

**Preserve Integrity of Authentic Digital Islamic Assets Using Corda Blockchain**



**By**

**Hafiz Kamran Arshad**

**MSIS-21**

**(Registration No: 00000431931)**

**Supervisor**

**Dr Shahzaib Tahir**

**Department of Information Security**

**A research work (thesis) submitted in partial fulfillment of the requirements for the degree of  
Master of Science in Information Security (MSIS) -21**

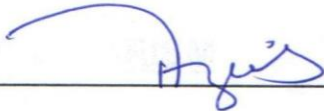
**In**

**Military College of Signals (MCS),**

**National University of Sciences and Technology (NUST), Islamabad, Pakistan.**


**THESIS ACCEPTANCE CERTIFICATE**

Certified that final copy of MS/MPhil thesis written by Mr/MS **Hafiz Kamran Arshad**, Registration No. **00000431931**, of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.


Signature: 

Name of Supervisor Dr. Shahzaib Tahir

Date: 23/8/24

Signature (HoD): 

Date: 23/8/24

Signature (Dean/Principal): 

Date: 27/8/24

**NATIONAL UNIVERSITY OF SCIENCES & TECHNOLOGY**  
**MASTER THESIS WORK**

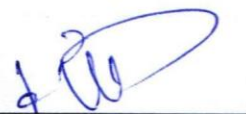
We hereby recommend that the dissertation prepared under our supervision by **Hafiz Kamran Arshad MSIS-21 Course** Regn No **00000431931** Titled: "**Preserve Integrity of Authentic Digital Islamic Assets Using Corda Blockchain**" be accepted in partial fulfillment of the requirements for the award of **MS Information Security** degree.

**Examination Committee Members**


1. Name : **Dr. Imran Makhdoom**

Signature: 

2. Name: **Maj Bilal Ahmed**

Signature: 


3. Name: **Maj Ammar Hassan**

Signature: 

Supervisor's Name: **Dr Shahzaib Tahir**

Signature: 

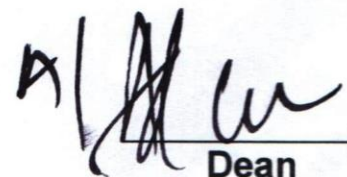
Date: 23/8/24

  
 Head of Department

23/8/24  
 Date

**COUNTERSIGNED**

Date: 29/8/24

  
 Dean

## CERTIFICATE OF APPROVAL

This is to certify that the research work presented in this thesis, entitled "Preserve Integrity of Authentic Digital Islamic Assets Using Corda Blockchain" was conducted by Hafiz Kamran Arshad under the supervision of Dr. Shahzaib Tahir No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Military College of Signals, National University of Science & Technology Information Security Department in partial fulfillment of the requirements for the degree of Master of Science in Field of Information Security Department of information security National University of Sciences and Technology, Islamabad.

**Student Name:** Hafiz Kamran Arshad

Signature: 

Examination Committee:


a) External Examiner 1: Name Dr. Imran Makhdoom. (MCS)

Signature: 

b) External Examiner 2: Name Maj Bilal Ahmed. (MCS)

Signature: 

c) External Examiner 3: Name Maj Ammar Hassan. (MCS)

Signature: 

Name of Supervisor: Dr. Shahzaib Tahir

Signature: 

Name of Dean/HOD. Dr Muhammad Faisal Amjad

Signature: 



## AUTHOR'S DECLARATION

I Hafiz Kamran Arshad hereby state that my MS thesis titled Preserve Integrity of Authentic Digital Islamic Assets Using Corda Blockchain is my own work and has not been submitted previously by me for taking any degree from National University of Sciences and Technology, Islamabad or anywhere else in the country/ world. At any time if my statement is found to be incorrect even after I graduate, the university has the right to withdraw my MS degree.

Student Signature: \_\_\_\_\_

Name: Hafiz Kamran Arshad

Date: \_\_\_\_\_

23/8/24

## **PLAGIARISM UNDERTAKING**

I solemnly declare that research work presented in the thesis titled **Preserve Integrity of Authentic Digital Islamic Assets Using Corda Blockchain** is solely my research work with no significant contribution from any other person. Small contribution/ help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero-tolerance policy of the HEC and National University of Sciences and Technology (NUST), Islamabad towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of MS degree, the University reserves the rights to withdraw/revoke my MS degree and that HEC and NUST, Islamabad has the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized thesis.

Student Signature: \_\_\_\_\_

Name: Hafiz Kamran Arshad

Date: 23/8/24

## **Dedication**

My research work (thesis) is dedicated to Allah Almighty, the source of all knowledge and wisdom, for His endless guidance and blessings throughout this journey. It is also an immense pleasure of mine to dedicate this work to my respected parents, teachers and beloved family, whose unwavering love and support have been the driving force behind my academic journey. I am grateful for inculcating in me the values of hard work, discipline and dedication. Your guidance and encouragement throughout the research tenure have been invaluable. That's why I am forever grateful for all the support you have done for me. This thesis is a testament to all that I have learned from you and a dedication to your unwavering support.

## **Acknowledgments**

I express my gratitude to all individuals who helped me in completing my research work. I am indebted to their help and invaluable guidance throughout the journey.

I further want to extend my deepest appreciation to my supervisor Professor Dr. Shahzaib Tahir for his exceptional guidance and mentorship during my research journey. Dr. Shahzaib Tahir has been a driving force behind our quest for knowledge, broadening my vision and challenging me to explore new horizons and pushing the boundaries of our understanding. I am extremely grateful for the mentorship of Professor Dr. Shahzaib Tahir, as he not only enriched my research skills but has also left an indelible mark on my academic pursuits.

Consequently, I would like to express my gratitude to the respected faculty of the NUST University for creating an intellectually stimulating academic environment. Their expertise, teachings skills, thought-provoking lectures, and engaging discussions have significantly expanded my knowledge and profoundly persuaded my perspective in latest technologies.



## Table of Contents

<b>List of Figures.....</b>	<b>10</b>
<b>List of Tables .....</b>	<b>11</b>
<b>1 INTRODUCTION .....</b>	<b>12</b>
1.1 Background.....	12
1.2 Level of Research Already Carried out on the Proposed Topic.....	12
1.3 Reason/ Justification for the Selection of the Topic.....	12
1.4 Objectives.....	12
1.5 Relevance to National and Army Needs.....	12
1.6 Advantages.....	12
1.7 Areas of Application .....	13
1.8 Inadequacies of Present Technologies and the Justification for Adoption of Blockchain	13
1.8.1 Inadequacies of Present Technologies .....	13
1.9 Motivation.....	14
1.10 Thesis Outline.....	15
<b>2 BLOCKCHAIN TECHNOLOGIES .....</b>	<b>16</b>
2.1 Blockchain Categories .....	17
2.1.1 Public Blockchain.....	17
2.1.2 Private Blockchain.....	17
2.1.3 Hybrid Blockchain.....	17
2.1.4 Consortium Blockchain.....	17
2.2 Public & Pseudo-anonymous Vs Private & Identified .....	18
2.3 Advantages.....	20
2.4 Disadvantages.....	20
2.5 Adoption of Blockchain .....	20
2.6 Architecture of blockchain .....	21
2.6.1 Traditional Blockchain Architecture.....	22
2.7 Different types of Blockchain Technologies .....	23
2.8 Comparison of Blockchain technologies .....	25
2.9 Consensus Algorithms .....	29

2.9.1	Proof of Work (PoW) .....	29
2.9.2	Proof of Stake (PoS).....	29
2.9.3	Delegated Proof-of-Stake (DPoS) .....	29
2.9.4	Proof of Elapsed Time (PoET).....	29
2.9.5	Practical Byzantine Fault Tolerance (PBFT) .....	30
2.9.6	Directed Acyclic Graph (DAG) .....	30
2.9.7	Smart Contracts .....	30
<b>3</b>	<b>LITERATURE REVIEW .....</b>	<b>31</b>
3.1	Digital Copyright and Integrity Protection Mechanisms .....	31
3.1.1	E-Book Copyright and Integrity Protection.....	31
3.1.2	Cross-Platform E-Book Development in the Era of Web 3.0.....	31
3.1.3	Challenges in E-Book Copyright Protection .....	31
3.1.4	Concealing Information in HTML Tags .....	32
3.1.5	Invisible Characters for Information Hiding .....	32
3.1.6	Blank Characters in English Sentences.....	32
3.1.7	Information Hiding in XML .....	32
3.1.8	Enhancing Data Integrity in Cloud Storage.....	32
3.1.9	Blockchain Technology in Cloud Storage Services.....	33
<b>4</b>	<b>CORDA - AN OVERVIEW WITH FRAMEWORK.....</b>	<b>35</b>
4.1	Introduction.....	35
4.2	Key Features of Corda .....	35
4.2.1	Ledger .....	35
4.2.2	States.....	36
4.2.3	Transactions .....	36
4.2.4	Smart Contracts .....	37
4.2.5	Flows.....	37
4.2.6	Consensus .....	38
4.2.7	Notaries .....	38
4.2.8	Vault.....	38
4.2.9	Nodes .....	39
4.3	Proposed Framework .....	39

4.4	Methodology .....	40
4.4.1	System Architecture.....	40
4.5	Appealing Remedies for Issues.....	40
4.6	Inadequacies of Present Technologies .....	40
4.6.1	Content Integrity for E-Books, eQuran, Hadees Shareef, and Fatwas: .....	40
4.6.2	Protection Against Sophisticated Attacks .....	40
4.6.3	Motivation for Blockchain Adoption.....	40
.....		42
4.6.4	Roles and Responsibilities .....	42
4.6.5	Network Structure:.....	42
4.6.6	Transaction Flow .....	44
<b>5</b>	<b>Implementation &amp; Results .....</b>	<b>45</b>
5.1	Implementation.....	45
•	Environment Setup .....	45
5.1.1	Comparative Analysis .....	45
5.1.2	Corda Setup .....	45
5.1.3	Steps for Implementation .....	45
5.2	Corda .....	49
5.2.1	Workflow .....	49
5.3	Implementation Flow .....	53
5.3.1	Client Endpoint Api.....	53
5.3.2	Transactions .....	53
5.3.3	Vault Query Command on Running Node Console.....	54
5.3.4	Gradle Commands: .....	54
5.4	Results .....	55
5.4.1	Comparison of Network Latency Between Corda and Ethereum .....	55
5.4.2	Corda Network Latency.....	55
5.4.3	Ethereum Network Latency .....	55
5.4.4	Observations.....	55
5.4.5	Detailed Comparison of Write Time Between Corda and Ethereum.....	56
5.4.6	Detailed Comparison of Read Time Between Corda and Ethereum.....	58

5.4.7	Detailed Comparison of Write Operation Duration Between Corda and Ethereum.....	59
5.4.8	Corda Local vs Remote Write and Read Comparison .....	61
5.4.9	Conclusion .....	61
<b>6</b>	<b>CONCLUSION AND FUTURE WORK.....</b>	<b>63</b>
6.1	Future Work .....	63
6.2	Acknowledgement.....	64
	References.....	65



## List of Figures

Figure 1 Basic architecture of Blockchain .....	22
Figure 2 architecture diagram .....	40
Figure 3 Flow Diagram.....	42
Figure 4 Transection Flow .....	43
Figure 5 Running Http Server.....	46
Figure 6 Deploy Smart contract using Remix IDE.....	46
Figure 7 Ganache Blockchain with Accounts.....	47
Figure 8 HTML Page (Portal) with JavaScript for Analysis .....	47
Figure 9 Transaction Flow .....	48
Figure 10 Ethereum Blockchain Write and Read Analysis .....	48
Figure 11 Ethereum Blockchain Write and Read Analysis .....	49
Figure 12 Directory Structure of Corda Project.....	49
Figure 13 Nodes in Running Condition .....	49
Figure 14 Corda Explorer Login Screen Connected with Our Nodes .....	50
Figure 15 Corda Blockchain Node Information .....	50
Figure 16 Geo Location of Nodes Shown on Map .....	51
Figure 17 Graphical Flow Execution .....	51
Figure 18 Output of Executed Flow.....	52
Figure 19 Vault State .....	52
Figure 20 Settings to run Corda Explorer .....	52
Figure 21 The Vault of Corda Editor Node .....	53
Figure 22 Network Latency Comparison Between Corda and Ethereum Network.....	55
Figure 23 Corda vs Ethereum 2408 Character Writing Comparison.....	56
Figure 24 Corda Vs Etereum Read Comparison.....	58
Figure 25 Corda Vs Ethereum Write Comparison.....	59
Figure 26 Corda Local and Remote Node Write Comparison.....	60
Figure 27 Corda Local and Remote Node Read Comparison.....	61

## List of Tables

Table 1 Area of Application.....	13
Table 2 Blockchain Categories .....	18
Table 3 Comparison Between Public & Private Blockchain Networks.....	18
Table 4 Comparison of Blockchain technologies .....	25
Table 5 Advantages and Disadvantages of Blockchain Technologies.....	27
Table 6 Literature Review Summary .....	33
Table 7 Security Analysis .....	61

## **ABSTRACT**

My research introduces a novel technique for ensuring the integrity of authentic digital Islamic data assets e.g. Quran Pak, Hadees Shareef, and Fatwa over the cyber space. My study explores various information hiding techniques and proposes the adoption of advanced blockchain technology, specifically Corda Blockchain, for the protection of data integrity. Through a thorough comparative analysis, my paper evaluates capabilities of Corda blockchain against Ethereum. Highlighting its advantages in delivering robust and efficient data integrity solutions. My approach aims to address existing gaps in digital asset protection by leveraging blockchain's secure and transparent framework. Which safeguard the integrity of authentic digital Islamic content.

**Keywords**—Islamic Data Integrity protection, Quran Pak, Hadees Shareef, Fatwa, blockchain, Corda

## 1 INTRODUCTION

### 1.1 Background

The internet has revolutionized our lives by integrating information technology into our daily routines. This influence permeates every aspect of our lives, from social interactions and sports to shopping and education. Consequently, an enormous volume of information is now stored and shared digitally. The advancement of internet services and the abundance of digital Islamic assets such as eQuran Pak, hadees shareef , fatwas, and other materials, underscore the urgent need for robust copyright and integrity protection of digital data [1].

The digital age has transformed how we consume and publish literature, making eBooks increasingly popular. However, the digital format also introduces challenges related to the integrity of eBooks, including piracy, unauthorized modifications, and disputes over authorship and royalties. Blockchain technology solves these problems by improvising a transparent and secure way to preserve eBook integrity. There is much research on data integrity, authentication, and copyright protection in the literature, however, there is a gap in the implementation of both in one scenario without performance compromise [2, 3, 4, 5].

### 1.2 Level of Research Already Carried out on the Proposed Topic.

There is much research on data integrity, authentication, and copyright protection in the literature, however, there is a gap in the implementation to achieve immutability without performance compromise.

### 1.3 Reason/ Justification for the Selection of the Topic.

The justification for selecting the topic arises from the identified gap in the implementation of data integrity and authentication protection without compromising performance. As I mentioned, there is much research on individual components but there is need of a practical solution with granular level access control to enhancing privacy, security, and compliance. This highlights the significance of exploring my topic.

### 1.4 Objectives.

The main objectives of thesis are:-

- To protect the integrity of Authentic Digital Islamic Assets through Corda Blockchain
- POC of Comprehensive solution with Corda Blockchain
- Performance analysis between Ethereum and Corda

### 1.5 Relevance to National and Army Needs.

The National and army needs are evident within the context of the digital age's impact and the challenges introduced by the digital format. In this era, where an enormous volume of digital content is stored and shared, robust integrity and authenticity protection of digital data is imperative. It is not limited to eBooks rather this solution can be applied to any digital assets stored and shared over the public and private cloud.

### 1.6 Advantages.

The solution based on Corda Blockchain will give granular level access control with numerous advantages, including enhanced security through fine-grained access permissions, improved data integrity



by preventing unauthorized modifications, and transparent transactions that foster accountability and trust. Overall, Corda's access control features provide a robust framework for securely managing sensitive data and assets, making it a valuable solution for addressing the complex challenges of digital data management in contexts of national security and military operations.

### 1.7 Areas of Application.

Corda blockchain may be implemented in public and private sector to maintain integrity of digital assets shown in table as proffered: -

**Table 1 Area of Application**

<b>Sector</b>	<b>Application</b>	<b>Description</b>
Public	Identity Management	Secure and verifiable application for digital identities of citizens and government officials.
	Voting Systems	Tamper-proof and transparent voting processes.
	Land Registry	Immutable and transparent records of property ownership and their transfers.
	Supply Chain Management	Enhanced tracking and transparency of goods and services in public procurement. Like Cement Supply Chain [24][38]
	Healthcare	Secure sharing of patient records and interoperability among healthcare providers.
Private Sector	Financial Services	Systematic and Secure processes for transactions, settlements, and auditing.
	Trade Finance	Reduced financial fraud and increased efficiency in trade operations.
	Insurance	Automated claims processing and risk management through smart contracts.
	Real Estate	Efficient property transactions with transparency in ownership management
	Supply Chain and Logistics	Enhanced visibility with traceability of transactions in whole supply chain.

## 1.8 Inadequacies of Present Technologies and the Justification for Adoption of Blockchain

### 1.8.1 Inadequacies of Present Technologies

1. In the era of digitization, everything is being generated, managed and spread over the internet. The widespread adoption of digital content e.g. e-books in general and eQuran, Hadees Shareef

and Fatwa specifically are hindered by the lack of robust mechanisms. To ensure integrity of the content, existing approaches for safeguarding digital assets, like those used for multimedia files, rely on modifying files or embedding hidden information in those files. However, these methods may not be suitable for all e-book formats, especially with the rise of Web 3.0 and cross-platform e-book development.

2. Past studies encompass different ways to hide information in hypertext files. These include changing HTML tags or using invisible special characters. These methods are beneficial by offering some protection, but they might not hold much data or stand up to smart attacks. The e-book world still faces big issues with copyright protection and keeping content intact. Current e-book formats like Amazon Kindle, Adobe PDF, and EPUB can fall victim to copyright theft and unwanted changes.
3. Researchers have suggested watermarking to protect e-book copyrights. But these fixes rely on a central body to check things, which hackers can target. Also, using HTML, XML, and JavaScript to make e-books work on many platforms brings new problems for checking and controlling content. The e-book world needs a full flexible answer to its copyright and integrity problems. Blockchain technology might help make e-books safer and more open. It uses a spread-out unchangeable record system that could solve many of these issues.

## 1.9 Motivation

The digital age has changed our lives. It brings information technology into our life's daily routines and creates a huge amount of digital data. This includes a lot of digital Islamic content such as the Holy Quran, Bukhari Shareef, and Fatwas. This highlights the pressing need to protect the authenticity and integrity of this content. Yet, keeping these assets safe has many challenges.

- **Digital Asset Management Issues:**

- Many people have a role in managing digital Islamic assets. These include religious scholar digital archivists, publishers, and IT service providers. Old-fashioned digital asset management systems might not tackle the current threats in real-time due to central in nature. This can lead to issues like changes made without permission, data leaks, and higher costs to run things.

- **Scalability:**

To manage and keep digital Islamic assets safe on a large scale involves many sources big data storage, and complex ways to check and validate the things. The amount of data and transactions that come from such a big system can be too much for centralized systems to handle. As the necessity of digital data increases day by day, the ability to grow becomes a big issue.

- **Lack of Transparency and Traceability:** Ineffective transparency and traceability for auditing purposes in the digital management process can make it difficult to identify the compromised source of errors or disruptions. This can result in delays, inefficiencies, and challenges in addressing and rectifying issues, particularly those concerning the authenticity and integrity of digital Islamic assets.

