ABSTRACT

In today's technologically driven world, social media has become an increasingly important part of our daily lives. It lets people interact with one another over the internet, which makes communication much easier. All of these advantages, however, appear to be too good to be true. However, all of these features and services come at the cost of our privacy. They monitor our daily activities on these platforms in order to provide targeted advertising and generate revenue. To overcome this problem, we suggest utilizing blockchain technology to build a completely decentralized social media platform in which no single organization or individual owns the data. This helps to assuage our privacy concerns. Online social networks have become increasingly prevalent in people's daily lives, but the centralized nature of popular social networks raises concerns around security, privacy, and management. To address these issues, researchers have proposed a decentralized framework for online social networks, using blockchain technology to provide greater security and privacy. We propose a decentralized application for an online social network, enhanced by Solana blockchain technology. The current centralized data management mechanism used by online social networks has resulted in privacy leaks. The main goal of the Decentralized Social-Media - DSM framework is to address the privacy and security issues that exist in traditional online social networks. By leveraging blockchain technology and smart contracts, Decentralized Social-Media - DSM offers a decentralized social framework that integrates the advantages of both centralized and decentralized networks, using the blockchain as a trusted server to provide central services.

CHAPTER I

1.INTRODUCTION

In recent years, the landscape of social media has undergone a paradigm shift, with users increasingly concerned about privacy, data ownership, and censorship. Enter decentralized social media, a groundbreaking concept empowered by blockchain technology, poised to redefine the way we interact and share online. Decentralized social media platforms operate on the principles of blockchain, a distributed ledger technology renowned for its transparency, security, and immutability. Unlike traditional social media giants that centralize control and data ownership in the hands of a few, decentralized platforms distribute power among all participants, fostering a democratic and censorship-resistant environment.

At the heart of decentralized social media lies the blockchain, a tamper-proof digital ledger that records every transaction and interaction. Through this decentralized infrastructure, users regain control over their data, deciding what to share, with whom, and for how long. This shift from centralized data silos to user-owned data empowers individuals, mitigating concerns over data exploitation and privacy breaches.

Moreover, blockchain technology ensures the integrity of content shared on decentralized social media platforms. By leveraging cryptographic techniques and consensus algorithms, misinformation and fake news can be effectively curtailed, fostering a more informed and trustworthy online community. Beyond data ownership and content integrity, decentralized social media platforms enable new avenues for monetization and incentivization. Through token economies and smart contracts, content creators can be directly rewarded for their contributions, eliminating intermediaries and empowering grassroots content creators.

In essence, decentralized social media represents a departure from the status quo, offering a compelling alternative that prioritizes user autonomy, data sovereignty, and community governance. As we navigate an era marked by digital transformation and increasing scrutiny of centralized platforms, decentralized social media emerges as a beacon of innovation, promising a more inclusive, transparent, and equitable digital future.

1.1 DOMAIN INFORMATION

A blockchain is a growing distributed ledger that keeps a permanent record of all transactions that have taken place in a secure, chronological, and immutable way. It was conceptualized and first used in 2008 by an unknown person or group named Satoshi Appl. Sci. 2022, 12, 6567 3 of 25 Nakamoto to create the Bitcoin cryptocurrency. The primary aim is to use a cryptosystem to encrypt the sequence of bits in electronic files so as not to be tampered with. When evaluating a blockchain, the notable characteristics to consider include audibility, privacy, confidentiality, consistency, decentralization, and integrity. Blockchain technologies can be categorized into three types: Public Blockchains (anyone can join the network), Private Blockchains (the members are chosen based on conditions), and Consortium Blockchains (semiprivate blockchains limited to a group). All three types can additionally be classified as Permission less (public Blockchain), permissioned (private Blockchain), or both (Consortium blockchain). A Blockchain network comprises several components and attributes, such as a distributed and immutable ledger, Peer-toPeer (P2P) networks, a consensus mechanism, and smart contracts.

A. PROBLEM STATEMENT

In recent years, major social media has been frequently plagued by privacy abuse and data breaches scandals. Facebook has been accused of selling or abusing user data in 2018, leading to identity theft and other related issues. As a result, Facebook lost over $120 billion in market cap. The event has intensified distrust of centralized OSNs. In a word, the privacy issues become a major problem that should be resolved for the existing centralized OSNs, which have prompted researchers to consider the decentralization framework for online social networks.

