2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN) | 979-8-3503-3802-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/CICTN57981.2023.10141385

Chat Web App using Blockchain

Mayank Mohan
CSE Department, ABES Engineering College, Ghaziabad

Kadambari Agarwal
CSE Department, ABES Engineering College, Ghaziabad
Kadambriagarwal@gmail.com

Kaushlendra Gupta
CSE Department, ABES Engineering College, Ghaziabad

Mohammad Arsalan
CSE Department, ABES Engineering College, Ghaziabad

***Abstract* – As today's world is the world of the technology and we all are depends on technology in one way or in another way.We all are using the apps which are secure we can't say as our all the data is stored to the companies whose app we are using. As today's app which we are using are not pretty secure and the administration can change the data or may misuse the data.So to protect the users data we are developing the app using blockchain. Blockchain apps are also known as the Decentralised apps which uses the peer-to-peer network and it ensures that due to central node failure no other network failure should be there. The Blockchain apps treats as immutable ledger that allow the chatting in a decentralized manner. A Decentralized apps for conversation and exchange of data is a need in today's world because keeping data and information on a centralised server can be risky and it may be costly too. We can implement different ways to share data and to communicate to others using decentralised apps. By gathering the Blockchain and decentralised apps we can make a better and secure apps which will be secure a,easy to use and less costly.**

Keywords—Decentralised, Blockcahin, Smartcontract, chat web app, nodejs, expressjs, end to end encryption, secure, cost reliable.

I. INTRODUCTION

As in today's world people are using the apps very frequently many more things are doing using application from shopping to selling everything people are doing using applications. So during use of these apps we do a lot of data sharing and information sharing which are stored by the apps server which are mainly centralised which may get disclosed or may get breached or leaked by the company of by any hacker so to save from all these problems we need security tow awards our data[1]. Also, the traditional apps used the centralised server to store the data which means once the server get damaged the whole network of the apps will get destroyed. For example, the WhatsApp uses the centralized server so once the single server gets down the whole whatsapp faces the problems. To overcome all these problems, we proposed our paper which is chat web app using the blockchain. It used the decentralized manner to store the data which are very safe and secure. The blockchain [2] used the decentralised network in which the nodes are there which are connected to each other peer to peer. In our application the data are stored on the nodes which are connected to each other in a decentralized manner, so if the anybody wants to change our data or want to steal our data then he/she mush have to visit multiple nodes on which our data are stored which are impossible to find and by this way we can secure our data and maintain our privacy.Also the data stored used a hashing fucntion(256 bits) for the encryption .

A. Problem Background

People are using the apps from centuries but as the people are developing the apps in smart way the bad minded people are also searching a new way to harass the people .And now a days security is very big issue for the people.People are using the traditional apps which are deployed on the servers and are storing the data on the servers.For example, JBoss Application server,GlassFish, or Tomcat.But we will use blockchain to deploy the apps and to store the data in a decentralised manner.

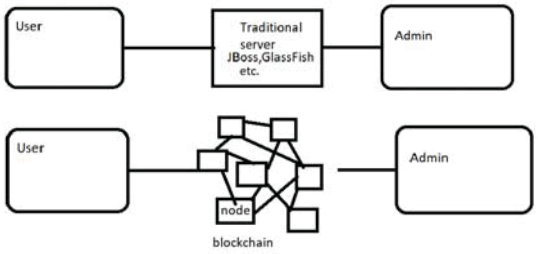


Fig. 1. Compare between traditional and blockchain server.

After Proposing the traditional apps system, we made the decentralised app system.

B. Problem Statement

To develop a secure and trustworthy decentralized chat web application which should be free from all types of security breaching, easy to use, secure your data and should be cost effective.

C. Research objective

The main purpose of the research paper is to provides the solution towards the traditional app which are storing the data on the centralized server by providing the app using blockchain and decentralized manner of storing the data. To provide the more secure platform for chatting and resource sharing. To decrease the immutability possibility.

II. MOTIVATION

Blockchain have become the great interest to the engineers and the companies because it is so immense and it has so much commercial potential and it it spreading very rapidly as the cryptocurrency. The proposal to build a decentralized domain name server on Bitcoin was also released as the first alternative coin, BitDNS called Namecoin. Bitcoin has great computing power to protect blockchain data [3]. However, very difficult to modify the bitcoin with the new functionality because of its complexity and it requires the consensus breaking changes. The blockchain is growing very rapidly with the exponential rate that extends and store Secure end to end information based on blockchain. Ethereum

is both a platform and a type of blockchain, used for decentralized applications called smart contracts.
Ethereum addresses are unique identifiers, so ownership does not change and activity can be tracked and analysed. A smart contract is executable code running on the blockchain that allows two parties to reach agreement automatically. Problems posed by the age of digitalization of security of the data so to secure the data the more securable app is required and hence our app will be beneficial for all such communication which are to be secure.