## 1.10 Thesis Outline

- **Chapter 1:** A brief introduction of the topic is given. The problem statement is highlighted followed by the motivation behind this research along with research objectives.
- **Chapter 2:** A thorough description of Blockchain, Its comparison between the similar technologies, pros and cons along with consensus Algorithms etc.
- **Chapter 3:** It gives a detailed Literature review of Integrity protection of digital assets including eBooks, pdfs and Islamic asset as Quran, Hadees, Fatwas and its challenges. Drawbacks and advantages are also highlighted.
- **Chapter 4:** Introduction and harnessing of Corda Blockchain technology which is used for the project and its features as well as a detailed framework with working methodology.
- **Chapter 5:** Implementation and analysis of proposed prototype of Corda blockchain with Ethereum blockchain.
- **Chapter 6:** Concluding the research work with mentioning dimensions of future work.

## 2 BLOCKCHAIN TECHNOLOGIES

Blockchain technology is considered as one of the glaring distribution ledgers over a network of computers that helps securely log transactions. It is decentralized sharing of resources [44]. Initially, Blockchain was headed as the primary technology emphasizing the cryptocurrency Bitcoin, but over past few years it has technologically advanced, and several uses were observed in a range of sectors.

The sequence of blocks is called blockchain, each of which encompasses a cluster of validated transactions (Tx). The logged data is ensured to be truthful and unalterable as these blocks are linked via cryptographic methods. An outline of the foremost bits and traits of blockchain technology is bestowed below:

- **Decentralization:** In contrast to conventional centralized systems that depend on a single authority, blockchain functions in a decentralized fashion. Amid plentiful network nodes (computers), blockchain diffuses the data transaction, inhibiting single point of failure and strengthening security of data.
- **Consensus Mechanism:** Consensus procedures are employed to authenticate the legitimacy of valid transactions and insert those into the ledger of a blockchain network. The mostly used consensus mechanism are as under and all have a distinct strategy for reaching consensus.:-
  - Proof of Work (PoW)
  - Proof of Stake (PoS)
  - Delegated Proof of Stake (DPoS)
- **Immutability:** When data is stored on blockchain, it is principally unchangeable. Since the consensus system is cryptographic, altering previous records in the block would imply changing successive blocks, which is computationally not possible. This reliability blocks tampering and guarantees integrity of data.[45-47]
- **Transparency:** Transactions made on a blockchain are visible to all network users. Since each participant has a manuscript of the entire ledger that's why blockchain is fully transparent and auditable.
- **Security:** Security is exceptional recognition to the cryptographic architecture of blockchain technology. To protect transactions, public private key cryptography is used, furthermore the decentralized structure of network reduces the prospect of hacking and illegal access.
- **Smart Contracts:** Self-executing programs known as "smart contracts" implement an agreement's terms automatically whilst certain criteria are persuaded. Due to this it is possible for automated, trustless transactions, which often cut off the need for middlemen.
- **Transparency:** By means of cutting-edge cryptographic methods several blockchains provide privacy measures that protect sensitive data. Zero-knowledge proofs and Private transactions are two main examples.
- **Interoperability:** It is progressively significant that numerous blockchain networks interrelate together as the blockchain ecosystem develops. In the direction of facilitation of smooth transfer of data and communication amongst numerous blockchains, solutions for interoperability are designed.



- **Scalability:** Traditional blockchains like Ethereum have emerging issues and can just process a limited number of transactions per unit time or (transactions per second, TPS).
- Researchers and developers are finding a way to use blockchain technology beyond finance and cryptocurrencies now a days. For greater transparency, productivity, and security in the processes, sectors like banking sector, logistics, healthcare, and identity management positively accepted blockchain. As technology progresses positively, it is expected that it will have a great impact on different areas of the digital world, and it will reshape the digital world.

## 2.1 Blockchain Categories

Blockchain serves as a communal and immutable ledger, streamlining the transaction recording and monitoring of assets within a business network. The technology's immutability confirms that once information is added to the blockchain, then it becomes resistant to alteration, enhancing the integrity and security of recorded data. Additionally, the owner of the assets cannot deny or manipulate transaction records, fostering transparency and trust within the network. This capability minimizes risks and lowers expenses for all participants in the network. Blockchain can be grouped into public, private, hybrid and consortium, where each have its own usability and pros and cons:

### 2.1.1 Public Blockchain:

Public blockchain is a decentralized network open to anyone, where participants can join, justify transactions, and contribute to the consensus process[39]. Examples include layer 1 Bitcoin (base layer) and layer 2 Ethereum (has more capabilities compared to Bitcoin) that provide transparency and security through a distributed ledger. Advantages include decentralization, transparency, and censorship resistance. Conversely, they might suffer issues like scalability and low transaction speed, due to the public and its computationally complex consensus mechanisms.

### 2.1.2 Private Blockchain:

As the name specifies, it is restricted to a specific group or organization giving them control over access and permissions [40]. Some businesses that wanted to use blockchain tech in a closed system often choose these blockchains, like Hyperledger Fabric. Private blockchains offer better privacy, boost productivity, and speed up transactions. Yet, they give up decentralization and might fail at a single point if not set up right.

### 2.1.3 Hybrid Blockchain:

As the name hints hybrid blockchains mix parts of public and private blockchains. This allows users to tailor privacy and openness. They let some data stay private while still getting the safety and spread-out nature of a public blockchain. This setup works well for apps that need to balance openness with secrecy. The good points include adaptability, room to grow, and more privacy. But they can get complex and need careful handling.

### 2.1.4 Consortium Blockchain:

A group of organizations working together on a blockchain network forms a consortium blockchain. These organizations share control over how the network will run[41-42]. The goal of these blockchains is to find a middle ground between being spread out and having control among a small number of trusted groups. Consortium blockchains, like R3 Corda, are well-suited for industries where collaboration is essential but complete decentralization is not feasible. Advantages include increased efficiency,

collaboration, and shared control. Nevertheless, they face challenges in terms of trust among consortium members and may still be vulnerable to collusion.

**Table 2 Blockchain Categories**

Aspect	Public	Private	Hybrid	Consortium
Pros	Decentralization, transparency, security	Enhanced privacy, efficiency, control	Flexibility, scalability, improved privacy	Increased efficiency, collaboration, shared control
Cons	Scalability issues, slower transactions	Sacrifices decentralization, potential single point of failure	Complexity, management challenges	Trust issues, vulnerability to collusion
Usage	Cryptocurrencies, open applications, Document validation	Enterprise solutions, internal processes, Asset Ownership	Customized applications, supply chain, Medical Records, Real Estate	Banking, Industry collaborations, shared processes

## 2.2 Public & Pseudo-anonymous Vs Private & Identified

Comparison between public and pseudo-anonymous blockchain networks (Bitcoin and Ethereum) and private and identified blockchain networks (Corda, Quorum, and Hyperledger):

**Table 3 Comparison Between Public & Private Blockchain Networks**

Feature	Public & Pseudo-Anonymous (Bitcoin/Ethereum)	Private & Identified (Corda/Quorum/Hyperledger)
Participant Identity	Pseudo-anonymous addresses (alphanumeric)	Real-world, identified participants
Access Control	Open to anyone; permissionless	Restricted membership; permissioned
Membership Approval	No approval process; decentralized	KYC process; centralized approval
Transaction Anonymity	High level of anonymity	Identity tied to transactions
Transaction Transparency	Fully transparent on the public ledger	Transparent within the approved network
Immutability	Immutable transactions on the	Immutable within the approved network

	public ledger	
Fraud Risk	Potential for man-in-the-middle attacks	Mitigated through KYC and identity verification
Transaction Validation	Decentralized consensus mechanisms	Centralized consensus mechanisms (vary by platform)
Flexibility and Customization	Limited due to decentralized nature	More control and customization options
Use Cases	Decentralized applications, open finance	Business applications, supply chain, finance
Privacy	Limited privacy features	Enhanced privacy controls and confidentiality
Scalability	Faces challenges due to global consensus	Potentially higher scalability within a closed network
Consensus Mechanisms	Proof-of-work (Bitcoin), proof-of-stake (Ethereum)	PBFT, Raft, or other tailored mechanisms
Smart Contracts	Limited functionality and security considerations	More complex and feature-rich due to known participants
Regulatory Compliance	Challenging due to pseudo-anonymous nature	Easier adherence with identified participants
Cost of Transactions	Variable and influenced by network congestion	More predictable and controlled transaction costs
Governance	Decentralized decision-making through consensus	Potentially more centralized governance structure
Network Security	Relies on cryptographic algorithms and network size	Can benefit from tailored security measures due to closed nature

Choice between public and private blockchain networks depends on the specific use case, requirements, and trust model. Public networks offer openness and decentralization, while private networks provide controlled access, identity verification, and enhanced privacy features. For this research we will focus on private network implementation as it offers more control over the copyright protection of assets involved.

Blockchain evolution can be classified in three different stages as under [26]:

- Blockchain layer 1 can be described as a digital currency system, which is exemplified by Bitcoin. Excluding Bitcoin cryptocurrency, there are beyond 1000 distinct types of cryptocurrencies that have been founded which are still increasing.

- Blockchain layer 2 focuses on the financial sector and the advent of smart contracts is the symbol of this generation. With smart contracts, the other forms of assets can be converted and related together that grow the applications of blockchain.
- Blockchain layer 3 is configurable through programming, which means blockchain can be operated by government, medicine, culture, research and environment based on internet technologies.

### 2.3 Advantages

Cryptocurrencies have six main advantages. No need of central body for financial transactions to complete as it can legalise transactions all by themselves. It gives benefits for the regions and countries of reducing bank transactions cost, like El Salvador became the first country to adopt Bitcoin as a legal tender as the remittances make up 23% of its GDP and only 30% citizens own individual bank account [23]. Cryptocurrency is an international currency which can be operated. Cryptocurrencies are nationally and internationally available to operate and do not belong to any specific country or organization. Compared with traditional payments methods, not only payments can be processed and settled faster, but there is no need to physically go by the individuals to financial institutions. Moreover, no matter what kind of deal is going to be happen or what the amount of capital is. Additionally, cryptocurrencies have high security with the help of cryptographic technologies that make duplication or counterfeit cryptocurrencies impossible. Cryptocurrencies have built-in feature which is inflation protection. Inflation is always a significant problem in traditional payment methods. Cryptocurrencies are distributed with standard circulation supplies which make cryptocurrencies immune to inflation. The last but not the least advantage of cryptocurrency is transparency. The cryptocurrencies are based on blockchain to operate, which saves data on multiple computers and all users in a network have a key that provides transparency and security.

### 2.4 Disadvantages

Cryptocurrencies have three main disadvantages. The main is lack of supervision. Blockchain with cryptographic technology is complex that requires technical knowledge for the individuals to make it usable. Which might increase the difficulty for the public private sector to supervise. The transactions between cryptocurrencies are irreversible. Once the transactions are finalized, there's no refund or cancellation which is designed as such to prohibit cheating others' money. Illegal activities may occur if cryptocurrencies are employed. Since the user's information cannot be tracked down by the government due to encryption, cryptocurrencies can also generate a dark web or black market to do illegal activities. [25]

### 2.5 Adoption of Blockchain

1. In contrast to centralized systems, blockchain provides a tamper-proof record of transactions and content, ensuring the authenticity and integrity of e-books. The decentralized nature of blockchain eliminates single points of failure, making it resistant to hacking and unauthorized modifications. Smart contracts, embedded within the blockchain, can automate copyright



- management and royalty distribution, providing a transparent and efficient mechanism for authors and publishers.
2. By leveraging blockchain technology, the e-book industry can establish a secure and trustworthy environment for content creation, distribution, and consumption. . This will protect the rights of authors and publishers while making the reading experience better for its users. While modern technologies used like watermarking and encoding methods protect integrity and have helped over the years, they have some downsides and limits that might reduce productivity, effectiveness, and openness.
  3. In the same way methods used currently in order to preserve the digital Islamic assets depend on centralized systems and old technologies. These methods don't do a good job of keeping these valued resources secure and protected. Centralized systems have a flaw: they can fail at one point. This makes them an easy target for hackers who want to steal data or modify it without permission. Old technologies often made before the digital age might not be strong or safe enough to protect against new threats to digital data. These problems make it hard to keep digital Islamic assets safe. For example, the Holy Quran, Hadith collections, and scholarly opinions (Fatwas) could easily be changed, tapered, misunderstood, or even removed when stored in weak centralized databases. The lack of transparency in old traditional systems makes this problem worse. It's hard to see or trace the history of changes being made and to authenticate whether these digital assets are even real or not.
  4. In these modern times, the need for a safer, clearer, and more authentic system where one could easily access authentic resources has become very obvious and important. Blockchain technology gives a hopeful answer to fix these weak spots. Its spread-out record system and code-based safety can boost the trustworthiness and realness of digital Islamic assets a lot thus providing an authentic and genuine resource pool . Blockchain's spread-out nature gets rid of single weak points making it hard to hack or leak data. The unchangeable record makes sure that any data changes are always noted and clear to see so it's impossible to mess with the content without getting caught. Also, the code-based safety steps in blockchain guard against unwanted access and changes, which further boosts the trustworthiness of the stored data.
  5. Therefore, the adoption of blockchain technology for preserving digital Islamic assets is not merely a technological upgrade but a necessary step to ensure the accuracy, sanctity, and long-term preservation of these invaluable resources for future generations.
  6. This blockchain technology, therefore, is not just a simple upgrade in technology but a necessity to preserve these valuable and important assets for our future generations. Blockchain technology offers a promising solution to these problems of digital tampering. It improves how digital Islamic assets are handled in a few keyways.

## 2.6 Architecture of blockchain

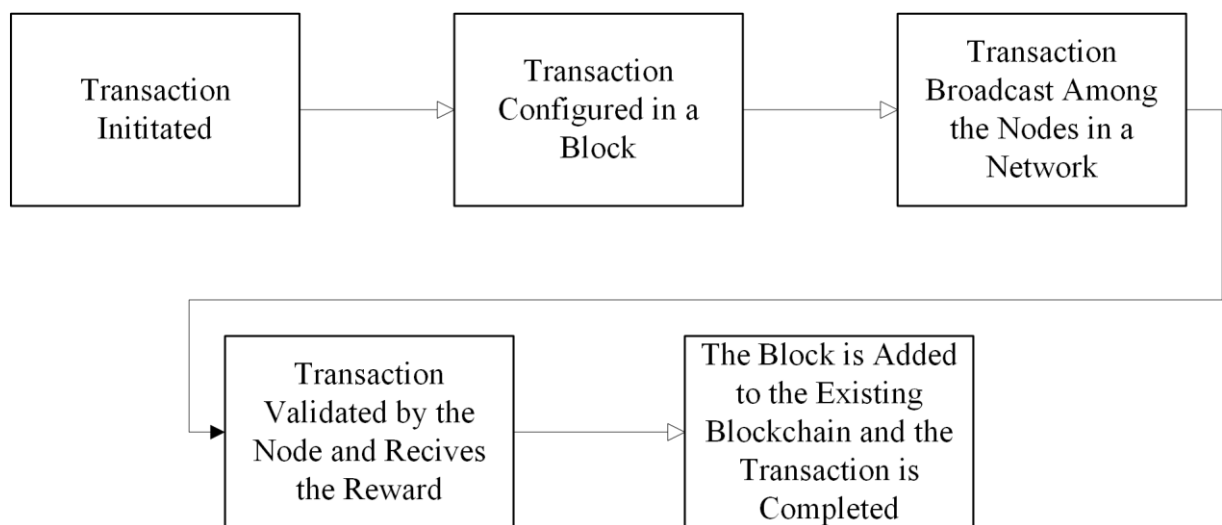
By referring to figure 1 which explains the basic flow of blockchain, the architecture of this blockchain can be easily understood.

- The data-source module is used in "distributed and shared databases" to help build the blockchain [43]. Blockchain guarantees that the data which users retrieve is accurate and undamaged. The main traits of blockchain are tamper-proofed storage with any form, data

immutability, and shareable data ledger through the "Application Programming Interface (API)".

- The "journey of a transaction in blockchain" is auditable, managed, enabled, and supported by the transaction module. It facilitates inclusion to the blockchain and helps authenticate transactions. Data transport occurs through and after the validation of smart contracts.
- The blockchain is used to create information flow across the Smart Contract (SC) as well as shared visibility of transactions. A block of transactions is bundled together and sent to all nodes. Be aware that after a transaction has been sent to the blockchain, it is very hard to redo or reverse it.
- Module for creating blocks: Blocks can be seen as the miners' own data structures. They contain data and transaction details that are copied to all network nodes. By giving the hash values and connections of the preceding block, the block creation module facilitates the insertion of additional blocks to an already-existing SC. "Chronological blocks" are used to hold transaction sequences, and they make it simple to identify and trace blocks that contain incorrect transactions. Almost no data on the blockchain can be changed because of the architecture.

*Figure 1 Basic architecture of Blockchain*



### 2.6.1 Traditional Blockchain Architecture

- **Blocks**
  - **Data Structure:** Each block contains a list of transactions.
  - **Header:** Each block has a header containing metadata such as the previous block's hash, timestamp, and nonce.
- **Chain**
  - **Linking Blocks:** Blocks are chained together in a chronological order, forming a chain.

Each block references the hash of the previous block.

- **Immutability:** Once a block is added, it cannot be changed without altering all subsequent blocks.
- **Nodes**
  - **Participants:** Computers participating in the blockchain network.
  - **Full Nodes:** Store a complete copy of the blockchain.
  - **Light Nodes:** Store only a subset of the blockchain.
- **Transactions**
  - **Transfer of Value:** Transactions represent the transfer of value (e.g., cryptocurrency) between participants.
  - **Validation:** Nodes validate transactions before including them in a block.
- **Consensus Mechanisms**
  - **Proof of Work (PoW):** To add a new block miners solve computational puzzles.
  - **Proof of Stake (PoS):** Validators are selected based on the quantity of coins they hold and are willing to "stake."
  - **Other Mechanisms:** Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), etc.
- **Cryptography**
  - **Hash Functions:** Used to make unique identifiers for blocks and transactions.
  - **Public-Key Cryptography:** Ensures secure transactions between users.
- **Smart Contracts**
  - **Automated Agreements:** Self-executing contracts with the terms of the agreement directly written into code.
  - **Decentralized Applications (DApps):** Applications that run on the blockchain using smart contracts.
- **Decentralization**
  - **Distributed Network:** No single point of control; all nodes have equal power.
  - **Fault Tolerance:** The network can continue to operate even if some nodes fail.

## 2.7 Different types of Blockchain Technologies

- **Ethereum**

Distributed platforms like Ethereum (ETH) allow the creation and deployment of programs i.e., smart contracts and decentralized applications (dApps). It promoted the idea of configurable and programmable blockchain, which lead programmers to build unique tokens and meet the solutions for challenging tasks on the blockchain.

- **Bitcoin**

Bitcoin is the first and most well-known cryptocurrency application of Ethereum blockchain. Who can perform without any middlemen like banks, it functions as a peer-to-peer (P2P) digital cash system, allowing secure and borderless transactions.

- **Hyperledger Fabric**

The Hyperledger project of the Linux Foundation has created Hyperledger Fabric, an enterprise-grade blockchain platform. With increased privacy and scalability, it focuses on building private, permissioned blockchain networks for corporate applications.

- **Ripple (XRP)**

Ripple (XRP) is a blockchain technology envisioned for fast and budget friendly cross-border transactions. Which is made for targeting the international remittances and financial sector, and it guarantees to make swift and inexpensive money transfers everywhere.

- **Stellar (XLM)**

Blockchain platform Stellar was created mainly for rapid and reasonable international trade and issuance of assets. It aims to make financial institutions and make money and remittances transfer in quick manners.

- **Cardano (ADA)**

It's a blockchain platform belongs to the 3rd generation and created to solve the sustainability, scalability, and issues like interoperability that were present in prior blockchains. It provides decentralized applications (dApps) and smart contracts a more firm and scalable foundation.

- **PolkaDot (Dot)**

A multi-chain blockchain technology offers interoperability between different blockchains is called Polkadot (DOT). It expands the ecosystem usefulness and scalability by permitting connections between different blockchain networks, sharing of information and asset transfers.

- **Tezos (XTZ)**

Tezos is a self-configurable blockchain platform, which allows stakeholders to revise and modify the protocol without the need for hard forks. It attempts to strengthening network consensus to develop over time.

