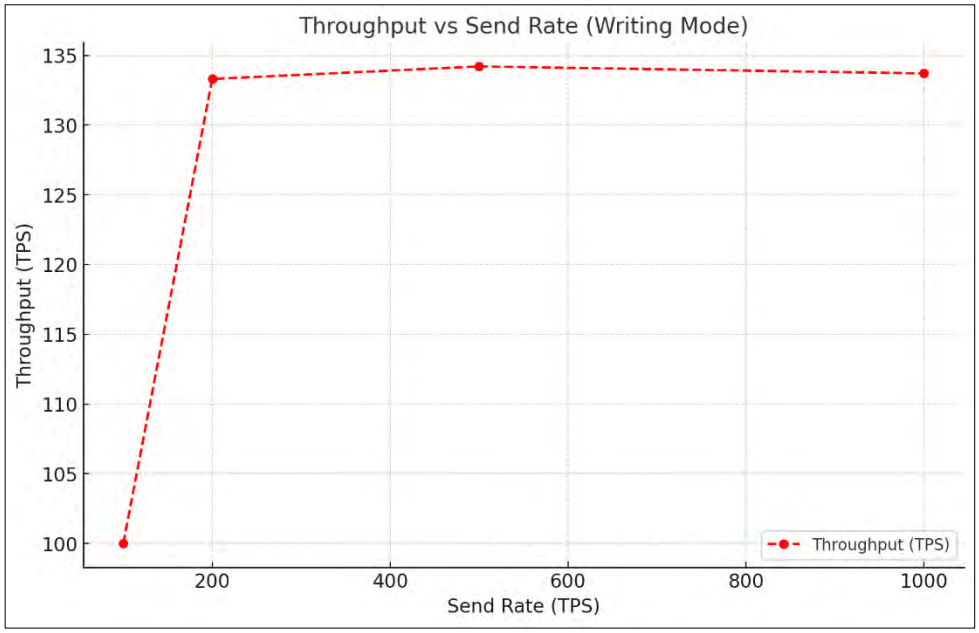

Figure 5. 14 Throughput vs. Send Rate at Writing Mode of Experiment 1

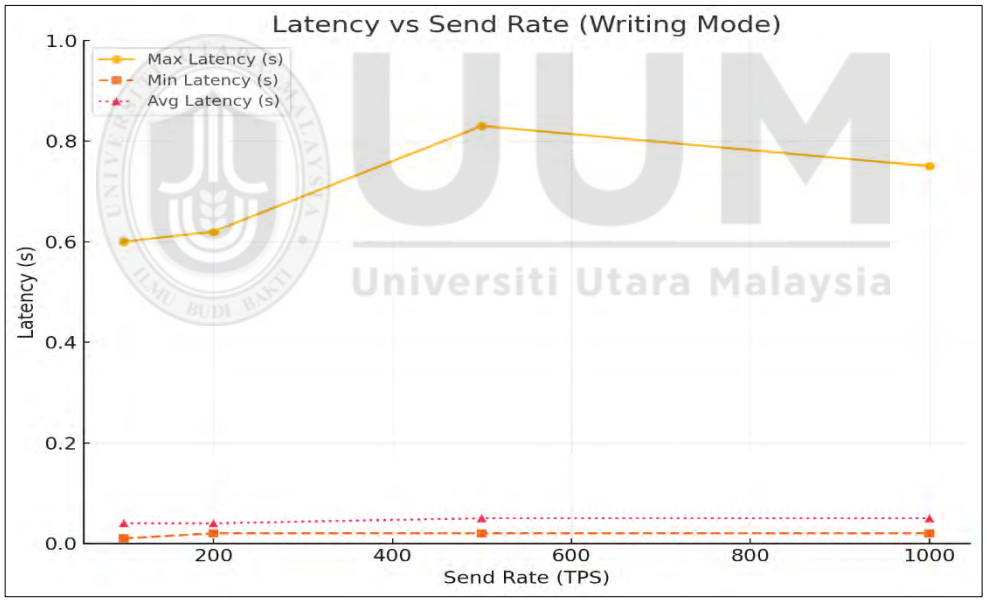

Figure 5. 15 Latency vs. Send Rate at Writing Mode of Experiment 1

Throughput Analysis

As shown in Figure 5.14**,** the throughput in writing mode scales with the send rate at lower levels, matching the send rate at 100 TPS and increasing to approximately 133 TPS at 200 TPS. However, the throughput stabilizes around 134 TPS at higher send rates (500 and 1000 TPS). This plateau suggests that the system reaches its processing

limit for writing transactions around 134 TPS, which is consistent across higher load conditions.

This capped throughput at higher send rates indicates that, while the system performs reliably under moderate transaction loads, further optimization may be necessary to achieve higher throughput for writing operations if increased demand is anticipated.

Latency Analysis

Latency trends, depicted in Figure 5.15**,** reveal the following:

a) **Maximum Latency**: The maximum latency slightly increases as the send rate rises, from 0.6 seconds at 100 TPS to 0.83 seconds at 500 TPS, before dropping to 0.75 seconds at 1000 TPS. This pattern indicates that while the system experiences an increase in delay under higher loads, it remains within reasonable limits for writing operations.

b) **Minimum Latency**: Minimum latency is consistently low at 0.01–0.02 seconds across all send rates, demonstrating the system's ability to maintain quick responses for some transactions, even under heavy loads.

c) **Average Latency**: The average latency is stable, remaining around 0.04 seconds at lower send rates (100 and 200 TPS) and slightly increasing to 0.05 seconds at higher send rates (500 and 1000 TPS). This consistent average latency indicates that while there is a minor increase in response times as load intensifies, the framework effectively maintains efficient processing across different load conditions.

The SecureBlockCert Blockchain demonstrates stable performance in writing mode under moderate to high transaction rates, with steady throughput and minimal latency fluctuation. The observed throughput limit at 134 TPS suggests that the system is

optimized for moderate loads and may need additional scaling strategies to handle higher volumes efficiently. However, the consistent average latency of 0.04–0.05 seconds across different loads is a positive indicator, showing that the framework can reliably manage write operations without significant delays.

Experiment 2: Fixed Rate Reading and Writing Performance Analysis [2000, 4000, 6000, 8000]

In Experiment 2, the SecureBlockCert Blockchain framework was evaluated for its performance under high fixed rates of 2000, 4000, 6000, and 8000 transactions per second (TPS) for both reading and writing transactions. The goal was to examine how the framework handles significantly increased transaction volumes, with results summarized in Tables 5.8 and 5.9 and illustrated in Figures 5.16 and 5.17 for reading mode, and Figures 5.18 and 5.19 for writing mode.

Table 5. 8 Summary of the Results on Reading Mode on Fixed Rate [2000, 4000, 6000, 8000]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
2000	6001	0	100	0.78	0.01	0.03	100
4000	9253	0	154.2	1.07	0.01	0.04	154.2
6000	9316	0	155.3	1.17	0.01	0.04	155.2
8000	9323	0	155.4	1	0.01	0.03	155.4

Table 5. 9 Summary of the Results on Writing Mode on Fixed Rate [2000, 4000, 6000, 8000]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
2000	6001	0	100	0.94	0.01	0.04	100
4000	8000	0	133.3	1.32	0.02	0.05	133.3
6000	8088	0	134.8	1.26	0.02	0.05	134.8
8000	8061	0	134.4	1.23	0.02	0.06	134.2

Reading Mode Performance Analysis of Experiment 2

Throughput: As seen in Figure 5.16, the throughput remains capped around 155 TPS for reading mode across higher send rates of 4000, 6000, and 8000 TPS. This plateau suggests that the system's processing limit for read transactions maxes out at around 155 TPS, indicating a scalability constraint at high transaction rates.

Latency: In Figure 5.17, maximum latency increases from 0.78 seconds at a 2000 TPS send rate to 1.17 seconds at 6000 TPS, before reducing slightly to 1.0 seconds at 8000 TPS. The minimum latency remains steady at 0.01 seconds across all rates, while average latency fluctuates between 0.03 and 0.04 seconds. These results imply that the framework handles high transaction volumes with relatively consistent performance, although maximum latency can spike under peak loads. The capped throughput and modest increases in latency suggest that while the SecureBlockCert Blockchain can handle moderate loads efficiently in reading mode, its performance could be further optimized to support larger transaction volumes.

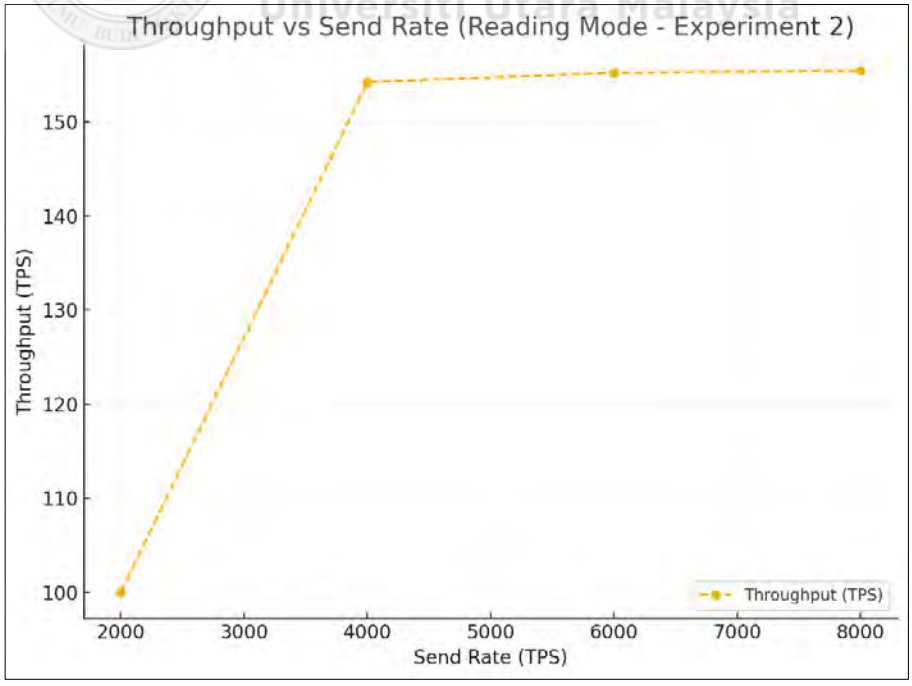

Figure 5. 16 Throuput vs. Send Rate at Reading Mode of Experiment 2

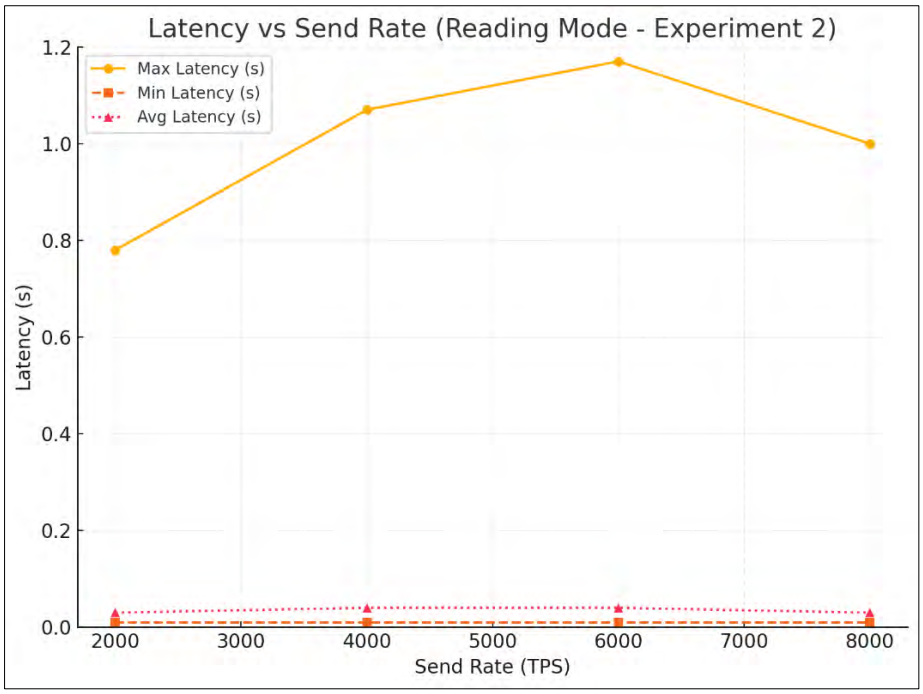

Figure 5. 17 Latency vs. Send Rate at Reading Mode Experiment 2

Writing Mode Performance Analysis of Experiment 2

In writing mode, the SecureBlockCert Blockchain framework's performance was evaluated at fixed transaction rates of 2000, 4000, 6000, and 8000 TPS. The results highlight key insights into the system's handling of high transaction volumes during write operations.

Throughput

As shown in the table**,** throughput increases with the send rate but reaches a plateau at around 134 TPS. At the lowest rate of 2000 TPS, the system achieves a throughput of 100 TPS. However, as the send rate increases to 4000, 6000, and 8000 TPS, throughput stabilizes between 133.3 and 134.8 TPS. This consistency in throughput across higher rates indicates that the framework hits a performance ceiling in writing mode, suggesting a scalability limit for handling write-heavy workloads at higher transaction rates.

a) **Maximum Latency**: The maximum latency gradually increases from 0.94 seconds at 2000 TPS to 1.32 seconds at 4000 TPS, then reduces slightly to 1.23 seconds at 8000 TPS. This fluctuation suggests that the system can manage high write loads relatively well, although it experiences temporary latency spikes under the initial increase in load.

b) **Minimum Latency**: Minimum latency remains consistent at 0.01 seconds at 2000 TPS, rising slightly to 0.02 seconds at higher send rates. This low minimum latency indicates that the system can process some transactions quickly, even under higher loads.

c) **Average Latency**: The average latency shows a slight upward trend, moving from 0.04 seconds at 2000 TPS to 0.06 seconds at 8000 TPS. This minor increase suggests that while the system maintains relatively stable performance for most transactions, higher loads lead to a gradual increase in processing time.

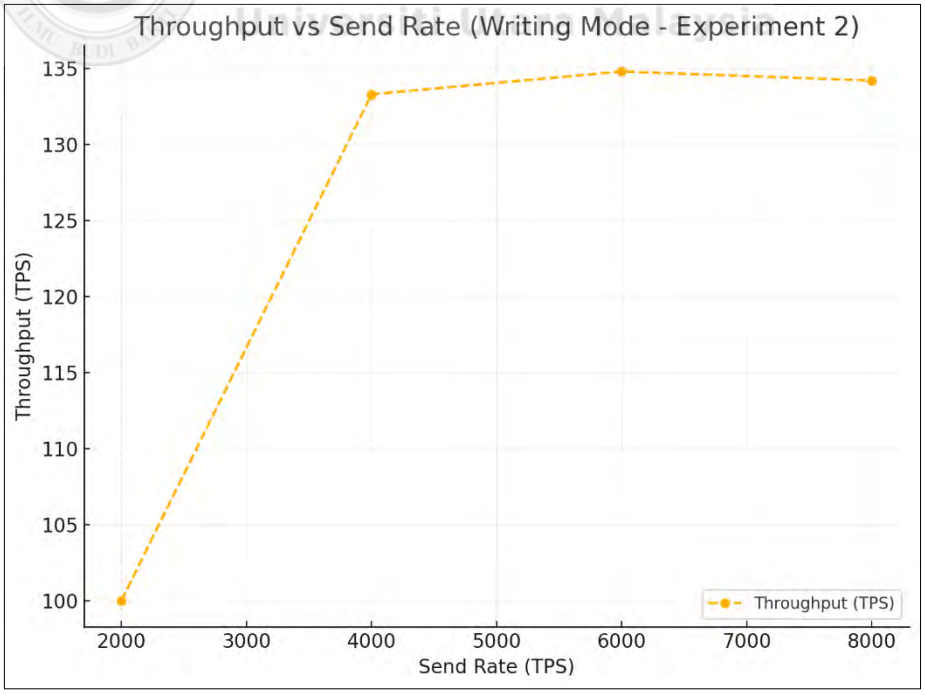

Figure 5. 18 Throuput vs. Send Rate at Writing Mode Experiment 2

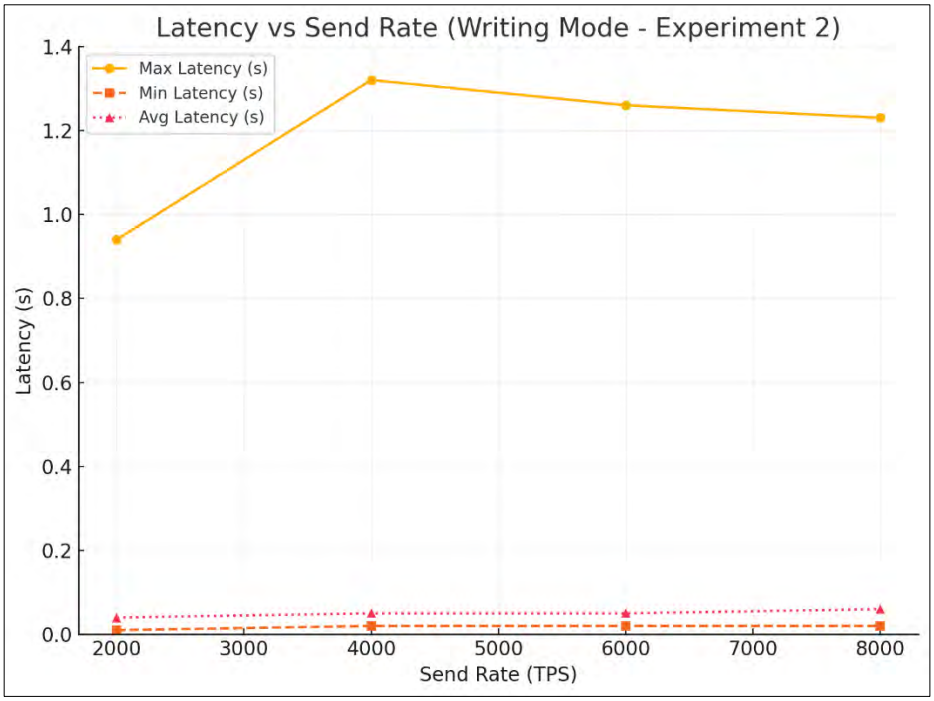

Figure 5. 19 Latency vs. Send Rate at Writing Mode Experiment 2

Experiment 3: Fixed Rate Reading and Writing Performance on [10, 30, 50, 100]

In this experiment, the SecureBlockCert Blockchain was evaluated under lower fixed transaction rates (10, 30, and 50 TPS) to examine the framework's performance in both reading and writing modes. The results, detailed in Tables 5.10 and 5.11 and illustrated in Figures 5.20 through 6.23, offer insights into the system's efficiency at handling lower loads.

Table 5. 10 Summary of the Results on Reading Mode on Fixed rate [10,30,50]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
10	6001	0	100	0.99	0.01	0.03	100
30	8909	0	148.5	1.3	0.01	0.05	148.5
50	8978	0	149.6	1.51	0.01	0.04	149.6

Table 5. 11 Summary of the Results on Writing Mode on Fixed rate [10,30,50]

Fixed-rate	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
10	6001	0	100	1.63	0.01	0.06	100
30	8011	0	133.5	1.26	0.02	0.05	133.5
50	8051	0	134.2	1.67	0.02	0.06	134.1

Reading Mode Performance Analysis of Experiment 3

Throughput Analysis

In Figure 5.20, we observe that throughput scales closely with the send rate, reaching approximately 100 TPS at 10 TPS and stabilizing near 149 TPS at 30 and 50 TPS. This increase and subsequent plateau suggest that the SecureBlockCert Blockchain can effectively handle lower reading transaction loads, but it reaches an efficiency limit at around 150 TPS, even at the low end of transaction rates.

Latency Analysis: In Figure 5.21, we see that:

a) Maximum Latency increases with higher send rates, moving from 0.99 seconds at 10 TPS to 1.51 seconds at 50 TPS. This indicates that while the system can handle low loads, increased loads introduce additional delay.

b) Minimum Latency remains stable at 0.01 seconds across all send rates, showing that certain transactions are consistently processed with minimal delay.

c) Average Latency slightly fluctuates, from 0.03 to 0.05 seconds, showing that while there's a small delay with higher send rates, the system maintains efficiency in processing most reading requests.

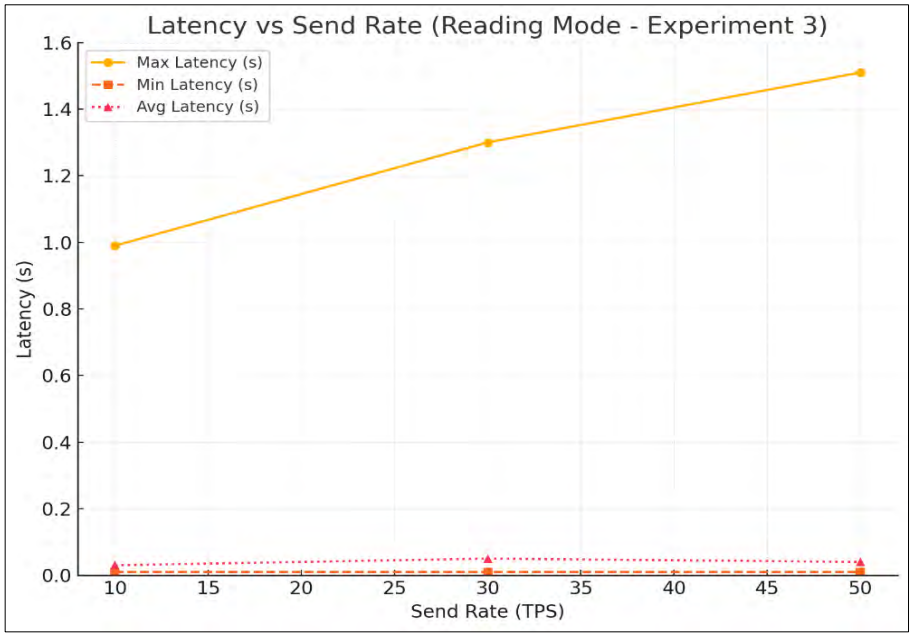

Figure 5. 20 Latency vs. Send Rate at Reading Mode of Experiment 3

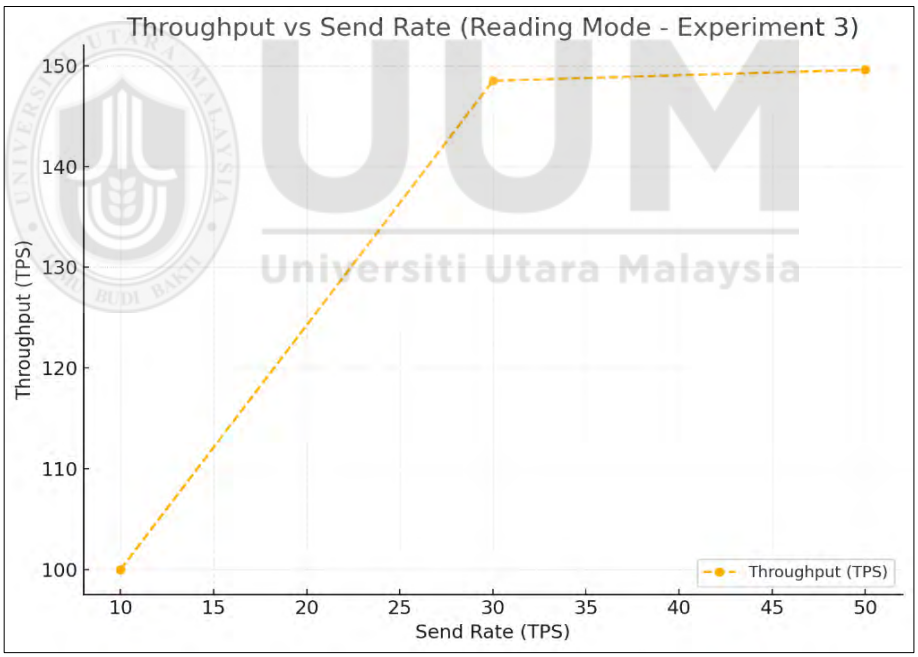

Figure 5. 21 Throughput vs. Send Rate at Reading Mode of Experiment 3

Writing Mode Performance Analysis of Experiment 3

Throughput Analysis

As shown in Figure 5.22, throughput in writing mode scales up to approximately 134 TPS at send rates of 30 and 50 TPS, suggesting a performance cap similar to that seen

in higher transaction rates in Experiment 2. This plateaued throughput implies that while the system handles lower loads effectively, it is constrained by a throughput limit, likely due to resource or processing limitations within the blockchain framework.