III. Literature Review

The literature reviews are so much important part of the research paper as from the literature of the previous people we can know the previous work done by anyone and hence it is one of the important part of the research paper.We first review the previous papers and then according to then we will classify that what work have been done and what we have to add now ,what changes we can do and when.Here we have done some literature review of the paper written by some other researcher.

The application of Blockchain on social media-College of Electronic and Information Engineering, Tongji University, Shanghai 201804, China; mahamat@tongji.edu.cn (M.A.H.)

It is a social media using blockchain survey in which they are providing the different aspect of the blockchain on social media. But they are not building any chatting application instead they are using multiple technologies for the security of the data.

Blockchain Technology chat Application-School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India.In this paper the they are also working on the decentralised app but not developed till , but our software is developed and will give a very efficient result and they are not using nay hashing method for the data compression and data encryption.

Chat-bot application using cryptocurrency-Department of Computer Science and Electrical Engineering, UMBC, USA.This is the research paper the researcher is telling about the chat bot application using cryptocurrency in which the data is collected and the chatbot is first trained with the huge amount and then the chatbot will work and there is no surity of efficiency of correct answers, but our app will work in the Realtime and it is a chat application, the individuals can chat through this.

IV. Proposed Methodology

In this method we are using the many advanced technologies such as for front end HTML5, CSS, JavaScript and for the backend ExpressJs ,Reacts, mongoDB, NodeJs based web application where the users can do the conversation and can share the information and data. The information of all the users will be saved on the block of the blockchain that is linked to each other. Firstly, the user will make their own emailids and credential id using emailid and then they will do the sign in to the page after signing he/she can do the conversation using the platform[6].

After the user get login, the user will check the other user to whom he/she wants to talk if the other user will have account, then it will show to first user and the conversation will be happen but if the other user is not available then the first user can sent the invitation link to the other user and may invite to join their chat.

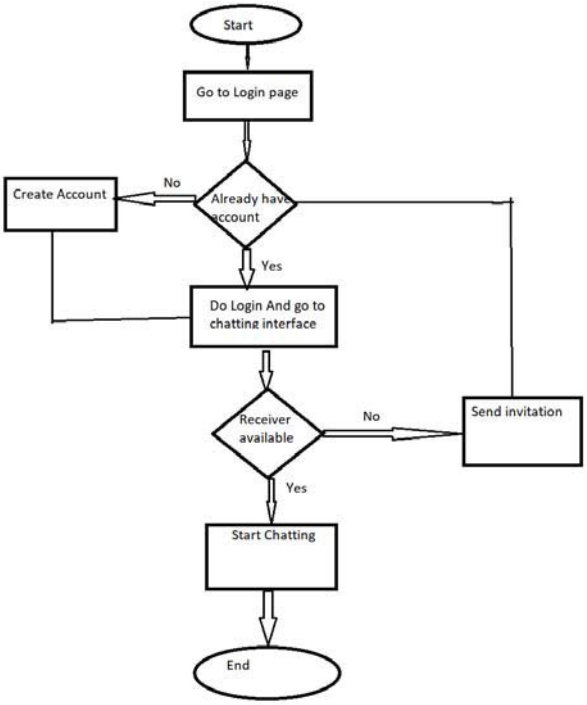


Fig. 2. Flowchart for the working of chat application.

V. Overview of Blockchain, Contracts and Other Technologies

A. Blockchain

The blockchain is a new growing technology, and it is a distributed ledger which are used to store the information and data permanently of all the data that are being used in chatting and sharing of data, it stores the data in a secure, immutable and chronological manner. It basically uses the nodes which are connected to each other to keep the data secure.

Blockchain can be categorised basically into three types Private Blockchain (the member is chosen based on conditions), Public Blockchain (blockchain used by anyone) and Consortium Blockchain (also known as semiprivate blockchains limited to some group).

The Blockchain tech comprises of several components a such as distributed and immutable ledger,a consensus mechanism and smart contracts.

