iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42479

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Real-Time Communication over Blockchain

Tushar Gupta[1], Harshit Dhyani[2], Piyush Kumar[3], Vishesh Gupta[4], Ankita Sharma[5]
[1, 2, 3, 4, 5]*Computer Science & Engineering HMRITM, Delhi, India*

Abstract: ***Blockchain Technology becoming popular with time giving rise to Web 3.0 and this technology will change the way we see the Internet. Blockchain is a decentralized, digitally dis- tributed immutable ledger that allows real-time communication to happen securely; this is the reason we need blockchain in a social networking websites as these websites keep the data on centralized servers that can be risky as the data can easily be stolen and can easily be distributed with third parties without the need of users consent. But with the help of Blockchain and DApps, we can create a reliable and efficient way to share messages and media on secured networks without any third party interference. In this paper, we are going to discuss how we make use of smart contracts and peer-to-peer networks like Ethereum to create such applications and allow users to share their messages and other forms of information without any fear of data getting lost or being shared without user consent, we also going to discuss how this method is different from the current method which social networking websites use to secure users data, and how Web 3.0 is going to be different from current Web 2.0 in terms of a social network.***

Index Terms: decentralization, blockchain, Apps(Decentralized applications), Ethereum

I. INTRODUCTION

With the evolution of cryptocurrencies i.e BTC(Bitcoin) and the application of blockchain in various industries that can use blockchain as a fundamental technology has gradually attained global attention [1].Nick Szabo proposed The concept of ”smart contract” in 1995 [2], defined as ”Smart contract may be a set of digitally outlined obligations, together with contracts that enable participants within the contract to meet those obligations”.Smart contracts is a set of instructions that will only run when certain conditions get fulfil. They are generally used to reduce the need of trusted inter-mediators and fraud losses, without any intermediary’s involvement or time loss. As a core technology of the blockchain, blockchain- based smart contracts have been widely used in blockchain projects with strong influence, such as Ethereum.

DApps or suburbanized Apps area unit pc applications that run on blockchain rather than a central node system. These Apps area unit engineered on the Ethereum platform and don’t seem to be in hand by any single organization rather DApps distribute tokens that represent ownership [3] These tokens are distributed according to a programmed algorithm to the users of the system, diluting ownership and control of the DApp [4].

The four logical components of blockchain ecosystem are as follows:

1) Node
2) Ledger
3) Consensus Algorithm
4) Virtual Machine

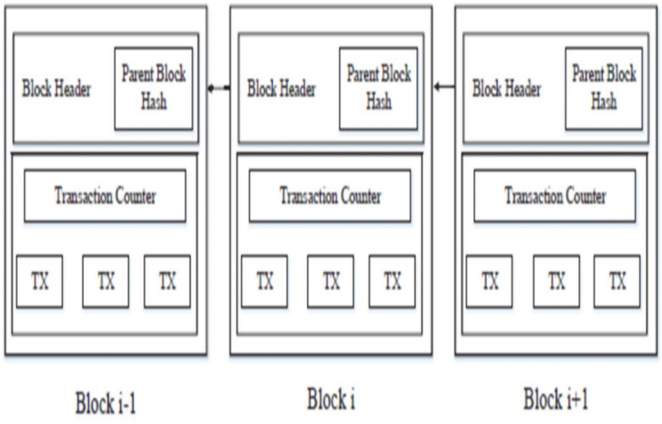


Fig. 1. Example of blockchain with multiple sequence of blocks.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

a) *Node:* Any laptop connected to the net that wishes to participate within the blockchain system should have a computer application before the system it desires to join. Nodes area unit liable for storing information entered into the immutable ledger. The nodes will save all copies of the shared ledger to the system.

b) *Ledger:* A common ledger is maintained within the node application. It is accessible to all users of the blockchain ecosystem. When a hacker tries to hack into the system, it becomes very difficult for the hacker because he has to make changes to every node in the ledger in order to manipulate the data.

c) *Consensus Algorithm:* It provides the rules that all users of the blockchain network follow to share the current common state of the shared ledger. The algorithm works on three methods, namely: "Proof-Of-Work, Proof-Of- Stake, Proof-Of-Elapsed-Time" [2].

d) *Virtual Machine:* It is a computer program that runs on blockchain and allows smart contacts to communicate with each other. Blockchain is only accessible inside the virtual machine beyond that it does not exist, in order to protect your system from malicious software getting installed on your computer.

