Turkish Online Journal of Qualitative Inquiry (TOJQI)

Volume 12, Issue6, July , 7260- 7268

Research Article

Blockchain Technology: Chat Application

Vikas Bhardwaj,

School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

Raja Ram Sharma,

School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

Akhilesh Kumar,

School of Computer Science and Engineering, Galgotias University, Greater Noida, Uttar Pradesh, India

ABSTRACT

Blockchain is a method of storing data that makes it extremely difficult, if not impossible, to edit, hack, or update the system. As time passes, blockchain technology becomes more popular, and blockchain-based applications, also known as DApps, which will be used in this article, are becoming more widely recognised. We will construct a chat application based on a decentralised network in this article to eliminate its absolute reliance on centralised players. On a peer-to-peer network like Ethereum, the actual message and data will be kept. To offer decentralised storage and efficient lookup, we will employ a blockchain and distributed hash table (DHT). which will describe what we will do, which is a trendy issue among academics and trades. Except for the fact that DApps are important, we currently have a limited grasp of DApps and nature. To close the data gap, this paper presents a file for the most comprehensive blockchain-based DApps analysis to date, which includes 995 Ethereum DApps data and 29,846,075 dealings logs above them. We usually do a descriptive investigation of Dapp preferences, characterise patterns of how Dapps use good contracts to gain access to fundamental blockchain, and evaluate the results issues with the post and misuse of DApps In support of the findings, we propose a large number of Results for DApp users to choose the best DApps. Dapp developers must work harder in order to create more efficient DApps, and vendors must likewise support them.

Keywords—Blockchain, DApps (Decentralized applications), Ethereum, Smart contract

I. INTRODUCTION

Satoshi Nakamoto founded cryptocurrency in 2008, and the money is known as bitcoin [2]. Blockchain technology has quickly expanded, attracting a lot of attention from academia and industry. The blockchain has been relocated and distributed as a digital public book for documenting transactions on many nodes for every record concerned; it cannot be changed by reversal without causing all subsequent blocks to be modified.The blockchain has emerged as one of the most promising infrastructure technologies within next generation of online-based programmes, such as

social services, the internet of Things (IoT), name systems, and security [3], due to the benefits of power allocation, consistency, security, and transparency. Blockchain, in fact, is a collection of distributed software packages that give procedural power for applications that use several computation nodes.They do not have a single management, but they are maintained according to approved compatibility standards, and they are used in blockchains for shared use, a unique type of package in which the application is not owned by a single company. DApps are typically seen as apps that run on a Peer-to-Peer (P2P) network of laptops rather than on a single computer.

Many fashionable DApps, such as BitTorrent file sharing, BitMessage rapid electronic communication, and Popcorn video streaming time, have been established and are widely used. Blockchains provide a standard release of calculation with a method of intelligent agreements, making it easier to develop DApps for a variety of scenarios. The Ethereum blockchain, for example,offers comprehensiveAlan Mathison is a British actor. Partnerships for Turing intelligence developers to create programmes with a common goal. Numerous distributed ledger technology DApps are now available and accepted in virtually every place as a result of the development of blockchains. Ethereum The DApp Market, as shown in a new analysis, the biggest market cryptocurrency based on DApp, has surpassed billions of dollars since January 2019[4]. The blockchain app based on DApps is becoming increasingly popular these days, however there is a lack of knowledge of such blockchain-based systems[5]. The normal use of data, such as the number of transactions and the number of daily active users, is heavily emphasised in industry reports . The underlying blockchain system and the mechanism of smart contracts performed on block chain networks , are the key topics of education study[6]. Some researches delve into the characteristics and development practices of blockchain-based DApps.

There are four components in the blockchain system:

1. node application
2. shared ledger
3. consensus algorithm
4. virtual machine

- Node Application:

  Computers that are linked to the internet must instal and operate a computer application in order to provide an environment to the computer, as well as a client node. In the case of a cloud system, for illustration, cloud service providers must be installed to develop a great ecosystem.

- Shared ledger:

  A shared ledger is the fundamental component of the blockchain ecosystem. It is a data node that is shared by all programme users; hence, modifying one data node will automatically destroy the file, making it difficult for a hacker to get access to the system. It's a data model that's controlled by the node application.

- Consensus Algorithm:

  This is a necessary part of the block chain environment. It is, in essence, a technique that is involved in the implementation of the node application. It will demonstrate how well a blockchain technology can get a same ledger result.

- Virtual Machine:

  A virtual machine is the last fundamental piece of the bitcoin network. It is deployed as

the subject of a node application that is run by each platform stakeholder.