- **VeChain (VET)**

A blockchain network which focuses on the supply chain management with product's authenticity confirmation. It allows a tamper-proof record and visibility of product information in the network with traceability and its legitimacy.

- **IOTA (MIOTA)**

A Blockchain platform IOTA (MIOTA) was specially designed for the Internet of Things (IoT) environment. It operates on a novel Tangle-like structure, contrary to conventional blockchain, with ability to provide an ecosystem which is cost effective, scalable for IoT devices to share data.

- **EOS (EOS)**

EOS is designed for efficient transactions processing and scalability. It is intended for the large scale dApps because it uses a consensus protocol; delegated proof-of-stake (DPoS) to provide high

throughput and low latency.

- **Corda**

An open source blockchain technology created especially for business use cases and financial institutions in mind is called Corda. It is developed by the R3 organization, which provides scalability, interoperability with strong emphasis on privacy. It is efficient and provides high throughput through its distinct Notary method. It enables peer-to-peer transactions while preserving sensitivity of data with sharing transactions only with involving parties. For financial organizations or other corporate procedures which require high throughput with security and anonymity, Corda is the best choice.

## 2.8 Comparison of Blockchain technologies

*Table 4 Comparison of Blockchain technologies*

Technology	Consensus Mechanism	Scalability	Smart Contracts	Interoperability	Privacy	Use Cases and Features
Ethereum (ETH)	Proof of Work (PoW)	Moderate	Yes	Limited	Limited	programmable blockchain, decentralized apps (dApps), and token production
Bitcoin (BTC)	Proof of Work (PoW)	Limited	No	Limited	Limited	Peer-to-peer exchanges and digital currencies
Hyperledger Fabric	Pluggable Consensus	High	Yes	Yes	Yes	solutions for business blockchain, private networks, and permissioned networks
Ripple (XRP)	Ripple Protocol Consensus	High	No	Limited	Yes	Financial sector, remittances, and international payments
Stellar (XLM)	Stellar Consensus Protocol	High	No	Limited	Limited	Transacting internationally and issuing assets

Technology	Consensus Mechanism	Scalability	Smart Contracts	Interoperability	Privacy	Use Cases and Features
Cardano (ADA)	Ouroboros Proof of Stake	High	Yes	Limited	Yes	Smart contracts, scalability, sustainability
Polkadot (DOT)	Nominated Proof of Stake	High	Yes	Yes	Yes	Blockchain interoperability and chain-to-chain communication
Tezos (XTZ)	Liquid Proof-of-Stake (LPoS)	Moderate, with ongoing improvements via protocol upgrades	Yes	Potential, adaptable through protocol upgrades	Potential, adaptable through protocol upgrades	On-chain governance, formal verification of smart contracts, staking and baking, DeFi and dApps, token issuance, sustainability
VeChain (VET)	Proof of Authority (PoA)	High	No	Limited	Yes	Verification of product authenticity and supply chain management
IOTA (MIOTA)	The Tangle	High	No	Yes	Yes	Data and value transfer via the Internet of Things (IoT), including cost-free transactions
EOS (EOS)	Delegated Proof-of-Stake (DPoS)	High, designed for large-scale dApps	Yes	Limited, focused on scalability within the EOS ecosystem	Limited, not a primary focus	High throughput and low latency transactions, large-scale dApps, decentralized application development

Technology	Consensus Mechanism	Scalability	Smart Contracts	Interoperability	Privacy	Use Cases and Features
Corda	Pluggable Consensus	High	Yes	Limited	Yes	Enterprise blockchain for privacy-focused applications, supply chain management, and complex financial arrangements

*Table 5 Advantages and Disadvantages of Blockchain Technologies*

Technology	Advantages	Disadvantages
Ethereum (ETH)	- A sizable, decentralized apps (dApps) developer community.	- Problems with scalability caused by expensive transaction costs and extended processing times.
	- A blockchain that can be programmed to support smart contracts and unique tokens.	- Proof of Work (PoW) consensus mechanism.
Bitcoin (BTC)	- Created the first decentralized payment system and digital money.	- Limited scalability which leads to higher transaction fees and slower confirmation times.
	- A peer to peer ledger that is transparent and secure.	- Proof of Work (PoW) consensus mechanism.
Ripple (XRP)	- Cross-border transactions that are quick and affordable, boosting remittances.	- Centralized validators raise concerns about decentralization.
	- Aimed at financial organizations for efficient international money transfers.	- Relies on a unique consensus protocol, not fully permissionless

<b>Technology</b>	<b>Advantages</b>	<b>Disadvantages</b>
Hyperledger Fabric	<ul style="list-style-type: none"> <li>- Appropriate for business apps with a privacy-focused design.</li> </ul>	<ul style="list-style-type: none"> <li>- For maintaining the network, it Requires a consortium or membership</li> </ul>
	<ul style="list-style-type: none"> <li>- Modular architecture that is adaptable to individual company requirements.</li> </ul>	<ul style="list-style-type: none"> <li>- Higher complexity in implementation.</li> </ul>
Cardano (ADA)	<ul style="list-style-type: none"> <li>- Blockchain protocol that has undergone peer review and scientific investigation.</li> </ul>	<ul style="list-style-type: none"> <li>- Slower development due to a rigorous peer-review process.</li> </ul>
	<ul style="list-style-type: none"> <li>- Put an emphasis on scalability, governance on-chain, and sustainability.</li> </ul>	<ul style="list-style-type: none"> <li>- Limited number of developed dApps</li> </ul>
Stellar (XLM)	<ul style="list-style-type: none"> <li>- Created for international trade and asset issuance.</li> </ul>	<ul style="list-style-type: none"> <li>- Limited smart contract capabilities</li> </ul>
	<ul style="list-style-type: none"> <li>- Integration with the current financial infrastructure has been made simpler.</li> </ul>	<ul style="list-style-type: none"> <li>- Relatively lower adoption</li> </ul>
Polkadot (DOT)	<ul style="list-style-type: none"> <li>- Promotes communication between various blockchains.</li> </ul>	<ul style="list-style-type: none"> <li>- Complex architecture</li> </ul>
	<ul style="list-style-type: none"> <li>- Allows autonomous blockchains to safely link and exchange data.</li> </ul>	<ul style="list-style-type: none"> <li>- Immature ecosystem with fewer active dApps and users.</li> </ul>
VeChain (VET)	<ul style="list-style-type: none"> <li>- Improves supply chain management and the assurance of product authenticity.</li> </ul>	<ul style="list-style-type: none"> <li>- Mainly focused on supply chain use cases</li> </ul>
	<ul style="list-style-type: none"> <li>- Assures immutability and transparency for certified product data.</li> </ul>	<ul style="list-style-type: none"> <li>- Limited adoption and awareness outside of specific industries.</li> </ul>
IOTA (MIOTA)	<ul style="list-style-type: none"> <li>- A lightweight architecture appropriate for IoT devices and fee-free transactions.</li> </ul>	<ul style="list-style-type: none"> <li>- Vulnerabilities in the Tangle structure</li> </ul>
	<ul style="list-style-type: none"> <li>- Fast and scalable data and value transfers are made possible by The Tangle.</li> </ul>	<ul style="list-style-type: none"> <li>- Security issues and development challenges.</li> </ul>
Corda	<ul style="list-style-type: none"> <li>- Designed for supply chain management and complicated financial agreements.</li> </ul>	<ul style="list-style-type: none"> <li>- Limited adoption and recognition compared to major public blockchains.</li> </ul>



Technology	Advantages	Disadvantages
	<ul style="list-style-type: none"> <li>- Privacy-focused, only sharing information through notaries with parties who need it.</li> </ul>	<ul style="list-style-type: none"> <li>- Specific use case focus may limit broader adoption.</li> </ul>

## 2.9 Consensus Algorithms

Consensus protocol is primarily a set of rules that every single participant in the network must follow. Since blockchain is a decentralized system lacking a central authority, a distributed consensus method is required for all contributors to agree on its existing state. Due to limited resources, having more control over these resources leads to more influence over the blockchain's operations. Many types of consensus mechanisms have been developed for blockchains, including Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed Time (PoET) , Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), Directed Acyclic Graph (DAG) , Tendermint, Ripple, Scalable Byzantine Consensus Protocol (SCP), and Proof of Burn, tailored to meet specific needs.

### 2.9.1 Proof of Work (PoW)

Proof of Work involves solving a problem that can only be approached through guesswork. For instance, when generating and validating a complete block, the task is to find a nonce value so that the difficulty level matches the output of a hash function that uses the transaction data and the nonce value as inputs. Each node in the network guesses random nonce values until one eventually finds the correct one that meets the difficulty requirement. To successfully create a block, link it to the blockchain, and earn a mining reward (which is financial), a mining node must invest significant computational power and solve the problem faster than others.

### 2.9.2 Proof of Stake (PoS)

Proof of Stake, the second most common consensus method, requires less computational effort as compared to PoW. The consensus protocol PoS addresses the energy and time consumption issues of PoW, where finding a nonce requires electricity and time. In a PoS network, nodes must stake some funds to be eligible as the next block creator. The chosen block creator will receive the transaction fees associated with that block. If a block winner tries to add an invalid block, they will lose their stake. The transition from PoW to PoS is part of the Ethereum 2.0 upgrade.

### 2.9.3 Delegated Proof-of-Stake (DPoS)

In DPoS, each token holder can vote for delegates and assign voting authority to others. The voting power is relative to the number of tokens held. The elected delegates are responsible for validating transactions and blocks to secure the network. Unlike PoW and PoS, which reward miners with the most computational power or tokens, DPoS allows token holders to vote on who should mine new blocks and reward only the best performers. EOS is one blockchain system that uses the DPoS algorithm.

### 2.9.4 Proof of Elapsed Time (PoET)

Proof of Elapsed Time, developed by the Corporation of Intel, offers an alternative method for selecting a block miner. Each potential validation node in PoET requests a randomly generated waiting time from a trusted computing platform, such as Intel's SGX. The first node to end the waiting time wins the

validation and can add the new block. This system ensures that every node has a fair chance to win due to the trusted computing platform.

#### **2.9.5 Practical Byzantine Fault Tolerance (PBFT)**

Byzantine Fault Tolerance (BFT) aims to achieve consensus while addressing the issue of some participants being dishonest. PBFT optimizes BFT by ensuring that if the number of malicious nodes is less than one-third of all nodes, the blockchain system will reach consensus on its current state. The security of the blockchain system increases with the number of nodes. Hyperledger Fabric uses PBFT.

#### **2.9.6 Directed Acyclic Graph (DAG)**

Unlike traditional consensus mechanisms, Directed Acyclic Graphs (DAGs) consist of edges (paths connecting them) and vertices. The edges and vertices do not loop back on themselves and are directed in one direction. Each vertex denotes a transaction, and there are no blocks; transactions are added individually. A small PoW operation is performed when a node submits a transaction, confirming the validity of previous transactions and preventing network spam. IOTA uses the DAG consensus algorithm.

#### **2.9.7 Smart Contracts**

A notable feature of blockchain technology is the ability to write objective computer code that defines how processes will be managed and what actions will be taken when certain events occur. Smart contracts, introduced by Ethereum, break the limitations of Bitcoin. These contracts are designed to respond to specific events and do not necessarily need to be legally binding or involve more than two parties. Often called chain code, smart contracts integrate rules and decision-making into blockchain processes and transactions:

- Ensure automated transactions that adhere to the same regulations.
- Utilize blockchain technology.

Smart contracts form the foundation for enterprise blockchain applications and are set to transform business operations. They can be created without intermediaries, offering autonomy, effectiveness, efficiency, and cost savings.

## Chapter 3

### 3 LITERATURE REVIEW

#### 3.1 Digital Copyright and Integrity Protection Mechanisms

##### 3.1.1 E-Book Copyright and Integrity Protection

In the digital age, the dissemination of e-books is hampered by the absence of a definitive copyright and integrity protection mechanism. As a result, ensuring the copyright protection of e-book sales and rentals is of paramount importance. Current e-book format might be broadly categorized into six types: Kindle of Amazon, Microsoft Reader, Adobe PDF, EPUB, Mobi Pocket, and Palm doc.

##### 3.1.2 Cross-Platform E-Book Development in the Era of Web 3.0

The development of Web 3.0 has ushered in a new era of cross-platform e-book development, transforming the way people read and learn. Multimedia files, including images, videos, and audio, are inherently easier to protect due to their sensitivity to human perception and their file formats. The primary method for concealing digital watermark information involves altering multimedia files or modifying coefficient data within them.

###### 3.1.2.1 Hypertext Information Hiding

Sui and Luo [14] present a novel method for hiding information within hypertext files. They modified the existing characters in the hypertext markup language (HTML) tags. This approach maintains the original appearance of the file without presenting any noticeable changes. The algorithm functions by extraction of the bits from the hidden message which is then used to change certain HTML tags. This approach allows for concealing up to one-eighth of the markup letters in the hypertext file. The creators highlight the benefits of the technique being used, which includes being hard to detect and not adding much to the file size.

##### 3.1.3 Challenges in E-Book Copyright Protection

Yung-Chen Chou et al. [15] threw some light on the challenges related to copyright protection and content integrity, which have been a critical and major issue in today's era and is hindering the broader adoption of eBooks. The formats that serve today such as Amazon Kindle, Adobe PDF, and EPUB, are susceptible and prone to copyright concerns and highlight the need for some innovative solutions. The study builds upon prior research on watermarking technology by emphasizing its potential to safeguard eBook copyrights. Not importantly, it extends its focus to HTML and XML technologies to produce cross-platform eBooks. Not only this but the integration of JavaScript is introduced as a novel means to embed verification codes, which serves as a cherry on top as this adds an extra layer of protection and control over eBook content integrity.

### 3.1.4 **Concealing Information in HTML Tags**

Huang et al. [17, 18] proposed a method that uses the flexibility of HTML tags to hide data that is sensitive. They noticed that one HTML tag can have several attribute settings offering a discreet way to embed secret information. For instance, the tag `<HTML face="Times New Roman" colour="blue" size="5">` could be tweaked to hold hidden data in its attribute values.

### 3.1.5 **Invisible Characters for Information Hiding**

Katzen Beisser and Petit colas [16] came up with a new innovative way to embed secret information in a web page's source code. They did this by using special characters which is not visible to the users. These characters blend into the source code without changing how the page looks or works. This method helps to ensure that sensitive data is being transmitted covertly without messing up the user's experience.

### 3.1.6 **Blank Characters in English Sentences**

An information-hiding method was presented by Lee and Tsai [19] that leverages the abundance of blank characters in English sentences. The core principle was to replace the original blank characters with different specific codes, effectively embedding secret data within the text without altering or changing its overall appearance or experience. A subtle and robust mechanism for concealing sensitive information is possible by this approach.

### 3.1.7 **Information Hiding in XML**

In order to hide secret information in XML, an approach was highlighted by Inoue et al. [20]. According to this author, a comparatively variable approach is better as XML is extremely severe than HTML. Five different information-hiding techniques were proposed by this author.

### 3.1.8 **Enhancing Data Integrity in Cloud Storage**

P. Sharma and colleagues [21] put forward a compelling method to boost data integrity in cloud storage by combining blockchain technology with smart contracts (SCs) in a new different way. Their research tackles the key issues of confidentiality, availability, and integrity by zeroing in on threats to data integrity and suggesting a fresh architecture. The way they use Merkle trees to check data integrity, bring in smart contracts for user authentication, and break down the threat model shows how in-depth their approach is.

### 3.1.9 Blockchain Technology in Cloud Storage Services

Pinheiro et al. [22] show how Blockchain technology and SCs boost the security, transparency, and productivity of Cloud Storage Services (CSS). Their suggested setup brings key upgrades. It uses a Blockchain Network (BN) to store info about files. This ensures no one can change records and allows checking throughout file storage and integrity tests. The study adds a level of self-running and clear processes. This cuts down on possible teaming between untrustworthy Integrity Check Services (ICS) and CSS. It does this by adding SCs kept in the BN. This makes the integrity checking process even stronger.

**Table 6 Literature Review Summary**

**I = Integrity      B = Blockchain      C = Cloud      E=Efficiency**

Ref	Title	I	B	C	E	Pros	Cons
[14]	A new steganography method based on hypertext	Yes	No	Yes	No	<ul style="list-style-type: none"> <li>- Achieves secure information hiding in hypertext by modifying markup letters.</li> <li>- Demonstrated high efficiency and security in experiments and analysis.</li> </ul>	<ul style="list-style-type: none"> <li>- Traditional methods based on blanks and tabs are criticized for security and performance concerns.</li> <li>- Traditional methods are clearly detectable and prone to attack when opened in binary mode.</li> </ul>
[15]	Research on E-book Text Copyright Protection and Anti-tampering Technology	Yes	No	No	No	<ul style="list-style-type: none"> <li>- Compatibility with various mobile and tablets on cross-platform.</li> <li>- Resilience of watermarking through multiple embedding techniques</li> <li>- Acknowledgment of the importance of preventing unauthorized modifications through different integrity checks.</li> </ul>	<ul style="list-style-type: none"> <li>- Potential limitations in the widespread use of e-books due to lack of copyright protection.</li> <li>- Narrow focus on text content protection, with limited coverage of multimedia elements.</li> </ul>
[17]	Detection of hidden information in webpage	Yes	No	No	No	<ul style="list-style-type: none"> <li>- Efficient detection method</li> </ul>	<ul style="list-style-type: none"> <li>- Limited information on false negative rates</li> </ul>
[18]	An algorithm of webpage information hiding	Yes	No	No	No	<ul style="list-style-type: none"> <li>- Large, embedded capacity</li> </ul>	<ul style="list-style-type: none"> <li>- Limited information on false negative rates</li> </ul>

	based on attributes permutation						
[19]	Secret communication through web pages using special space codes in HTML files	Yes	No	No	No	<ul style="list-style-type: none"> <li>- Provides a covert communication method using web pages.</li> <li>-Utilizes special space codes for steganography.</li> <li>-Enhances security through randomization and secret key usage.</li> </ul>	<ul style="list-style-type: none"> <li>- Require careful handling of space codes to avoid unintended detection.</li> <li>- Dependence on the security of the web page server.</li> </ul>
[21]	Blockchain-based Integrity Protection System for Cloud Storage	Yes	Yes	Yes	No	<ul style="list-style-type: none"> <li>- The combination of blockchain and smart contracts delivers a transparent framework, which enhance the data integrity and user authentication in cloud storage with auditing enabled.</li> <li>- The user-focused design adds practical and accessible solution for organizations managing access on the cloud.</li> </ul>	<ul style="list-style-type: none"> <li>- Blockchain technology may pose a steep learning curve for the developers and organizations.</li> <li>- Scalability challenges associated with blockchain technology need further exploration to handle a large volume of users and transactions efficiently.</li> </ul>
[22]	Monitoring File Integrity Using Blockchain and Smart Contracts	Yes	Yes	Yes	No	<ul style="list-style-type: none"> <li>- Enhanced security and auditability through Blockchain, providing a tamper-proof and resilient base.</li> <li>- Automation and decentralization increase efficiency, reduce manual intervention and prevent collusion in integrity validation.</li> </ul>	<ul style="list-style-type: none"> <li>- Resource intensiveness may result from the decentralized and automated nature of the proposed solution.</li> </ul>

With the help of my novel methodology using Corda Blockchain and smart contracts, it is possible to achieve privacy, security and efficiency which can be utilized over the cloud as well.

## 4 **CORDA - AN OVERVIEW WITH FRAMEWORK**

### 4.1 **Introduction**

R3, a group of top financial and tech firms, created the Corda platform for distributed ledger technology (DLT). Corda offers a safe and expandable answer to complex deals and agreements meeting the needs of big companies and businesses. Unlike typical blockchains, Corda puts data privacy first. It shares each deal with those who need to know keeping sensitive info safe. This makes Corda perfect for uses that need strict privacy and rule-following.

Corda lets users build and run smart contracts, called "CorDapps," written in common coding languages. This makes them easy to use for coders of all skill levels. These smart contracts enforce agreements and improve business processes, cutting down on manual work and inefficient operations. Corda's speed and ability to grow are key points making it fit for big business uses that need quick and reliable deal processing.