Latency Analysis

Figure 5.23 reveals the following trends:

a) Maximum Latency fluctuates, with an increase to 1.67 seconds at 50 TPS, highlighting that writing operations are more sensitive to load, even at these lower transaction rates.

b) Minimum Latency is slightly higher at 0.02 seconds for 30 and 50 TPS, suggesting a marginal increase in baseline processing time as transaction rates increase.

c) Average Latency remains relatively stable between 0.05 and 0.06 seconds, indicating that the system maintains consistent processing times for the majority of writing requests under low-load conditions.

Comparative Observations

a) **Throughput Limits:** The plateau observed in both reading (around 150 TPS) and writing (around 134 TPS) modes indicates that SecureBlockCert Blockchain has a consistent throughput ceiling, even at low transaction loads.

b) **Latency Trends:** Maximum latencies for writing mode are higher than those for reading mode, suggesting that writing operations require more processing time and resources, potentially due to data integrity checks or consensus overhead.

At lower transaction rates, the SecureBlockCert Blockchain framework demonstrates stable performance with low average latencies and throughput that closely follows the

send rate. The observed throughput ceilings suggest that the framework is optimized for moderate loads but has limited scalability potential. Latency trends show that both reading and writing operations can maintain low average latency, making the framework suitable for environments with predictable, moderate loads.

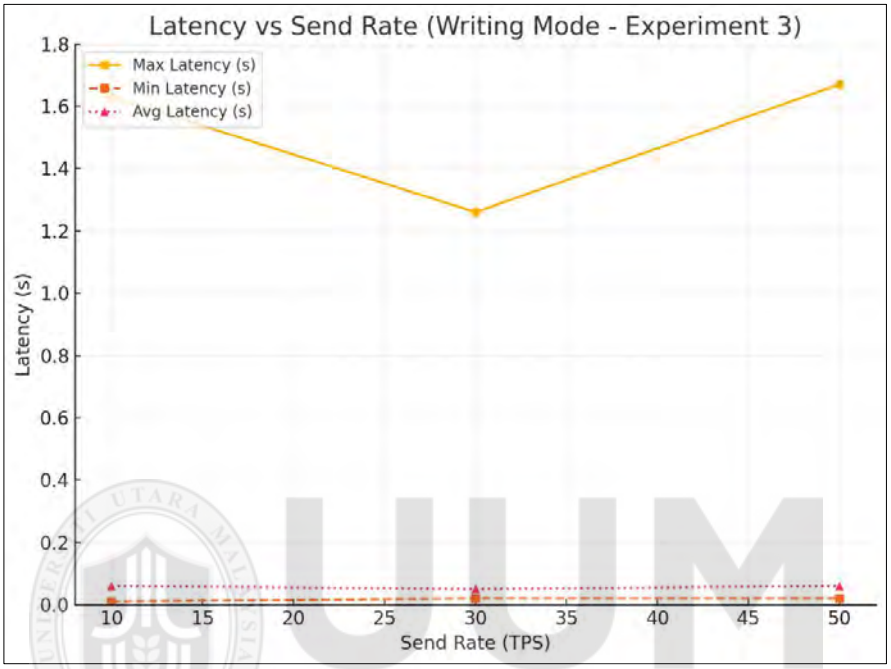

Figure 5. 22 Latency vs. Send Rate at Writing Mode of Experiment 3

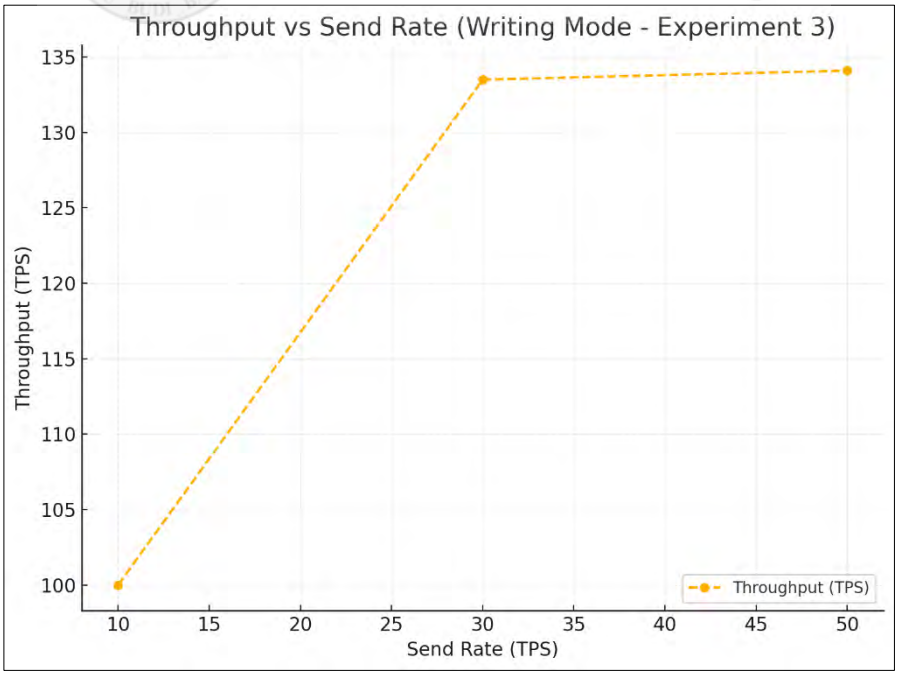

Figure 5. 23 Throughput vs. Send Rate at Writing Mode of Experiment 3

Experiment 4: Fixed Rate Reading and Writing Performance [50, 100, 200, , 300 , 400 , 500]

In this experiment, the SecureBlockCert Blockchain's performance was tested at higher fixed transaction rates (50, 100, 200, 300, 400, and 500 TPS) in both reading and writing modes. The results, summarized in Tables 5.12 and 5.13 and illustrated in Figures 6.24 through 6.27**,** provide insight into the system's scalability and efficiency under these increased loads.

Table 5. 12 Summary of the Results on Reading Mode on Fixed Rate [50, 100,200,300,400,500]

Fixed-rate(TPS)	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
50	6001	0	100	0.86	0.01	0.04	100
100	9142	0	152.4	0.13	0.01	0.02	152.3
200	9353	0	155.9	0.14	0.01	0.02	155.9
300	9270	0	154.5	0.16	0.01	0.02	154.5
400	9279	0	154.7	0.19	0.01	0.02	154.6
500	9373	0	156.2	0.3	0.01	0.02	156.2

Table 5. 13 Summary of the Results on Writing Mode on Fixed rate [150,100,200,300,400,500]

Fixed-rate (TPS)	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
50	6001	0	100	0.26	0.01	0.03	100
100	8163	0	136.1	0.2	0.02	0.04	136
200	8205	0	136.8	0.41	0.02	0.04	136.7
300	8241	0	137.4	0.41	0.02	0.04	137.3
400	8232	0	137.2	0.7	0.02	0.04	137.2
500	8239	0	137.3	0.15	0.02	0.03	137.3

Reading Mode Performance Analysis

Throughput Analysis

In Figure 5.24, we observe that throughput in reading mode scales up with the send rate but begins to plateau at approximately 156 TPS around 200 TPS and beyond. This limit suggests that the framework has an inherent throughput cap in reading mode, which restricts further scalability at higher transaction rates.

Latency Analysis

In Figure 5.25, the latency metrics reveal:

a) Maximum Latency gradually increases from 0.86 seconds at 50 TPS to 0.30 seconds at 500 TPS. This stability in maximum latency demonstrates the system's efficiency in handling reading requests without excessive delays, even under moderate load.

b) Minimum Latency remains consistently low at 0.01 seconds across all rates, highlighting a consistent baseline performance.

c) Average Latency stays stable at around 0.02 seconds, indicating that the system processes the majority of reading requests efficiently without significant delay, despite the plateau in throughput.

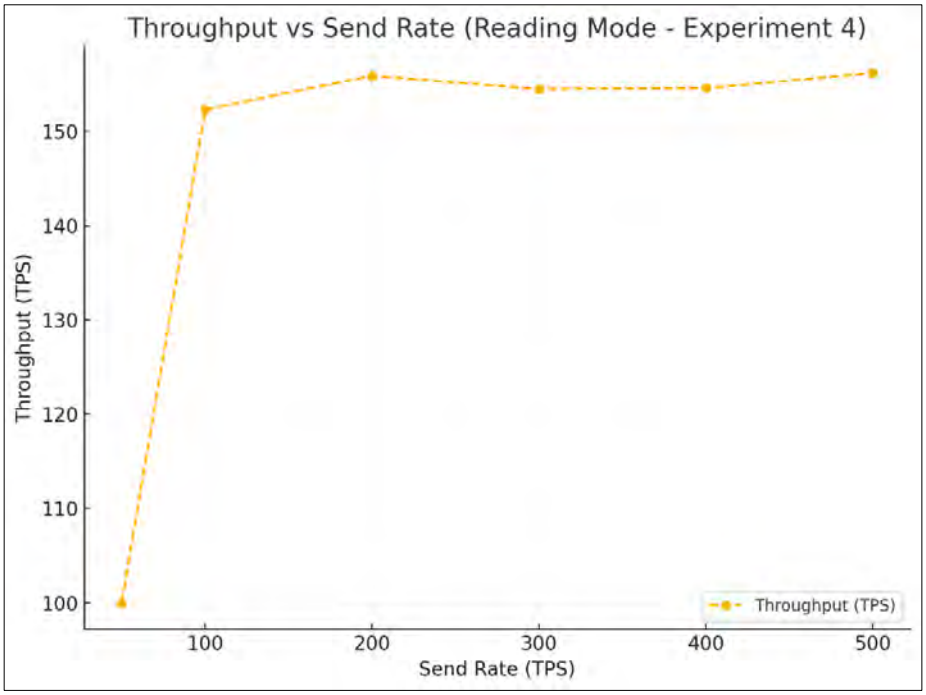

Figure 5. 24 Throughput vs. Send Rate at Reading Mode of Experiment 4

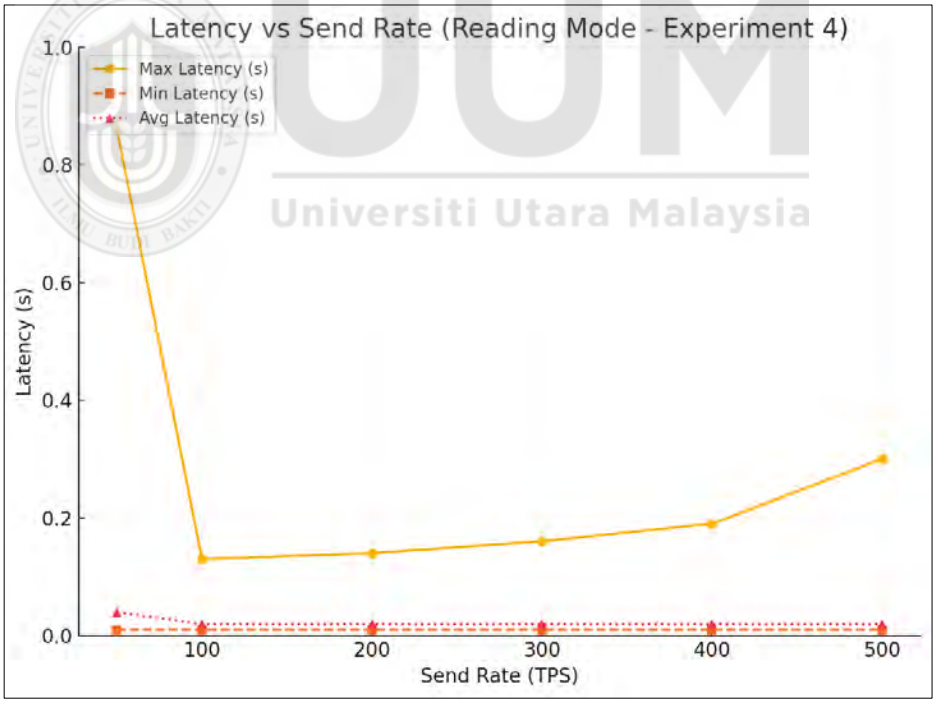

Figure 5. 25 Latency vs. Send Rate at Reading Mode of Experiment 4

Writing Mode Performance Analysis

Throughput Analysis

As shown in Figure 5.26, throughput in writing mode also scales with the send rate but reaches a limit of around 137 TPS as the send rate increases beyond 100 TPS. This ceiling on throughput suggests a performance limit, similar to that observed in reading mode that restricts scalability under higher transaction loads.

Latency Analysis

Figure 5.27 provides insights into latency trends:

a) Maximum Latency shows variation, with peaks at 0.70 seconds at 400 TPS, highlighting some fluctuations under load. However, the maximum latency returns to a lower level at 500 TPS, possibly due to internal resource management.

b) Minimum Latency remains stable at 0.02 seconds, and Average Latency stays around 0.03–0.04 seconds, indicating consistent and efficient processing times for most writing requests even under load.

Comparative Observations

a) **Throughput Limits:** Both reading and writing modes experience throughput plateaus around 156 TPS and 137 TPS, respectively. This throughput cap reflects a bottleneck in the SecureBlockCert Blockchain's processing capacity at higher transaction rates.

b) **Latency Trends:** Latency remains consistently low across both modes, with slightly higher maximum latency observed in writing mode. This stability suggests that the system can handle transaction loads efficiently but would require optimization to increase throughput at higher loads.

The observed throughput limitations highlight the need for optimizations or additional scaling mechanisms to enhance the framework's capacity for higher transaction volumes. The low average latency across different transaction rates is promising, indicating that the system is well-suited for applications requiring quick response times.

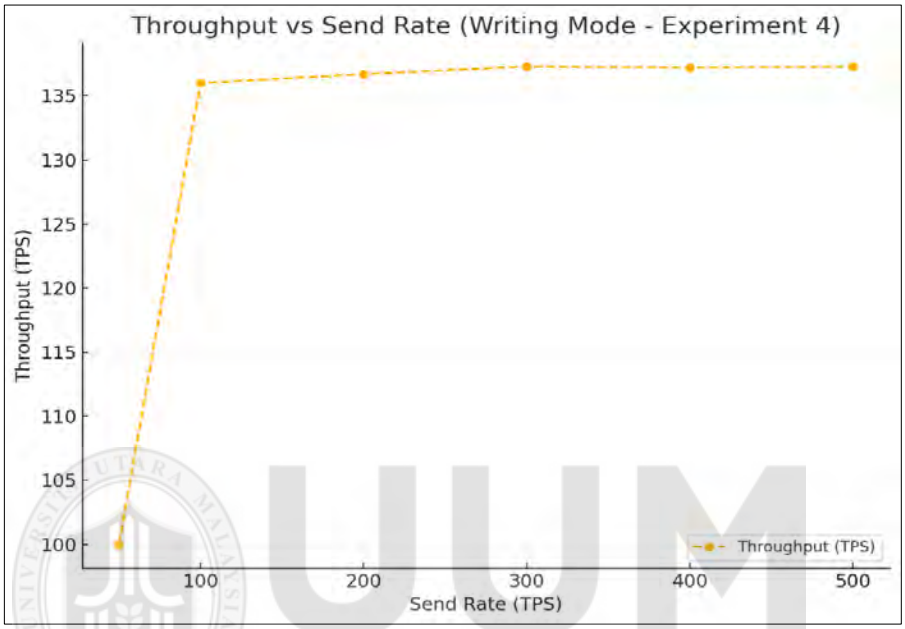

Figure 5. 26 Throughput vs. Send Rate at Writing Mode of Experiment 4

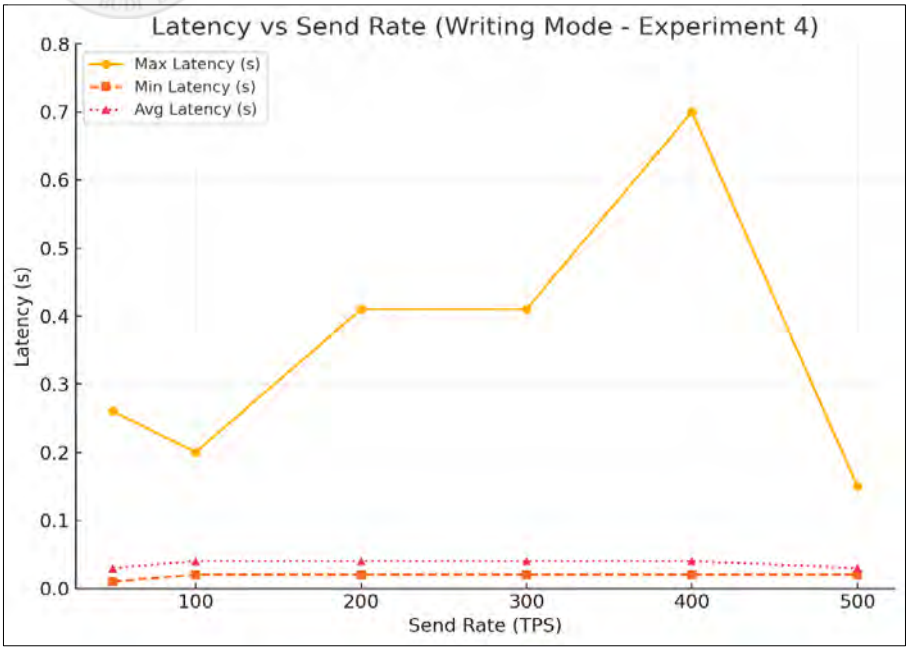

Figure 5. 27 Latency vs. Send Rate at Writing Mode of Experiment 4

5.6.4 Comparative Analysis

This section compares the SecureBlockCert framework with existing solutions, focusing on key performance metrics latency and throughput that are essential for achieving our research objectives of enhancing security, privacy, and scalability in educational credentialing. Maintaining low latency enables SecureBlockCert to support real-time, secure data handling, while high throughput provides scalability for handling high-demand periods in educational settings.

As highlighted in previous research, various studies have assessed latency and throughput on Hyperledger Fabric platforms at fixed rates [61], [60], [2], [67]. To facilitate direct comparison, this study evaluates SecureBlockCert's performance under equivalent fixed rates, enabling an accurate assessment of its capabilities in a controlled local environment against peer-reviewed benchmarks. Note that Leka and Selimi [60] is not included in this comparison as it was conducted on an Amazon EC2 testbed, which introduces variables that could significantly impact performance outcomes. In this comparative analysis, SecureBlockCert is evaluated against a current solution presented by Litoussi et al. [61] at fixed transaction rates of 100, 200, 500, and 1000 TPS, analyzing performance under different transaction volumes in both reading and writing modes.

Reading Mode Comparison

Fixed Rate: 100 TPS

Both SecureBlockCert and the current solution achieve a 100% success rate with no transaction failures.

Latency: SecureBlockCert records a higher maximum latency of 0.36 seconds, but it maintains a more favourable average latency of 0.02 seconds compared to the current

solution's 0.04 seconds. This indicates faster processing for most transactions in SecureBlockCert.

Throughput: Both solutions sustain a throughput of 100 TPS, meeting the fixed rate target.

Fixed Rate: 200 TPS

Both solutions continue to achieve a 100% success rate without failures.

Latency: SecureBlockCert's maximum latency rises slightly to 0.41 seconds, with a stable average latency of 0.02 seconds. This suggests that the framework can manage additional load without compromising average processing time.

Throughput: SecureBlockCert reaches 147.8 TPS, while the current solution sustains 200 TPS, indicating that the current solution meets the fixed rate, while SecureBlockCert's throughput falls slightly below.

Fixed Rate: 500 TPS

Success Rate: SecureBlockCert maintains a 100% success rate, while the current solution shows a decline, with a failure rate of approximately 1%.

Latency: The current solution experiences a significant latency spike, with maximum latency reaching 19.92 seconds, compared to SecureBlockCert's stable maximum latency of 0.45 seconds. Average latency also diverges, with SecureBlockCert at 0.02 seconds compared to the current solution's 10.73 seconds.

Throughput: SecureBlockCert achieves 149.8 TPS, while the current solution drops to 466.9 TPS due to failures, reflecting reduced performance under heavy load.

Fixed Rate: 1000 TPS

Success Rate: SecureBlockCert demonstrates robustness by achieving 1000 TPS without failures, while the current solution's failure rate increases to nearly 1%.

Latency: SecureBlockCert maintains low maximum (0.47 seconds) and average (0.02 seconds) latencies, while the current solution reaches a maximum latency of 21.51 seconds and an average latency of 13.97 seconds.

Throughput: SecureBlockCert sustains 150.6 TPS, while the current solution drops to 472.2 TPS, below the intended rate due to increased failures and latency.

Figure 5.28 illustrates these performance comparisons, highlighting SecureBlockCert's stable throughput and low latency across varying transaction rates. This consistency underscores its robustness and reliability in high-demand educational environments, whereas the current solution demonstrates limitations in both latency and throughput, suggesting potential scalability issues.

Lower Fixed Rate Comparison (10, 30, 50 TPS) [2]

Fixed Rate: 10 TPS

Success Rate: SecureBlockCert successfully processes all transactions at a send rate of 100 TPS, with a maximum latency of 0.99 seconds and an average latency of 0.03 seconds. The current solution operates at a fixed rate of 10 TPS with a lower average latency of 0.0926 seconds, benefiting from lower transaction demand.