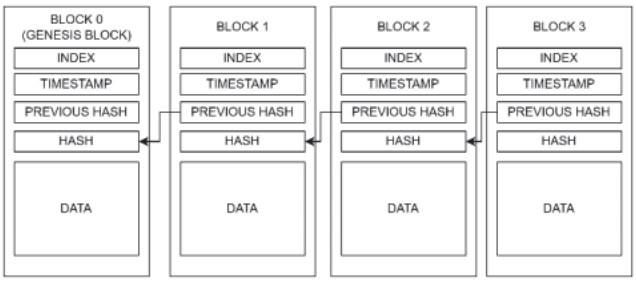


Fig. 3. Structure of Blockchain network.

B. CRYPTOGRAPHY AND Hash function

These functions are the algorithm for cryptography which are majorly uses in the technology of block chain. In this

algorithm when we give it a message it returns the string of bits with the fixed structures and also length. Output of this hash function is named as hash value. And it is formed using hashing algorithm from the data and it is always one way and it cannot be reversed.

RSA-256 is one of the most illustrious of all the cartographic hash functions.

RSA-256 main requirements are:

- Its computation is fast.
- It is not get hacked easily.
- It only supports Encryption.
- It is Deterministic.
- If any minor changes is done the whole data will change.

C. *Solidity*

It is generally an object-oriented language which is created by the Ethereum technology which is also a very big market of the Crypto currency. It is designed for the implementation of the Smart Contracts. It is also known as contract-oriented language, and it is highly influenced by the different programming language which runs on the Ethereum and different types of others crypto currency Virtual Machine (EVM). Solidity also supports the different types of complexity of algorithms and different types of users defined libraries and also different types of others functions, Programming and inheritance.

D. *SMART CONTRACTS*

Smart contracts are programs which basically runs on the Blockchain networks written in the Solidity Language which executes once when the specific condition is meet. Smart Contracts are also used to automate the workflow and for the triggering the next actions during particular condition. It is the only responsible for writing and the reading of the data on the blockchain and as well as for the logic. In our application the smart contracts are used to write the data of the users generated during the conversation. For this first we will create the front end using ReactJs and server using the NodeJS and installing all the requirements and after that we will write the smart contracts and then we will deploy it.

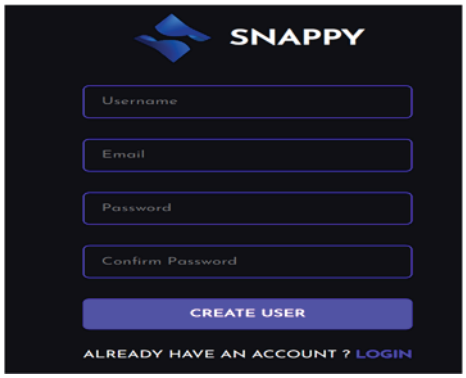
The Smart contract will store the data in the form of the object.

VI. IMPLEMENTATION AND RESULTS.

In this Paper the implementation, design and functioning of Chat web application using blockchain is discussed. The application which is made will be accessed by the user and admin but data will no be accessible by admin. The user can share the data and can change the data. There are various modules which we are using to make the web app unique.

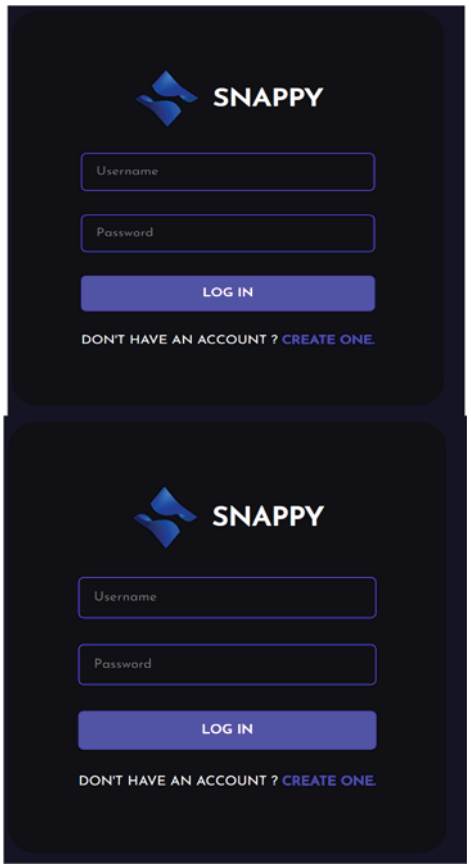
A. *Signup Module:*

This is the module used for the signup of the user, if the user Is already created an id then he/she will simply signup with id and password and then he can do the conversation. If the account is not created then the user will have to first make an account and then only he/she can do the signup and use the further facility of the app.