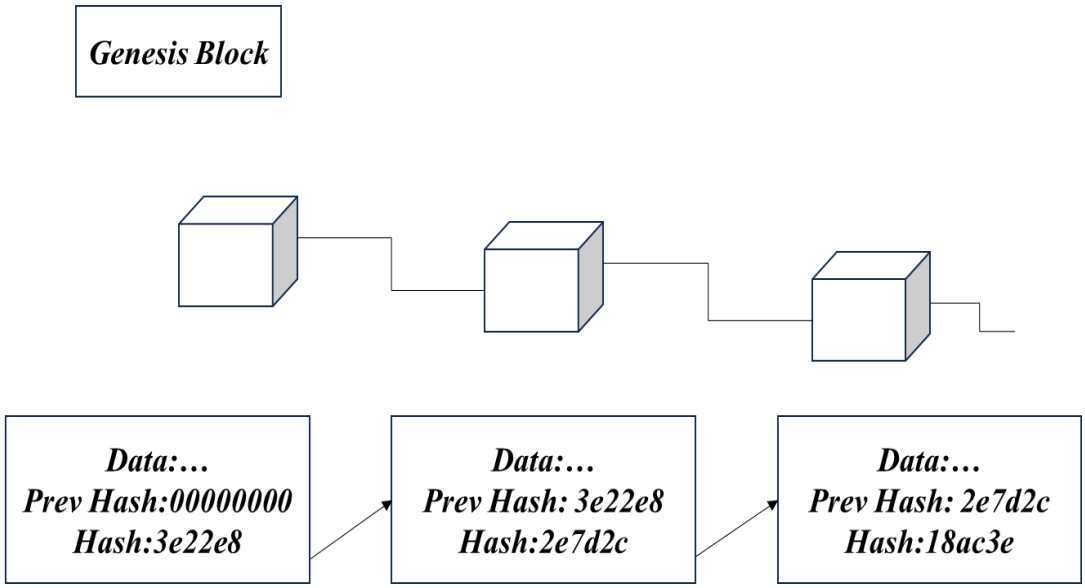


Fig 1, Illustration of Block chain

B. OBJECTIVE

- To overcome the main privacy issues in social media, fake news, and censorship.
- To achieve secure authentication while ensuring anonymity.
- To obtain transparent, immutable, and certifiable operation registry while producing a safe peer-to-peer environment for keeping and exchanging material.
- To find combating disinformation by tracing and checking the provenance of potentially perilous data.

C. MOTIVATION

Privacy for User Information

Since there is no third party involved, collecting and using personal information without consent is impossible. Thus eliminating data breaches, identity theft, and user commodification. **Freedom from censorship.**

Decentralized social networks offer a censor-free platform, reinstating this precious freedom. Users can freely share their opinions with a chosen audience without fear of any blocking or personal risk.

Enhanced Security

With blockchain, users can control feeds without letting a third party decide for them. Also, their data is stored in a decentralized network of servers that outside sources cannot access without authentication.

Opportunity for Fundraising

With the improved process and targeted control, users can undertake crowdfunding campaigns through which they can directly take peer-to-peer transactions to raise funds.

Increase Social Commerce

Blockchain in social media is nurturing in social commerce. This means even aspiring content creators can be rewarded with the native cryptocurrency.

D. SCOPE

Decentralized social networks have the potential to provide a better environment within which users can have more control over their privacy, and the ownership and dissemination of their information.

CHAPTER II

2 BACKGROUND

2.1 BLOCK CHAIN IN SOCIAL MEDIA

Developing a blockchain based Decentralized Social-Media - DSM application requires a comprehensive understanding of blockchain technology, which encompasses various types of blockchains, consensus mechanisms, and smart contracts. It is essential to consider the different types of blockchains, such as public and private blockchains, to determine which one is best suited for our specific use case. Consensus mechanisms, which validate transactions on the blockchain, are also crucial to the development process of Decentralized Social-Media - DSM. In our project, we utilized the Solana blockchain, which is known for its cost-efficiency and fast transaction processing. We created the Solana smart contract using Seahorse, a program that allows you to write Solana programs using Python.

