DIUCERTS DAPP: A BLOCKCHAIN-BASED SOLUTION FOR VERIFICATION OF EDUCATIONAL CERTIFICATES

BY

MD. SHAHRIAR KARIM SHAWON
ID: 171-15-1269

HOSNAIN AHAMMAD
ID: 171-15-1233

MST. SHUMROSE SULTANA SHETU
ID: 171-15-1339

MST. RAZMIN SULTANA
ID: 171-15-1241

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Amit Chakraborty Chhoton
Lecturer
Department of CSE
Daffodil International University

Co-Supervised By

Md. Sabab Zulfiker
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

JANUARY 2021

APPROVAL

This Project titled "**DIUcerts DApp: A Blockchain-Based Solution for Verification of Educational Certificates**", submitted by *Md. Shahriar Karim Shawon*, *Hosnain Ahammad*, *Mst. Shumrose Sultana Shetu*, and *Mst. Razmin Sultana* to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on *14-01-2021*.

BOARD OF EXAMINERS

Professor Dr. Touhid Bhuiyan **Chairman**
Professor and Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. S. M. Aminul Haque **Internal Examiner**
Assistant Professor & Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Amit Chakraborty Chhoton **Internal Examiner**
Lecturer
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. Mohammad Shorif Uddin **External Examiner**
Professor
Department of CSE
Jahangirnagar University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Amit Chakraborty Chhoton, Lecturer, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

____

Amit Chakraborty Chhoton
Lecturer
Department of CSE
Daffodil International University

Co-Supervised by:

____

Md. Sabab Zulfiker
Lecturer
Department of CSE
Daffodil International University

Submitted by:

____

Md. Shahriar Karim Shawon
ID: 171-15-1269
Department of CSE
Daffodil International University

____

Hosnain Ahammad
ID: 171-15-1233
Department of CSE
Daffodil International University

____

Mst. Shumrose Sultana Shetu
ID: 171-15-1339
Department of CSE
Daffodil International University

____

Mst. Razmin Sultana
ID: 171-15-1241
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project successfully.

We really grateful and wish our profound our indebtedness to **Amit Chakraborty Chhoton**, **Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Blockchain*" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Prof. Dr. Syed Akhter Hossain, and Head**,** Department of CSE, for his kind help to finish our project and also to other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

Educational certificate verification is the process of checking and verifying the certificate legitimacy of graduate students. It is a costly, lengthy, and time-consuming procedure as university authorities each year investing millions of dollars on maintaining the entire process. The employer also takes plenty of time for verifying the authenticity of the applicant’s certificate. The current certification system involves providing physical certificates to the candidates. For this reason, they aren’t tamper-resistant and can be lost anytime. Also due to counterfeiting the certificates by scammers and issued by a lot of illegal institutions is make the process hazardous. People frequently lie about their degrees and qualifications by counterfeiting certificates. A fake certificate generated by skillful scammers is always tough to identify and can be addressed as the original one. Therefore, there is a crucial need to upgrade the certification and verification process. In this article, we have introduced the DIUcerts - a blockchain-based decentralized platform to overcome the mentioned problem is stated. This platform offers an easy way to issue, check, and verify educational certificates. Additionally, in DIUcerts, data doesn’t have to be stored in one place as each certificate’s information is kept in an individual file and entire issuance and verifications are done through the Ethereum platform. With this infrastructure, the cost of maintaining a blockchain-based certificate verification system could be highly minimized as compared to building a similar application on a centralized database. As a result, DIUcerts can lead to better security, cost savings, and a time-saving platform.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
Introduction

1.1 Introduction:

Today’s generation has a boundless demand for increased productivity and efficiency. This pronouncement can be elaborated to around most of the sectors like healthcare, accounting, jurisdiction, land registry, etc. The traditional education systems are no anomaly for the necessity of including the most advanced technology to enhance their entire consistency. Blockchain technology provides the ground of a decentralized system environment where all data is immutable and once its verified, data cannot be altered. It also removes the involvement of third-party to a system. This decentralized technology is assumed to remodel the infrastructure of industry, merchandising, education, and contribute to the expeditious development and prosperity internationally. Distributed in nature, Blockchain uses consensus algorithms and cryptography techniques to records all the transactions and their details in multiple locations simultaneously. It also records the changes in the transaction and data transaction flow and provides a transparent, immutable record of all data. However, this decentralization, immutability, Traceability features of Blockchain ensure that the data is truthful, accurate, secured, and safe [1].

In the IT Industry, a common question is inconstantly mentioned: how to maintain trust and security with the traditional data management system? From this point of view, keeping the immutability of the data is one of the key features that help deal with faith or authenticity problems nowadays. For normal centralized applications, data immutability should be secured using centralized databases that support CRUD operations such as create, read, update, and delete. Meanwhile, decentralized applications(DApp) of Blockchain only support create and read operations. These DApps usually minimized the number of participants and eliminated the need for a trustworthy third party. That’s why, conducting with data integrity issue has an excellent impact to be utilized to the Blockchain-based decentralized applications, which generally make the evolution of the Internet. [2]. Blockchain is a conventional approach that is being intensively functioned for tackling a lot of complex problems in different fields. Currently, in the educational sector, the certification system involves providing physical certificates to the student after completion of a course. That means, the copies need to be dealt with in person, they aren't tamper-resistant and can be lost anytime. Here Blockchain brings to us a massive opportunity with a trustable interaction between student, university, and employer in the educational certificate verification process. The following figure 1.1 shows how Blockchain can be used in the educational certificate issues and verification process.

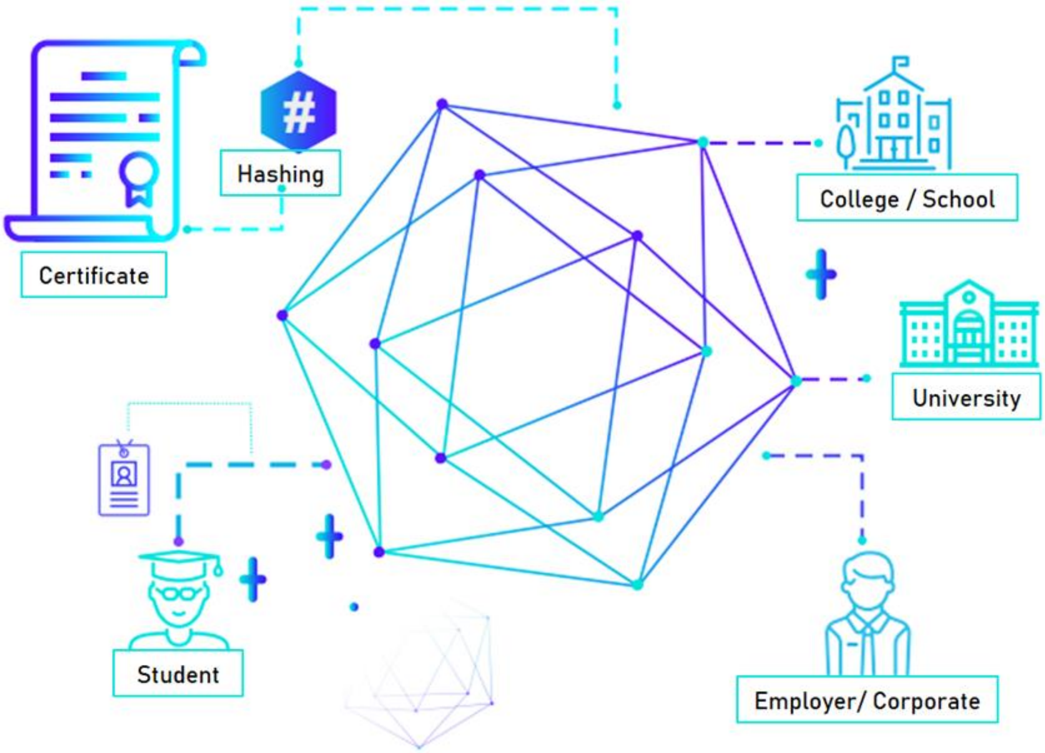


Figure 1.1: How Blockchain can be used in educational certificate issues and verification operation [3]

Additionally, in this system data doesn't have to be stored in one place as each certificate's details are stored in an individual file and all verifications are done through the Ethereum platform. With this framework, the cost of maintaining a Blockchain-based certificate system could be extremely reduced as compared to building a traditional centralized database. Therefore, it can lead to better security and cost savings. Furthermore, recruiters can also gain profit from such a system because when applicants submit a certificate to the recruiters, they (recruiters) don't need to send a certificate verification request to the authority to check the originality of the certificate.

1.2 Motivation:

Educational Certificate is issued after the accomplishment of an educational program or course and ordinarily, it is recognized as evidence or proof of its completion. It ensures the authenticity of the academic background of a candidate. It also validates the legitimacy of an employee's education qualification based on the degree, year of completion, passing grades, and other information about the respective program. Additionally, it also assures that the claimed educational degree, skill, or, training of the certificate of a candidate are true. Education certificate verification has become a very important procedure. It's essential portion to check the quality of applicants before employment. This leading role of a certificate engage fraud and scammer and stimulate them to try getting jobs by fabricating educational certificates. To evade this, the recruiters usually submit a request of verification to the respective university authority of the received documents from the employer for verifying the legitimacy, and university authorities spend millions of dollars annually for maintaining this complex and lengthy verification process. Also, the traditional verification process is a time-intensive process where human interaction exists, and that can conduct educational certificates fraud. This entire process takes a huge amount of time to execute the selection process. According to [4] Forged university education certificate has been recognized as a significant problem in the educational society. Employees generate fake education certificates with the help of scammers or fraud to achieve their dream jobs. [5] mentioned that, there are approximately 2 million fake educational certificates generated in the United States alone and 300 unauthorized universities operating in the U.S market with 800 operating worldwide. [6] indicated that counterfeiting educational certificates requires employers roughly $ 500-600 billion annually

[7] also indicated educational certificates issued by a lot of illegal institutions that are unregistered/unaccredited to permit such credentials papers or commit unconfirmed arguments about their identification and accreditations are a forgery. Hence, one major key challenge in the field of education is to tackle this severe and alarming issue by stopping counterfeit certificates and also find an efficient way of minimizing the cost, time, and also

the complexity of certificate verification process. Moreover, applicants, issuers, and employers everybody need a trustable platform that will help to overcome all of these problems.

1.3 Objectives:

The principal objectives of our works are:

- To build a Blockchain-based Decentralized Application (DApp) for Verification and issuance of Educational Certificates.
- To remove the entire third-party interaction in the verification process.
- To reduce the cost and time of the verification process.
- To secure the certificate verification and issuance process from fraud and scammers.
- To ensure the authenticity of the certificate of an educational institution.
- To provide benefit to the students, institution, and employers using Blockchain-based certificate verification system.

The objectives of our works are supposed to be answered by the following questions:

- What are the present flaws in the certificate verification system?
- How these present flaws are eliminated using Blockchain Technology?
- How can these obstacles be tackled and what are the potential solutions?

1.4 Research Contribution:

This report presents a decentralized application (DApp) named DIUcerts of a blockchain-based Educational system. Our DIUcerts - decentralized blockchain application allows educational institutions to create certificates for their students by creating a digital representation of academic certificates and publishing them onto the blockchain platform like Ethereum with the help of our DIUcerts DApp. Once the certificates are deployed on a public ledger onto Ethereum through smart contracts (blockchain chain code), they are permanent and immutable. It cannot be changed or modify by anyone.

After successfully publishing the certificate on the Ethereum network, Our DApp also allows the authority to view the digital certificate which also provides a Certificate ID and Certificate Transaction Hash key. Both keys ensure the authenticity of the certificate and can be used for retrieving and verification the certificate later. So, there is no need for a third-party or traditional centralized database server or extra maintenance cost.

1.5 Organization of Report:

The remaining part of this report contains the following chapters:

- Chapter 2 states the literature review of Blockchain technology, architecture, core components, and pillar of Blockchain, decentralized application(DApp), and some related work of our project
- Chapter 3 represents the methodology including the proposed model design and different components of building DApp.
- Chapter 4 demonstrates the Implementation & Evaluation of our work
- Chapter 5 presents the conclusion, strengths and limitations, and future scope of our project

CHAPTER 2
Literature Review

2.1 Blockchain:

A Blockchain is a decentralized, shared, fault-consuming, and append-only database. Which tries to manage the records in blocks. For any kind of transaction, blockcha-in doesn't need to be dependable on the trust. Solving the problem regarding double-spending is one of its features. Furthermore, it has a benefit like the recording of any transaction is not transferable to a third party as long as the valid core of the system manipulates the power of the CPU. In a time of need, nodes can join or exit the network. Achieving the majority by voting with CPU power, a valid block is detected and others are said to be invalid. Blockchain provides the feature of numerous applications like Decentralized Applications, cross-border payments, asset management, supply chain and logistic monitoring, voting system, etc. [8].

