DeMedia: Decentralization of Social Media

Perera B.S.S.
Department of Information Technology,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka.
it20254698@my.sliit.lk

Bandara A.M.C.A.
Department of Information Technology,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka.
it20159726@my.sliit.lk

Dhananjani G.G.S.
Department of Information Technology,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka.
it20137496@my.sliit.lk

Abeykoon A.W.Y.I.K.
Department of Information Technology,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka.
it20157432@my.sliit.lk

Kavinga Yapa Abeywardena
Department of Computer Systems Engineering,
Sri Lanka Institute of Information Technology,
Malabe, Sri Lanka
kavinga.y@sliit.lk

***Abstract*— Social media networks have become an essential part of the modern world, with billions of people using them as an integral part of their daily lives. Despite their popularity, these networks are centralized, allowing the companies that own them to monitor and track their users' activities. This has given rise to serious concerns regarding the privacy and security of user data, which are often sold to third parties for profit. Given the massive value of user data in today's and tomorrow's world, many people are concerned about this issue. While decentralized, community-driven applications have emerged as a potential solution to this problem, none have yet been able to compete with centralized social network platforms. Due to those facts, this research aimed to propose a decentralized social network architecture that would incorporate the basic functionalities of a social media platform while ensuring the privacy and security of users' data, which would be stored locally on their devices. A thorough study of the existing centralized and decentralized social media platforms was conducted to identify the path for this research. The proposed protocol offers a decentralized and secure social media platform architecture that provides true ownership of user data along with decentralized data integrity and caching.**

Keywords- Social media, Peer-to-peer networking, Data integrity, Data caching, Decentralization, Privacy, Security, Data ownership, Distributed networks

I. Introduction

Social media has become an integral part of modern life. Today, there are numerous social networks, such as Facebook, WhatsApp, Instagram, Twitter, and others, and their usage continues to grow [1]. These platforms enable users to connect with others, share information, and stay updated on global events. The popularity of social media can be attributed to various factors, including the need for connectivity, real-time updates, entertainment, and the ability to express opinions. Additionally, businesses have shifted their marketing strategies towards online platforms, targeting specific audiences [2]. Centralization of these social networks has led to various problems, which have recently become hot topics, such as the spread of false news, misinformation, privacy concerns, and the lack of regulation [3]. To address these challenges, people are looking into Web 3.0 technologies, which offer potential solutions within the decentralized protocol. The progression of Web 3.0, driven by the evolution of cryptocurrencies like Bitcoin, indicates a shift towards decentralization in social media [4]. When searching for suitable Web3 social media platforms, it is crucial to consider factors such as internet freedom, free speech, data privacy, and data control. Mastodon and DeSo are two prominent decentralized social networking platforms currently in use. These platforms aim to confront and overcome the issues associated with centralized social media by empowering users and distributing control. They seek to challenge the monopolistic control of leading social media corporations and prioritize the interests of the platform's users [5].

Despite many decentralized social media platforms, several limitations and challenges remain. Many of these platforms rely on blockchain technology, which can result in higher processing costs and slower speeds. Achieving scalability and efficiency while maintaining the advantages of decentralization remains an ongoing concern.

Currently, most social media platforms are centralized, meaning they are owned and operated by a single entity and have a central server that manages all user data and content [6]. Both centralized and decentralized social media platforms serve as websites or applications that enable users to create and share information, communicate with others, and participate in social networking. The platform owner holds full control over features, policies, and access to user data. While convenient and user-friendly, centralized platforms pose risks to data privacy and security. Users must trust the platform owner to handle their data responsibly, and there is always a potential for data breaches or misuse.

On the other hand, decentralized social media platforms distribute control and ownership among users rather than relying on a single entity [7]. Users have direct control over their data and content, enhancing privacy and security. Data and content are stored on a distributed network of computers, and decentralized social media protocols employ mechanisms like cryptographic hashing and encryption to ensure data integrity[8].

