DEMEDIA – DECENTRALIZED SOCIAL MEDIA PROTOCOL

2023-234

Project Proposal Report

IT20137496 - Dhananjani G. G. S.

B.Sc. (Hons) in Information Technology Specializing in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

March 2023

MECHANISM FOR DATA INTEGRITY PRESERVATION

2023-234

Project Proposal Report

IT20137496 - Dhananjani G. G. S.

Supervisor: Mr. Kavinga Abeywardena

Co-Supervisor: Miss Laneesha Ruggahakotuwa

B.Sc. (Hons) in Information Technology Specializing in Information Technology

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

March 2023

Declaration

"I declare that this is our own work, and this proposal does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to Sri Lanka Institute of Information Technology, the nonexclusive right to reproduce and distribute my dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books)."

Name	Student ID	Signature
Dhananjani G.G.S.	IT20137496	

The above candidates are carrying out research for the undergraduate Dissertation under my supervision.

Signature of the Supervisor: ……

Date: ……

Acknowledgment

I would like to express my sincere gratitude to my supervisor Mr. Kavinga Abeywardena, and the co-supervisor Miss Laneesha Ruggahakotuwa, for their guidance, support, and motivation throughout this research. I am also grateful to the Department of Information Technology at Sri Lanka Institute of Information Technology and the CDAP lecturers and staff for their assistance and providing the opportunity to undertake this research.

Abstract

The decentralized social media protocol is a modern technology that aims to address the issues of centralized social media platforms, including censorship and data privacy concerns. This protocol allows users to have control over their data. It enables users to communicate and interact with others without involving a central or single source.

Our research will involve developing a protocol called "DeMedia" that aims to resolve the limitations and constraints associated with centralized social media platforms. The DeMedia protocol will be designed to provide users with more control over their data and privacy. Through the development of this protocol, we aim to address the concerns of data privacy, security, and ownership, while providing users with a more private and safe social media experience.

The Data Integrity component of our research primarily focuses on preserving the integrity of user data. The aim of this component is to have a cryptographic system implemented that enables the secure storage of signed user data on the user's device. This mechanism will improve the security and reliability of the user's data by ensuring that it remains tamper-proof and unaltered. Develop an effective and efficient system that maintains user privacy and control while enhancing data integrity. Building user trust requires ensuring the legitimacy and authenticity of the data given on the platform. The data integrity component utilizes cryptographic techniques such as hashing mechanism and data encryption mechanisms to secure the data and prevent unauthorized modifications or access.

Ultimately, the decentralized social media protocol and its data integrity component provide a hopeful solution for developing a more transparent and secure social media platform. With the increasing of data privacy and censorship of user data, this technology could revolutionize the way people communicate and share information online.

Keywords: *Decentralized, Data Integrity, Privacy, Security, Protocol, Cryptographic Techniques, Hashing Mechanism*

TABLE OF CONTENT

List Of Figures

List Of Tables

List of Abbreviations

IPFS - InterPlanetary File System

DeSo - Decentralized Social

CBC - Cipher Block Chaining

1.0 INTRODUCTION

A Social media platform is a website or application that enables users to create and share information, communicate with others, and take part in social networking. Typically, social media platforms provide their users with the tools and capabilities they need to create and publish various types of content including text, images, videos, and audio. [1] These platforms have grown in popularity, and billions of people use them to communicate with friends and family, share information and news, and interact with community groups and cultures from across the globe. [2]

Social media platforms can be broadly categorized into two types as centralized and decentralized. At the moment, the majority of social media platforms are centralized, which means that they are owned and operated by a single entity and have a central server that manages all user data and content. And the platform owner has full control over the platform's features, policies, and access to user data. [3] Centralized social media platforms are convenient and easy to use, but they also present some risks in terms of data privacy and security. Users must trust the platform owner to manage their data responsibly, and there is always the risk of data breaches or abuse by the platform owner or their partners. [4]

Decentralized social media platforms are designed to distribute the control and ownership of the platform among its users, rather than being owned and operated by a single entity. Users have direct control over their data and content, which can help to strengthen privacy and security. User data and content are stored on a distributed network of computers. [5] Decentralized social media protocols use various mechanisms to ensure data integrity, including cryptographic hashing and encryption methods. By dispersing power and ownership among its users and ensuring data integrity, decentralized social media platforms can provide their users more control over their privacy, security, and decision-making. [6]

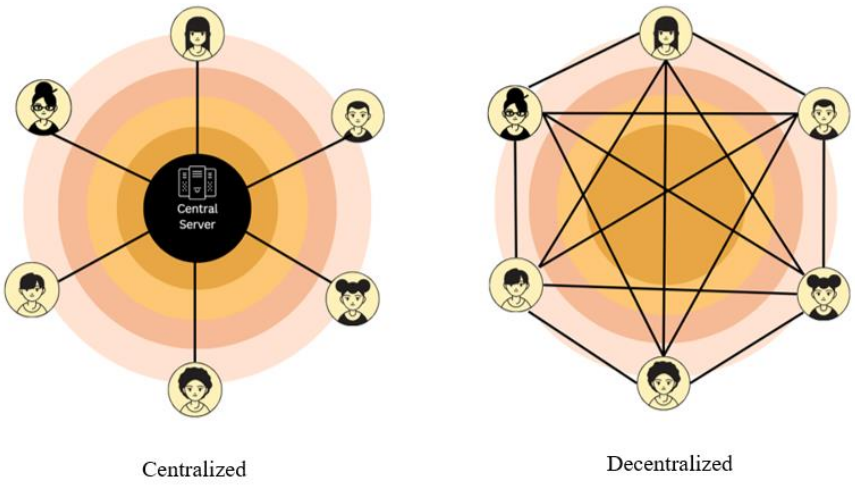

Figure 1.0.1: Centralized vs Decentralized

“DeMedia” is a decentralized social media protocol that allows anyone to build their own decentralized application using its data layer and caching mechanism. With DeMedia, even nontechnical users can easily deploy peers on their devices with low operational cost. To ensure the integrity of user data, DeMedia uses a cryptographic mechanism that publishes the hash of set of hashes on IPFS network. [7] This mechanism helps to ensure that user data cannot be tampered with or corrupted by anyone. It provides greater security and trust in the platform.