II. HEADINGS

1. Introduction
2. Aim and Objective
3. Literature Survey
   - 3.1 Blockchain Application
   - 3.2 Peer-to-Peer Application
   - 3.3 Security
   - 3.4 Performance
4. Problem Statement
5. Figures and Result figures
6. Scope
7. Proposed System
8. System Architecture
9. Advantages
10. Results
11. Conclusion
12. References

III. AIM AND OBJECTIVE

- The aim of this paper is to provide details about our research and to disseminate data protection information using blockchain solutions.
- We will limit the likelihood of any change to the system or alteration that can be made as a matter of fact, resulting in an immutable system. The system will keep functioning even if a node goes down, making it crash-proof.

IV. LITERATURE SURVEY

[1] It is a paper in which the writer proposes all of the conceivable uses and applications of the blockchain in conjunction with decentralisation. The article also underlines what future blockchain uses will entail. There's also a full analysis on the benefits it offers, as well as the various areas wherein blockchain may improve computation and how it compares to traditional approaches.

To the best of our knowledge, our research isn't the first detailed analysis of blockchain-based DApps. During this section, we will first examine the similar research of blockchain environments that require it to run, after which we will shed some light on P2P applications, which are the most common type of DApps.normal sort of DApps

1. Blockchain application

   For its decentralization, tenacity, data and verifiability, Blockchain is commonly used in incognito commerce, permanence services, and bridge transactions due to its decentralisation, toughness, data, and repeatability. As a result, block chain [7], IoT (Internet of Things) [8], information security [9], [10], edge computing [11], and application software engineering [12] are widely used in banking services.

2. Peer-to-peer Applications

   DApps are applications built on decentralisation, often known as a peer-to-peer

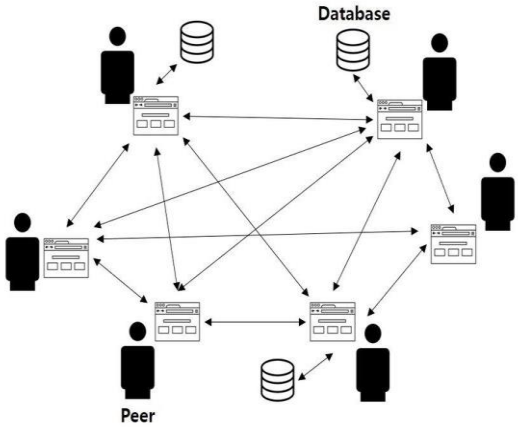
network [13], which necessitate a significant amount of research and investment in addition to security, application, and scalability.

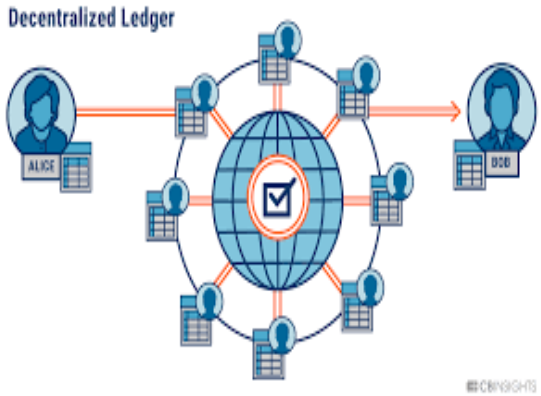
3. Security

   P2P entire network is divided into two parts: P2P network security and unethical network users who can jeopardise the network's protection. Researchers detect assaults [14], employ more technologies like reliable computing [15], and style new rules [16] to improve the security of the P2P network. Additionally, several detrimental behaviour in P2P applications have been discovered [17].