II. LITERATURE SURVEY

In this section of the article, the author suggests all pos- sible ways along with decentralization to create a real-time web messaging app. Also, the author explains the future of blockchain applications. In this section, our main goal is to explain blockchain systems and how P2P applications work.

A. Blockchain Application

Blockchain is typically used in cross structure transactions because of the data transparency and verifiablity used widely in the financial services [5], information security [6] and software package engineering [7].

B. Peer-to-peer Applications

Applications based on peer-to-peer network are called de- centralized apps [8], the P2P network allows hardware and software to communicate without the need of the server. There is no central server for processing the request in P2P network.

C. Security

P2P networks can posses a danger from unethical users of the network in order to detect attacks [9],researchers use technologies like trustworthy computing [10].

D. Performance

The applications running on P2P network experience low performance rate the the central network. Researchers are trying to evolve the applications based on P2P network by optimizing the application layerer [11] and network layer [12].

III. REAL-TIME COMMUNICATION WITH WEBRTC

Real-time communication (RTC), a new industry-wide technique that extends the net browsing model and provides unified communications and access to data such as social networks, chat, video conferencing and calls over the net. WebRTC may be a variety of open supply time period communication technology that adds AN API (Application Programming Inter- face) commonplace to change time period media transmission like voice and video from an internet browser while not aplug- in that gives high-quality multimedia system communication. between peers. net developers while not existing plugins.

A. WebRTC Architecture

WebRTC follows the client-server linguistics organizer as a thought of peer-to-peer communication between browsers. Connections manage media methods to allow direct streaming between browsers. Network signals are sent by Internet servers and facilitate changing, interpreting, or manipulating PRN signals by Internet sockets or HTTP. communication between browsers and servers was ascertained to be non-uniform within the application section, WebRTC. Internet servers will communicate victimization customary communication protocols like the session data formatting protocol (SIP) or Jingle. or else, the property communication protocol will be used for this purpose.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

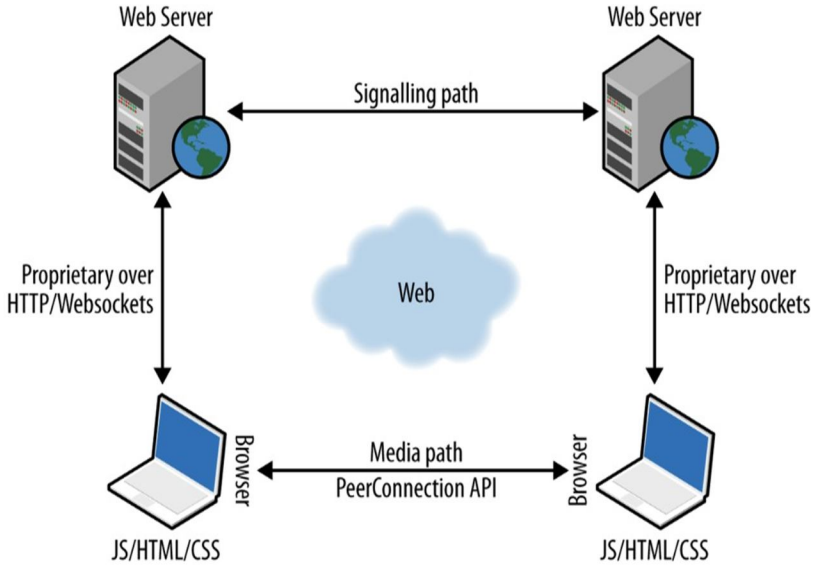


Fig. 2. The WebRTC trapezoid.

B. WebRTC API

The WebRTC API allows applications to take advantage of the real-time capabilities of uncommon browsers. The real- time browser function , which was implemented at the browser center,provides the necessary function for setting the video, audio,and data channel required. The basic concepts that have been relied upon in the design of the API. MediaStream, PeerConnection, DataChannel [13].