Data Integrity is a main aspect of any application. [8] And it is one of the key components of the decentralized social media protocol. Because in a decentralized environment, user data and information are stored on a distributed network of computers rather than a central server managed by the platform owner. The integrity of this data must be guaranteed to be unaltered and uncorrupted, as well as accurate and consistent. [9] Without data integrity, users could not have confidence in the platform's ability to preserve their data and might be afraid to utilize the platform. By ensuring data integrity, decentralized social media platforms can provide a secure and trustworthy environment for users to share and communicate without having to worry about the security of their data. Moreover, since the data is not owned by a single entity, hackers and other malicious attackers cannot exploit a single point of failure to their gain.

Currently, there are various mechanisms available to maintain the integrity of data in decentralized application. Therefore, as my research component, I try to implement a proper data integrity mechanism on top of IPFS. DeMedia, which is a decentralized social media protocol that stores user data on the user's device, letting them have full control over it and making changes as their discretion. As a result, there is less chance of data corruption or tampering by outside parties and users have more control over their data. [10] Ensuring data integrity means ensuring that user data is accurate, consistent, and secure from tampering or corruption. Decentralized social media platforms can secure user data even in the absence of a centralized authority by implementing data integrity methods including cryptographic hashing and data encryption.

It enables a way to validate the legitimacy of user data and content by implementing hashing algorithms as a cryptographic mechanism to establish a hash value for each piece of user-generated content or data. [11] Because each piece of data has a unique hash value. A different hash value will be generated if the data is modified or tampered with in any way by someone. The platform is able to identify any attempts to alter or tamper with the user data by comparing the original hash value to the recently generated hash value.

There are two approaches to measure the data integrity of decentralized social media protocols such as quantitatively and qualitatively. In quantitative measurements, the level of accuracy, consistency, and reliability of the data can often be evaluated

numerically. [12] Quantitative measures involve evaluating the redundancy and consistency of the data stored on the IPFS network, which provides a distributed file system. In Qualitative measures, it is possible to check the hash value or compare the encrypted data with the initial data to make sure it has not been modified. It implies non-numerical measurement of the data's reliability, credibility, and validity. Both quantitative and qualitative measures are important for evaluating the data integrity of decentralized social media protocols. [13]

1.1.Background and Literature

Data Integrity is a main aspect of both centralized and decentralized social media platforms. Considering the possibility of user data being altered or corrupted, which can cause erroneous information or compromising privacy and security. For instance, tampering with a user's private messages or personal information might have huge consequences for the user's privacy and security. [8] Therefore, data integrity has received increasing attention in many research.

In a decentralized social media platform, user data and content are stored on user's device and a distributed network such as IPFS network instead of a central server. [7] Hence, maintaining the accuracy, integrity, and security of user data requires assuring data integrity. Furthermore, establishing trustworthiness among users of a decentralized social media site requires data integrity. Users may be unwilling to use the system or share their private information if they do not feel secure that their data is accurate, reliable, and safe.

The amount of data that has to be saved is increasing fast in the big data era. As a result, due to its accessibility and huge capacity, cloud storage has become increasingly popular as a way to store information storage. To reduce expenses, certain cloud service providers, however, could remove information that is not usually accessed, which could lead to users losing important data. A new technique based on blockchain technology has been recommended for validating the integrity of recoverable information saved to the cloud storage in order to allay issues about data security and privacy. [14]

There are several benefits to using blockchain technology to preserve the integrity of information in decentralized social media networks, there are some possible drawbacks as well. [15] One of the main challenges with using blockchain for data integrity is scalability. A network of nodes that process blockchain transactions must decide on each transaction's legitimacy. The blockchain network could get slower and less effective as more transactions are added, which might result in delays and blocks. Decentralized social media networks that produce a lot of information and content could struggle with this issue in particular. [16]

DeMedia is not a blockchain-based decentralized social media network due to these difficulties with the blockchain. For address these concerns in integrity of user data, uses a method where a hash value of a user's data is created and encoded, and then stored on the user's device. And then a set of these hash values are also stored on the IPFS network. [7] IPFS is a distributed system that allows for the storage of immutable data, eliminates redundancy. Moreover, it offers address information for storage nodes to make it easier to discover files on the network. [17] When it comes to decentralized user data storage, IPFS has several advantages, including increased security,

performance, and reliability. [18] When a user wants to retrieve their data, DeMedia decrypts the hash value to ensure that the data hasn't been altered. In this manner, the data's integrity is ensured, and tampering is prevented.

DeMedia stores user's data as a hash value. The users' data can be hashed to generate a fixed-length digest that can then be signed with the user's private key. [19] As any modifications to the data will result in a different digest value and this assures that the data has not been altered.

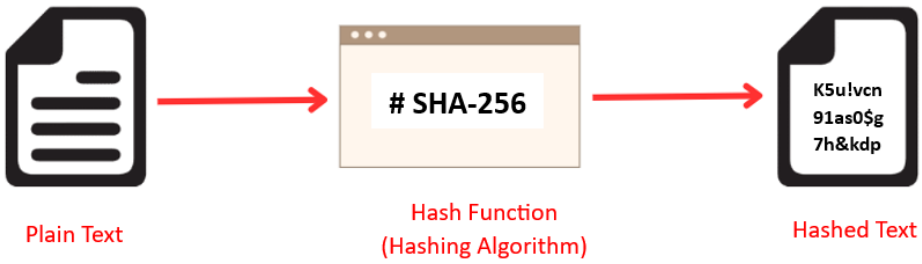

Figure 1.1.1: Hashing Algorithm

After generating hash value for user data, it can be signed using a digital signature. Digital signature is a cryptographic method that offers a way to determine the authenticity of messages. It ensures that the message is authentic and came from the specified source. The sender signed the message using the private key and the receiver can verify the message using sender's public key. Decentralized social media protocols can offer a secure and trustworthy platform for communication and data sharing by using digital signatures.