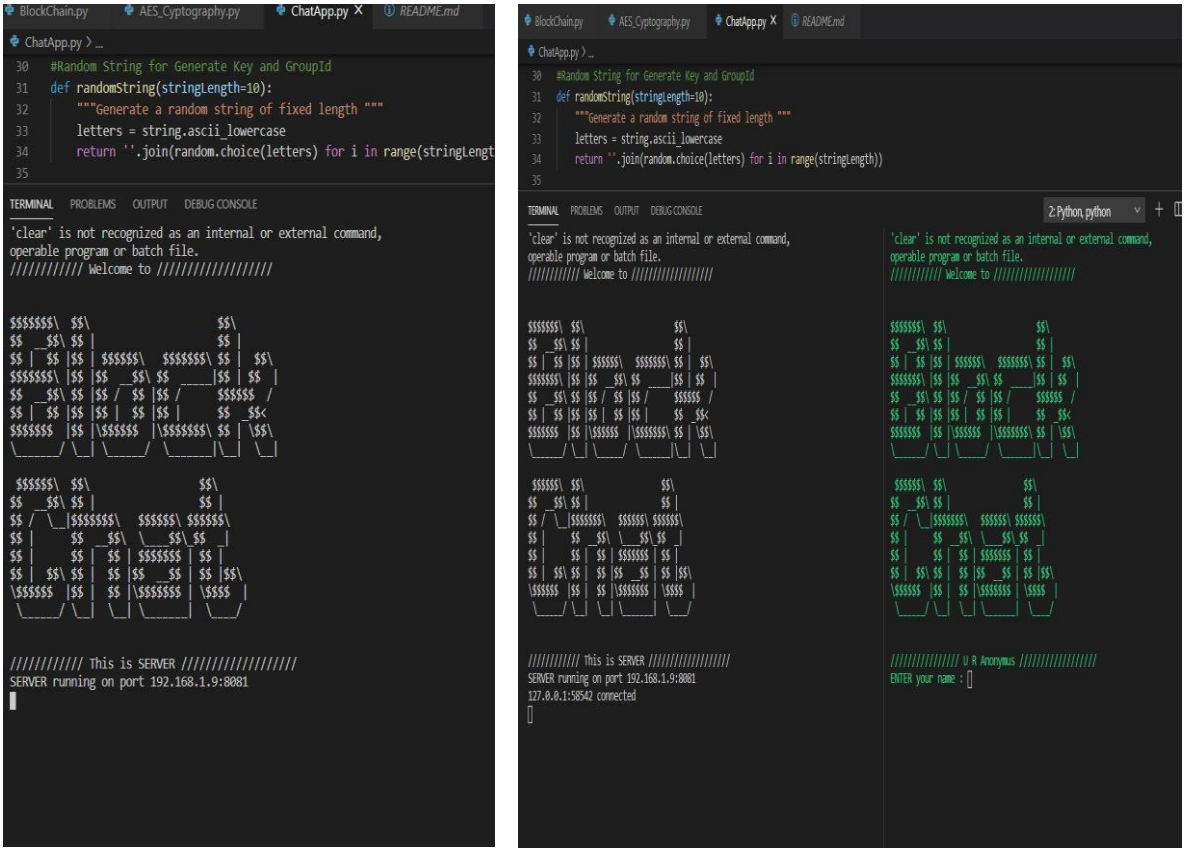
4. Performance

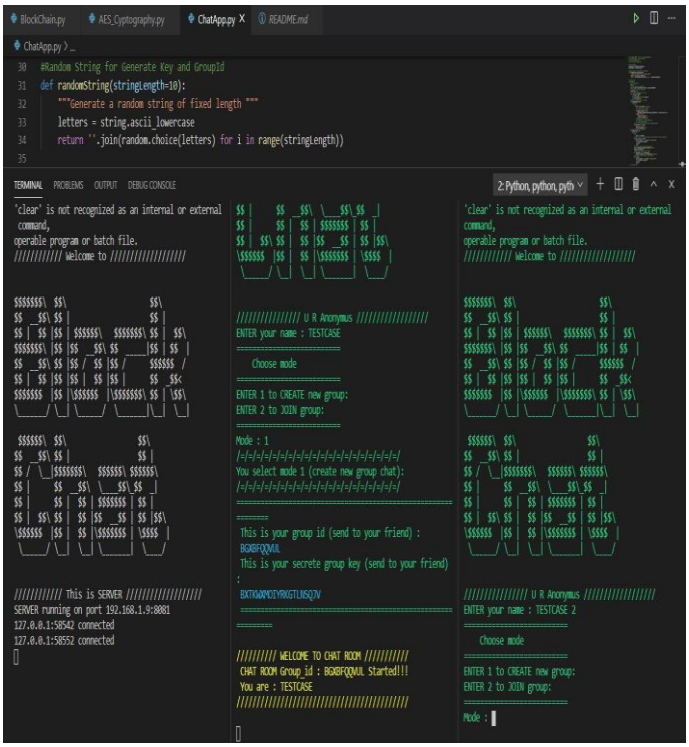
   The applications that use the P2P network, particularly file sharing systems, are subject to becoming a major workload for the local network. Researchers are constantly evaluating the effectiveness of P2P networks [18], [19], and are attempting to evolve P2P-based applications by optimising the application layerer [20] and network layer [21]. Application. P2P technology is widely used in a variety of fields, including digital information, shared calendars, developmental [22], privacy, and many others. Cryptocurrencies, for illustration, a currency digital currency was created in 2009 and is similarly based on a peer-to-peer network. There are a huge number of cryptocurrencies that have been released, which has led to the rise of blockchain technology, particularly distributed ledger technology [23]. According to CoinMarketCap, there are currently over a pair of cryptocurrencies in the globe. Few studies have been conducted on blockchain-based DApps, yet these DApps have a significant impact on the blockchains on which they operate. There's been some work done to help developers make Blockchain-based DApps [24].