Fixed Rate: 30 TPS

SecureBlockCert maintains a 100% success rate at a higher send rate of 148.5 TPS, with maximum latency at 1.3 seconds and average latency at 0.05 seconds. The current solution achieves a lower average latency of 0.253 seconds, which reflects the impact of a reduced processing load.

Fixed Rate: 50 TPS

SecureBlockCert processes all transactions without failure at a send rate of 149.6 TPS, recording a maximum latency of 1.51 seconds and an average latency of 0.04 seconds.

The current solution, though achieving a comparable average latency of 0.4 seconds, operates at a lower actual send rate, reflecting limitations in higher-load conditions.

Writing Mode Comparison

Fixed Rate: 10 TPS

SecureBlockCert achieves a 100% success rate at a high send rate of 100 TPS, with a maximum latency of 1.63 seconds and an average latency of 0.06 seconds. The current solution's higher average latency of 1.8896 seconds indicates potential inefficiencies.

Fixed Rate: 30 TPS

SecureBlockCert completes all transactions with zero failures at a send rate of 133.5 TPS, achieving a maximum latency of 1.26 seconds and an average latency of 0.05 seconds. In contrast, the current solution exhibits an average latency of 5.8528 seconds, indicating slower processing.

Fixed Rate: 50 TPS

SecureBlockCert sustains a high success rate at a send rate of 134.2 TPS, with a maximum latency of 1.67 seconds and an average latency of 0.06 seconds. The current solution's average latency of 9.8269 seconds shows a marked decline in performance, indicating challenges in handling increased loads.

Figures 5.29–5.30 compare the proposed SecureBlockCert's performance with the current solutions across these fixed rates. The results demonstrate SecureBlockCert's consistent low latency and stable throughput across both reading and writing modes, illustrating its ability to maintain quality performance under varying transaction demands.

Across both reading and writing modes, SecureBlockCert significantly outperforms the current solution, achieving higher throughput and maintaining low average latencies. The consistent performance under increased transaction rates indicates

SecureBlockCert's robustness, whereas the current solution's latency spikes and declining throughput suggest potential bottlenecks. High latencies and limited throughput scalability may impact user experience and operational efficiency in high-demand environments.

5.6.5 Implications for Scalability

The consistent, low-latency performance of SecureBlockCert across all fixed rates highlights its suitability for educational credentialing applications requiring high transaction volumes and time-sensitive processing. Conversely, the current solution's limited scalability and increased failure rates under higher loads suggest that it may not meet the demands of high-throughput environments without significant performance degradation. Given the disparity in performance, organizations that prioritize reliability and scalability in blockchain-based systems would benefit from SecureBlockCert over the current solution, assuming other considerations such as cost, security, and integration align with operational needs. SecureBlockCert's resilience under higher transaction loads underscores its potential for enterprise-grade applications.

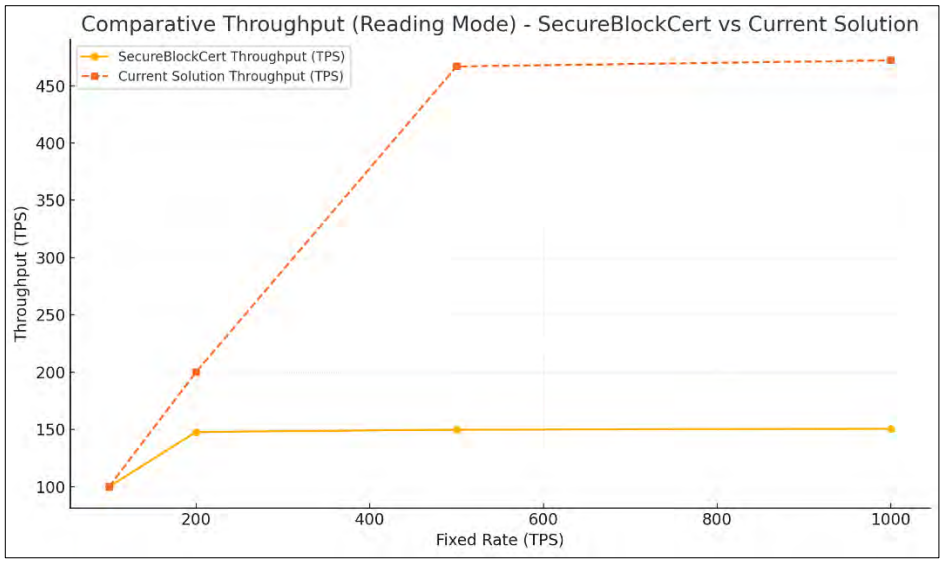

Figure 5. 28 Comparative throughput at Reading Mode

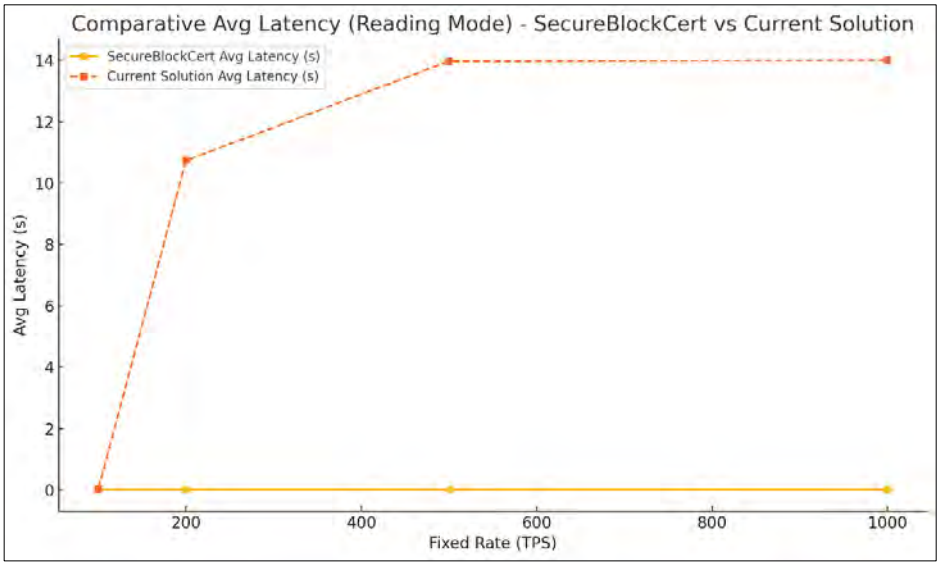

Figure 5. 29 Comparative Avg Latency at Reading Mode

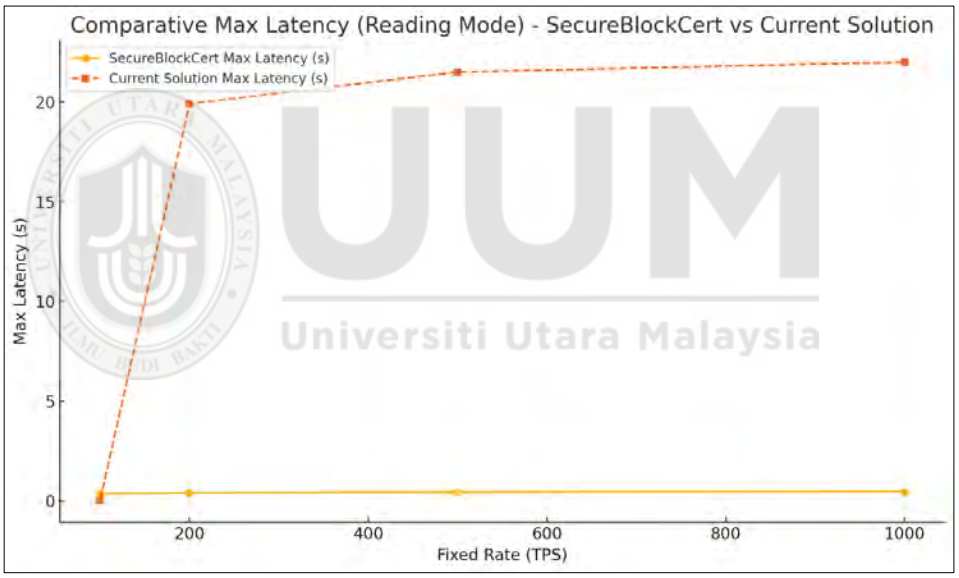

Figure 5. 30 Comparative Max Latency at Reading Mode

SecureBlockCert's objectives are to establish a secure and privacy-preserving credentialing framework. Throughput plays a critical role in maintaining system security during peak demand periods, as a high transaction-processing capacity prevents potential bottlenecks that could expose sensitive data to unauthorized access. By ensuring that the system can handle large transaction volumes, SecureBlockCert minimizes the risk of data compromise, thus supporting the goal of a secure

framework. Similarly, latency is essential for privacy, as swift credential issuance and verification reduce the likelihood of data interception during processing. SecureBlockCert's low-latency performance facilitates secure and efficient transactions, which is fundamental to preserving the privacy of credential data. Moreover, each metric is tied to specific security mechanisms such as encryption and authentication that are integral to SecureBlockCert's architecture, reinforcing its role as a secure and privacy-centric solution for educational credential management.

The technical performance metrics, particularly throughput and latency, have substantial implications for real-world applications in educational credentialing. High throughput ensures that the system can manage large volumes of credential transactions efficiently, especially during critical periods like enrollment and graduation, when demand for credential verification is at its peak. By maintaining this capacity, SecureBlockCert offers uninterrupted, reliable service to students, educational institutions, and verifiers, fostering user trust and a seamless user experience. SecureBlockCert demonstrates:

a) **High throughput for moderate loads**: Stable performance with low latency across reading and writing modes.
b) **Scalability challenges at higher loads**: Throughput plateaus suggest bottlenecks that require optimization for larger transaction volumes.

These findings position SecureBlockCert as a robust solution for educational credentialing applications, offering consistent performance in moderate-load scenarios and potential for scaling with future enhancements.

5.7 Experiments Results of Issuance and Verification based on DID and VC

This section presents the experimental evaluation of the SecureBlockCert Blockchain framework's efficiency in issuing and verifying Decentralized Identifiers (DIDs) and

Verifiable Credentials (VCs)**.** The experiments were conducted across transaction rates ranging from 1 to 999 transactions per second (TPS)**,** with a focus on latency as the primary performance metric. Latency is a critical indicator of system responsiveness, particularly in real-time credentialing applications. Table 5.14 summarizes the average latency results, with detailed experimental data available in **Appendix C**.

Table 5. 14 Summary Results of Latency of DID and VC Issuance and Verification

Function	DID Issuance	DID Verification	VC Issuance	VC Verification
Avg Latency (s)	0.001	0.005	0.007	0.007

5.7.1 Key Findings

The experimental outcomes highlight the SecureBlockCert Blockchain framework's robustness in managing high transaction volumes with exceptionally low latency:

a) **DID Issuance:** With an average latency of just 0.001 seconds, DID issuance is nearly instantaneous. This rapid processing underscores the framework's potential for real-time credential creation, making it ideal for applications requiring fast deployment of identifiers.

b) **DID Verification:** DID verification recorded an average latency of 0.005 seconds, showcasing not only the system's speed but also its capability to verify identities securely and swiftly. Such a low latency indicates that the verification process is efficient, allowing for near-instantaneous user authentication.

c) **VC Issuance and Verification:** For Verifiable Credentials, both issuance and verification maintained an average latency of 0.007 seconds. This consistency

reflects the framework's balanced performance across both processes, ensuring that credential issuance and validation are conducted without significant delays, even at high transaction rates. Figure 5.31 provides a visual representation of these latency averages for DID and VC issuance and verification, clearly illustrating the SecureBlockCert Blockchain framework's rapid response times.

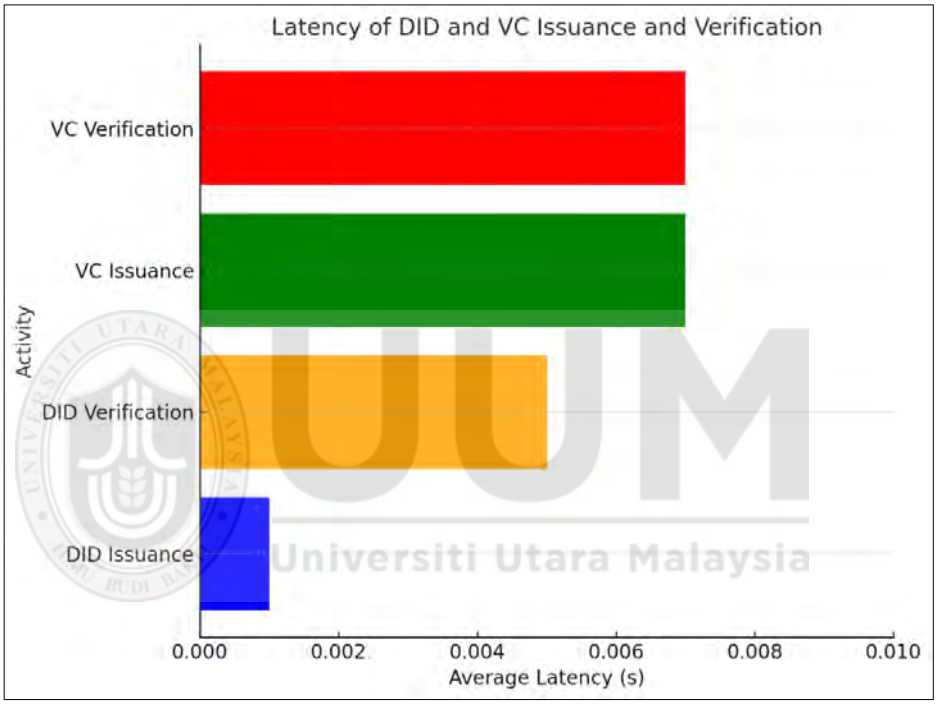

Figure 5. 31 Average Latency of DID and VC Issuance and Verification

5.7.2 Comparative Insights

SecureBlockCert Blockchain framework as a highly responsive and reliable solution for managing digital credentials, particularly in real-world applications where rapid issuance and verification are essential. The observed low latencies across all functions indicate that SecureBlockCert can handle high transaction volumes efficiently, which is critical for scaling in practical educational and organizational settings. The framework's ability to achieve sub-second average latencies in both issuance and

verification processes supports its potential as an ideal solution for digital credential management. This responsiveness not only facilitates seamless user experiences but also allows organizations to manage and authenticate credentials quickly, even under heavy transaction loads. The experimental outcomes further emphasize the scalability and robustness of SecureBlockCert, positioning it as a suitable framework for high-speed credential management in educational and institutional environments. Future real-world testing would further validate these results, especially under varying network conditions and real-time operational demands.

5.8 Comparative Analysis of SecureBlockCert and Existing Solutions for Security and Privacy in Digital Credentials

SecureBlockCert's unique features distinguish it from existing blockchain-based credentialing solutions, such as EduCTX and ECBC. Unlike these frameworks, SecureBlockCert integrates advanced cryptographic protocols, including Elliptic Curve Cryptography (ECC) and Edwards-curve Digital Signature Algorithm (EdDSA), to strengthen the security of digital identities. Additionally, homomorphic encryption ensures that data remains encrypted even during processing, providing a higher level of privacy compared to other systems.

SecureBlockCert also leverages Hyperledger Fabric and its smart contract capabilities, enabling automated, transparent management of credentials. This setup streamlines credential issuance and verification, setting SecureBlockCert apart from other frameworks that may rely on less efficient methods. The integration of these advanced technologies demonstrates SecureBlockCert's novel approach to security and privacy, highlighting its potential impact as a secure and scalable credentialing system for educational institutions.

The proposed solution, SecurBlockCert, presents a significant advancement in addressing the security and privacy concerns prevalent in the educational digital credential system on the blockchain as shown in the chapter 2, table 2.2 . By incorporating cutting-edge techniques such as ECC and EdDSA for heightened security and fully homomorphic encryption coupled with SHA-256 for comprehensive privacy protection, SecurBlockCert ensures that educational records remain safeguarded against fraudulent activities and unauthorized access. Moreover, the integration of smart contracts within the Hyperledger Fabric framework streamlines the management of digital credentials, offering an efficient and transparent process for issuance, sharing, and verification. The solution's impressive performance, as evidenced by high throughput rates and low latencies in experimental evaluations, underscores its ability to handle large transaction volumes with efficiency and reliability. Furthermore, the thorough evaluation process, including expert reviews, protocol verification using Tamarin Prover, and extensive experimentation with Hyperledger Caliper, instils confidence in the solution's effectiveness and robustness. However, it is essential to acknowledge that SecurBlockCert's reliance on Hyperledger Fabric may introduce dependencies and limitations associated with the platform's capabilities, necessitating careful consideration and ongoing refinement to ensure long-term scalability and viability.

5.9 Evaluation of Security and Privacy Features in SecureBlockCert

This section provides a theoretical assessment of the security and privacy mechanisms within SecureBlockCert, examining its designed resilience against common threats and adherence to privacy standards. The evaluation is organized into two main subsections: Security Analysis and Privacy Auditing.

5.9.1 Security Analysis

In a blockchain-based credentialing system, numerous security threats may arise, ranging from identity spoofing to data tampering. SecureBlockCert's architecture integrates multiple cryptographic and protocol-based defenses to mitigate these threats effectively:

a) **Fake Student Nodes (Identity Spoofing)**:

- **Attack Scenario**: An attacker could attempt to impersonate a student by gaining unauthorized access to a student's private key and using it with the public key of the education authority. Such impersonation could allow unauthorized access to sensitive academic records.
- **Mitigation:** SecureBlockCert employs strict authentication protocols, including Elliptic Curve Digital Signature Algorithm (EdDSA), to ensure that private keys remain secure and cannot be misused by unauthorized entities.

b) **Man-in-the-Middle Attack (Data Interception)**:

- **Attack Scenario**: An adversary could intercept transactions between students and educational authorities, potentially exposing sensitive information.
- **Mitigation**: SecureBlockCert secures transactions using end-to-end encryption with SHA-256 hashing, which ensures that each transaction's integrity remains intact. Furthermore, every transaction is stored in encrypted form within Hyperledger Fabric's ledger. The use of Transport Layer Security (TLS) for all data exchanges between nodes also prevents unauthorized access to the data being transmitted, effectively blocking any attempts to eavesdrop on the network.

c) **Dishonest CA Attack (Malicious Credential Issuance)**:

- **Attack Scenario**: A malicious Certificate Authority (CA) may issue incorrect or fraudulent credentials to new nodes, potentially compromising the system's integrity.
- **Mitigation**: SecureBlockCert includes a security protocol that requires multiple peer nodes to confirm a new node's credentials, reducing reliance on a single CA. Additionally, threshold signatures could be applied, whereby a majority of CAs must validate a node before it is accepted into the network. This way, even if one CA is compromised, it would be unable to unilaterally issue incorrect credentials.

d) **Transaction Integrity (Tampering Prevention)**:

- **Attack Scenario**: An attacker might attempt to modify transaction data in the ledger, altering records to gain unauthorized access or modify grades or credentials.
- **Mitigation**: SecureBlockCert employs SHA-256 hashing to create unique identifiers for each transaction, generating a transaction header that links to the preceding block. Any alteration in a transaction results in a hash mismatch, triggering the network to flag the block as tampered. Additionally, using **Merkle trees** further reinforces data integrity by allowing quick verification of large data sets without altering individual transactions, thus preventing undetected tampering.

e) **DDoS (Distributed Denial of Service) Attack**:

- **Attack Scenario**: Adversaries could flood CA nodes or other critical components of the network with excessive requests, disrupting service availability.

- **Mitigation**: SecureBlockCert integrates rate-limiting protocols and node clustering to distribute network load. By isolating CA nodes into clusters with dedicated load balancers, the framework minimizes the risk of a DDoS attack affecting the entire network.

f) **Tamper Attack by Verifier**:

- **Attack Scenario**: A verifier may attempt to tamper with a transaction's details (e.g., modifying a credential's attributes).
- **Mitigation**: SecureBlockCert uses a tamper-resistant framework where each transaction is signed with EdDSA and compressed with homomorphic encryption. This ensures that any modifications to transaction data invalidate the digital signature, which is verified against the original sender's public key. Because only the original private key can generate a valid signature, any tampering by the verifier will be detectable by other nodes, maintaining data integrity across the network.

5.9.2 Privacy Auditing

Privacy is a primary concern in digital credentialing, as student records contain sensitive data. SecureBlockCert includes privacy protection measures specifically designed to address these concerns:

a) **Selective Homomorphic Encryption (H.E.)**: SecureBlockCert allows for selective encryption of private information within each transaction. By applying homomorphic encryption to sensitive data, the framework enables private data processing without decrypting it, allowing peers to verify credentials or attributes without exposing the underlying data. This privacy

feature is particularly beneficial in educational environments where students' records are shared with external verifiers but must remain protected.

b) **Privacy-Aware Transactions**: Each transaction involving private information includes an encryption option that activates when data privacy is required. This flexibility enables the system to securely process sensitive data only when necessary, minimizing unnecessary exposure of private information.

c) **Key Management and Access Control**: SecureBlockCert incorporates strict access control mechanisms and key management policies that ensure only authorized parties can decrypt sensitive data. Each participant is assigned a unique key pair for encrypting and decrypting transactions, and multi-layered access control restricts data access based on role and authorization level. This system further strengthens privacy by ensuring that only verified and authorized entities can access encrypted data.

5.10 Conclusion

This chapter reviewed the implementation and evaluation of the SecureBlockCert framework, designed to securely manage digital credentials on a blockchain. SecureBlockCert aims to enhance security and privacy for educational credentials while ensuring high performance and scalability. Key security technologies, including Elliptic Curve Cryptography (ECC), EdDSA signatures, homomorphic encryption, and SHA-256 hashing, were integrated to protect digital identities and maintain data integrity.

Leveraging smart contracts within Hyperledger Fabric, SecureBlockCert enables efficient credential issuance, sharing, and verification processes, reducing administrative overhead and fostering trust in digital credential management. Evaluation results demonstrated low latency and high reliability, with

SecureBlockCert handling transactions efficiently, even under substantial load, thus outperforming traditional systems.

Comparative analysis highlighted significant security and privacy improvements over existing credentialing methods. SecureBlockCert's robust performance at scale makes it a promising solution for real-world educational credentialing, offering a secure, private, and scalable approach to digital credential management.

CHAPTER SEX
CONCLUSION AND FUTURE WORK

6.1 Introduction

This concluding chapter summarizes the research and accomplishments of the SecureBlockCert Blockchain framework, designed to enhance the security, privacy, and efficiency of digital credential management within educational settings. Section 6.2 reviews the key findings aligned with each research objective, while Section 6.3 discusses the unique contributions SecureBlockCert makes to the field. Section 6.4 addresses limitations encountered during the study and proposes improvements. Finally, Section 6.5 outlines potential directions for future research to expand upon the findings and advance the SecureBlockCert framework.