In 2008, Satoshi Nakamoto conceived the idea of "Blockchain". Using the hash method, he improved the model. In this model, he used timestamp blocks. These blocks were not being required to be approved by a trusted party. Besides, he used a difficulty parameter in order to stabilize the block rates which were added to the chain. Moreover, he used the cryptocurrency bitcoin to avail all the transactions on its network. In order to do that, the core component of the bitcoin worked as the public ledger. It was August 2014, bitcoin blockchain storage reached 20 GB (gigabytes). Moreover, Blockchain technology was discrete from the currency as well as its potential for other financial, inter-organizational transactions were explored this year. Then here came the Ethereum blockchain which introduced computer programs into the blocks by representing financial instruments, like bonds. Commonly it is known as a smart contract. After that, blockchain became popular day by day which enables it to reach 200 Gibibytes by early 2020. [14]

2.1.1 Variants of Blockchain:

There are primarily two variants of blockchains. Which are Private and Public blockchain. Although, there are several variations, like Hybrid and Consortium blockchains. Consisting of a package of nodes working on a peer-to-peer (P2P) network system. Updating timely, the list of each transaction can be regulated by every node.. In figure 2.1 shows the model of public, private and consortium blockchain.

Public:

The catalog of this type of blockchains are visible to all who are connected to the Internet. There is open permission to review, add or subtract any block of transactions by allowing various devices on this network.

Private:

packages of people including any definite organization who are allowed to verify or add transaction blocks in Private blockchain. Else one who is connected to this network can view.

Consortium: For adding and verification of the transactions this type of Blockchain is used. It is often more efficient both collectively and individually. The regulation with pre-authorized nodes, anyone including organizations can use this Blockchain.

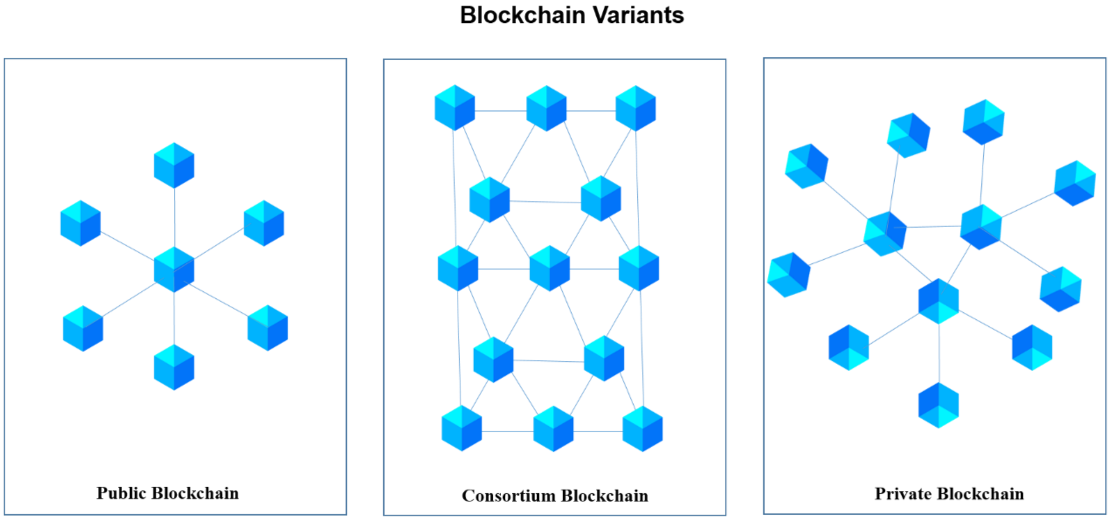


Figure 2.1.1: Public, Private & Consortium Blockchain Model

2.1.2 Pillars of Blockchain Platform:

Nowadays, there are many public and private blockchain platforms obtainable in the marketplace. For that, one has to gingerly choose a decent option based on one's obligations. This has to be appreciated based on the pillars of the blockchain platform as listed below:

Decentralized network: One of the key architectural morals of the blockchain platform is its decentralized temperament. This means the transaction in the blockchain network is replicated across all the nodes of the network and all the nodes are associated. This blockchain platform is immensely feasible as there is no possibility of tampering with the transaction document because it is copied to all the nodes — and tampering with all the nodes in the network is effectively improbable at any given time.

Platform security: Though the blockchain platform is decentralized in behavior with many users being a section of the workflow scheme and engaging in the several periods of executing the transaction, there is a superior level of security convinced in any blockchain platform due to its decentralized mold and multi-node record copy. In addition, different blockchain platforms clinch upper degrees of platform security like the consensus algorithm, permissionless ledgers, usage of cryptocurrency for transactions, and the smart contract amenity, to name a few.

Record immutability: The decentralized network of block chain platform and ledger mimicked across all the nodes of same network certify that the record kept in the ledger for execution of any transaction are absolute enough to swap in a record is adopted only when it is accepted by all the participants across nodes. Being anonymous, there are limitations in the network to change the record of all ledger. Emendation of any record in the network is altered as a new processing stage of transactions so that they can keep it as exclusive entries.

2.1.3 Blockchain Architecture:

The architecture of block chain includes database and network of nodes. A block chain database is split, fault tolerant, append only and distributed. All records are perpetuated in blocks. Though users approach the blocks, they cannot expunge them. Each block is connected to one another by chain and they all have unique hash value. Every block accommodates assorted demonstrated transactions. Furthermore, each block incorporates a timestamp stipulating fabrication time, a contingent number for doing cryptographic operations. The block chain network embodies nodes which sustains the block chain in a peer to peer and distributed craze. Unreserved supervision is restricted ,though nodes are entranceable.

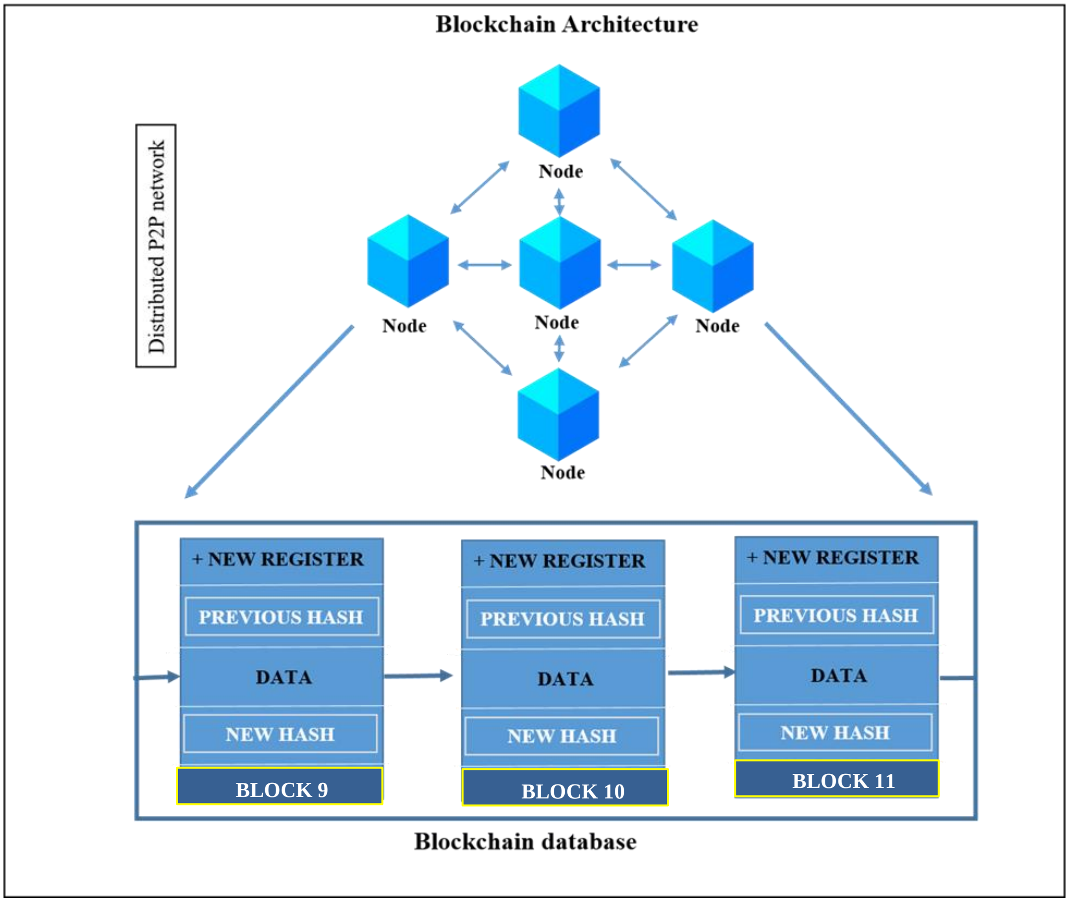


Figure 2.1.2:   Architecture of Blockchain p2p Network

In the figure 2.1.2 shown the point to point distributed network architecture of Blockchain technology which also represents the architectural view of block, node, key and data. A block chain database and network is decentralized and distributed. Construction of a block in a block chain network is combined mainly three things: Data, Hash and hash of previous block. Data principally holds information about transactions. In the case of Bitcoin, data predominantly holds details about from where to whom a transaction is transpired and the amount of transaction. The most important part of a block is hash. It is unique totally. Hash value is created at the time of generation of a block. It is a kind of identity of a block. Another main thing is previous has which is needed to create a chain as Blockchain is a chain of blocks. Hash of the previous block is interlinked with new block hash to interconnect with each other. When a block is found valid in the Blockchain network, it is fixed to the Blockchain database. Once a block is attached, it is hard to alter or amend. For supporting money, assets and smart contract transactions, Blockchain technology has three generations. Among them the first one is Bitcoin Cryptocurrency to transact money and the last generation is Smart contract. The capabilities of Blockchain are augmented significantly by Smart contract which led to its worldwide admiration. [9].

2.1.4 Core Components of Blockchain:

Node:

Node means user or computer who connects to the Blockchain network. It follows consensus rules and determines whether the transactions are valid or not. Nodes can be any kind of device and data is stored there. In a network Each node has a copy of the whole Blockchain, so every transaction is known. Basically, a node is like a device that contains an entire copy of the transaction ledger of the Blockchain.

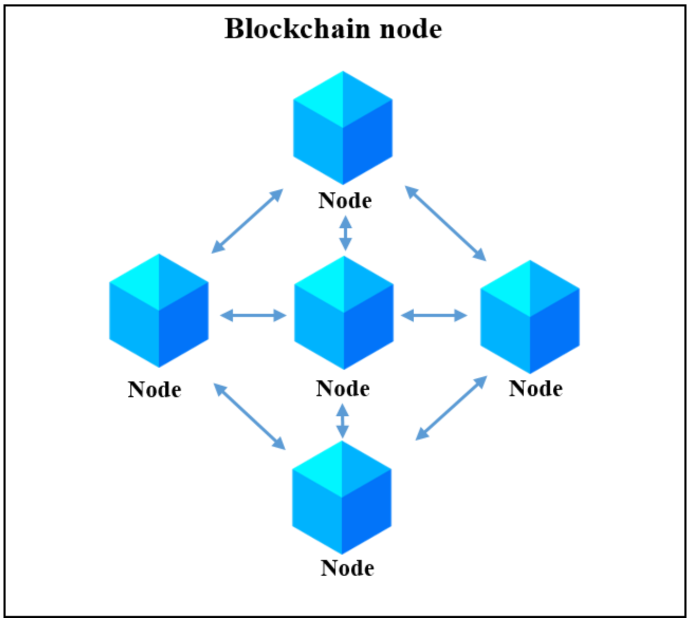


Figure 2.1.3: Nodes connection of Blockchain Network

In figure 2.1.3: there are 5 nodes, all nodes are connected with each other to run a Blockchain together.

Main Data:

Transaction types determine main data. It is substantially a transformation of two nodes in a network. However, money transfer or record transfer can be a good example of this type of main data.

Hash Values:

Hash is the unique value of a block. The message to be hashed is called input and the function used to do so is called the hashed function and the output is called hash value. There are many formulas to hash a message but a cryptographic hash function needs to have some qualities. Function required for hashing is a one-way function. Each hash value for output has to be unique. In a Blockchain hashes are used to represent the current state of a blockchain. These are helpful to authenticate the integrity of block's.

A slight change of hash value will change the whole. If the block's hash value remains the same for a long time, it will give the user a high level of credence. It makes users trustworthy to the transaction history of blockchain [10].

Hash of the Previous Block:

With the completion of a transaction, a hash is engendered and broadcasted. Merkle Tree is the most prevalent algorithm at the formation of hash as it allows easy hash and easy de-hash options [10].

Hash of the Current Block:

Current hash blocks mean the final hash which is stored in the block. Blocks have a fixed size that's why there are restrictions on transactions number

Transaction:

Transactions are the miniature blocks in the system. They ordinarily include addresses of the sender, receiver, and a value. Credit card assertion is the standard example of it. Addition of previous transaction and the receiver's public key construct hash by the digital signature of the relocated value of owner. Then transactions are brazenly declared. Transactions are bunched and released to each node in the form of a block. An independent verification process is executed by each node when new transactions are allocated. Each of them is time-stamped and culled in a block.