II. Background and Literature Review

Decentralized social media platforms have become a prominent topic of discussion among researchers due to concerns over the monopoly held by social media corporations and the rapid increase in social media users. According to a survey by the Global Web Index in July 2020 [9], social media usage increased by 10.5% over 2019. Furthermore, the global number of people utilizing social media has surpassed 4.48 billion, doubling the figure reported in 2015. The most widely used social media platforms are based on centralized servers, which makes them vulnerable to several dangers. Data can be easily altered, sold, or stolen if the data owner is not actively controlling it. Blockchain technology [10] has been integrated with social media platforms to address these problems.

The Internet's future, Web 3.0 [11], is expected to adopt a decentralized architecture. However, there are some challenges that restrict the decentralized Web 3.0, fully replacing the current centralized Web 2.0 infrastructure [12]. In the research field, efforts are being made to create decentralized social networks using the Ethereum platform as a base. These efforts aim to provide higher privacy, ownership of data, and services guided by the community.

Although Ethereum and similar blockchain technologies have clear potential, they also have limitations [13]. However, current efforts are focused on improving efficiency and dealing with these limitations. Interestingly, even major companies such as Facebook and Google are exploring decentralized technologies [14]. This highlights how decentralization is becoming important for the digital future.

There are certain disadvantages associated with blockchains [15]. One challenge is the low transaction processing speed of blockchain systems. As an example, while payment systems like VISA can process about 1,667 transactions per second, the Ethereum network can only manage about 20 transactions per second [16]. The complexity of scalability increases as the number of nodes increases. On-chain storage also presents performance and cost concerns. Storing large amounts of data on-chain can be significantly more expensive compared to centralized storage solutions, affecting the synchronization of new blockchain nodes and consuming transaction throughput.

Existing decentralized social media platforms have been analyzed to identify implemented features and necessary enhancements. However, the centralized nature of these platforms raises concerns about data protection. Businesses often exploit user data, transferring it to third parties and profiting from it without users' explicit consent. This issue has led to an increased interest in decentralized social media platforms, where users have greater control over their data. Decentralized social media networks distribute network resources and services, and user data and content are stored on blockchains and independent servers, removing centralized control by a single corporation.

III. Methodology

As discussed in the previous section, it is evident that traditional social media platforms encounter numerous challenges in user data privacy and security perspectives in the dynamic technological landscape. DeMedia, a decentralized social media protocol, is being proposed as an alternative to solve these challenges. This protocol provides a revolutionary path by allowing the establishment of decentralized social media platforms that do not rely on traditional blockchain technology to store user data. At its core, this architecture allows users to store their data on their devices and have control over the data.

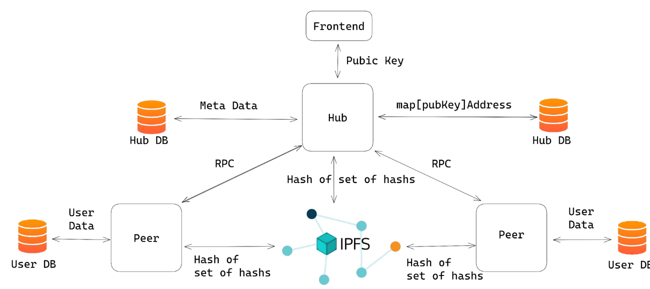

Figure 1. High-level architecture Diagram.

Recognizing the growing concerns surrounding centralized control, data privacy, and security, the DeMedia protocol forms a transformative proposal for a decentralized social media platform. This paradigm shift introduces a novel structure consisting of four key components, each designed to address the limitations of conventional platforms while providing users with remarkable control over their data.

The data decentralization is the core concept of the DeMedia architecture. Unlike traditional social media platforms that collect user data within centralized servers, this empowers users by allowing them to store their personal information on their own devices. This significant change represents a major step towards controlling personal data, encouraging a feeling of authority that has been lacking in the current social media environment. Users can protect their privacy and strengthen their security by avoiding the drawbacks of centralized data storage. This helps them defend against data leaks and unauthorized access.

The second important aspect of the DeMedia architecture focuses on peer-to-peer communication. By leveraging this approach, the architecture facilitates direct interaction between users through a dedicated communication hub. This new approach reduces the significant dependence on centralized servers that often serve as intermediaries in conventional platforms. Consequently, communication speed and efficiency are significantly enhanced, enabling real-time interactions without the bottlenecks introduced by intermediaries.

