IMPLEMENTING A BLOCK CHAIN TO PROVIDE SECURITY FOR CHAT APPLICATIONS

Mrs. T. Sujatha Jayakrishnan
Assistant Professor, Department of Computer Applications and Technology,
SRM Arts and Science College, Kattankulathur
sujathajayakrishnancat@srmasc.ac.in
https://doi.org/10.34293/9789361639715.shanlax.ch.037

Abstract

The Blockchain-Based Chat Application project uses blockchain technology's decentralized and secure features to build a powerful messaging platform that prioritizes privacy. This project uses a decentralized architecture on the blockchain to address security, privacy, and centralization issues that plague traditional messaging programs. In order to prevent single points of failure, messages are dispersed throughout the network rather than on a single server. Only the intended receivers may access the contents of messages thanks to end-to-end encryption, which secures communications. The Blockchain-Based Chat Application prioritizes user privacy, security, and decentralization through blockchain technology in order to give users all over the world a dependable, impenetrable, and decentralized communication platform.

Keywords: *Decentralized, Blockchain-Based, Distributed, Secure, End-to-end encryption, privacy and security.*

Introduction

With the rapid evolution of communication technology, user data centralization, security and privacy have become an area of concern. Centralized Servers: Traditional messaging apps often rely on centralized servers, which adds a layer of vulnerability to data breaches and privacy infringements. In response, the Blockchain-Based Chat Application project has emerged as a creative solution that redefines communication through the secure and decentralized properties of blockchain. Blockchain - A concept first developed for cryptocurrencies like Bitcoin, the basic ideas of decentralization, transparency, and immutability within blockchains make them a great match to combat the issues of centralized messaging.

In an age where data breaches, surveillance concerns, and a general distrust towards entities handling user data are on the rise, the need for a secure and private messaging platform has become apparent. The blockchain-based chat app project aims to transform communication by offering a decentralized alternative that prioritizes privacy and security. By leveraging blockchain technology, the project aims to create a secure, private, and decentralized platform that enables seamless connectivity between users. From cross-platform support to smart contract integration for features and community governance to empower user decision-making, blockchain-based chat applications represent a new paradigm of secure, decentralized communication. Decentralized networks of nodes work together using blockchain technology to improve security and transparency without a single entity controlling the network. By writing messages to the tamper-proof blockchain, they can validate communication, and users can have confidence. These features include smart contracts that allow for the automation of predefined actions in a trustless manner and native

tokens that can be used to incentivize users and facilitate microtransactions. Privacy controls such as anonymous messaging and user-managed access to private data solve data privacy issues and give users more control over their information. Though these applications increase security and user control, there are challenges around scalability and widespread adoption when creating and implementing them. The decentralized blockchain chat app could have native tokens that can help in supporting the important functions of the platform. These tokens can be used to reward user engagement and incentivize active users and network node operators. They would also make micropayments possible in the messaging system. Tokens introduce an additional dimension to user engagement, which can contribute to the growth and sustainability of the network.

Aim and Objective

By leveraging the inherent capabilities of blockchain technology, blockchain-based chat applications strive to transform traditional communication platforms. The development and distribution of such apps is driven by some goals:

Decentralization: One of the core goals of blockchain chat applications is to be decentralized. As a result, the applications offer greater resiliency, as they utilize a network of nodes to share control, instead of servers, which also can reduce the risk of single point of failures and the risk of censorship or data manipulation. Such decentralized applications are in line with the ethos of blockchain, and it's likely in the future that they will provide a stronger and more trustless communications infrastructure. In addition to the need for security, privacy is a major goal. Security: Blockchain chat applications leverage the power of cryptography, such as end-to-end encryption and decentralized storage, to ensure the confidentiality and integrity of user data. This helps in securing the users from unauthorized access and to safeguard the privacy of the communications. Tokenization is used for various purposes in blockchain chat applications. Tokenization generates the active community - The introduction of native tokens encourages active user engagement, rewards users for participation and enables micro-transactions, leading to the creation of a self-sustaining ecosystem where users are motivated to actively contribute to the network. Tokens can also be used to build an economic layer that adds value to the overall experience.

Existing Systems

Blockchain technology has been used to develop a host of chat programs, each with different features and applications. The main idea behind these decentralized applications (dApps) is that they aim to offer secure and private communication interfaces to users on the blockchain.