Block:

Blocks are the storage of data in a blockchain network. Their main intention is to bundle sets of transactions and replicate them to all nodes in the network. Miners generate blocks in the blockchain. To manufacture a valid block, the most preferable operation to all networks is mining. Storing of transaction records in the blockchain, nodes are going through some steps like verification of the pending transaction, checking cryptographical seal, and wrapping into the blocks. Block header plays an important role like metadata in verifying block's validity. The main themes of metadata of the block are shown below:
The rest of the block accommodates transactions. It can be any number of transactions clumped in a block depending on the choice of a miner.
Types of Blocks:

1. Main branch blocks expand the current main Blockchain which is the longest chain in a network.
2. Side branch blocks mention a parent block except for the longest chain.
3. Orphan blocks credential a parent block which has no knowledge of node processing. From the diverging concept, when fewer blocks are mined, side branch blocks cannot be considered as a part of the main branch. They are considered as parent blocks only when more blocks are mined. But a discrete side branch will be restructured into the main branch.

P2P Network:

Based on the IP protocol, the blockchain is a peer to peer (P2P) network operating system. It is a smooth topology with decentralized nodes. In this network, all nodes are equitably provided and can ingest services in case of consensus algorithms. As P2P networks have no single ambushing or collapsing point, they have more security. Permissioned and permissionless are the types of a blockchain network. In a permissionless blockchain, anyone can be added to the network. while a permission-based blockchain has restrictions to add new members. To add new member's pre-verification is mandatory for a permission-based blockchain or private blockchain. In a Blockchain structure, every single node in a network conserves a replication of the blockchain. The decentralization of blockchain architecture is the solitary credit of the P2P network that it is built on.

Miners

In Blockchain, miners play a vital role. They validate new added transactions and record the block in blockchain public ledger. After a successful execution of adding block in the blockchain ledger, they get rewards as the gas fee which is paid by the users who actually want to add their block in the Blockchain network.

Smart Contracts:

The digital quality of Blockchain has led to it being attendant with smart contracts. A deal with the corporal world is a covenant among parties that executes certain proviso and the transfer of an asset will happen. To initiate the asset transfers and meet the validated conditions by machines, the code of smart contract codifies these attributes. Additionally, processing or validating the contractual transaction, Blockchain platform may furnish the computational materials where other parties are fascinating in the transaction, thereby gaining a stake in the transaction to verify the ledger. Ethereum is an example (an open-source, public, Blockchain-enabled computing platform) that allows users to connect smart contracts. Users need to pay fees to put up computational resources, delegate smart contracts and validate the transactions in ethereum [10].

Private smart contract:

In the field of business, permissioned blockchain is getting admiration day by day. For business transactions, it has a very shortage number of stakeholders which provides superior speed of transaction. In comparison with a public blockchain, a private blockchain has a lower validation cost. In the case of a restricted amount of nodes, private blockchain can be coherent. Consensus mechanisms for both types will contradict. A private blockchain is dependent on business requirements. According to the requisition, it uses the following algorithm: PXOS, RBFT, BFT, PBFT, RAFT, Suitable environment to generate business application provided by IBM are Hyperledger Composer, Hyperledger Fabrics, Hyperledger Indy and Hyperledger SideDB [3]. Among them, now the trendiest platform is Hyperledger fabric for its development parts which are called members. Every peers of member organization gets certified by certificate authority [8].

Public smart contract:

Permissionless blockchain is an independent platform because it has no requirements to cooperate with its peer nodes. In the system, every node has authorization over installing smart contracts. But the validation cost of a public blockchain is very lavish as members have to pay a nominal fee to avert spamming, executing, and instantiating smart contracts. To make contractual terms, bitcoin scripts has developed bitcoin. Many applications used Ethereum to control money and construct decentralized applications. The environment of Ethereum developed a cryptocurrency which is known as Eth. [8].

Mining Techniques:

Mining is a way of including transaction records to the blockchains public ledger. It happens so that every transaction can be confirmed securely, and also every single user of the network can access this ledger easily. There are lots of mining techniques available in blockchain technology. In the table 1, we can see the comparison of different types of mining techniques.

TABLE 1: COMPARISON OF DIFFERENT MINING TECHNIQUES [9]

MINING TECHNIQUES	RESOURCE	RANDOMNESS	EXAMPLES	MINERS REWARD
Proof of Work	High computation energy & power	NO	BITCOIN	YES
Proof of Stake	Assets or stake	Randomized selection of Blockchain	ETHEREUM	NO
Proof of Space	Huge Storage	NO	PERMACION	YES
Proof of Importance	Significance of Node	NO	NEM WALLET	YES
Measure of trust	Reliability	NO	NO	YES (TRUST)

In the Table 1, it represents the different mining Techniques of blockchain. All mining techniques are demonstrating bellow:

Proof-of-Work:

PoW is an algorithm in a blockchain network which is used to confirm transactions and turn out newly created blocks to the chain. Miners do a competition to finalize transactions and get rewarded in PoW.

Proof of Stake:

Bitcointalk forum was launched PoS consensus algorithm back in 2011 to solve the problems which are generated by PoW. Reaching consensus is the main goal of both of them. But their process of reaching their goal is different.

Proof of Space:

At the time of mining, mining nodes need to have an upper level of storage capacity instead of having higher computational potentiality. Several theoretical and instrumental implementations of PoS has deliverance. However, the essential higher space of memory is the main challenge like the challenge of computation of PoW.

Proof of Importance:

PoI is a one kind of mining technique that calculates the consequence of an independent node on the basis of transaction amount and the balance of that node. It allows priority to the most significant nodes with a hash calculation and choose the nodes for next block formation.

Measure of Trust:

Trustworthiness is the most important issue to initiate a block. Nodes are getting priority on the basis of their behavior. Good behaving nodes go after the protocols and get rewarded.

TABLE 2: BLOCKCHAIN PLATFORMS FOR RAPID PROTOTYPING [9]

Name	**Working Types**	**Cost Evaluation**	**Language Supported**
Ethereum Blockchain	Public & Smart Contract based	Ether for the transaction and computational services	Python, Go, C++
Hyper ledger	Private & Public	Open-Source	Python
Multi-chain	Private & Permissioned	Free & Open-Source	Python, JS, PHP, Ruby, C#,
IBM Blockchain	Private or Permissioned	Limited & enterprise plan (free/paid)	Go, JS

From Table 2, it gives us an idea about how different types of blockchain platform and their popularity, activity, types of network, pricing and the languages they are supported for development purpose.

Ethereum:

Ethereum is a common platform for both private and public blockchain. Performing business logic at first the blockchain holds the smart contract. It generates the smartest contracts and decentralized autonomous organizations. Ethereum would take over the whole world as the global computing system if the Bitcoin blockchain are scrutinized as a global payment network, Furthermore, Like Android, ethereum is also a platform of open-source (developed by Google). It provides a basic structure that is very helpful to the developers to create applications. Ethereum and developers maintain and flourish the infrastructure [8].

Hyper ledger:

Hyperledger is considered as an umbrella project of open-source blockchain and related tools, started in December 2015 by the Linux Foundation, which has already received huge amount of benefaction from IBM, Intel, and SAP Ariba which supports the blockchain-based distributed ledgers.

Multi-chain:

The MultiChain technology is a policy of helping users to institute certain private Blockchains that can be used by the organizations which are performing financial transactions. Multichain provides us a very simple API and a command-line embrasure. This is helpful to safeguard and set up the chain.

2.2 Decentralized Application (DApp):

Decentralized applications are doing race on a P2P network of computers except an isolated computer, and any single authority does not control them. Bit Torrent, Kazaa, and Tor are some classical specimens of DApps which are not employed in a blockchain framework. Blockchain provided users the capacity to trust decentralized applications. It intercepted some of the applications' curbs, such as the virus affected software and missing nodes. In order to function aptly, decentralized applications exist on the blockchain that require the disposal of a smart contract [11].

2.2.1 Cipher

Avanza's Blockchain implementation platform is known as Cipher. It is a platform-agnostic solution that can steer on any kind of underlying Blockchain technology. For government agencies and regulators in different locales, Cipher behaves as middleware that reinforces a portfolio of four blockchain DApps. The kingpin areas of Cipher's blockchain-based solutions are Transformation of Digital Government and Financial Regulation & Supervision.

Cipher will take action as the enablement layer to ensure that next-generation blockchain technocrats keep performing well, as the world is turning towards decentralization [12].

2.2.2 Chainlink

According to Chainlink's official website, "Chain Link network provides reliable tamper-proof inputs and outputs for complex smart contracts on any blockchain." This platform issues a trustable and immutable end-to-end.

Chain Link ensures data integrity and uses same consensus algorithm that blockchain used in their platform. Moreover, Chain Link imparts your smart contract with all the inputs and outputs it needs to gain its full potential [12].

2.2.3 EOS Dynasty

It is the earliest RPG and PvP game on the blockchain where players can intensify their heroes through collecting materials, forging equipment, and domestication mounts. The game enables players to get conferred. Three Kingdoms Tokens (TKTs), which is a finite cryptocurrency which allows user to store data that is based on a smart contract. Not only this, but premiums are also only awarded from the games, once players stick out to particular military ranks. [12].

2.2.4 Trace Donate

As present-day benefaction sectors suffer a lot from the lack of transparency and traceability, Trace Donate is inaugurated to eradicate such issues. It is an identity management platform depicted for a secured and transparent way of executing and also tracing the process of Cross Border Remittances. Trance Donate enables the charity to collect donation in a secured way. So, the donor keeps faith in the donation process.

With this DApp, donors accrue real-time updates via SMS and email about how the donation is used and for what purpose [12].

2.2.5 Brave Browser

Brave is a such kind of web browser with vigorous users, attempts to generate a blockchain-based and web 3.0 enabled platform that keep the user's privacy and secured personal data.

This decentralized app manufactures a new appraise way of advertising world, where "consumer attention" is utilized to monitor the unverified or unauthenticated clicks as well as views on the web page.

This allows the users to a new business models with Brave Rewards that can be easily traded same as bitcoin platform [12].

2.3 Related work

Some related educational certificates in blockchain are given bellow in TABLE: 3.

In, Table 3, it demonstrates some educational certificate verification platform and explained their features, functionalities and also discussed the limitations of their feature:

TABLE 3: BLOCKCHAIN CERTIFICATE VERIFICATION PLATFORM [13]

Institution/project	**Salient features/functionalities**	**Shortcomings in feature/ functionality**
KMI, OU- UK	Badges, certificates, and web reputation in the blockchain	-Does not support employers as an entity -Data is stored on a public blockchain -The certificate is vulnerable to manipulation -No clear method of the authenticity of parties
UNIC	Resolve fake certificates Tools available for the authenticity of the certificate Food in integrity, privacy, and ownership	-Requirements for an employer to verify the certificate is inadequate -A student cannot authorize the prospective employer to verify the certificate

		-No clear method of the authenticity of parties
MIT Media Lab	Offers more control to students Uses digital keys	-The level of trust is low -The certificate can be accessed by everyone -No clear method of the authenticity of parties
Blockcert	Open Standard Platform	-No separate verification services -Vulnerable to spoofing attacks
Smart Cert	Resolves problem of fake certificate Student shares hash with the employer	-Vulnerable to attacks -Need for basic information security measures -No clear method of the authenticity of Parties
Records Keeper	Proof of authenticity in the certificate The entire verification process is based on ownership	-Certificate tampering vulnerability Participants can verify after obtaining ownership

DOCSCHAIN [24]	OCR used for scanning certificate, Blockchain-Based IOT features for verification.	-Only ready the grayscale image - No user interface - Not evaluated cost and time.
OPENCERTS [25]	Provides a digital unique code with certificate File comparison check in the blockchain network. Supported View, Check, Verify	-Printing certificate is not supported

CHAPTER 3

Methodology & Model Design

3.1 Methodology:

The proposed methodology utilizes Blockchain technology through the functionality of a decentralized application using a smart contract and developed based on an Education certificate verification and creation system. All transactions recorded and verified on the Blockchain cannot be modified, hacked, or deleted. The main purpose of the proposed DApp is to empower the educational certificate verification system to a trustable platform and reduce the complexity and server maintenance cost of the system.

For developing the DApp, we utilized the Solidity language for smart contract implementation on the ethereum platform. We also used the web3.js ethereum library which allows DApp developers to interact with the Ethereum Blockchain as a local or remote node in ethereum platform with the help of HTTP, WebSocket, or IPC.We also deployed our smart contracts through the Remix IDE. This DApp was first tested on the Ropsten Test Network before executing on the Ethereum Mainnet. For performing the blockchain transaction, we choose Metamask which is a crypto wallet & gateway to blockchain apps.

In the front-end, we have used the React.JS, javascript library for building user interfaces. It ensures faster rendering and interactive single-page web applications and allows users to easily interact with the smart contract.

3.1.1 Solidity Language

The Solidity language has been created by Ethereum's team and introduced in 2014. It's a high-level, OOP language for writing and developing smart contracts and also it supports many libraries and inheritance.

Solidity is powered by C++, JavaScript, Python, and intended to target the EVM.

EVM stands for Ethereum Virtual Machine [15].

Main Advantages of Solidity for creating Smart Contracts in Ethereum Blockchain:

Functional: Solidity is used for smart contracts. This is mostly used in money-related needs (such as auctions, crowdfunding, or multi-signature feature enabled wallets). However, we can create other decentralized applications like voting, Land registration, healthcare, and so on.