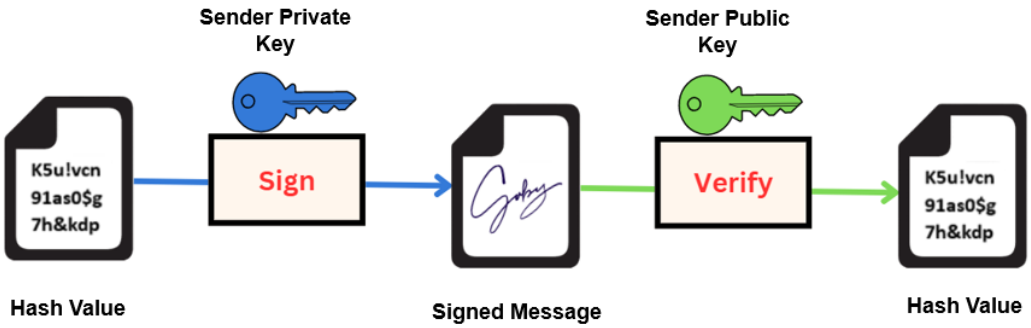

Figure 1.1.2: Digital Signature Mechanism

The digitally signed data is saved in the user's device. Then get the set of signed hash values which is saved in the user's device and generate a single hash value for the set of hashed data. The set of hash values can be a hundred or thousand hash values. After that, the hashed set of signed value is stored in the IPFS distributed network. To store in IPFS, the hashed value is split into smaller chunks using Cipher Block Chaining (CBC) encryption method, that is a mechanism for ensuring the integrity and confidentiality of the data. The hashed value is divided into blocks of a fixed size. When retrieving the data, storing the hash values on the IPFS network, and comparing them to the computed hash values ensure that the data has not been altered or corrupted.

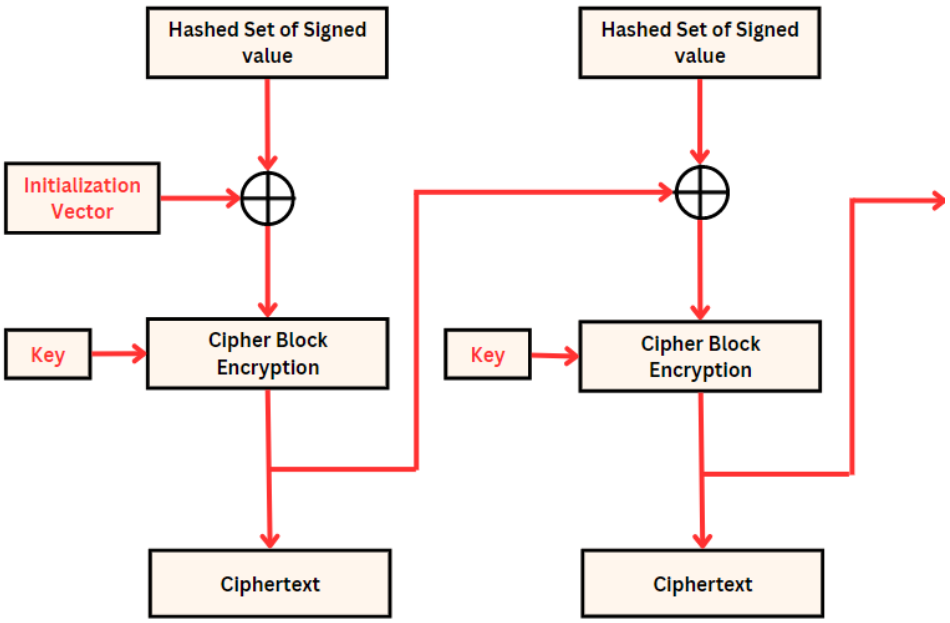

Figure 1.1.3: Cipher Block Chaining Encryption

1.2.Research Gap

The primary research gap in this research aims to fill the gap that exists in current methodologies in data integrity of decentralized social media platforms.

	Mastodon	**DeSo**	**DeMedia**
Generate hash for user data	Yes	Yes	Yes
Sign user data	Yes	Yes	Yes
Keep data Integrity in User's device	No	No	Yes
Use IPFS for keep Integrity	No	No	Yes

Table 1.2.1: Comparison of existing decentralized social media platforms

Mastodon is a popular decentralized social media platform which uses blockchain mechanism for store data. It generates hash values for user data and signs using digital signature. But it does not keep data with user device and does not use IPFS distributed network for store hashed and signed user data.

DeSo is a currently available decentralized social media platform. It uses first layer blockchain to build and scale storage-heavy applications to billions of users around the world. [20] Therefore, it does not keep data in user's device. By utilizing blockchain technology and decentralized infrastructure, DeSo is focused on providing a social media experience that is more transparent, reliable, and safe data processing and user centric. [21] It does not use IPFS network for store data.

Although Mastodon and DeSo are decentralized social media platforms, they have some issues because of using blockchain technology. There are some considerable drawbacks to blockchains. [22] Such as slower processing, harder to scaling, high power consumption, high cost and store immutable data. Therefore, it is not appropriate to use blockchain technology for a decentralized social media network.

However, although a lot of research has been done about data integrity of decentralized social media platforms, no research has been done to provide a data integrity mechanism for stored user hash data in user's device and stored set of signed hashes in IPFS distributed network. Therefore, this research aims to explore the feasibility and effectiveness of using a decentralized approach to maintain data integrity of both stored user data in the user's device and IPFS distributed network.

2.0 RESEARCH PROBLEM

Existing centralized social media platforms need to be improved to better serve the needs of users and society. These platforms have several data integrity issues that create massive ethical, privacy, and public policy concerns. The following issues are widespread currently on social media platforms in user data integrity.

Users may have limited control over their data and platform owners have the authority to control user data. Owners of centralized social media platforms gather and store enormous quantities of personal information about their users, which is vulnerable to hacking, misuse, and abuse. Large volumes of user data are stored on a central server by centralized social media platforms. This makes them a tempting target for hackers. And Users' personal information, login passwords, and private messages may be compromised by data breaches. Centralized platforms have the authority to censor both content and users, potentially compromising the platform's data integrity. Overall, data integrity, privacy, and security are severely impacted by the centralized approach of social media networks.

Decentralized social media protocol is a solution to address the issues of centralization. There are several research problems that need to be addressed to implement a decentralized data integrity mechanism.