6.2 Research Summary

The primary aim of this research was to design and develop the SecureBlockCert Blockchain framework to enhance security, privacy, and efficiency in blockchain-based digital credential systems for educational institutions. This was accomplished through a series of targeted objectives, each carefully pursued to establish a comprehensive solution for managing digital credentials.

Objective 1: To develop a security mechanism within the SecureBlockCert framework that enhances authentication during entity registration, using cryptographic schemes to improve data integrity and protect against unauthorized access.

This objective was met through the development of a security mechanism within the SecureBlockCert Blockchain framework, employing asymmetric cryptography for robust entity authentication during the registration phase. The mechanism leverages Elliptic Curve Cryptography (ECC) alongside EdDSA digital signatures to verify user

identities, facilitating secure and exclusive access to the credentialing system. Additionally, the protocol incorporates nonces and timestamped exchanges, further enhancing the security of interactions and mitigating the risk of replay attacks. Collectively, these cryptographic elements establish a trusted and secure registration process, achieving the objective of protecting against unauthorized access and ensuring data integrity within the system.

Objective 2: To design a privacy-preserving mechanism within the SecureBlockCert framework using homomorphic encryption and access control algorithms to safeguard sensitive data during credential issuance and verification.

This objective was met by implementing a privacy-preserving mechanism centered on homomorphic encryption, ensuring that credential data remains encrypted and confidential throughout the verification process. Homomorphic encryption enables secure computations directly on encrypted data, allowing credential validation without exposing sensitive information. The mechanism also integrates an access control mechanism that restricts data visibility to authorized entities, maintaining robust privacy protections and limiting data exposure. Additionally, by combining homomorphic encryption with secure hashing functions, the framework ensures that credential data is securely stored and processed, aligning with strict privacy standards. This approach successfully addresses the objective of safeguarding sensitive educational data while enabling secure credential verification within a blockchain-based system.

Objective 3: To construct an efficient issuance and verification mechanism within the SecureBlockCert framework using smart contracts to address issues of transparency, latency, and immutability in digital credential systems.

This objective was accomplished by designing a decentralized, smart contract-driven system that automates the credentialing process through five principal smart contracts—Add Authority, Add University, Issue Certificate, Share Certificate, and Verify Certificate. Each contract plays a vital role in managing the lifecycle of digital credentials, from authorizing and onboarding institutions to issuing, sharing, and verifying credentials with third-party entities. These processes leverage Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), empowering users with greater control over their digital identities and supporting verifiable credential exchanges.

By recording each transaction immutably on the blockchain, the SecureBlockCert framework provides a transparent and tamper-resistant environment for credential management. The smart contracts streamline interactions, significantly reducing latency while ensuring each credential's integrity. This approach meets the objective by establishing an efficient, secure, and transparent system for issuing and verifying digital credentials within the blockchain environment

Objective 4: To evaluate the performance and security of the SecureBlockCert Blockchain framework using metrics, including throughput, latency, and resistance to attacks.

This objective was accomplished through a multi-faceted evaluation approach, which included expert reviews, formal security analysis, and comprehensive performance benchmarking. Six blockchain and security experts conducted in-depth reviews of the framework, providing valuable feedback that led to key design adjustments. To rigorously test the security features, the Tamarin Prover tool was employed to validate the cryptographic protocols, confirming essential security properties such as authentication and data confidentiality. Additionally, the framework's operational performance was assessed using Hyperledger Caliper, which measured metrics

including throughput, latency, and scalability. Results from this benchmarking revealed that SecureBlockCert handles high transaction volumes efficiently, maintaining minimal latency and surpassing the performance of existing credentialing systems. This thorough evaluation process, combining expert insights, formal security validation, and empirical testing, successfully fulfills the objective of demonstrating the SecureBlockCert framework's robust security and performance capabilities.

6.4 Limitations

While the SecureBlockCert Blockchain framework advances the security and privacy of digital credential systems, it is accompanied by several limitations that highlight areas for further exploration and improvement:

a) **Scalability Constraints**: As the volume of transactions grows, maintaining low latency and high throughput becomes increasingly challenging. Although SecureBlockCert demonstrates solid performance metrics, scaling the framework to accommodate larger, more complex networks may require enhanced optimization and infrastructure.

b) **Dependency on Cryptographic Assumptions**: The framework relies on the robustness of current cryptographic algorithms, such as ECC and homomorphic encryption. Advances in cryptanalysis or quantum computing could potentially weaken these assumptions, necessitating future updates to the cryptographic foundations of SecureBlockCert.

c) **Interoperability Challenges**: The SecureBlockCert framework, built on Hyperledger Fabric, may face compatibility challenges when integrating with other blockchain platforms or legacy systems. Developing cross-platform interoperability solutions would increase SecureBlockCert's adaptability across different institutional environments.

d) **Privacy Trade-offs in Verification**: Although the framework enhances privacy, the process of credential verification may still involve limited disclosures that could pose privacy risks under specific conditions. Balancing complete privacy with effective verification remains a challenging area that requires further refinement.

Addressing these limitations will be essential to fully realize the potential of SecureBlockCert, driving future research and development efforts aimed at creating an even more robust, flexible, and universally adaptable credential management solution.

6.5 Future Directions

The identified limitations of the SecureBlockCert Blockchain framework pave the way for several promising research and development avenues aimed at advancing the system's capabilities and resilience:

a) **Enhanced Scalability Solutions**: Future research could focus on optimizing SecureBlockCert for large-scale implementations, exploring advanced consensus mechanisms, such as sharding or off-chain processing, to maintain high performance as transaction volumes increase.

b) **Quantum-Resistant Cryptography**: Given the evolving landscape of cryptographic threats, including potential risks posed by quantum computing, integrating quantum-resistant cryptographic algorithms could bolster the framework's long-term security and resilience.

c) **Cross-Platform Interoperability**: To improve compatibility with diverse blockchain and legacy systems, research into cross-chain interoperability protocols and integration standards will be critical, expanding

SecureBlockCert's applicability across various educational and institutional environments.

d) **Enhanced Privacy Mechanisms**: Investigating zero-knowledge proofs technique could offer more refined privacy solutions, allowing for credential verification that maintains full confidentiality of underlying data without compromising verification accuracy.

e) **Optimization of Resource Efficiency**: Research focused on reducing the computational demands of privacy-preserving techniques, such as homomorphic encryption, would support broader adoption by enabling deployment in resource-limited environments, such as smaller institutions with constrained IT infrastructure.

REFERENCES

[1] S. Alam, H. A. Y. Ayoub, R. A. A. Alshaikh, and A. H. H. Al-Hayawi, "A blockchain-based framework for secure educational credentials," *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 5157–5167, 2021. [Online]. Available: https://www.researchgate.net/publication/351356935

[2] T. R. Reddy, P. V. G. D. P. Reddy, R. Srinivas, Ch. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," *EURASIP Journal on Information Security*, vol. 2021, no. 7, 2021. [Online]. Available: https://doi.org/10.1186/s13635-021-00122-5

[3] A. Mühle, K. Assaf, D. Köhler, and C. Meinel, "Requirements of a digital education credential system," in *Proceedings of the IEEE Global Engineering Education Conference (EDUCON)*, May 2023. [Online]. Available: https://doi.org/10.1109/EDUCON54358.2023.10125183.

[4] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A systematic literature review on blockchain-based systems for academic certificate verification," *IEEE Access*, vol. 11, pp. 64679–64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[5] R. Q. Castro and M. Au-Yong-Oliveira, "Blockchain and higher education diplomas," in *Proceedings of the 16th International Conference on Education and New Learning Technologies (EDULEARN)*, 2021, pp. 154–167.

[6] R. H. Sayed, "Potential of blockchain technology to solve fake diploma problem," *University of Jyväskylä, Department of Computer Science and Information Systems*, 2019. [Online]. Available: http://urn.fi/URN:NBN:fi:jyu-201906253406

[7] M. Baldi, F. Chiaraluce, M. Kodra, and L. Spalazzi, "Security analysis of a blockchain-based protocol for the certification of academic credentials," *CEUR Workshop Proceedings*, vol. 2580, pp. 1–12, 2020.

[8] Q. Tang, "Towards using blockchain technology to prevent diploma fraud," *IEEE Access*, vol. 9, pp. 168678–168688, 2021, doi: 10.1109/ACCESS.2021.3137901.

[9] J. B. Bernabe, R. T. Moreno, J. L. Canovas, J. L. Hernandez-Ramos, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[10] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: Problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019, doi: 10.1109/ACCESS.2019.2957660.

[11] W. She, J. S. Chen, Q. Liu, Y. Hu, Z. Gu, Z. Tian, and W. Liu, "New blockchain technology for medical big data security sharing," *Journal of Chinese Computer Systems*, vol. 40, no. 7, pp. 1449–1454, 2019.

[12] S. Figueroa-Lorenzo, J. A. Benito, and S. Arrizabalaga, "Modbus access control system based on SSI over Hyperledger Fabric blockchain," *Sensors*, vol. 21, no. 16, 2021, doi: 10.3390/s21165438.

[13] D. J. Dharani, K. Sundarakantham, K. Singh, and M. S. Shalinie, "A privacy-preserving framework for endorsement process in Hyperledger Fabric," *Computers & Security*, vol. 116, p. 102637, May 2022, doi: 10.1016/j.cose.2022.102637.

[14] A. Satybaldy, A. Subedi, and M. Nowostawski, "A framework for online document verification using self-sovereign identity technology," *Sensors*, vol. 22, no. 21, 2022, doi: 10.3390/s22218408.

[15] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 4, pp. 1503–1514, 2022, doi: 10.1109/TCSS.2022.3188453.

[16] T. Nargis, P. Salian, J. Vanajakshi, G. R. Manasa, and S. Salian, "A secure platform for storing, generating and verifying degree certificates using blockchain," in *Proceedings of the 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2023, pp. 532–536, IEEE.

[17] P. Herbke, T. Cory, and M. Migliardi, "Decentralized credential status management: A paradigm shift in digital trust," *arXiv preprint*, arXiv:2406.11511, Jun. 17, 2024. [Online]. Available: https://doi.org/10.48550/arXiv.2406.11511

[18] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 71–78, 2020, IEEE.

[19] M. Al Hemairy, M. Abu Talib, A. Khalil, A. Zulfiqar, and T. Mohamed, "Blockchain-based framework and platform for validation, authentication, and equivalency of academic certification and institution's accreditation: UAE case study

and system performance," *Education and Information Technologies*, 2024, doi: 10.1007/s10639-024-12493-6.

[20] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, p. 341, Nov. 21, 2022.

[21] B. Bhushan, P. Sinha, K. M. Sagayam, and A. J., "Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications, and future research directions," *Computers & Electrical Engineering*, vol. 90, p. 106897, 2021, doi: 10.1016/j.compeleceng.2020.106897.

[22] K. Ansar, M. Ahmed, M. Helfert, and J. Kim, "Blockchain-based data breach detection: Approaches, challenges, and future directions," *Mathematics*, vol. 12, no. 1, pp. 1–21, 2024, doi: 10.3390/math12010107.

[23] F. J. de Haro-Olmo, Á. J. Varela-Vaca, and J. A. Álvarez-Bermejo, "Blockchain from the perspective of privacy and anonymization: A systematic literature review," *Sensors*, vol. 20, no. 24, p. 7171, 2020, doi: 10.3390/s20247171.

[24] S. Gilda and M. Mehrotra, "Blockchain for student data privacy and consent," in *Proceedings of the 2018 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, 2018, pp. 1–5, doi: 10.1109/ICCCI.2018.8441445.

[25] Y. Xu, S. Zhao, L. Kong, and Y. Zheng, "ECBC: A high-performance educational certificate blockchain with efficient query," in *Proceedings of the International Conference on Blockchain and Information Technology*, 2017, vol. 1, pp. 288–304, doi: 10.1007/978-3-319-67729-3.

[26] C. Delgado-Von Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information," *Applied Sciences*, vol. 11, no. 10, 2021, doi: 10.3390/app11104537.

[27] J. Kaneriya and H. Patel, "A secure and privacy-preserving student credential verification system using blockchain technology," *International Journal of Information and Education Technology*, vol. 13, no. 8, pp. 1251–1260, 2023, doi: 10.18178/ijiet.2023.13.8.1927.

[28] M. F. Molina, G. Betarte, and C. Luna, "A privacy and security-aware blockchain-based design for a digital certificates system," *CLEI Electronic Journal*, vol. 26, no. 1, pp. 1–23, 2023, doi: 10.19153/cleiej.26.1.3.

[29] A. Wahab, M. Barlas, and W. Mahmood, "Zenith certifier: A framework to authenticate academic verifications using tangle," in *Proceedings of the International Conference on Blockchain Technology and Applications*, May 2018, doi: 10.5171/2018.370695.

[30] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, "PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities," *Computers & Security*, vol. 88, p. 101653, 2020, doi: 10.1016/j.cose.2019.101653.

[31] T. R. Reddy, P. V. G. D. P. Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," *EURASIP Journal on Information Security*, vol. 2021, no. 1, 2021, doi: 10.1186/s13635-021-00122-5.

[32] T. Arndt and A. Guercio, "Blockchain-based transcripts for mobile higher-education," *International Journal of Information and Education Technology*, vol. 10, no. 2, pp. 84–89, 2020, doi: 10.18178/ijiet.2020.10.2.1344.

[33] B. M. Nguyen, T. C. Dao, and B. L. Do, "Towards a blockchain-based certificate authentication system in Vietnam," *PeerJ Computer Science*, vol. 2020, no. 3, 2020, doi: 10.7717/peerj-cs.266.

[34] M. R. Manu, N. Musthafa, B. Balamurugan, and R. Chauhan, "Blockchain components and concept," in *Blockchain Technology and Applications*, 1st ed., Boca Raton, FL, USA: Auerbach Publications, 2020, pp. 21–50, eBook ISBN: 9781003081487.

[35] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[36] K. Patel and M. L. Das, "Transcript management using blockchain-enabled smart contracts," in *Lecture Notes in Computer Science*, vol. 11969, pp. 392–407, 2020, doi: 10.1007/978-3-030-36987-3_26.

[37] C. Wang, H. Jiang, J. Zeng, M. Yu, Q. Huang, and Z. Zuo, "A review of blockchain layered architecture and technology application research," *Wuhan University Journal of Natural Sciences*, vol. 26, no. 5, pp. 415–428, 2021, doi: 10.19823/j.cnki.1007-1202.2021.0052.

[38] M. Dabbagh, M. Kakavand, M. Tahir, and A. Amphawan, "Performance analysis of blockchain platforms: Empirical evaluation of Hyperledger Fabric and Ethereum," in *Proceedings of the 2020 IEEE 2nd International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)*, Sep. 2020, pp. 1–6.

[39] V. Garcia-Font, "Blockchain: Opportunities and challenges in the educational context," in *Engineering Data-Driven Adaptive Trust-based e-Assessment Systems: Challenges and Infrastructure Solutions*, Springer, 2020, pp. 133–157.

[40] K. Kumutha, "Hyperledger Fabric blockchain framework: Efficient solution for academic certificate decentralized repository," in *Proceedings of the 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, 2021, pp. 1584–1590, doi: 10.1109/I-SMAC52330.2021.9640785.

[41] A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. K. Hung, "A permissioned blockchain-based system for verification of academic records," in *Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2019, pp. 1–5, doi: 10.1109/NTMS.2019.8763831.

[42] I. Alnafrah and S. Mouselli, "Revitalizing blockchain technology potentials for smooth academic records management and verification in low-income countries," *International Journal of Educational Development*, vol. 85, 2021, doi: 10.1016/j.ijedudev.2021.102460.

[43] D. Boughaci and O. Boughaci, "A comparative study of three blockchain emerging technologies: Bitcoin, Ethereum, and Hyperledger," in *Communications in Computer and Information Science*, vol. 1097, pp. 3–7, 2019, doi: 10.1007/978-3-030-36365-9_1.

[44] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification, and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[45] C. S. Hsu, S. F. Tu, and P. C. Chiu, "Design of an e-diploma system based on consortium blockchain and facial recognition," *Education and Information Technologies*, vol. 27, no. 4, pp. 5495–5511, 2022, doi: 10.1007/s10639-021-10840-5.

[46] R. Taufiq *et al.*, "Robust crypto-governance graduate document storage and fraud avoidance certificate in Indonesian private university," in *Proceedings of the 2019 International Conference on Information Management and Technology (ICIMTech)*, vol. 1, 2019, pp. 339–344, doi: 10.1109/ICIMTech.2019.8843784.

[47] J. Karamachoski, N. Marina, and P. Taskov, "Blockchain-based application for certification management," *Tehnički Glasnik*, 2020, doi: 10.31803/tg-20200811113729.

[48] Y. Xu, S. Zhao, L. Kong, and Y. Zheng, "ECBC: A high-performance educational certificate blockchain with efficient query," in *Proceedings of the International Conference on Blockchain Technology*, 2017, pp. 288–304, doi: 10.1007/978-3-319-67729-3.

[49] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A blockchain-based higher education credit platform," *IEEE Access*, vol. 6, pp. 5112–5127, 2018, doi: 10.1109/ACCESS.2018.2789929.

[50] J. Santos, "Hypercerts: A non-siloed blockchain-based certification service," *Journal of Information Technology Management*, vol. 18, pp. 1–19, 2017.

[51] M. Han, Z. Li, J. He, D. Wu, Y. Xie, and A. Baba, "A novel blockchain-based education records verification solution," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, 2018, pp. 178–183.

[52] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, *An Educational Blockchain for the University of Zurich (UZHBC)*, Master's thesis, Department of Informatics (IFI), University of Zurich, Zurich, Switzerland, 2018.

[53] S. S. Kumari and D. Saveetha, "Blockchain and smart contract for digital document verification," *International Journal of Engineering and Technology*, vol. 7, no. 4.6, pp. 394–397, 2018.

[54] R. Arenas and P. Fernandez, "CredenceLedger: A permissioned blockchain for verifiable academic credentials," in *Proceedings of the IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 2018, pp. 1–6, doi: 10.1109/ICE.2018.8436324.

[55] T. T. Huynh, T. T. Huynh, D. K. Pham, and A. K. Ngo, "Issuing and verifying digital certificates with blockchain," in *Proceedings of the International Conference on Advanced Technologies for Communications (ATC)*, Oct. 2018, pp. 332–336, doi: 10.1109/ATC.2018.8587428.

[56] S. Mthethwa, N. Dlamini, and G. Barbour, "Proposing a blockchain-based solution to verify the integrity of hardcopy documents," in *Proceedings of the 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*, 2019, pp. 1–5, doi: 10.1109/ICONIC.2018.8601200.

[57] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, "The proposal of a blockchain-based architecture for transparent certificate handling," in *Lecture Notes in Business Information Processing*, vol. 339, pp. 185–196, 2019, doi: 10.1007/978-3-030-04849-5_16.

[58] E. E. Bessa and J. S. B. Martins, "A blockchain-based educational record repository," *Journal of the British Blockchain Association*, vol. 3, no. 2, pp. 1–8, 2019, doi: 10.31585/jbba-3-2-(7)2020.

[59] E. Y. Daraghmi, Y. A. Daraghmi, and S. M. Yuan, "UniChain: A design of blockchain-based system for electronic academic records access and permissions management," *Applied Sciences*, vol. 9, no. 22, p. 4966, 2019, doi: 10.3390/app9224966.

[60] E. Leka and B. Selimi, "BCERT: A decentralized academic certificate system distribution using blockchain technology," *International Journal on Information Technologies & Security*, vol. 12, no. 4, pp. 103–118, 2020.

[61] M. Litoussi, M. Fartitchou, K. El Makkaoui, A. Ezzati, and Z. El Allali, "Digital certifications in Moroccan universities: Concepts, challenges, and solutions," *Procedia Computer Science*, vol. 201, pp. 95–100, 2022, doi: 10.1016/j.procs.2022.03.015.

[62] P. Haveri, U. B. Rashmi, D. G. Narayan, K. Nagaratna, and K. Shivaraj, "EduBlock: Securing educational documents using blockchain technology," in *Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, July 2020, pp. 1–7, doi: 10.1109/ICCCNT49239.2020.9225411.

[63] C. Castro-Iragorri, F. Lopez-Gomez, and O. Giraldo, "Academic certification using blockchain: Permissioned versus permissionless solutions," *The Journal of the British Blockchain Association*, vol. 3, no. 2, pp. 1–8, 2020.

[64] R. Mukta, J. Martens, H. Y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-based verifiable credential sharing with selective disclosure," in *Proceedings of the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 959–966, doi: 10.1109/TrustCom50675.2020.00128.

[65] C. Brunner, F. Knirsch, and D. Engel, "SPROOF: A platform for issuing and verifying documents in a public blockchain," in *Proceedings of the 5th International*

Conference on Information Systems Security and Privacy (ICISSP), 2019, pp. 15–25, doi: 10.5220/0007245600150025.

[66] A. W. S. Abreu, E. F. Coutinho, and C. I. M. Bezerra, "A blockchain-based architecture for query and registration of student degree certificates," in *ACM International Conference Proceedings Series*, pp. 151–160, 2020, doi: 10.1145/3425269.3425285.

[67] N. Chaniago, P. Sukarno, and A. A. Wardana, "Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain," *Register: Journal of Information Systems and Technology*, vol. 7, no. 2, pp. 149–163, 2021, doi: 10.26594/REGISTER.V7I2.1959.

[68] P. Rani, R. Kumar, and S. Sonal, "Educert-chain: A secure and notarized educational certificate authentication and verification system using permissioned blockchain," *Cluster Computing*, vol. 5, 2024, doi: 10.1007/s10586-024-04469-5.

[69] R. A. Mishra, A. Kalla, A. Braeken, and M. Liyanage, "Privacy protected blockchain-based architecture and implementation for sharing of students' credentials," *Information Processing & Management*, vol. 58, no. 3, p. 102512, 2021, doi: 10.1016/j.ipm.2021.102512.

[70] N. K. Dewangan, P. Chandrakar, S. Kumari, and J. J. P. C. Rodrigues, "Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file system," *Multimedia Tools and Applications*, vol. 82, no. 8, pp. 12595–12614, 2023, doi: 10.1007/s11042-022-13915-8.

[71] P. S. Rani, "Security-aware and privacy-preserving blockchain chameleon hash functions for education system," *ECTI Transactions on Computer and Information Technology*, pp. 225–234, 2023, doi: 10.37936/ecti-cit.2023171.252014.

[72] C. Labadie and C. Legner, "Building data management capabilities to address data protection regulations: Learnings from EU-GDPR," *Journal of Information Technology*, vol. 38, no. 1, pp. 16–44, 2023.