The third component of the DeMedia architecture is decentralized data storage. This aspect is fulfilled by the utilization of the Interplanetary File System (IPFS), a technology that establishes a secure and fault-tolerant decentralized file-sharing network. The adoption of IPFS ensures that the platform's data storage is distributed across a network of interconnected nodes, mitigating the risks associated with a single point of failure. As a result, the architecture enhances the platform's resilience against potential outages or attacks and maintains uninterrupted access to shared content.

The last component of the DeMedia architecture is the emphasis on data integrity within a decentralized network. This critical element endorses the commitment to maintain the security, reliability, and tamper-proof nature of the stored data. Utilizing advanced cryptographic techniques and fortified security measures, the architecture takes an uncompromising stance on data integrity. As a result, the platform promotes an environment where users can confidently engage in online activities, knowing that their contributions and interactions remain unaltered and authentic.

The DeMedia architecture's ultimate aspiration is to redefine the landscape of social media by embracing decentralization while prioritizing privacy, security, and user data control. As the digital world evolves, the necessity for platforms that support these values becomes even more essential. By offering users control over their data, facilitating direct communication pathways, utilizing advanced decentralized data storage techniques, and safeguarding data integrity, the architecture stands as proof of the possibilities that arise at the nexus of technology and user-centric design.

A. *Peer-to-peer Communication*

Peers play a crucial role in facilitating communication within this decentralized landscape. Acting as clients, they connect users to a central hub, enabling seamless content sharing and exchange. Users have the freedom to host their own hubs or connect to hubs operated by third-party entities. This decentralized hosting approach ensures a diverse and inclusive network, enabling a rich exchange of ideas and perspectives.

The peer-to-peer communication mechanism is the backbone of the decentralized social media protocol. It allows users to establish connections with one another through a network of peers. These peers, also referred to as clients, act as intermediaries, enabling users to interact with a central hub where content is shared and distributed.

By connecting directly to hubs using peers, users enhanced privacy and control over their data. Furthermore, the decentralized nature of peer-to-peer communication fosters an inclusive and diverse network. Users from various backgrounds and regions can connect and share their content freely, enriching the social media experience with a wide range of perspectives and ideas.

B. *Data Decentralization*

The hub acts as the central communication point, orchestrating smooth interactions between peers. By retrieving aggregated metadata from peers, the hub facilitates the distribution of user data to other connected peers interested in the specific context. This decentralized communication architecture mitigates risks associated with data centralization and censorship, promoting free and unrestricted connection.

In decentralized social media, hubs emerge as the facilitators of seamless communication between peers. The hub is the central point of interaction, which plays a major role in enabling users to connect and share their content with others across the network.

In this decentralized communication model, hubs do not possess centralized authority or control over user data. Instead, they act as neutral facilitators, enabling content to flow freely between connected peers. This decentralization mitigates the risks associated with data centralization, ensuring that no single entity can direct the flow of information or impose censorship.

A. *Data Integrity Preservation*

The most important thing is ensuring the security and authenticity of user data. This comprehensive approach empowers users with robust control over their data, protecting it from tampering and unauthorized access.

When users share their content with the hub, the data signing process comes into play. This process involves the creation of a unique signature that incorporates various elements, including peer metadata, content specifics, and hub metadata. This signature acts as a digital signature, guaranteeing the authenticity and integrity of the shared content.

This is achieved by utilizing a cryptographic hash function, Keccak-256. This produces a fixed-size hash value from variable-sized data, which can be used to verify the authenticity of the data later.

The process of generating a signature using Keccak-256 involves feeding the data into the algorithm and obtaining the resulting hash value. The formula for this process can be represented as

$$S = Keccak256(D) \quad (1),$$

Where 'S' is the signature generated, and 'D' is the data being processed.

The same formula is applied to the data to verify the signature, and the resulting hash value is compared with the originally generated signature. The formula for this process can be represented as

$$V = Keccak256(D \mid\mid S) \quad (2),$$

Where 'V' represents the verification result. If 'V' matches the originally generated signature 'S', then the data has not been tampered with, and the signature is considered valid. Otherwise, the signature is deemed invalid.