The first problem is how to maintain the integrity of signed user data that is stored on the user device. The stored data should be ensured the integrity. The second problem is to identify the best mechanism for achieving user data integrity. Because there are many mechanisms that are already used in decentralized social media platforms. The third problem is how to ensure user data integrity using the IPFS network. It is essential to ensure data integrity in IPFS, because IPFS is a distributed network for storing user data. By addressing these research problems, Data integrity can be verified in a decentralized social-media protocol.

3.0 OBJECTIVES

3.1 Main Objective

Implement a mechanism for decentralized data integrity preservation for user data that facilitates the development of decentralized social media protocol.

3.2 Specific Objectives

The following are the sub-objectives of this research.

- Ensure consistency in preparation for hashing and signing.
- Ensures the data security distributed across multiple nodes.
- Verify the authenticity of the data.
- Ensure that the data has not been altered or tampered with during storage.

4.0 METHODOLOGY

4.1 Requirement Gathering

The initial step of this research component is to gather the requirements for the new data integrity mechanism. The requirements are gathered from the existing data integrity mechanisms.

4.1.1 Past Research Analysis

The second step of this research is to analyze the past research of the data integrity mechanisms. The analysis is done to identify the problems of the existing data integrity mechanisms.

4.1.2 Refer Official Documentations

Official documentation offers current details on the technology we'll be using to create the system that we've proposed. Although previous research publications contain a tremendous amount of information because the technologies we use are constantly updated, they may contain out-of-date information.

4.1.3 Identify Existing Methodologies

There are several decentralized social media platforms that currently exist and provide user integrity of data. Nevertheless, those technologies did not provide an approach to further secure and protect user data.

4.2 Feasibility Study

4.2.1 Technical Feasibility

It is technically feasible to develop data integrity in a decentralized social media protocol that utilizes hashing algorithms, digital signatures, encoding, and data integrity mechanism in IPFS (InterPlanetary File System). Thorough testing and optimization will be important to address the challenges and ensure successful implementation of the protocol for decentralized social media with data integrity.

4.2.2 Schedule Feasibility

The research project has been planned with the expectation that the component will be finished in approximately ten months. A Gantt chart has been designed to illustrate the work that has to be completed under certain time frames. This component can be considered schedule-feasible after considering all the mentioned factors.

4.3 Software Development Life Cycle (SDLC)

The SCRUM framework, an Agile software development framework, will be used as the primary software project management framework throughout the research. The reason to choose agile methodology over other software project management methodologies such as Lean, Waterfall model, and Six Sigma is because it is best adapted for rapid and effective software development. According to the article [23], SCRUM is a popular agile framework because it defines the systems development process as a loose collection of activities combining the finest tools and techniques a development team can devise to create a system. According to additional information in the same article [23], SCRUM implies that the systems development process is unpredictable, complex and can only be described as an overall progression.

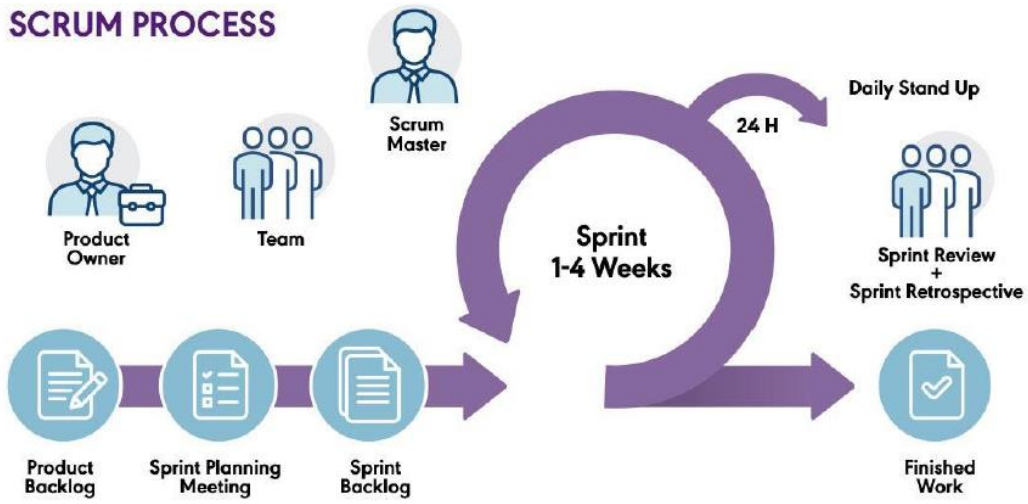

Figure 4.3.1: Software Development Life Cycle

A systematic allocation and organization of the work have been used to achieve the research's outlined objectives and achieve the desired outcomes. A detailed schedule, complete with a Gantt chart, has been made to give each part of the research sufficient time to be finished on time. In addition, the selection of appropriate technologies to effectively implement the proposed solution and demonstrate the intended results of this research has been carefully considered. As evidenced by the detailed preparation and strategic decisions made throughout this research, each step has been taken to ensure a well-structured and systematic approach to achieving the research objectives.

