STUDENTS CREDENTIALS SHARING BASED ON DECENTRALIZED APPLICATION

Project Phase-I Report

Submitted to APJ Abdul Kalam Technological University in partial

fulfillment of requirements for the award of degree

Bachelor of Technology

in

Computer Science and Engineering

by

ADITYA R NAIR	**-**	**STC20CS006**
ANN MARIA SUNNY	**-**	**STC20CS018**
NADAR NAWAS	**-**	**STC20CS040**
STEEVE BINU BABY	**-**	**STC20CS055**

Guided by

Mr. RAHUL GOPAL
Assistant professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

St. Thomas College of Engineering & Technology

Kozhuvalloor, Chengannur

DECEMBER 2023

STUDENTS CREDENTIALS SHARING BASED ON DECENTRALIZED APPLICATION

Project Phase-I Report

Submitted to the APJ Abdul Kalam Technological University in partial

fulfillment of requirements for the award of degree

Bachelor of Technology

in

Computer Science and Engineering

by

ADITYA R NAIR	**-**	**STC20CS006**
ANN MARIA SUNNY	**-**	**STC20CS018**
NADAR NAWAS	**-**	**STC20CS040**
STEEVE BINU BABY	**-**	**STC20CS055**

Guided by

Mr. RAHUL GOPAL
Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

St. Thomas College of Engineering & Technology

Kozhuvalloor, Chengannur

DECEMBER 2023

St. Thomas College of Engineering & Technology

Kozhuvalloor, Chengannur

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Project Phase-I work report titled **STUDENTS CREDENTIALS SHARING BASED ON DECENTRALIZED APPLICATION** submitted by **ADITYA R NAIR**(STC20CS006), **ANN MARIA SUNNY**(STC20CS018), **NADAR NAWAS** (STC20CS040), **STEEVE BINU BABY**(STC20CS055) to the APJ Abdul Kalam Technological University, Kerala in partial fulfillment of the B.Tech. Degree in Computer Science and Engineering is a bonafide record of the Project Phase-I work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Guide

Mr. RAHUL GOPAL
Assistant professor
Dept of CSE

Head of Department

Dr. SHYJITH M B
Dept of CSE

Supervisor

Mr. ROY T P
Assistant professor
Dept of CSE

INSTITUTION VISION

St. Thomas College of Engineering and Technology, Chengannur intends to be an institution of repute recognized for excellence in education, innovation and social contribution.

INSTITUTION MISSION

M1: **Infrastructural Relevance**

Develop, maintain and manage our campus for our stakeholders.

M2: **Life Long Learning**

Encourage our stakeholders to participate in lifelong learning through industry and academic interactions.

M3: **Social Connect**

Organize socially relevant outreach programs for the benefit of humanity.

DEPARTMENT VISION

To create industry ready and socially skill computer science engineers

DEPARTMENT MISSION

M1. Provide a learning platform that encourages thinking and analytical ability in the area of computer software and hardware.

M2. Inculcate lifelong and professional skill through the interaction of academicians and industrialist.

M3. Engage with society through social programs in and out of campus.

St. Thomas College of Engineering & Technology

Kozhuvalloor, Chengannur

PROGRAM EDUCATIONAL OBJECTIVES(PEOs)

The Graduates in Computer Science and Engineering will be able to:

PEO1: Professional Practices

Apply engineering practices required for software development, hardware development and embedded system.

PEO2: Intrapreneurial Skills

Exhibit innovation, self-confidence and teamwork skills in the organization and society.

PEO3: Lifelong Learning

Upgrade knowledge in data science and software engineering required for executing the software and hardware projects.

PROGRAM SPECIFIC OUTCOMES(PSOs)

PSO1: Professional Skills

Ability to understand the architecture and working of computer hardware and software.

PSO2: Design and Development Skills

Ability to design and develop software for technology application to fulfill industrial and social needs.

DECLARATION

We undersigned hereby declare that the Project Phase-I report **STUDENTS CREDENTIALS SHARING BASED ON DECENTRALIZED APPLICATION** submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul KalamTechnological University, Kerala, is a bonafide work done by us under the supervision of Mr. ROY T P, Assistant Professor and Dr. SHYJITH M B, Head of the Department, Department of Computer Science and Engineering, St Thomas College of Engineering and Technology. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis forth award of any degree, diploma or similar title of any other University.

27-11-2023

ADITYA R NAIR
ANN MARIA SUNNY
NADAR NAWAS
STEEVE BINU BABY

ACKNOWLEDGEMENT

We thank Almighty God for giving us the blessings to complete our Project Phase-I preliminary works successfully. We sincerely appreciate the inspiration, support and guidance of all those people who have been instrumental in making the Project Phase-I work a success.

We would like to sincerely thank **Er. JOSE THOMAS**, Secretary of St Thomas Educational Society for making the resources available at right time and providing valuable insights leading to the successful completion of Project Phase-I preliminary work.

We express our sincere thanks to **Dr. SHAJAN KURIAKOSE,** the Principal of our college for supporting us all the way long.

We express our special gratitude to **Dr. SHYJITH M B,** Head of the Department of Computer Science and Engineering for providing constant guidance and encouragement throughout the Project Phase-I preliminary work.

We express our sincere gratitude to the Project Phase-I Supervisor **Mr. ROY T P**
, Assistant Professor Department of Computer Science and Engineering for the inspiration and timely suggestions.

We also express sincere gratitude to our guide **Mr. RAHUL GOPAL,** Assistant Professor, Department of Computer Science and Engineering for his guidance and support. We have to appreciate the guidance given by the panel members during the Project Phase-I Preliminary presentations, thanks to their comments and advice. Last but not least we place a deep sense of gratitude to our family members and friends who have been a constant source of inspiration during the preparation of the Project Phase -I.

ADITYA R NAIR
ANN MARIA SUNNY
NADAR NAWAS
STEEVE BINU BABY

ABSTRACT

In the era of digital transformation, traditional methods of verifying and sharing academic credentials face numerous challenges, including fraud, inefficiency, and a lack of transparency. This abstract outlines the development of a decentralized application (DApp) utilizing blockchain technology to securely manage and share student credentials. This introduces a novel approach to credential sharing by leveraging the power of blockchain, specifically Ethereum, to create a tamper-proof, transparent, and user-centric system. In this decentralized ecosystem, students are given ownership of their academic records, ensuring privacy and control over their data. The paper aims to resolve security issues revolving around the sharing of students' credentials by leveraging the blockchain technology. It proposes a novel blockchain-based architecture followed by its implementation as a decentralized application (DApp). Further, the cost & the performance analysis are carried out based on the experiments conducted. Sharing of students' credentials is a necessary and integral process of an education ecosystem that comprises various stakeholders like students, schools, companies, professors and the governmental authorities. As of today, all these stakeholders have to put-in an enormous amount of efforts to ensure the authenticity and privacy of students' credentials. Despite these efforts, the process of sharing students' credentials is complex, error-prone and not completely secure. Our aim is to leverage blockchain technology to mitigate the existing security-related issues concerning the sharing of students' credentials. Thus, the paper proposes a tamper-proof, immutable, authentic, non-repudiable, privacy protected and easy to share blockchain-based architecture for secured sharing of students' credentials. To increase the scalability, the proposed system uses a secure off-chain storage mechanism. The performance and viability of the proposed architecture is analyzed by using an Ethereum based prototypical implementation.

TABLE OF CONTENTS

LIST OF DIAGRAMS

CHAPTER 1

INTRODUCTION

1.1 Introduction

Transcripts, diploma & degree certificates, internship & training certificates, migration & transfer certificates, character certificate, letter of recommendation, etc. are the set of essential credentials that stay with an individual for his/her lifetime. Issuing and sharing of these credentials is an integral process of our education ecosystem and plays a vital role during the recruitment drives of companies. To enhance security of the issued credentials, educational institutes make use of numerous methods like assigning unique identification number, putting uniquely distinguishable hologram, affixing student’s passport-sized photograph, printing the details of the students like date of birth, place of birth, parents’ name, registration/enrollment number, etc. Moreover, at the time of recruitment process, companies also need to verify the credentials that it receives directly from the applicants. Indeed, many times, companies contact the parent institution to endorse the credentials it has received from applicants. Such kind of process is tedious, costly and time-consuming. There is still a need to design a working prototype of student-credential sharing platform which can offer services for all the stakeholders in the education ecosystem. The paper modestly claims three-fold contribution: A novel yet pragmatic blockchain-based architecture is proposed for secure sharing of students’ credentials among various stakeholders. A prototype of the proposed architecture is developed as a Decentralized Application (DApp) using Ethereum. Performance analysis in terms of execution & transaction cost of the developed smart contracts and the execution time of important operations are carried out. The primary benefit of using block chain technology for sharing students' credentials is that certificates issued by educational institutions can be counterfeited, but this technology addresses the issue by storing certificate images in the form of hash codes that cannot be accessed by anyone .The Inter Planetary File System (IPFS) is typically used for storing data like certificate images in the form of cryptographic hashes .This does not allow users to share information with specific parties. The education ecosystem would benefit from a prototype student-credential sharing platform that would be useful to all parties involved. The data in block chain is stored in the form of blocks and for every new transaction a new block will be created that is linked to previous block. This study makes three quite modest statements about its significance: To facilitate the safe transfer of student credentials between different parties, we propose a unique but practical block chain-based architecture and create a Decentralized Application (DApp) on the Ethereum block chain to test its viability. The performance of the created smart contracts is evaluated by calculating the time it takes for critical activities to complete and the amount of money it costs to execute them.

1.1.1 Blockchain

Blockchain technology is a technology that uses decentralized ledgers to keep transaction records. The record of transactions is kept in a peer-to-peer network. There is no central authority needs to confirm the transactions. The transactions are verified by the participants in peer to peer networks. There is no need for any central authority for any kind of trade settlement, voting, or money transactions.

1.1.2 The Importance of Blockchain

The field of Blockchain in the IT sector is growing very fast. It is estimated that Blockchain technology has been adopted by more than one-third of the companies in the world and demand for blockchain developers are ever increasing. Blockchain technology provides one of the most secure and safe online transactions which has shaken all industries. Due to its numerous benefits to the industry, many companies and professionals have started to adopt blockchain technology.

- Security - is the primary concern for all kinds of online activities. Lots of data are stolen, and information is breached in this world of digital. Blockchain provides a very high level of security which makes it impossible to breach for anyone because of the decentralized nature of blockchain.
- Transparency - The blockchain technology is very transparent as everything is visible to all the participants from the beginning till date. One can see each and everything on the decentralized network which makes it very open technology. It reduces the chance for any kind of discrepancy in the system because nothing is hidden.
- Inexpensive - Blockchain technology is the most reasonable financial model available right now in the world. If one compares it with traditional economic models, then it is very less expensive. Lots of companies are now looking to use the blockchain technology because they can save lots of cost in their economic model, it is especially beneficial for banking industries.