A few examples: Status is an open source, mobile Ethereum-based application, serves as a messaging and decentralized application browser, users can message, voice/video call and access Ethereum dapps. Censorium is a decentralized messaging platform that implements blockchain technology to achieve message integrity and confidentiality for a secure and private communication channel, using the SNT cryptocurrency for governance, transactions, and more. Censorium is a new kind of Ardor-built communication application that seeks to

establish a platform where users are free to communicate without censorship and enjoy features such as end-to-end encryption and decentralized storage.

BeeChat is a decentralized instant messaging application that runs on its own blockchain to offer users secure messaging, voice and video calls, and in-app transactions using its own native Bee token. By leveraging the power of blockchain technology, BeeChat aims to provide a transparent and secure decentralized communication experience.

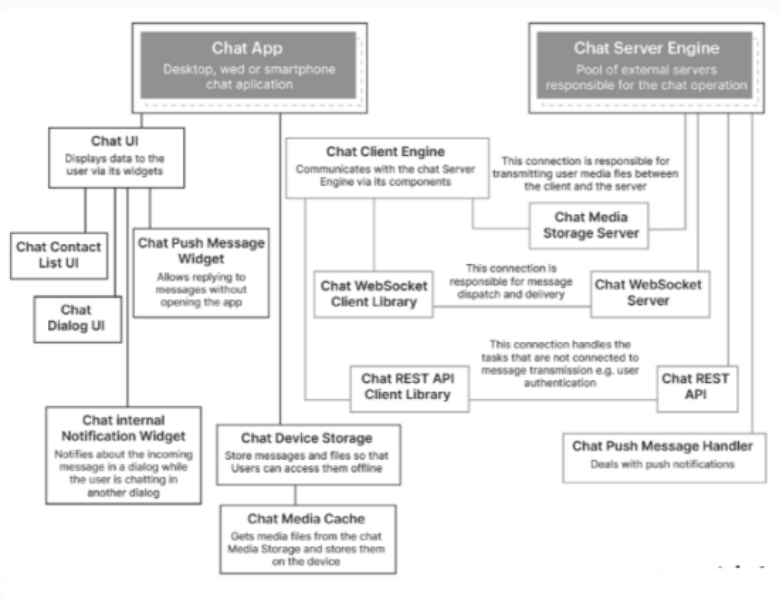
Session - Session is a messaging app built on the Loki blockchain that places a strong focus on privacy. End-to-end encryption and onion routing are used to ensure user communications are secure and to protect user anonymity. Session values privacy and strives to offer a decentralized and censorship-resistant messaging platform to users.

Sylo is a decentralized messaging, voice, and video calling platform. Running on the Sylo blockchain and using the SYLO token as the currency, Sylo focuses on privacy and security as a means to deliver a decentralized communication experience to its users, with the inclusion of blockchain technology to help make interactions transparent and secure.

Proposed System

A proposed design for a chat application based on blockchain network is full of many technical challenges, such as peer-to-peer communication, secure message transmission, decentralized identity management, user data control, and incentives.

End-to-end encryption protects the privacy of messages. Ethereum blockchain stores identities in a secure way. A peer-to-peer network removes the dependence on central servers to carry messages. Users have control over their identities and preferences, and have the power to own their data. A Token system is a way to incentivize users to provide some resources to the network, such as running nodes and validating transactions. wnyIOS and web provide an identical user experience that can be used across devices. The Ethereum blockchain can be used to create smart contracts to verify and register users. Smart contracts create user accounts and make the access permissions transparent on the blockchain when users create accounts for the chat application. The decentralized Ethereum protocol is the main messaging layer of the application. The communication between users is transformed into transparent immutable transactions on the blockchain and Ethereum's decentralized consensus increases the security of communication. The proposed framework can mint native ERC-20 or ERC-721 tokens to support transactions among the chat application. Tokens are often used as rewards to incentivize users who participate in the network, help secure it, or complete certain activities. The tokens can also be used to access special features such as additional storage or increased privacy. In addition, decentralized autonomous organizations (DAOs) can be established in the system for community governance. Collective Decision Making: DAOs allow all members to make collective decisions about how the chat application is developed, what features to include, and what policies to enforce. Democracy: The platform is democratic, allowing users to participate in the development of the platform.



System Architecture

Methodology

A disciplined approach is needed in developing a chat application in the blockchain technology. Define the goals of the application and outline the security requirements, privacy requirements, decentralization requirements, and user experience requirements. Then, do market research and analyze the opportunities and challenges in the blockchain and messaging industries. The next step is to select a suitable blockchain platform based on factors such as smart contract capabilities and consensus mechanisms. Develop the full architecture, add encryption and identity management, add tokens for incentives, and write smart contracts for control. Add messaging functionality, settings, and other options when implementing performance and security monitoring Continuous improvements to the program through evaluation of user satisfaction and planning updates to reflect user feedback and changing requirements. Through this organized methodology the development process will be directed towards the attainment of the project's objectives.