4.4 Proposed System Design

4.4.1 System Overview Diagram (Overall)

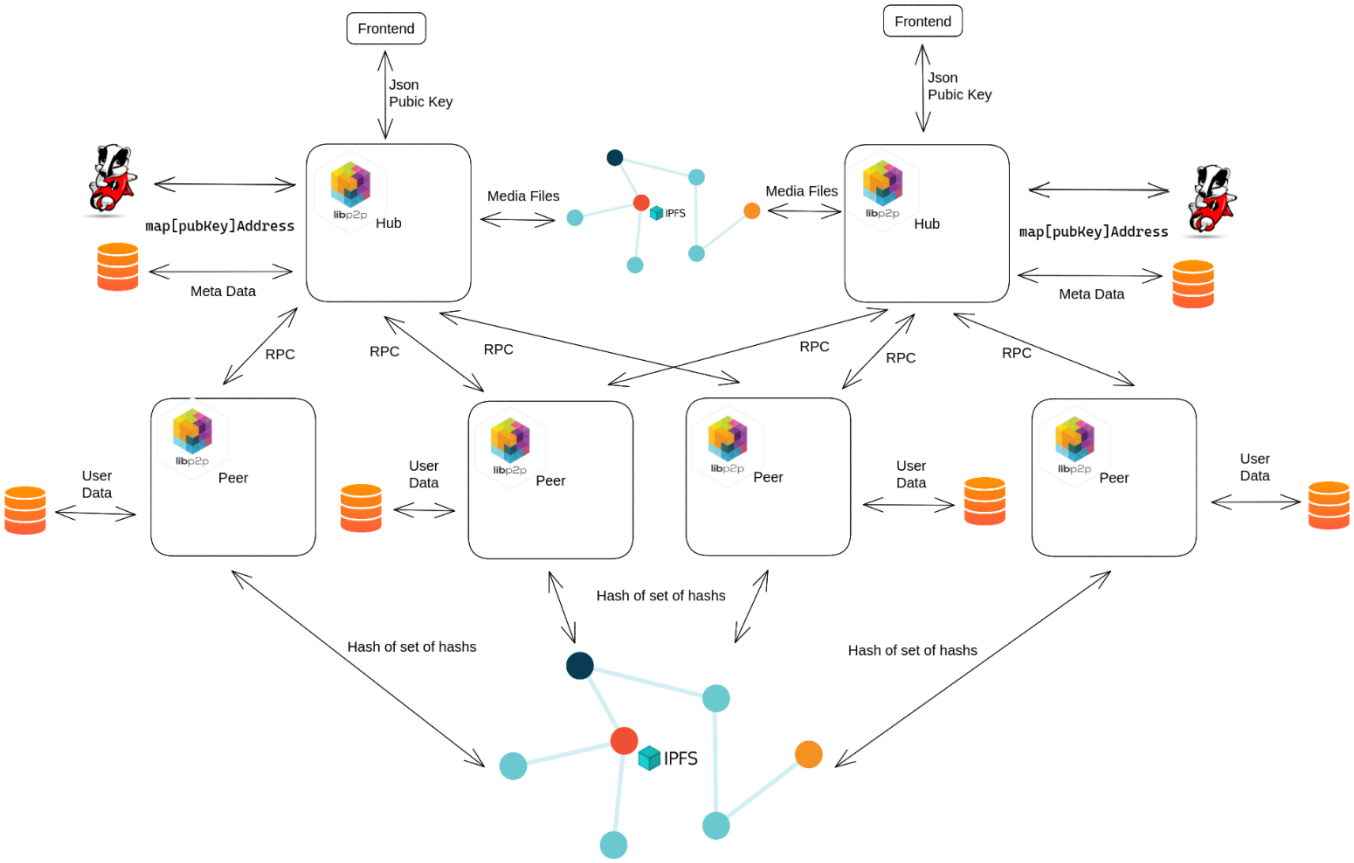

Figure 4.4.1.1: System Overview Diagram

This diagram presents an overall overview of the DeMedia architecture. DeMedia comprises four major components: data decentralization protocol, peer-to-peer communication, decentralized data storage, and data integrity in a decentralized network. A social network platform will be designed with IPFS to display these capabilities. This system infrastructure will consist of hubs, peers, and a decentralized data storage network. This diagram illustrates a high-level architectural perspective of the presented social network platform.

4.4.2 System Overview Diagram (Individual)

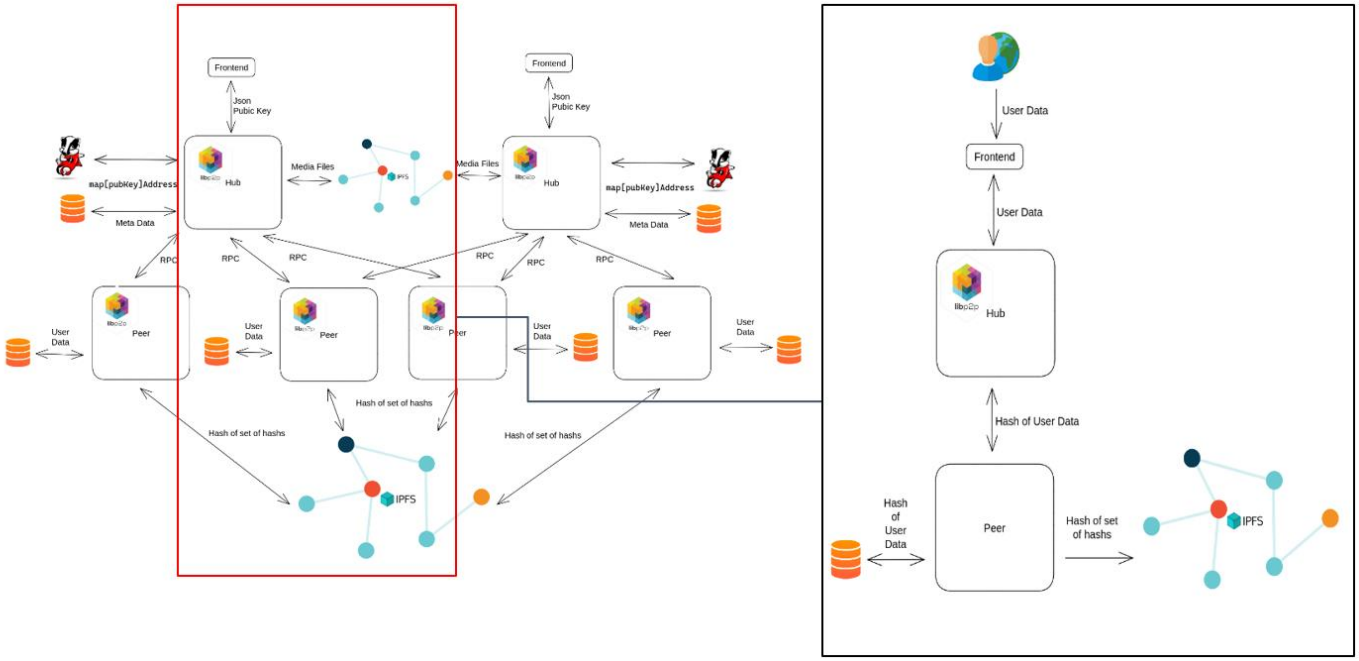

Figure 4.4.2.1: Proposed Diagram for Data Integrity

In this research component, a data integrity mechanism will be implemented for decentralized social media protocol. The hash of user data which is digitally signed is saved in user's device and hash of set of hash values is stored in IPFS distributed network.