- Time of Transaction is Less - The transactions that take place using blockchain technology take very little time to complete. It is a lot faster than the transaction time taken in traditional technology. Within a couple of minutes, one can receive or send financial documents and money. There is no burden to wait for hours in this blockchain technology.
- Increased Efficiency in Finance - There is no involvement of any third party in blockchain technology. Thus, it saves a lot of intermediaries cost, and all transactions happen directly from an individual to another individual. In the traditional banking system, the price is more to process financial transactions. Using blockchain technology, banks and companies can increase their economic efficiency.
- Fraud Protection for Businesses - Due to the high transparency of transactions in blockchain technology, any kind of fraud can be easily identified. So, any fraud that has happened in the open-source ledger of Blockchain cannot stay hidden, and businesses are always protected from fraud.
- Increased Use of Blockchain Token - Using Blockchain, a token can be used to represent any piece of information. This includes an identity for an IoT device, instructions for an algorithm, Origin Information about a product, patents, a vote in the election, an energy Kilowatt, a certificate credit, digital ownership certificate, share in a company, ownership of a house, and many more.
- Scope of Innovation - There is a massive scope in Blockchain technology because its features are open and programmable. It helps to rebuild systems in various fields which gives numerous possibilities for innovations also. It can also reduce the level of bureaucracy because the blockchain technology is transparent and efficient.
- No Middlemen in Transaction - In blockchain technology, there is no chance for any kind of mediators or intermediaries in any transactions such as for digital payments, for insurance claims, for asset management, for the stock exchange, for land registry and many more.
- Prevention of Data Leaks and Hacking - There have been numerous hacking and data leaks incident in the past that has shaken the trust of people to keep their data and personal information with companies. But with the use of blockchain technology, Data and information are very much secured, and there is no possibility of any kind of data leaking and hacking.
- Provenance - In the technology of Blockchain, one can quickly know the ownership of an asset since the beginning of the asset it first appeared. The occurrence of misselling of high-value intellectual & asset properties, fraud, theft, and many more will be reduced.

1.1.3 Types of Blockchain

Private and public blockchains are the two main styles of blockchains. There are, however, several variants, such as Consortium and Hybrid blockchains. Any Blockchain is made up of a group of nodes linked by a peer-to peer (P2P) network. Each network node has a copy of the mutual ledger, which is maintained regularly. Each node has the ability to validate transactions, send and receive messages, and building blocks.

1.1.3.1 Public Blockchain

A public blockchain is a non-restrictive, permissionless distributed ledger system. As an authorized node, anybody with an internet connection can access a blockchain platform and become a network user. A public Blockchain node or user can search current and historical records, verify transfers, proof-of-work incoming blocks, and mine. Cryptocurrency mining and trading are the most common uses of shared blockchains. As a result, the most commonly used decentralized blockchains are Bitcoin and Litecoin. Public blockchains are largely secure if users closely apply safety guidelines and procedures.

1.1.3.2 Private Blockchain

A permissioned or limited blockchain can only be used in a protected network known as a private blockchain. Private blockchains are usually used by an organization or business where only a small number of users can join a blockchain network. The level of conformity, authorizations, licenses, and accessibility are all determined by the governing organization. As a result, private blockchains are functionally similar to public blockchains, but their network is smaller and more limited. Private Blockchain is generally applied in voting, supply-chain, digital identity, wealth management, and other applications.

1.1.3.3 Consortium/ Federated Blockchain

A consortium blockchain is a semi-decentralized ledger that a group of companies or institutions manages. In comparison, a private blockchain, which a single person owns, looks like this. More than one person may act as a node in such a Blockchain for transacting data or mining. Government departments, financial institutions and other organizations also use consortium blockchains.

1.1.3.4 Hybrid Blockchain

A hybrid blockchain combines the benefits of both proprietary and public blockchains. It incorporates features from all forms of blockchains, allowing for both a private permission-based and a public permission-less scheme. Users will monitor who has access to which data held in the Blockchain with a hybrid network like this. A few of the Blockchain's data or documents will be made available, with the remainder remaining private in the private network. Users will conveniently access a private network or several public blockchains thanks to Blockchain's hybrid framework.

1.1.4 The Impact of Cyber Attack

New technologies come with new tools and methods for exploitation, and blockchain is no exception. A new class of cyber threats is emerging, involving tactics unique to blockchain networks. These include the following:

- **51% attacks** are when the majority of a network conspires against a minority of participants, as seen in several incidents involving platforms such as Ethereum Classic, Verge Currency and ZenCash (now Horizen). In a 51% attack, a malicious miner or group of miners gains control of more than 50% of a network's hash use or computing resources, giving them the ability to alter the blockchain. The controlling party could then prevent transactions, halt payments, reverse transactions and conduct double-spend, a type of fraud that occurs when coins are used in more than one transaction.
- **Flash loan attacks** are with smart contracts that are designed to support flash loans -- loans that let users borrow assets without collateral -- are attacked to siphon assets elsewhere. These attacks exploit uncollateralized loans by manipulating smart contract inputs, as seen in the $24 million attack on xToken and $80 million attack on Beanstalk Farm.
- **Rug pulls** are when insiders -- such as crypto developers, criminal groups or paid influencers -- create hype about a project only to abandon it and run off with investors' funds. Such pump-and-dump schemes resulted in $170 million in losses across just 48 attacks in 2022 and made up more than half of all fraud schemes on cryptocurrency platforms, according to Crystal Blockchain.
- **Phishing attacks** involve malicious actors using social engineering techniques to attain users'

credentials, install malware on user's devices, and obtain user's private keys and seed phrases --recovery phrases generated by crypto wallets during setup that enable users to access their wallets if they forget their password or lose their device.

- **Sybil attacks** are when bad actors create and use multiple false identities to flood, overtake or crash a system - usually to undermine authority. Some of the first instances of Sybil attacks were on peer-to-peer networks. In a blockchain context, Sybil attacks involve attackers using multiple fake nodes on the blockchain network, enabling them to prevent connections and transactions, take control of the network and conduct 51% attacks.
- **DDoS attacks** occur when attackers overwhelm their target network, causing the system to slow down or crash, thus denying services to legitimate users. A DDoS attack on a blockchain network has the same goal of taking down the system. In a blockchain DDoS attack, malicious actors could, for example, flood the network with spam transactions, causing operations to slow and preventing legitimate users from accessing it.

1.1.5 Possible Blockchain Use Cases for Cybersecurity

1. **IoT security**: With the increasing application of AI and IoT, the security of data and sytems for hackers has always been a major concern. Usage of Blockchain for improved security by using device-to-device encryption to secure communication, key management techniques, and authentication is a potential use case to maintain cybersecurity in the IoT system.
2. **The integrity of software downloads:** Blockchain can be utilized to verify updates and installers to prevent malicious software from infecting the devices. Here, hashes are recorded in the blockchain and new software identities can be compared to the hashes to verify the integrity of the downloads.
3. **Data transmission protection:** By using encryption, the data in transit will be protected from unauthorized access.
4. **Decentralized storage of critical data:** With the exponentially increasing data generated every day, blockchain-based storage solutions help achieve decentralized storage thus protecting digital information.
5. **Mitigating DDoS Attacks:** One of the most popular cyberattacks today is DDoS attacks where hackers aim to generate a flood of Internet traffic and thus disrupt the flow of services. The properties of immutability and cryptography help Blockchain prove to be an effective

solution for these attacks.

6. **DNS security:** The Domain Name System (DNS) is similar to a public directory that links domain names to their IP addresses. Over time, hackers have tried to access the DNS and exploit these links thus crashing sites. Due to Blockchain's properties of immutability and decentralized systems, the DNS can be stored with enhanced security.

1.1.6 Application Area for Blockchain

Since cryptocurrencies account for a significant portion of current blockchain networks, most scholars divide them into financial and non-financial categories. Others categorize them based on blockchain versions. We present some blockchain-based applications:

- **Financial applications:**
  Blockchain technology is currently being used in various financial areas, including business services, financial asset settlement, prediction markets, and economic transactions. Marketplace systems (PMS), which operate as oracles or intelligence sources, are another fascinating area that can influence companies and cryptocurrencies. Blockchain is set to play a critical role in the financial economy's long-term viability, benefiting investors, the existing banking system, and society as a whole.

- **Governance:**
  Governments have been tasked with managing and maintaining official accounts of residents and/or businesses for several years. Through disintermediating transactions and record-keeping, blockchain-enabled applications can transform the way local and state government's function. Blockchain's transparency, automation, and security for managing public information could potentially prevent corruption and improve government services. Blockchain may be used as a secure networking network for combining physical, social, and industrial infrastructures in a smart city framework. Blockchain governance aims to have the same resources as the state and its related public bodies in a decentralized and effective manner whilst retaining the same legitimacy.

- **Citizenship and user service:**

  The incorporation of emerging technology into daily life necessitates systems such as Blockchain to reliably identify and certify users' primary attributes such as identity, address, credit history, and other personal characteristics.

- **Voting**

  E-voting is being proposed as a promising and game-changing technology to ease out the election process, reduce the law and order complications and reduce time and financial expenditure. Still, due to security issues and cybersecurity threats, it has not gained momentum. Blockchain can provide a trusted and secure platform for e-voting that can remain consistent with domestic laws

- **Internet of Things (IoT):**

  The application of the Internet of Things (IoT) to population growth has resulted in its applications in each daily life domains and become critical for growth. Although there are many advantages of using IoT, various security threats outnumber these advantages. Due to limited hardware capabilities, the traditional cryptographic security mechanism cannot be applied in such an environment. Blockchain can provide a platform and mechanism for securing the IoT network, and it can provide an open IoT network for a secure, reliable and interoperable IoT network.

- **Healthcare management:**

  Blockchain technology may provide a critical solution for the healthcare providers that have implementations in healthcare management, demographic healthcare history, electronic insurance claims settlement and remote patient patient’s medical data sharing. It will provide user-oriented medical investigation, stop counterfeit products & medicines, and manage clinical trial data. In specific, Blockchain along with Smart Contracts, may solve issues such as clinical trial outcomes' scientific credibility and patient informed consent.

- **Privacy and security:**

  Significant amounts of confidential and classified knowledge are amassed through centralized institutions, both public and private. Despite the GDPR's goal of regulating the production of this data, there is still a significant gap to be filled. Compared with other reliable computing mechanisms that use data mining techniques, Blockchain is seen as a way to improve the reliability and scalability of big data. As a result, the literature contains privacy and security-oriented applications based on blockchain technologies.

- **Business and industrial applications:**

  Blockchain may become an important source of novelty in business and management through reinforcing, optimizing, and automating enterprise processes. The IoT and the Blockchain are spawning a slew of innovative e-business models. In a business model, SCs are used to carry out transactions between devices on a distributed network based on Blockchain.