Flexible: We can use a Remix IDE or download a command-line compiler on PC to write smart contracts. Both options are free for creating, compiling, and deploying.

Improving: Solidity language updates continuously, such as new features or bug fixes, are introduced constantly.

3.1.2 Remix IDE

Remix IDE is a browser-based open-source ide. It has an expeditious advancement cycle and has a superb number of plugins with built-in graphical user interface. The remix ide is used for the development of smart contracts as well as an immersive platform for learning the Ethereum Blockchain.

It is a development tool that uses a plugin-based architecture. It has also massive module features like various solidity compiler, EVM version, web.3 environments, metamask wallet support, debugger, and one-click deployment tool.

Remix is a robust browser-based open-source tool that assists you to write, debug and deploy smart contracts directly from the browser. [16]

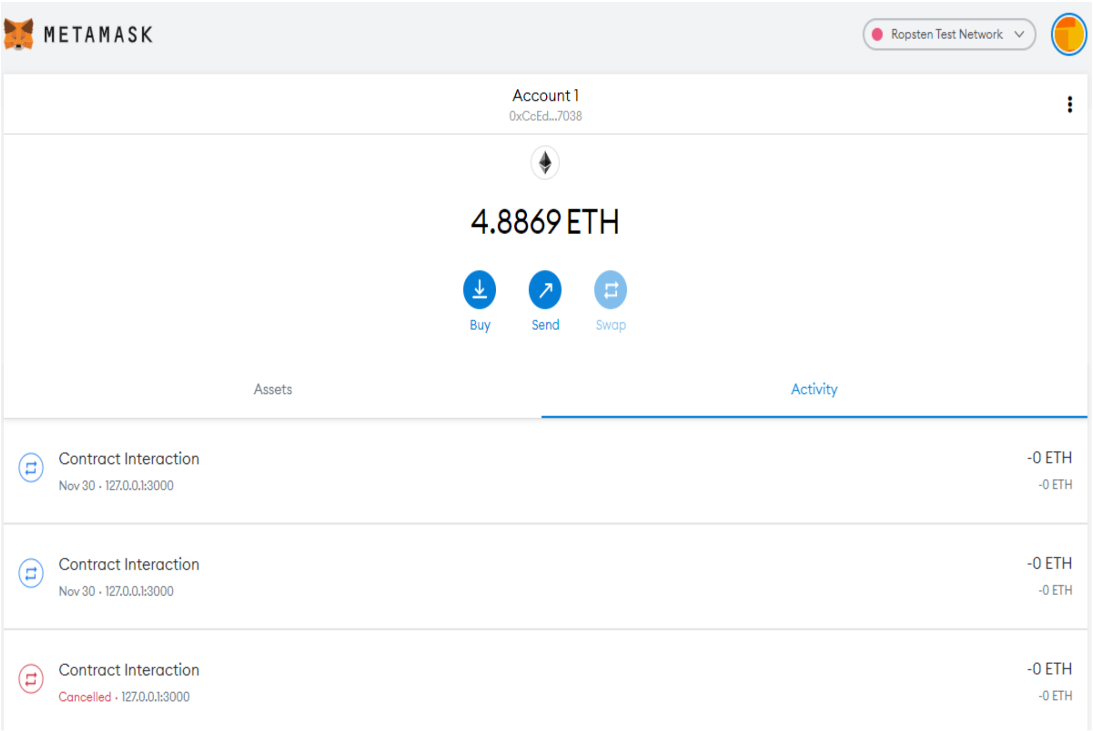
3.1.3 Metamask Wallet:

The main features of the metamask wallet given below:

- MetaMask is a browser plugin that serves as an Ethereum wallet. It’s a crypto wallet and a gateway to experience the blockchain DApps.
- MetaMask is available at browser extension in chrome, Microsoft edge, Firefox and also available in the mobile application store. It provides you with a secure login, key vault, token wallet, and also balance transfer access— it supports you with everything need to manage digital assets.

- It also provides the most manageable yet most reliable, secured and easiest getaway to connect with the Blockchain-based applications.
- It provides passwords and key, so only you have entrance to your accounts and personal data. Just choose what to share and what to keep private. [17]

The following figure 3.1.1 shows the user interface of metamask wallet.



Account 1
0xCcEd...7038

4.8869 ETH

Contract Interaction
Nov 30 · 127.0.0.1:3000
-0 ETH
-0 ETH

Contract Interaction
Nov 30 · 127.0.0.1:3000
-0 ETH
-0 ETH

Contract Interaction
Cancelled · 127.0.0.1:3000
-0 ETH
-0 ETH

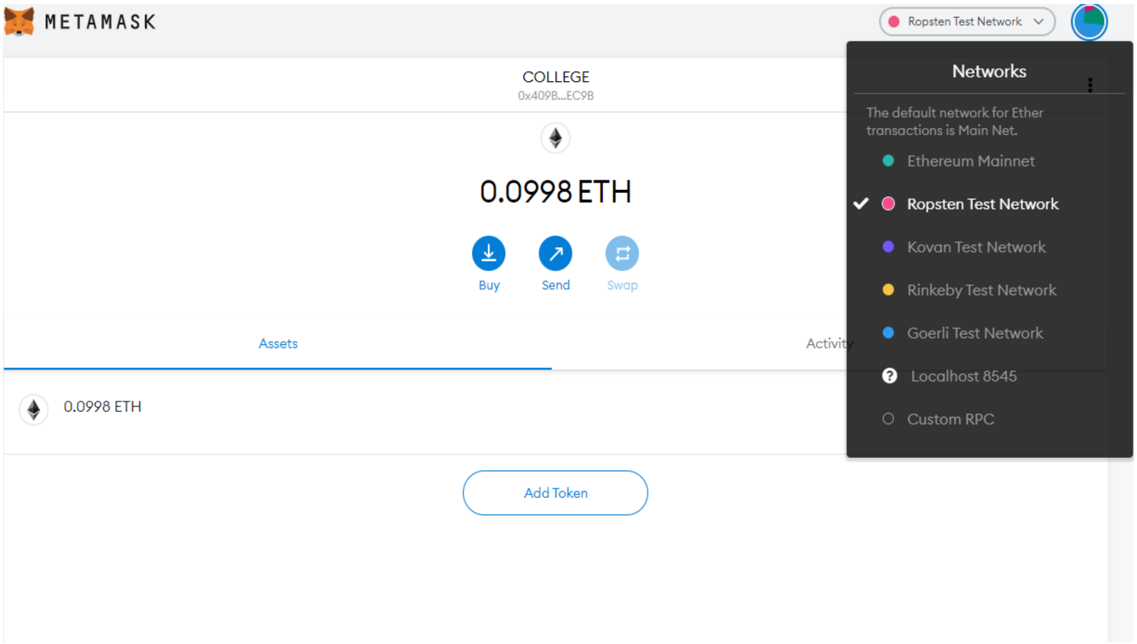
Figure 3.1.1: User Interface of Metamask Wallet (Browser Extension)

3.1.4 Ropsten Test Network

The Ropsten test network is a POW (proof-of-work) test net for the Ethereum platform. To acquire ETH on Ropsten, anyone can willing to mine on the network.

The Ethereum blockchain has a few test-nets like kovan,rinkeby, and goerli test net. The Ropsten test-net supports blockchain developments to test their work in a convenient setting but without the need for real ETH like ethereum main-net. Moreover, this offers the ability to perform transactions without facing any significant gas fees or risking main-net 2KEY. It’s is an exact copy of the real main-net Network, and it allows anyone to engage without requiring real ETH tokens. [18]

The following figure 3.1.2 represents the user interface of the Ropsten Test Network in the metamask wallet.



The default network for Ether transactions is Main Net.

Figure 3.1.2: User Interface of Ropsten Test Network Metamask Wallet

3.1.5 Web3.js Library

Web3.JS is an assortment of libraries that grants you to communicate with the local or remote server of ethereum node with the help of HTTP, IPC, or WebSocket. It’s also a collection of modules that include functionality for the ethereum ecosystem. Alternatively, we denoted this as an Ethereum JavaScript API.

- **WEB3-ETH**
- **WEB3-SHH**
- **WEB3-BZZ**
- **WEB3-UTILS**

We have only used web3.eth for our Blockchain and Smart Contracts development purpose.

Benefits of Web 3.0 Technology

- Transparency
- Fewer Middlemen
- Privacy-preserving and interoperability protocols
- Data Ownership & Sharing Ability
- Decentralized Identity
- Trust Verification
- Decentralized infrastructure and application platforms

Web 3.0 is the new era of the internet, where all applications become smarter, more private, and more decentralized, and also more secured. As the new foundation and platforms come online, the experience of using the internet will change adequately. The present web is a stunning asset, and it empowers us to do effective things. Nevertheless, it also requires us to give immense amounts of data to middlemen companies who aren’t honest about their practices. Web 3.0 endeavors to change that and create a more open and transparent internet.

The following figure 3.1.3 provides an informative idea of the History of Web Evolution from Web 1.0 to Web 3.0 era.

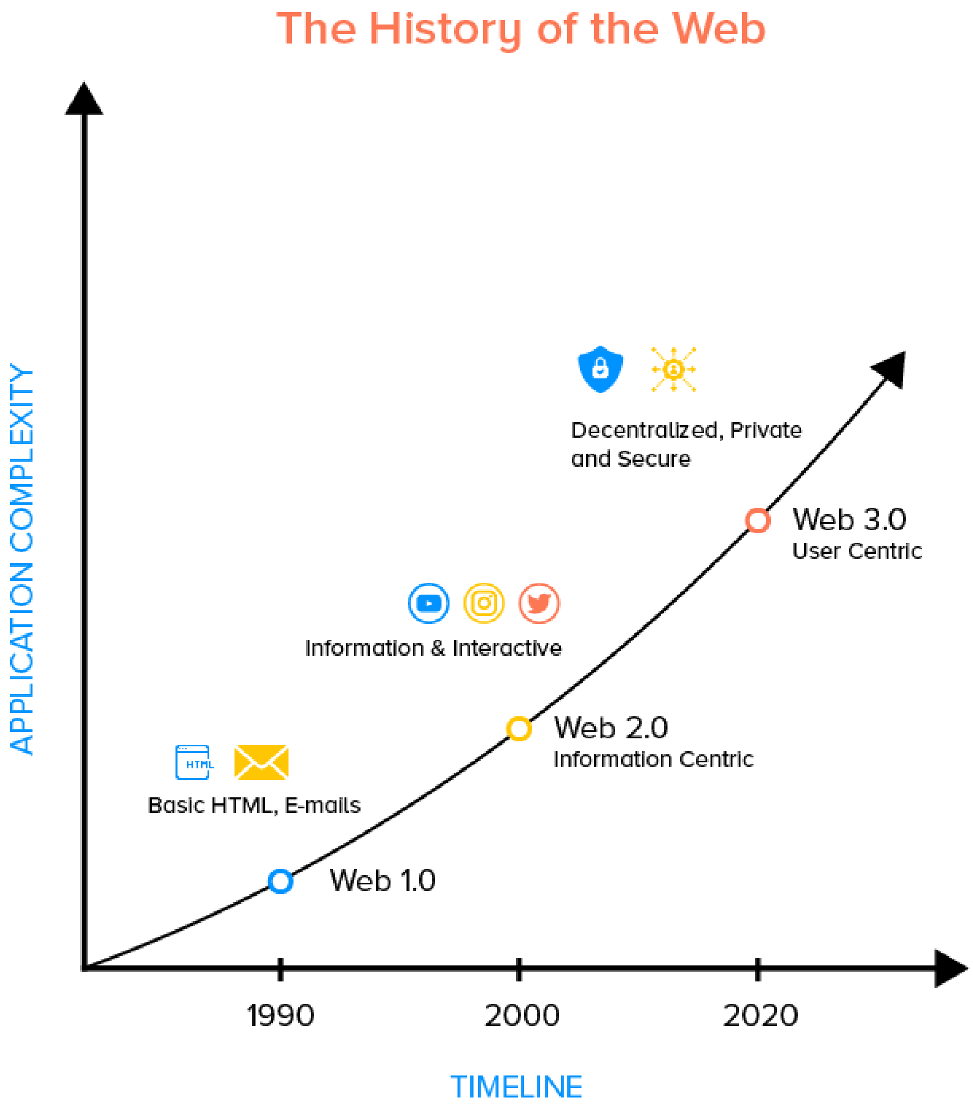


Figure 3.1.3: History of Web: Web Evolution from 1.0 to 3.0 [20]

In the following figure 3.1.4, we can easily get some idea about the Web.30 applications in this era.