Corda's design focuses on working well with other systems allowing smooth integration with existing networks. This lets businesses use blockchain tech without changing their current setup. The platform uses a special way to agree on things. It has a group of "notaries" who check and confirm transaction details. This makes sure transactions are final and can't be changed. It doesn't need the heavy computer work that regular blockchains do.

People use Corda in many different areas. These include managing trade money, tracking product journeys, insurance, healthcare, buying and selling houses, and money services. Corda is good at keeping things private, handling lots of work and working with other systems. It's a strong and flexible system for big companies to handle complex deals in an efficient way.

### 4.2 **Key Features of Corda**

#### 4.2.1 **Ledger**

- A distributed ledger is a fact database shared, replicated, and synchronized among multiple users in a network.
- Nodes have a copy of the ledger in their vault, and it saves transactions to avoid double spending.
- Every node has a distinct perspective of the ledger based on the facts it shares or receives.
- Before declaring the fact, the nodes must reach a consensus.
- Information between two nodes shared on the ledger is always displayed in exactly the same form.
- In Corda, data repository is distributed. Each node maintains a database of facts—things it knows to be true based on interactions. For example, if Alice lends money to Bob, nodes representing Alice and Bob will keep the same record of the loan details. Only Alice and Bob will see or store this data if they are the only parties to the loan.

## 4.2.2 States

A state in Corda is an immutable object representing a fact known by one or more nodes at a specific point in time. States can describe any type of information or fact, such as a financial instrument, Know Your Customer (KYC) information, or identity details. States are immutable; they cannot be altered. Corda uses sequences of states to track the evolution of facts. When a fact changes, a participant creates a new state, marking the old state as historic.

Each node maintains an up-to-date vault, which is the node's database for tracking both current and historical states in which it participates.

## 4.2.3 Transactions

The Corda ledger can only be modified by adding new transactions; it cannot be edited. A transaction updates the ledger by consuming existing input states and generating new states, rendering the consumed states "historic."

Every state is immutable and cannot be altered. This is known as the UTXO (unspent transaction output) model.

- Transactions can include any number of inputs, outputs, and references of any type. Different types of states representing various financial products, such as cash or bonds, can be included in transactions.
- Issuing states are created by producing a transaction without inputs, ensuring no new states replace any existing ones marked as "historic."
- States are excited by creating transactions without outputs, which means the consumed states are not replaced by new ones.
- Fungible assets can be consolidated or divided, such as creating a \$7 cash state by combining a \$2 state and a \$5 state.
- Transactions are atomic; either all proposed changes are accepted, or none are.

**The two main types of transactions are:**

- Transactions for changing the notary for a state.
- General transactions for all other purposes.

### 4.2.3.1 Transaction Backchains

Transaction backchains allow a node to verify that each input originated from a legitimate sequence of transactions. This process, known as "walking the chain," ensures the validity of transactions. States can be reissued to improve performance by limiting the number of transactions a node needs to examine or to maintain the privacy of previous transactions.

Input state references are linked over time to form backchains, allowing earlier transactions' outputs to be used as inputs for new transactions.



References to input states include:

- The hash of the input's creation transaction.
- The backchain's index of the input in the prior transaction's outputs.

#### 4.2.3.2 Transaction Validity

Adding a transaction to the ledger requires more than just obtaining the necessary signatures; it must also be:

- Valid: The proposed transaction and every transaction in its backchain must be signed by all required parties.
- Unique: None of the inputs to the proposed transaction have been used by any previously committed transaction, as determined by a notary.

If a transaction gathers all necessary signatures but does not meet these criteria, its outputs are invalid and cannot be used as inputs for subsequent transactions.

#### 4.2.4 Smart Contracts

Smart contracts in Corda digitize agreements by converting contract terms into code that automatically executes when the terms are met. This means:

- Parties do not need to trust each other to uphold the agreement terms.
- External enforcement is unnecessary.
- There is always a consensus on how to interpret the contract.
- Each network node has a copy of the contract code, and network participants must agree that all contract requirements are met before it is executed.

Corda's smart contracts have unique characteristics:

- They can only be updated and replaced, not changed.
- Once implemented, the outcomes are immutable.

#### 4.2.5 Flows

Corda networks use point-to-point communication instead of a global broadcast model. Network members must determine what information to share, with whom, and in what order to update the ledger.

Corda uses flows to automate this process, so there is no need to specify these steps explicitly. A flow is a set of instructions that guides a node on how to perform a specific ledger update, such as issuing an asset or completing a deal.

Node operators use RPC calls to start a specific flow, which abstracts all networking, I/O, and concurrency concerns from the node operator. These flows govern all behaviour on the node. Unlike contracts, flows do not execute in a sandbox, allowing nodes to engage in networking, I/O, and randomness sources during a flow.

Corda offers a library of flows for common operations, so developers do not have to rewrite the logic for routine procedures such as:

- Notifying and recording an event.
- Collecting counterparty node signatures.
- Verifying the transaction sequence.

#### 4.2.6 **Consensus**

Before adding a proposed transaction to the ledger, there must be agreement that it is legitimate. Blockchains uses consensus mechanisms to validate transaction and achieve an agreement, trust, and security across decentralized networks. Popular mechanisms include proof-of-stake and proof-of-work.

Corda's consensus mechanism is unique. Consensus is reached by proving that a transaction is both valid and unique. Validity consensus tests ensure:

- The proposed transaction and each transaction in its backchain are legally binding.
- The transaction has all necessary signatures.

For instance, if a node proposes a transaction to transfer a treasury bond, the bond transfer is only legitimate if:

- The central bank issued the bond in a valid issuance transaction.
- All subsequent transfers of the bond were also valid.

#### 4.2.7 **Notaries**

The notary is a distinct consensus service provided by Corda. It prevents double-spends by ensuring each transaction contains unique input states. A notary service consists of one or more notaries acting as a notary cluster. The notary's role is to verify the uniqueness of each transaction's input states. Once confirmed, the notary cluster signs the transaction. If any input state matches those in a previous transaction, the cluster rejects the transaction, indicating a double-spend attempt.

Each state has an assigned notary cluster, which will only notarize a transaction if it is the designated notary cluster for every state in the transaction.

#### 4.2.8 **Vault**

A Corda vault is a database that stores all ledger information relevant to a node. The database tracks consumed and unconsumed states. From a business perspective, this involves tracking all transaction states that the node owner can spend and all spent states from transactions involving the node. It functions like a bitcoin wallet, tracking your spendable and spent funds transaction. Any transaction in the vault can have a descriptive text note attached to it.

#### 4.2.9 Nodes

A Corda node has a distinctive network identity and operate in the Java Virtual Machine (JVM) runtime environment. The JVM provides a stable platform for deploying and running Java applications, including Corda services and CorDapps.

Key components of the node architecture include:

- A persistence layer for data storage.
- A network interface for node communication.
- An RPC interface for node-owner interactions.
- A service hub for internal node service calls from flows.
- A CorDapp interface and provider for adding CorDapps to the node.

#### 4.3 Proposed Framework

This research presents a prototype for the novel methodology to maintain the integrity of Authentic Digital Islamic Assets using the blockchain technology Corda. The proposed architecture is for the sharing of Islamic data among the world while maintaining its transparency and its integrity. Our prototype basically has three actors i.e. Notary, data editor, and viewer. But for this prototype we have only shown the transactions between data editor and viewer.

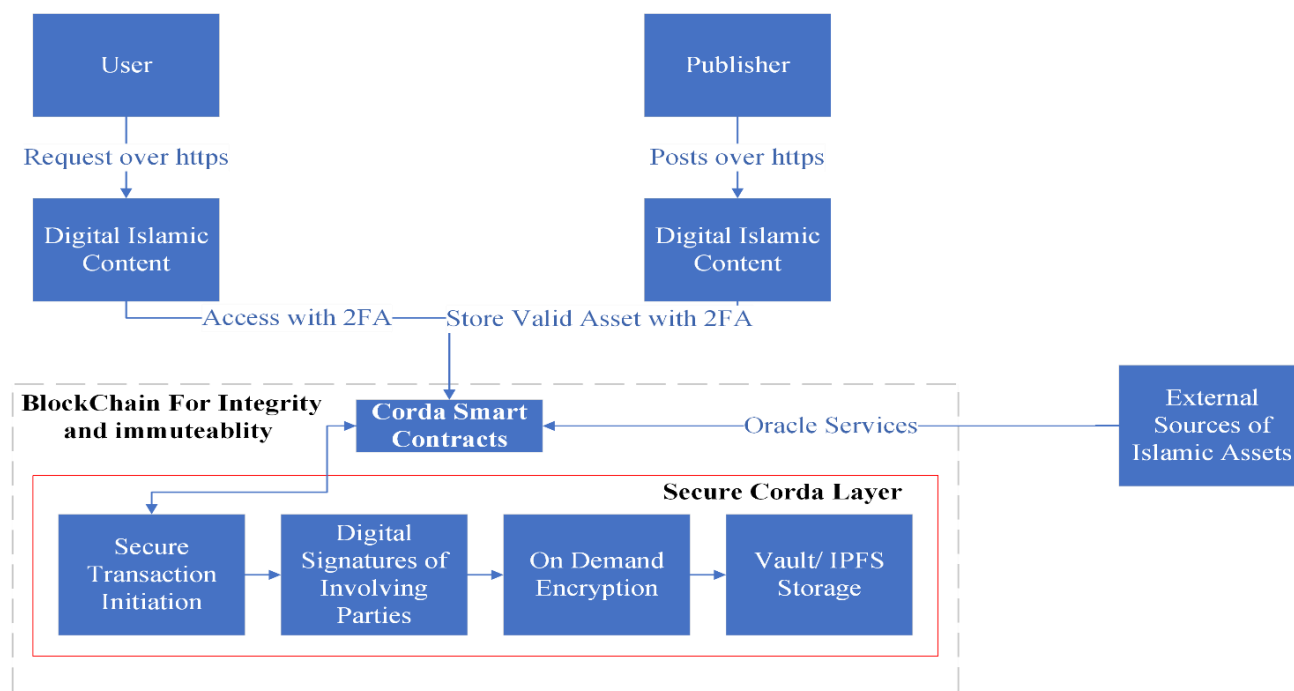
This novel methodology prevents transparent transaction history on the blockchain as well as corda feature. Furthermore, different techniques can be implemented (discussed above in chapter 3 literature review) e.g., steganography will be incorporated for document integrity during uploads and watermarking for full document retrieval. These techniques contribute to a more robust content protection system, discouraging tampering, unauthorized distribution, and providing traceability in case of leaks. In our proposed framework, we are focusing on corda blockchain and assuming that data is already authenticated till uploading on our system.

The research work aims to ensure the integrity of authentic digital Islamic assets by leveraging the Corda blockchain platform. This system involves all member countries of the Organisation of Islamic Cooperation (OIC) acting as nodes, with a leading country (Saudi Arabia) responsible for entering authenticated data and validate data.

## 4.4 Methodology

### 4.4.1 System Architecture

Figure 2 architecture diagram



## 4.5 Appealing Remedies for Issues

For addressing the above-mentioned inadequacies of present technologies and fulfill the needs outlined using Corda blockchain, I can leverage capabilities of blockchain to ensure content integrity and improve digital asset management for digital Islamic content. How Corda can address each of the mentioned shortcomings is as proffered:

## 4.6 Inadequacies of Present Technologies

### 4.6.1 Content Integrity for E-Books, eQuran, Hadees Shareef, and Fatwas:

Corda utilizes its immutable ledger to construct a decentralized and immutable record of digital content. Each entry can be cryptographically signed by authorized entities (e.g., religious scholars, publishers) ensuring that any alteration in the content is easily detectable.

### 4.6.2 Protection Against Sophisticated Attacks:

- **Corda Solution:** Used advanced cryptographic techniques to secure content against unauthorized modifications. By recording each transaction on a decentralized ledger, the integrity of the content can be maintained even in the face of sophisticated attacks.

### 4.6.3 Motivation for Blockchain Adoption

#### 4.6.3.1 Inefficiencies in Digital Asset Management:

- Utilize Corda's capabilities to provide real-time visibility and traceability of digital Islamic assets. The decentralized nature of Corda ensures that all stakeholders have

access to the same immutable data, reducing the risk of unauthorized modifications and data breaches.

#### 4.6.3.2 Scalability:

- The Corda's architecture allows it to handle big operations with efficacy. It can deal with many transactions and large data stores by using its point-to-point communication model.

#### 4.6.3.3 Enhanced Transparency:

- Blockchain gives a spread-out and immutable record letting all allowed parties see transactions as they happen. This transparency cuts down on info gaps and builds trust among those involved.
- The blockchain's immutable record-keeping ensures a fixed and correct history of each transaction and change in digital content. This feature helps for auditing and helps to trace the origin of problems.
- We can trace any digital asset transactions from its source, making it easier to spot and fix mistakes or problems. This uses Corda blockchains' ability to give a clear and traceable record of all transactions.

#### 4.6.3.4 Deploy the Corda Network:

- Build a Corda network with nodes that stand for different people involved (scholars, publishers, IT help providers) with the granular permissions and abilities to work with the digital content.

#### 4.6.3.5 Consensus-Based Data:

- In a blockchain network, all nodes must agree on changes made, making sure everyone's on the same page and cutting down on data discrepancies. This way of agreeing makes digital Islamic assets integrity trustworthy.

#### 4.6.3.6 Enhanced Security:

- Blockchain uses cryptographic procedures to secure data, making it nearly impossible to alter or manipulate information. This ensures the integrity of authentic digital Islamic content and protects it from fraudulent activities.

#### 4.6.3.7 Automation of Smart Contracts:

- Smart contracts on the blockchain can automate the execution and enforcement of agreements based on predefined criteria. This automation streamlines contract management and eliminates the need for intermediaries.

#### 4.6.3.8 Components:

- **Nodes:**
  - Represent each OIC member country.
  - Maintain a copy of the distributed ledger.
- **Leading Node Content Editor (Saudi Arabia):**
  - Central authority for data entry and validation.
  - Responsible for initiating authentic data transactions and authenticating and validating transactions of others.
- **Notary Node:**
  - Ensures uniqueness and prevents double-spending.
  - Validates the authenticity of transactions.
- **User Web Portal:**
  - Interface for users to access digital Islamic assets.
  - Provides read-only access to ensure data integrity.

#### 4.6.4 Roles and Responsibilities

##### 4.6.4.1 Nodes

- Act as part of the Corda network.
- Receive and store copies of the distributed ledger.
- Initiate transactions that require validation.

##### 4.6.4.2 Leading Country (Saudi Arabia)

- Central authority for data entry.
- Validates and authenticates digital Islamic asset data.
- Publishes validated transactions to the network.

##### 4.6.4.3 Notary

- Ensures the uniqueness of each transaction.
- Prevents double-spending and maintains ledger integrity.

##### 4.6.4.4 Users

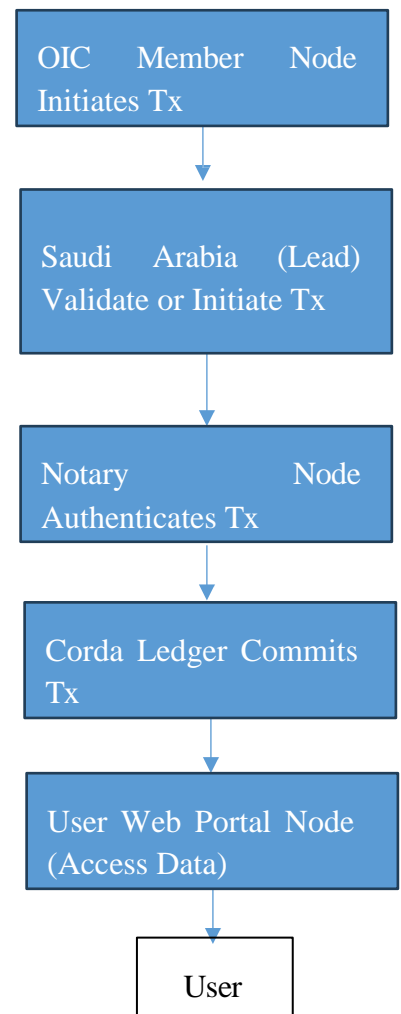
- Access digital Islamic assets through the web portal.
- View data in a read-only format to ensure integrity.

#### 4.6.5 Network Structure:

##### 4.6.5.1 Node Countries

- All OIC member countries will act as nodes in the Corda network.
- Saudi Arabia will serve as the leading node, responsible for entering and validating data.

*Figure 3 Flow Diagram*



#### 4.6.5.2 Data Entry and Validation:

- Saudi Arabia will input authenticated digital Islamic asset data into the system.
- Other nodes can also add content but that will be validated by the leading country.
- The data will be distributed to all nodes in the network signature of Notary node.

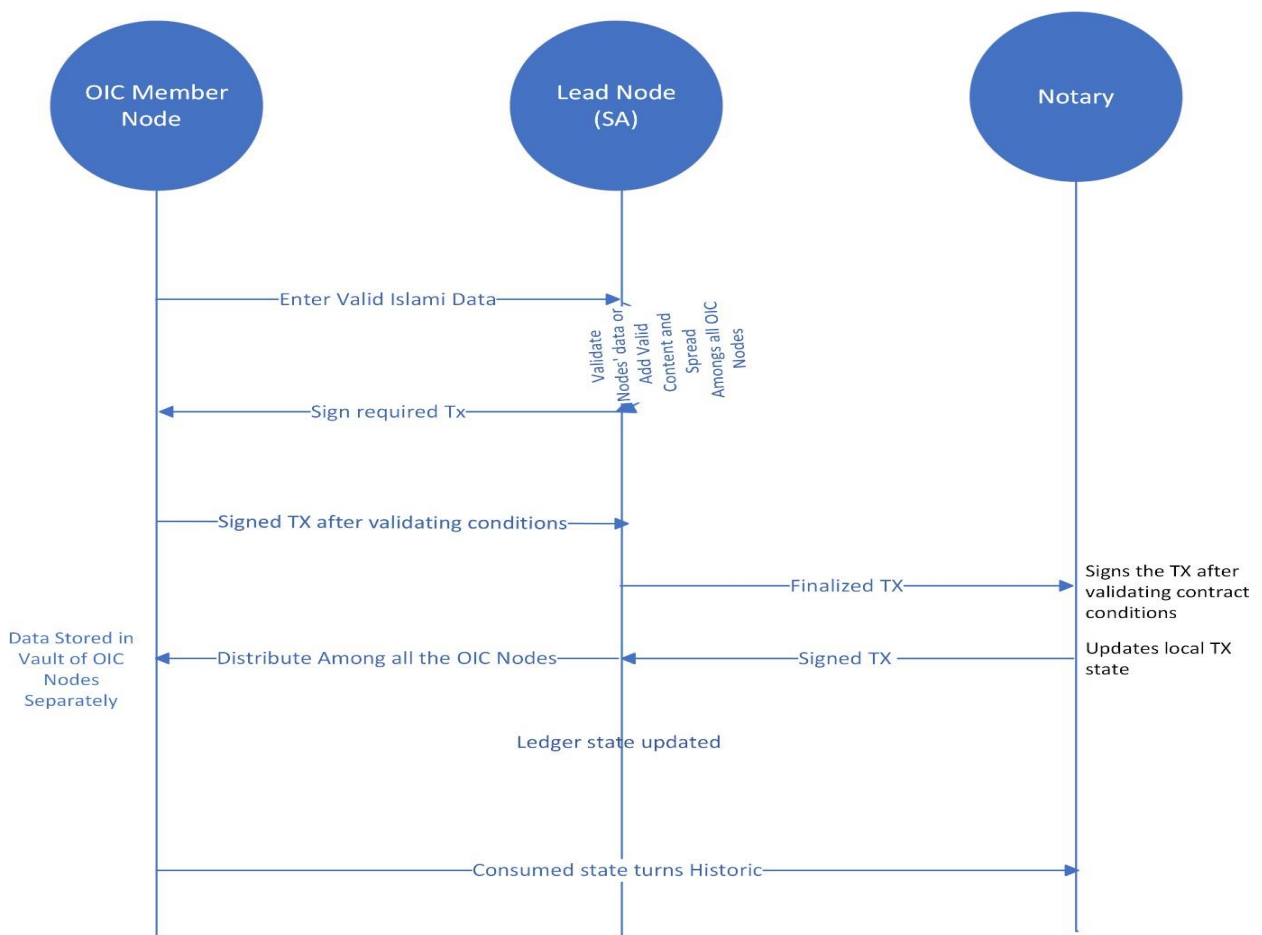
#### 4.6.5.3 User Access:

- Users can access this information through a web portal secure with 2FA authentication minimum.
- Every node is assigned X.509 certificate known to each node in a corda network including Web Portal Node.