- **Supply chain management:**

  Blockchain is expected to improve supply chain efficiency and accountability, allowing for more flexible value chains. Blockchain-based technologies, in particular, have the potential to revolutionize supply chains in three areas: visibility, optimization, and demand. Blockchain can be used in distribution, counterfeit commodity detection, document load collection, origin monitoring, and buyers and sellers to trade directly without intermediaries.

- **Energy sector:**

  Blockchain's potential applications in the energy market are many, and they would have a significant impact on both processes and networks. Blockchain can minimize costing and enable new business models, while marketplaces and grids could be best equipped to manage sophistication, data security, and ownership. It can also make the power grid operate more efficiently and effectively control demand response and provide a foundation for more proficient resource consumption monitoring and billing in energy sources.

- **Data management:**

  Blockchain is a very suitable technology for data management. Since all of their processes are verifiable, implementations and frameworks built on this technology have improved data protection and allowed by default auditability. This final section on blockchain-based applications cites related literature aimed at data storage that is reliable, safe, and verifiable.

1.1.7 Miscellaneous applications

Crowdfunding is a suitable use case of blockchain technology. In the humanitarian and philanthropic fields, blockchain implementations may be used to tackle hunger. Blockchain can also build intelligent, secure, distributed, and autonomous transportation networks and securely manage event tickets in smart city contexts. Edge computing and the creation of computational resource sharing networks, grid computing, cloud computing, and the usage of Blockchain as a device connector are several of the IT-related blockchain applications that are of particular concern.

1.1.8 Blockchain in Education

The Blockchain can help educational institutions strengthen their ability to assist teachers, deliver knowledge to guardians and community members, empower new learning systems, and expand and provide learning opportunities for more students. Figure depicts the general structure of Blockchain and users in the domain of education. There are several uses and advantages of using blockchain technology in the field of education:

1.1.8.1. Online Education

Online education, also known as distance learning or electronic learning, uses data and internet technology to deliver information and facilitate learning. It's referred to as a web-based learning technique. With blockchain invention, an ideal solution to online learning issues, such as legitimacy and protection, will be offered. The Blockchain will also create non-modifiable learning documents for online teaching without the need for third-party oversight, ensuring that course credits are adequately recognized.

1.1.8.2. Student records

Academic transcripts are one of the most time-consuming and labour-intensive processes in higher education. Each entry must be manually checked for authenticity before a validated record of a student's grades is available. Course content certification is another type of student record that is often sought. Each page should be signed and stamped for each student who requests this record (to ensure accuracy). If material courses and academic accomplishments were stored on a blockchain, an individual could get an accurate, authenticated record with just a few taps.

1.1.8.3. Diplomas and certificates

Diplomas and certificates for students could be provided and stored on a blockchain, much like grades. Employers will then need to be given a referral to a digital certificate instead of requiring the agency that issued the diploma to certify a paper copy. It is also in progress. Since most of the available instructive credential administrations are unable to guarantee the confidentiality and reliability of student data. Although using Blockchain to address confidence problems could be a viable solution, Blockchain has drawbacks that limit its complete adoption. Small throughput and access time are found in Blockchain. It stops users from using fake degrees or certificates to possible employers or institutions for higher education.

1.1.8.4. Badges

Aside from degrees, a standard resume provides a wealth of additional details that employers can find helpful. We're talking about qualities like foreign language proficiency, engineering competence, or unique talents that aren't inherently relevant to one's occupation. However, these abilities are difficult to prove. However, an individual may hire a third-party professional to validate their competence and issue a credential or badge. If these are stored on a blockchain, they can be used to show that an individual has the necessary skills. Open Badge Passport, for example, is the first step in this direction.

1.1.8.5. Student Examination and Evaluation

Students will then take the test remotely using personal computers or smartphones, with the Blockchain performing the evaluation. Teachers would have more time to devote to other scholarly or cultural pursuits if they didn't have to grade tests. Teachers can use smart contract and Blockchain with defining the correct answers and scoring criteria for evaluation. Student's will then appear for the examination on their PC or devices. Students' academic success and academic successes in education, preparation, tournaments, work, and other events outside of school can be measured using blockchain technologies to assess their capability, which benefits both students and businesses looking to hire them. A blockchain-based student technical skill assessment system that can test student ability measurement methods using a clustering algorithm. The framework can also allow for the development of a student skill assessment ecosystem.

1.1.8.6. Lessons and courses

Many blockchains also support smart contracts. It ensures that lessons and courses can be coded into the Blockchain and run spontaneously when those criteria are encountered. An instructor may assign students assignments. The smart contracts on the Blockchain could verify the execution of each mission automatically. Teachers could be paid in crypto tokens for finishing all assignments, and students can get credits. This method may be used to layout whole classes also.

1.1.8.7. Intellectual property protection and Publishing

Undergraduate and graduate students, instructors, scholars, and researchers actively produce high-quality content, but getting it published is difficult. Although growth in the amount and types of ways to publish academic work, questions about peer review accuracy, plagiarism, the lack of audience and patient participation, publication prejudice, predatory reporting, the expense of open access publishing, and the opacity of science research's "pedigree" remain. Academic transparency, reproducibility, and the prevention of evidence falsification and manipulation are all at the centre of debates aimed at preserving public interest in the scientific method. Blockchain can sort out these issues.

1.1.8.8. Admission Process

Most educational institutions operate based on a model in which they have authority over students' records and qualifications. As a result, there's a chance the data will be changed, lost, or destroyed. Data can be securely shared to interested parties using distributed ledger technologies running on a decentralized network. It will also help to prevent theft. It will inspire students to adopt mobile learning modes, as they will be able to effectively complete the admission requirements of various universities around the world.

1.1.9 Benefits of blockchain technology in education

Blockchain technology is an innovative new field of blockchain technology with a lot of potentials to transform the education industry. The advantages of blockchain technology in education range from data management to data authentication without jeopardizing legitimacy. The blockchain data is accessible and verifiable 24 hours a day, seven days a week, with complete accountability. Blockchain technology is commonly used to issue and authenticate educational credentials such as degrees, transcripts, and students' competencies, qualifications, and technical abilities, which employers can check all over the world. The credential process is streamlined thanks to blockchain technologies, and employers can expend less time verifying academic performance. It supports the education sector by offering a secure forum for sharing student data, increasing confidence, lowering costs, and increasing accountability. Blockchain technology holds a complete record of the course in data blocks that are ordered by timestamps in a chronological sequence. The cryptographic algorithm avoids computer tampering and frauds by preventing the deletion of old and new data blocks. It creates a virtual infrastructure for paper collection and keeps track of students' qualifications and accomplishments throughout their lives.

1.1.10 Issues of applying blockchain technology in education

It is undeniable that using blockchain technology in education could have drawbacks. Teachers must subjectively evaluate all cognitive patterns and learning outcomes, such as essays and educational presentations, as part of a complex structure. Without human interaction, a pre-programmed smart contract can't test these kinds of learning activities. If educational blockchain technology was introduced in schools, all students' academic data will be integrated into blockchain ledgers. It is undeniable that using blockchain technologies in education could have negative consequences. As part of a dynamic system, teachers must subjectively analyze both processing behaviours and learning outputs, such as essays and instructional presentations. A pre-programmed smart contract can't measure these types of learning experiences without human intervention. Students' educational data can be incorporated into blockchain ledgers if educational blockchain technology is implemented in classrooms. Blockchain technologies' immutability would have a double-edged effect. It reduces the possibility of modifying a student's school records for legitimate reasons for certain applicants. Furthermore, many technical barriers or roadblocks to using Blockchain in education have not been addressed. The standard Proof of

Work consensus method, for example, is a waste of time. It has a low number of transactions per second, which adds to the expense and prevents it from being used in classrooms.

1.2 Defining Smart contracts

Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.

1.3 How smart contracts work

Smart contracts work by following simple "if/when…then…" statements that are written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results. Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the "if/when...then…" rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes. Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

1.4 Benefits of smart contracts

- Speed, efficiency and accuracy - Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

- Trust and transparency - Because there’s no third party involved, and because encrypted records of transactions are shared across participants, there’s no need to question whether information has been altered for personal benefit.
- Security - Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.
- Savings - Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

1.5 Decentralized Application

Decentralized Application or DApp is like a digital app found on any smartphone or laptop, with the additional feature of employing blockchain technology to keep user’s data out of the hands of the organizations behind it. Just like cryptocurrency is decentralized money, DApp are decentralized apps. The blockchain stores copies of its expanding stack of data on a large number of participating computers, known as “nodes,” all at once. These computers are owned by users, not by the creators of the DApp. A full explanation of how blockchain technology works can be found here. DApp are as varied as conventional apps: They can provide social networks, games, entertainment, productivity tools and so on. Many are designed as tools to help consumers access decentralized financial services, or DeFi. This latter function is so widespread that the Ethereum network white paper categorized DApps into "financial," "semi-financial" and other. Ethereum has been the dominant host for DApp so far. At its foundation, one of the primary goals of the network was to make DApp easier to create. DApp users may feel more secure in the knowledge that the creators of the application cannot control how it is used - at least, not in the conventional way. For example, the creators of a social network DApp are powerless to remove a post or exclude a user. They are also unable to sell users’ data to other entities because DApp run autonomously once they’re launched. It’s all down to the use of smart contracts – computer programs deployed and on a blockchain designed to execute the rules of a contract without human involvement. For example, a smart contract could be coded to issue a loan once a user deposits a sufficient amount of collateral into it. DApp are also commonly open source, meaning that anyone can view and use the underlying code. They aim to use an intricate arrangement of smart contracts to achieve the functions of a traditional organization without the need for corporate executives and hierarchies.

CHAPTER 2

LITERATURE SURVEY

2.1 Overview of Literature Survey

This literature survey aims to provide an extensive overview of key research papers, books, articles and resources related to student's credentials sharing based on decentralized application.

1. **Implementation and Analysis of Block chain Based DApp for Secure Sharing of Students' Credentials by Raaj Anand Mishra, Anshuman Kalla, Nimer Amol Singh, Madhusanka Liyanage**

The paper aims to resolve security issues revolving around the sharing of students' credentials by leveraging the blockchain technology. It proposes a novel blockchain-based architecture followed by its implementation as a decentralized application (DApp). Further, the cost & the performance analysis are carried out based on the experiments conducted. Transcripts, diploma & degree certificates, internship & training certificates, migration & transfer certificates, character certificate, letter of recommendation, etc. are the set of essential credentials that stay with an individual for his/her lifetime. Issuing and sharing of these credentials is an integral process of our education ecosystem and plays a vital role during the recruitment drives of companies. To enhance security of the issued credentials, educational institutes make use of numerous methods like assigning unique identification number, putting uniquely distinguishable hologram, affixing student's passport-sized photograph, printing the details of the students like date of birth, place of birth, parents' name, registration/enrollment number, etc. Moreover, at the time of recruitment process, companies also need to verify the credentials that it receives directly from the applicants. Indeed, many times, companies contact the parent institution to endorse the credentials it has received from applicants. Such kind of process is tedious, costly and time-consuming. Some of the recent papers presented the benefits and the challenges of using blockchain technology in education. However, there is still a need to design a working prototype of student-credential sharing platform which can offer services for all the stakeholders in the education ecosystem. The paper modestly claims three-fold contribution: A novel yet pragmatic blockchain-based architecture is proposed for secure sharing of students' credentials among various stakeholders. A prototype of the proposed architecture is developed as a Decentralized Application (DApp) using Ethereum. Performance analysis in terms of execution & transaction cost of the developed smart contracts and the execution time of important operations are carried out.

