IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

State of Art in Message Delivery System using Blockchain Technology

Oluyinka I Omotosho, Gabriel O. Olatoye

Department of Cyber Security Science, Ladoke Akintola University of Technology, Ogbomosho - Nigeria

Department of Computer Science, Ladoke Akintola University of Technology, Ogbomosho - Nigeria

ABSTRACT: For years messaging technology has gained a lot of attractions in the social environment even within firms, businesses,organisations and academic environment, messaging systems are now widely used across different regions and countries.Because of this wide acceptance, there is need for more secure and privacy preserving messaging platforms which will enable users to send message without the need to be bothered about security issues.Geographical Distances and sensitivity in most transactions now envisages decentralized messaging system or platform, which evolves conversation controls and permissions away from centralized systems like Facebook, Whatsapp,Twitterand so on.This workdives into the features and additional technology behind message delivery system that uses blockchain technology, as well as its pros and cons in the message delivery system using blockchain technology.

I. INTRODUCTION

Blockchain-based messaging system is a messaging system that uses blockchain technology to store and transmit messages. Blockchain is a distributed database that allows for secure, transparent and tamper-proof transactions. This makes it an ideal platform for messaging systems, as it can provide a high level of security and privacy.

1.1 Blockchain

A blockchain is essentially a fault-tolerant distributed database of records of a public ledger of all transactions that have been executed and shared among participating parties. Each transaction in the public ledger is verified by a consensus of a majority of participants in the system. Blockchain provides a tool for increasing data integrity using a combination of cryptography and consensus. As such, there is no central server point of control. The in-4 KahinaKhacef , Guy Pujolle formation is stored in blocks, Each block contains transactions, a timestamp and a link to the previous block, and is cryptographically protected. What makes it secure is:

- **Public key infrastructure**: It uses public/private key encryption and data hashing to store and exchange data safely.
- **Distributed ledgers**: There is no central authority to hold and store thedata, it removes the single point of failure
- **Peer to peer Network**: The communication is based on the P2P network architecture and inherits the decentralized characteristics.
- **Cryptography**: Blockchain uses a variety of cryptographic techniques, hash functions, Merkle trees, public and private key]. It is difficult to alter the blockchain, to make a modification, it is necessary to succeed in a simultaneous attack on more than 51% of the participants.
- **Consensus Algorithm**: The rules which the nodes in the network fol- low to verify the distributed ledger. Consensus algorithms are designed to achieve reliability in a system involving multiple unreliable nodes. A consensus of the nodes validates the transactions. Choice of consensus algorithm has significant implications for performance, scalability, latency and other Blockchain parameters. The consensus algorithms must be fault tolerant.
- **Transparency**: Each transaction is visible to anyone with access to the system. If an entry can not be verified, it is automatically rejected. The data is therefore wholly transparent. Each node of a blockchain has a unique address that identifies it. A user may choose to provide proof of identity to others.

1.2 Blockchain-Based Message Delivery Systems Architecture

Blockchain-based messaging systems are a new way to communicate that offers several advantages over traditional methods. Using a decentralized network of nodes to route messages, blockchain-based messaging is highly secure and cannot be tampered with or intercepted. In addition, messages are delivered quickly and reliably.

Users can send messages to each other directly, or through a public channel. Public channels allow anyone to join in the conversation, making them ideal for announcements or discussion forums. All messages are broadcasted to all nodes in the network, ensuring that they are delivered quickly and reliably.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

Blockchain-based messaging systems offer a more secure and efficient way to communicate than traditional methods. With quick delivery and high security, they are ideal for both personal and public communication.

1.3 Prons Of Blockchain-Based Message Delivery System

There are many benefits attached using a blockchain-based messaging system, including:

1.3.1 Better Data Security

One of the main benefits of using a blockchain-based messaging system is data security. With messages stored on a decentralized network, they are much less vulnerable to hacks and breaches. Additionally, each message is encrypted and can only be accessed with the correct key, making it even more difficult for unauthorized individuals to access them.

1.3.2 Increased Privacy

Another benefit of blockchain-based messaging systems is privacy. Since messages are not stored on a central server, they cannot be monitored or censored by any central authority. This makes them ideal for users who value their privacy and want to avoid having their messages monitored or censored.