#### 4.6.5.4 Transaction Initiation:

- If another country initiates a transaction, it will be sent to the leading country (Saudi Arabia) in our example for validation.
- Once validated, the transaction will be published and available to all nodes as immutable.

**Figure 4 Transection Flow**



#### 4.6.6 **Transaction Flow**

##### 4.6.6.1 **Data Entry:**

- The leading country (Saudi Arabia) inputs authenticated digital Islamic asset data to the system.
- Data is distributed to all nodes in the Corda network after being signed by the notary node to avoid double spending and duplication.

##### 4.6.6.2 **Data Access:**

- Users access data through a web portal.
- Data is available in a read-only format to ensure integrity.



## 5 Implementation & Results

### 5.1 Implementation

- **Environment Setup:**

- **Hardware:** Latitude 7480 with i5-6300U (4 CPUs), 16 GB RAM.
- **Virtual Machine:** Single node deployed on virtual machine with 4 Gb Ram, 10 GB HDD, 2 processors, Lubuntu OS
- **Software: Corda Version:** 4.10 Community Edition, **IDE:** IntelliJ version 2022.3.1,**JDK:** Java ZULU JDK 8,**Build Tool:** Gradle, **Version Control:** Git.

#### 5.1.1 Comparative Analysis:

- **Configured two blockchains:** Ethereum and Corda.

#### 5.1.2 Corda Setup:

- Cloned the Corda sample project, Opened the project in IntelliJ and make build using Gradle, Created the frontend in HTML and Spring Boot APIs.

**Ethereum Setup:** Deployed on the Ganache blockchain, Used Remix IDE with JavaScript, MetaMask wallet for transactions, HTTP server using python -m http.server,**Data Source:** tanzil.net.

#### 5.1.3 Steps for Implementation:

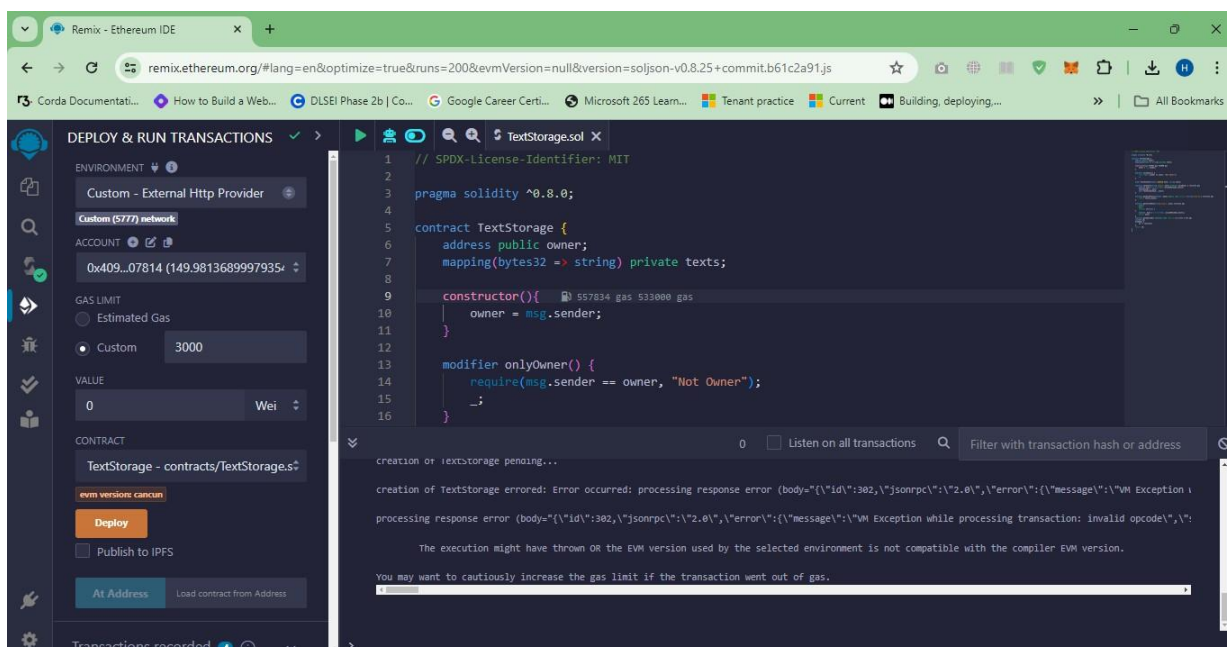
Follow the R3 instructions to setup Corda first time using link: <https://docs.r3.com/en/platform/corda/4.10/community/tutorial-cordapp.html>

- **Clone Corda Sample Project:** Git installed and set up, Clone the project repository using git repo as:- [git clone <https://github.com/corda/samples-java>].
- **Open and Build Project in IntelliJ:** Open the cloned project in IntelliJ, Ensure that Gradle is configured properly, Build the project to resolve dependencies.
- **Create Frontend with Spring Boot APIs:** Use Spring Boot to create RESTful APIs for the frontend, Implement the frontend in HTML.
- **Deploy Ethereum on Ganache:** Install Ganache and set it up, Use Remix IDE for smart contract development and deployment on the blockchain, Use MetaMask for transaction signing and management.
- **Run HTTP Server:** Use the command python -m http.server to run a simple HTTP server for making post requests using JavaScript.
- **Data Integration:** Get the Quran Ayat from tanzil.net for the Corda blockchain project.

Figure 5 Running Http Server

```
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
:::1 - - [03/Jun/2024 08:31:25] "GET / HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:26] "GET /favicon.ico HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:32] "GET /performancetest.html HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:32] "GET /styles.css HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:32] "GET /script.js HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:33] "GET /books.png HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:31:36] "GET /testing.html HTTP/1.1" 200 -
:::1 - - [03/Jun/2024 08:50:50] code 404, message File not found
:::1 - - [03/Jun/2024 08:50:50] "GET /tesing.html HTTP/1.1" 404 -
:::1 - - [03/Jun/2024 08:52:08] code 404, message File not found
:::1 - - [03/Jun/2024 08:52:08] "GET /performancetesting.html HTTP/1.1" 404 -
:::1 - - [03/Jun/2024 09:13:44] "GET / HTTP/1.1" 200 -
```

Figure 6 Deploy Smart contract using Remix IDE



**Figure 7 Ganache Blockchain with Accounts**

The screenshot shows the Ganache interface with a dark theme. At the top, there are navigation tabs for ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. Below these are various system metrics like CURRENT BLOCK (3455), GAS PRICE (2000000000), and NETWORK ID (5777). The main section displays a list of accounts with their addresses, balances, and transaction counts.

ADDRESS	BALANCE	TX COUNT	INDEX
0x4096F1dd457C91F9C9AC4991AA81E92fc4A07814	149.98 ETH	89	0
0x2763D503b6e6a9bdC4261b4CD699312eA96b4722	50.00 ETH	1	1
0xbE2Eae0c39B78f4bb21Bd740d5b66D04Bf26B679	100.00 ETH	0	2
0x471f8193DE69252549338b54bd70E75F30CA9471	100.00 ETH	0	3
0x608D62aa0C139dCF6a55AB351555C998A58e862a	100.00 ETH	0	4
0xdAB4cDE840fb114f84a52BF682e3F8Ee97D0327	100.00 ETH	0	5

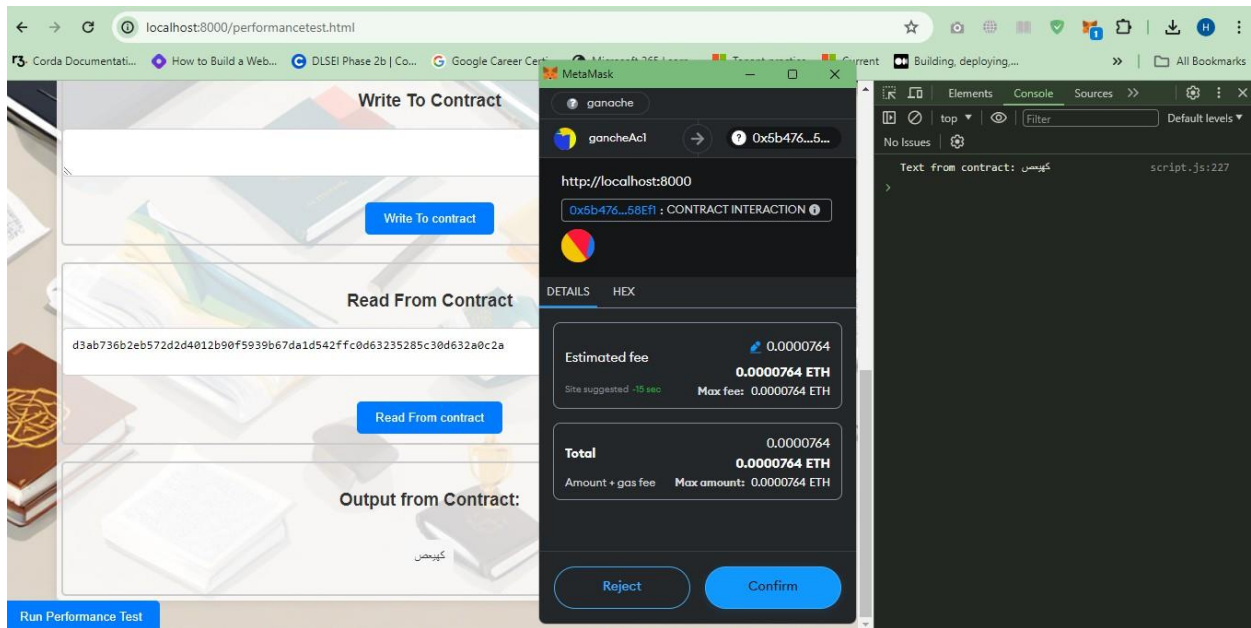
**Figure 8 HTML Page (Portal) with JavaScript for Analysis**

The screenshot shows a web portal titled "Integrity Protection of Digital Islamic Assets". It features a language selection menu (English, Urdu, Arabic) and several interactive sections:
 

- Generate keccak256 Hash Code:** A text input field with a "Generate keccak256 Hash Code" button.
- Unicode Output:** A section for displaying the result of the hash generation.
- Keccak256 Hash Code Output:** A section for displaying the generated hash code.
- Connect Wallet:** A button to connect a wallet.
- Write To Contract:** A text input field with a "Write To contract" button.
- Read From Contract:** A text input field with a "Read From contract" button.
- Output from Contract:** A section for displaying the result of the contract interaction.

 A "Run Performance Test" button is located at the bottom left of the page.

*Figure 9 Transaction Flow*



*Figure 10 Ethereum Blockchain Write and Read Analysis*

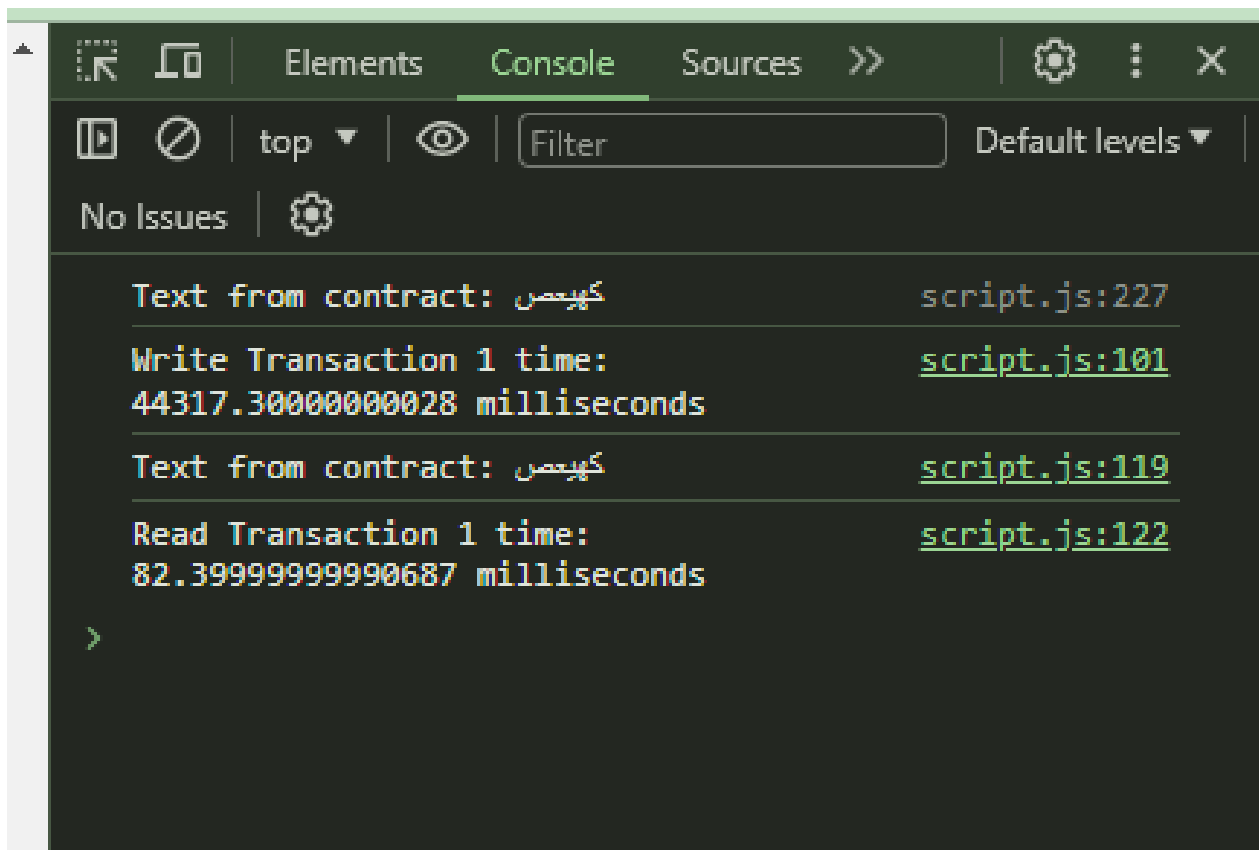


Figure 11 Ethereum Blockchain Write and Read Analysis

```
Transaction Successful
Transaction Hash: 0xc3ae64f33387fe58e5b85186d2b88e5daac908326ff1a1aa05606e4d433f27344
Write Start Time: 831.3696
Write End Time: 2006.8605
Write Time Taken: 1175.4909 ms
Network Latency: 5.038099999999986 ms
Transaction Successful
Transaction Hash: 0xc8e4d36f49dcb28e4c4c9d02148cd03b80fbac88e648182ecf125fd1b31f8d6
Write Start Time: 2018.3889
Write End Time: 11224.4187
Write Time Taken: 9206.0298 ms
Network Latency: 2.375 ms
Read Start Time: 11230.3631
Read End Time: 11252.7732
Read Time Taken: 22.410099999999147 ms
Network Latency: 3.085900000000038 ms
Read Start Time: 11257.8391
Read End Time: 11275.3575
Read Time Taken: 17.518400000000838 ms
Network Latency: 1.989000000001397 ms
Average Write Time: 5190.7603500000005 ms
Minimum Write Time: 1175.4909 ms
Maximum Write Time: 9206.0298 ms
Standard Deviation of Write Time: 4015.2694500000002 ms
Average Read Time: 19.964249999999993 ms
Minimum Read Time: 17.518400000000838 ms
Maximum Read Time: 22.410099999999147 ms
Standard Deviation of Read Time: 2.4458499999991545 ms
Average Network Latency: 3.122000000000355 ms
Minimum Network Latency: 1.989000000001397 ms
Maximum Network Latency: 5.038099999999986 ms
Standard Deviation of Network Latency: 1.1741422848186647 ms
PS D:\Degree\IS\04 Semester\Implementation\Ethereum\Ethereum with ganache\Script>
```

## 5.2 Corda

### 5.2.1 Workflow

The basic files which were used for the prototype are as follows:

We first build the project and after that run nodes by following commands:

- ./gradlew clean deployNodes
- .\build\nodes\runnodes.bat

Figure 13 Nodes in Running Condition

```
My professor accused me of plagiarism.
His words, not mine!

--- Corda Community Edition 4.10 (fa98aa7) ---

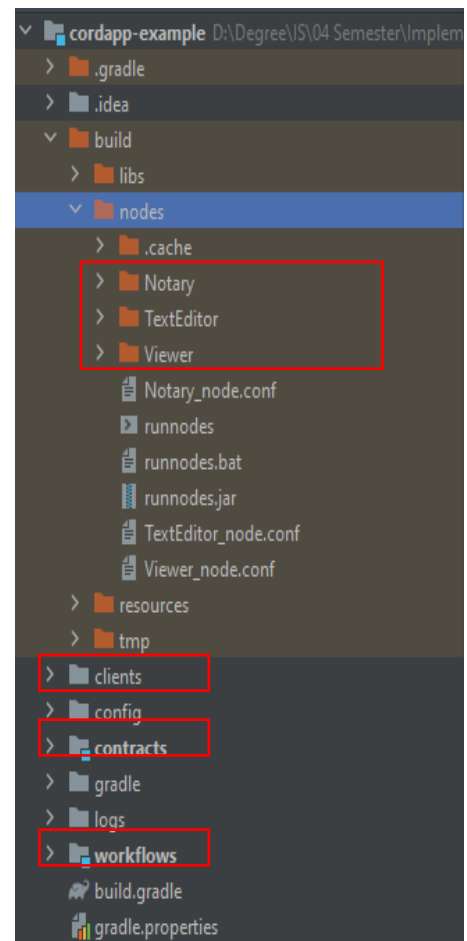
Logs can be found in : D:\Degree\IS\04 Semester\Implementation\Corda\cordapp-example\build\nodes\Notary\logs
! ATTENTION: This node is running in development mode. This is not safe for production deployment.
Jolokia: Agent started with URL http://127.0.0.1:7005/jolokia/
Advertised P2P messaging addresses : localhost:10002
RPC connection address : localhost:10003
RPC admin connection address : localhost:10043
Loaded 2 CorDapp(s) : Contract CorDapp: FarmData-example Contracts version 1 by vendor Corda Open Source with licence Apache License, Version 2.0, Contract CorDapp: FarmData-example Contracts version 1 by vendor Corda Open Source with licence Apache License, Version 2.0
Node for "Notary" started up and registered in 132.54 sec

Welcome to the Corda interactive shell.
You can see the available commands by typing 'help'.

Running P2PMessaging Loop
Mon Jun 03 09:34:54 PKT 2024>>>

Logs can be found in : D:\Degree\IS\04 Semester\Implementation\Corda\cordapp-example\build\nodes\Viewer\logs
! ATTENTION: This node is running in development mode. This is not safe for production deployment.
Jolokia: Agent started with URL http://127.0.0.1:7007/jolokia/
Advertised P2P messaging addresses : localhost:10008
RPC connection address : localhost:10009
RPC admin connection address : localhost:10049
Loaded 2 CorDapp(s) : Contract CorDapp: FarmData-example Contracts version 1 by vendor Corda Open Source with licence Apache
```

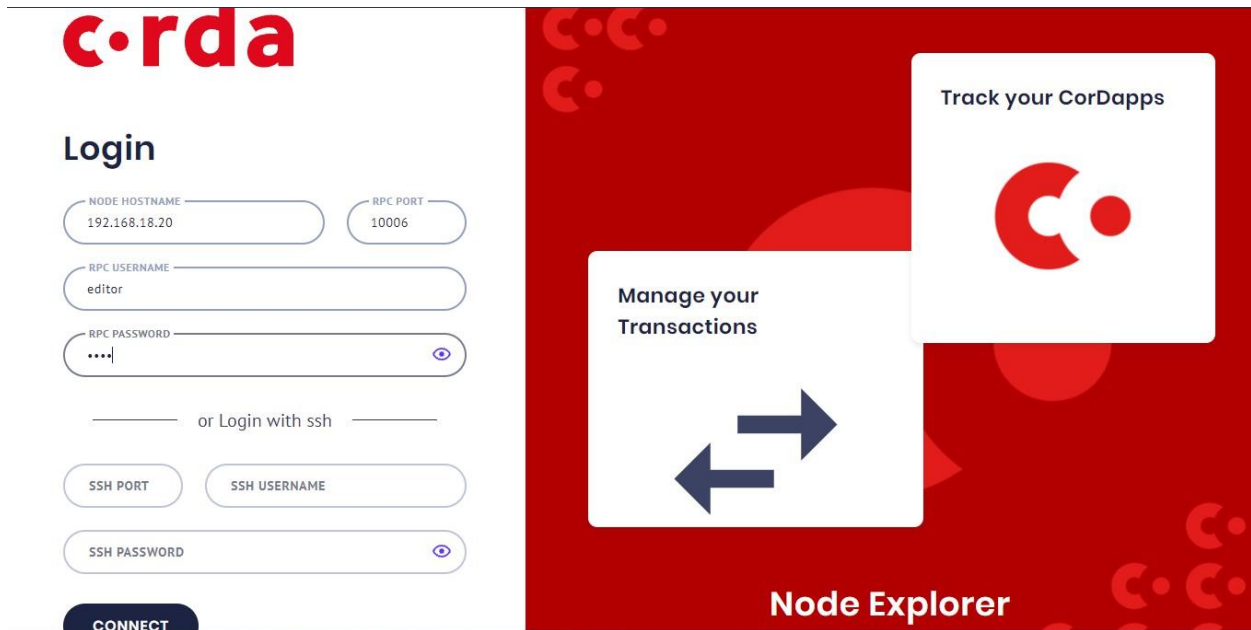
Figure 12 Directory Structure of Project





The actors we have are actually our nodes which we defined in Corda – An overview chapter so after running nodes, a terminal will open for each node along with notary as shown in above figure.