2.1.1. PRIVATE BLOCKCHAIN

A private blockchain is a permissioned blockchain since it is run by a network administrator and only approved users can connect to the network. The network is controlled by one or more organizations, which makes it necessary to conduct transactions via third parties. Only the parties involved in the transaction will know about it in this sort of blockchain; others won't be able to access it, making the transaction private.

2.2.2. PUBLIC BLOCKCHAIN

Public blockchains, sometimes referred to as permissionless blockchains, are totally open and strictly adhere to the decentralisation principle. Public blockchains include ones like Bitcoin and Ethereum. Anybody with access to the network can contribute blocks to the chain. In contrast to private blockchains, where the identities of the parties to a transaction are kept secret, public blockchains are likewise mostly anonymous.

2.2.3. SMART CONTRACTS IN BLOCKCHAIN

Smart contract is the agreement involving two parties that are maintained in computer code. It does not necessitate the involvement of a third party. Smart contracts function similarly to traditional contracts in which specific code can be inserted immediately and the parties

concerned can check the respective code before the deadline. Blockchain technology is a distributed ledger that is immutable and has a more complex fault tolerance rate. [3]. Smart contracts include certain terms and circumstances that must be adhered to. Adhering to agreements, defining regulations and executing the business logic, relying on blockchain technology for encryption to help protect and authenticate all messages it contains, processing, and lastly updating the blockchain network are all part of a smart contract's anatomy. It is stored in a database because it works with blockchain and is irreversible. A smart contract's transactions must be handled primarily by blockchain technology, which eliminates the need for a third party and, as a result, saves time.

CHAPTER III

3 TECHNICAL BACKGROUND

3.1 SOLANA

Solana plays a crucial role in decentralized social media using blockchain technology by providing a high-performance and scalable blockchain infrastructure. Solana is renowned for its scalability, capable of processing thousands of transactions per second (TPS) with low latency and minimal fees. This scalability is vital for decentralized social media platforms, which often require fast and efficient transaction processing to support a large user base and high throughput of content interactions. Solana's architecture is designed for speed, leveraging innovations such as a unique consensus mechanism called Proof of History (PoH) and a network of distributed nodes to achieve fast transaction finality. This ensures that interactions on decentralized social media platforms, such as posting content, liking, commenting, or transferring tokens, can be executed swiftly, providing users with a seamless experience. Solana's efficient design and scalability contribute to low transaction costs, making it economically viable for users to engage with decentralized social media platforms without being burdened by high fees. This affordability encourages broader participation and ensures accessibility for users with varying economic means. Solana prioritizes security, utilizing robust cryptographic techniques and a decentralized network of validators to protect the integrity of transactions and data stored on the blockchain. This security is essential for decentralized social media platforms to safeguard user data, content, and digital assets from unauthorized access, tampering, or censorship. Solana has a vibrant and growing ecosystem with extensive developer support, tools, and resources for building decentralized applications (dApps). This ecosystem support facilitates the development and deployment of decentralized social media platforms, providing developers with the infrastructure and frameworks needed to create innovative solutions. Solana is designed to be interoperable with other blockchain networks and protocols, enabling seamless integration and data exchange. This interoperability is valuable for decentralized social media platforms seeking to leverage assets or functionalities from other blockchains, enhancing the flexibility and utility of their offerings. In summary, Solana's scalability, speed, low costs, security, ecosystem support, and interoperability make it an ideal blockchain infrastructure for decentralized social media platforms. By leveraging Solana's capabilities, developers can create decentralized social media experiences that are fast, efficient,

secure, and accessible to users worldwide, contributing to the advancement of decentralized communication and interaction on the blockchain.