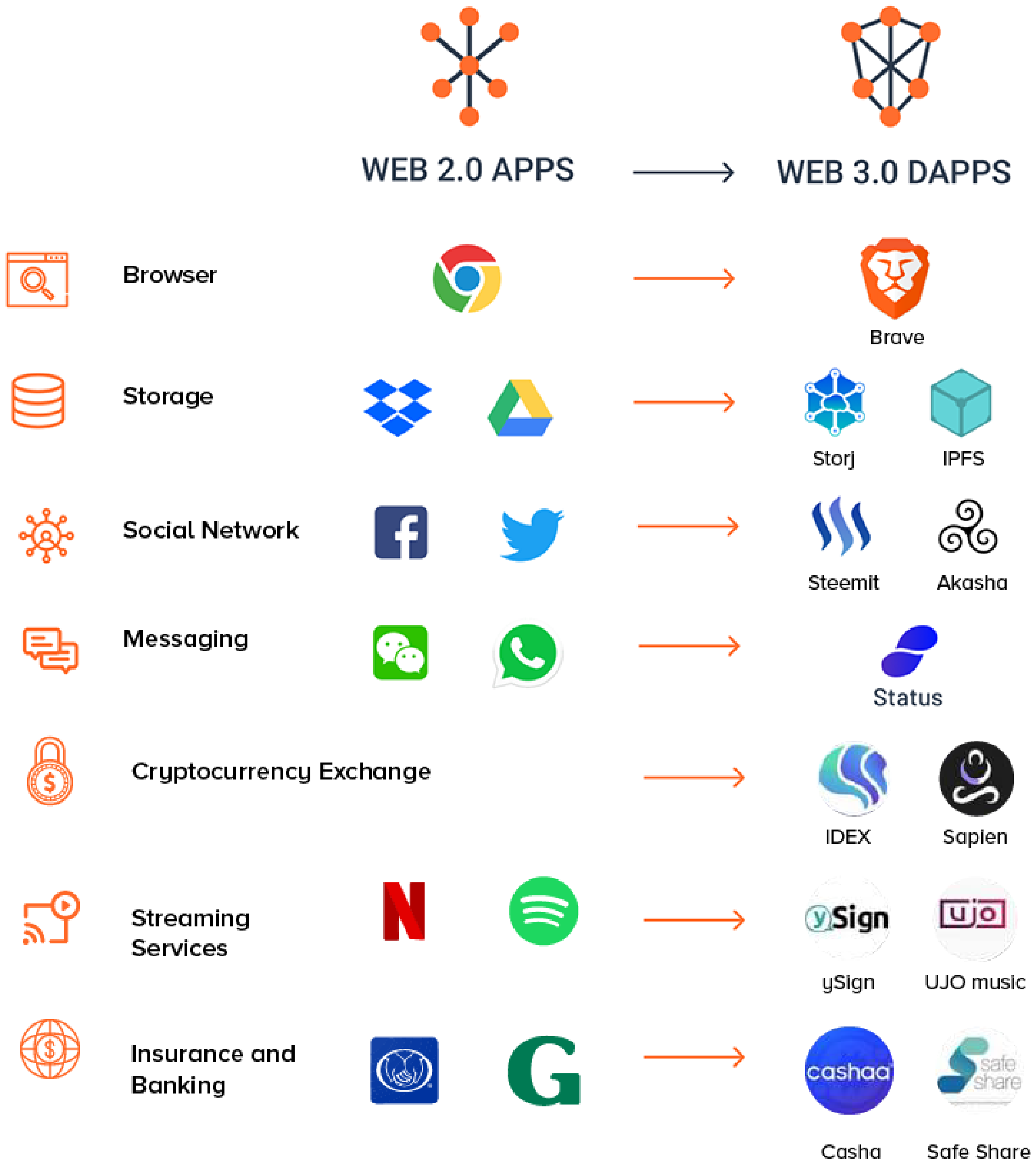


Figure 3.1.4: Real-Life Application of Web 3.0 Dapps [20]

3.2 Proposed Model Design

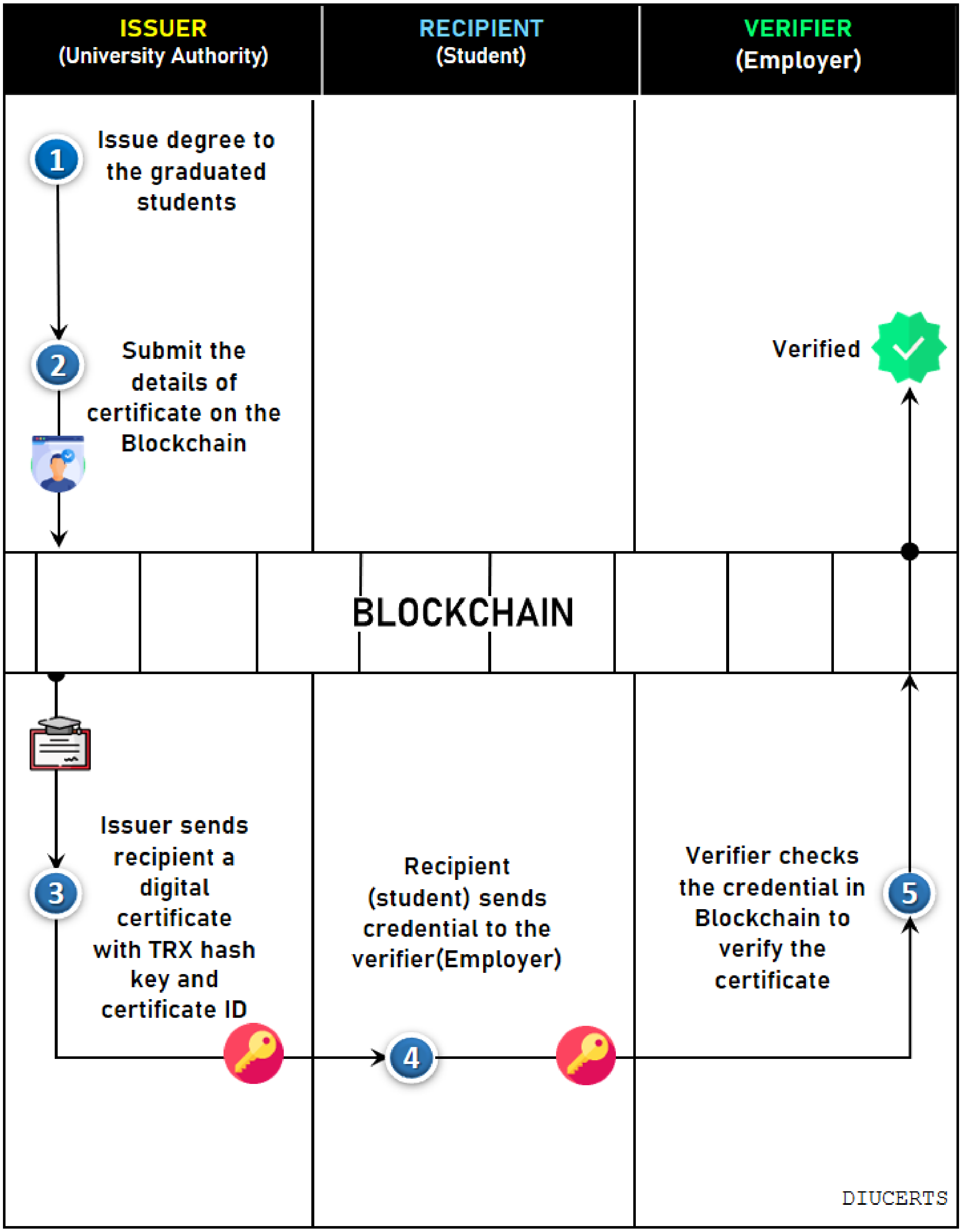

ISSUER
(University Authority)
RECIPIENT
(Student)
VERIFIER
(Employer)
1
Issue degree to the graduated students
2
Submit the details of certificate on the Blockchain
Verified
BLOCKCHAIN
3
Issuer sends recipient a digital certificate with TRX hash key and certificate ID
Recipient (student) sends credential to the verifier(Employer)
4
Verifier checks the credential in Blockchain to verify the certificate
5
DIUCERTS

Figure 3.2.1: The workflow of Certificate Issuance and Verification Through DIUcerts

Figure 3.2.1 shows the workflow of our proposed model: Educational certificate issuance and verification process.

Here is the explanation of each step which is mentioned in Figure 3.2.1 and:

1. At first, issuers such as university authorities proceed with a list of graduation
2. Then issuer submits all the information on the Blockchain through our DIUcerts DApp.
3. After that, DIUcerts forced to store all the data on the blockchain through smart contracts and after a successful transaction, DIUcets automatically provide a digital certificate attached with a certificate ID and transaction hash key. Then authority sends the digital certificate, transaction hash key, and certificate ID for verification purposes.
4. Thereafter, students submit the digital certificate to the verifier (employer) for verification of the certificate.
5. Afterward, the verifier team can check the legitimacy of the certificate information from our DIUcerts DApp. They have to submit the certificate ID for verification. When they submit the certificate ID in our DApp, it checks the blockchain data from the Ethereum network and return a confirmation message if the certificate is valid. Else, it will return an error message. So, the verifier able to find easily the legitimacy of the certificate without any hassle or trust issues.

The workflow of our model engaged with three types of participants, such as:

1. Issuer
2. Recipient
3. Verifier.

Issuer:

The issuer could be a university authority. They have the exclusive functionality to add data to the blockchain. Each university authority has a different smart contract blockchain address. So, all the data stored on the blockchain network for different university authorities separately. An issuer cannot remove, modify, or alter the data of the certificate. Not only the issuer, no one can hack, modify the data, once it's created.

Recipient:

The recipient could be a student. They have the right to see the digital certificate by submitting the certificate ID on our DApp. They also can print the certificate as they want.

Verifier:

The verifier could be an employer or recruiter. Employers have the option to verify the legitimacy of the certificate by submitting the certificate ID. They can also verify the transaction details if they have any trust issues.

Figure 3.2.1 also represents the first contribution of the DIUcerts, which shows the independence of our proposed model, and its facilities to the issuer without suffering any detrition from our application. At present, verifiers and students always follow the traditional methods of submitting and collecting the educational certificate individually. But through our decentralized application, the verifiers can easily verify the certificate with an automatic verification process.

CHAPTER 4

Implementation & Evaluation

4.1 Implementation:

Modern web applications are based on such a foundation in which a single case of downfall normally exists. DApp aims to reduce these problems by distributing crucial components that store data of infrastructure between various nodes. For this reason, when developing DApp we should be taken into deliberation the security, cost, usability, complexity features.

In this project, we focus on the certificate store on the blockchain and also retrieve data from the blockchain. So, we have used some dependency, tools, and technology to create a simple educational certificate verification application system.

4.1.1 DApp Setup Requirements:

Tools and Technology used in DIUcerts DApp:

- Blockchain Framework: **Ethereum**
- Language for implementing smart contracts: **Solidity**
- IDE for deploying smart contracts: **Remix IDE**
- Ethereum wallet: **Metamask**
- Blockchain Network: **Ropsten Test Network**
- Front-end: **React.JS**
- Web Technology: **Web 3.0**
- Web 3.0 Module: **Web3.JS library, web.th**

4.1.2 Creating React App:

React allows us to build a single page web application. It supports a modern build setup with no additional external configuration. We choose to react for the front-end because it allows us to create reusable UI components and React's strings are immutable.

We need some dependencies to create react application. First dependency we need NPM. Node Package Manager shortly called NPM which comes with Node.js [21].

Then after installing node.js, to create and run a fresh react app, we run this command using git or terminal in Linux or cmd in windows.

❑ npm init react-app my-application, or npx create-react-app my-application
*We should use always npx. Because it always creates updated version of react.

❑ cd my-application

❑ npm start – to deploy the application.

4.1.3 Inject web3.js on DApp:

We already know about web3.js and its functionality in chapter 3.1.5

Now we have installed it in our React Application. Web3.js is a perfect and convenient way to interact with the ethereum blockchain network.

To integrate the web3.js to our project, this can be performed using the following command in git, cmd, or terminal: [22]

❑ npm install web3

4.1.4 Front-end User Interface:

We created a front end user interface for our application where the issuer, recipient, and verifier can easily interact with the blockchain. We have used html, css, bootstrap, react JavaScript library to build the frontend user interface.

Certificate Registration Web-interface:

Figure 4.1.1 shows the certificate registration page where the issuer registers all the certificates and this page is built with react-bootstrap.