1.3.3 Tamper-Proof Data Storability

Another advantage of using a blockchain-based messaging system is that messages are tamper-proof. Once a message has been added to the chain, it cannot be altered or deleted. This makes it impossible for anyone to change the content of the message or delete it altogether. This feature is especially useful for businesses who need to ensure that their communications are tamper-proof.

1.4 Cons OfBlockchain-Based Message Delivery System

In the wake of recent data breaches, many companies are turning to blockchain-based messaging systems in an effort to improve security. However, there are several potential drawbacks to using such a system.

1.4.1 Data Breaches

Perhaps the biggest drawback of using a blockchain-based messaging system is the potential for data breaches. Because messages are stored on a decentralized network, it can be difficult to track down the source of a leak or hack. Additionally, if one node on the network is compromised, all of the data stored on that node is at risk.

1.4.2 Slow and Expensive

Another downside of blockchain-based messaging systems is that they can often be slower and more expensive than traditional messaging platforms. This is due to the fact that each transaction must be verified by all nodes on the network before it can be completed. For large organizations with thousands of employees, this verification process can take considerable time and resources.

II. RELATED WORKS

Telegram and Whatsapp, two of the most popular encrypted messaging apps, were born out of this demand for secure instant communication. Nevertheless, the use of blockchain-based messaging apps is growing and several new platforms are entering the market. The following are the most current and most promising blockchain-based messaging platforms currently available.

2.1 Secterum

Secretum is a revolutionary decentralized, encrypted, and secure messaging service based on the Solana blockchain. It also allows users to exchange crypto assets as easy as sending an SMS, thanks to its cutting-edge architecture. The qualities and benefits of Secretum are unrivaled:

In contrast to cloud-based messaging services like WhatsApp, all user messages are securely encrypted and stored on authenticated, independent nodes in the Secretum network, ensuring that hackers cannot access them.

The most secure and anonymous sign-up process, which requires only a s crypto wallet address — ensures that all users have complete and uncompromised anonymity.

There is no single point of failure or data storage, avoiding large-scale hacks or leaks like the ones that have damaged Telegram, Facebook, and WhatsApp.

Users who message and contribute additional nodes to expand the Secretum network are rewarded with staking and the native SER coin.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

To send and receive cryptocurrencies and Non-Fungible Tokens, a simple, intuitive, and entirely P2P trading interface is available (NFTs).

Solana's potential of 700,000 transactions per second with an average cost per transaction of around $0.00025 allows for record low costs and almost immediate exchanges.

2.2Cryptviser

Decentralized Cryptviser eliminates the threat of man-in-the-middle (MITM) attacks. A majority of messengers keep your personal information in a single database. Those in control of the information can simply censor, obstruct, or take control of these systems. Removed from the equation are central servers and user information, which Cryptvisor eliminates.

This company's chief commercial officer (CCO), Mark Babbitt, told App Developer Magazine in an interview that its goal is to provide the same level of protection for everyday consumers as it does for enterprises and governments worldwide. On to the Internet of Things (IoT), he went on to say, and how it will only exacerbate the demand for privacy.

2.3 Dust

One of the first blockchain-based messaging platforms to hit the market was Dust. On March 1, 2014, a Los Angeles-based encryption app launched. Having Mark Cuban as a significant backer of the platform led to much media attention.

Dust comes with a few unique characteristics for its customers. Sender and recipient phones automatically delete messages after 24 hours, referred to as "dusting" by some. After receiving their confirmation message, you can also choose to delete their messages from your inbox.

2.4 Echo

The Echo messenger uses the GrapheneBlockchain to keep your conversations private and secure.Sending multimedia messages with live encryption of all audio and video streams is possible with this service. Users can transmit crypto payments directly from the app thanks to the platform's decentralized nature and built-in ability.

According to the company's CEO, ChristophHering, Echo uses an IPFS protocol called Interplanetary File System (IPFS) to speed up messaging. Rather than using the standard HTTP protocol, IPFS uses a content-addressed approach. It is customary for blockchain-based messaging apps to require that the recipient and sender have direct access to the blockchain, which can be resource-intensive. The IPFS client of Echo eliminates this requirement.

