CHAPTER I
INTRODUCTION

1.1 Background

Research on the utilization of a Delay Tolerant Network (DTN) has emerged as a vital endeavor to ensure effective emergency communication when conventional communication infrastructure becomes inoperative [1]. DTN networks face vulnerabilities associated with non-cooperative nodes in message delivery, necessitating the establishment of adequate incentives to stimulate participation among these nodes [2]. Additionally, the collaborative efforts of message-sending nodes within DTN networks play a pivotal role, particularly in mitigating the challenges of limited communication accessibility during military operations and disasters [3] [4].

DTN exhibits distinctive characteristics compared to Internet Protocol (IP) networks. While IP networks rely on continuous end-to-end connectivity for data transmission, DTN is designed to advance wireless traffic even in challenging conditions, including situations involving hostile environments, jamming, or nodes that may be moved or damaged [5]. These unique attributes render DTN particularly well-suited to address various challenges, including extended delays, asymmetric data rates, sporadic connectivity, elevated error rates in harsh environments, and communication across vast distances encountered in interplanetary space [6]. These distinctions clearly differentiate DTN from IP networks.

As a complementary technology, the integration of blockchain can further enhance the capabilities of DTN networks, addressing the challenges of security, privacy, and communication reliability during emergencies or when conventional communication infrastructure falls short [7]. When considering the realm of blockchain technology, it is crucial to distinguish between blockchain DTN and blockchain IP, as they serve different networking environments. In situations where connectivity is intermittent, as in DTN, blockchain enables secure and disruption-resistant data storage and transactions, ensuring the safety and integrity of data even in unstable network conditions [8]. Meanwhile, blockchain IP primarily caters to networks based on IP, characterized by continuous connectivity like the internet, aiding in user identification, transparent transaction tracking, and data security through reliance on stable connectivity [9].

Integrating blockchain technology and DTN in military applications offers a

revolutionary solution to address the communication challenges often encountered in military operations within inaccessible and unstable network infrastructure environments [10]. Blockchain, with its high-security features and decentralized nature, ensures data integrity, transparency, and resistance to manipulation, which are crucial in the military context [11]. Meanwhile, DTN enables reliable and efficient communication in areas with limited or intermittent connectivity by storing and forwarding data until it can reach its final destination [12]. The combination of these technologies can enhance logistical efficiency, troop coordination, and information security, thereby supporting more effective and responsive military missions in various challenging battlefield conditions.

Additionally, DTN combined with blockchain is also suitable for disaster recovery communication systems [13]. In such scenarios, where conventional networks are often damaged or overloaded, DTN ensures message delivery despite network fragmentation, while blockchain provides data integrity and security. This combination can facilitate reliable and secure information exchange among rescue teams, aiding in coordination and resource allocation during critical times. Similarly, in remote rural areas lacking robust communication infrastructure, DTN with blockchain can enable secure and dependable communication for vehicular communications [14].

In this research, we investigate the integration of communication among nodes using blockchain technology within the DTN framework. Messages exchanged between nodes will be encrypted to enhance security and privacy, and all transaction records and message content will be securely stored on a private blockchain network. The study involves three research scenarios: a DTN without blockchain, a DTN with blockchain, and a security assessment of the blockchain. Within these scenarios, we utilize various DTN routing protocols, including Epidemic, Spray-and-Wait, MaxProp, First Contact, and Direct Delivery, to analyze their performance under the same conditions but with different protocols. Key performance metrics for the first two scenarios include delivery probability, overhead ratio, average latency, and average buffer time. For the blockchain, additional metrics such as block number, gas usage, and generated transaction hashes are considered. The third scenario focuses on evaluating the security aspects of the blockchain, including data integrity and privacy preservation. By evaluating these metrics, we aim to assess the system's efficiency using blockchain in DTNs, message delivery effectiveness, trade-offs in each metric, and security. The comparative analysis of these routing protocols will provide insights into the potential benefits and limitations of integrating blockchain technology into DTN environments, highlighting how differ-

ent routing strategies impact the overall performance and security of the network.