*Figure 14 Corda Explorer Login Screen Connected with Our Nodes*



*Figure 15 Corda Blockchain Node Information*

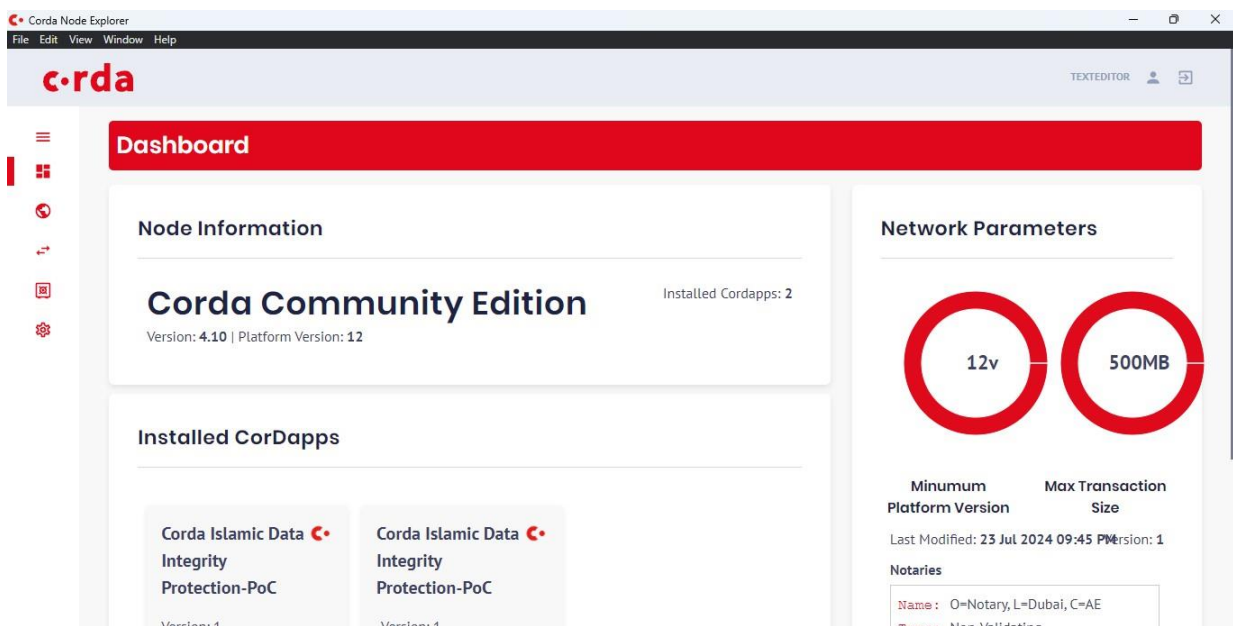


Figure 16 Geo Location of Nodes Shown on Map

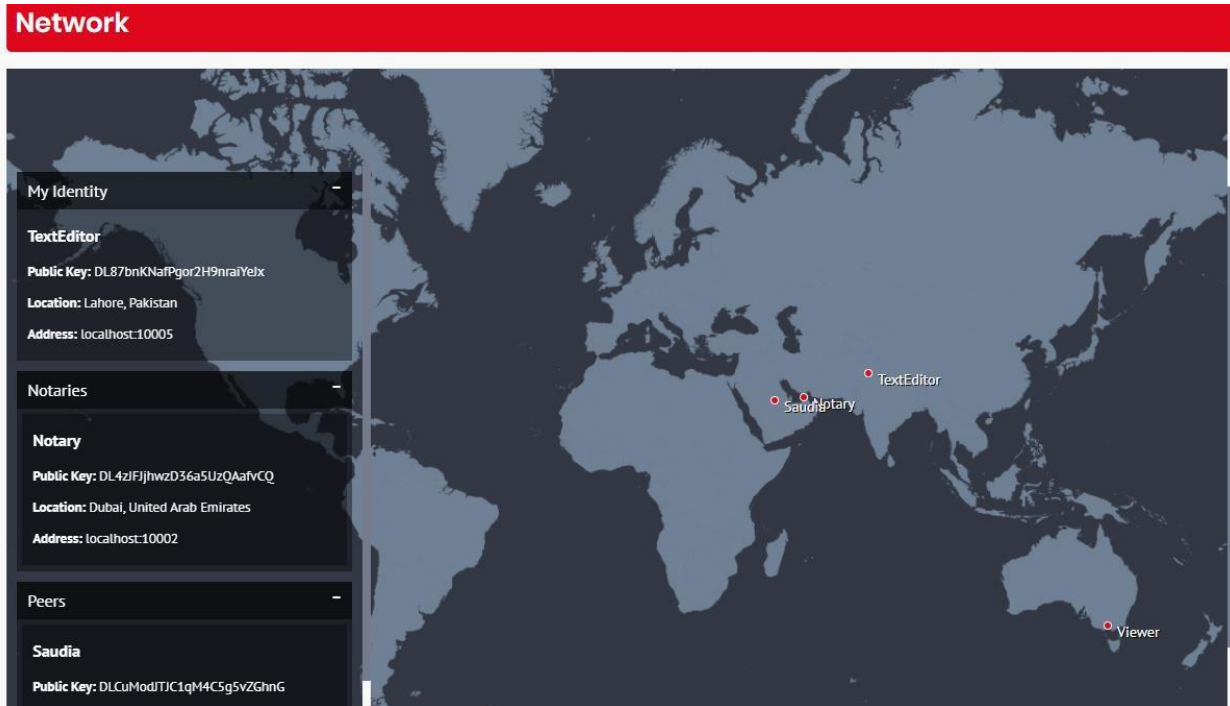


Figure 17 Graphical Flow Execution

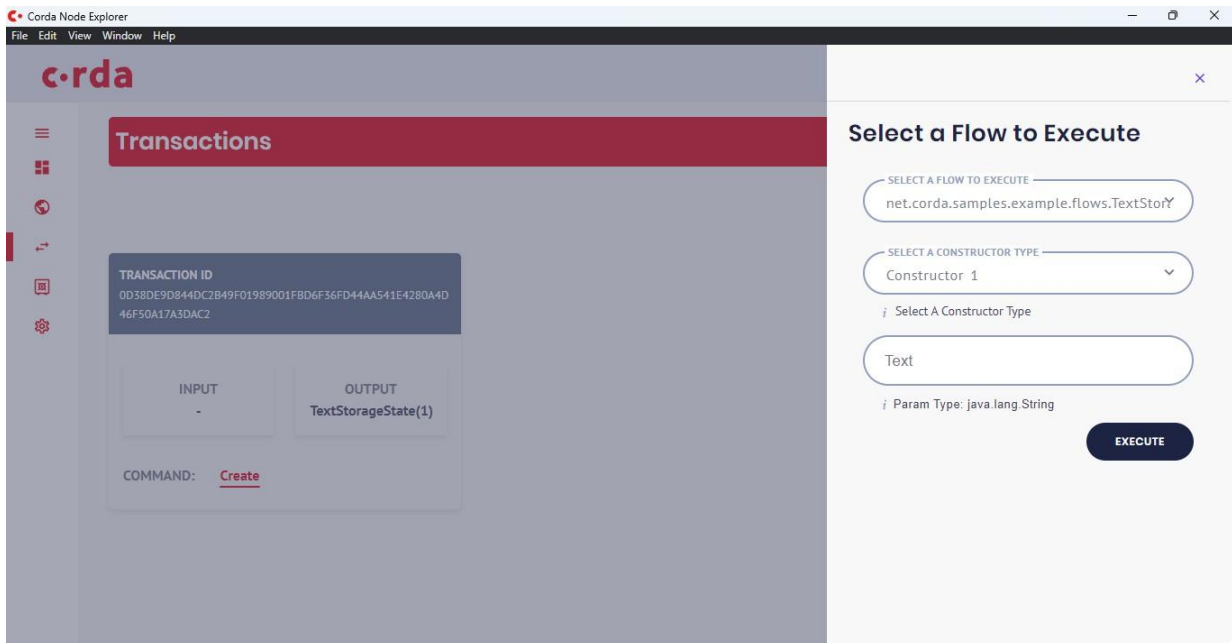


Figure 18 Output of Executed Flow

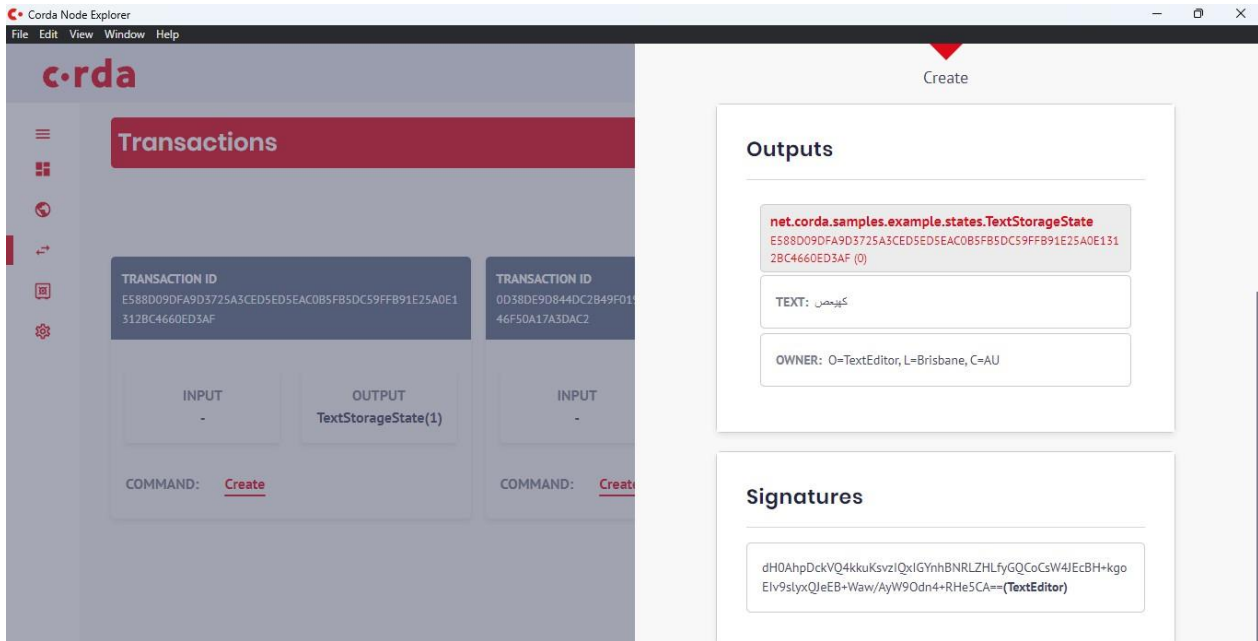


Figure 19 Vault State

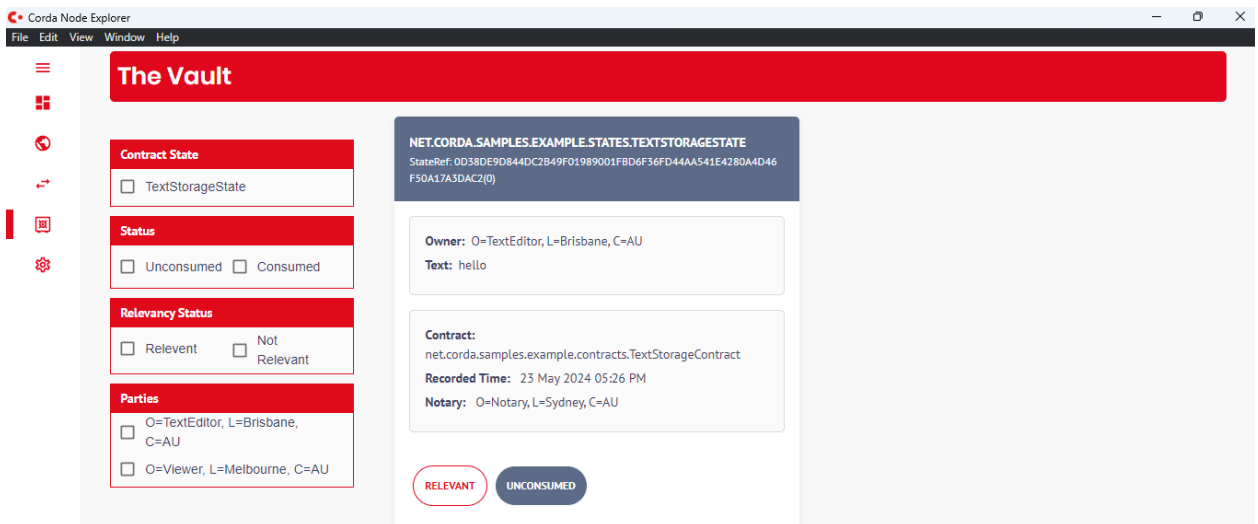


Figure 20 Settings to run Corda Explorer

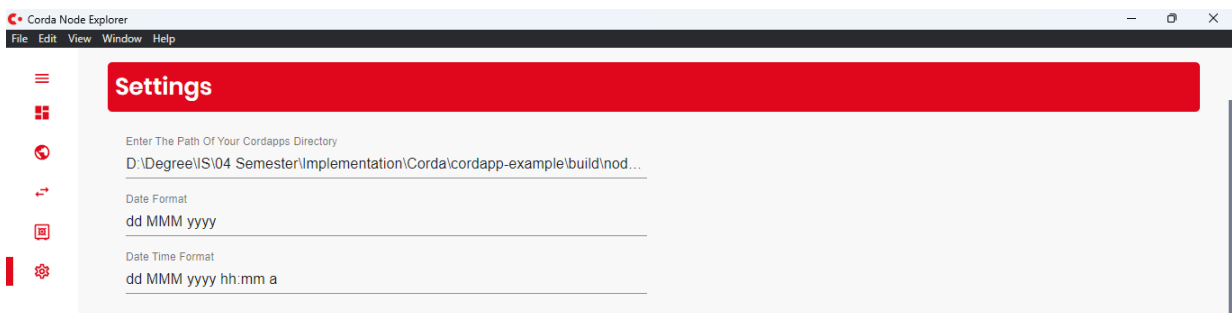
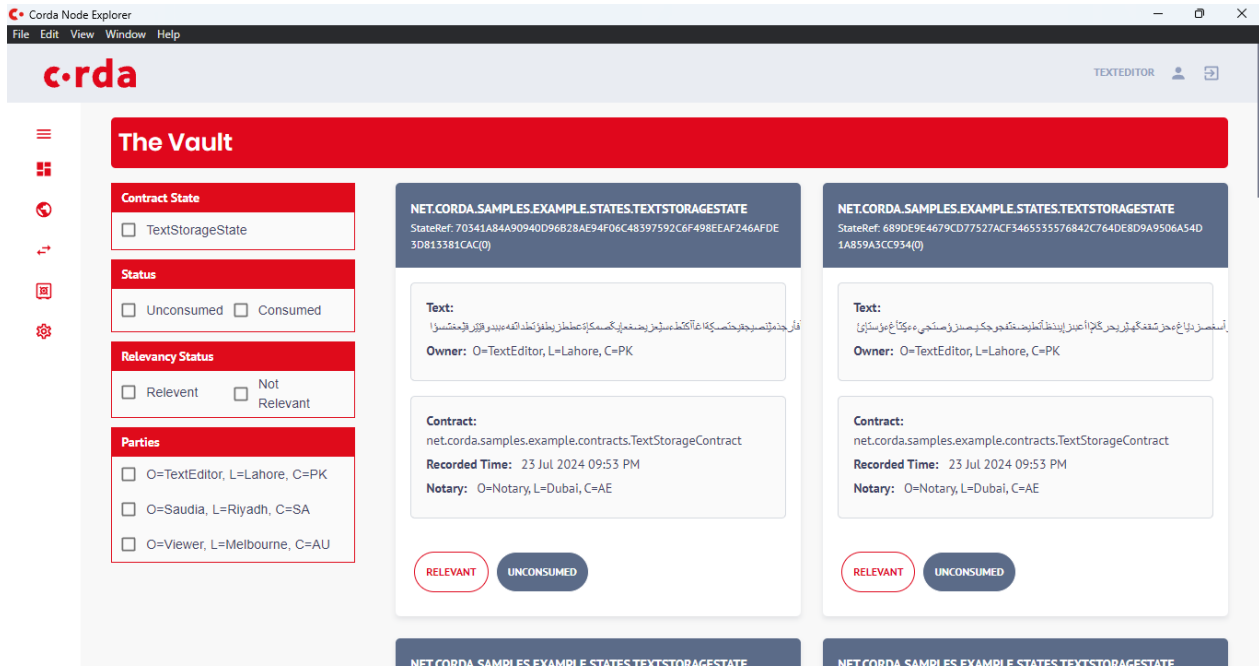




Figure 21 The Vault of Corda Editor Node



### 5.3 Implementation Flow

#### 5.3.1 Client Endpoint Api

- A client web application is designed for user interaction. It is accessible on localhost port 50005. To open the client web application, navigate to: <http://localhost:50005> after executing.
- Party A Server: `.\gradlew.bat runPartyAServer (Editor)`
- Party A Server: `.\gradlew.bat runPartyBServer (Viewer)`

#### 5.3.2 Transactions

Here are the commands and URLs for various transactions and interactions with the application:

##### 5.3.2.1 Save Text:

URL: <http://localhost:50005/save-text>

```
curl -X POST http://localhost:50005/save-text -H "Content-Type: application/x-www-form-urlencoded" -d "text=Arabic Text Here "
```

##### 5.3.2.2 Save Texts with Count:

```
curl -X POST http://localhost:50005/save-texts -H "Content-Type: application/x-www-form-urlencoded" -d "text= Arabic Text Here &count=10"
```