2.5 E-Chat

It is possible to use IPFS technology and a peer-to-peer messaging service with the e-Chat software. No central data storage is provided, unlike other typical messaging networks. As a result of this decentralization, MITM attacks are eliminated. In addition, the site allows consumers to reward content creators with monetary compensation. Users can create subscription channels called Crypto, like in the platform's content producer section.

You can make contactless NFC and QR payments right on the e-chat platform. You can send money or cryptocurrency via private messages with this. A built-in cryptocurrency conversion tool is included in the platform, which allows users to swap digital currency right from the wallet app on their phone. You can use a fingerprint scanner, face recognition, or your wallet's private keys to access your personal information.

2.6 Telegram

More than $1.7 billion was raised through an ICO by Telegram, the widely used messaging service (ICO). Telegram has been offering encrypted chat services for some time now, but now the firm plans to go all-in on crypto-friendly integrations. Passport, new software for verifying identity, was the first of these interfaces to go live this month.

Personal and confidential papers can be stored on Telegram's secure blockchain network using Passport. The company uses end-to-end encryption, and the corporation claims that it does not have access to your data.

2.7 Status

Ethereum's well-developed blockchain helps Status keep its clients' private information safe from snoops. Every message that passes through the system is protected by end-to-end encryption. The platform's built-in browser also allows you to explore various decentralized programs (Dapps).

In addition to the decentralized job market, exchange, prediction system, and digital ID service available to Status users, they also have access to several other unique features. Artists may use the Ethereumblockchain for advertising and distributing their work safely.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

III. CHALLENGES IN DEVELOPING BLOCKCHAIN-BASED MESSAGE DELIVERY SYSTEM

Before beginning the development of your messaging app, think about the following issues that may arise along the route. This guide will show you how to avoid common errors and safeguard your messaging app from potential dangers and problems in the future.

3.1 Defining Real-Time Feature Definitions

To be honest, it's going to be challenging to compete with the titans in the messaging app sector. In contrast, we have customers who desire additional features, stability, and usefulness on the other hand. The messaging app needs to be much more than a chat app if it wants to be a competition.

To ensure a happy customer base after a successful launch of your MVP, consider these features:

1. Fonts and stickers are available as per your specifications
2. muting the chat
3. Updates on your privacy status
4. Calls can be either video or audio.
5. Transfer of data

3.2 Security related Issues

App security and protection are at the top of the to-do list for messaging app developers. The security of individual data, the encryption of messages, and the development of a secure project architecture are necessities.

1. Protect yourself to the fullest extent possible, i.e.
2. Through protocols, end-to-end security (e.g. XMPP)
3. use of digital signatures
4. the product's architecture should be designed to keep data safe
5. Ensure that your chat app includes a privacy policy.
6. create additional messenger security functionality that the user can enable.

3.2.1 Stack of Tools

The first step in getting your software to work is making sure it is appropriately packed and built. The easiest way to figure out what tech stack to use for your project is to look at similar ones.

3.2.2 Overloaded Server

This problem may occur when the number of people using apps increases. WhatsApp's optimization necessitates a significant investment in time and resources on the part of skilled programmers.

To quickly assure app scalability, select the server configuration and capacity and appropriate hardware. During periods of high demand, make sure servers are configured to offer stable service.

It is highly recommended to create a list of potential server bottlenecks and an action plan to address them.

3.2.3 Error-Free Update of Your App

Messaging apps constantly process users' messages and data. Ensure that existing data is not lost during the deployment of new features and app updates.

Real-time chat app scalability is a difficult task heavily reliant on the system's underlying design.

3.2.4 Reliable Linkage

Switching from mobile internet or Wi-Fi to a cellular data network might be caused by many factors. In a temporary interruption, the last message may be lost.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

In other words, you should develop a message-sending app that portrays itself as a dependable tool that can reliably maintain a connection and restore any communications that have been lost due to an interruption.