4.5 Work Breakdown Structure (WBS)

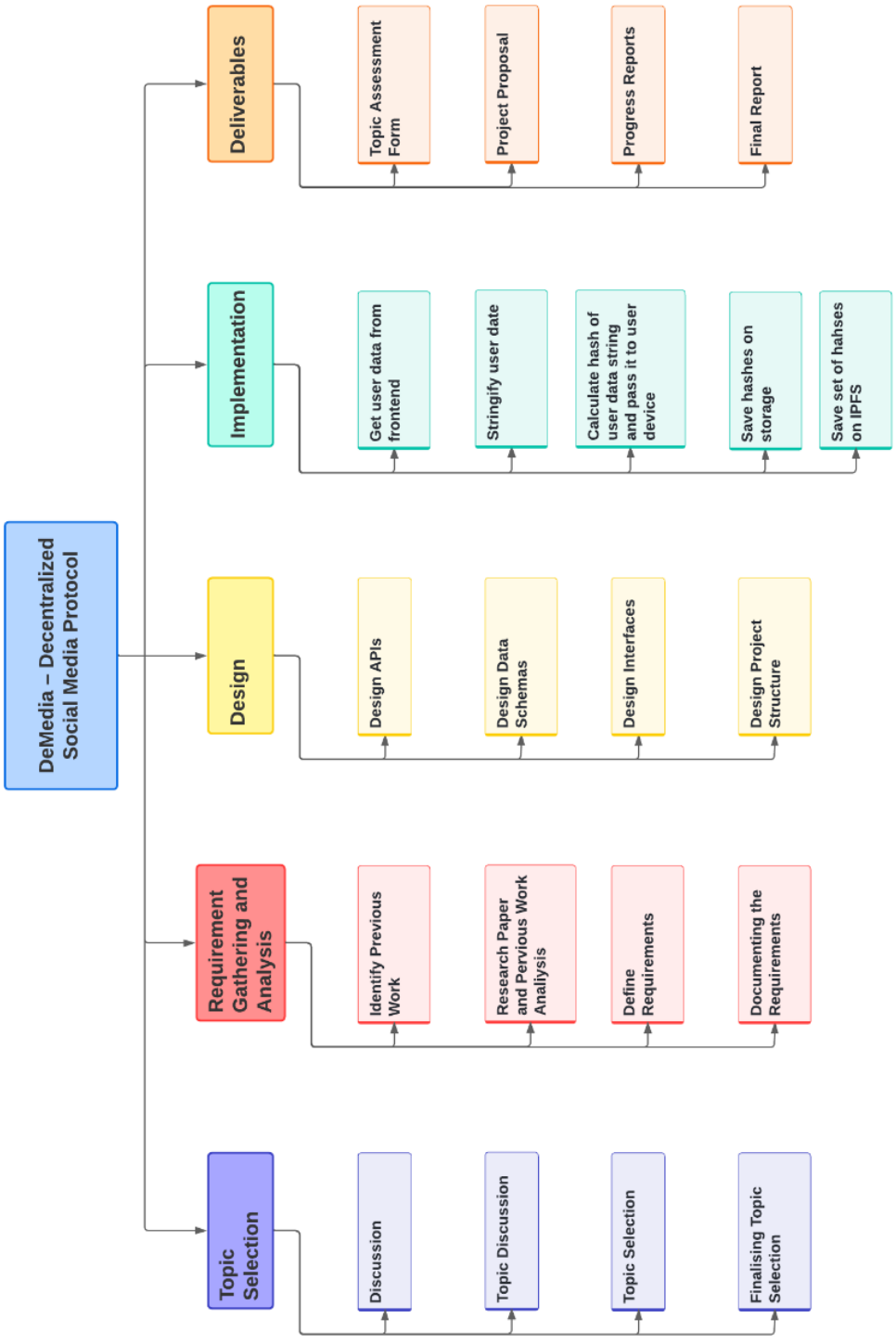

Figure 4.5.1: Work Breakdown Structure

4.6 Timeline

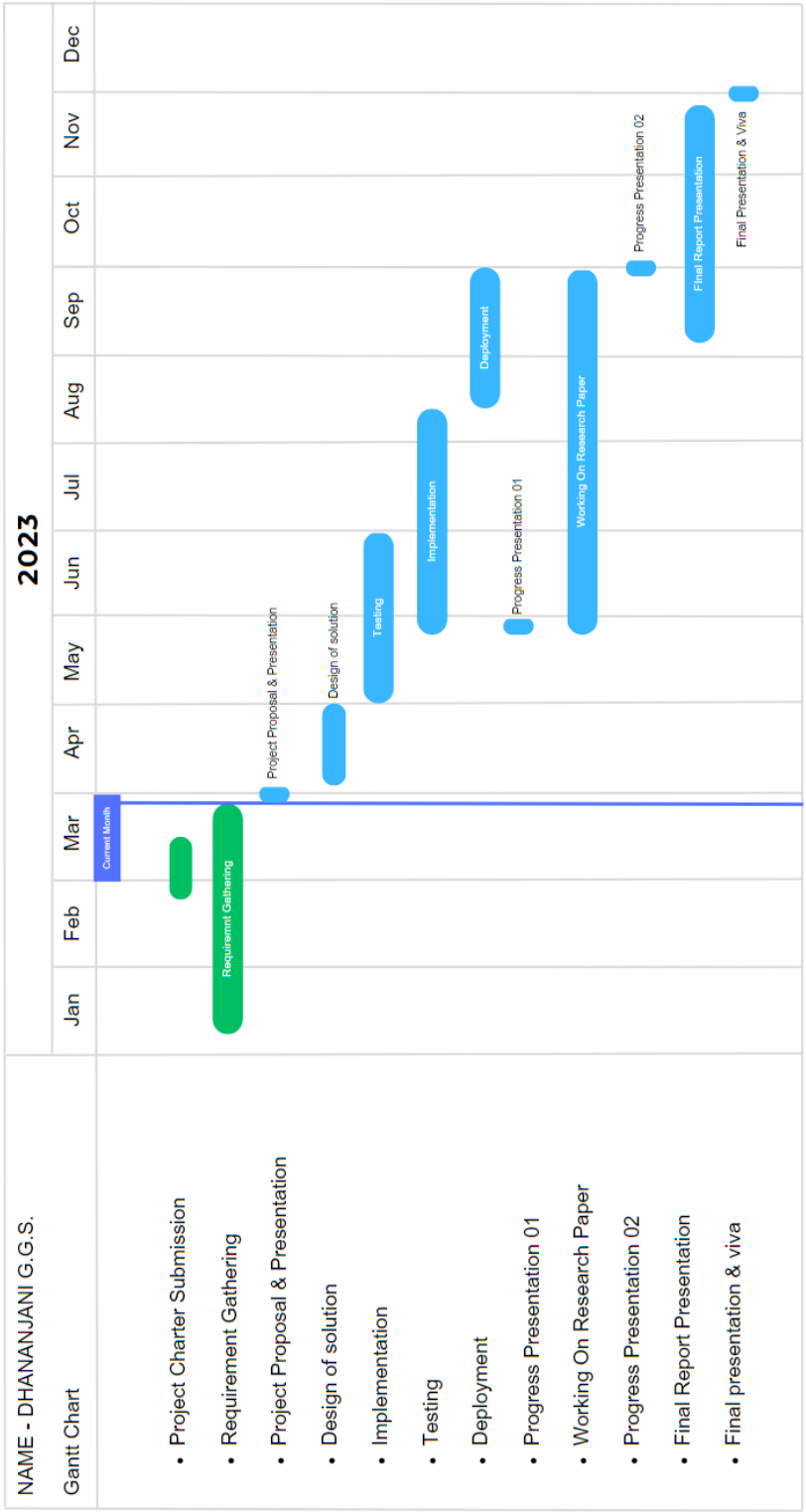

Figure 4.6.1: Gantt Chart

4.7 Proposed Tools and Technologies

Tool/Technology	Purpose
Quasar	Frontend Development
Go Lang	Backend Development
Libp2p, Markdown	Libraries
IPFS, PostgresSQL	Data Storage
VScode, GoLand	IDEs
GitHub	Version Control System
GitLab	CI/CD
AWS	Cloud Service
Microsoft planner	Project Management
Microsoft Teams, WhatsApp	Communication

Table 4.7.1: Proposed Tools and Technologies

5.0 SOFTWARE SPECIFICATIONS

5.1 Functional Requirements

Following are the functional requirements of the proposed system.

- Hashing algorithm
- Digital signatures
- Maintain data integrity of saved user data in user device.
- Hash the set of signed hash values.
- Maintain data integrity in IPFS.

5.2 Non-Functional Requirements

The following are the non-functional requirements focused on during the proposed system's development.

- Integrity
- Security
- Privacy
- Availability
- Usability
- Reliability

6.0 PERSONAL AND FACILITIES

IT number	Name	Tasks
IT20137496	Dhananjani G.G.S.	• Conduct a comprehensive review of data integrity preservation mechanism and associated research. • Develop a cryptographic mechanism to save data in user's device. • Generate hash value for user data using the hashing algorithm. • Sign hash values using digital signature and encode it. • Maintain data integrity of stored set of signed values in IPFS network.

Table 6.0.1: Personal and Facilities

7.0 BUDGET AND BUDGET JUSTIFICATION

The initial phase of the project does not entail any budgeted tasks as the process of requirement gathering is accomplished through an analysis and review of previous work conducted for research or field study purposes. As the recommended technologies and tools are open source and do not incur any costs, their utilization is free of charge. However, expenses are incurred during the development phase, as it necessitates the use of cloud service providers' services.

Task	Estimated budget (LKR)
Documenting and Planning	8,000
Cloud services	21,000
Other (Internet, Travelling etc.)	5,000
Total	**34,000**

Table 7.0.1: Proposed Budget

8.0 COMMERCIALIZATION

DeMedia is focused on developing an open-source protocol that facilitates the creation of decentralized social media platforms which can be self-hosted. The project aims to provide a base model for free, which can be used by anyone interested in creating a decentralized social media platform.