3.1 PHANTOM

Phantom is a cutting-edge decentralized finance (DeFi) platform that offers users a secure and efficient way to store and manage their digital assets. Built on the robust Solana blockchain, Phantom provides a decentralized solution for users seeking to safeguard their cryptocurrencies while maximizing their earning potential. At its core, Phantom leverages Solana's high-performance blockchain technology to deliver lightning-fast transaction speeds and minimal transaction fees. This ensures seamless and cost-effective asset management for users, even during periods of high network congestion. One of the standout features of Phantom is its innovative approach to security. By employing advanced cryptographic techniques and decentralized governance mechanisms, Phantom mitigates the risk of hacks and unauthorized access, providing users with peace of mind knowing that their assets are safe and secure. In addition to its focus on security, Phantom offers users the opportunity to earn passive income through a variety of yield-generating strategies. Whether through staking, liquidity provision, or yield farming, users can put their assets to work and earn attractive returns on their investments. Furthermore, Phantom prioritizes user experience, offering an intuitive and user-friendly interface that makes it easy for both novice and experienced users to navigate the platform and access its features. Phantom represents a next-generation DeFi platform that combines cutting-edge technology with robust security measures and lucrative earning opportunities. Whether you're looking to securely store your digital assets or maximize your investment returns, Phantom provides a comprehensive solution tailored to meet your needs in the fast-paced world of decentralized finance.

3.2 META MASK

Meta Mask plays a pivotal role in decentralized social media using blockchain technology by serving as a bridge between users and the blockchain-powered social media platforms. Meta Mask acts as a digital wallet, enabling users to securely store their cryptocurrency funds, such as Ethereum (ETH) and other ERC-20 tokens. Users can connect their Meta Mask wallet to decentralized social media platforms, allowing them to transact, earn rewards, and participate in the platform's ecosystem. Meta Mask facilitates identity verification on decentralized social media platforms through cryptographic signatures. Users can sign messages or transactions with their private keys stored in Meta Mask, proving ownership of their accounts and maintaining control over their identity and data. Many

decentralized social media platforms utilize smart contracts to govern interactions, such as content publishing, voting, and rewards distribution. Meta Mask enables users to interact with these smart contracts seamlessly, executing transactions and participating in platform governance directly from their wallets. Meta Mask provides a secure authentication mechanism for accessing decentralized social media platforms. Users can log in to these platforms using their Meta Mask wallets, eliminating the need for traditional username-password combinations and enhancing security by leveraging cryptographic keys. Meta Mask simplifies transaction management by providing users with an intuitive interface for sending, receiving, and monitoring blockchain transactions. This functionality is essential for users engaging in various activities on decentralized social media platforms, such as tipping content creators, purchasing digital goods, or transferring tokens. In essence, Meta Mask serves as a crucial tool for users participating in decentralized social media ecosystems, offering them secure access to blockchain functionalities, seamless interaction with smart contracts, and robust transaction management capabilities. By integrating Meta Mask into their platforms, decentralized social media projects can empower users to take full control of their digital identities, assets, and interactions within a trust less and censorship-resistant environment.

3.3 SEAHORSE

Seahorse could potentially serve as a decentralized identity management and authentication solution for users of decentralized social media platforms on the blockchain. Seahorse could provide users with the ability to create and manage their digital identities on the blockchain in a decentralized manner. Each user could have a unique identity represented by cryptographic keys, ensuring privacy, security, and user control over personal data. Seahorse could facilitate secure authentication and access control mechanisms for users accessing decentralized social media platforms. Users could authenticate their identities using Seahorse's decentralized identity solution, eliminating the need for traditional username-password combinations and enhancing security. Seahorse could enable users to maintain ownership and control over their personal data, allowing them to securely share and transfer data across different decentralized social media platforms. This would promote data portability and interoperability while ensuring user sovereignty over their digital identities and interactions. Seahorse could prioritize user privacy and security by implementing robust encryption techniques, decentralized storage solutions, and privacy-enhancing features. Users would have the assurance that their personal data is protected from unauthorized access, surveillance, and exploitation. Seahorse could integrate seamlessly with various blockchain platforms commonly used for decentralized social

media applications, such as Ethereum, Solana, or others. This integration would enable users to leverage Seahorse's identity management and authentication services across different blockchainbased social media platforms.