By utilizing Keccak-256, the DeMedia protocol has ensured that the stored data remains secure and tamper-proof, promoting trust and reliability among its users.

With this comprehensive approach to data signing, users retain full control over their data even after it has been shared within the network. The signature serves as a digital fingerprint, allowing users to verify the origin and integrity of their content at any given time.

Users can ensure that their content and other user's content remain unaltered and secure within the social media ecosystem, empowering them with a sense of trust and ownership over their digital environment.

C. Decentralized storage of media objects

In social media, storing and sharing media objects, such as images, videos, and audio files, poses a significant challenge. The size of these media objects can degrade network performance and seamless data exchange.

To overcome this challenge, DeMedia adopted a decentralized file system. This file system, known as the InterPlanetary File System (IPFS), transforms the storage and sharing of media items on social media platforms.

The IPFS operates on a peer-to-peer architecture, wherein media objects are distributed and stored across multiple nodes within the network. Each media object receives a unique identifier, allowing users to access it efficiently from various sources. This decentralized approach to data storage not only enhances scalability and efficiency but also ensures that media objects are securely accessible, even in the absence of a central server.

By leveraging the IPFS, the protocol removes the bottleneck associated with centralized data storage, enabling unrestricted and seamless data exchange. Users can share and access media objects without experiencing delays or performance issues, enabling a seamless and enriching social media experience.

IV. RESULTS AND DISCUSSIONS

This section presents the outcomes of the research and the practical application of the protocol, followed by a detailed discussion highlighting the findings' significance and their implications for the future of social media architecture.

D. Protocol effectiveness and usability assessment

The development of a demo social media platform provided a practical approach to evaluate the effectiveness and usability of the DeMedia protocol. Through the deployment and testing of this platform, the protocol's features and mechanisms were put to the test in a real-world setting. Users engaged with the platform interacted with peers, and shared content, thereby simulating the actual usage scenario. This usability assessment served as a validation of the protocol's design principles and its applicability to real-life social media interactions.

E. Data integrity verification

A verification mechanism built into the demo platform demonstrated the protocol's commitment to data integrity. Hubs can verify the integrity of the data stored on user devices by checking the cryptographic signatures associated with users' content, generated when the content is stored on the device and published to the network. This verification process provided the platform users with a tangible assurance of shared data's authenticity and unaltered nature, provided control over their data, and demonstrated the cryptographic techniques that enable the protocol's data integrity strategies.

A. IPFS media object caching

Integrating the InterPlanetary File System (IPFS) for media object storage was an important architectural aspect of the protocol. In the demo platform, media objects were cached on IPFS, allowing users to access and share content efficiently. This caching mechanism showcased the protocol's ability to leverage decentralized data storage while ensuring seamless content retrieval. The media object caching capability shows the protocol's scalability and potential to reduce demand for network resources and control the cache handed over to the user.

B. Benchmark tests and performance evaluation

Significant insights have been obtained regarding the operational efficiency of the DeMedia protocol by conducting thorough benchmark testing and rigorous performance evaluation. It was observed that certain aspects of DeMedia's performance were marginally below initial expectations, warranting attention for further optimization in pursuing enhanced network efficiency.

TABLE I. BENCHMARK TEST RESULTS

Test Type	REST (Time in ms)	DeMedia/IPFS (Time in ms)
REST API call vs DeMedia	182.88	432.26
Direct DB fetch vs DB Fetch Through DeMedia	3.35	432.26
Direct DB fetch vs REST API call	3.35	182.88
Time Elapsed to Fetch Image 01	36.62	23.01
Time Elapsed to Fetch Image 02	4.81	9.29

DeMedia API calls and traditional REST API calls were compared in the benchmark testing. Additionally, the performance of data retrieval was examined, comparing the speed of fetching data directly from the DeMedia database to traditional database retrieval methods. The outcomes showed that although DeMedia performed effectively, there was a deviation from the expected efficiency expectations.