[73] A. Srivastava, P. Bhattacharya, A. Singh, A. Mathur, O. Prakash, and R. Pradhan, "A distributed credit transfer educational framework based on blockchain," in *Proceedings of the 2018 2nd International Conference on Advanced Computing, Control and Communication Technologies (IAC3T)*, 2019, pp. 54–59, doi: 10.1109/IAC3T.2018.8674023.

[74] A. Shettima Musti, S. Kant, and T. Khanna, "DegChain: Development of blockchain framework for generation and verification of educational certificates," in

Proceedings of the 2022 IEEE 7th International Conference on Convergence of Technology (I2CT), 2022, pp. 1–7, doi: 10.1109/I2CT54291.2022.9824282.

[75] H. M. Kyi, "Educational certification system framework based on blockchain technology," *Journal of Computer Applications and Research*, vol. 1, no. 1, pp. 11–17, 2020. [Online]. Available: https://www.ucstgi.edu.mm/wp-content/uploads/2020/10/JCAR2020_11_17.pdf

[76] F. Masood and A. R. Faridi, "A blockchain framework to increase the security and verifiability of educational certificates," in *Communications in Computer and Information Science*, vol. 1487, pp. 3–17, 2021, doi: 10.1007/978-981-16-8059-5_1.

[77] S. S. Dhanda, B. Singh, and P. Jindal, "Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 463–470, 2020, doi: 10.1080/09720502.2020.1731959.

[78] D. Mahto and D. Kumar Yadav, "Performance analysis of RSA and elliptic curve cryptography," *International Journal of Network Security*, vol. 20, no. 4, pp. 625–635, 2018, doi: 10.6633/IJNS.201807.

[79] A. Alenezi, H. F. Atlam, and G. B. Wills, "Expert reviews of a cloud forensic readiness framework for organizations," *Journal of Cloud Computing*, vol. 8, no. 1, 2019, doi: 10.1186/s13677-019-0133-z.

[80] I. Almarashdeh and M. Alsmadi, "Heuristic evaluation of mobile government portal services: An experts' review," in *Proceedings of the 2016 11th International Conference on Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 427–431, IEEE, doi: 10.1109/ICITST.2016.7856746.

[81] E. Vinarskii, A. Demakov, A. Kamkin, and N. Yevtushenko, "Verifying cryptographic protocols by Tamarin Prover," in *Proceedings of the 2020 Ivannikov Memorial Workshop (IVMEM)*, 2020, pp. 69–75, IEEE, doi: 10.1109/IVMEM51402.2020.00019.

[82] Y. Wang and A. Kogan, "Designing confidentiality-preserving blockchain-based transaction processing systems," *International Journal of Accounting Information Systems*, vol. 30, pp. 1–18, 2018, doi: 10.1016/j.accinf.2018.06.001.

[83] K. Saito and S. Watanabe, "Lightweight selective disclosure for verifiable documents on blockchain," *ICT Express*, vol. 7, no. 3, pp. 290–294, 2021, doi: 10.1016/j.icte.2021.08.012.

[84] A. E. N. Saah, J.-J. Yee, and J.-H. Choi, "Securing construction workers' data security and privacy with blockchain technology," *Applied Sciences*, vol. 13, no. 24, p. 13339, 2023, doi: 10.3390/app132413339.

[85] O. S. Saleh, O. Ghazali, and N. B. Idris, "Enhancing academic certificate privacy with a Hyperledger Fabric blockchain-based access control approach," *SN Computer Science*, vol. 4, no. 5, 2023, doi: 10.1007/s42979-023-02060-0.

[86] A. C. Tran, H. Van Kieng, D. X. Mai, and V. L. N. Huu, "A consortium blockchain-based platform for academic certificate verification," in *Communications in Computer and Information Science*, vol. 1500, pp. 346–360, 2021, doi: 10.1007/978-981-16-8062-5_23.

[87] L. Chen, K. Chen, S. Zhong, and D. Ye, "Privacy protection method of document management based on homomorphic encryption on the Fabric platform," in *ACM International Conference Proceedings Series*, pp. 31–37, 2019, doi: 10.1145/3376044.3376063.

[88] T. Manoj, K. Makkithaya, and V. G. Narendra, "A blockchain-based decentralized identifier for entity authentication in electronic health records," *Cogent Engineering*, vol. 9, no. 1, 2022, doi: 10.1080/23311916.2022.2035134.

[89] M. Kang and V. L. Lemieux, "A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage," *Ledger*, vol. 6, pp. 126–151, 2021, doi: 10.5195/LEDGER.2021.239.

[90] T. T. Thwin and S. Vasupongayya, "Blockchain-based access control model to preserve privacy for personal health record systems," *IEEE Access*, vol. 7, pp. 125–143, 2019, doi: 10.1109/ACCESS.2019.2950872.

[91] A. E. N. Saah, K. G. Kogos, and K. S. Filippova, "Fully homomorphic encryption: Current state of the art," in *Proceedings of the International Conference on Computer Science and Engineering*, 2012, pp. 463–466.

[92] Z. Ma, J. Wang, K. Gai, P. Duan, Y. Zhang, and S. Luo, "Fully homomorphic encryption-based privacy-preserving scheme for cross edge blockchain network," *Journal of Systems Architecture*, vol. 134, p. 102782, 2023.

[93] A. S. Karale and H. Khanuja, "Implementation of blockchain technology in education system," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, pp. 3823–3828, 2019, doi: 10.35940/ijrte.B2462.078219.

[94] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates," *Software: Practice and Experience*, vol. 52, no. 4, pp. 841–867, 2022, doi: 10.1002/spe.2983.

[95] M. M. Merlec, M. M. Islam, Y. K. Lee, and H. P. In, "A consortium blockchain-based secure and trusted electronic portfolio management scheme," *Sensors*, vol. 22, no. 3, p. 1271, 2022, doi: 10.3390/s22031271.

[96] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, "Twisted Edwards curves," in *Proceedings of the International Conference on Computer Science*, 2012, pp. 389–405.

[97] W. Gao, X. Hei, and Y. Wang, "The data privacy protection method for Hyperledger Fabric based on Trustzone," *Mathematics*, vol. 11, no. 6, pp. 1–16, 2023, doi: 10.3390/math11061357.

[98] B. H. Awaji, "The adoption of blockchain technology for developing a trusted achievement record system in higher education," Ph.D. dissertation, Newcastle Univ., 2022.

[99] R. K. Kaushal and N. Kumar, "Exploring Hyperledger Caliper Benchmarking Tool to Measure the Performance of Blockchain-Based Solutions," in *Proceedings of the 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, 2024, pp. 1–6, IEEE.

[100] P. K. Pal, S. Khanna, S. Shukla, and V. Shukla, "Securing and visualizing sensor data on private blockchain," in *Proceedings of the 2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2023, pp. 711–715, IEEE.

Appendix A

Secure Block Cert Framework Evaluation Form

Expert Information:

- **Name**:
- **Affiliation**:
- **Expertise Area**:
- **Years of Experience:**

Evaluation Category:

- ☐ Security Effectiveness
- ☐ Privacy Protection
- ☐ Blockchain Technology

1. Review Feedback:

Clarity and Comprehensiveness:

- **Rating** (Scale of 1-5):
  - ☐ 1 - Very Poor
  - ☐ 2 - Poor
  - ☐ 3 - Average
  - ☐ 4 - Good
  - ☐ 5 - Excellent
- **Comments**:----------
- ----------
- ----------

Thoughts on SecureBlockCert:

- **Comments**:----------
- ----------
- ----------

Innovative Aspects:

- **Comments**:----------
- ----------
- ----------

Concerning Aspects:

- **Comments**:----------

- ----------
- ----------

Recommendations or Areas of Improvement:

- **Comments**: ----------
- ----------
- ----------

2. Interview Feedback:

Security Enhancement:

- **Authentication Mechanisms**:
  - **Assessment**:
    - ☐ Highly Robust
    - ☐ Moderately Robust
    - ☐ Satisfactory
    - ☐ Needs Improvement
  - **Comments**:----------
    - ----------
    - ----------
- **Resilience Against Cyber-Attacks**:
  - **Assessment**:
    - ☐ Highly Resilient
    - ☐ Moderately Resilient
    - ☐ Satisfactory
    - ☐ Vulnerable
  - **Comments**:----------
  - ----------
  - ----------

Privacy Protection:

- **Privacy Enhancement Component**:
  - **Effectiveness Assessment**:
    - ☐ Highly Effective
    - ☐ Moderately Effective
    - ☐ Satisfactory
    - ☐ Ineffective

- **Comments**:----------
- ----------
- ----------

- **Access Control Mechanisms**:
  - **Assessment**:
    - ☐ Highly Secure
    - ☐ Moderately Secure
    - ☐ Satisfactory
    - ☐ Weak
  - **Comments**:----------
  - ----------
  - ----------
- **Homomorphic Encryption and Hashing Techniques**:
  - **Assessment**:
    - ☐ Highly Effective
    - ☐ Moderately Effective
    - ☐ Satisfactory
    - ☐ Ineffective
  - **Comments**:----------

- **Suggestions for Optimization**:
  - **Comments**:----------
  - ----------
- **Blockchain Technology:**

• **Smart Contracts/chain-code:** Evaluate the security measures implemented for smart contracts, such as code auditing and testing.

- **Assessment**
  - - [ ] Highly Secure
  - - [ ] Moderately Secure
  - - [ ] Satisfactory
  - - [ ] Vulnerable

• **Comments:**

• **Data Immutability:** Evaluate the framework's ability to maintain data integrity and prevent unauthorized modifications.

- **Assessment**
  - - [ ] Highly Immutable
  - - [ ] Moderately Immutable
  - - [ ] Satisfactory
  - - [ ] Limited Immutability

• **Comments**: ----------

• **Blockchain Governance:** Evaluate the governance model implemented within the Hyperledger fabric blockchain network and its impact on decision-making and network evolution.

- **Assessment**
  - - [ ] Highly Effective
  - - [ ] Moderately Effective
  - - [ ] Satisfactory
  - - [ ] Ineffective

• **Comments:** ----------

Appendix B

The Overall Verification Form

Please indicate whether the proposed Framework is:

Clear: The framework's objectives and methodologies are articulated clearly and unambiguously.

Comprehensive: The framework accurately addresses the security and privacy concerns of the digital certificates system on the blockchain.

Well-organized: The framework is logically structured and easy to navigate.

Innovative: The framework introduces novel approaches to enhancing the security and privacy of blockchain-based digital certificates.

- **Assessment:**
  - - [ ] Agree
  - - [ ] Diagaree

Comments/ Suggestions:----------

Submission:

- **Date of Submission**: _____
- **Signature**: _____

Appendix C

Experiments of DID and VC Latency

Table 1 *Distribution of DID Issuance Times*

Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency
0	0.007	100	0.009	200	0.015	300	0.008	400	0.013	500	0.013003	600	0.012	700	0.013	800	0.012	900	0.013
1	0.010	101	0.009	201	0.009	301	0.009	401	0.008	501	0.013986	601	0.008	701	0.013	801	0.008	901	0.014
2	0.009	102	0.009	202	0.008	302	0.014	402	0.012	502	0.014005	602	0.013	702	0.013	802	0.009	902	0.013
3	0.009	103	0.008	203	0.008	303	0.013	403	0.014	503	0.012016	603	0.013	703	0.014	803	0.007	903	0.013
4	0.011	104	0.009	204	0.009	304	0.013	404	0.011	504	0.013023	604	0.013	704	0.011	804	0.008	904	0.013
5	0.009	105	0.008	205	0.008	305	0.010	405	0.014	505	0.013019	605	0.009	705	0.013	805	0.013	905	0.012
6	0.010	106	0.009	206	0.008	306	0.010	406	0.012	506	0.013003	606	0.012	706	0.014	806	0.014	906	0.012
7	0.008	107	0.008	207	0.013	307	0.013	407	0.013	507	0.012007	607	0.009	707	0.013	807	0.013	907	0.013
8	0.010	108	0.010	208	0.011	308	0.014	408	0.012	508	0.012002	608	0.014	708	0.014	808	0.012	908	0.013
9	0.009	109	0.008	209	0.008	309	0.010	409	0.009	509	0.013018	609	0.009	709	0.013	809	0.013	909	0.014
10	0.009	110	0.009	210	0.010	310	0.013	410	0.008	510	0.013003	610	0.010	710	0.013	810	0.008	910	0.014
11	0.010	111	0.012	211	0.008	311	0.012	411	0.011	511	0.013003	611	0.008	711	0.013	811	0.012	911	0.013
12	0.008	112	0.007	212	0.012	312	0.012	412	0.011	512	0.012987	612	0.013	712	0.013	812	0.012	912	0.013
13	0.009	113	0.012	213	0.014	313	0.014	413	0.007	513	0.013000	613	0.013	713	0.013	813	0.009	913	0.014
14	0.009	114	0.011	214	0.009	314	0.008	414	0.008	514	0.013003	614	0.011	714	0.013	814	0.014	914	0.013
15	0.011	115	0.008	215	0.008	315	0.009	415	0.008	515	0.013005	615	0.013	715	0.014	815	0.012	915	0.014
16	0.011	116	0.009	216	0.010	316	0.009	416	0.013	516	0.013018	616	0.014	716	0.013	816	0.008	916	0.013
17	0.009	117	0.009	217	0.009	317	0.014	417	0.014	517	0.012998	617	0.013	717	0.013	817	0.012	917	0.013
18	0.014	118	0.009	218	0.009	318	0.011	418	0.008	518	0.013020	618	0.013	718	0.014	818	0.014	918	0.014
19	0.010	119	0.007	219	0.008	319	0.009	419	0.013	519	0.014003	619	0.013	719	0.013	819	0.009	919	0.013
20	0.008	120	0.012	220	0.013	320	0.009	420	0.009	520	0.013020	620	0.013	720	0.013	820	0.009	920	0.012
21	0.009	121	0.008	221	0.010	321	0.012	421	0.012	521	0.012989	621	0.013	721	0.013	821	0.011	921	0.012
22	0.009	122	0.008	222	0.007	322	0.014	422	0.007	522	0.012017	622	0.013	722	0.013	822	0.013	922	0.013

23	0.009	123	0.009	223	0.012	323	0.013	423	0.010	523	0.013019	623	0.012	723	0.014	823	0.012	923	0.014
24	0.013	124	0.010	224	0.013	324	0.008	424	0.012	524	0.013003	624	0.012	724	0.014	824	0.013	924	0.013
25	0.009	125	0.008	225	0.010	325	0.010	425	0.009	525	0.013000	625	0.013	725	0.013	825	0.012	925	0.012
26	0.008	126	0.013	226	0.009	326	0.009	426	0.012	526	0.013020	626	0.012	726	0.013	826	0.008	926	0.012
27	0.012	127	0.008	227	0.010	327	0.009	427	0.009	527	0.013003	627	0.012	727	0.012	827	0.008	927	0.013
28	0.008	128	0.008	228	0.010	328	0.012	428	0.009	528	0.013000	628	0.012	728	0.012	828	0.009	928	0.012
29	0.010	129	0.008	229	0.011	329	0.009	429	0.014	529	0.013005	629	0.013	729	0.013	829	0.008	929	0.013
30	0.010	130	0.012	230	0.008	330	0.008	430	0.008	530	0.017003	630	0.013	730	0.013	830	0.014	930	0.013
31	0.010	131	0.007	231	0.009	331	0.008	431	0.008	531	0.015004	631	0.012	731	0.013	831	0.011	931	0.013
32	0.009	132	0.010	232	0.012	332	0.009	432	0.008	532	0.013001	632	0.013	732	0.013	832	0.013	932	0.013
33	0.009	133	0.008	233	0.013	333	0.008	433	0.013	533	0.014016	633	0.013	733	0.013	833	0.014	933	0.014
34	0.012	134	0.008	234	0.013	334	0.013	434	0.008	534	0.013006	634	0.014	734	0.012	834	0.014	934	0.013
35	0.014	135	0.011	235	0.009	335	0.013	435	0.010	535	0.013989	635	0.014	735	0.013	835	0.012	935	0.014
36	0.009	136	0.007	236	0.013	336	0.010	436	0.009	536	0.013999	636	0.012	736	0.013	836	0.011	936	0.012
37	0.009	137	0.009	237	0.009	337	0.011	437	0.008	537	0.012000	637	0.015	737	0.013	837	0.013	937	0.013
38	0.010	138	0.007	238	0.009	338	0.009	438	0.009	538	0.012002	638	0.013	738	0.014	838	0.009	938	0.013
39	0.012	139	0.009	239	0.008	339	0.011	439	0.007	539	0.012002	639	0.013	739	0.014	839	0.014	939	0.013
40	0.010	140	0.009	240	0.010	340	0.011	440	0.008	540	0.012005	640	0.014	740	0.013	840	0.010	940	0.013
41	0.009	141	0.008	241	0.008	341	0.008	441	0.007	541	0.012992	641	0.013	741	0.013	841	0.013	941	0.013
42	0.011	142	0.012	242	0.013	342	0.014	442	0.011	542	0.013020	642	0.013	742	0.013	842	0.011	942	0.014
43	0.010	143	0.008	243	0.013	343	0.012	443	0.013	543	0.013986	643	0.014	743	0.013	843	0.013	943	0.013
44	0.009	144	0.009	244	0.013	344	0.008	444	0.007	544	0.012020	644	0.012	744	0.014	844	0.011	944	0.013
45	0.009	145	0.008	245	0.011	345	0.008	445	0.009	545	0.012002	645	0.013	745	0.014	845	0.012	945	0.012
46	0.008	146	0.010	246	0.008	346	0.008	446	0.007	546	0.013020	646	0.014	746	0.014	846	0.013	946	0.013
47	0.009	147	0.009	247	0.009	347	0.008	447	0.012	547	0.012007	647	0.015	747	0.014	847	0.009	947	0.012
48	0.008	148	0.009	248	0.012	348	0.013	448	0.013	548	0.011892	648	0.014	748	0.014	848	0.009	948	0.013
49	0.009	149	0.007	249	0.009	349	0.008	449	0.008	549	0.013021	649	0.013	749	0.013	849	0.008	949	0.013
50	0.009	150	0.008	250	0.011	350	0.015	450	0.009	550	0.012025	650	0.013	750	0.013	850	0.013	950	0.013
51	0.008	151	0.013	251	0.011	351	0.013	451	0.010	551	0.013003	651	0.012	751	0.013	851	0.011	951	0.014

52	0.009	152	0.009	252	0.008	352	0.011	452	0.013	552	0.011984	652	0.014	752	0.013	852	0.008	952	0.012
53	0.009	153	0.009	253	0.011	353	0.008	453	0.009	553	0.012025	653	0.013	753	0.013	853	0.013	953	0.013
54	0.010	154	0.007	254	0.012	354	0.011	454	0.011	554	0.012988	654	0.014	754	0.013	854	0.011	954	0.013
55	0.011	155	0.010	255	0.008	355	0.012	455	0.014	555	0.012019	655	0.014	755	0.014	855	0.013	955	0.014
56	0.008	156	0.008	256	0.012	356	0.009	456	0.012	556	0.013002	656	0.012	756	0.014	856	0.008	956	0.013
57	0.009	157	0.010	257	0.008	357	0.015	457	0.014	557	0.013003	657	0.013	757	0.013	857	0.013	957	0.012
58	0.008	158	0.009	258	0.010	358	0.013	458	0.014	558	0.013003	658	0.012	758	0.014	858	0.008	958	0.014
59	0.010	159	0.013	259	0.013	359	0.013	459	0.013	559	0.013003	659	0.013	759	0.013	859	0.013	959	0.013
60	0.009	160	0.011	260	0.012	360	0.008	460	0.014	560	0.013003	660	0.012	760	0.014	860	0.013	960	0.014
61	0.010	161	0.008	261	0.009	361	0.013	461	0.013	561	0.013002	661	0.008	761	0.013	861	0.013	961	0.015
62	0.010	162	0.013	262	0.013	362	0.009	462	0.013	562	0.012986	662	0.013	762	0.013	862	0.009	962	0.014
63	0.008	163	0.012	263	0.012	363	0.011	463	0.013	563	0.014020	663	0.013	763	0.013	863	0.013	963	0.013
64	0.009	164	0.008	264	0.011	364	0.014	464	0.013	564	0.012001	664	0.009	764	0.012	864	0.013	964	0.013
65	0.008	165	0.014	265	0.011	365	0.013	465	0.013	565	0.012849	665	0.010	765	0.013	865	0.013	965	0.013
66	0.011	166	0.013	266	0.008	366	0.009	466	0.012	566	0.013003	666	0.013	766	0.013	866	0.010	966	0.013
67	0.010	167	0.012	267	0.014	367	0.013	467	0.012	567	0.012002	667	0.011	767	0.014	867	0.012	967	0.013
68	0.009	168	0.012	268	0.014	368	0.013	468	0.013	568	0.013006	668	0.013	768	0.013	868	0.010	968	0.012
69	0.010	169	0.008	269	0.009	369	0.010	469	0.013	569	0.012020	669	0.013	769	0.014	869	0.010	969	0.013
70	0.009	170	0.009	270	0.013	370	0.008	470	0.013	570	0.012000	670	0.013	770	0.014	870	0.009	970	0.012
71	0.011	171	0.007	271	0.013	371	0.012	471	0.012	571	0.012719	671	0.013	771	0.013	871	0.013	971	0.013
72	0.010	172	0.012	272	0.009	372	0.013	472	0.014	572	0.014003	672	0.013	772	0.013	872	0.010	972	0.013
73	0.009	173	0.010	273	0.012	373	0.012	473	0.014	573	0.014020	673	0.013	773	0.013	873	0.014	973	0.012
74	0.012	174	0.009	274	0.008	374	0.007	474	0.012	574	0.013003	674	0.012	774	0.012	874	0.013	974	0.012
75	0.009	175	0.009	275	0.011	375	0.009	475	0.013	575	0.013002	675	0.013	775	0.013	875	0.013	975	0.012
76	0.010	176	0.011	276	0.008	376	0.008	476	0.013	576	0.014003	676	0.014	776	0.013	876	0.015	976	0.012
77	0.009	177	0.014	277	0.013	377	0.013	477	0.013	577	0.013003	677	0.012	777	0.014	877	0.012	977	0.013
78	0.009	178	0.008	278	0.010	378	0.012	478	0.013	578	0.012987	678	0.012	778	0.013	878	0.009	978	0.012
79	0.011	179	0.011	279	0.013	379	0.013	479	0.012	579	0.013018	679	0.013	779	0.014	879	0.013	979	0.013
80	0.009	180	0.014	280	0.014	380	0.013	480	0.013	580	0.013986	680	0.012	780	0.013	880	0.014	980	0.013