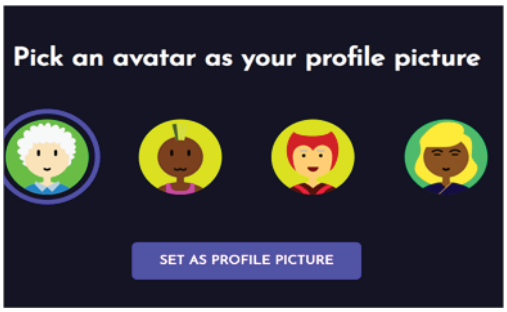
B. *Login Module:*

Int this module the user can do the login into the app using id and password then only the user can access the other services of the app first when the user will login then an otp will send to the user's emailid and using that OTP the user can do the login.



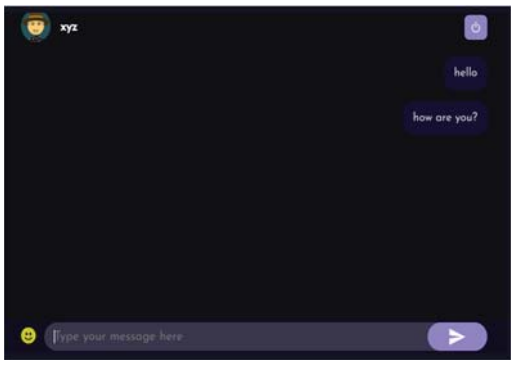
C. *Avatar Module:*

In this module the user can choose the avatars as the profile picture during the making of the user id as per their choice.



D. User chatting Module:

Here the user's ids are shown who are made the ids on the web app named as Snappy and the platform is shown for the chatting where the users can do the chatting with the others users.



VII. Future Scope

This paper is very fruitful for the future aspects as day by day the problem of the breaching of data is increasing and the hacker are becoming very active who can steal the data. So to save the data from stealing and making the information more secure this app will be very fruitful. This app will provide the decentralised storage of the data which will be very tough or impossible for the hacker to steal the data. So in future all the company will use this idea of storing the data so that they could provide the security to the data of the people.

VIII. Evaluation

A. Advantages:

In our research paper the approach we used will remove the central authorities and will use public blockchain technology such as a distributer, the ledger of the identity and the associated public keys. We will use the blockchain to store the digital signature and the public keys and the peer-to-peer confidential information. Once it is started then it will work automatically and will save the data in a secure manner which will not be accessed by any other user rather than admin.

This follows the three security formulas the integrity, confidentiality and the reliability.

Confidentiality: Once the communication between the two users will start then their data and information will save on the blockchain and will be peer to peer encrypted and can be accessed by the users whose data is this.

Integrity: The blockchain always check the validity of the information which are being shared such that the information is true or fraud. It will always check that the data belongs to that person is only opened by that user only and other cannot use that information.

Reliability: It is very tough to shut down all the machines participating in the blockchain technology simultaneously, hence the data will be always online and the user can access the data at any time anywhere and the changes for the data loss will be very less

B. Limitations:

In the blockchain technology or apps the smart contracts which are executed sequentially may affect the performance and efficiency of the blockchain app in a negative manner. After sometime when the smart contract will be more than a limit then it will reduce the efficiency of the blockchain or app.And in actual it is very tough to modify the existing nodes of blockchain technology. So that the design of the blockchain is done with very attentively such there is no chance of any mistake.

IX. Uniquness

As now a days many more software's are using for the purpose of chatting and data sharing. But the main problem for the software now a days is security and privacy. And hence many such software are then presented which are providing the end-to-end encryption such as WhatsApp and telegram but they are also not able to provide the data security when the data server is hacked, they the data will be breached. But in our app this bug is not there in our app the information will be secure even after the server is getting hacked because our data is deployed on the nodes of the blockchain which is impossible to creack till now.

X. DISCUSSION

In our Paper the scope is unlimited to a very large scale it is the future of the technology that in the coming days all the companies will use this technology for the security purpose of the data. As the day by day the data leakage is happening and in the coming days the data will be the weapon to kill anyone. So, this app will be more secure but require a large infrastructure to store the data and to secure the data. Also, along with the chat it will resolve the fake new or data problems. As now a days the fake data is shared on the WhatsApp and Facebook type social media but this app will store only the authorised data which will be real.