2. EduCTX: A Blockchain-Based Higher Education Credit Platform by Muhamed Turkanović ,Marko Hölbl ,Kristjan Košič, Marjan Hericko ,Aida Kamisalic

By eliminating the need for a central authority to record or verify transactions or store user data, blockchain technology makes possible a truly decentralized system. Every single transaction that has ever taken place is recorded in an immutable public ledger. We offer EduCTX, a worldwide network for higher education credit based on blockchain technology. The ECTS (European Credit Transmission and Accumulation System) serves as the conceptual backbone of this platform. It represents a globally recognized, decentralized credit and grading system for higher education that may provide a unified perspective for students and HEIs, as well as other prospective stakeholders like enterprises, institutions, and organizations. We provide a working prototype of the environment based on the publically available Ark Blockchain Platform to demonstrate its viability. Credits earned by students for courses taken and passed will be represented by ECTX tokens, which will be processed, managed, and controlled by EduCTX through a globally decentralized peer-to-peer network. Peers on the blockchain network are HEIs. The platform represents an early stage in the development of a more open and technologically sophisticated approach to higher education. The EduCTX platform is the foundation of the EduCTX project, which seeks to eliminate linguistic and bureaucratic obstacles to higher education by encouraging HEIs to collaborate on the development of a universal, streamlined, and efficient learning environment. In light of this, we strongly suggest that HEIs join the EduCTX project and the EduCTX bitcoin network.

3. The Potential and Pitfalls of Blockchain Technology for Classroom Use

Blockchain, a widely used information technology, is changing many sectors, including the educational system, in significant ways. Blockchain technology has the potential to hasten China's push toward a more contemporary educational system, meet the country's evolving demands for disease control, and inspire a new approach to how higher education is administered and taught. Since blockchain software is decentralized, tamper-proof, easily identifiable, trackable, open, and transparent, it can facilitate the realization of student-centered educational environments and an open, transparent teaching process, both of which can increase the desire to learn of English majors and the efficiency of student management and training automobiles. This article's goal is to investigate the viability of implementing a leadership and education model for English majors that uses blockchain technology to improve upon the subpar accuracy of current approaches to classifying students' levels of English proficiency. We present a Discrete Hopfield Neural Networking (DHNN)-based model for skill assessment. Before classifying students into five distinct bands based on their English proficiency, a hierarchical analysis is performed to create an assessment index system. Students English-language skills are classified by the network using the memory associated with of the grouping criteria, and the findings are compared to those of the the BPNN model. The simulation results demonstrate that the BPNN model achieves an accuracy of 80.0% in classifying data, whereas the DHNN model achieves an accuracy of 100.0%. The accuracy of classification and generalization capacity of the DHNN model have increased, and the model construction method and results are straightforward, proving the model's efficacy.

4. **Privacy Protected Blockchain Based Architecture and Implementation for Sharing of Students’ Credentials by Raaj Anand Mishra, Anshuman Kalla, An Braeken, Madhusanka Liyanage**

Student’s credentials like transcripts, letter of recommendation and all kinds of certificates (like diploma, degree, internship, training, migration, and character certificates) are important documents that stay with an individual for the entire lifetime. Secure sharing of these students’ credentials is an integral part of both the education ecosystem and the recruitment process of companies. Every year several student’s add one (or more) credentials to their academic portfolio. All such credentials need to be carefully created, issued to students and relevant data must be preserved for future use by educational institutes, without exception. Many higher education institutions have their dedicated department for managing such a kind of academic information system that deals with student’s credentials. As of now, to make the credentials legitimate and tamper proof, institutes make use of numerous methods like assigning a unique number, putting a hologram, affixing a student’s photograph, inscribing all the possible details of the students like date of birth, place of birth, parent’s name, and registration/enrollment number, on the credentials itself. Over the years, the process has become quite complicated and time-consuming. A similar level of complexities arises for all the entities, who are dealing with student’s credentials, like companies, professors and other institutes. For instance, when a student applies for a job, the company carefully checks the authenticity of the received credentials. If required, the company may contact the host institution by phone-call or email to endorse the validity of the credentials. In spite of following such a tedious process, the overall system is insecure, and is facing difficulty to deal with tampered and fake credentials. To resolve the above challenges, the paper proposes the utilization of blockchain technology along with smart contracts. The main contributions of this paper are: Introduce a novel blockchain-based pragmatic architecture for secure sharing of student’s credentials among all the stakeholders in the education ecosystem. Propose a novel privacy mechanism to protect the privacy of the students’ credentials. Utilize an off-chain storing mechanism to improve the scalability of the blockchain system. Develop a Decentralized Application (DApp) using Ethereum blockchain as a proof-of-concept of the proposed architecture. Conduct numerous tests to check the viability, compute costs, measure execution times and gauge the scalability of the developed prototypical DApp. Analyze the robustness of the developed DApp against the most widespread security attacks.

5. **A Blockchain-based framework for secure Educational Credentials Shadab Alam, Huda Abdullah Yousef Ayoub, Rafan Abdulhaq Ahmed Alshaikh, Asmaa Hayawi Hussen AL-Hayawi**

Blockchain provides a creative approach to storing information, executing transactions, conducting tasks, and building trust. Some see Blockchain as a revolutionary technology for cryptography and cybersecurity, with applications ranging from cryptocurrency to healthcare, smart contracts, Internet of Things, smart grids governance, supply-chain etc. This research work would offer a detailed analysis of blockchain Security, Privacy and Trust. It further studies the applications of blockchain technology in the domain of education and involved challenges. Finally, it proposes a blockchain-based framework for secure and reliable student's record management. Blockchain as a revolutionary technology for cryptography and cybersecurity, with applications ranging from cryptocurrency to healthcare, smart contracts, Internet of Things, smart grids governance, supply-chain etc. This research work would offer a detailed analysis of blockchain Security, Privacy and Trust. This project aims to recognize various blockchain implementation fields that are already in use and potential blockchain applications in education. It focuses on three key themes: (1) blockchain-based educational technologies, (2) the opportunities that blockchain technology could bring to education, and (3) the complexities of implementing blockchain technology in education. Document authentication is a critical topic with a variety of challenging and time-consuming procedures to authenticate. Various reports are also available, including banking notes, government documents, transaction documents, and educational certificate. Educational credentials are the most important records granted by universities to students. Fake certificates are easy to make since the issuance mechanism is not straightforward and verifiable. A well-crafted false certificate is often challenging to spot and can be mistaken for the real thing. Hashing is a mathematical process that generates a value or values from a string of text. When a message is meant for a single recipient, hashing is one way to ensure confidentiality during the transmission process. The hash is produced using an algorithm, which helps to protect the transmission's protection from tampering. Hashing is also a tool for efficiently sorting key values in a database table. MD5 and SHA-1 are traditional cryptographic hash functions with a single goal: transforming the source input (message) into a fixed-length bit string (hash). And if they all have a somewhat different function, they are often referred to as (digital) signatures, checksums, or simply hash values. Inverting cryptographic hash functions, that is, recreating the input data solely from its hash value, is considered virtually impossible.

6. **DApp (Decentralized Application) Development and Evaluation for Safe Student Credential Sharing on the Blockchain by Farooq Sunar Mahammad, S. Sai Shreya, H. Beebe Hazeera, P. Sravani, R. Pavani, C. Ramya**

A person's vital credentials include their transcripts, diplomas, degrees, certificates of completion for internships and training, certificates of completion for migration and transfers, certificates of good character, letters of reference, etc. The issuing and dissemination of such credentials is a crucial part of our educational ecosystem and is widely valued by businesses in their hiring efforts. Educational institutions use a variety of measures, including the assignment of a unique identification number, the application of a distinguishable hologram, the attachment of a passport-sized photograph of the student, and the printing of personal information like the student's date of birth, where they were born, parents' names, registration/enrolment number, and so on, to confirm authenticity of the credentials that are issued. A company must also check the credentials it gets directly from candidates throughout the hiring process. The reverse is also true; sometimes, businesses will get in touch with the issuing school to confirm the authenticity of an applicant's credentials. To put it simply, it's a lengthy, expensive, and time-consuming procedure. The primary benefit of using block chain technology for sharing students' credentials is that certificates issued by educational institutions can be counterfeited, but this technology addresses the issue by storing certificate images in the form of hash codes that cannot be accessed by anyone. The Inter Planetary File System (IPFS) is typically used for storing data like certificate images in the form of cryptographic hashes. This does not allow users to share information with specific parties. The education ecosystem would benefit from a prototype student-credential sharing platform that would be useful to all parties involved. The data in block chain is stored in the form of blocks and for every new transaction a new block will be created that is linked to previous block. This study makes three quite modest statements about its significance: To facilitate the safe transfer of student credentials between different parties, we propose a unique but practical block chain-based architecture and create a Decentralized Application (DApp) on the Ethereum block chain to test its viability. The performance of the created smart contracts is evaluated by calculating the time it takes for critical activities to complete and the amount of money it costs to execute them.

7. **A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology Jayana Kaneriya and Hiren Patel**

Advancements in digital technologies have made the storage, sharing, and verification of educational credentials extremely important for entities such as students, universities, institutions, and companies. Digital credentials play an important role in students' lives as a lifelong learning passport. The educational field is experiencing numerous issues such as academic record forgery, record misuse, credential data tampering, time-consuming verification procedures, and issues related to ownership and control. Modern-day technology, Blockchain, is an appropriate alternative to resolve these issues and increase trust among entities. In this research, we intend to propose a Blockchain-based educational digital credential issuance, and verification model that addresses these issues in the education system using Ethereum Blockchain and smart contracts. The method we propose offers a way to demonstrate the correctness of specific credential attributes without revealing other attributes, thereby leading to ownership, minimal disclosure, and control. We offer an interface for storing massively encrypted academic records in a decentralized file system like Interplanetary File System (IPFS). Furthermore, Ethereum provides tamper-resistant chains to maintain the integrity of digital credentials. Finally, in comparison with the time it requires to issue credentials, our model safely accelerates the verification process by about 8%. Existing educational systems do not offer complete control and independence of credentials such as mark sheets, degree certificates, letters of recommendation, training certificates, and character certificate to the real identity owner, i.e., students. These credentials are building blocks for students' career and selection criteria for recruiters. So, smooth and secure sharing of such credentials with recruiters and other institutions is required to showcase the ability of a student. A similar level of complexity arises for a verifier to validate the integrity and authenticity of a credential submitted by a student. Cryptographic techniques used in Blockchain enhance the security and integrity of transactions recorded by a distributed ledger. Blockchain solves the problem of lack of trust by maintaining transaction records to each participating node. Transactions are recorded in a block which is added by a miner using a consensus algorithm. In addition, the Merkle tree generates a cryptographic fingerprint of the entire set of transactions for a block to ensure its integrity and inclusion. The chain is created by storing the cryptographic fingerprint of the previous block. Blockchain is immune to attacks because the entire ledger is chained, and altering one transaction requires, subsequent blocks to be altered, which is nearly impossible. Therefore, Blockchain can effectively solve existing problems such as the issuance, maintenance, integrity, privacy, and authenticity of credentials in the education domain.