This variation indicates a significant field for future research and development. Optimization of network efficiency remains a critical path for DeMedia to reach its full potential in real-world applications. To address this issue, the protocol's complexities will be refined, procedures will be streamlined, and network interactions will be fine-tuned to achieve adequate performance and responsiveness.

The benchmark test results, together with the practical development and testing of the demo social media platform, highlight the transformational potential of the DeMedia decentralized social media protocol. These findings emphasize its viability and usability in real-world scenarios. At the same time, the observations gained through benchmark testing and performance evaluation provide a degree of realism to the assessment of operational efficiency.

The usability assessment demonstrated through the demo platform validated the protocol's design principles and emphasized its applicability in authentic social networking contexts. The integration of the hub panel and data integrity verification mechanisms facilitated transparency and highlighted the protocol's commitment to enabling user control and ensuring data authenticity.

Integrating the InterPlanetary File System (IPFS) for media object caching effectively addressed the data storage and retrieval challenges. It provided the scalability and efficiency of the protocol in storing media objects.

V. LIMITATIONS

Several limitations suggest the areas requiring further investigation and refinement. One significant limitation is the insufficient exploration of scalability challenges within decentralized networks, restricting the widespread adoption of such platforms. Additionally, while the research identifies potential enhancements for the DeMedia protocol's performance, it lacks in-depth insights into strategies for optimizing network efficiency, indicating a need for more comprehensive approaches. Despite the IPFS, the absence of an extensive exploration into alternative decentralized storage technologies beyond blockchains suggests a limitation in understanding and addressing diverse technological landscapes. Furthermore, the oversight of potential challenges in user adoption, including user experience design and the transition from centralized to decentralized platforms, highlights an area demanding focused attention. Lastly, the limited examination of the regulatory landscape governing decentralized social media platforms underscores a gap in understanding the broader regulatory implications associated with their adoption. Recognizing and addressing these limitations will contribute to a thorough understanding and effective development of decentralized social media protocols.

VI. POTENTIAL FUTURE WORK

Future research efforts could strategically target enhancing the DeMedia protocol's network efficiency. This involves improving the network efficiency, simplifying processes, and reducing complexities to achieve better performance and responsiveness. Additionally, there's potential for significant improvements in user experience within decentralized social media through a focus on user-centric design. This includes exploring and implementing easy-to-use interfaces, effective onboarding processes, and educational strategies for users. Another area of exploration involves hybrid models that combine the strengths of both decentralized and centralized architectures, providing a potential solution to scalability issues while maintaining decentralization benefits. Furthermore, incorporating artificial intelligence (AI) and machine learning (ML) techniques could elevate platform functionality, including content recommendation, user personalization, and moderation—all while prioritizing user privacy. Real-world case studies are essential to observe the practical implementation of the DeMedia protocol, considering various user demographics and usage scenarios for valuable insights into its adaptability and effectiveness. Addressing regulatory challenges associated with decentralized social media requires thorough investigation and the proposal of strategies to ensure compliance with privacy laws, data protection regulations, and other legal protocols. Exploring models for community engagement and decentralized governance is crucial, allowing users to play a meaningful role in shaping the platform's evolution—potentially through mechanisms for voting on platform upgrades and feature implementations. Lastly, researching the implementation of economic incentives within the decentralized social media ecosystem is vital to encourage user participation, content creation, and effective network maintenance.

VII. CONCLUSION

In conclusion, this research introduces DeMedia, a decentralized social network protocol that addresses the privacy and security concerns inherent to centralized social media platforms. The protocol's innovative approach enables users to retain full ownership of their data by storing it locally on their devices, mitigating vulnerabilities associated with centralized servers. Employing peer-to-peer networking and cryptographic techniques ensures data privacy and integrity. By leveraging decentralized technologies like peer-to-peer networking and IPFS, the DeMedia protocol offers users a more secure and private social media experience. This approach empowers users with data ownership and control while negating the necessity for costly blockchain infrastructure. The protocol also features tools for optimizing data storage and maintaining data integrity, such as data cache and integrity preservation. Ultimately, the proposed protocol establishes a secure and decentralized social media network that grants users autonomy and facilitates direct interactions, freeing them from reliance on centralized intermediaries. This advancement holds substantial potential for revolutionizing the landscape of social media architecture.