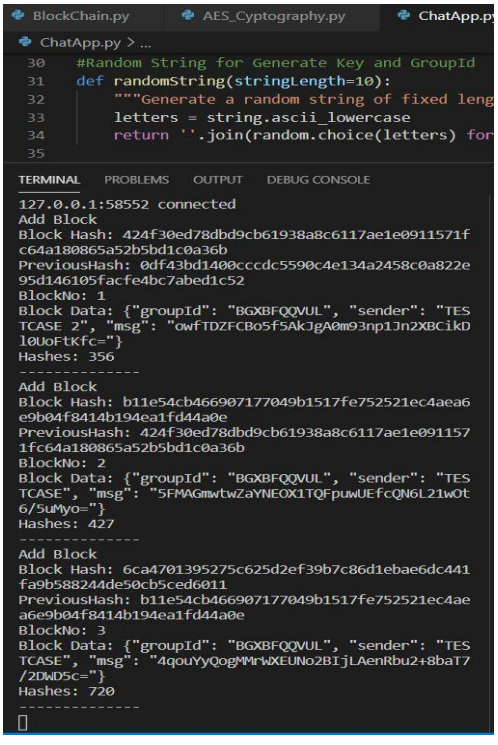




V. FIGURES AND RESULT FIGURES







VI. PROBLEM STATEMENT

The solution we're utilising right now takes a centralised approach to information sharing and communication among applications that are related. Because the data is stored in a centralised data warehouse, there is a significant risk of data loss if the base station fails. There are numerous data and information forgeries. Without any recognised root offender, products post advertisements on social media networks (like whatsapp and telegram). Data on the web system can be tampered with or exploited. So, to address all of these issues, we'll create a safe blockchain application.

VII. SCOPE

The goal of the project is to create software that will provide every one of the capabilities that the existing system provides, as well as some additional apps that are relevant in today's society and are in demand by people, such as adding a blockchain wallet, cloud, and other future aspects of the programme. As a result, we must address the shortcomings of the previous system. The software that will be created will be far more safe and dependable than the current programme.

VIII. PROPOSED SYSTEM

All of the user's information is saved on a block that is linked to other blocks in a chain. There is no centralised server in a decentralised application. It's a peer-to-peer system. Furthermore, the data saved in the block is extremely difficult to decrypt due to the use of highly secure encryption and hashing methods (256 bits). In addition, if a hacker wishes to correct the content in a block, he or she will have to update all of the copies of that block throughout the blockchain network, which may be difficult. Despite the fact that the block is present on all nodes, only the individual whose first information is intended could read it.

IX. SYSTEM ARCHITECTURE

A transaction number and deals make up a block body. The maximum number of transactions that a block may contain is determined by the block size and hence the size of each transaction. To confirm transaction identification, Blockchain employs an asymmetric cryptography method. In an untrustworthy environment, digital signatures with uneven cryptography are used. We now have a tendency to quickly rationalise the use of a digital signature.

Block

A block includes the block header and therefore the block body. The block header consists of:

a) Block version: specifies the block validation procedure to use..
b) Merkle tree root hash: this is the location where all of the changes' hash values are stored.
c) Timestamp: Since January 1, 1970, the Greenwich Mean Time has been used.
d) n-Bits: target threshold of a legitimate block hash.
e) Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.

.

f) Parent block hash: a 256-bit hash value which points to the block ahead .

X. ADVANTAGES

1) Protected: The app that will be created will be more secure. Due to the extreme implementation of the blockchain technology, privacy will be assured. As we said in the paper, blockchain is a distributed ledger, which means that every user of the system owns a copy of the data. As a result, changing data is difficult. It is based on encryption, decentralisation, and consensus principles, which maintain operation trust. The data in many other blockchains or distributed ledger (DLT) is organised into blocks, with each block containing one or more transactions
2) Fast and Efficient: Because the blockchain network has numerous nodes, it will take a long time for the transaction to propagate.
3) Decenterlization: The consensus mechanism in blockchain technology achieves decenterlization. In a decentralised context, this will preserve data integrity and permanence.
4) Immutibility: Because a blockchain public network employs a separate security method, it is almost impossible to modify the data stored by a significant number of customers