8. Blockchain-based Verifiable Credential Sharing with Selective Disclosure Rahma Mukta, James Martens, Hye-young Paik, Qinghua Lu and Salil S. Kanhe

Sharing credentials could raise privacy concerns. For digital credentials to be widely accepted, there is a need for an end-to-end system that provides (i) secure verification of the participant identities and credentials to increase trust, and (ii) a data minimisation mechanism to reduce the risk of oversharing the credential data. This paper proposes CredChain, a blockchain-based Self-Sovereign Identity (SSI) platform architecture that allows secure creation, sharing and verification of credentials. Beyond the verification of identities and credentials, a flexible selective disclosure solution is proposed using redactable signatures. The credentials are managed through a decentralized application/wallet which allows users to store their data privately under their full control and re-use as necessary. Our evaluation results show that CredChain architecture is feasible, secure and exhibits the level of performance that is within the expected benchmarks of the well-known blockchain platform, Parity Ethereum. A selective disclosure scheme for credential sharing using redactable signatures. This design is flexible in that the user has full control of the credentials with regards to when, how long (i.e., time constrained access) to share them and with whom. The user can generate new redacted credentials without having to re-issue them every time they are shared. An SSI-focused decentralized architecture for credential management, which stores and shares credentials to/from a user wallet for better access and control on the data from the user's viewpoint. The architecture includes a service layer that encapsulates data minimization strategies, of which selective disclosure is one example.

9. Blockchain for Credibility in Educational Development: Key Technology, Application Potential, and Performance Evaluation by Yan Wang , Xin Cong , Lingling Zi , and Qiuyan Xiang

With ongoing educational reform, many researchers have focused on the issue of trust in the education field. Educational trust is a relationship of affirmative dependent on the educational system arising from the interaction between the trusting willingness of the educational subject and the trustworthy quality of the educational object. Anwar et al. pointed out that in the current educational environment, building trust in education is urgent. It is worth paying attention to the fact that the conventional educational paradigm can hardly adapt to the advancements in science and technology, as reflected in the following aspects. In the past, traditional educational trust relationships were usually based on geography and kinship, with emotional ties as the basic feature, and such relationships were vulnerable to artificial interference, not solid and strong enough, and not scientific enough, which has become a problem for credible educational development. The educational process is implicit and is not conducted under public scrutiny, there can be irregularities, and the results of such education can easily be questioned. In order to address such issues, the establishment of a credible mechanism for education seems extremely necessary. However, in this environment, it is very difficult to establish an open and transparent education credible system without reliable technical support. Considering the previous studies, decentralized technology such as blockchain is introduced to exclude human factors that affect the fairness of the education system and solve the trust crisis in education. Therefore, for educated people, they do not have the ability to assess information on their own and cannot actively choose educational environments and methods that interest them, thus lacking initiative. For teachers, they have no uniform criteria for assessing educated people as a whole, resulting in a reduction. Moreover, educational institutions are not transparent in the process of handling all educational data, and there is no supervisory body, leading to easy leakage of data privacy and reducing data authenticity. Therefore, it is essential to establish an educational credibility mechanism in order to ensure the fairness of the educational process and the effectiveness of the educational results. The main contributions of this paper can be summarized as follows: (1) We summarize the application architecture of blockchain in educational credibility, including core technology and attributes. We highlight the core technologies, such as digital signature, consensus mechanism, encryption algorithms, and smart contracts. (2) On this application architecture, we demonstrate the application potential of blockchain in four aspects and for each aspect, we analyze current credibility issues in education and how blockchain can help address them. (3) To evaluate the performance of the blockchain-based systems, we provide basic performance metrics and specialized metrics. The former evaluates the important performance of the blockchain system itself, while the latter gives the unique evaluation method for assessing credibility.

10. Smart Education Based on Blockchain Technology by Shubham Dubey Dr. Aditya Kumar Tiwary

This research study explores the potential benefits and challenges of integrating blockchain technology into the education sector. Specifically, it examines the concept of "smart education," which utilizes blockchain to create a secure, decentralized, and transparent learning environment. This study provides an overview of blockchain technology and its applications in education, including the use of smart contracts, digital credentials, and decentralized learning platforms. It also discusses the potential advantages of smart education, such as increased security and privacy, improved student tracking and data analysis, and costs. The ability to securely store, verify, and share educational credentials on a decentralized, transparent platform made possible by blockchain technology which has the potential to revolutionize the education sector. To fully realize the advantages of blockchain in education, there are several obstacles that must be overcome. The practical application of the technology is one of the main obstacles to its use in education. There are few set norms and protocols for using blockchain technology in education yet because it is still in its early phases. Getting educational institutions and businesses to use blockchain technology for the verification of educational credentials is another challenge. Due to a lack of knowledge or confidence in the technology, many educational institutions might be hesitant to adopt it. The education blockchain provides solutions for evaluation security based on consensus processes, data security based on distributed storage, and security based on smart contracts. As a result, several educational blockchains and the platforms that support them have become major sources of worry. A "digital asset market" endeavour entails the development of new markets that make it easier to create and trade new digital assets. The "Efficiency Play" initiative brings together businesses or sectors looking to use blockchain technology to make their current business operations more efficient. The "record keeping" effort is when businesses or institutions who guarantee that records cannot be tampered with and can be audited upon request come together. In this study, the applications of blockchain in the field of smart education were reviewed, where a transparent system has been introduced such as certificate verification, credit transfer which will improve data security and reduces the fear of data loss at some extent.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Expected System Requirement

The specific system requirements may vary depending on the blockchain platform used and the features implemented in the DApp. For example, if the DApp uses a resource-intensive blockchain platform, such as Ethereum, then the user may need a powerful computer with more RAM and CPU cores. Additionally, if the DApp implements features such as file storage or streaming, then the user may need ore disk space and bandwidth.

- Hardware: A computer with a modern processor and atleast 8GB of RAM. An internet connection with sufficient bandwidth to support blockchain transactions.
- Software: A blockchain wallet to store and manage the user's digital currency or tokens.A web browser or other application that can interact with the blockchain DApp.
- Additional requirements: The user must have a basic understanding of blockchain technology and how to use a blockchain wallet. The user must have an account with the blockchain DApp.
- Optional requirements: A mobile device with the blockchain DApp installed. A hardware wallet to store and manage the user's digital currency or tokens more securely.

Here are some of additional requirements that may be relevant for a blockchain-based student credential sharing system:

- The system should be able to handle a large number of concurrent users, as many students and recruiters may be using the system at the same time.
- The system should be highly scalable to accommodate future growth.
- The system should be secure and resistant to attack.
- The system should be easy to use for students, recruiters and educational institutions**.**

CHAPTER 4

METHODOLOGY

4.1 Methodology

All citizens are given official identification by the government. Individual accounts for all other parties involved are then set up using these identities. In order to grant and distribute credentials, schools maintain a list of students who are currently enrolled at that institution. Nonetheless, a new school may need to review the student's transcripts and other documents supplied by their former institution if the student applies to enroll there (s). College-goers are interested in seeing a copy of your transcript. In addition, applicants need a mechanism to make their credentials available to their preferred institution upon application or employer throughout the hiring process. Applicants' academic and professional records are something all hiring organizations must see. Instead, students would get certificates upon finishing an internship or training programmes. In order to fill jobs such as Ph.D., Postdoc, etc., professors, like businesses, must look at the applicant's qualifications. Instead, instructors may need to provide students with a certificate of completion for an internship or a letter of reference.

4.2 Requirements

Languages used

- Web3js
- Solidity
- React
- Node.js

Front End (Web Dapp)

- React

Back End

- Node.JS
- Web3.JS

Hosting Services

- Metamask

4.3 Implementation

For the first-level implementation, three different types of stakeholders are considered:

1. School
2. Student
3. Company

- School dashboard has two options:

(i) to add students to the list of enrolled students

(ii) to upload credentials for already enrolled students. When a credential is uploaded on IPFS, a hash value is returned. This hash value along with the metadata of the credential is pushed to the Ethereum such that only intended student can view it.

- Student dashboard offers three options:

(i) to view the uploaded credentials

(ii) to view the access requests sent by the companies

(iii) to grant access after viewing those access requests.

- Company dashboard has three options:

(i) to view the list of schools and the students enrolled under a selected school

(ii) to send an access request

(iii) to view the credentials once the students grants access.

4.4 Key Challenges regarding the systems

- Confidentiality: Student credentials are often stored in centralized repositories, which makes them vulnerable to unauthorized access. The proposed system stores credentials on the blockchain, which is a decentralized and immutable ledger. This makes credentials more difficult to tamper with or steal
- Authentication: Traditional student credential sharing systems often rely on intermediaries to verify the authenticity of credentials. This can be time-consuming and costly. The proposed system allows students to grant or revoke access to their credentials on a granular basis.
- Access control: Students should have complete control over who can access and share their credentials. The proposed system allows students to grant or revoke access to their credentials on a granular basis.

CHAPTER 5

EXISTING SYSTEM

5.1 Introduction

A blockchain-based solution for credential sharing can bring many benefits: the credentials or their fingerprints stored and shared on the blockchain are tamper-proof; a malicious user cannot alter any documents stored on-chain. The decentralized and immutable nature of blockchain provides participants with a trusted neutral credential sharing platform and undeniable evidence of all recorded transactions. There are a few solutions in recent literature that utilize these features. However, systematic management of digitally verifiable claims should also include:

(i) effective management of verifiable identity of the entities who issue, receive and verify the credentials as the fundamental building block of trust, and

(ii) privacy-aware solutions with flexibility for sharing claims with other entities. In this regard, the concept of Self-Sovereign Identity (SSI) is proposed under the premise of allowing users to exert full control over their identities and credentials and enforcing the data minimization principle. However, similar to the W3C's verifiable claims2, SSI by itself does not provide a detailed implementation architecture. Some recent efforts, such as Sovrin3 or uPort4, are guided by the SSI principles such as user-controlled identities, transparent data access and processing environment, but they support different subsets of the principles with varying degree of completeness. There is a need for a systematic architecture design that can serve as a template for developing blockchain-based SSI system.

