#### table of Contents

CONTENTS PAGE NO.

1. Abstract ii
2. List of Figures iii
3. **INTRODUCTION 1**
   1. **BACKGROUND AND DEFINATIONS 1**
   2. **FUNDAMENTALS OF BLOCKCHAIN 4**
4. **LITERATURE REVIEW 7**
5. **PROBLEM IDENTIFICATION & OBJECTIVES**
   1. **EXISTING SYSTEM 11**
   2. **PROPOSED SYSTEM 13**
6. **SYSTEM METHODOLOGY**
   1. **USE CASE DIAGRAM 17**
   2. **SEQUENCE DIAGRAM 18**
   3. **ACTIVITY DIAGRAM 19**
   4. **CLASS DIAGRAM 20**
7. **OVERVIEW OF TECHNOLOGIES**
   1. **DJANGO FRAMEWORK 21**
   2. **BLOCKCHAIN TECHNOLOGY 22**
      1. **BLOCKCHAIN ARCHITECTURE 23**
   3. **CONSENSUS ALGORITHMS (PROOF-OF-WORK) 23**
   4. **JSON (JAVASCRIPT ORIENTED NOTATION) 25**
8. **IMPLEMENTATION**
   1. **SAMPLE CODES 26**
   2. **TESTING 29**
9. **RESULTS AND DISCUSSION**
   1. **RESULTS 36**
   2. **DISCUSSION ON GOAL OF PROJECT 39**
10. **CONCLUSION AND FUTURE SCOPE**
    1. **CONCLUSION 41**
    2. **FUTURE SCOPE 42**
11. **REFERENCES 43**

# Abstract

Blockchain technology has been seeing widespread interest as a means to ensure the integrity, confidentiality, and availability of data in a trustless environment. They are designed to protect data from both internal and external cyber-attacks by utilizing the aggregated power of the network to resist malicious efforts. In this article, we will create our decentralized messaging application utilizing the Ethereal Whisper protocol. Our application will be able to send encrypted messages both securely and anonymously. We will utilize the ethereal platform to deploy our blockchain network. This application would be resistant to most suppression tactics due to its distributed nature and Adaptability of its communication protocol.

1) Mist Browser: an interface to access various dApps.

2) Decentralized Applications.

3) Whisper: it is Ethereum’s P2P communication protocol for decentralized applications. P2P communication between nodes in the Whisper network utilizes the D Vp2p Wire Protocol. A dApp instance can create an identity within a node that is connected to Whisper. This identity is needed to send or receive messages. Once a message is sent, it is, in theory, supposed

to be routed through every Whisper node. This makes it necessary to implement a PoW algorithm to prevent denial-of-service (DoS) attacks. Messages are only processed and further routed if their PoW is found to exceed a predefined threshold.

## LIST OF FIGURES

FIGURES PAGE NO.

Fig. 1.1. Ethereal technology stack **3**

Fig 1.2. The information a block (transaction) **5**

Fig 1.3. Chord-based distributed system **6**

Fig 3.1. Stakeholders from the traditional IdMS model **12**

Fig. 3.2 Software network architecture **15**

Fig. 3.3 Message transmission process **16**

FIG 4.1 USE CASE DIAGRAM FOR USER **17**

Fig 4.2 SEQUENCE DIAGRAM OF THE APPLICATION **18**

Fig 4.2.1 Sequence of project in backend **18**

Fig 4.3 flow of data throughout the project **19**

Fig 4.4 SOME classes involved throughout the project **20**

Fig 5.1Long Term Support (LTS) versions of the softwarE **21**

Fig.5.2 Block structure **23**

FIG. 5.3 Proof of Work **24**

Fig.6.1 The user interaction page of the project **29**

Fig 6.2 local server on the particular port mentioned **30**

Fig 6.3 application on the particular port mentioned. **31**

Fig 6.4. INDEX PAGE WHERE MESSAGE IS ENTERED **32**

Fig 6.5 The message is displayed on the screen **33**

Fig 6.6 resynchronizing the second user’s blockchain as well **34**

Fig 6.7 TERMINAL OUTPUT FOR THE LOGS IN THE BACK-END SERVER **35**

Fig 6.8 OUTPUT FOR THE LOGS IN THE APPLICATION ON BROWSER. **35**

Fig 7.1 output after resynchronizing blockchain **36**

Fig 7.2 output after resynchronizing all user’s blockchain **37**

Fig 7.3. Brooklyn microgrid network **38**

Fig 7.4. Block generation time in Bitcoin **38**

Fig 7.5. Performance of dishonest miner **38**