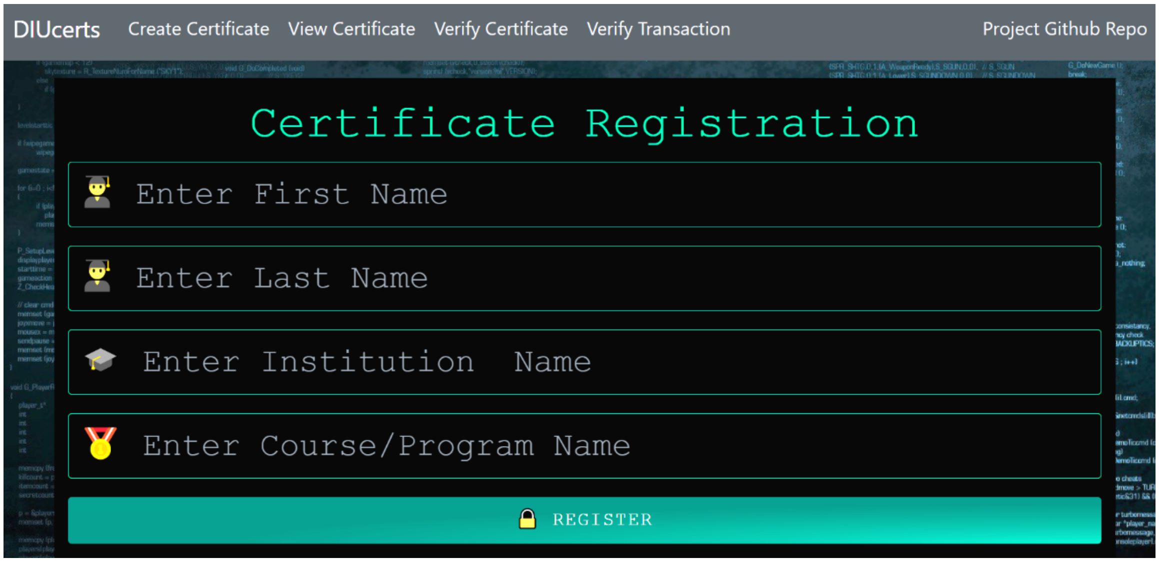


Figure 4.1.1: Certificate Registration web-interface:

Certificate Verification Web-interface:

Figure 4.1.2 shows the certificate verification page where the verifier can verify all the certificates and this page is built with react-bootstrap.

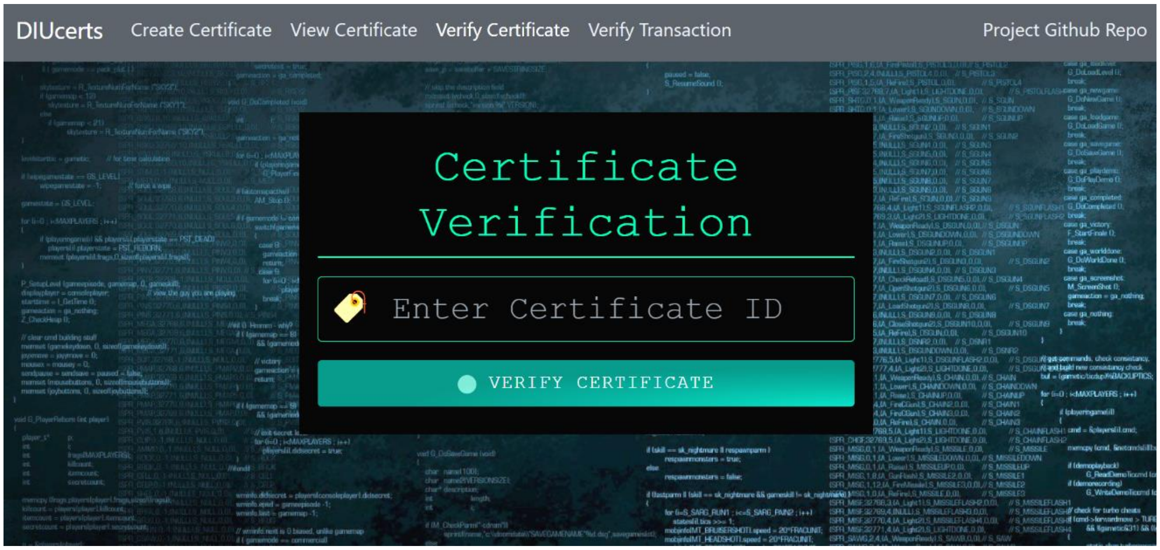


Figure 4.1.2: Certificate Verification web-interface:

Transaction Verification Web-interface:

Figure 4.1.3 shows the transaction verification page where the verifier can verify all the certificates and this page is built with react-bootstrap.

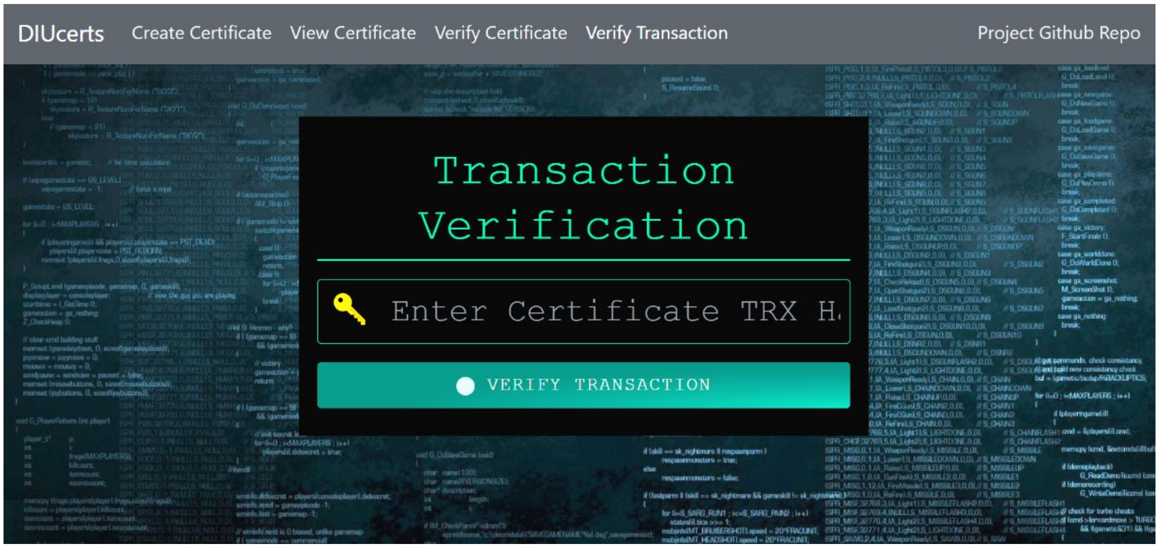


Figure 4.1.3: Transaction Verification web-interface:

4.1.5 Building Smart Contract:

We already know that solidity language is used for writing and developing the smart contracts in DApp applications in chapter 3.1.1. Remix is extremely suitable platforms for creating, managing, testing and deploying of the smart contracts. When we used Remix IDE in the web browser as a web application, we can also use Visual Studio Code in offline on a computer. These two are the perfect combination for building Decentralized Applications.

Hence, to store our certificate and verification process we write a simple smart contracts for our project:

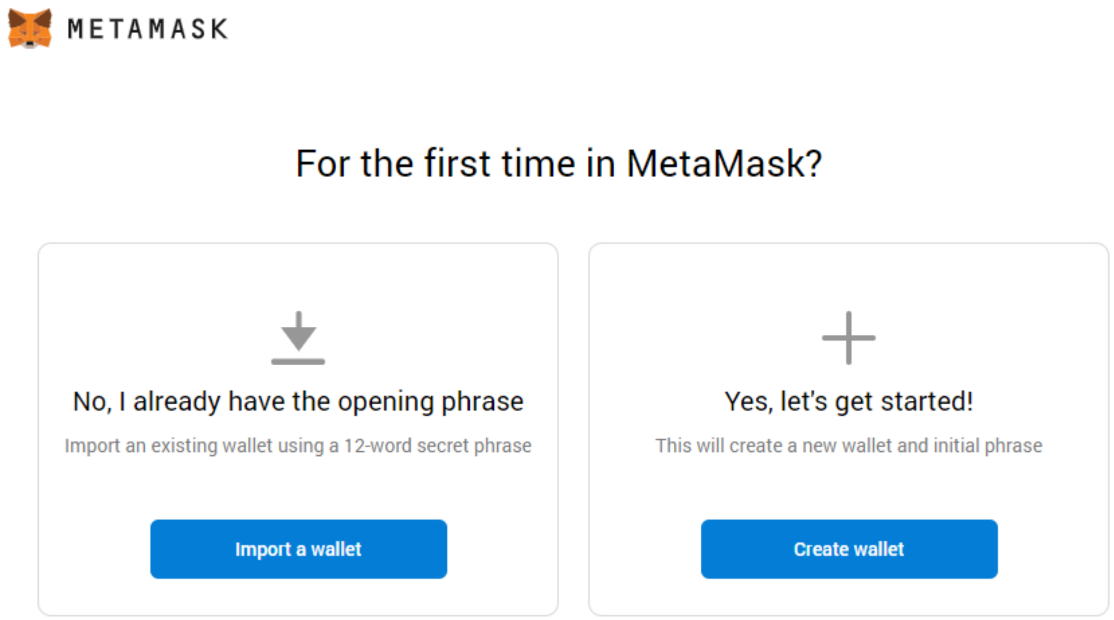
```
pragma solidity ^0.5.0;
contract certificate{
   struct certificate_details{
      string name;
      string institution;
      string course;
   }
   mapping(address=>certificate_details) certificates;
   address owner;
   constructor() public {
      owner=msg.sender;
   }
   modifier ownerOnly{
      require(owner==msg.sender);_;
   }
   event certificateadded(string name,string institution,string course);
   function viewcertificate(address sender) view public returns(string memory name){
      return certificates[sender].name;
   }
   function addcertificate(string memory name,string memory institution,string memory
course) public{
        certificates[msg.sender]=certificate_details(name,institution,course);}
}
```

Contract Explanation:

- pragma solidity ^0.5.0, denotes the solidity version compiler of the smart contract.
- struct certificate_details {} - keep track of all certificate details in a library
- mapping(address=>certificate_details) certificates;
  - Mapping is only a storage type and generally used for state variables. Here, we created a different mapping for certificates and institution to initiate ethereum address storage.
- viewcertificate(),addcertificate() function used to check the verification id , view the certificate in DIUcerts and also certificate registration.

4.1.6 Setup Metamask Account:

To use metamask wallet, we have to install it via chrome extension. After the installation process, we can see the option like figure 4.1.4. If you have a previous wallet, then choose import a wallet else create a new wallet. We have added some faucet (test-net ethereum) from [23].



For the first time in MetaMask?

No, I already have the opening phrase

Import an existing wallet using a 12-word secret phrase

Import a wallet

Yes, let's get started!

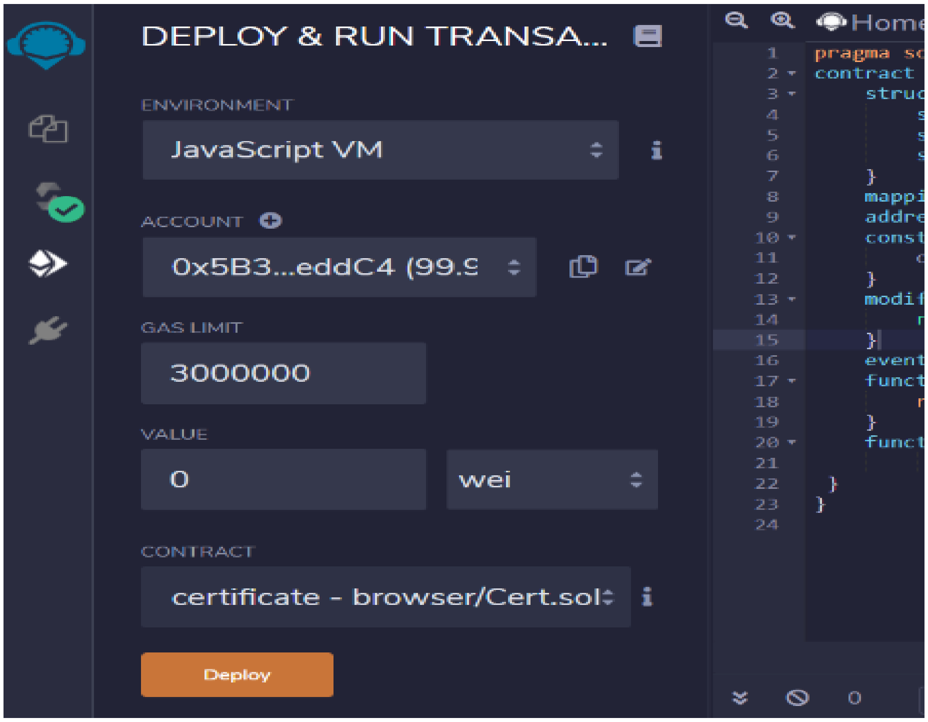
This will create a new wallet and initial phrase

Create wallet

Figure 4.1.4: Metamask Wallet Initialization

4.1.7 Deployment of Smart Contracts:

To deploy the smart contract, we choose Remix IDE. Here is figure 4.1.5 shows the deployed smart contract of our project in remix IDE which is web3 environment supported.



ENVIRONMENT
JavaScript VM

ACCOUNT
0x5B3...eddC4 (99.9

GAS LIMIT
3000000

VALUE
0 wei

CONTRACT
certificate - browser/Cert.sol

```
pragma so
contract
    struc
        s
        s
        s
    }
    mappi
    addre
    const
        c
    }
    modif
        r
    }
    event
    funct
        r
    }
    funct

  }
}
```

Figure 4.1.5: Deployment of Smart Contracts in Remix IDE

4.1.8 Smart Contracts Connection:

We connected the smart contract with our DApp by using our deployed contract address in remix IDE and web3.