This work contributes towards blockchain-based SSI architecture designs, in particular, with a focus on a flexible selective disclosure solution applicable to generic credential sharing scenarios, which is a necessary architectural component of data minimization. Architecture, named CredChain allows a user to request a credential from a registered issuer via a blockchain DApp and store the credential in his/her private wallet. Furthermore, when a credential is shared, the user can redact parts of the credential to minimize the private data being shared, while maintaining the validity of the credential. Also a time constraint can be set for each sharing instance to limit the verifier's access period. This paper claims the following contributions:

- A selective disclosure scheme for credential sharing using redactable signatures Our design is flexible in that the user has full control of the credentials with regards to when, how long (i.e., time constrained access) to share them and with whom. The user can generate new redacted credentials without having to re-issue them every time they are shared.
- An SSI-focused decentralized architecture for credential management, which stores and shares credentials to/from a user wallet for better access and control on the data from the user's viewpoint. The architecture includes a service layer that encapsulates data minimization strategies, of which selective disclosure is one example.

5.2 A Motivating Scenario and Preliminaries

This section introduces our motivating scenario and defines the key concepts in credential sharing systems.

Scenario. Jane is a student at University X who recently completed his undergraduate degree. She is applying for a postgraduate position at an overseas institute, University Y. Bob, the admission coordinator at University Y has received some fake transcripts from foreign applicants in recent months, so he wishes to verify Jane's identity and transcripts from University X. Jane is willing to share the credentials, but she is also cautious about her privacy and wishes to share only the essential information that would satisfy Bob.

From the scenario, we make a few observations about the required functionality of a verifiable credential system. First, the entities in the system must establish verifiable identities for the interactions to be considered trustworthy. Secondly, to avoid oversharing, users should be allowed to minimize the data to be exchanged (e.g., only disclose grades, but not birth date in the certificates). Finally, storing credentials in a private data store will allow users to readily re-use issued credentials and increase the level of privacy.

SSI Concepts. SSI can be realized in different architectures, but blockchains present innate characteristics that are conducive to supporting SSI principles such as transparency and decentralization of authority. Our design follows the architecture proposed in where the W3C Decentralized IDentifiers (DID) represent the identities of the users and blockchains act as a neutral third party to register/verify the DIDs. The architecture is drawn from a comprehensive SSI usage pattern analysis, and includes an extensible service layer into which new SSI concerns, such as data minimization, can be introduced. This paper focuses on the extended components of the architecture. However, to make the paper self-contained, briefly describe the basics of an SSI system according to the architecture. First, the identities of the users are established by DIDs which are generated and registered by the SSI system cryptographically. Each DID is associated with a DID Document (DDO) which contains a public verification key, the environment of interaction between two DIDs (e.g., communication protocol) and service endpoints (e.g., HTTPS URLs) used for interactions. The DIDs are stored on the blockchain. A user can prove the ownership of a DID using the associated public key from DDO. For instance, the issuer, e.g., University X, signs a credential with the private key associated with the issuer DID. The verifier, e.g., Bob, can query the ledger to obtain the corresponding DID and verify the issuer's signature in the credential.

SSI-based Credential Sharing: Based on the SSI concepts described above, introduced the key terms and user roles exist within a verifiable identity and credentials sharing system.

- **An Issuer**: This is an entity, e.g., University X, that is responsible for issuing a credential. In the most general sense, an issuer could be anyone registered with the system, but in our system, an issuer is a pre-registered entity with an SSI platform.
- **A Recipient**: This is an entity, e.g., Jane, who requests and receives a credential from an issuer (hence also known as the holder of a credential). A recipient can share credentials with verifiers. The identity of the recipient is registered with an SSI platform.
- **A Verifier**: This is an entity, e.g., Bob, who receives a credential from the recipient and verifies it with the system. This can be anyone with a credential to verify.
- **Credential:** A verifiable credential (or credential for short) is a tamper-evident set of statements made by an entity (i.e., issuer) about another entity (i.e., recipient), which can be cryptographically verified (i.e., by verifier). The pieces of personal information

on a credential, such as address or birth date are called “credential attributes” (or attributes for short). Verifiable credentials are used to generate claims.

- **Claim**: A claim is an assertion made about the recipient and generally constitutes a subset of attributes from a credential. In our scenario, if Jane is selecting a subset of the credential attributes to share with Bob, Jane is creating a claim from the issued credential.

Selective Disclosure Techniques: Selective disclosure allows a recipient to share a subset of credential attributes. Selective disclosure techniques can be categorized as atomic credentials, hashed values and selective disclosure signature. Atomic credential creates multiple credentials with each credential containing exactly one attribute about the recipient. Hashed values generates a general credential consisting of multiple attributes, but each attribute is hashed with a different nonce. For an attribute that the recipient wishes to disclose, she will share the attribute value and its associated nonce. The verifier, who already knows the hash value of the attribute will verify the attribute value using the nonce. In selective disclosure signature, a generic credential is issued, but certain signature schemes let the issuer sign on only those attributes which need to be revealed to a verifier. The verifier only sees the disclosed attribute while still being able to verify the credential as a whole. Amongst these, atomic credential is the simplest solution from the issuer’s viewpoint as the technique decomposes the credential into individual attributes (say n), and signs each attribute. This approach however, imposes an added cost on the issuer and the verifier (i.e., generating, managing and verifying n signatures), as well as higher communication overhead as the size of the payload per credential is increased (up to n times the length of a signature). The hashed values technique is not suitable for generic selective disclosure solutions as it requires prior knowledge of the matching hash of each attribute at the verifier’s end. Our proposed scheme takes the selective disclosure signature approach. Most other signature schemes used for selective disclosure either require the issuer to sign a new claim every time the recipient wishes to disclose a different subset of attributes on the same credential, or need a trusted third party in the workflow. Using redactable signature a credential is signed only once and multiple claims can be generated without the issuer’s re-signing or any third party interaction. In addition, the reduced number of interactions between the issuer and the recipient can prevent the issuer from correlating the recipient's credential sharing activities.

5.3 Selective Disclosure with Redaction

It uses a cryptographic primitive known as a redactable signature proposed by Johnson et al. However, Johnson's method allows the recipient to redact arbitrary bit positions in the document. This may create two potential problems for the context of sharing credentials. First, the generated signatures which depend on the number of redacted parts could be very large. This can be attributed to the bit level granularity of this scheme. Second, it may increase the possibility of inaccurate redaction. For example, an attribute such as GPA:3.29 could be partially disclosed to become 3. 9. For these reasons, we set our minimal level of redaction granularity to credential attributes. In the following, we describe the key elements of our design, highlighting the redactable signature generation, redaction and verification functions in the context of credentials.

5.4 Signature Generation

The tree structure of the signature is generated by the following steps: (phase 1 - Expansion), a pseudo random value is generated at each node from a random seed L using GGM, working down the tree, followed by (phase 2 - Hashing), Merkle-tree construction working up the tree using Merkle tree hashing. The leaf node values are hashed along with the random value from phase 1. The hash values of left(L) and right(R) child nodes are concatenated and hashed to generate the value of intermediate nodes. Hashing up the tree, the hashed root R is signed to produce σ = Sign0(R) at (phase 3-Signing). Finally, the extended signature Sign(C) on credential C is generated as (L, σ) along with the random seed of GGM tree. For easy interpretation, we have shown all phases in a single figure, though "expansion" and "hashing" require traversal of the entire tree separately before signing the root at phase 3. In the leaf nodes are considered as bits of strings as the scheme is intended for a document. However, in our implementation, each leaf node corresponds to a claim of a particular credential attribute.

5.5 Credential Redaction

In the first instance, the recipient can redact any subset of attributes from the credential. In the second instance, the issuer can limit the scope of redaction by setting certain attributes as 'not redactable'. This may be necessary in cases where the issuer needs to define mandatory disclosure components in their credentials.

5.6 Credential Sharing Services

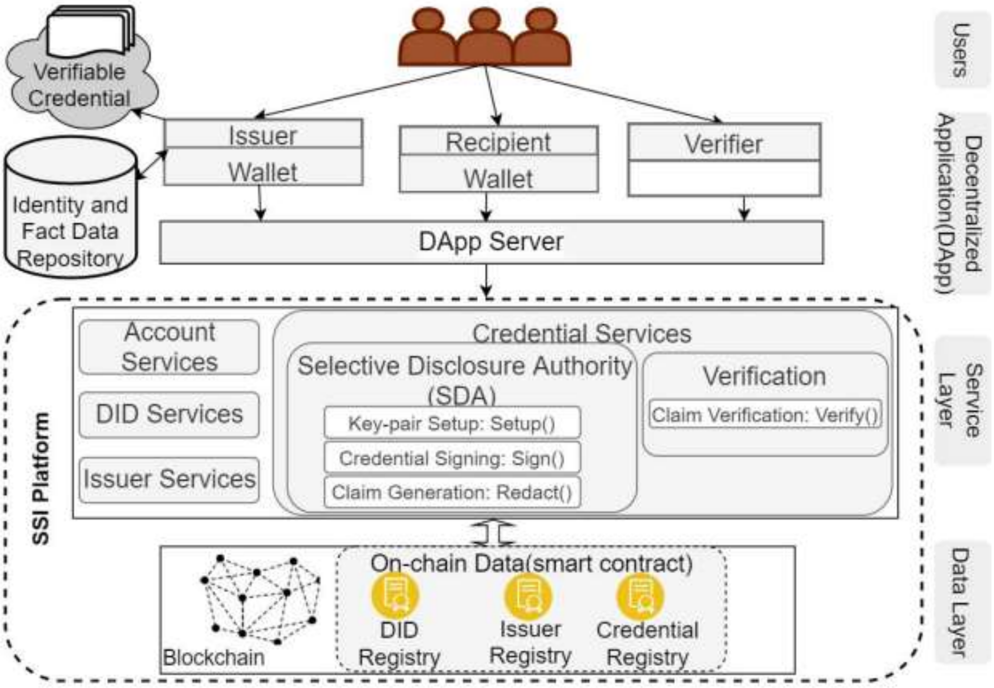

Fig 5.6: CredChain Architecture

The architecture, shown in Fig 5.6, is comprised of two parts: the SSI platform and a decentralized application layer which provides the means for users to interact with the blockchain network using a client wallet application. Each registered issuer hosts Identity and Fact Data Repository to store recipient's identity data and facts (e.g., Jane's course enrolment data at University X), and a cloud storage called Verifiable Credential to store and share generated credentials. The SSI platform includes two layers: data and service.

The data layer includes on-chain data (the registry smart contracts). The service layer includes Account Services (for blockchain account management), DID Services (for managing DIDs), Issuer Services (for managing issuer eligibility to sign credential) and Credential Services (for managing credentials). Note that the core of this architecture is the service layer which abstracts and exposes all necessary functionality to manage identities in a blockchain-based SSI platform. This paper focuses on privacy mechanisms for managing credentials in Credential Services**.** Fig 5.6 highlights the abstract components within Credential Services that are relevant to providing the selective disclosure services namely Selective Disclosure Authority (SDA) and Verification. SDA provides the redactable signature service on the credentials and includes the functions: Setup(), Sign() and Redact(). Verification includes the Verify() function for verifiers. It is noted that the service-based design of this layer allows different selective disclosure schemes to be incorporated for credential management by replacing or adding different Selective Disclosure Authority (SDA) and Verification components.