81	0.011	181	0.014	281	0.015	381	0.012	481	0.013	581	0.013021	681	0.012	781	0.013	881	0.009	981	0.013
82	0.011	182	0.009	282	0.008	382	0.013	482	0.013	582	0.013002	682	0.013	782	0.014	882	0.012	982	0.014
83	0.009	183	0.012	283	0.008	383	0.013	483	0.013	583	0.012986	683	0.013	783	0.014	883	0.013	983	0.013
84	0.009	184	0.013	284	0.010	384	0.013	484	0.013	584	0.012002	684	0.013	784	0.013	884	0.008	984	0.013
85	0.009	185	0.013	285	0.013	385	0.013	485	0.013	585	0.013020	685	0.013	785	0.013	885	0.013	985	0.013
86	0.010	186	0.008	286	0.012	386	0.014	486	0.009	586	0.013003	686	0.014	786	0.013	886	0.009	986	0.013
87	0.010	187	0.007	287	0.013	387	0.014	487	0.010	587	0.013004	687	0.012	787	0.013	887	0.007	987	0.013
88	0.008	188	0.009	288	0.009	388	0.013	488	0.013	588	0.013001	688	0.013	788	0.014	888	0.013	988	0.013
89	0.011	189	0.008	289	0.008	389	0.013	489	0.009	589	0.012019	689	0.013	789	0.013	889	0.013	989	0.013
90	0.010	190	0.009	290	0.013	390	0.013	490	0.012	590	0.013020	690	0.012	790	0.013	890	0.013	990	0.014
91	0.010	191	0.014	291	0.014	391	0.013	491	0.013	591	0.014004	691	0.013	791	0.012	891	0.013	991	0.013
92	0.011	192	0.012	292	0.008	392	0.013	492	0.013	592	0.013003	692	0.013	792	0.012	892	0.009	992	0.014
93	0.010	193	0.014	293	0.013	393	0.013	493	0.009	593	0.012988	693	0.013	793	0.012	893	0.008	993	0.013
94	0.010	194	0.013	294	0.009	394	0.014	494	0.008	594	0.012192	694	0.013	794	0.012	894	0.008	994	0.014
95	0.010	195	0.010	295	0.007	395	0.013	495	0.013	595	0.011020	695	0.013	795	0.013	895	0.013	995	0.014
96	0.010	196	0.013	296	0.011	396	0.014	496	0.013	596	0.008877	696	0.013	796	0.014	896	0.012	996	0.017
97	0.011	197	0.009	297	0.014	397	0.013	497	0.013	597	0.013998	697	0.013	797	0.014	897	0.008	997	0.014
98	0.009	198	0.010	298	0.008	398	0.013	498	0.009	598	0.012019	698	0.014	798	0.014	898	0.014	998	0.014
99	0.010	199	0.009	299	0.009	399	0.009	499	0.013	599	0.009002	699	0.013	799	0.010	899	0.013	999	0.014

Table 2 *Distribution of DID Verification Times*

Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency
0	0.010	100	0.008	200	0.011	300	0.006	400	0.006	500	0.003	600	0.004	700	0.003	800	0.009	900	0.004
1	0.010	101	0.015	201	0.010	301	0.007	401	0.006	501	0.004	601	0.004	701	0.006	801	0.010	901	0.003
2	0.010	102	0.011	202	0.005	302	0.006	402	0.006	502	0.004	602	0.005	702	0.004	802	0.010	902	0.004
3	0.011	103	0.012	203	0.010	303	0.006	403	0.005	503	0.004	603	0.003	703	0.003	803	0.010	903	0.003
4	0.010	104	0.006	204	0.005	304	0.006	404	0.005	504	0.003	604	0.005	704	0.008	804	0.010	904	0.004

5	0.010	105	0.010	205	0.011	305	0.006	405	0.006	505	0.003	605	0.003	705	0.003	805	0.010	905	0.004
6	0.010	106	0.008	206	0.006	306	0.005	406	0.005	506	0.004	606	0.005	706	0.003	806	0.010	906	0.003
7	0.007	107	0.010	207	0.011	307	0.005	407	0.005	507	0.004	607	0.003	707	0.003	807	0.011	907	0.005
8	0.008	108	0.005	208	0.008	308	0.005	408	0.005	508	0.004	608	0.003	708	0.003	808	0.011	908	0.003
9	0.010	109	0.010	209	0.009	309	0.007	409	0.005	509	0.004	609	0.003	709	0.003	809	0.010	909	0.005
10	0.010	110	0.021	210	0.006	310	0.007	410	0.006	510	0.003	610	0.003	710	0.004	810	0.010	910	0.003
11	0.010	111	0.021	211	0.008	311	0.005	411	0.006	511	0.004	611	0.005	711	0.004	811	0.010	911	0.003
12	0.011	112	0.022	212	0.006	312	0.006	412	0.005	512	0.004	612	0.003	712	0.003	812	0.010	912	0.003
13	0.010	113	0.024	213	0.007	313	0.007	413	0.005	513	0.004	613	0.005	713	0.003	813	0.010	913	0.004
14	0.010	114	0.021	214	0.010	314	0.007	414	0.005	514	0.004	614	0.003	714	0.003	814	0.011	914	0.004
15	0.009	115	0.027	215	0.009	315	0.006	415	0.006	515	0.003	615	0.004	715	0.003	815	0.010	915	0.003
16	0.010	116	0.017	216	0.006	316	0.005	416	0.005	516	0.004	616	0.003	716	0.005	816	0.010	916	0.005
17	0.010	117	0.015	217	0.011	317	0.006	417	0.005	517	0.003	617	0.003	717	0.003	817	0.010	917	0.003
18	0.009	118	0.024	218	0.006	318	0.006	418	0.007	518	0.004	618	0.003	718	0.003	818	0.009	918	0.003
19	0.010	119	0.017	219	0.005	319	0.006	419	0.005	519	0.003	619	0.003	719	0.003	819	0.004	919	0.003
20	0.010	120	0.027	220	0.006	320	0.005	420	0.005	520	0.003	620	0.003	720	0.003	820	0.004	920	0.003
21	0.010	121	0.026	221	0.008	321	0.007	421	0.005	521	0.003	621	0.003	721	0.004	821	0.004	921	0.004
22	0.010	122	0.027	222	0.005	322	0.007	422	0.005	522	0.004	622	0.003	722	0.003	822	0.004	922	0.003
23	0.010	123	0.025	223	0.010	323	0.006	423	0.006	523	0.005	623	0.004	723	0.003	823	0.004	923	0.004
24	0.010	124	0.026	224	0.008	324	0.007	424	0.005	524	0.004	624	0.004	724	0.005	824	0.003	924	0.004
25	0.010	125	0.026	225	0.006	325	0.007	425	0.006	525	0.004	625	0.003	725	0.003	825	0.005	925	0.004
26	0.010	126	0.026	226	0.011	326	0.006	426	0.005	526	0.004	626	0.004	726	0.003	826	0.003	926	0.003
27	0.010	127	0.026	227	0.006	327	0.006	427	0.005	527	0.003	627	0.003	727	0.003	827	0.004	927	0.003
28	0.010	128	0.025	228	0.008	328	0.007	428	0.005	528	0.003	628	0.003	728	0.003	828	0.006	928	0.005
29	0.010	129	0.022	229	0.008	329	0.006	429	0.007	529	0.004	629	0.003	729	0.004	829	0.003	929	0.004
30	0.010	130	0.023	230	0.005	330	0.006	430	0.005	530	0.004	630	0.005	730	0.003	830	0.003	930	0.003
31	0.010	131	0.019	231	0.011	331	0.005	431	0.004	531	0.005	631	0.003	731	0.004	831	0.003	931	0.004
32	0.010	132	0.019	232	0.008	332	0.008	432	0.005	532	0.003	632	0.004	732	0.003	832	0.003	932	0.003
33	0.010	133	0.020	233	0.006	333	0.007	433	0.005	533	0.003	633	0.003	733	0.003	833	0.003	933	0.003

34	0.010	134	0.012	234	0.010	334	0.007	434	0.005	534	0.003	634	0.004	734	0.004	834	0.003	934	0.003
35	0.010	135	0.010	235	0.010	335	0.006	435	0.005	535	0.003	635	0.003	735	0.003	835	0.004	935	0.003
36	0.011	136	0.006	236	0.010	336	0.005	436	0.006	536	0.003	636	0.003	736	0.004	836	0.003	936	0.003
37	0.012	137	0.006	237	0.010	337	0.006	437	0.005	537	0.004	637	0.003	737	0.005	837	0.004	937	0.003
38	0.011	138	0.007	238	0.010	338	0.005	438	0.004	538	0.004	638	0.004	738	0.005	838	0.003	938	0.004
39	0.012	139	0.007	239	0.010	339	0.008	439	0.004	539	0.005	639	0.003	739	0.008	839	0.003	939	0.003
40	0.007	140	0.007	240	0.010	340	0.006	440	0.005	540	0.004	640	0.003	740	0.005	840	0.004	940	0.005
41	0.007	141	0.006	241	0.010	341	0.006	441	0.005	541	0.004	641	0.004	741	0.005	841	0.003	941	0.004
42	0.011	142	0.008	242	0.011	342	0.006	442	0.004	542	0.003	642	0.003	742	0.004	842	0.003	942	0.004
43	0.010	143	0.007	243	0.010	343	0.006	443	0.004	543	0.006	643	0.004	743	0.004	843	0.003	943	0.004
44	0.011	144	0.006	244	0.010	344	0.005	444	0.004	544	0.004	644	0.003	744	0.004	844	0.003	944	0.004
45	0.010	145	0.006	245	0.010	345	0.006	445	0.007	545	0.003	645	0.004	745	0.004	845	0.004	945	0.003
46	0.010	146	0.006	246	0.010	346	0.006	446	0.004	546	0.003	646	0.003	746	0.003	846	0.003	946	0.003
47	0.010	147	0.006	247	0.010	347	0.006	447	0.004	547	0.003	647	0.004	747	0.003	847	0.004	947	0.005
48	0.010	148	0.006	248	0.010	348	0.006	448	0.004	548	0.004	648	0.005	748	0.004	848	0.005	948	0.003
49	0.010	149	0.008	249	0.010	349	0.007	449	0.005	549	0.004	649	0.004	749	0.003	849	0.003	949	0.004
50	0.010	150	0.007	250	0.010	350	0.006	450	0.005	550	0.003	650	0.004	750	0.004	850	0.004	950	0.003
51	0.010	151	0.007	251	0.011	351	0.007	451	0.004	551	0.006	651	0.003	751	0.004	851	0.004	951	0.003
52	0.008	152	0.007	252	0.011	352	0.006	452	0.004	552	0.006	652	0.003	752	0.005	852	0.003	952	0.004
53	0.006	153	0.007	253	0.010	353	0.006	453	0.004	553	0.004	653	0.004	753	0.004	853	0.003	953	0.003
54	0.006	154	0.005	254	0.010	354	0.005	454	0.004	554	0.004	654	0.003	754	0.004	854	0.005	954	0.003
55	0.006	155	0.006	255	0.009	355	0.005	455	0.004	555	0.004	655	0.003	755	0.004	855	0.003	955	0.003
56	0.006	156	0.006	256	0.011	356	0.005	456	0.004	556	0.004	656	0.003	756	0.003	856	0.003	956	0.003
57	0.006	157	0.007	257	0.009	357	0.006	457	0.004	557	0.003	657	0.003	757	0.003	857	0.004	957	0.005
58	0.006	158	0.007	258	0.011	358	0.005	458	0.004	558	0.003	658	0.005	758	0.004	858	0.004	958	0.004
59	0.007	159	0.007	259	0.010	359	0.006	459	0.004	559	0.005	659	0.003	759	0.003	859	0.004	959	0.003
60	0.007	160	0.005	260	0.011	360	0.006	460	0.004	560	0.003	660	0.004	760	0.004	860	0.004	960	0.005
61	0.006	161	0.006	261	0.010	361	0.006	461	0.004	561	0.004	661	0.004	761	0.003	861	0.003	961	0.003
62	0.005	162	0.005	262	0.009	362	0.006	462	0.004	562	0.004	662	0.003	762	0.003	862	0.003	962	0.004

63	0.006	163	0.006	263	0.010	363	0.005	463	0.004	563	0.004	663	0.003	763	0.004	863	0.005	963	0.003
64	0.006	164	0.005	264	0.010	364	0.006	464	0.004	564	0.003	664	0.003	764	0.004	864	0.004	964	0.003
65	0.006	165	0.007	265	0.011	365	0.005	465	0.004	565	0.004	665	0.003	765	0.003	865	0.004	965	0.004
66	0.005	166	0.007	266	0.009	366	0.006	466	0.004	566	0.003	666	0.003	766	0.003	866	0.004	966	0.003
67	0.007	167	0.006	267	0.006	367	0.006	467	0.004	567	0.004	667	0.003	767	0.003	867	0.004	967	0.004
68	0.008	168	0.006	268	0.006	368	0.006	468	0.004	568	0.005	668	0.004	768	0.003	868	0.003	968	0.003
69	0.006	169	0.005	269	0.006	369	0.006	469	0.004	569	0.003	669	0.004	769	0.003	869	0.003	969	0.004
70	0.007	170	0.005	270	0.007	370	0.006	470	0.006	570	0.005	670	0.004	770	0.004	870	0.004	970	0.004
71	0.006	171	0.006	271	0.005	371	0.005	471	0.004	571	0.003	671	0.003	771	0.003	871	0.005	971	0.004
72	0.005	172	0.006	272	0.005	372	0.005	472	0.004	572	0.003	672	0.003	772	0.003	872	0.004	972	0.003
73	0.005	173	0.005	273	0.005	373	0.005	473	0.005	573	0.003	673	0.005	773	0.003	873	0.003	973	0.004
74	0.005	174	0.006	274	0.005	374	0.006	474	0.004	574	0.004	674	0.003	774	0.004	874	0.005	974	0.003
75	0.006	175	0.005	275	0.005	375	0.005	475	0.004	575	0.004	675	0.004	775	0.009	875	0.003	975	0.004
76	0.012	176	0.007	276	0.005	376	0.006	476	0.004	576	0.005	676	0.003	776	0.003	876	0.004	976	0.005
77	0.011	177	0.007	277	0.005	377	0.005	477	0.003	577	0.003	677	0.004	777	0.004	877	0.003	977	0.003
78	0.011	178	0.006	278	0.005	378	0.006	478	0.004	578	0.004	678	0.004	778	0.003	878	0.003	978	0.004
79	0.010	179	0.006	279	0.006	379	0.006	479	0.004	579	0.003	679	0.003	779	0.003	879	0.003	979	0.003
80	0.010	180	0.005	280	0.006	380	0.006	480	0.004	580	0.004	680	0.003	780	0.003	880	0.004	980	0.005
81	0.010	181	0.005	281	0.006	381	0.006	481	0.004	581	0.003	681	0.005	781	0.003	881	0.003	981	0.005
82	0.010	182	0.005	282	0.005	382	0.006	482	0.003	582	0.003	682	0.004	782	0.010	882	0.004	982	0.003
83	0.008	183	0.005	283	0.006	383	0.005	483	0.004	583	0.003	683	0.003	783	0.010	883	0.003	983	0.003
84	0.010	184	0.005	284	0.006	384	0.006	484	0.005	584	0.003	684	0.005	784	0.010	884	0.004	984	0.003
85	0.010	185	0.006	285	0.005	385	0.006	485	0.004	585	0.004	685	0.004	785	0.010	885	0.005	985	0.003
86	0.009	186	0.005	286	0.006	386	0.006	486	0.004	586	0.003	686	0.008	786	0.010	886	0.004	986	0.005
87	0.008	187	0.006	287	0.005	387	0.006	487	0.003	587	0.005	687	0.004	787	0.010	887	0.004	987	0.004
88	0.009	188	0.006	288	0.006	388	0.006	488	0.004	588	0.003	688	0.003	788	0.011	888	0.003	988	0.004
89	0.008	189	0.005	289	0.005	389	0.006	489	0.003	589	0.003	689	0.005	789	0.010	889	0.005	989	0.004
90	0.008	190	0.005	290	0.006	390	0.006	490	0.004	590	0.003	690	0.003	790	0.010	890	0.005	990	0.003
91	0.009	191	0.005	291	0.006	391	0.005	491	0.004	591	0.003	691	0.003	791	0.010	891	0.003	991	0.004

92	0.014	192	0.006	292	0.006	392	0.006	492	0.003	592	0.004	692	0.003	792	0.010	892	0.003	992	0.003
93	0.007	193	0.007	293	0.007	393	0.011	493	0.003	593	0.003	693	0.004	793	0.010	893	0.003	993	0.003
94	0.008	194	0.007	294	0.006	394	0.009	494	0.004	594	0.004	694	0.003	794	0.010	894	0.003	994	0.003
95	0.012	195	0.007	295	0.006	395	0.006	495	0.005	595	0.003	695	0.008	795	0.010	895	0.003	995	0.004
96	0.019	196	0.009	296	0.006	396	0.007	496	0.004	596	0.003	696	0.003	796	0.010	896	0.003	996	0.003
97	0.021	197	0.006	297	0.005	397	0.005	497	0.004	597	0.003	697	0.004	797	0.010	897	0.004	997	0.003
98	0.011	198	0.006	298	0.005	398	0.006	498	0.003	598	0.004	698	0.003	798	0.010	898	0.003	998	0.004
99	0.014	199	0.007	299	0.006	399	0.006	499	0.003	599	0.005	699	0.004	799	0.010	899	0.005	999	0003

Table 3 *Distribution of DID authentication time*

Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency
0	0.011003	100	0.010984	200	0.010009	300	0.005019	400	0.005998	500	0.004007	600	0.003008	700	0.004009	800	0.010000	900	0.003999
1	0.011009	101	0.011023	201	0.007004	301	0.005020	401	0.006001	501	0.003009	601	0.004009	701	0.004006	801	0.011002	901	0.004013
2	0.011020	102	0.016016	202	0.005997	302	0.005020	402	0.006002	502	0.003010	602	0.003015	702	0.005016	802	0.010001	902	0.003999
3	0.010004	103	0.009019	203	0.008000	303	0.007019	403	0.005997	503	0.004004	603	0.003998	703	0.004030	803	0.011002	903	0.004023
4	0.010001	104	0.006018	204	0.006017	304	0.005000	404	0.005999	504	0.003999	604	0.005004	704	0.004999	804	0.011006	904	0.004001
5	0.010019	105	0.012002	205	0.008000	305	0.005002	405	0.005002	505	0.004009	605	0.004007	705	0.006009	805	0.010019	905	0.004001
6	0.010002	106	0.006019	206	0.010024	306	0.006003	406	0.008001	506	0.004009	606	0.003988	706	0.004984	806	0.009995	906	0.004001
7	0.005833	107	0.010998	207	0.010001	307	0.005990	407	0.006002	507	0.006010	607	0.004011	707	0.004000	807	0.010023	907	0.004001
8	0.004898	108	0.008020	208	0.009016	308	0.007000	408	0.006998	508	0.003006	608	0.004989	708	0.004006	808	0.009999	908	0.003009
9	0.010013	109	0.012020	209	0.006017	309	0.005654	409	0.006019	509	0.004007	609	0.005002	709	0.003999	809	0.010002	909	0.003007
10	0.010019	110	0.016007	210	0.006021	310	0.006999	410	0.005002	510	0.004021	610	0.003992	710	0.004002	810	0.009985	910	0.002999
11	0.010017	111	0.022988	211	0.008018	311	0.006008	411	0.006002	511	0.003999	611	0.003010	711	0.003998	811	0.010001	911	0.005006
12	0.010002	112	0.022016	212	0.006001	312	0.006019	412	0.006020	512	0.004008	612	0.003001	712	0.003999	812	0.010018	912	0.004015
13	0.012002	113	0.025022	213	0.007019	313	0.006019	413	0.005019	513	0.004009	613	0.004012	713	0.005010	813	0.009986	913	0.004006
14	0.013006	114	0.025006	214	0.009996	314	0.005990	414	0.004990	514	0.005001	614	0.004008	714	0.003003	814	0.010015	914	0.003987
15	0.010020	115	0.009003	215	0.005019	315	0.005999	415	0.006011	515	0.004013	615	0.004007	715	0.003989	815	0.011008	915	0.003000

16	0.010016	116	0.023022	216	0.010987	316	0.005578	416	0.005019	516	0.004003	616	0.003798	716	0.004015	816	0.010005	916	0.005016
17	0.010018	117	0.024028	217	0.005016	317	0.005018	417	0.005013	517	0.004001	617	0.004006	717	0.004016	817	0.011000	917	0.003006
18	0.012003	118	0.021004	218	0.006019	318	0.005000	418	0.005019	518	0.004012	618	0.004001	718	0.005023	818	0.010020	918	0.004002
19	0.011014	119	0.018021	219	0.010001	319	0.006000	419	0.005018	519	0.004009	619	0.003999	719	0.005022	819	0.006002	919	0.004005
20	0.011019	120	0.027005	220	0.007018	320	0.006989	420	0.005000	520	0.004002	620	0.005013	720	0.004020	820	0.003999	920	0.003954
21	0.011009	121	0.026005	221	0.007023	321	0.006992	421	0.005001	521	0.004007	621	0.004012	721	0.004000	821	0.004001	921	0.003002
22	0.011002	122	0.025004	222	0.010002	322	0.005018	422	0.006002	522	0.002954	622	0.005001	722	0.003007	822	0.004008	922	0.005002
23	0.011001	123	0.026006	223	0.009001	323	0.006001	423	0.006001	523	0.003014	623	0.003012	723	0.004010	823	0.004000	923	0.003999
24	0.009985	124	0.025003	224	0.006018	324	0.006020	424	0.005994	524	0.004001	624	0.003009	724	0.003016	824	0.003000	924	0.003991
25	0.010002	125	0.027006	225	0.011013	325	0.006020	425	0.004996	525	0.003008	625	0.004006	725	0.003993	825	0.004005	925	0.005008
26	0.010002	126	0.027023	226	0.006000	326	0.005008	426	0.005000	526	0.003010	626	0.004009	726	0.004999	826	0.005018	926	0.004023
27	0.010025	127	0.026023	227	0.006023	327	0.006000	427	0.005018	527	0.004007	627	0.004013	727	0.004013	827	0.003008	927	0.003001
28	0.010018	128	0.026026	228	0.011019	328	0.004980	428	0.006002	528	0.004006	628	0.004001	728	0.004007	828	0.004012	928	0.004001
29	0.011003	129	0.023002	229	0.009018	329	0.006021	429	0.010002	529	0.004008	629	0.004014	729	0.003006	829	0.004000	929	0.004018
30	0.010994	130	0.023002	230	0.009002	330	0.007002	430	0.008002	530	0.003013	630	0.003995	730	0.003013	830	0.004012	930	0.004001
31	0.011013	131	0.021021	231	0.010984	331	0.010010	431	0.007001	531	0.003993	631	0.003014	731	0.003011	831	0.003989	931	0.004000
32	0.011019	132	0.019004	232	0.007001	332	0.009001	432	0.005002	532	0.005997	632	0.003007	732	0.005012	832	0.004006	932	0.004025
33	0.010019	133	0.021002	233	0.006001	333	0.009001	433	0.004000	533	0.004000	633	0.003006	733	0.003008	833	0.004001	933	0.004001
34	0.010025	134	0.012001	234	0.010017	334	0.005002	434	0.004003	534	0.004006	634	0.004000	734	0.003002	834	0.003999	934	0.004001
35	0.010025	135	0.008001	235	0.008014	335	0.004999	435	0.005001	535	0.003006	635	0.004014	735	0.004008	835	0.004001	935	0.005001
36	0.010019	136	0.008002	236	0.010020	336	0.006012	436	0.005018	536	0.002998	636	0.005004	736	0.004000	836	0.003995	936	0.004000
37	0.011020	137	0.007004	237	0.010024	337	0.004990	437	0.004000	537	0.003010	637	0.003987	737	0.004016	837	0.004004	937	0.003000
38	0.010002	138	0.006008	238	0.010025	338	0.005999	438	0.005017	538	0.003013	638	0.005002	738	0.004002	838	0.003999	938	0.003012
39	0.011002	139	0.007019	239	0.010005	339	0.006001	439	0.004996	539	0.004016	639	0.005017	739	0.006002	839	0.004006	939	0.004000
40	0.010998	140	0.006020	240	0.010018	340	0.007009	440	0.005000	540	0.003002	640	0.004001	740	0.003993	840	0.003001	940	0.004001
41	0.006025	141	0.007019	241	0.009983	341	0.005000	441	0.004000	541	0.004010	641	0.004000	741	0.018107	841	0.004002	941	0.003000
42	0.011009	142	0.006001	242	0.010025	342	0.005994	442	0.005010	542	0.004000	642	0.003008	742	0.005112	842	0.004000	942	0.004001
43	0.009017	143	0.006000	243	0.011019	343	0.007015	443	0.004008	543	0.004006	643	0.005013	743	0.004008	843	0.004005	943	0.003000
44	0.010019	144	0.006002	244	0.010018	344	0.007020	444	0.005010	544	0.004015	644	0.005014	744	0.004007	844	0.003999	944	0.003000