##### 5.3.2.3 Reading Text by Hash

To read text by hash, use the following URL:

<http://localhost:50005/read-text?hash=DDA37C2DF75FB78941075096AB4F7473B0DFFE3F1C5AB2E2A4CD24EEACF4AA44>

### 5.3.2.4 My Texts:

*http://localhost:50005/my-texts*

### 5.3.2.5 Performance Testing

To perform and analyze the application's performance, use the following URLs and commands:

### 5.3.2.6 Performance Test:

*URL: http://localhost:50005/performance-test*

*curl -X GET <http://localhost:50005/performance-test>*

*http://localhost:50005/performance-test?numTransactions=10*

### 5.3.3 Vault Query Command on Running Node Console:

*run vaultQuery contractStateType: net.corda.samples.example.states.TextState*

```
Mon Jun 03 10:00:40 PKT 2024>>>
Mon Jun 03 10:00:40 PKT 2024>>> run vaultQuery contractStateType: net.corda.samples.example.states.TextStorageState
states:
- state:
  data: !<net.corda.samples.example.states.TextStorageState>
    text: "hello"
    owner: "0=TextEditor, L=Brisbane, C=AU"
    contract: "net.corda.samples.example.contracts.TextStorageContract"
    notary: "0=Notary, L=Sydney, C=AU"
    encumbrance: null
    constraint: !<net.corda.core.contracts.SignatureAttachmentConstraint>
      key: "aSq9DsNNvGhYxYyqA9wd2eduEAZ5AXWgJTbTEw3G5d2maAq8vtLE4kZHgCs5jcB1N31cx1hpsLeqG2ngSysVHqcXhbNts6SkRWDaV7xNcr6MtcbufGUchxredBb6"
  ref:
    txhash: "0D38DE9D844DC2B49F01989001FBD6F36FD44AA541E4280A4D46F50A17A3DAC2"
    index: 0
- state:
  data: !<net.corda.samples.example.states.TextStorageState>
    text: "?????"
    owner: "0=TextEditor, L=Brisbane, C=AU"
    contract: "net.corda.samples.example.contracts.TextStorageContract"
    notary: "0=Notary, L=Sydney, C=AU"
    encumbrance: null
    constraint: !<net.corda.core.contracts.SignatureAttachmentConstraint>
      key: "aSq9DsNNvGhYxYyqA9wd2eduEAZ5AXWgJTbTEw3G5d2maAq8vtLE4kZHgCs5jcB1N31cx1hpsLeqG2ngSysVHqcXhbNts6SkRWDaV7xNcr6MtcbufGUchxredBb6"
  ref:
    txhash: "E588D09DFA9D3725A3CED5ED5EAC0B5FB5DC59FFB91E25A0E1312BC4660ED3AF"
    index: 0
statesMetadata:
- ref:
  txhash: "0D38DE9D844DC2B49F01989001FBD6F36FD44AA541E4280A4D46F50A17A3DAC2"
  index: 0
  contractStateClassName: "net.corda.samples.example.states.TextStorageState"
  recordedTime: "2024-05-23T12:26:15.026Z"
```

### 5.3.4 Gradle Commands:

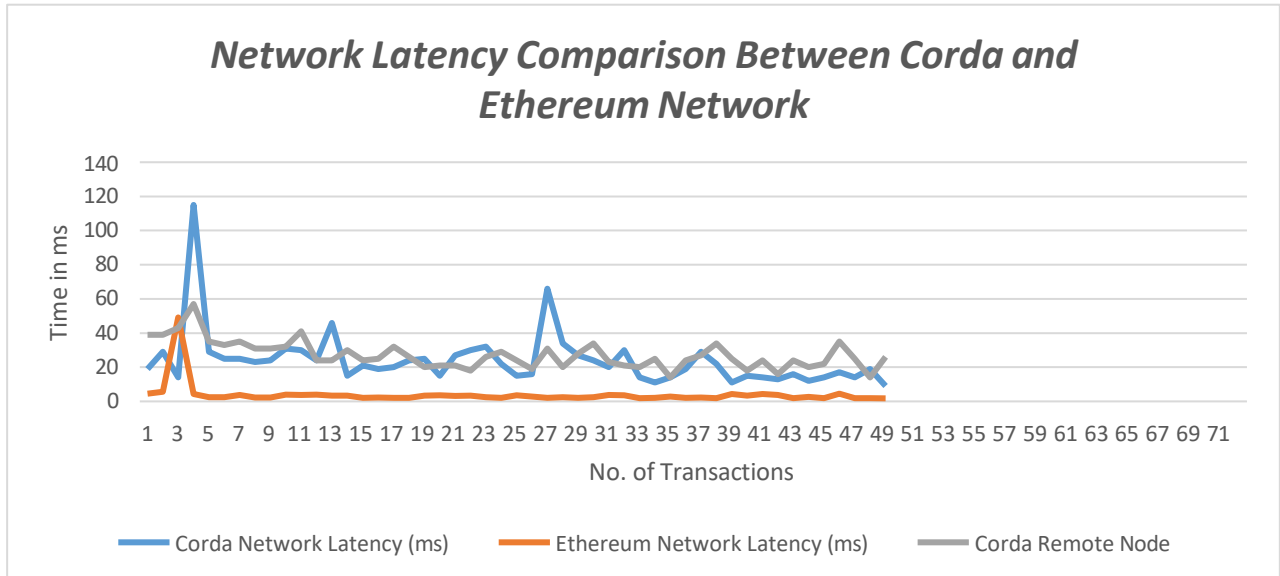
- - Refresh dependencies:

*./gradlew.bat --refresh-dependencies*

- - Run Party A Server:

*.\gradlew.bat runPartyAServer*

**Figure 22 Network Latency Comparison Between Corda and Ethereum Network**



## 5.4 Results

### 5.4.1 Comparison of Network Latency Between Corda and Ethereum

The graph here is depicting network latency (in milliseconds) of transactions on the Corda and Ethereum networks. Below is a detailed analysis based on the provided values.

#### 5.4.2 Corda Network Latency

- Minimum Latency: 9 ms
- Maximum Latency: 115 ms
- Average Latency: 23.57 ms

#### 5.4.3 Ethereum Network Latency

- Minimum Latency: 1.7805 ms
- Maximum Latency: 49.1426 ms
- Average Latency: 3.04 ms

#### 5.4.4 Observations

##### 5.4.4.1 Range of Latency:

- **Corda:** The latency ranges from 4 ms to 115 ms. The average latency is reasonably low, with most values clustering in between 14 ms to 30 ms, revealing stable network performance.
- **Ethereum:** The latency ranges from 1.7805 ms to 49.1426 ms. Despite the occasional high latency, Ethereum generally maintains a low latency specially on ganache blockchain.
- **Remote Node:** The Corda remote node values range from 14 to 57. These values are also in between the range of Corda latency on local network, which suggests that remote nodes might not be the primary factor affecting latency.

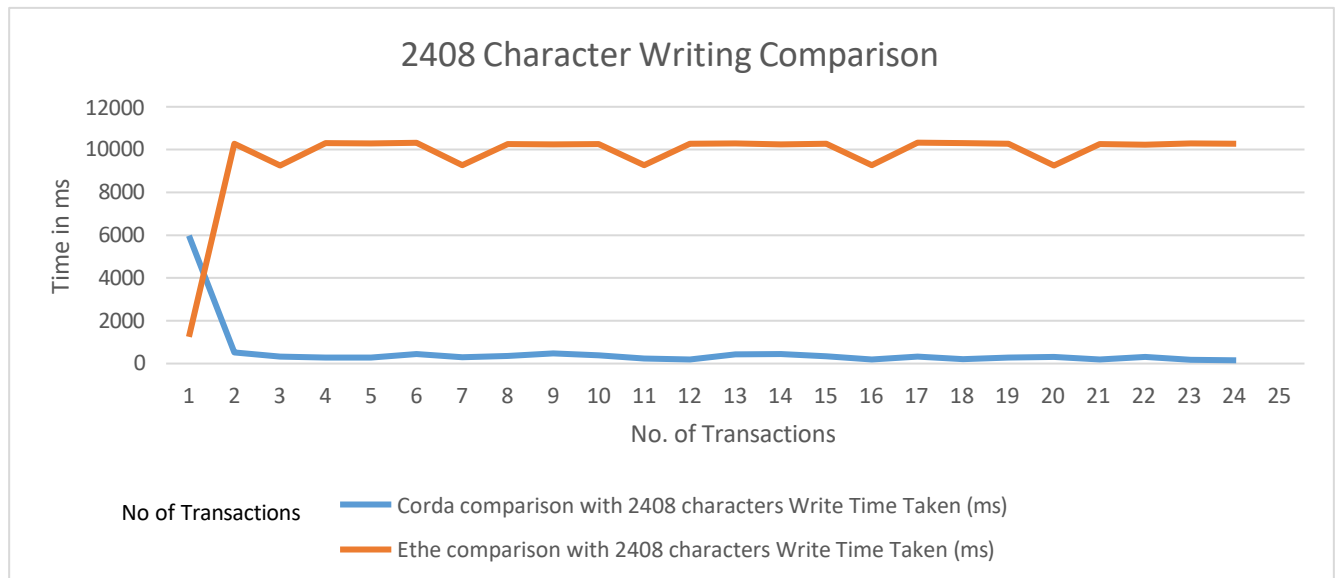
##### 5.4.4.2 Consistency:

- **Corda:** The data shows a wide range of latency values, suggesting variability in the

network's performance.

- **Ethereum:** Ethereum exhibits more consistency with the majority of latency values clustering around the lower end of the spectrum.

**Figure 23 Corda vs Ethereum 2408 Character Writing Comparison**



#### 5.4.5 Detailed Comparison of Write Time Between Corda and Ethereum

The graph analysing the data of 2408 char long and comparing the write time (in milliseconds) of transactions on the Corda and Ethereum networks. Here is a detailed analysis based on the provided values:

##### 5.4.5.1 Corda Write Time

- Minimum Write Time: 152 ms
- Maximum Write Time: 5979 ms (first few transactions to initiate the network, certificates etc)
- Average Write Time: 464.5 ms

##### 5.4.5.2 Ethereum Write Time

- Minimum Write Time: 9254.3519 ms
- Maximum Write Time: 10325.0422 ms
- Average Write Time: 10265.524 ms

##### 5.4.5.3 Observations

- **Corda:** The write time ranges from 152 ms to 5979 ms. This indicates that while Corda can perform writes quickly in some cases, there are instances where the write time is significantly higher.
- Justification
  - The first transaction in Corda tends to take more time than subsequent transactions due to several initialization processes and network-related factors that occur

primarily during the first transaction. Here are the key reasons:

- **Node Warm-up:** When a Corda node starts, it requires some time to initialize its internal services, load configurations, and set up network connections. This initialization can cause the first transaction to be delayed as these processes complete.
  - **Network Handshakes:** The first transaction often has an influence on initial network handshakes between nodes. This includes setting up secure connections checking certificates, and making sure the nodes are authenticated. These handshakes can add delays to the first transaction.
  - **Class Loading and JVM Warm-up:** Corda nodes run on the Java Virtual Machine (JVM). The first transaction might need to load classes and JAR files, which the JVM doesn't have preloaded. Later transactions work faster because these resources are already in memory.
  - **Database Connections:** Setting up initial database connections and making any needed schema changes or migrations can slow down the first transaction. After these connections are in place later transactions can reuse them, which cuts down their wait time.
  - **Transaction Validation:** The first transaction might need to go through initial checks such as loading the required smart contract code and checking the transaction against the current state of the ledger. While this happens for all transactions, the first one has to deal with the extra work of loading and getting these parts ready.
  - **Node Cache Initialization:** Corda nodes keep caches to store data they often need. The first transaction might need to set up and fill these caches, which can take extra time. Later transactions are quicker because they use caches that are already full.
  - **Network Map Service Lookup:** The first transaction might need to search the network map service to find details about other nodes in the network. This service gives info on the identities of nodes and where to find them on the network.
  - **Notary Interaction:** The first transaction typically involves interaction with a notary service for transaction validation and conflict resolution. Initial communication with the notary can involve setup time that is not required for later transactions.
  - Overall, the increased time for the first transaction is primarily due to the initialization and setup processes that are amortized across subsequent transactions. Once these initial steps are completed, the node can process later transactions more efficiently, leading to reduced latency.
- **Ethereum:** The write time ranges from 9254.3519 ms to 10325.0422 ms, indicating a consistently high write time.

#### 5.4.5.4 Consistency:

- **Corda:** The data shows a wide range of write times, suggesting variability in the network's performance.
- **Ethereum:** Ethereum exhibits more consistency with write times clustering around the

higher end of the spectrum.

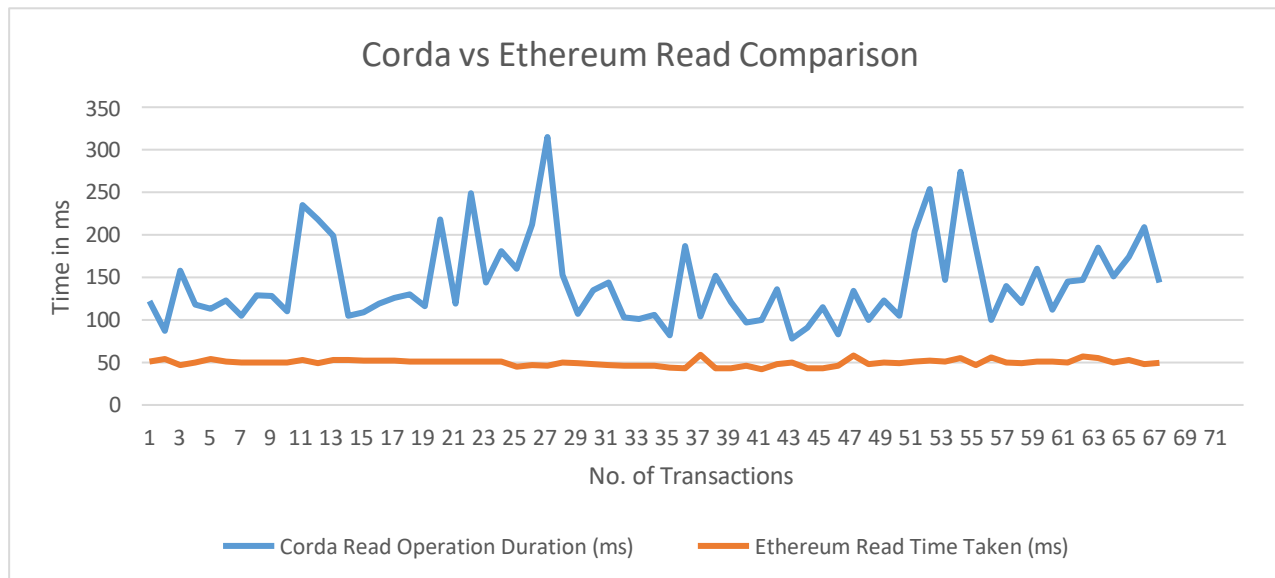
#### 5.4.5.5 Performance Comparison:

- In most cases, Corda demonstrates significantly lower write times compared to Ethereum. The average and median values are both much lower for Corda, indicating quicker write operations on average.

#### 5.4.5.6 Conclusion

Corda generally provides lower, and more variable write times compared to Ethereum. For applications requiring faster write operations, Corda might be the preferable choice. However, the variability in Corda's write times should be taken into consideration for applications requiring consistent performance.

**Figure 24 Corda Vs Ethereum Read Comparison**



#### 5.4.6 Detailed Comparison of Read Time Between Corda and Ethereum

Given data compares the read time (in milliseconds) of transactions on the Corda and Ethereum networks where the text string is of 2408 char long. Here is a detailed analysis based on the provided values:

##### 5.4.6.1 Corda Read Time

- Minimum Read Time: 78 ms
- Maximum Read Time: 315 ms
- Average Read Time: 144 ms

##### 5.4.6.2 Ethereum Read Time

- Minimum Read Time: 42 ms
- Maximum Read Time: 59 ms
- Average Read Time: 50 ms

### 5.4.6.3 Observations

#### 5.4.6.3.1 Range of Read Times:

- **Corda:** The read time ranges from 78 ms to 315 ms. This indicates some spikes and high variability in read performance as compared to Ethereum, but graph is linear in nature which not much difference. Additionally, this application is not a critical application where delay of seconds in reading the data can affects someone's life.
- **Ethereum:** The read time ranges from 42 ms to 59 ms, showing much less variability compared to Corda.

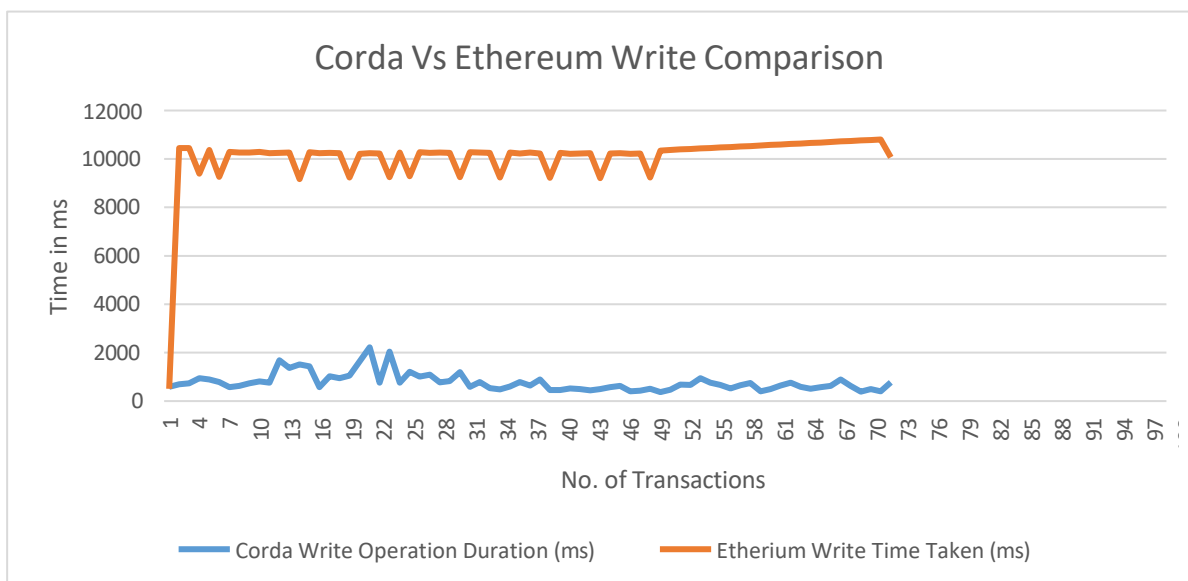
#### 5.4.6.3.2 Consistency:

- **Corda:** The data shows a wide range of read times, suggesting variability in the network's performance. It might be the due to my systems specifications.
- **Ethereum:** Ethereum exhibits more consistency with read times clustering around the lower end of the spectrum.

#### 5.4.6.4 Performance Comparison:

- **Read Time:** Ethereum demonstrates significantly lower and more consistent read times compared to Corda. The average and median values are both much lower for Ethereum, indicating quicker and more reliable read operations.