XI. RESULTS

We've created a chat application that utilises Blockchain technology. This programme runs on a central computer, providing users with a high level of confidentiality and anonymity.
This particular strategy can be employed in defence as well as by various security agencies, as they are constantly at high risk of intrinsic security breaches

XII. CONCLUSION

We are working on an application that allows efficient use of blockchain in the this work. We can also ensure the safety and quantity of information and communication by removing the centralised method. Multiple conversations are more fast and clear with decentralised apps. Traditionally, an intermediary node is used in the conferencing method, but our software does not utilise one, meaning that everyone is linked through a peer-to-peer network. dimensional balance If you're using mixed units, make sure to explicitly explain the items for each number in a calculation.

XIII. REFERENCE

[1] 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).
[2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” (2008)
[3] 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).
[4] 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)
[5] 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
[6] 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.

[7] Wörner, A., Meeuw, A., Ableitner, L. et al. Trading solar energy within the neighborhood: field implementation of a blockchain-based electricity market. Energy Inform 2, 11 (2019)

[8] Chris Reed, Uma M Sathyanarayan, Shuhui Ruan, Justine Collins, Beyond BitCoin—legal impurities and off-chain assets, International Journal of Law and Information Technology, Volume 26, Issue 2, Summer 2018

[9] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach and N. Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications," in IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1256-1270, Nov. 2020

[10] Nguyen HL., Eisenbarth JP., Ignat CL., Perrin O. (2018) Blockchain-Based Auditing of Transparent Log Servers. In: Kerschbaum F., Paraboschi S. (eds) Data and Applications Security and Privacy XXXII. DBSec 2018. Lecture Notes in Computer Science, vol 10980. Springer, Cham

[11] J. Xu, S. Wang, B. K. Bhargava and F. Yang, "A BlockchainEnabled Trustless Crowd-Intelligence Ecosystem on Mobile Edge Computing," in IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3538-3547, June 2019

[12] C. Liao, C. Cheng, K. Chen, C. Lai, T. Chiu and C. Wu-Lee, "Toward A Service Platform for Developing Smart Contracts on Blockchain in BDD and TDD Styles," 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA), 2017, pp. 133-140

[13] K. Nakayama, R. Moslemi and R. Sharma, "Transactive Energy Management with Blockchain Smart Contracts for P2P Multi-Settlement Markets," 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2019

[14] Pandurangan, G., Robinson, P. & Trehan, A. “DEX: selfhealing expanders. Distrib. Computing”. 29, 163–185 (2016)

[15] X. Zhang, S. Chen and Ravi Sandhu, "Enhancing data authenticity and integrity in P2P systems," in IEEE

[16] M. E. Locasto, J. J. Parekh, A. D. Keromytis and S. J. Stolfo, "Towards collaborative security and P2P intrusion detection," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, 2005

[17]] J. Liang, R. Kumar, Y. Xi and K. W. Ross, "Pollution in P2P file sharing systems," Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., 2005.

[18] Q. Lian, Z. Zhang, M. Yang, B. Y. Zhao, Y. Dai and X. Li, "An Empirical Study of Collusion Behavior in the Maze P2P FileSharing System," 27th International Conference on Distributed Computing Systems (ICDCS '07), 2007

[19] Stefan Saroiu, P. Krishna Gummadi, and Steven D. Gribble "Measurement study of peer-to-peer file sharing systems", Proc. SPIE 4673, Multimedia Computing and Networking 2002, (10 December 2001)

[20] Pouwelse J., Garbacki P., Epema D., Sips H. (2005) The Bittorrent P2P File-Sharing System: Measurements and Analysis. In: Castro M., van Renesse R. (eds) Peer-to-Peer Systems IV. IPTPS 2005

[21] J. K. Nurminen, A. J. R. Meyn, E. Jalonen, Y. Raivio and R. Garcıa Marrero, "P2P media streaming with HTML5 and WebRTC," 2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2013

[22] M. Amad, A. Meddahi and G. Vanwormhoudt, "A selfadaptive ALM architecture for P2P media streaming," 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015

[23] Kaidong Wu, Yun Ma, Gang Huang, Xuanzhe Liu, A first look at blockchain-based decentralized applications, Software: Practice and Experience, 10.1002/spe.2751, 0, 0, (2019)

[24]Kaidong Wu, Yun Ma, Gang Huang, Xuanzhe Liu, A first look at blockchain-based decentralized applications, Software: Practice and Experience, 10.1002/spe.2751, 0, 0, (2019)