However, the majority of prior studies have yet to explore the specific dynamics of integrating blockchain technology into DTNs, particularly in the context of The ONE (Opportunistic Network Environment) simulation environment. The novelty of this research lies in the fact that, to the best of our knowledge, no previous studies have simulated the integration of DTN and blockchain on The ONE, explicitly showcasing the blockchain parameters used. This simulation platform offers a unique advantage due to its opportunistic network simulation capabilities. Our research is driven by the importance of secure and reliable communication in critical applications, where timely and trustworthy information exchange is paramount. The outcomes of this study have the potential to impact various domains, including emergency response and space communication, offering valuable insights into the development of more resilient and secure communication systems for the future.

1.2 Problem Identification

The problem identification in integrating blockchain technology into Delay Tolerant Networks (DTNs) encompasses several critical points. Firstly, despite DTN being recognized as a crucial solution for ensuring effective emergency communication, especially in military operations and remote areas, it remains vulnerable to non-cooperative nodes, necessitating adequate incentives to stimulate their participation. Secondly, while DTN offers advantages in challenging communication environments, integrating blockchain technology becomes essential to enhance security, privacy, and communication reliability in situations where conventional infrastructure is insufficient. However, there needs to be more in-depth research exploring this integration, particularly in simulated environments like The ONE, explicitly showcasing the blockchain parameters used. This highlights the need for comprehensive security evaluations of blockchain usage in DTNs. Additionally, evaluating the interaction between various DTN routing protocols and blockchain integration is crucial to understanding how it improves network efficiency and security, emphasizing the importance of assessing data integrity and user privacy in unstable network conditions.

1.3 Objective and Contributions

In this section, we outline the objective and contributions of our research, focusing on investigating the integration of blockchain technology into DTNs to bolster

security, privacy, and communication reliability in challenging environments.

1. **Objective:**

    - To investigate the integration of blockchain technology into DTNs to enhance security, privacy, and communication reliability in challenging environments.

2. **Contributions:**

    - Analysis of the performance of DTNs with and without blockchain integration under various routing protocols, including Epidemic, Spray-and-Wait, MaxProp, First Contact, and Direct Delivery.
    - Evaluation of key performance metrics such as delivery probability, overhead ratio, average latency, and average buffer time for both scenarios.
    - Examination of additional blockchain-specific metrics, including block number, gas usage, and generated transaction hashes.
    - Assessment of the security aspects of blockchain integration in DTNs, focusing on data integrity and privacy preservation.
    - Comparative analysis of the impact of different routing strategies on the overall performance and security of DTN networks with blockchain integration.

1.4 Scope of Work

The scope of this research encompasses the following key activities:

1. Investigating the integration of private blockchain technology into DTNs to enhance security, privacy, and communication reliability.
2. Implementing and simulating DTNs with and without blockchain integration using The ONE simulation environment.
3. Analyzing the performance of various DTN routing protocols, including Epidemic, Spray-and-Wait, MaxProp, First Contact, and Direct Delivery, in scenarios with and without blockchain.
4. Evaluating key performance metrics such as delivery probability, overhead ratio, average latency, and average buffer time for both scenarios.

5. Examining additional blockchain-specific metrics, including block number, gas usage, and generated transaction hashes.

6. Assessing the security aspects of blockchain integration in DTNs, focusing on data integrity and privacy preservation.

7. Conducting a comparative analysis of the impact of different routing strategies on the overall performance and security of DTN networks with blockchain integration.