On config.js in our react application:

import web3 from "./web3";

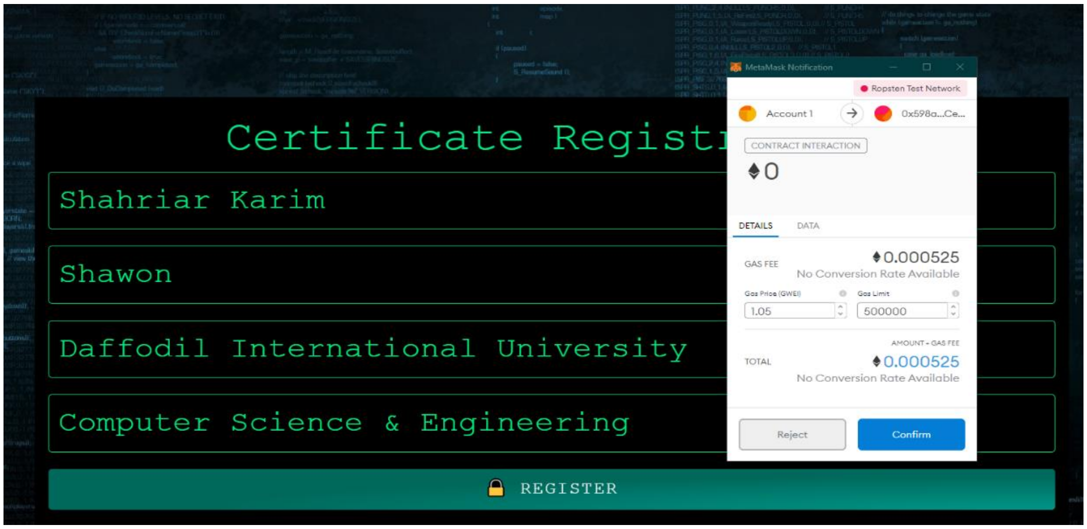
export const address = "0x598xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";

This address is the deployed smart contract address

Now our Decentralized application DIUcerts is fully ready for deployment.

4.1.9 Working procedure:

To create a certificate on our app, the issuer has to submit all information that is required on the form same as in figure 4.1.6. It will cost some ether as a gas fee for the miner to complete the transaction.



Certificate Registr

Shahriar Karim

Shawon

Daffodil International University

Computer Science & Engineering

MetaMask Notification

Ropsten Test Network

Account 1 → 0x598a...Ce...

CONTRACT INTERACTION

0

DETAILS DATA

GAS FEE 0.000525
No Conversion Rate Available

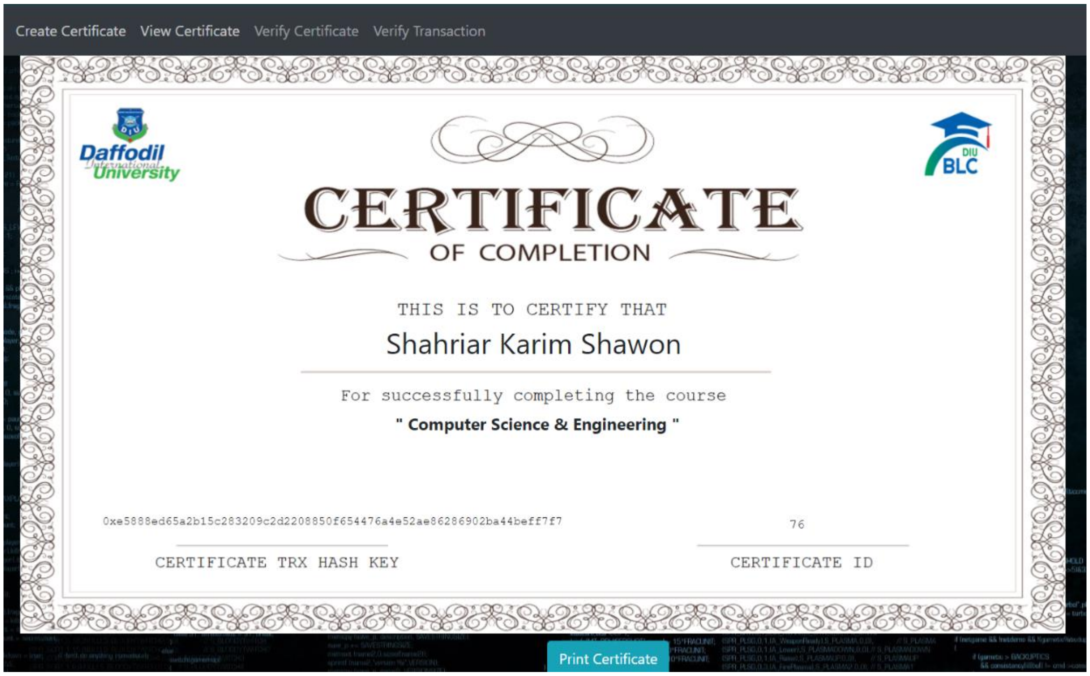
Gas Price (GWEI): 1.05

Gas Limit: 500000

AMOUNT + GAS FEE

TOTAL 0.000525
No Conversion Rate Available

Figure 4.1.6: Certificate Registration Procedure



CERTIFICATE

OF COMPLETION

THIS IS TO CERTIFY THAT

Shahriar Karim Shawon

For successfully completing the course

" Computer Science & Engineering "

0xe5888ed65a2b15c283209c2d2208850f654476a4e52ae86286902ba44beff7f7

CERTIFICATE TRX HASH KEY

76

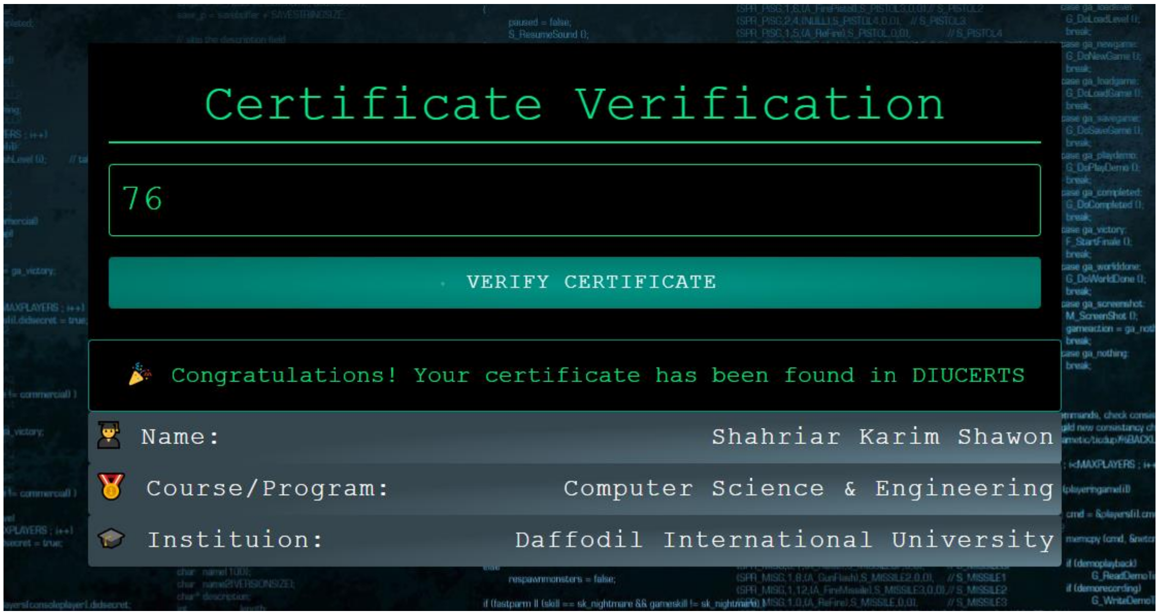
CERTIFICATE ID

Figure 4.1.7: DIUcerts Digital Certificate

On the view certificate page, the issuer can see the published certificate with Transaction Hash key and Certificate ID as shown in figure 4.1.7

Afterwards, the authority can send the digital certificate to the student with all the information.

Now, the verifier can verify the certificate with the certificate ID as shown in figure 4.1.8



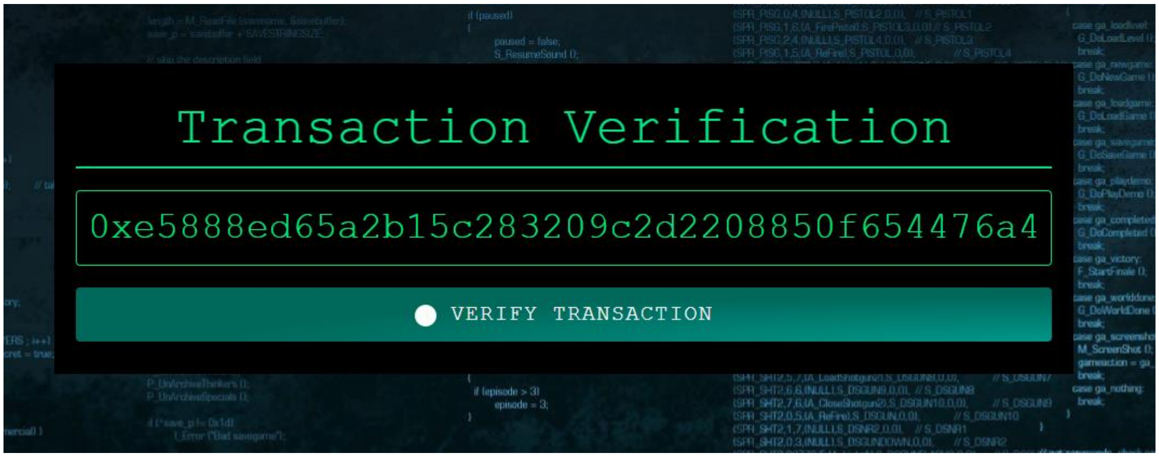
Certificate Verification

76

🎉 Congratulations! Your certificate has been found in DIUCERTS

Name:	Shahriar Karim Shawon
Course/Program:	Computer Science & Engineering
Instituion:	Daffodil International University

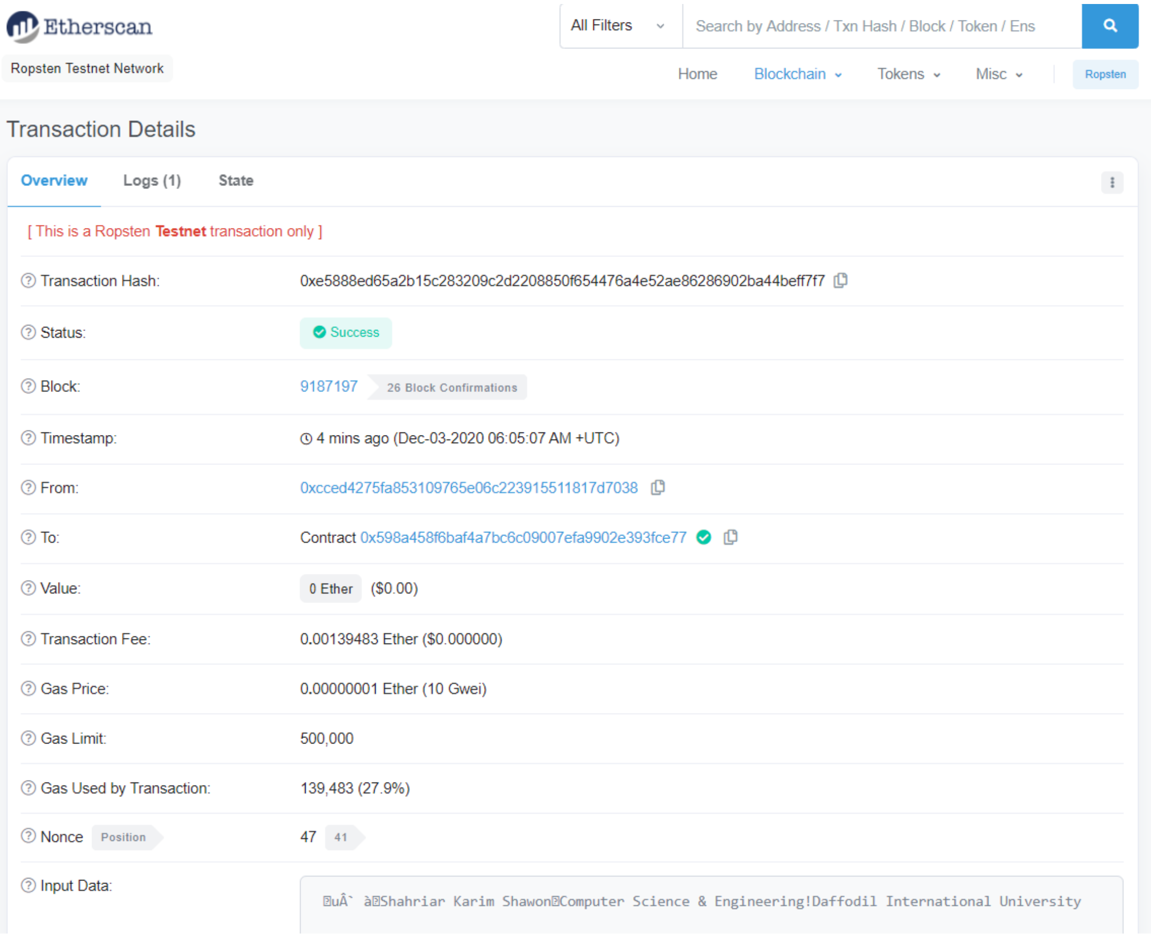
Figure 4.1.8: Certificate Verification Procedure



Transaction Verification

0xe5888ed65a2b15c283209c2d2208850f654476a4

Figure 4.1.9: Transaction Verification Procedure



Transaction Details

[This is a Ropsten **Testnet** transaction only]

Transaction Hash:	0xe5888ed65a2b15c283209c2d2208850f654476a4e52ae86286902ba44beff7f7
Status:	Success
Block:	9187197 26 Block Confirmations
Timestamp:	4 mins ago (Dec-03-2020 06:05:07 AM +UTC)
From:	0xcced4275fa853109765e06c223915511817d7038
To:	Contract 0x598a458f6baf4a7bc6c09007efa9902e393fce77
Value:	0 Ether ($0.00)
Transaction Fee:	0.00139483 Ether ($0.000000)
Gas Price:	0.00000001 Ether (10 Gwei)
Gas Limit:	500,000
Gas Used by Transaction:	139,483 (27.9%)
Nonce Position	47 41
Input Data:	uÂ` àShahriar Karim ShawonComputer Science & Engineering!Daffodil International University

Figure 4.1.10: Etherscan Transaction Details

If verifiers have any doubt about certificate ID, they also can verify the certificate transaction by submitting the transaction hash key same as in figure 4.9. After a few seconds, it redirects the requested transaction hash key to the Etherscan (Blockchain Public Ledger Transaction Explorer). In etherscan, verifiers can find all details about the requested transaction as shown in figure 4.1.10.