CHAPTER V

5. SYSTEM REQUIREMENT SPECIFICATION

5.1 HARDWARE REQUIREMENT

This section gives the details and specification of the hardware on which the system is expected to work

Processor	x86 64-bit CPU (Intel/AMD architecture)
RAM	4GB
Hard Disk	5GB free disk space

5.2 SOFTWARE REQUIREMENT

This section gives the details of the software that are used for the development

Front-end	React JS, Tailwind CSS
Back-end	Solana-Python

5.3 OTHER NON-FUNCTIONAL REQUIREMENTS

A non-functional requirement is a determination that depicts the framework's activity abilities and requirements that improve its usefulness.

Some of them are as follows:

- **Regularity Compliance:** The platform should comply with relevant regulations and legal requirements, especially concerning data protection, financial transactions, and user rights. Implementing compliance measures such as KYC (Know Your Customer) and AML (AntiMoney Laundering) procedures may be necessary.

- **Security:** The platform must ensure the security of user data, transactions, and digital assets. This includes protection against hacking, fraud, and unauthorized access.

- **Scalability:** The platform should be able to handle a growing user base and increasing transaction volume without sacrificing performance or experiencing network congestion.

CHAPTER VI

6 MODULE DESCRIPTION

A module is defined as the unique and addressable components of the software which can be solved and modified independently without disturbing (or affecting in very small amount) other modules of the software. Thus, every software design should follow modularity.

6.1 METAMASK MODULE:

This module is used for connecting MetaMask that is a popular browser extension and wallet provider for allowing the users to interact with the Ethereum blockchain and decentralized applications (dApps) directly from their web browsers.

6.2 ACCOUNT CREATION MODULE:

In the Account Creation Module, the user can create an account

6.3 CONNECTING PHANTOM WALLET:

The register functionality involves creating a unique user identity using a wallet address that is stored on the blockchain. The identity is encrypted using secure algorithms to prevent unauthorized access. The user can then use this identity to access the platform.

6.4 POST CREATION:

The post can be created by giving the URL and caption.

6.5 POST DELETION:

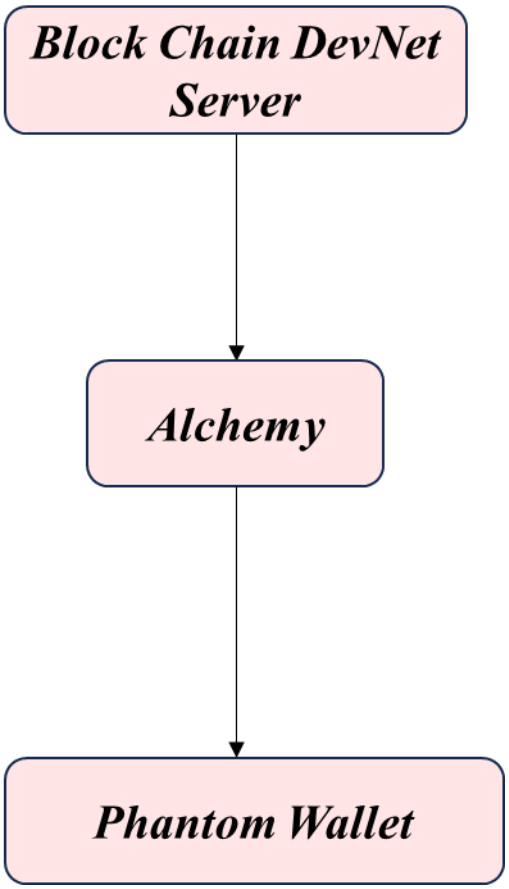
The delete post functionality allows users to delete their posts from the Decentralized Social Media - DSM. This is achieved by using smart contracts to remove the post from the blockchain and updating the user's identity accordingly.