*Figure 25 Corda Vs Ethereum Write Comparison*



### 5.4.7 Detailed Comparison of Write Operation Duration Between Corda and Ethereum

This data about writing transactions is making significance change while comparing the write operation duration (in milliseconds) of transactions on the Corda and Ethereum networks. Here is a detailed analysis based on the provided values:

### 5.4.7.1 Corda Write Operation Duration

- Minimum Write Duration: 371 ms
- Maximum Write Duration: 2221 ms
- Average Write Duration: 777 ms

### 5.4.7.2 Ethereum Write Time Taken

- Minimum Write Duration: 507 ms
- Maximum Write Duration: 10803 ms
- Average Write Duration: 10180.65 ms

### 5.4.7.3 Observations

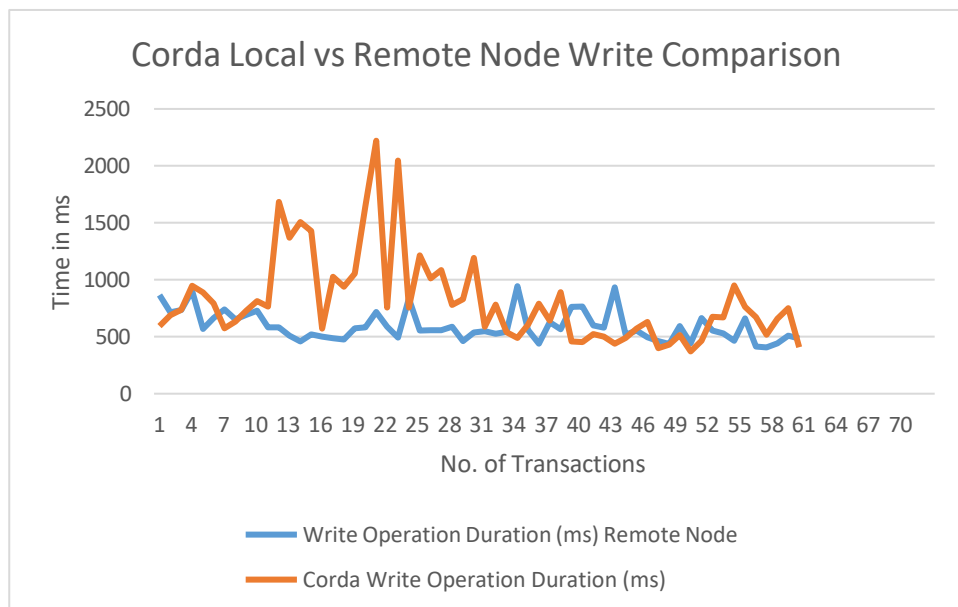
#### 5.4.7.3.1 Range of Write Durations:

- **Corda:** The write duration ranges from 371 ms to 2221 ms. This indicates a moderate variability in write performance.
- **Ethereum:** The write duration ranges from 507 ms to 10803 ms, showing degraded performance while writing and generally much longer durations compared to Corda.

### 5.4.7.4 Performance Comparison:

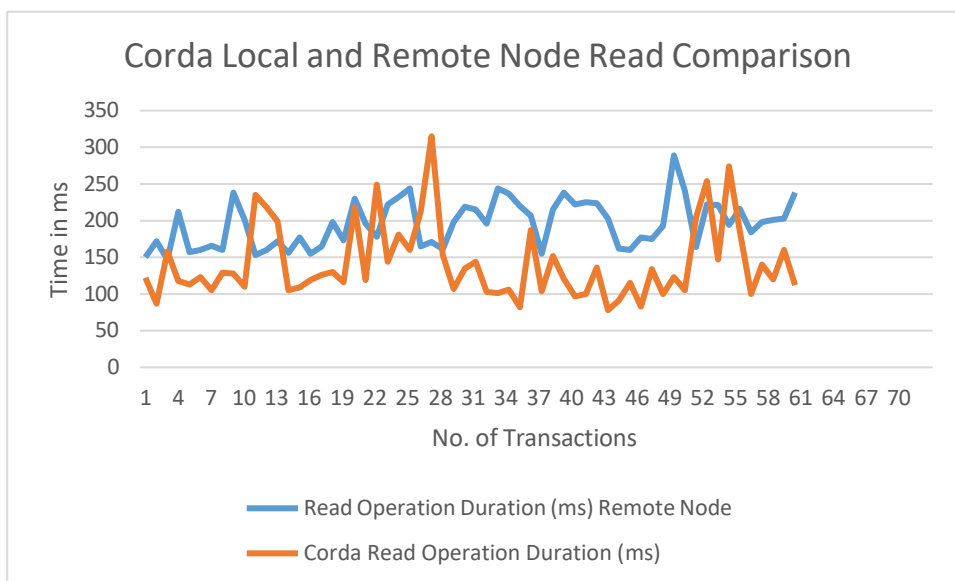
- **Write Duration:** Corda demonstrates significantly lower write durations compared to Ethereum. The transaction and average value are considerably lower for Corda, indicating quicker and more reliable write operations.

*Figure 26 Corda Local and Remote Node Write Comparison*





**Figure 27 Corda Local and Remote Node Read Comparison**



**5.4.8 Corda Local vs Remote Write and Read Comparison**

- o Interestingly, adding remote node using virtual machine enhanced the write and read performance marginally, due to better resource management of system. So, there is no difference adding remote nodes.

**5.4.9 Conclusion**

Corda provides lower and efficient write durations compared to Ethereum. For applications requiring fast and predictable write operations, Corda might be the preferable choice. Ethereum's longer and more variable write durations could impact performance in applications where timely data writing is critical.

**Table 7 Security Analysis**

<b>Security-Related Benefit</b>	<b>Corda</b>	<b>Ethereum</b>
<b>Confidentiality and Privacy</b>	Selective data sharing	Shared in a Ethereum network gives limited privacy
<b>Fine-Grained tuning for Access Control</b>	Granular level control over data	Access controls are limited
<b>Identity in the Network</b>	For Identification X.509 certificates used	Public key cryptography used
<b>Immutable Transactions</b>	Hash taken Cryptographically ensures immutability	Consensus mechanisms and Hashing ensures Immutability
<b>Programming Languages for Secure</b>	Kotlin and Java languages	Solidity and Vyper languages

<b>Security-Related Benefit</b>	<b>Corda</b>	<b>Ethereum</b>
<b>Smart Contracts</b>		
<b>Secure Channels</b>	Private channels used for secure communication	Public transactions visible to everyone by default

## 6 CONCLUSION AND FUTURE WORK

Today's digital age has revolutionized the way we access, store, and share information, posing significant challenges for maintaining the integrity and authenticity of digital content, especially for valuable resources like digital Islamic assets. Regular centralized systems aren't doing enough to protect these assets from tampering, changes without permission, and data theft. Blockchain technology provides a strong answer. It creates a decentralized, transparent, and unchangeable record, which keeps digital Islamic content safe and reliable.

Blockchain makes things more authentic, easier to track with consensus-based data management and cryptographic security. The implementation of smart contracts can further streamline content management and reduce any discrepancies and disputes by the removing intermediaries. It is possible to build a safe place to create, share, and save digital Islamic asset using blockchain. Blockchain isn't just about upgrading technology but something we need to do in order to safeguard and ensure the precision and sanctity of online Islamic materials and assets for generations to come.

### 6.1 Future Work

Future research in the blockchain domain can explore several avenues to further enhance the preservation and management of digital Islamic assets as proffered along with emerging threats on the blockchain with its mitigation.

- **Integration with Artificial Intelligence (AI):** AI based services for automated verification and validation of digital Islamic content can automatically validate the content by reducing manual interference. AI can help in detecting anomalies, unauthorized modifications, and ensuring compliance with religious and scholarly standards as oracle services.
- **Scalability Solutions:** Will be crucial to handle the growing volume of digital Islamic assets and number of nodes along with increasing network performance.
- **Interoperability with Existing Systems:** Researching methods to seamlessly integrate blockchain technology with existing digital libraries, databases, and content management systems will ensure a smooth transition and wider adoption of blockchain-based solutions.
- **Enhanced Security Protocols:** Developing advanced cryptographic techniques and security protocols to further safeguard digital Islamic assets against evolving cyber threats and attacks.
- **There are many sophisticated attacks which need to be covered as under:-**
- **Quantum attacks:**  
Quantum computing present a major threat[27] to blockchains due to their capability in solving complex problems. Quantum computers have the possibility to easily break existing encryption techniques[28] and may provide enough resources to perform 51% attacks in the future (Figure 5 shows various types of attacks possible of blockchain). Various studies such as References 29-33 have discussed such security issues.
- **Scalability:**  
Many efficient consensus mechanisms are being developed to reduce the energy consumption and the time taken to process a transaction. However, blockchain still faces scalability issues when it

comes to the number of transactions it can process per unit time.[34]

- **Protecting blockchain from intelligent attacks:** With the increasing possibility of more advanced types of attacks such as machine learning and game-theory based attacks on blockchain networks[35-36] it has become a necessity to secure blockchain against such attacks.
- **Reducing computational power usage:** Blockchain, in general, requires high computational power which is a drain on resources. This hinders the development of the technology for many applications such as drone/UAV networks [37] where computational power is scarce.

## 6.2 Acknowledgement

The authors extend their deepest appreciation to Professor Dr. Shahzaib Tahir for his exceptional guidance and unwavering support throughout our research journey. Dr. S. Tahir has been a driving force behind our pursuit of knowledge, challenging us to explore new horizons and pushing the boundaries of our understanding. We are truly grateful for the mentorship of Professor Dr. S. Tahir, as he not only enriched our research skills but has also left an indelible mark on our academic pursuits.

## References

1. L. Goyal, M. Raman, P. Diwan, M. K. Vijay, "A Robust method for integrity protection of digital data in text document watermarking", *International Journal for Innovative Research in Science & Technology*, vol. 6, PP. 14-18, 2014.
2. M. Kaur and K. Mahajan, "An Existential Review on Text Watermarking Techniques," *International Journal of Computer Applications*, vol. 120, no. 18. Foundation of Computer Science, pp. 29–32, Jun. 18, 2015. doi: 10.5120/21330-4300.
3. Chin-Chen Chang, Kuo-Feng Hwang, and Min-Shiang Hwang, "A block based digital watermarks for copy protection of images," Jan. 1999, doi: <https://doi.org/10.1109/apcc.1999.820427>.
4. C. Y. Lin, C. C. Wu, M. S. Hwang, "Research on e-book security tracking schemes," *International Journal of Network Security*, vol. 23, no. 4, pp. 549-557, 2021.
5. C.-Y. Tsai, C.-Y. Yang, I.-C. Lin, and M.-S. Hwang, "A Survey of E-book Digital Right Management.," *Int. J. Netw. Secur.*, vol. 20, pp. 998–1004, Jan. 2018.
6. C.-C. Chang, K.-F. Hwang, and M.-S. Hwang, "A Digital Watermarking Scheme Using Human Visual Effects," *Informatica (slovenia)*, vol. 24, no. 4, Jan. 2000.
7. C.-C. Chang, K.-F. Hwang, and M.-S. Hwang, "A FEATURE-ORIENTED COPYRIGHT OWNER PROVING TECHNIQUE FOR STILL IMAGES," *International Journal of Software Engineering and Knowledge Engineering*, vol. 12, no. 03, pp. 317–330, Jun. 2002, doi: <https://doi.org/10.1142/s0218194002000937>.
8. Chou, Jue-Sam & Chen, Yalin & Chan, Chung-Ju. (2007). Cryptanalysis of Hwang-Chang's a Time-Stamp Protocol for Digital Watermarking. *IACR Cryptology ePrint Archive*, vol. 2007, pp. 4, 2007.
9. C.-C. Chang, "Digital watermarking of images using neural networks," *Journal of Electronic Imaging*, vol. 9, no. 4, p. 548, Oct. 2000, doi: <https://doi.org/10.1117/1.1289357>.
10. C.-C. Wu, S.-J. Kao, W.-C. Kuo, and M.-S. Hwang, "A Robust-Fragile Watermarking Scheme for Image Authentication," Jan. 2008, doi: <https://doi.org/10.1109/icicic.2008.616>.
11. C.-C. Chang, K.-F. Hwang, and M.-S. Hwang, "A Digital Watermarking Scheme Using Human Visual Effects," *Informatica (slovenia)*, vol. 24, no. 4, Jan. 2000.
12. M. R. Xie, C. C. Wu, J. J. Shen, M. S. Hwang, "A survey of data distortion watermarking relational databases", *International Journal of Network Security*, vol. 18, no. 6, pp. 1022-1033, 2016.
13. M.-R. Xie, Chia-Chun Wus, J.-J. Shen, and M.-S. Hwang, "A Survey of Data Distortion Watermarking Relational Databases," *International journal of network security*, vol. 18, no. 6, pp. 1022–1033, Nov. 2016, doi: [https://doi.org/10.6633/ijns.201611.18\(6\).03](https://doi.org/10.6633/ijns.201611.18(6).03).
14. H. Huang, J. Tan, X. Sun, and L. Liu, "Detection of Hidden Information in Webpage Based on Higher-Order Statistics," *Digital Watermarking*. Springer Berlin Heidelberg, pp. 293–302, 2009. doi: 10.1007/978-3-642-04438-0\_25.
15. Yung-Chen Chou, Kurnia Anggriani, Nan-I Wu, and Min-Shiang Hwang, "Research on E-book Text Copyright Protection and Anti-tampering Technology," *International Journal of Network Security*, vol. 23, no. 5, Sep. 2021, doi: 10.6633/IJNS.202109\_23(5).01.
16. S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography*

and Digital Watermarking. Boston, MA: Artech House, 2000.

17. H. Huang, X. Sun, Z. Li, and G. Sun, "Detection of Hidden Information in Webpage," Jan. 2007, doi: <https://doi.org/10.1109/fskd.2007.247>.
18. H. Huang, S. Zhong, and X. Sun, "An Algorithm of Webpage Information Hiding Based on Attributes Permutation," Aug. 2008, doi: <https://doi.org/10.1109/iih-msp.2008.195>.
19. I-Shi. Lee and W.-H. Tsai, "Secret Communication through Web Pages Using Special Space Codes in HTML Files," *International Journal of Applied Science and Engineering*, vol. 6, no. 2, pp. 141–149, Nov. 2008, doi: [https://doi.org/10.6703/ijase.2008.6\(2\).141](https://doi.org/10.6703/ijase.2008.6(2).141).
20. S. Inoue, K. Makino, I. Murase, O. Takizawa, T. Matsumoto, H. Nakagawa, "A Proposal on Information Hiding Methods using XML," Aug. 13, 2021. (*International Journal of Network Security*, Vol.23, No.5, PP.739-749, Sept. 2021 (DOI: 10.6633/IJNS.202109 23(5).01))
21. P. Sharma, R. Jindal, M. D. Borah, "Blockchain-based Integrity Protection System for Cloud Storage" in proceedings of 4th Technology Innovation Management and Engineering Science International Conference, (TIMES-iCON), Bangkok, Thailand, 2019
22. Y. Wang et al., "Security enhancement technologies for smart contracts in the blockchain: A survey," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12. Wiley, Aug. 16, 2021. doi: 10.1002/ett.4341.
23. L. Williams, "El Salvador Adopts Bitcoin as a Currency: 3 Reasons Why That Matters," MUO, Sep. 11, 2021. <https://www.makeuseof.com/el-salvador-adopts-bitcoin-reasons-why-that-matters/>
24. R. Hamood, I. Makhdoom, W. Iqbal, and T. Jamil, "Supply Chain Optimization in Cement Industry Using Blockchain Technology," 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, Dec. 04, 2023. doi: 10.1109/csde59766.2023.10487674.
25. M. Hashemi Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," *Managerial Finance*, vol. 46, no. 6. Emerald, pp. 715–733, Aug. 27, 2019. doi: 10.1108/mf-09-2018-0451.
26. B. Fu, "Application of Blockchain Technology in Cryptocurrency," *BCP Business & Management*, vol. 23. Boya Century Publishing, pp. 198–205, Aug. 04, 2022. doi: 10.54691/bcpbm.v23i.1351.
27. X. Zhang, F. Wu, W. Yao, W. Wang, and Z. Zheng, "Post-Quantum Blockchain over Lattice," *Computers, Materials & Continua*, vol. 63, no. 2, pp. 845–859, 2020, doi: <https://doi.org/10.32604/cmc.2020.08008>.
28. Joshi, Aayush & Kumbhar, Rutuja & Shetty, Harshith & Mehta, Akshat. (2022). Breaking RSA Encryption Using Quantum Computer.
29. D. Aggarwal, G. Brennen, T. Lee, M. Santha, and M. Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger*, vol. 3. University Library System, University of Pittsburgh, Oct. 17, 2018. doi: 10.5195/ledger.2018.127.
30. Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, and Y.-X. Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain," *IEEE Access*, vol. 6. Institute of Electrical and Electronics Engineers (IEEE), pp. 27205–27213, 2018. doi: 10.1109/access.2018.2827203.

31. A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732. Springer Science and Business Media LLC, pp. 465–467, Nov. 2018. doi: 10.1038/d41586-018-07449-z.
32. K. Ikeda, "Security and Privacy of Blockchain and Quantum Computation," *Advances in Computers*. Elsevier, pp. 199–228, 2018. doi: 10.1016/bs.adcom.2018.03.003.
33. B. Rodenburg and S. P. Pappas, "Blockchain and Quantum Computing," 16094, 2017, doi: 10.13140/RG.2.2.29449.13923.
34. S. Kim, Y. Kwon, and S. Cho, "A Survey of Scalability Solutions on Blockchain," 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE, Oct. 2018. doi: 10.1109/ictc.2018.8539529.
35. Z. Liu et al., "A Survey on Blockchain: A Game Theoretical Perspective," *IEEE Access*, vol. 7. Institute of Electrical and Electronics Engineers (IEEE), pp. 47615–47643, 2019. doi: 10.1109/access.2019.2909924.
36. V. Hassija, V. Chamola, G. Han, J. J. P. C. Rodrigues, and M. Guizani, "DAGIoV: A Framework for Vehicle to Vehicle Communication Using Directed Acyclic Graph and Game Theory," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4. Institute of Electrical and Electronics Engineers (IEEE), pp. 4182–4191, Apr. 2020. doi: 10.1109/tvt.2020.2968494.
37. V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149. Elsevier BV, pp. 51–61, Jan. 2020. doi: 10.1016/j.comcom.2019.09.021.
38. M. Deimel, M. Frentrup, and L. Theuvsen, "Transparency in food supply chains: empirical results from German pig and dairy production," *Journal on Chain and Network Science*, vol. 8, no. 1. Brill, pp. 21–32, Feb. 29, 2008. doi: 10.3920/jcns2008.x086.
39. Y. Ren et al., "Data Query Mechanism Based on Hash Computing Power of Blockchain in Internet of Things," *Sensors*, vol. 20, no. 1. MDPI AG, p. 207, Dec. 30, 2019. doi: 10.3390/s20010207.
40. G.-J. Ra, C.-H. Roh, and I.-Y. Lee, "A Key Recovery System Based on Password-protected Secret Sharing in a Permissioned Blockchain," *Computers, Materials & Continua*, vol. 65, no. 1. Computers, Materials and Continua (Tech Science Press), pp. 153–170, 2020. doi: 10.32604/cmc.2020.011293.
41. X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making Knowledge Tradable in Edge-AI Enabled IoT: A Consortium Blockchain-Based Efficient and Incentive Approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12. Institute of Electrical and Electronics Engineers (IEEE), pp. 6367–6378, Dec. 2019. doi: 10.1109/tii.2019.2917307.
42. Doku R, Rawat DB, Liu C. On the blockchain-based decentralized data sharing for event-based encryption to combat adversarial attacks. *IEEE Trans Netw Sci Eng*. 2020.
43. A. Kaur, A. Nayyar, and P. Singh, "BLOCKCHAIN," *Cryptocurrencies and Blockchain Technology Applications*. Wiley, pp. 25–42, May 22, 2020. doi: 10.1002/9781119621201.ch2.
44. V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in

- V2G Network,” IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5799–5812, Jun. 2020, doi: <https://doi.org/10.1109/tvt.2020.2967052>.
45. S. Goyal, “Centralized vs Decentralized vs Distributed,” Delta Exchange, Jul. 01, 2015. <https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868>
46. Y. Ren, F. Zhu, K. Zhu, P. K. Sharma, and J. Wang, “Blockchain-based trust establishment mechanism on the internet of multimedia things,” Multimedia Tools and Applications, vol. 80, no. 20, pp. 30653–30676, Aug. 2020, doi: <https://doi.org/10.1007/s11042-020-09578-y>. Hosen AS, Singh S, Sharma PK, et al. Blockchain-based transaction validation protocol for a secure distributed IoT network. IEEE Access. 2020;8:117266-117277.