Defining objectives: Clearly outline the goals and objectives for the chat application based on blockchain, including considerations like decentralization, security, privacy, and potential integration with blockchain capabilities such as smart contracts and tokens. Then, enumerate the use cases and features that the application is intended to support based on those objectives: For the chat application choose a blockchain platform with strong smart contract capabilities, such as Ethereum, Binance Smart Chain, Polkadot, or custom blockchains, as appropriate to your needs. Write smart contracts to securely handle user registration, authentication, token transactions, messaging, and end-to-end encryption. Key logic and capabilities required for the chat application need to be coded in smart contracts, and blockchain-based authentication needs to be implemented for secure users onboarding. Decentralised identity solutions such as self-sovereign identity (SSI) could help users control their own personal data while ensuring security. Also explore decentralised storage systems like ipfs to store the message content and media.

Result

Based on the blockchain technology, we have designed a chat application. This program runs on a local server, and therefore offers the users a high degree of confidentiality and anonymity. Since these types of apps are always under threat of security breaches from within their own organization, they can be used in defense and by various security agencies.

Conclusion

Following our research, we designed and deployed Chat Secure, a blockchain-based chat application that represents an important step in the right direction for a private, secure, and decentralized communication platform. Our objective during the development process was to leverage the blockchain technology to eliminate the limitations of traditional messaging ecosystems. The key messages of our contribution are summarized in the following conclusions. End-to-end encryption is effectively implemented into the program to ensure the confidentiality and security of user messages. We have minimized the chance that the centralized messaging platforms will contain faults in security by deploying cryptography methods and centralizing users' data and information.

As the application is decentralized on a distributed blockchain network, it takes away the vulnerabilities of centralized servers. This not only increases the resistance of the system to attacks but also aids in censorship resistance for free communication by users. Immutability and Data Integrity: Storing chat histories on the blockchain ensures immutability and data integrity.

Future Work

Work on a blockchain-based chat application will be an ongoing process, one of iteration and expansion, of adapting to the needs of new users and new technology. The potential points of further development of blockchain chat application are illustrated below. Explore and implement scalability solutions for an increasing user base. You can also consider optimizations such as sharding, layer 2 scaling solutions, or other innovations to increase transaction throughput. Leverage robust offline messaging capabilities to improve the resiliency of the application.

Find ways to securely store and transmit messages while users are off the network Keep up with blockchain technology developments and consider integrating with new and emerging blockchain platforms or technologies that may provide better scalability, privacy features, or interoperability. Interoperability: Look for opportunities to integrate with other decentralized applications and services. For instance, integration with decentralized finance (DeFi) applications or file storage systems can contribute to the overall utility of the chat platform. Extends the community governance model with additional features for transparent decision-making, proposal funding, and voting.

This can also allow the community to have a more active role in the development of the application. Integrate with emerging decentralized identity solutions to increase user privacy and control of their digital identities. This can help to create a more seamless and secure cross-platform experience. Keep track of and regulate blockchain and cryptocurrency

technologies related regulatory developments and changes Ensure that the application remains compliant with changing legal frameworks whilst maintaining the application's principles of privacy and decentralisation. Integrate advanced cryptographic techniques: Explore the integration of advanced cryptographic techniques, such as zero-knowledge proofs, to further improve the privacy and security of user communication. Build an open source community around the project - organize developers, security experts, and fans to contribute to the project's codebase, security, and functionality.

References

1. Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, ―An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends‖, 2017 IEEE 6th International Congress on Big Data.
2. S. Nakamoto, ―Bitcoin: A peer-to-peer electronic cash system,‖ 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
3. G. W. Peters, E. Panayi, and A. Chapelle, ―Trends in cryptocurrencies and blockchain technologies: A monetary theory and regulation perspective,‖ 2015. [Online]. Available: http://dx.doi.org/10.2139/ssrn. 2646618.
4. G. Foroglou and A.-L. Tsilidou, ―Further applications of the blockchain,‖ 2015.
5. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, ―Hawk: The blockchain model of cryptography and privacypreserving smart contracts,‖ in Proceedings of IEEE Symposium on security and Privacy (SP), San Jose, CA, USA, 2016, pp. 839–858.
6. W. Akins, J. L. Chapman, and J. M. Gordon, ―A whole new world: Income tax considerations of the bitcoin economy,‖ 2013.
7. Y. Zhang and J. Wen, ―An iot electric business model based on the protocol of bitcoin,‖ in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.