CHAPTER VII

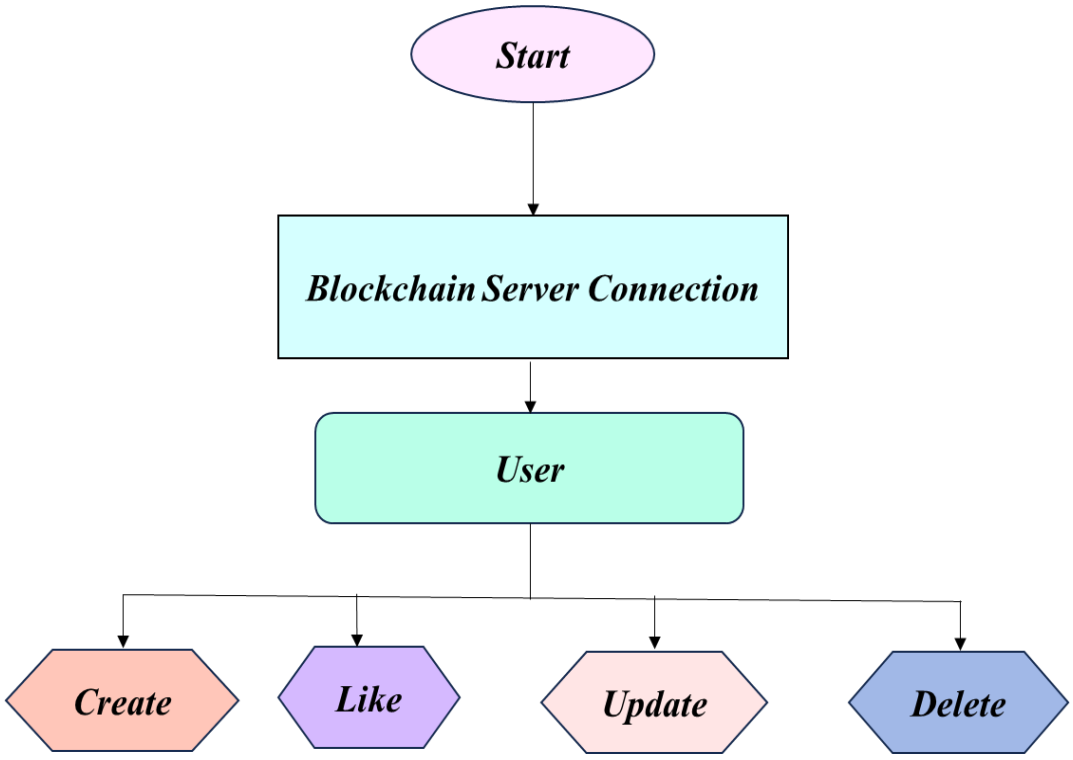
7.SYSTEM DESIGN

7.1 DATA FLOW DIAGRAM

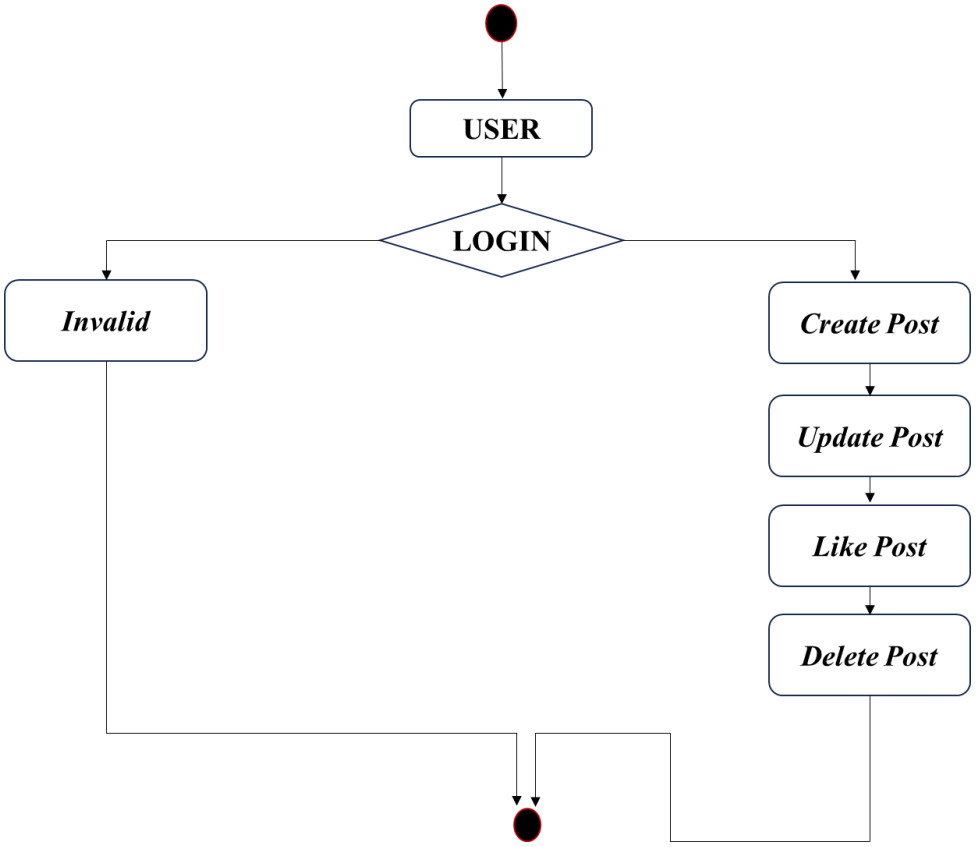
LEVEL 0:



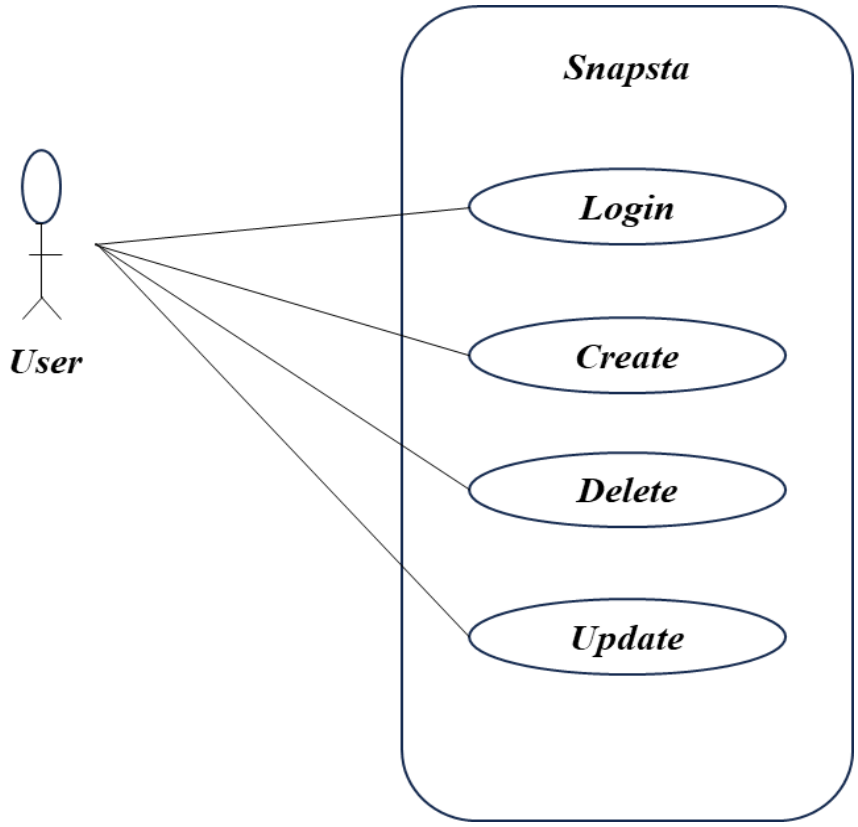
LEVEL 1:


Start
Blockchain Server Connection
User
Create
Like
Update
Delete

7.2 ACTIVITY DIAGRAM



7.3 USE CASE DIAGRAM



7.4 DATABASE DESIGN

DETAILS:

USER:

Key	Value
Wallet Address	ChGMWrykjpqKf6m6otwJy6xZcXKnnK2fFbLrCWJm9MJH
Password	“123@”

POST:

Key	Value
PostOwner_id	ChGMWrykjpqKf6m6otwJy6xZcXKnnK2fFbLrCWJm9MJH
Image Address	
Caption	
Likes	

LIKE:

Key	Value
Post_id	
Post_owner	
Liker_address	

CHAPTER VIII

8 SYSTEM TESTING AND IMPLEMENTATION

8.1 SYSTEM TESTING

Software testing is a critical element of software quality assurance and represents the ultimate review of specification, design and coding. In fact, testing is the one step in the software engineering process that could be viewed as destructive rather than constructive. A strategy for software testing integrates software test case design methods into a well-planned series of steps that result in the successful construction of software. Testing is the set of activities that can be planned in advance and conducted systematically. The underlying motivation of program testing is to affirm software quality with methods that can economically and effectively apply to both strategic to both large and small-scale systems.