45	0.010020	145	0.006001	245	0.009997	345	0.006001	445	0.003991	545	0.004000	645	0.004995	745	0.004003	845	0.004002	945	0.004001
46	0.009980	146	0.006001	246	0.011008	346	0.005001	446	0.005019	546	0.004013	646	0.003009	746	0.004014	846	0.005004	946	0.004001
47	0.009985	147	0.007009	247	0.010018	347	0.004982	447	0.005023	547	0.004008	647	0.003006	747	0.005012	847	0.003007	947	0.003000
48	0.010020	148	0.006001	248	0.011024	348	0.004982	448	0.006020	548	0.003006	648	0.003001	748	0.003982	848	0.003001	948	0.004018
49	0.010002	149	0.006023	249	0.011001	349	0.005001	449	0.004993	549	0.002994	649	0.003991	749	0.004006	849	0.005008	949	0.006001
50	0.009991	150	0.007001	250	0.010024	350	0.005992	450	0.005022	550	0.004015	650	0.003999	750	0.004000	850	0.004013	950	0.004001
51	0.010018	151	0.006018	251	0.010017	351	0.005993	451	0.005017	551	0.003009	651	0.003990	751	0.005022	851	0.004021	951	0.004000
52	0.010024	152	0.005019	252	0.010002	352	0.006019	452	0.005011	552	0.003015	652	0.003998	752	0.003995	852	0.004023	952	0.004001
53	0.006990	153	0.006023	253	0.010008	353	0.006016	453	0.005014	553	0.002995	653	0.003006	753	0.006983	853	0.003000	953	0.004001
54	0.005990	154	0.007010	254	0.010020	354	0.006001	454	0.005016	554	0.005008	654	0.003841	754	0.004000	854	0.004018	954	0.004017
55	0.007001	155	0.006010	255	0.011004	355	0.006022	455	0.004019	555	0.004002	655	0.005004	755	0.003016	855	0.003000	955	0.004001
56	0.007013	156	0.006000	256	0.010001	356	0.006009	456	0.004016	556	0.003005	656	0.003006	756	0.004104	856	0.004001	956	0.004001
57	0.006016	157	0.005983	257	0.011000	357	0.006000	457	0.005012	557	0.003995	657	0.004008	757	0.003990	857	0.003009	957	0.005002
58	0.007010	158	0.006093	258	0.009999	358	0.005997	458	0.004022	558	0.005002	658	0.003001	758	0.004996	858	0.002998	958	0.003010
59	0.007007	159	0.006011	259	0.011023	359	0.006006	459	0.004018	559	0.004010	659	0.003008	759	0.003009	859	0.003010	959	0.004002
60	0.006016	160	0.006008	260	0.009018	360	0.005992	460	0.004994	560	0.003993	660	0.004006	760	0.003009	860	0.003013	960	0.003002
61	0.007017	161	0.005019	261	0.009985	361	0.005020	461	0.004001	561	0.003994	661	0.003010	761	0.003006	861	0.005001	961	0.003022
62	0.007001	162	0.007004	262	0.011019	362	0.005012	462	0.004019	562	0.003000	662	0.005996	762	0.003012	862	0.004000	962	0.005012
63	0.005006	163	0.008018	263	0.012015	363	0.006018	463	0.004994	563	0.004010	663	0.004000	763	0.003000	863	0.004011	963	0.003009
64	0.006024	164	0.006006	264	0.010017	364	0.005009	464	0.004003	564	0.003012	664	0.004997	764	0.003001	864	0.004008	964	0.004012
65	0.006982	165	0.006023	265	0.008019	365	0.005993	465	0.004992	565	0.004988	665	0.003999	765	0.005008	865	0.003008	965	0.004018
66	0.007019	166	0.005023	266	0.011002	366	0.006001	466	0.003993	566	0.002998	666	0.003843	766	0.004264	866	0.003002	966	0.003009
67	0.007014	167	0.005019	267	0.006018	367	0.006001	467	0.004011	567	0.004961	667	0.004001	767	0.003013	867	0.003000	967	0.003941
68	0.006023	168	0.005002	268	0.006000	368	0.005009	468	0.004019	568	0.004002	668	0.003011	768	0.004011	868	0.004010	968	0.002998
69	0.006002	169	0.006012	269	0.006001	369	0.005007	469	0.004004	569	0.003994	669	0.003016	769	0.003001	869	0.004016	969	0.005014
70	0.005009	170	0.007297	270	0.006015	370	0.006001	470	0.004001	570	0.004000	670	0.004995	770	0.003988	870	0.003004	970	0.002999
71	0.006016	171	0.006001	271	0.005994	371	0.006021	471	0.003010	571	0.005016	671	0.003006	771	0.003981	871	0.003007	971	0.003011
72	0.006022	172	0.006001	272	0.005012	372	0.006011	472	0.004007	572	0.004006	672	0.003999	772	0.004007	872	0.004010	972	0.003009
73	0.006022	173	0.006019	273	0.005989	373	0.005018	473	0.006006	573	0.002994	673	0.002994	773	0.003000	873	0.004007	973	0.002995

74	0.006019	174	0.005014	274	0.007017	374	0.006000	474	0.004004	574	0.003009	674	0.003018	774	0.003002	874	0.003007	974	0.003006
75	0.011001	175	0.005019	275	0.006993	375	0.006003	475	0.004006	575	0.003016	675	0.004000	775	0.009013	875	0.004011	975	0.004011
76	0.009001	176	0.006011	276	0.006994	376	0.006019	476	0.004010	576	0.004015	676	0.004001	776	0.004000	876	0.003011	976	0.003006
77	0.012003	177	0.007019	277	0.008010	377	0.006002	477	0.005076	577	0.004006	677	0.004001	777	0.003001	877	0.004000	977	0.004008
78	0.010023	178	0.007002	278	0.006010	378	0.006011	478	0.005002	578	0.005010	678	0.003001	778	0.004017	878	0.004010	978	0.002995
79	0.010029	179	0.006019	279	0.004999	379	0.006015	479	0.003997	579	0.004013	679	0.005001	779	0.003002	879	0.004002	979	0.003999
80	0.010010	180	0.006006	280	0.006018	380	0.006011	480	0.004001	580	0.004995	680	0.004001	780	0.003017	880	0.002999	980	0.004009
81	0.010019	181	0.010011	281	0.005980	381	0.006000	481	0.005000	581	0.004016	681	0.003000	781	0.003018	881	0.003010	981	0.003015
82	0.008004	182	0.008023	282	0.006012	382	0.006012	482	0.004011	582	0.004013	682	0.003008	782	0.005022	882	0.003992	982	0.005008
83	0.010016	183	0.006011	283	0.006020	383	0.006018	483	0.005018	583	0.004016	683	0.005003	783	0.008001	883	0.002994	983	0.004004
84	0.009012	184	0.007023	284	0.006002	384	0.006001	484	0.004017	584	0.003990	684	0.002996	784	0.010018	884	0.003008	984	0.003999
85	0.009019	185	0.007022	285	0.006001	385	0.006012	485	0.004010	585	0.003016	685	0.003012	785	0.010002	885	0.004006	985	0.003998
86	0.009014	186	0.008006	286	0.006000	386	0.006012	486	0.005000	586	0.003000	686	0.004004	786	0.010020	886	0.003009	986	0.002987
87	0.009994	187	0.006016	287	0.006001	387	0.006009	487	0.004007	587	0.004015	687	0.002999	787	0.010018	887	0.003008	987	0.003013
88	0.007999	188	0.006991	288	0.005017	388	0.006012	488	0.005000	588	0.004013	688	0.004009	788	0.009017	888	0.003007	988	0.004011
89	0.009006	189	0.006002	289	0.006012	389	0.005012	489	0.004005	589	0.004003	689	0.004001	789	0.010000	889	0.003003	989	0.004001
90	0.009003	190	0.009016	290	0.005998	390	0.006001	490	0.003011	590	0.004000	690	0.003006	790	0.010020	890	0.004016	990	0.003002
91	0.009002	191	0.006001	291	0.006013	391	0.006948	491	0.004006	591	0.004001	691	0.004002	791	0.010001	891	0.004011	991	0.005016
92	0.010002	192	0.006024	292	0.005012	392	0.009001	492	0.003981	592	0.003000	692	0.004009	792	0.010002	892	0.005990	992	0.003991
93	0.012000	193	0.005001	293	0.005014	393	0.012002	493	0.004009	593	0.004015	693	0.004008	793	0.009984	893	0.003986	993	0.004002
94	0.013017	194	0.011020	294	0.006017	394	0.006000	494	0.003010	594	0.002993	694	0.003007	794	0.010002	894	0.005009	994	0.002999
95	0.009000	195	0.006001	295	0.005008	395	0.008000	495	0.003016	595	0.003991	695	0.009004	795	0.009024	895	0.005010	995	0.005016
96	0.019021	196	0.005000	296	0.005020	396	0.007001	496	0.005003	596	0.004004	696	0.002994	796	0.010000	896	0.004005	996	0.004015
97	0.021008	197	0.006001	297	0.006019	397	0.006996	497	0.003001	597	0.004777	697	0.002989	797	0.010002	897	0.005010	997	0.004001
98	0.012019	198	0.006001	298	0.007000	398	0.004999	498	0.005001	598	0.002999	698	0.003000	798	0.011020	898	0.004002	998	0.002996
99	0.018003	199	0.005023	299	0.005009	399	0.005998	499	0.005007	599	0.003009	699	0.004898	799	0.010016	899	0.004011	999	0.006004

Table 4 *Distribution of VC Issuance Times*

Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency
0	0.004999	100	0.005015	200	0.008012	300	0.007991	400	0.009003	500	0.008001	600	0.008169	700	0.007016	800	0.009019	900	0.008985
1	0.009003	101	0.007017	201	0.008019	301	0.005022	401	0.007984	501	0.008023	601	0.008019	701	0.007872	801	0.008002	901	0.009021
2	0.008002	102	0.007177	202	0.007011	302	0.005982	402	0.008023	502	0.007902	602	0.007986	702	0.007019	802	0.008984	902	0.009001
3	0.007944	103	0.006983	203	0.004973	303	0.008017	403	0.007018	503	0.009005	603	0.008000	703	0.008983	803	0.008023	903	0.009003
4	0.007018	104	0.008003	204	0.007020	304	0.008020	404	0.008019	504	0.007999	604	0.008019	704	0.008002	804	0.008149	904	0.009017
5	0.008003	105	0.007011	205	0.005999	305	0.009001	405	0.008001	505	0.008024	605	0.008002	705	0.008017	805	0.008865	905	0.008002
6	0.009001	106	0.006991	206	0.005012	306	0.008987	406	0.008002	506	0.008025	606	0.006929	706	0.007988	806	0.007018	906	0.008019
7	0.008002	107	0.006020	207	0.009003	307	0.008017	407	0.008019	507	0.009002	607	0.008926	707	0.008018	807	0.008005	907	0.008985
8	0.009020	108	0.005010	208	0.005008	308	0.006983	408	0.008985	508	0.008002	608	0.010005	708	0.007857	808	0.007019	908	0.007023
9	0.008984	109	0.007075	209	0.006006	309	0.006001	409	0.008001	509	0.008001	609	0.009003	709	0.008002	809	0.008994	909	0.009019
10	0.009007	110	0.006946	210	0.005001	310	0.008024	410	0.009020	510	0.007023	610	0.008003	710	0.008002	810	0.007010	910	0.007985
11	0.008999	111	0.006001	211	0.007001	311	0.009001	411	0.007817	511	0.009986	611	0.007018	711	0.008013	811	0.006932	911	0.010020
12	0.009001	112	0.007985	212	0.006001	312	0.007972	412	0.008000	512	0.009021	612	0.007018	712	0.008002	812	0.008155	912	0.007988
13	0.008453	113	0.006064	213	0.007002	313	0.007160	413	0.008020	513	0.008000	613	0.007017	713	0.009170	813	0.008004	913	0.009015
14	0.008002	114	0.005948	214	0.007019	314	0.007844	414	0.009001	514	0.009006	614	0.007886	714	0.007993	814	0.007019	914	0.009002
15	0.009020	115	0.006001	215	0.008018	315	0.009133	415	0.007984	515	0.008019	615	0.008017	715	0.009019	815	0.008007	915	0.009001
16	0.008984	116	0.005241	216	0.006167	316	0.008025	416	0.008004	516	0.008985	616	0.006836	716	0.008001	816	0.007016	916	0.007985
17	0.009020	117	0.006778	217	0.007836	317	0.009984	417	0.007999	517	0.008090	617	0.008015	717	0.009002	817	0.008531	917	0.008013
18	0.008983	118	0.006990	218	0.005995	318	0.009002	418	0.008023	518	0.008931	618	0.007984	718	0.009007	818	0.007991	918	0.008985
19	0.009002	119	0.006027	219	0.008008	319	0.008002	419	0.009003	519	0.007017	619	0.008019	719	0.008002	819	0.008001	919	0.008018
20	0.009020	120	0.006017	220	0.005983	320	0.005004	420	0.009002	520	0.009985	620	0.008002	720	0.009020	820	0.007984	920	0.010003
21	0.007984	121	0.005982	221	0.008018	321	0.009005	421	0.008984	521	0.008008	621	0.008002	721	0.007984	821	0.008001	921	0.008001
22	0.009002	122	0.006012	222	0.006002	322	0.008018	422	0.010004	522	0.009018	622	0.007910	722	0.008001	822	0.008023	922	0.007996
23	0.009002	123	0.005938	223	0.006002	323	0.008024	423	0.009018	523	0.008002	623	0.008170	723	0.008011	823	0.007984	923	0.008018

24	0.009019	124	0.007014	224	0.008000	324	0.008001	424	0.008001	524	0.008003	624	0.007016	724	0.009004	824	0.007933	924	0.008984
25	0.008985	125	0.005992	225	0.005557	325	0.009020	425	0.008019	525	0.009018	625	0.008018	725	0.008000	825	0.008002	925	0.008019
26	0.009002	126	0.005998	226	0.008000	326	0.005023	426	0.008082	526	0.008985	626	0.008001	726	0.010003	826	0.008000	926	0.008009
27	0.009003	127	0.006998	227	0.008002	327	0.008002	427	0.008019	527	0.008018	627	0.008019	727	0.009004	827	0.008203	927	0.007981
28	0.009019	128	0.006025	228	0.004961	328	0.004930	428	0.008048	528	0.008140	628	0.007994	728	0.008015	828	0.008192	928	0.008003
29	0.009002	129	0.005982	229	0.008603	329	0.008985	429	0.009006	529	0.008147	629	0.008004	729	0.008998	829	0.008005	929	0.008018
30	0.008985	130	0.004018	230	0.005983	330	0.008002	430	0.008166	530	0.008872	630	0.008283	730	0.008189	830	0.007993	930	0.008004
31	0.009019	131	0.004018	231	0.006001	331	0.008024	431	0.009837	531	0.007739	631	0.008021	731	0.008019	831	0.009001	931	0.008017
32	0.009001	132	0.005019	232	0.004994	332	0.004941	432	0.008018	532	0.008002	632	0.007982	732	0.008089	832	0.008023	932	0.008019
33	0.010002	133	0.005001	233	0.005024	333	0.010003	433	0.009002	533	0.008013	633	0.008018	733	0.008019	833	0.009002	933	0.008011
34	0.009001	134	0.005002	234	0.007002	334	0.008001	434	0.008002	534	0.008995	634	0.008473	734	0.007983	834	0.008020	934	0.009003
35	0.009002	135	0.005016	235	0.007023	335	0.007004	435	0.008015	535	0.008004	635	0.008001	735	0.008019	835	0.009001	935	0.008000
36	0.009002	136	0.005192	236	0.005899	336	0.008000	436	0.008001	536	0.008002	636	0.007985	736	0.007987	836	0.009002	936	0.009019
37	0.009002	137	0.005802	237	0.004954	337	0.010020	437	0.009001	537	0.008987	637	0.007984	737	0.008018	837	0.007920	937	0.008051
38	0.009002	138	0.005009	238	0.008049	338	0.007986	438	0.009016	538	0.008000	638	0.007023	738	0.008000	838	0.009986	938	0.007998
39	0.010003	139	0.004019	239	0.004976	339	0.009017	439	0.008019	539	0.008017	639	0.007019	739	0.009001	839	0.008018	939	0.009003
40	0.009051	140	0.004904	240	0.005181	340	0.009002	440	0.010984	540	0.007984	640	0.006821	740	0.008002	840	0.008985	940	0.007983
41	0.009002	141	0.005150	241	0.005828	341	0.006002	441	0.009000	541	0.009020	641	0.008018	741	0.007999	841	0.007005	941	0.009020
42	0.009002	142	0.005874	242	0.005012	342	0.007023	442	0.008020	542	0.007018	642	0.008002	742	0.008002	842	0.009019	942	0.009001
43	0.010002	143	0.005986	243	0.007986	343	0.009001	443	0.007925	543	0.008023	643	0.009014	743	0.009018	843	0.008987	943	0.009003
44	0.011003	144	0.005023	244	0.005018	344	0.007002	444	0.008100	544	0.007012	644	0.008003	744	0.007990	844	0.009017	944	0.007984
45	0.010002	145	0.005001	245	0.007984	345	0.009001	445	0.008002	545	0.008989	645	0.008019	745	0.008998	845	0.008002	945	0.009002
46	0.008984	146	0.004968	246	0.009000	346	0.007002	446	0.008001	546	0.007985	646	0.008002	746	0.008018	846	0.009002	946	0.008001
47	0.010019	147	0.005019	247	0.007005	347	0.005018	447	0.007997	547	0.010001	647	0.008001	747	0.008984	847	0.012021	947	0.009024
48	0.010004	148	0.004982	248	0.006002	348	0.008985	448	0.008000	548	0.008002	648	0.008002	748	0.008018	848	0.008983	948	0.008001
49	0.007993	149	0.005019	249	0.005019	349	0.008022	449	0.009018	549	0.008018	649	0.007000	749	0.008002	849	0.008019	949	0.008984
50	0.009019	150	0.005983	250	0.006000	350	0.009068	450	0.008001	550	0.008985	650	0.008825	750	0.009002	850	0.007797	950	0.008002
51	0.008985	151	0.006001	251	0.007002	351	0.008924	451	0.008986	551	0.009002	651	0.008002	751	0.009002	851	0.007009	951	0.009002
52	0.011020	152	0.005021	252	0.007019	352	0.004999	452	0.009003	552	0.010021	652	0.008002	752	0.009016	852	0.007770	952	0.008019