In addition to the free model, DeMedia will also offer two paid models.

- Subscription-based membership model
- Advertising-based revenue model

These paid models can be governed by the host, allowing them to generate revenue from their platform. Therefore, one could describe DeMedia as a research project focused on commercializing the development of decentralized social media platforms. The project is developing a range of monetization models that can be used by hosts to generate revenue from their platforms, thereby enabling commercialization of the technology.

To further elaborate on the commercialization aspect of DeMedia, it's important to understand that the project is focused on creating a technology that can enable the development of decentralized social media platforms. By providing a free base model, DeMedia is making it easier for individuals or organizations to create their own social media platforms that are not controlled by a centralized authority. However, to sustain and grow these platforms, there needs to be a way to generate revenue. This is where the two paid models offered by DeMedia come in.

The subscription-based membership model allows hosts to charge users for access to premium features or content on their platform. This revenue can be used to cover the costs of hosting and maintaining the platform.

On the other hand, the advertising-based revenue model enables hosts to generate revenue by displaying ads on their platform. Hosts can charge advertisers to display their ads on the platform, and this revenue can be used to cover the costs of hosting and maintaining the platform, as well as generating profits.

As a summery about this proposed system, DeMedia is enabling the commercialization of decentralized social media platforms by providing a technology that allows anyone to create their own platform, along with monetization models that enable hosts to generate revenue and sustain their platforms. This could lead to a more diverse and decentralized social media ecosystem, with a greater range of platforms catering to specific sectors and communities.

9.0 CONCLUTION

The main objective of the proposed research component is to provide a data integrity mechanism to preserve user data in decentralized social media protocol. Data integrity is a critical aspect of any decentralized social media protocol, and DeMedia provides a robust mechanism to ensure the integrity of user data. It provides users security, privacy, and a trustworthy environment for users to share and communicate without having to worry about the security of their data.