ACKNOWLEDGMENT

The authors of this paper express gratitude to the Sri Lanka Institute of Information Technology (SLIIT) and the Department of Information Technology for the opportunity, along with all supporters and inspirations that contributed to the success of this research.

References

[1] "The evolution of social media: How did it begin and where," 03 March2021.[Online].Available:https://online.maryville.edu/blog/evolution-social-media/. (accessed Aug. 3, 2023).

[2] Y. K. Dwivedi et al., “Setting the future of digital and social media marketing research: Perspectives and Research Propositions,” International Journal of Information Management, vol. 59, p. 102168, 2021. doi:10.1016/j.ijinfomgt.2020.102168

[3] B. Olaniran and I. Williams, “Social Media Effects: Hijacking democracy and civility in Civic Engagement,” Platforms, Protests, and the Challenge of Networked Democracy, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7343248/ (accessed Aug. 3, 2023).

[4] T. Stackpole, “What is web3?,” Harvard Business Review, https://hbr.org/2022/05/what-is-web3 (accessed Aug. 3, 2023).

[5] S. Dhawan, S. Hegelich, C. Sindermann, and C. Montag, “Re-start social media, but how?,” Telematics and Informatics Reports, vol. 8, p. 100017, 2022. doi:10.1016/j.teler.2022.100017.

[6] A. Datta, S. Buchegger, L.-H. Vu, T. Strufe, and K. Rzadca, “Decentralized Online Social Networks,” Handbook of Social Network Technologies and Applications, pp. 349–378, 2010. doi:10.1007/978-1-4419-7142-5-17

[7] M. Qamar et al., “Centralized to decentralized social networks,” Advances in Data Mining and Database Management, pp. 37–54, 2016. doi:10.4018/978-1-4666-9767-6.ch003

[8] J. Benet, “IPFs - content addressed, versioned, P2P file system,” arXiv.org, https://arxiv.org/abs/1407.3561 (accessed Aug. 3, 2023).

[9] S. Kemp, “Digital 2020: July global statshot - datareportal – global digitalinsights,”DataReportal, https://datareportal.com/reports/digital-2020-july-global-statshot (accessed Aug. 3, 2023).

[10] “What is blockchain technology? - IBM Blockchain,” IBM, https://www.ibm.com/topics/blockchain (accessed Aug. 3, 2023).

[11] W. Gan, Z. Ye, S. Wan, and P. S. Yu, “Web 3.0: The future of internet,” Companion Proceedings of the ACM Web Conference 2023, 2023. doi:10.1145/3543873.3587583

[12] C. B. Onete, I. Albăstroiu, and R. Dina, “Consumer between web 2.0 and web 3.0,” Consumer Behavior - Practice Oriented Perspectives, 2017. doi:10.5772/intechopen.71268

[13] P. De Filippi, M. Mannan, and W. Reijers, “The alegality of Blockchain technology,” Policy and Society, vol. 41, no. 3, pp. 358–372, 2022. doi:10.1093/polsoc/puac006

[14] Karim, “Web 3.0 tools: Analyzing facebook and Google’s role,” Coinwut,https://coinwut.com/facebook-google-web-3-0-tools/ (accessed Aug. 3, 2023).

[15] V.Budhi, “Advantages and disadvantages of Blockchain technology,”Forbes,https://www.forbes.com/sites/forbestechcouncil/2022/10/20/advantages-and-disadvantages-of-blockchain-technology/?sh=42cb2a0e3453 (accessed Aug. 3, 2023).

[16] D. Mechkaroska, V. Dimitrova, and A. Popovska-Mitrovikj, “Analysis of the possibilities for improvement of Blockchain technology,” 2018 26th Telecommunications Forum (TELFOR), 2018. doi:10.1109/telfor.2018.8612034 Y. K. Dwivedi et al., “Setting the future of digital and social media marketing research: Perspectives and Research Propositions,” International Journal of Information Management, vol. 59, p. 102168, 2021. doi:10.1016/j.ijinfomgt.2020.102168