5.7 Workflows for Credential Management

This subsection details the main workflows of the service layer, focusing on SDA and Verification components.

Identifier Registration. Creating an account in the SSI platform generates a blockchain account, key pair, and registers a new DID for the user. The key pair is used primarily for signing the credentials. Upon successful registration, the DID Registry smart contract is initiated to store the DID and associated DDO. We assume that issuers are already registered in the system and their information is stored on another smart contract Issuer Registry after getting approval from the platform owner.

Credential Issuance. For credential issuance, first, the participants identify themselves to each other using identities with credentials registered on the blockchain, and communicate via the DApp server as shown in Fig. 5.7.1 The process begins by a recipient (1) sending an access request to the DApp server along with his DID, and information relevant for the issuer (e.g., Jane in our scenario may send the student ID of University X). The DApp server (2) collects the issuer identification details and (3) forwards the access request to that issuer. The issuer verifies recipient’s information against the course enrolment data from Identity and Fact Data Repository and obtains the recipient's service endpoint from provided DID, then (4) sends an acceptance notification to the recipient via the DApp server. After identities have been established, as illustrated in Fig.5.7.2, the recipient (1) sends a request for a credential to the DApp server. The server (2) verifies the identity against the DID Registry and (3) forwards the request to the issuer along with the recipient's DID. Upon receiving the credential request, the issuer fetches relevant data from its Identity and Fact Data Repository and create a credential C. The issuer then calls the function Sign() from SDA to sign the generated credential. Next, the issuer (4) creates a blockchain transaction to store the hash of signed credential in the Credential Registry as a record of the issuance. Following that, the issuer uploads the credential to their private cloud storage Verifiable Credential and generates a shareable link, then (5) sends it to the recipient via the DApp server which then (6) notifies the recipient. The recipient in turn may view the credential and (7) downloads it to their device. The link is encrypted with the recipient's public key to ensure the credential is only accessible to the correct recipient.

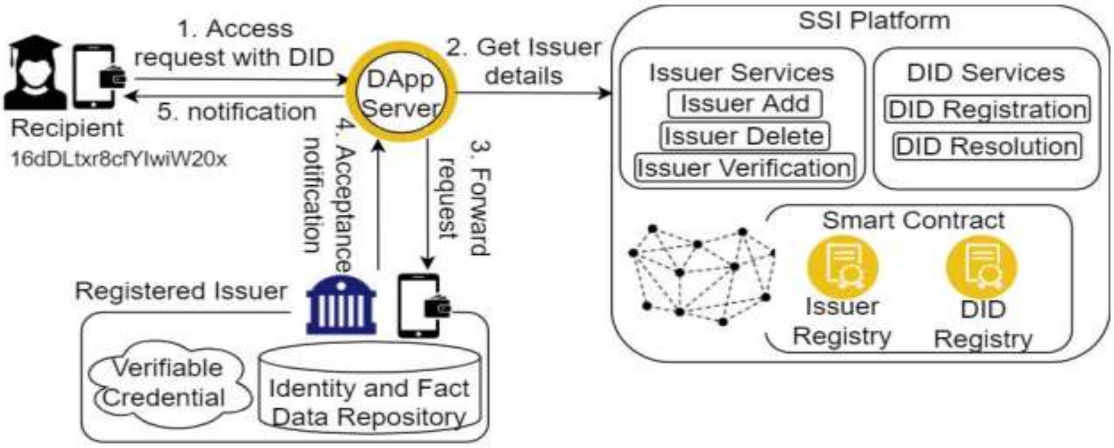

Figure 5.7.1 Identity Verification

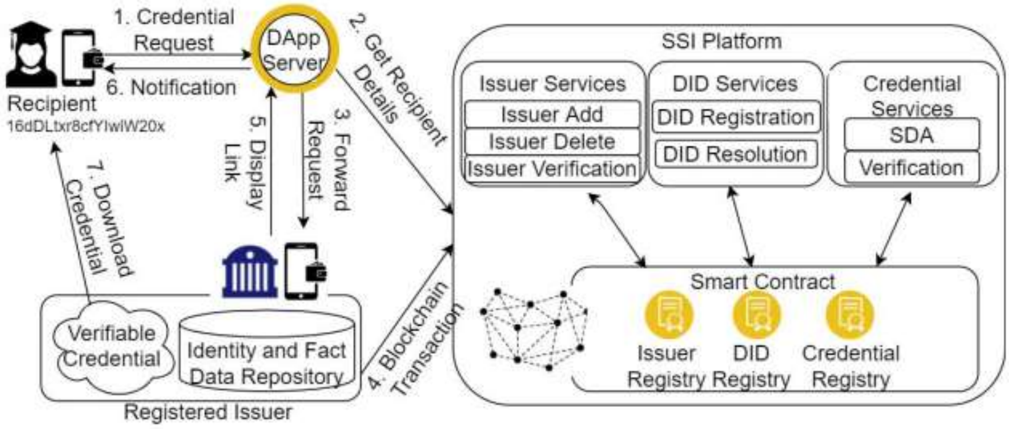

Figure 5.7.2 Issue Credential

5.8 Selective disclosure and verification.

The recipient may redact some of the attributes in the credential by calling the function Redact() from SDA. The redacted credential (claim) is stored on recipient's private cloud storage and a shareable link is generated for the verifier. Along side the claim, the platform generates a JSON Web Token (JWT) for the claim based on the recipient defined accessible time limit (e.g. for next seven days). This JWT allows recipient to specify verifier's access time on shared data. The link to claim with specified access period and its associated JWT are sent to the verifier. Finally, the verifier takes the JWT and the claim to invoke Verification module from credential services. The module first decodes the JWT and checks whether the access period is valid and then calls Verify() which verifies the authenticity and integrity of the claim.

5.9 Implementation

Implementation of the DApp server is based on nodeJS6 and uses JSON as payload. Assume that participants communicate with the DApp server through their personal devices. Hence, the only requirement to use the system is that the device can access the HTTP URL referenced in the users' DIDs. It is noted that the DApp server does not store any information locally but instead interacts with blockchain core to retrieve DID's for facilitating communications among the participants. To interact with blockchain network we use the Web3 Javascript API (Web3.js). All entries to the blockchain (such as DID registration) occur through smart contracts that are written in Solidity. Parity5 was chosen as the blockchain network for the on-chain data layer. The client application was developed using flutter7 on both Android and iOS devices. In the architecture, the issuer makes an issued credential available to the recipient through a private cloud storage hosted by the issuer. As an approximation, we used a Google Drive8 account held by the issuer. The issued credentials are uploaded by the issuer and shared through the share links generated by Google Drive. In the same manner, our implementation assumes the recipient shares the credentials with the verifier via a shared link generated from their personal cloud storage account.

5.10 Performance Results

Deployed the Parity blockchain node with the registry smart contracts and DApp server on a Linux Virtual Machine with 4 cores and 16GB RAM in Microsoft Azure. The inter-block time was set to 5 seconds as recommended by the Parity test network guidelines. The client requests were generated via JMeter on a local virtual machine with 4 cores and 8GB RAM. Performed tests on credential issuance and claim verification as they involve generating and verifying the signatures in the credentials, thus expected to contribute the most in terms of computing time and overall performance besides the regular network communications.

Performance of Credential Issuance: The workflow includes (i) building the tree structure to generate the signature for a credential and (ii) making the credential available for the recipient by uploading it to Google Drive and generating a share link. The second component of the workflow, link sharing time, is measured from the time the issuer uploads a credential to Google Drive, generates a share link, and returns the link. The average time taken, over 20 runs, is 2.03 seconds. Next, to understand the overhead of generating signatures, we measured the execution time of the tree generation algorithm. Increased the number of attributes from 4 to 128. Each data point shows the average time taken over 20 runs. The results show that the execution time increases proportional to the size of the attributes, but even with 128 attributes, the overhead generated is about 8ms which constitutes a fraction of the overall execution time of the credential issuance workflow. The x-axis represents the number of concurrent threads. At each data point, we send 10,000 requests in total (i.e., sending 10,000 request with 5 threads, 10 threads, so on). The y-axis represents the average throughput (transactions/second) over 20 runs. The results show the system consistently reaching the throughput range of 103-108 TPS.

Performance of Claim Verification: The verifier's workflow of claim verification includes (i) downloading a credential from the recipient's cloud storage (via a share link), (ii) re-constructing the tree to verify the signature, (iii) verifying issuer's identity by looking up the issuer registry in the blockchain. The execution time of the complete workflow is less than 1.5 seconds (averaged over 20 runs). Given that the tree re-construction time is the same as the credential issuance and the issuer registry lookup on the blockchain is a read-only operation and does not require any blockchain transaction, most of the execution time is contributed by the download time.

Performance of the Blockchain: Finally, measured the response time of the blockchain transactions. Performed the tests using the credential registry smart contract, invoking it to store a 4-attribute long credential. The average response time measured is 4.984 seconds. According to the official website of the Parity test network, the average response time is 4 seconds. Our observed response time was 0.984 second higher. There is a difference of 0.016 second between the block time and average response time. The additional delay is due to the time required for execution of smart contracts.

5.11 Privacy and Security Analysis Privacy.

Privacy: CredChain provides the recipients full control of their own identity and credentials. The recipients may have multiple DIDs, each representing a different identity (e.g., Jane could have one DID as a University X student and a separate DID for liaising with government agencies) This helps to minimize the risk of information being correlated on a single identifier. DIDs can also offer anonymity as they can be used as a pseudonym instead of exposing real identities. Adding to this, CredChain provides selective disclosure as a data minimizing tool.

Security: CredChain satisfies several security properties, including data confidentiality, data integrity and availability. Data confidentiality in the claims is achieved through the random values generated in the GGM tree during signature tree generation. This also helps with cases where the attribute size at the leaf node is considered small (i.e., easy to guess) and vulnerable to brute-force attacks, as the scheme adds random values to each leaf node prior to hashing for the Merkle-tree. Data integrity is accomplished by applying one way hash functions in Merkle hash construction, hence an attacker cannot modify the transmitted credential. The men in-the-middle attack is mitigated by ensuring that credential data is encrypted with the recipient's public key and signed with issuer's private key. External Attacker. A large number of fake claims sent by an attacker could deny service to honest verifiers. However, these fake claims are readily detected by the verifier and not processed.

i. Internal Attacker. The issuer and recipient form the internal participants. CredChain only allows legitimate internal participants' access. Issuers are verified by the SSI platform owner through Account services which takes an issuer DID and check its validity by querying the Issuer Registry. Recipients are authenticated by the respective issuer before issuing credentials.

