

# TABLE OF CONTENTS

CONTENTS	PAGE NO.
i. Abstract	ii
ii. List of Figures	iii
<b>1. INTRODUCTION</b>	<b>1</b>
<b>1.1. BACKGROUND AND DEFINATIONS</b>	<b>1</b>
<b>1.2. FUNDAMENTALS OF BLOCKCHAIN</b>	<b>4</b>
<b>2. LITERATURE REVIEW</b>	<b>7</b>
<b>3. PROBLEM IDENTIFICATION &amp; OBJECTIVES</b>	
<b>3.1. EXISTING SYSTEM</b>	<b>11</b>
<b>3.2. PROPOSED SYSTEM</b>	<b>13</b>
<b>4. SYSTEM METHODOLOGY</b>	
<b>4.1. USE CASE DIAGRAM</b>	<b>17</b>
<b>4.2. SEQUENCE DIAGRAM</b>	<b>18</b>
<b>4.3. ACTIVITY DIAGRAM</b>	<b>19</b>
<b>4.4. CLASS DIAGRAM</b>	<b>20</b>
<b>5. OVERVIEW OF TECHNOLOGIES</b>	
<b>5.1. DJANGO FRAMEWORK</b>	<b>21</b>
<b>5.2. BLOCKCHAIN TECHNOLOGY</b>	<b>22</b>
<b>5.2.1. BLOCKCHAIN ARCHITECTURE</b>	<b>23</b>
<b>5.3. CONSENSUS ALGORITHMS (PROOF-OF-WORK)</b>	<b>23</b>
<b>5.4. JSON (JAVASCRIPT ORIENTED NOTATION)</b>	<b>25</b>
<b>6. IMPLEMENTATION</b>	
<b>6.1. SAMPLE CODES</b>	<b>26</b>
<b>6.2. TESTING</b>	<b>29</b>
<b>7. RESULTS AND DISCUSSION</b>	
<b>7.1. RESULTS</b>	<b>36</b>
<b>7.2. DISCUSSION ON GOAL OF PROJECT</b>	<b>39</b>
<b>8. CONCLUSION AND FUTURE SCOPE</b>	
<b>8.1. CONCLUSION</b>	<b>41</b>
<b>8.2. FUTURE SCOPE</b>	<b>42</b>
<b>9. REFERENCES</b>	<b>43</b>

# 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 Ethereum Whisper protocol. Our application will be able to send encrypted messages both securely and anonymously. We will utilize the ethereum 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 5.1 LONG 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