By utilizing cryptographic hashing and data encoding, DeMedia establishes unique hash values for each piece of user-generated content or data, making it difficult for data to be tampered with or corrupted by external parties. This helps to build trust and confidence among users, as they have control over their data and can verify its legitimacy. DeMedia also offers both quantitative and qualitative measures to evaluate data integrity, allowing for a comprehensive assessment of the accuracy, consistency, and reliability of the data stored on the IPFS network.

DeMedia's data integrity mechanisms provide several advantages. First, they allow even non-technical users to easily deploy peers on their devices with low operational costs, making it accessible for a wide range of users. Second, by giving users full control over their data and enabling them to make changes at their discretion, DeMedia reduces the risk of data corruption or tampering by outside parties. This empowers users to have greater ownership and control over their data, enhancing their trust in the platform.

As a summary, DeMedia's data integrity mechanisms provide a secure and trustworthy environment for users to share and communicate on a decentralized social media platform. By ensuring the integrity of user data, DeMedia enhances user confidence in the platform, mitigates the risk of data tampering or corruption.

REFERENCES

[1] https://brand-experience.ieee.org/guidelines/social-media/social-media-overview/#:~:text=IEEE%20social%20media%20consists%20of,and%20respond%20to%20that%20content, IEEE

[2] Bogdan Tiganoaia, Alexandra Cernian, Andrei Niculescu, "The use of social platforms and personal data protection - An exploratory study" IEEE, 2017.

[3] Tharuka Sarathchandra, Damith Jayawikrama, "A decentralized social network architecture", IEEE 2021.

[4] Maryam Qamar, Mehwish Malik, Saadia Batool, Sidra Mehmood, "Centralized to Decentralized Social Networks", ResearchGate 2016.

[5] Shuai Zeng, Yong Yuan, Fei-Yue Wang, "A decentralized social networking architecture enhanced by blockchain", IEEE 2019.

[6] Biwen Chen, Libing Wu, Huaqun Wang, Lu Zhou, Debiao He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks", IEEE 2019.

[7] Kelsie Nabben, "Decentralized Technology in Practice: Social and technical resilience in IPFS", IEEE 2022.

[8] Subhashish Mazumdar, "From data integrity to inference integrity", IEEE 2017.

[9] Vishwanath G. Garagad, Nalini C. Iyer, Heera G. Wali, "Data Integrity: A security threat for Internet of Things and Cyber-Physical Systems", IEEE 2020.

[10] Ting Cai, Zicong Hong, Shuo Liu, Wuhui Chen, Zibin Zheng, Yang Yu, "SocialChain: Decoupling Social Data and Applications to Return Your Data Ownership", IEEE 2017.

[11] Chhavi Tuteja, Nitesh Saxena, Prashant Johri, Vikas Rao Vadi, "Blockchain Technology: A case study of its Decentralized Use", IEEE 2022.

[12] Ruibo Cao, Kun Meng, Kai Sun, Ziqiang Zheng “Evaluation Model of Data Consistency Mechanism in Decentralized Network Application”, IEEE 2021.

[13] “Data Integrity–Based Methodology and Checklist for Identifying Implementation Risks of Physiological Sensing in Mobile Health Projects: Quantitative and Qualitative Analysis”, No.12, 2018.

[14] Reza Nourmohammadi, Kaiwen Zhang, "An On-Chain Governance Model Based on Particle Swarm Optimization for Reducing Blockchain Forks", IEEE 2022.

[15] Thomas Paul, Antonino Famulari, Thorsten Strufe, "A survey on decentralized Online Social Networks", ScienceDirect, 2014.

[16] [Online] available: https://ethtps.info

[17] Quanqing Xu, Zhiwen Song, Rick Siow Mong Goh, Yongjun Li, "Building an Ethereum and IPFS-Based Decentralized Social Network System", IEEE 2018.

[18] Van-Duy Pham, Canh-Tuan Tran, Thang Nguyen, Tien-Thao Nguyen, Ba-Lam Do, "B-Box - A Decentralized Storage System Using IPFS, Attributed-based Encryption, and Blockchain", IEEE 2020.

[19] Manjula K Pawar, Prakashgoud Patil, Manisha Sharma, Megha Chalageri, "Secure and Scalable Decentralized Supply Chain Management Using Ethereum and IPFS Platform", IEEE 2021.

[20] [Online] available: https://www.deso.com/

[21] Julija Golosova, Andrejs Romanovs, "The Advantages and Disadvantages of the Blockchain Technology", IEEE 2018.

[22] Nursena Baygin, Mehmet Baygin, Mehmet Karakose, "Blockchain Technology: Applications, Benefits and Challenges", IEEE 2019.

[23] R. Keefe, “5 popular project management methodologies and when to use them,” Toggl Blog, 13-Sep-2022. [Online]. Available: https://toggl.com/blog/5-popular-project-management-methodologies-and-when-to-use-them. [Accessed: 20-Mar-2023].

GLOSSARY

- Centralization - A system in which power and decision-making are concentrated in a single entity or a group.
- Decentralization - A system in which power and decision-making are distributed among multiple entities or individuals.
- Encrypt - To convert information or data into a secret code to prevent unauthorized access or interception.
- Decrypt - To convert an encrypted code back into its original, readable form.
- Cryptography - The practice of secure communication using codes and ciphers.
- Peer - A computer or device connected to a network that shares data and resources with other peers.
- Caching - The process of storing frequently accessed data in a temporary storage location to improve access time and reduce network traffic.
- Network - A group of interconnected devices and communication channels that enable communication and data exchange.
- Protocol - A set of rules and procedures that govern the communication and exchange of data between devices on a network.
- Algorithm - A step-by-step set of instructions for solving a problem or performing a task.
- Hash - A unique numerical value generated by a mathematical function that represents a digital file or data.
- Blockchain - A decentralized, distributed digital ledger that records transactions across multiple devices and networks.
- Public key - A unique cryptographic code that is available to everyone and used to encrypt data.
- Private key - A unique cryptographic code that is kept secret and used to decrypt data.
- Cipher - An algorithm used to encrypt or decrypt data.
- Hacker - A person who gains unauthorized access to computer systems or networks with malicious intent or for personal gain.