STRATEGIC APPROACH TO SOFTWARE TESTING

The software engineering process can be viewed as a spiral. Initially system engineering defines the role of software and leads to software requirement analysis where the information domain, functions, behavior, performance, constraints and validation criteria for software are established. Moving inward along the spiral, we come to design and finally to coding. To develop computer software, we spiral in along streamlines that decrease the level of abstraction on each turn.

- UNIT TESTING
- MODULE TESTING
- SUB – SYSTEM TESTING
- SYSTEM TESTING
- ACCEPTANCE TESTING

➢ UNIT TESTING

- Unit testing focuses verification effort on the smallest unit of software design, the module.
- The unit testing we have is white box oriented and some modules the steps are conducted in parallel.

➢ WHITE BOX TESTING

- All independent paths have been exercised at least once.
- All logical decisions have been exercised on their true and false sides.
- All loops are executed at their boundaries and within their operational bounds

➢ CONDITIONAL TESTING

- In this part of the testing each of the conditions were tested to both true and false aspects.
- And all the resulting paths were tested.
- So that each path that may be generate on particular condition is traced to uncover any possible errors.

➢ LOOP TESTING

- All the loops were tested at their limits, just above them and just below them. All the loops were skipped at least once.
- For nested loops test the inner most loop first and then work outwards.
- For concatenated loops the values of dependent loops were set with the help of connected loop. • Unstructured loops were resolved into nested loops or concatenated loops and tested as above.

8.2 SYSTEM IMPLEMENTATION

During the software-testing phase each module of software is thoroughly tested for bugs and for accuracy of output. The system developed is very user-friendly and the detailed documentation is also given to the user as online help wherever necessary. The implementation phase normally ends with the formal test involving all the components.

CHAPTER IX

9. CONCLUSION AND FUTURE WORK

9.1 CONCLUSION

In this project, we have developed a decentralized application called Decentralized Social-Media - DSM, using blockchain technology. Decentralized online social networks do not have a central authority or server to control. the information flow, and all data is stored in a decentralized ledger. We have implemented the functionalities of our application by coding the smart contract. We chose Solana as our blockchain platform instead of Ethereum, which is the most popular blockchain technology. Solana blockchain is cost-effective and faster than Ethereum blockchain, validating transactions using the consensus mechanism called proof-of-history. Solana is capable of handling far more transactions per second than Ethereum, and also offers lower transaction costs, making it an efficient and secure blockchain platform. During the first phase of our project, we conducted a comprehensive literature survey on decentralized online social media to identify the activities required in each phase of our project. In the next phase of this project, we implemented Decentralized Social-Media, taking the first step towards building a decentralized online social network. The second step is to code the smart contracts and front-end of our project and test them. The Decentralized Social-Media - DSM, aims to provide higher security and privacy to its users. This proposed system intends to replace traditional social networks by resolving security and privacy issues. In such networks, there is no central authority to control the information flow, and each member has a copy of the distributed ledger. The Decentralized Social-Media - DSM provides no single point of failure, and data is added through group consensus.

9.2 FUTURE WORK

The future of decentralized social media on the blockchain holds immense potential for innovation and evolution. Future decentralized social media platforms may incorporate advanced privacy features, such as zero-knowledge proofs, ring signatures, and decentralized identity solutions, to offer users greater control over their personal data and interactions. Future decentralized social media platforms may explore new content monetization models, such as tokenized subscriptions, pay-per-view content, decentralized advertising networks, and creator-owned marketplaces, to empower content creators and incentivize high-quality content production. Decentralized social media platforms could further enhance their community governance mechanisms, implementing decentralized autonomous organizations (DAOs), liquid democracy systems, and quadratic voting mechanisms to enable more transparent, inclusive, and democratic decision-making processes.