4.2 Performance Evaluation

Our proposed DIUcerts DApp was first tested on the Ethereum Ropsten Test Network, and then it was executed and evaluated on the. Ethereum Mainnet. The address of the smart contract of our DApp is the following:

"0x598xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

All transactions executed using the deployed smart contract which is publicly available on Etherscan. Etherscan allows anyone to explore the Ethereum blockchain for transactions, addresses, and other activities that are taking place. Besides, to interact with the deployed smart contract in ethereum, the ABI (application binary interface) is required. So, without the deployed smart contract address and ABI, no one can interact with this creation and verification process. For this reason, no fraud or scammer cannot interact with the application.

Tables 4 and 5 present the gas limit and gas price needed for the deployment of the smart contract, along with the transaction fees of each process. In the Ethereum network transaction processs, gas is a unit of cost for a specific function that needs to be executed in the smart contracts and the gas limit is the highest number of gas value a user is ready to spend on a transaction for faster performance, and the gas cost is the Gwei price per unit of gas. For each deployment, or function call, Ethereum asked for a particular volume of gas limit that is required for every transaction, which value depends on the smart contract requirements, and it can be adjusted. If a lower amount of gas limit is used, the contract deployment, or the function call, will be dropped sometimes, so it is advised to use the default gas limits or even increase them for better performance.

The value of the gas price is also adjustable depends on the contracts. This value influences the transaction execution time: the higher the gas price will be used, the quicker the deployment or function call will be verified on the ethereum Blockchain. As already mentioned, Table 4 presents the gas values used for contract deployment, and Table 5 outlines the gas values used for the registration of a certificate.

TABLE 4: ESTIMATED EXECUTION GAS FEE AND TRANSACTION FEE FOR SMART CONTRACT DEPLOYMENT PROCESS IN THE ETHEREUM PUBLIC LEDGER

	Gas Limit	Gas Price(Gwei)	Total Transaction Fee (Eth)	Total Transaction Fee ($)
Smart Contract Deployment	555154	1.05	0.000583	0.35$

TABLE 5: ESTIMATED EXECUTION GAS FEE AND THE TRANSACTION FEE FOR CERTIFICATE REGISTRATION

	Gas Limit	Gas Price(Gwei)	Total Transaction Fee (Eth)	Total Transaction Fee ($)
Certificate Registration	500,000	1.05 Gwei	0.000146	0.086$

Finally, our DIUcerts DApp costs only 0.35$ for the deployment of the smart contract and it is a one-time payment. Besides, the total cost for each certificate registration is only 0.086$ and it’s also a one-time payment. With the number of gas values adjusted this cost may become lower or higher.

CHAPTER 5

Conclusion and Future Work

5.1 Conclusion:

In our research work, a Blockchain-based Educational Certificate Verification decentralized application named DIUcerts was developed in the Ethereum Blockchain platform. The first objective of our research work was achieved by the progressive and effective implementation of our proposed model and also developed DApp. The proposed DApp was evaluated and tested on the Ethereum Ropsten Test Network which is the same as like Ethereum main network and the execution result of our project was introduced in this report. Based on our research work and deployed decentralized application, we may demonstrate that any expert or professional developer can utilize Blockchain technology for developing a secured, immutable and transparent application. We are also able to remove the middleman or any third party in the certificate verification process. One of our goal is to diminish the cost and time of the verification process. Surprisingly, we evaluate the cost of our decentralized app and it cost less than a dollar without any server maintenance cost. However, our main challenge is to eradicate fake educational certificates and our DApp almost met all the conditions to fight against this fraud and scam channel. In conclusion, from this work, we encourage that developers should be considered the ethereum Blockchain platform for developing decentralized applications on Blockchain and it will turn an interesting sector for the upcoming generation. We have also demonstrated the literature survey of Blockchain. Then, a conceivable combination of tools and technologies required to develop the decentralized applications with the Ethereum platform is shown. In the proposed smart contract example, step by step is explained, and also an application development environment is described. We have also represented a way that how web3, react.js, and ethereum can be a powerful combination to build a Decentralized Application.

5.2 Strengths and Limitations:

The Strengths offered by our DApp:

- DIUcerts change the process students receive their educational certificates. Students can easily access their digital certificates that are immutable, tamper-resistant, unaltered, and permanent through this platform.
- There is no need to get physical copies of educational certificates as this platform enables the way to share digital certificates directly to employers or universities.
- DIUcerts can entirely eliminate the need for universities or institutions to issue physical certificates.
- In a traditional platform, the authority has to pay a massive amount to deploy and maintain the server each year. But, through this platform, there is no need for investing to maintain the server.
- DIUcerts makes the way of verifying a certificate's legitimacy extremely simple. Employers can easily check the authenticity of the certificates of anyone.
- DIUcerts also save time spent on the entire verification process effectively.
- Our platform is web 3.0 enabled and in the front-end, we have used react.js that ensures super-fast performance with an interactive user interface.
- Our platform is user-friendly. Hence, without technical expertise, anyone can easily understand and use the system.

Though Blockchain technology creates hyped but still now there are not enough implementations of real-world application for understanding the concept properly. Blockchain-based applications are still in their babyhood as industries believe that Blockchain technology is hard to understand and implement and also troublesome for them to keep trust in new technology. Our research work also appears with few limitations but mentioned that they can be eventually eliminated once more and more progressive work is performed in this field and which makes Blockchain-based all solution systems start demonstrating to be a trustworthy, accurate, and reliable platform.

Limitations of our work are as follows:

- Lack of testing Security vulnerabilities
- Different templates for a different university instead of the same certificate template.
- Different smart contracts for different universities instead of using the same smart contract for all institutions.

5.3 Future scope

DIUcerts has introduced an innovative technique of Blockchain-based Educational Certificate Verification System, and therefore, it can be magnified, enhanced, and developed in various ways. The following are the most significant advancements and improvements that can increase the capability of the DIUcerts.

- A modified consensus algorithm may reduce the gas fee and transaction cost.
- Currently, DIUcerts uses different templates for different universities. In future, we will upgrade this platform entirely globally and provide the same template to all applicants
- The current version of DIUcerts has no access directly for the institution to use this application. In the future, An improved version will make it open for all where any institution will be able to get access to the platform through their blockchain address.
- In this work, we focused on the issuance and verification process only. Afterward, we will develop the rest functionalities such as testing security vulnerabilities, login-signup functionally with the JWT token.
- We will implement a QR code functionality instead of providing hash key and certificate ID to the recipients.

In the end, we further plan to extend our work and the DIUcerts platform to be an appropriate version of the Blockchain-based certificate issuance and verification technology where all limitations will be removed and provide a better solution for students, university authorities, or employers.

References

[1] G. Chen, B. Xu, M. Lu, and N.-S. Chen, “Exploring blockchain technology and its potential applications for education,” Smart Learn. Environ., vol. 5, no. 1, Jan. 2018, doi: 10.1186/s40561-017-0050-x.

[2] B. M. Nguyen, T.-C. Dao, and B.-L. Do, “Towards a blockchain-based certificate authentication system in Vietnam,” PeerJ Computer Science, vol. 6, p. e266, Mar. 2020, doi: 10.7717/peerj-cs.266.

[3] NonceBlox: Blockchain Your Assets, available at <<https://www.nonceblox.com/edublox.php>>, last accessed on 29-11-2020 at 6.00 PM.

[4] P. E. Gundgurti, K. Alluri, P. E. Gundgurti, S. Harika K. and G. Vaishnavi, "Smart and Secure Certificate Validation System through Blockchain," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 862-868, doi: 10.1109/ICIRCA48905.2020.9182975.

[5] G. Grolleau, T. Lakhal, and N. Mzoughi, “An Introduction to the Economics of Fake Degrees,” Journal of Economic Issues, vol. 42, no. 3, pp. 673–693, Sep. 2008, doi: 10.1080/00213624.2008.11507173.

[6] E. C. GARWE, “Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe,” JSE, vol. 5, no. 2, p. 119, Apr. 2015, doi: 10.5296/jse.v5i2.7456.

[7] E. Ben Cohen and R. Winch, “Diploma and accreditation mills: New trends in credential abuse,” 2011.

[8] Dinesh Kumar K,Senthil P, and Manoj Kumar D.S, “Educational Certificate Verification System Using Blockchain”, International Journal of Scientific & Technology Research, ISSN2277-8616,Vol.9, No. 3,pp.82-85, 2020

[9] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security Services Using Blockchains: A State of the Art Survey,” IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 858–880, 2019, doi: 10.1109/comst.2018.2863956.

[10] Chris Jaikaran,Blockchain: Background and Policy Issues, R45116 - Version: 3, Library of Congress. Congressional Research Service , February 28, 2018 , page no:2

[11] Panayiotis Christodoulou, Klitos Christodoulou and Andreas Andreou, “A decentralized application for logistics: Using blockchain in real-world applications”, Cyprus Review, 30, 181-193, Sep 2018

[12] Introduction to Decentralized apps, available at <<https://www.blockchain-council.org/blockchain/top-5-decentralized-apps-for-blockchain/>>, last accessed on 2-12-2020 at 4.00 PM.

[13] “BLOCKCHAIN BASED FRAMEWORK FOR EDUCATIONAL CERTIFICATES VERIFICATION,” jcr, vol. 7, no. 03, Jan. 2020, doi: 10.31838/jcr.07.03.13.

[14] Blockchain From Wikipedia, available at << https://en.wikipedia.org/wiki/Blockchain >>, last accessed on 2-12-2020 at 8.00 PM.

[15] Solidity, available at <<https://docs.soliditylang.org/en/v0.7.4/>>, last accessed on 1-12-2020 at 1.00 PM.

[16] Remix IDE, available at <<https://remix-ide.readthedocs.io/en/latest/>>, last accessed on 1-12-2020 at 1.30 PM.

[17] Metamask, available at <<https://metamask.io/index.html>>, last accessed on 1-12-2020 at 1.40 PM.

[18] Ropsten Test Network, available at <<https://ropsten.etherscan.io/>>, last accessed on 1-12-2020 at 2.00 PM.

[19] Web3.Js, available at <<https://web3js.readthedocs.io/en/v1.3.0/#web3-js-ethereum-javascript-api>>, last accessed on 1-12-2020 at 2.30 PM.

[20] Web3.Js, availableat<<https://appinventiv.com/blog/web-3-0-blockchain-impact-on-businesses/>>, last accessed on 1-12-2020 at 3.00 PM.

[21] Download Node JS, available at<<https://nodejs.org/en/>>, last accessed on 1-12-2020 at 7.00 PM.

[22] web3.js ,availableat<<https://web3js.readthedocs.io/en/v1.3.0/getting-started.html>>, last accessed on 1-12-2020 at 8.00 PM.

[23] Ropsten Ethereum Faucet, available at<<https://faucet.dimensions.network/>>, last accessed on 1-12-2020 at 10.00 PM.

[24] S. Rasool, A. Saleem, M. Iqbal, T. Dagiuklas, S. Mumtaz and Z. u. Qayyum, "Docschain: Blockchain-Based IoT Solution for Verification of Degree Documents," in IEEE Transactions on Computational Social Systems, vol. 7, no. 3, pp. 827-837, June 2020, doi: 10.1109/TCSS.2020.2973710.

[25] OpenCerts, available at<<https://www.opencerts.io/>>, last accessed on 7-12-2020 at 6.00 PM.