53	0.008547	153	0.004024	253	0.007018	353	0.005023	453	0.009017	553	0.008017	653	0.008002	753	0.008002	853	0.008002	953	0.009017
54	0.007999	154	0.005018	254	0.006012	354	0.007987	454	0.008075	554	0.007896	654	0.009003	754	0.007012	854	0.007733	954	0.008001
55	0.008027	155	0.005006	255	0.004990	355	0.008016	455	0.008914	555	0.008000	655	0.008001	755	0.007985	855	0.007023	955	0.010003
56	0.008983	156	0.004483	256	0.005023	356	0.009004	456	0.007962	556	0.008023	656	0.009002	756	0.008008	856	0.007966	956	0.008001
57	0.008016	157	0.005007	257	0.005984	357	0.004999	457	0.008025	557	0.008002	657	0.007984	757	0.008017	857	0.008002	957	0.008013
58	0.009022	158	0.005023	258	0.005023	358	0.008004	458	0.008020	558	0.008002	658	0.008016	758	0.007957	858	0.008002	958	0.009985
59	0.009000	159	0.006008	259	0.007983	359	0.006016	459	0.008002	559	0.008019	659	0.009003	759	0.009019	859	0.008019	959	0.008001
60	0.009002	160	0.005009	260	0.005162	360	0.008001	460	0.008033	560	0.008147	660	0.009007	760	0.008071	860	0.008011	960	0.009000
61	0.008985	161	0.006002	261	0.008846	361	0.008019	461	0.008008	561	0.007019	661	0.008980	761	0.008016	861	0.008992	961	0.008019
62	0.010004	162	0.006001	262	0.005000	362	0.006001	462	0.008009	562	0.007844	662	0.008018	762	0.009002	862	0.008001	962	0.007828
63	0.011019	163	0.005157	263	0.008002	363	0.006018	463	0.009012	563	0.008017	663	0.009003	763	0.007984	863	0.009019	963	0.008002
64	0.010002	164	0.005956	264	0.008002	364	0.007924	464	0.008002	564	0.008002	664	0.008001	764	0.008020	864	0.008001	964	0.008002
65	0.009032	165	0.007018	265	0.008016	365	0.008999	465	0.008018	565	0.008019	665	0.008986	765	0.007845	865	0.008002	965	0.008002
66	0.009017	166	0.005000	266	0.007035	366	0.006006	466	0.008017	566	0.008002	666	0.011003	766	0.009005	866	0.009002	966	0.008002
67	0.008986	167	0.006016	267	0.007965	367	0.009019	467	0.008001	567	0.008106	667	0.009002	767	0.007999	867	0.009020	967	0.007626
68	0.009018	168	0.004982	268	0.007023	368	0.005983	468	0.008986	568	0.007897	668	0.009017	768	0.007978	868	0.007985	968	0.009005
69	0.008988	169	0.005023	269	0.005023	369	0.008018	469	0.008018	569	0.006943	669	0.009002	769	0.007812	869	0.008018	969	0.007999
70	0.008998	170	0.005017	270	0.008001	370	0.009003	470	0.007843	570	0.008018	670	0.007984	770	0.008017	870	0.008988	970	0.009002
71	0.008995	171	0.004024	271	0.004997	371	0.008000	471	0.008017	571	0.008019	671	0.008001	771	0.007940	871	0.008998	971	0.008002
72	0.009009	172	0.005993	272	0.005010	372	0.007984	472	0.008986	572	0.009002	672	0.008932	772	0.009002	872	0.009020	972	0.009002
73	0.010002	173	0.006012	273	0.003994	373	0.006001	473	0.008001	573	0.008002	673	0.009004	773	0.009002	873	0.007984	973	0.008006
74	0.008986	174	0.005008	274	0.004937	374	0.008020	474	0.009020	574	0.008018	674	0.009011	774	0.008018	874	0.009019	974	0.009003
75	0.010017	175	0.005982	275	0.009021	375	0.006983	475	0.008022	575	0.008018	675	0.006991	775	0.009002	875	0.007984	975	0.009985
76	0.009001	176	0.006001	276	0.007045	376	0.008010	476	0.008981	576	0.008018	676	0.007000	776	0.008042	876	0.009019	976	0.008018
77	0.008018	177	0.006002	277	0.006999	377	0.008984	477	0.008518	577	0.007954	677	0.009006	777	0.008961	877	0.007002	977	0.009002
78	0.009002	178	0.005018	278	0.005023	378	0.008003	478	0.008006	578	0.009001	678	0.007016	778	0.007024	878	0.007738	978	0.008132
79	0.008002	179	0.008001	279	0.005983	379	0.007000	479	0.007023	579	0.009003	679	0.008003	779	0.008734	879	0.008047	979	0.008010
80	0.008984	180	0.006002	280	0.008006	380	0.008003	480	0.007937	580	0.008001	680	0.007999	780	0.009003	880	0.007956	980	0.008002
81	0.008007	181	0.006994	281	0.006156	381	0.007001	481	0.008045	581	0.007985	681	0.008011	781	0.008001	881	0.007931	981	0.007979

82	0.008013	182	0.008009	282	0.006847	382	0.009103	482	0.008959	582	0.008001	682	0.008009	782	0.008000	882	0.008001	982	0.007023
83	0.008024	183	0.006984	283	0.006001	383	0.008969	483	0.008005	583	0.008026	683	0.006994	783	0.008001	883	0.008002	983	0.008019
84	0.008002	184	0.005996	284	0.008003	384	0.008140	484	0.009017	584	0.006999	684	0.008018	784	0.009002	884	0.008985	984	0.007766
85	0.009002	185	0.005006	285	0.005000	385	0.008074	485	0.007999	585	0.008001	685	0.006983	785	0.009002	885	0.007023	985	0.008007
86	0.008987	186	0.008002	286	0.005001	386	0.008943	486	0.008015	586	0.007988	686	0.004998	786	0.010003	886	0.007936	986	0.008003
87	0.008999	187	0.008001	287	0.005020	387	0.008002	487	0.008019	587	0.008015	687	0.006002	787	0.009013	887	0.008184	987	0.009001
88	0.009020	188	0.008121	288	0.006008	388	0.009002	488	0.008000	588	0.007822	688	0.009013	788	0.007984	888	0.009018	988	0.009000
89	0.010036	189	0.006864	289	0.005018	389	0.008002	489	0.009003	589	0.008019	689	0.008991	789	0.008021	889	0.008003	989	0.008019
90	0.009968	190	0.005023	290	0.009004	390	0.008016	490	0.009018	590	0.008002	690	0.008015	790	0.007019	890	0.008001	990	0.007021
91	0.008988	191	0.006994	291	0.007000	391	0.007987	491	0.008002	591	0.008002	691	0.008997	791	0.008042	891	0.007864	991	0.009000
92	0.007023	192	0.005004	292	0.009002	392	0.008017	492	0.007999	592	0.009002	692	0.007019	792	0.008018	892	0.009003	992	0.008002
93	0.005014	193	0.006024	293	0.007001	393	0.007985	493	0.009003	593	0.008002	693	0.008733	793	0.007013	893	0.008142	993	0.008019
94	0.006001	194	0.005060	294	0.008015	394	0.008018	494	0.008001	594	0.007985	694	0.008002	794	0.008509	894	0.008872	994	0.007999
95	0.008013	195	0.004944	295	0.005018	395	0.008008	495	0.009022	595	0.008024	695	0.007984	795	0.008001	895	0.008019	995	0.008009
96	0.006992	196	0.006011	296	0.008003	396	0.008018	496	0.007999	596	0.008024	696	0.007018	796	0.007023	896	0.007993	996	0.008005
97	0.006000	197	0.007011	297	0.007983	397	0.009002	497	0.008002	597	0.009002	697	0.008003	797	0.008812	897	0.007996	997	0.008001
98	0.007013	198	0.006005	298	0.008002	398	0.008990	498	0.008984	598	0.007984	698	0.007018	798	0.009003	898	0.009019	998	0.007985
99	0.006991	199	0.008015	299	0.005023	399	0.008018	499	0.008024	599	0.007023	699	0.008004	799	0.007999	899	0.008002	999	0.007996

Table 5 *Distribution of VC Verification times*

Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency	Index	Latency
0	0.006001	100	0.017021	200	0.005982	300	0.007025	400	0.006983	500	0.006020	600	0.007021	700	0.006001	800	0.007004	900	0.010000
1	0.006001	101	0.017983	201	0.006001	301	0.005998	401	0.006020	501	0.005013	601	0.007002	701	0.007001	801	0.010004	901	0.010002
2	0.012004	102	0.017004	202	0.010024	302	0.006001	402	0.006001	502	0.006994	602	0.006984	702	0.006001	802	0.008998	902	0.009002
3	0.004982	103	0.017022	203	0.010996	303	0.008021	403	0.007001	503	0.007010	603	0.006000	703	0.006001	803	0.006023	903	0.010006
4	0.012019	104	0.010018	204	0.011012	304	0.006002	404	0.006022	504	0.007994	604	0.006027	704	0.007002	804	0.006002	904	0.009024
5	0.011002	105	0.010988	205	0.010001	305	0.006018	405	0.005004	505	0.006009	605	0.005990	705	0.009985	805	0.006000	905	0.010024

6	0.010003	106	0.017026	206	0.006983	306	0.007001	406	0.006019	506	0.007987	606	0.007020	706	0.005024	806	0.007002	906	0.010029
7	0.009984	107	0.017000	207	0.007002	307	0.006994	407	0.006988	507	0.006019	607	0.006995	707	0.008004	807	0.006015	907	0.009984
8	0.007010	108	0.016025	208	0.007001	308	0.006009	408	0.006018	508	0.006001	608	0.005001	708	0.005020	808	0.006983	908	0.010024
9	0.010019	109	0.016021	209	0.009014	309	0.006001	409	0.005876	509	0.006994	609	0.007023	709	0.005003	809	0.007002	909	0.010024
10	0.009985	110	0.016003	210	0.007009	310	0.006019	410	0.007002	510	0.005990	610	0.006982	710	0.007002	810	0.007018	910	0.010002
11	0.006019	111	0.016986	211	0.005983	311	0.006019	411	0.004982	511	0.007015	611	0.007015	711	0.006024	811	0.005019	911	0.010020
12	0.006002	112	0.017022	212	0.007011	312	0.006016	412	0.006999	512	0.006009	612	0.009009	712	0.007994	812	0.006982	912	0.010018
13	0.009983	113	0.015986	213	0.005009	313	0.006990	413	0.006023	513	0.006001	613	0.006024	713	0.006009	813	0.007013	913	0.009984
14	0.009021	114	0.016020	214	0.006995	314	0.007009	414	0.006001	514	0.006000	614	0.006023	714	0.006001	814	0.006001	914	0.010025
15	0.010001	115	0.017004	215	0.006009	315	0.006016	415	0.006010	515	0.007022	615	0.005982	715	0.006017	815	0.008016	915	0.010002
16	0.007020	116	0.017988	216	0.007001	316	0.006001	416	0.005009	516	0.006006	616	0.006007	716	0.006001	816	0.006007	916	0.009006
17	0.006001	117	0.018020	217	0.005994	317	0.007045	417	0.006004	517	0.004911	617	0.007002	717	0.007994	817	0.006001	917	0.010024
18	0.011002	118	0.018004	218	0.008023	318	0.005996	418	0.006017	518	0.007001	618	0.005975	718	0.007010	818	0.006001	918	0.010002
19	0.010018	119	0.010002	219	0.004993	319	0.006994	419	0.005993	519	0.006016	619	0.006021	719	0.006994	819	0.006007	919	0.009974
20	0.006990	120	0.016003	220	0.005017	320	0.006009	420	0.008014	520	0.007994	620	0.005018	720	0.006009	820	0.008012	920	0.010002
21	0.006002	121	0.016021	221	0.005005	321	0.006988	421	0.006991	521	0.006001	621	0.007004	721	0.005993	821	0.010010	921	0.011010
22	0.010002	122	0.017002	222	0.004989	322	0.005981	422	0.007015	522	0.007993	622	0.007018	722	0.007000	822	0.007002	922	0.010003
23	0.006007	123	0.017022	223	0.007021	323	0.005014	423	0.006007	523	0.006004	623	0.005982	723	0.008016	823	0.007002	923	0.010002
24	0.006002	124	0.017021	224	0.011002	324	0.007991	424	0.006018	524	0.006003	624	0.008024	724	0.007009	824	0.006994	924	0.010024
25	0.011000	125	0.017008	225	0.006999	325	0.006019	425	0.006019	525	0.006021	625	0.004878	725	0.007004	825	0.005990	925	0.010019
26	0.009025	126	0.016986	226	0.005990	326	0.007002	426	0.005994	526	0.006011	626	0.009983	726	0.006015	826	0.007008	926	0.010002
27	0.007921	127	0.017025	227	0.005002	327	0.005993	427	0.007990	527	0.007002	627	0.009002	727	0.005003	827	0.006018	927	0.011003
28	0.009002	128	0.017004	228	0.007002	328	0.006020	428	0.006012	528	0.007001	628	0.005016	728	0.007021	828	0.009002	928	0.010007
29	0.010002	129	0.017004	229	0.005002	329	0.005005	429	0.006009	529	0.006010	629	0.006023	729	0.006002	829	0.009002	929	0.010024
30	0.009020	130	0.018004	230	0.005013	330	0.006020	430	0.007984	530	0.005999	630	0.008002	730	0.006023	830	0.009024	930	0.010984
31	0.005018	131	0.017004	231	0.006015	331	0.006982	431	0.006019	531	0.007021	631	0.006982	731	0.006015	831	0.010984	931	0.009024
32	0.009004	132	0.017004	232	0.006982	332	0.006023	432	0.005985	532	0.007002	632	0.007015	732	0.008009	832	0.009982	932	0.010002
33	0.006001	133	0.016021	233	0.006018	333	0.006982	433	0.005535	533	0.006982	633	0.005988	733	0.005022	833	0.010042	933	0.010001
34	0.009986	134	0.016021	234	0.006001	334	0.006004	434	0.006001	534	0.006023	634	0.006022	734	0.007010	834	0.005989	934	0.010006

35	0.007001	135	0.017007	235	0.009002	335	0.007015	435	0.007002	535	0.008020	635	0.007002	735	0.006008	835	0.007002	935	0.011021
36	0.008003	136	0.017024	236	0.013008	336	0.005990	436	0.005989	536	0.007002	636	0.005003	736	0.010995	836	0.010021	936	0.011003
37	0.010017	137	0.017986	237	0.006000	337	0.008017	437	0.006020	537	0.005985	637	0.007024	737	0.006023	837	0.009951	937	0.009017
38	0.009984	138	0.017025	238	0.006001	338	0.006008	438	0.006994	538	0.006014	638	0.006019	738	0.010002	838	0.007994	938	0.010019
39	0.010026	139	0.016986	239	0.005983	339	0.005993	439	0.006001	539	0.006004	639	0.006002	739	0.005982	839	0.005993	939	0.011019
40	0.006217	140	0.017015	240	0.005001	340	0.005022	440	0.007001	540	0.005993	640	0.007002	740	0.009013	840	0.010007	940	0.009024
41	0.009785	141	0.015003	241	0.007020	341	0.006018	441	0.006023	541	0.006001	641	0.008016	741	0.006009	841	0.010983	941	0.010020
42	0.009983	142	0.010003	242	0.008018	342	0.006000	442	0.007008	542	0.007006	642	0.005990	742	0.005994	842	0.010021	942	0.010005
43	0.011003	143	0.009024	243	0.006001	343	0.005981	443	0.006016	543	0.006019	643	0.006022	743	0.007010	843	0.006018	943	0.010000
44	0.007020	144	0.012018	244	0.006742	344	0.007002	444	0.006001	544	0.006001	644	0.007001	744	0.006001	844	0.005000	944	0.010014
45	0.012002	145	0.012002	245	0.007001	345	0.006020	445	0.006010	545	0.007012	645	0.006019	745	0.006024	845	0.009990	945	0.010080
46	0.009003	146	0.010984	246	0.007002	346	0.008984	446	0.005990	546	0.005009	646	0.007001	746	0.005003	846	0.005001	946	0.010018
47	0.010002	147	0.010021	247	0.007001	347	0.005023	447	0.008000	547	0.006987	647	0.007002	747	0.007004	847	0.009775	947	0.010001
48	0.012002	148	0.012984	248	0.013003	348	0.007002	448	0.006020	548	0.005997	648	0.005994	748	0.005008	848	0.010025	948	0.010000
49	0.011003	149	0.009014	249	0.004999	349	0.006994	449	0.006016	549	0.007004	649	0.005002	749	0.006982	849	0.011002	949	0.011003
50	0.010002	150	0.010001	250	0.007002	350	0.007009	450	0.006009	550	0.007013	650	0.005015	750	0.010021	850	0.011002	950	0.010984
51	0.010999	151	0.008994	251	0.007001	351	0.008983	451	0.006008	551	0.007010	651	0.007002	751	0.008006	851	0.007983	951	0.010021
52	0.010024	152	0.006009	252	0.007002	352	0.006014	452	0.005990	552	0.006986	652	0.008002	752	0.006020	852	0.007020	952	0.011003
53	0.009991	153	0.005003	253	0.008002	353	0.005990	453	0.006021	553	0.006016	653	0.007016	753	0.006001	853	0.006002	953	0.010001
54	0.010019	154	0.007021	254	0.013003	354	0.004997	454	0.005979	554	0.006001	654	0.005986	754	0.007983	854	0.011001	954	0.009020
55	0.010020	155	0.006001	255	0.005414	355	0.005019	455	0.006001	555	0.006983	655	0.006003	755	0.007023	855	0.007020	955	0.009985
56	0.011003	156	0.005983	256	0.006002	356	0.006974	456	0.005024	556	0.005023	656	0.005010	756	0.007002	856	0.012002	956	0.010007
57	0.010002	157	0.005024	257	0.005001	357	0.005003	457	0.006003	557	0.006996	657	0.006022	757	0.006001	857	0.010003	957	0.010019
58	0.011003	158	0.006001	258	0.006005	358	0.006021	458	0.006019	558	0.005005	658	0.006001	758	0.006001	858	0.009983	958	0.010022
59	0.010018	159	0.007001	259	0.009013	359	0.006001	459	0.007002	559	0.006004	659	0.006001	759	0.006001	859	0.010982	959	0.010488
60	0.011003	160	0.005001	260	0.011991	360	0.006982	460	0.007002	560	0.006995	660	0.007994	760	0.009984	860	0.010024	960	0.011022
61	0.010985	161	0.006984	261	0.006001	361	0.006008	461	0.006994	561	0.005014	661	0.006023	761	0.010002	861	0.006002	961	0.011024
62	0.011019	162	0.011003	262	0.006019	362	0.006001	462	0.007015	562	0.006001	662	0.006987	762	0.007018	862	0.006001	962	0.010989
63	0.010985	163	0.008001	263	0.005994	363	0.006001	463	0.006009	563	0.007010	663	0.004988	763	0.008974	863	0.006001	963	0.010014

64	0.011004	164	0.005001	264	0.006009	364	0.007002	464	0.004986	564	0.006985	664	0.007005	764	0.009995	864	0.009017	964	0.010023
65	0.010999	165	0.005005	265	0.006001	365	0.005975	465	0.006744	565	0.006012	665	0.007020	765	0.010020	865	0.006018	965	0.010019
66	0.011020	166	0.006009	266	0.012000	366	0.004970	466	0.005023	566	0.006009	666	0.006983	766	0.010020	866	0.009001	966	0.010984
67	0.010985	167	0.005996	267	0.007015	367	0.004872	467	0.006984	567	0.007011	667	0.006002	767	0.010995	867	0.011020	967	0.011021
68	0.010019	168	0.006603	268	0.005009	368	0.005980	468	0.006017	568	0.005009	668	0.005002	768	0.011010	868	0.009002	968	0.010003
69	0.009986	169	0.005006	269	0.005009	369	0.006001	469	0.006001	569	0.007994	669	0.007004	769	0.007002	869	0.009024	969	0.010025
70	0.011005	170	0.006009	270	0.007002	370	0.005983	470	0.006006	570	0.007010	670	0.004991	770	0.008002	870	0.010984	970	0.011003
71	0.010016	171	0.009000	271	0.006009	371	0.006023	471	0.005018	571	0.006984	671	0.005018	771	0.006983	871	0.006024	971	0.010023
72	0.010007	172	0.006018	272	0.014003	372	0.006019	472	0.005001	572	0.006011	672	0.006001	772	0.010021	872	0.011984	972	0.010004
73	0.010010	173	0.011002	273	0.006001	373	0.007000	473	0.006002	573	0.005990	673	0.010020	773	0.006983	873	0.012004	973	0.010002
74	0.009995	174	0.005982	274	0.006017	374	0.006019	474	0.006023	574	0.008003	674	0.006994	774	0.009022	874	0.011019	974	0.010012
75	0.010006	175	0.010001	275	0.007002	375	0.005011	475	0.006994	575	0.006020	675	0.007019	775	0.010988	875	0.006001	975	0.011002
76	0.010008	176	0.009010	276	0.007994	376	0.007991	476	0.005991	576	0.006004	676	0.005994	776	0.005007	876	0.006020	976	0.009998
77	0.010000	177	0.006982	277	0.006009	377	0.006016	477	0.008009	577	0.006001	677	0.005019	777	0.007984	877	0.006018	977	0.010023
78	0.010013	178	0.010035	278	0.014003	378	0.005905	478	0.006007	578	0.006007	678	0.006023	778	0.005990	878	0.006984	978	0.010987
79	0.011002	179	0.011971	279	0.005987	379	0.007020	479	0.005009	579	0.005009	679	0.006024	779	0.006002	879	0.010020	979	0.011001
80	0.009987	180	0.008013	280	0.006010	380	0.006001	480	0.006980	580	0.006001	680	0.007002	780	0.005001	880	0.007001	980	0.011019
81	0.010002	181	0.005980	281	0.005009	381	0.006001	481	0.005022	581	0.006982	681	0.006001	781	0.005002	881	0.008018	981	0.011002
82	0.009002	182	0.008014	282	0.005011	382	0.007002	482	0.005995	582	0.006001	682	0.006023	782	0.010030	882	0.008987	982	0.010002
83	0.009959	183	0.005010	283	0.006020	383	0.005015	483	0.007008	583	0.007015	683	0.006994	783	0.010004	883	0.010019	983	0.009983
84	0.011003	184	0.007992	284	0.009995	384	0.006003	484	0.006995	584	0.006022	684	0.005981	784	0.004989	884	0.009002	984	0.010005
85	0.010001	185	0.006020	285	0.006001	385	0.005003	485	0.004968	585	0.005987	685	0.005004	785	0.005002	885	0.005022	985	0.009005
86	0.010986	186	0.006002	286	0.006009	386	0.007021	486	0.006001	586	0.005019	686	0.010019	786	0.008878	886	0.006002	986	0.009718
87	0.010001	187	0.006981	287	0.005996	387	0.005990	487	0.006018	587	0.005994	687	0.007023	787	0.007002	887	0.009983	987	0.010020
88	0.010019	188	0.006021	288	0.006004	388	0.007022	488	0.005982	588	0.006001	688	0.006982	788	0.006982	888	0.010025	988	0.010002
89	0.009969	189	0.006984	289	0.006001	389	0.007009	489	0.006023	589	0.005010	689	0.005003	789	0.006022	889	0.005982	989	0.010984
90	0.010020	190	0.006017	290	0.007021	390	0.007002	490	0.008002	590	0.006005	690	0.007005	790	0.009002	890	0.006001	990	0.010025
91	0.011003	191	0.005001	291	0.005994	391	0.006015	491	0.007002	591	0.004999	691	0.007004	791	0.009989	891	0.011007	991	0.010003
92	0.010002	192	0.008002	292	0.007001	392	0.006001	492	0.006994	592	0.005018	692	0.006001	792	0.010001	892	0.011017	992	0.009774

93	0.008984	193	0.006982	293	0.006009	393	0.007004	493	0.007001	593	0.007000	693	0.005019	793	0.006994	893	0.005983	993	0.009023
94	0.010024	194	0.007021	294	0.005994	394	0.005023	494	0.006009	594	0.006021	694	0.005018	794	0.011021	894	0.006026	994	0.010002
95	0.010987	195	0.006002	295	0.006001	395	0.006984	495	0.008012	595	0.008020	695	0.007002	795	0.007017	895	0.005999	995	0.010002
96	0.010017	196	0.006993	296	0.007994	396	0.006019	496	0.006006	596	0.007002	696	0.006001	796	0.004970	896	0.006019	996	0.010002
97	0.011003	197	0.005990	297	0.007010	397	0.005003	497	0.008000	597	0.006004	697	0.006001	797	0.006000	897	0.009986	997	0.010003
98	0.009986	198	0.006021	298	0.006997	398	0.007004	498	0.006004	598	0.005022	698	0.007002	798	0.006023	898	0.010019	998	0.010003
99	0.018003	199	0.009002	299	0.005986	399	0.006022	499	0.005005	599	0.005002	699	0.006001	799	0.010001	899	0.007001	999	0.010019