IV. STEPS AND PROCESS OF BUILDING BLOCKCHAIN-BASED MESSAGE DELIVERY SYSTEM

To build your own decentralized chat app there are certain steps you should follow. they are:

4.1.2 Choose the dependency on Platform

A cross-platform or native messaging app may be appropriate for your product's aims and capabilities. The critical difference is whether or not the app is available across several platforms simultaneously or separately for each operating system. There are advantages and disadvantages to both solutions. A greater level of system performance, stability, and security is ensured by native app development, but this comes at a higher cost.

4.1.3 Language to Use

PHP, Ruby, Erlang, and other server-side programming languages are all viable options for server-side software. When it comes to software development, your provider should be able to tell you what is best for your situation. The LAMP product architecture is also one of the most frequent. The operating system is Linux, the webserver is Apache, the database is MySQL, and the backend language is PHP. You can also utilize PostgreSQL, Nginx, Node.js, Ruby, or JavaScript for backend development.

4.1.4 Different services and libraries integration

Data storage services provided by Amazon.com. Connecting to the server via Socket.io, a library for real-time communication between a browser and server. Integration of social media platforms such as Facebook, Instagram, Twitter, etc. Flurry, Google Analytics, Firebase, MixPanel, etc., are some of the analytical tools available. Google Maps, Google Places – Maps & Navigation. Turnio offers SMS services. From MailChimp and Elastic emails: Email Marketing. Braintree, Stripe, PayPal, etc., are all examples of payment gateways.

4.1.5 Using open-source technologies

Using open-source technologies rather than proprietary ones is the general strategy. Instead, it is possible to use established libraries and frameworks that have already demonstrated their worth.

4.1.6 Developing the best User Experience

When choosing a tech stack for your messaging app, prioritize your users' experience and the chat app's speed, performance, and security.

V. CONCLUSION

Our proposed scheme can effectively handle the problem of the trustworthiness of event messages in a reliable way by using blockchain technology. We can conclude that while blockchain based message delivery system is secure in terms of privacy it is not an efficient implementation for message delivery system due to the aforementioned draw backs.

REFERENCES

[1] A. Lei, C. Oga[1] G. Martuscelli, A. Boukerche, P. Bellavista, Discovering traffic congestion alongroutes of interest using vanets, in: IEEE Global Telecommunications Conference,IEEE GLOBECOM, 2013.
[2] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash SyNakamoto, S. (2008),Bitcoin: a peer-to-peer Electronic Cash System, 39, 2008, p. 5367. Consulted, 19.doi:10.1007/s10838-008-9062-0stem, J. Gen. Philos. Sci., 1.
[3] Z. Zheng, S. Xie, H.N. Dai, H. Wang, Blockchain Challenges and Opportunities: ASurvey, Work Pap, December, 2016, pp. 1–9, 2016.
[4] A.M. Antonopoulos, Mastering Bitcoin, First Edit. United States of America: OReillyMedia, Inc., 2015.
[5] N.Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy tradingthrough multi-signatures, blockchain and anonymous messaging streams, IEEETrans. Dependable Secur. Comput. 15 (5) (2018), 840852.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 8, August 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0908049 |

[6] B. Ostermaier, F. Dotzer, M. Strassberger, Enhancing the security of localdangerwarnings in vanets-A simulative analysis of voting schemes, in: The 2nd International Conference on Availability, Reliability and Security, 2007,pp. 422–431.

[7] R. Shrestha, S.Y. Nam, Access point selection mechanism to circumvent rogueaccess points using voting-based query procedure, IET Commun. 8 (16) (6 11 2014)2943–2951.

[8] E. Al, A Secure Key Management Scheme for Heterogeneous SecureVehicular Communication Systems, vol. 111, ZTE Communication Magazine, 2016.

[9] B. Leiding, P. Memarmoshrefi, D. Hogrefe, Self-managed and blockchain-basedvehicular ad-hoc networks, in: Proc. 2016 ACM Int. Jt. Conf. Pervasive UbiquitousComput. Adjun. - UbiComp, vol. 16, 2016, p. 137140. January.

[10] A. Dorri, M. Steger, S. Kanhere, R. Jurdak, BlockChain: a distributed solution toautomotive security and privacy, IEEE Commun. Mag. Mag. 55 (12) (2017),



INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details