CHAPTER 6

PROPOSED SYSETM

6.1 Proposed System

An architecture comprising of five major stakeholders, blockchain infrastructure and file (or cloud) storage is depicted in figure. Decentralized application along with the smart contracts govern the interactions between multiple stakeholders. Next discuss the roles of various stakeholders. Government body creates unique identities for all the stakeholders. Based on these identities, accounts are created for all the other stakeholders. Schools have a list of enrolled students for whom it has to issue and share the credentials. On the contrary, when a student seeks admission to a new school, this school may need to view the applicant's credentials already issued by the previous school(s). Students want to view their academic credentials. Further, students need a way to provide access to their credentials to the intended school at the time of admission or the company at the time of recruitment. Companies, during recruitment, demand access to the applicant's credentials. Alternatively, a company would issue certificates to students on completion of training or internship. Like companies, Professors need to view the applicant's credentials for recruitment of positions like Ph.D., PostDoc, etc. Alternatively, professors may have to furnish a letter of recommendation or internship certificate to their students. The core functionalities of the proposed architecture are:

(i) Registration of User: assigns a unique ID to every user. The way to create unique IDs is discretion of the government body,

(ii) Sign-up and Login of User: allows users to undergo one-time sign-up process which would ease future logins,

(iii) Enrollment of Student: happens at the time of admission,

(iv) Uploading of Credential: by school or company or professor,

(v) Retrieval and Viewing of Credential: enables students to retrieve their credentials,

(vi) Searching Student Information: facilitates stakeholders to search student's information (Students can decide which of their information will be visible to stakeholders),

(vii) Sending Access Request: allows schools, professors and companies to send access request to students to view their credentials and

(viii) Granting Access Right: empowers students to approve the received access requests.

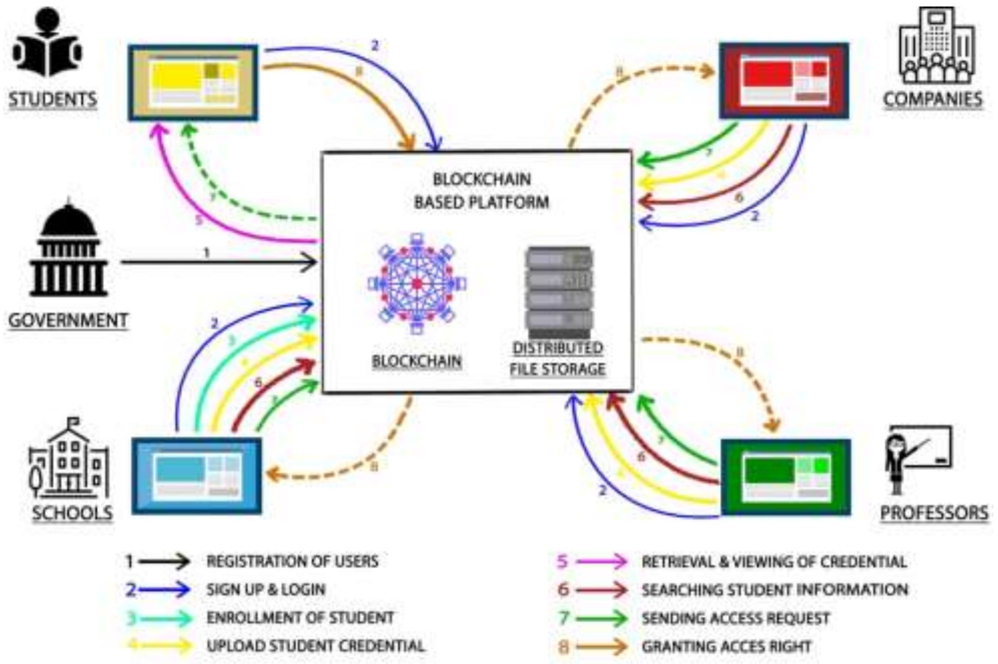

Fig. 6.1: Proposed Architecture for sharing students' credential

The proposed system work as follows:

1. Students upload their credentials to a decentralized storage system.
2. They then create a smart contract that specifies who is authorized to access their credentials.
3. They can then share their credentials with authorized parties by sending them a link to the smart contract.
4. When an authorized party accesses the smart contract, they can download the student's credentials.

The use of blockchain and smart contracts in the proposed system offers a number of advantages over traditional student credential sharing system:

- Security: The blockchain is a secure and tamper-proof ledger, which makes it ideal for storing sensitive data such as student credentials.
- Transparency: All transactions involving student credentials are recorded on the blockchain, which makes the system transparent and auditable.
- Efficiency: The use of smart contracts automates the credential sharing process, making it more efficient and less time-consuming.
- Reduced costs: By eliminating the need for intermediaries, the proposed system can help reduce the costs associated with student credential sharing.

6.2 Features of proposed system

- Decentralized storage: The proposed system stores student credentials on a decentralized storage system, such as IPFS. This means that the credentials are not stored on any single server, making them more difficult to hack or tamper with.
- Smart contract-based authentication: The proposed system uses smart contracts to authenticate the authenticity of student credentials. Smart contracts are self-executing contracts that are stored on the blockchain. This makes the authentication process more efficient and secure.
- Granular access control: The proposed system allows students to grant or revoke access to their credentials on a granular basis. This means that students can control who can view, download, or share their credentials.

A blockchain-based DApp for secure sharing of student’s credentials typically aims to leverage the advantages of blockchain technology, such as decentralization, transparency, and immutability, to enhance the verification and sharing of academic records and credentials.

1. Blockchain Infrastructure:
    - Public vs. Private Blockchain: Depending on the use case and requirements, the system may choose between a public blockchain (like Ethereum) for complete decentralization or a private blockchain for more control and privacy.

2. User Registration:
    - User Roles: Users can have different roles, such as students, educational institutions, employers, and verification agencies. Each role may have different privileges and responsibilities within the system.
3. Credential Issuance:
    - Digital Signatures: Educational institutions would digitally sign each credential they issue. This signature verifies the authenticity of the credential and the authority of the issuer.
4. Credential Storage:
    - Immutability: The blockchain's immutability ensures that once a credential is recorded, it cannot be tampered with. This feature is vital for preventing fraud or unauthorized alterations.
5. Smart Contracts:
    - Permission Logic: Smart contracts could define specific rules and permissions for accessing credentials. For example, a student can grant temporary access to their academic records to a potential employer.
6. Verification and Authentication:
    - Public Key Infrastructure (PKI): Users can use public keys to verify the authenticity of the credentials. The blockchain acts as a decentralized and trusted repository for these credentials.
7. Privacy and Security:
    - Data Encryption: To protect sensitive information, encryption techniques can be used to secure data on the blockchain.
    - Anonymity: Depending on the use case, the system might implement varying levels of anonymity to protect student's privacy.
8. Analysis and Performance:
    - Transaction Speed: Evaluate the transaction throughout of the blockchain to ensure it can handle the expected load, especially during peak verification periods (e.g. job application season).
    - Scalability: Assess how the system scales as the number of users and credentials grows.
    - Resource Utilization: Measure the storage and computational resources required for maintaining the blockchain.

9. User Experience:
    - Intuitive Interface: Design a user-friendly interface that simplifies credential sharing and management.
    - Accessibility: Ensure that the DApp is accessible to all users, including those with disabilities.
10. Compliance:
    - GDPR and Other Regulations: Ensure compliance with data protection regulations (e.g., GDPR in the European Union) and other relevant legal requirements in various jurisdictions.
11. Testing and Security Audits:
    - Penetration Testing: Conduct thorough security audits and penetration testing to identify vulnerabilities that could be exploited by malicious actors.
    - Bug Bounties: Encourage ethical hackers to find and report security issues by offering bug bounties.
12. Interoperability:
    - Consider how the system can interoperate with existing educational databases and systems to facilitate the transition to the blockchain-based solution.
13. Cost Analysis:
    - Evaluate the total cost of ownership (TCO) for implementing and maintaining the system, including blockchain network fees and infrastructure costs.
14. Scalability and Future Expansion:
    - Plan for the future by considering how the system can expand to support additional features and user groups.
15. User Education:
    - Provide education and training to all users to ensure they understand how to use the system effectively and securely.

CHAPTER 7

REFERENCES

- Anjali Singh, SPS Chauhan, Amit Kumar Goel, "Blockchain Based Verification of Educational and Professional Certificates", *2023 2nd International Conference on Computational Systems and Communication (ICCSC)*, pp.1-7, 2023.
- Shubham Dubey, Aditya Kumar Tiwary, "Smart Education based on Blockchain Technology", *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, pp.1485-1490, 2023.
- Aamna Tariq, Hina Binte Haq, Syed Taha Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System", *IEEE Transactions on Computational Social Systems*, vol.10, no.4, pp.1503-1514, 2023.
- Archana Bathula, Suneet kr. Gupta, Suresh Merugu, Sanagala S. Skandha, "Academic Projects on Certification Management Using Blockchain- A Review", *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)*, pp.1-6, 2022.15151515
- Swatesh Kumar Ambast, T A Sumesh, "A Blockchain Based Credential Verification System using IPFS", *2022 IEEE 19th India Council International Conference (INDICON)*, pp.1-5, 2022.
- Mercy Effiong, Alex Norta, Chibuzor Udokwu, Marie Hattingh, "Adoption of Blockchain Technology in Academic Certificate-Verification Systems", *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*, pp.1-6, 2022.
- Raihan Sulaiman, Andry Alamsyah, Puspita Wulansari, "Reshaping the Future of Recruitment through Talent Reputation and Verifiable Credentials using Blockchain Technology", *2022 10th International Conference on Information and Communication Technology (ICoICT)*, pp.316-321, 2022
- R. A. Mishra, A. Kalla, N. A. Singh and M. Liyanage, "Implementation and Analysis of Blockchain Based DApp for Secure Sharing of Students' Credentials," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV,

USA, 2020, pp. 1-2, doi: 10.1109/CCNC46108.2020.9045196

- B. Rodrigues, M. Franco, E. Scheid, S. Kanhere, and B. Stiller. A technology-driven overview on blockchain-based academic certificate handling. In Blockchain Technology Applications in Education, pages 197–223. IGI Global, 2020.
- R. Mishra, A. Kalla, N. Singh, and M. Liyanage. Implementation and analysis of blockchain based dapp for secure sharing of students' credentials. In IEEE CCNC, pages 1–2, 2020.
- M. Nguyen, T. Dao, and B. Do. Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science, 6(e266), 2020.
- K. Singh, O. Dib, C. Huyart, and K. Toumi. A novel credential protocol for protecting personal attributes in blockchain. Computers Electrical Engineering, 83:106586, 2020.
- M. Schanzenbach, G. Bramm, and J. Schütte. reclaimid: Secure, self-sovereign identities using name systems and attribute-based encryption. In 17th IEEE TrustCom/BigDataSE, pages 946–957, 2018.
- B. Hampiholi and G. Alpár. Privacy-preserving webshopping with attributes. In IEEE Symposium on Privacy-Aware Computing (PAC), pages 25–36, 2017.