XI. CONCLUSION

In this paper knows as Snappy we are developed and apps that are using the blockchain the the smart contracts in very efficient way Blockchain have shown the very efficient potential in the transformation of industry. Now we are planning to implement out paper for the base of our result imperially and to demonstrate the viability of the paper. And now in our paper we will apply the smart contracts technology which is used to store, validate and to provide the certificate of the public blockchain. The individuals' certificate will contain the public key, address [21] of the individual and the smart contract address. Also be eliminating the centralised server with the decentralised approach we are ensuring the more safety and security of the data and the communication. The communication using the decentralised application are making the intersection between two or more people very easy and efficient. The apps now a days used are using the intermediating node while our app will not use any intermediary node for the communication so that its security is more and are more efficient.

XI. References

[1] Hisseine, M.A.; Chen, D.;Yang, X. The Application of Blockchain social Media:A Systematic Literature Review. Appl.Sci. 2022,12, 6567.

[2] Sharma,R.R.;Kumar,A; Blockchain Technology: Chat Application 7260 Turkish Online Journal of Qualitative Inquiry (TOJQI) Volume 12, Issue6, July , 7260- 7268.

[3] Electronic Voting in Europe-Technology, Law, Politics and Society, vol. 47, pp. 83-100, 2004.

[4] Avasthi, S., Chauhan, R., & Acharjya, D. P. (2021). Techniques, applications, and issues in mining large-scale text databases. In Advances in Information Communication Technology and Computing (pp. 385-396). Springer, Singapore.

[5] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". 2017 IEEE International Congress on Big Data (BigData Congress) (2017).

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," (2008).

[7] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. "Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services", 14(4), 352. (2018).

[8] https://www.dapp.com/article/annual-dapp-market-report2018, Gregorian calendar month 2019 "Dapp.com 2018 Dapp Market Report" https://www.dapp.com/article/. (2019).

[9] R. Li and H. Asaeda, "A Blockchain-Based Data Life Cycle Protection Framework for Information-Centric Networks," in IEEE Communications Magazine, vol. 57, no. 6, pp.20-25, June 2019 .

[10] Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and PrivacyPreserving Smart Contracts," 2016 IEEE Symposium on Security and Privacy (SP), 2016.

[11] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system", [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[12] Harry Kalodner, Miles Carlsten, Paul Ellenbogen, Joseph Bonneau, Arvind Narayanan: An empirical study of Namecoin and lessons for decentralized namespace design. Blockchain (2014) .

[13] Lakshmi Siva Sankar,Sindhu M,M. Sethumadhavan: Survey of Consensus Protocols on Blockchain Applications, International Conference on Advanced Computing and Communication Systems (ICACCS -2017) .

[14] Du Mingxia, Ma Xiaofeng, Zhang Zhe, Wang =Xiangwei, Chen Qijin: A Review on Consensus Algorithm of Blockchain, IEEE (2017) .

[15] Dai, Yue Shi,Nan Meng, Liang,Zhiguo. From bitcoin to cybersecurity: a comparative study of blockchain application and security issues/ICSAI, pp 975– 979,(2017) .

[16] Munees Ali, Jude Nelson, Ryan shea, Michael J.Freedman.Blockstack:A global Naming and Storage System Secured by Blockchain, USENIX Annual Technical Conference (2016).

[17] Conner Fronknecht, Gragos Velicannu, Sophia Yakoubov, CertCoin: A Namecoin Based Decentralized Authentication System(2014) .

[18] Oleg Khovayko, Eugene Shumilov: EMCSSL Decentralized identity management,passwordless logins, and client SSL certificates using Emercoin NVS http://emercoin.com,(2016).

[19] Andrea Corbellini, https://andrea.corbellini.name/2015/05/30/ elliptic-curve-cryptography-ecdh-and-ecdsa.ECDH and ECDSA(2015).

[20] J. Grills. (2019, May 15) "Is voice activated chatbot better than the text-based chatbot?". Accessed: 2020-06-01. [Online]. Available: https://chatbotsmagazine.com/is-voice-activatedchatbot-better-than-the-text-based-chatbot-7230e9161620.

[21] E. Brill, "Transformation-based error-driven learning and natural language processing: A case study in part-of-speech tagging," Computational linguistics, vol. 21, no. 4, pp. 543–565, 1995.

[22] A. Shostack, Threat modeling: Designing for security. John Wiley & Sons, 2014.

[23] "Hyperledger Fabric". Accessed: 2020-07-10. [Online]. Available: https://www.hyperledger.org/use/fabric.