1.5 Hypothesis

This research hypothesizes that integrating blockchain technology into DTNs will significantly enhance the security, privacy, and communication reliability of these networks in challenging environments. It is posited that blockchain can mitigate the vulnerabilities associated with non-cooperative nodes and ensure secure and reliable communication during emergencies, such as military operations, and in remote areas. Additionally, blockchain is expected to enable secure data storage and transaction handling in DTNs, even under conditions of intermittent connectivity and high error rates typical of hostile or remote environments. This integration should improve the overall performance of DTNs, especially when evaluated with various routing protocols like Epidemic, Spray-and-Wait, MaxProp, First Contact, and Direct Delivery. By enhancing message encryption and securing transaction records on a private blockchain, significant improvements in data integrity and privacy preservation are anticipated. The study aims to verify these hypotheses through comprehensive simulation and analysis using The ONE simulation environment, providing insights into the potential benefits and limitations of blockchain-integrated DTNs.

1.6 Methodology

This thesis is divided into 5 Work Packages (WP):

- **WP1:** Literature Review and Theoretical Framework
  This work package involves a comprehensive review of existing literature on DTNs and blockchain technology. It includes identifying gaps in current research, establishing the theoretical framework, and formulating the research questions and hypotheses.

- **WP2:** System Design and Implementation
  This work package focuses on the design and implementation of the DTN and blockchain integration. It includes setting up the simulation environment using The ONE and implementing various DTN routing protocols with and without blockchain integration.

- **WP3:** Simulation and Data Collection
  In this work package, extensive simulations will be conducted to collect data on the performance of DTNs with and without blockchain integration. This includes measuring key performance metrics such as delivery probability, overhead ratio, average latency, and average buffer time, as well as blockchain-specific metrics like block number, gas usage, and generated transaction hashes.

- **WP4:** Data Analysis and Security Assessment
  This work package involves analyzing the collected data to evaluate the performance and security aspects of blockchain integration in DTNs. It includes assessing data integrity, privacy preservation, and the impact of different routing strategies on overall network performance and security.

- **WP5:** Documentation and Reporting
  The final work package focuses on documenting the research findings and preparing the thesis report. It includes writing detailed descriptions of the methodology, results, discussions, and conclusions, as well as preparing for the final presentation and defense of the thesis.

1.7 Research Methodology

The research methodology comprises several key steps designed to investigate the integration of blockchain technology into DTNs systematically:

1. **Literature Review**
   A comprehensive literature review will be conducted to understand the current state of research on DTNs and blockchain technology. This involves:

   - Identifying key concepts, theories, and previous studies related to DTNs and blockchain.
   - Highlighting the gaps in existing research that this study aims to address.
   - Formulating research questions and hypotheses based on the identified gaps.

2. **System Design**
   The system design phase will focus on setting up the simulation environment and implementing the necessary protocols:

   - **Simulation Environment:** The ONE simulation platform will be used to create a realistic environment for testing.
   - **DTN Routing Protocols:** Various DTN routing protocols, including Epidemic, Spray-and-Wait, MaxProp, First Contact, and Direct Delivery, will be implemented.
   - **Blockchain Integration:** Blockchain technology will be integrated to enhance security and privacy. This includes encrypting messages and securely storing transaction records on a private blockchain network.

3. **Simulation and Data Collection**
   Extensive simulations will be run to collect performance data under different scenarios:

   - **Performance Metrics:** Key performance metrics such as delivery probability, overhead ratio, average latency, and average buffer time will be measured for both DTNs with and without blockchain integration.
   - **Blockchain-Specific Metrics:** Additional metrics specific to the blockchain, such as block number, gas usage, and generated transaction hashes, will be recorded.

4. **Data Analysis and Security Assessment**
   The collected data will be analyzed to evaluate the impact of blockchain integration on the performance and security of DTNs:

   - **Comparative Analysis:** A comparative assessment of the different routing protocols and their influence on network efficiency and security will be conducted.
   - **Security Assessment:** The analysis will focus on data integrity and privacy preservation, evaluating how blockchain integration enhances these aspects in DTNs.

5. **Documentation and Reporting**
   The final step involves documenting the research findings and preparing the thesis report:

- **Thesis Report:** Detailed descriptions of the methodology, results, discussions, and conclusions will be included in the thesis.
- **Presentation and Defense:** Preparation for the final presentation and defense of the thesis, ensuring that the findings are clearly communicated and defended.