1) *MediaStream:* MediaStream refers to streaming me- dia from local media devices such as microphones and webcams. [14]. The web application must request user access to make and utilize a local stream through the "GetUserMedia ()" function.
2) *PeerConnection:* RTCPeerConnection reads the Medi- aStream output knowledge and creates the affiliation between 2 users. to form the affiliation, the Interactive property institution structure uses protocols as its core of NAT (Network Address Translator) wherever these protocols area unit provided by Google [15].
3) *DataChannel:* The Real Time Communication Data Channel API is a two-way data channel between two equals that provides a way to exchange random data among themselves.

C. System design

The system design to provide communication with the mechanism of user identification and discovery of other users of the system without installation or setup procedures.The proposed system is divided into several parts:In the proposed system All server-side and client-side information that trans- mitted is secure and encrypted using high secure protocols server which is used to distribute the content from different remote sources. Before data flow begins, the server application will verify user sessions and licenses for each demand. If the session has licenses for requested content and is valid,the flow will begin.

1) The information contained in any request is observed by the server and, on this basis, informs the user of the messages and calls incoming. This server listens for calls or calls during the requested request creation process, information about the paths between the users and request parameters required for each call participant will be transferred by the server. . Videos and image files that are uploaded by a user to the server will be compressed while maintaining a high resolution of uploaded files.
2) Create a database consisting of many tables that are used to store information about users and their activities such as video calls, user logins,and sessions. All important information in Database is encrypted by using a high complex encrypt method.
3) Using HTML5, CSS3, JavaScript and jQuery,JSON, AJAX Techniques on client-side and used PHP 5.5, PHP: PDO for SQL instructions and Node.JS on the server side.

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

IV. EVOLUTION OF THE WEB

Talking about the evolution of the web, 1.0, 2.0 and 3.0 are so far the most relevant to us, and have been fundamental to our daily experience of the world wide web and interaction in a broader sense.

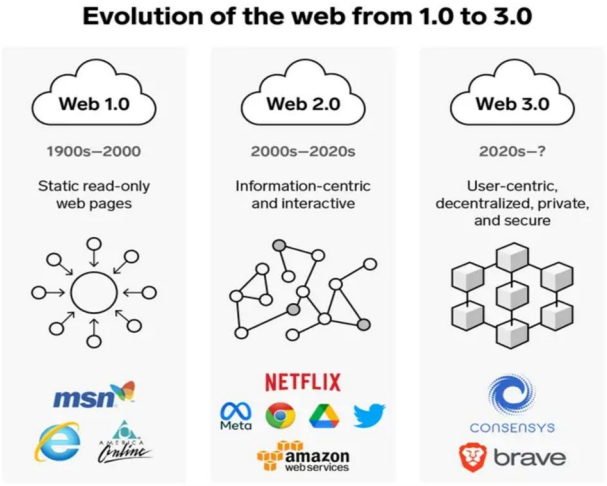


Fig. 3. Evolution of the web from 1.0 to 3.0.

Web 1.0 was the first phase of WWW's evolution. Pre- viously, content was created in scarcity with an abundance of consumers. Personal web pages or blogs were common, mainly static pages over ISP or on free web hosting services. The content was mostly put together as tables and frames. Web 2.0 is the current ongoing scenario, with websites consisting of global, user-generated content, accessibility, us- ability, and interoperability. It is social in nature. It is not a technical differentiation, but rather a matter of the way websites, pages, and apps are designed and accessed. It is beneficial. Interaction is enhanced, collaboration is promoted, and social dialogue is propagated through a virtual community, as an improvised version of Web 1.0.

Web 3.0 or semantic web or as we nowadays talk in terms of metaverse (an evolved sense of web and immersive interaction) claims to establish information around the world in an efficient and improvised way. It is particularly true from the machine's point of view as opposed to what the human understands.

V.DECENTRALIZED VS CENTRALIZED ARCHITECTURE

A. Decentralized interaction and centralized management in Real-time communications

Real-time communication is the most important component of various interactive multimedia uses on online platforms. According to some experts, in gossip protocols, a gossip- oriented supernode infrastructure presents a fundamental ar- chitecture crucial for routing and queries during communica- tion relaying [16]. Today, real-time systems are moving from a centralized architecture to a decentralized architecture. This is a factor in the high efficiency of such an infrastructure in the realization of real-time services. The distributed archi- tecture was discovered in real-time communication, and can be easily described in video-audio communication scenarios developed with advanced multimedia services.The decentral- ized architecture reinforces giant bandwidth with real-time video & audio communication and mechanical resources such as CPU.Because of the decentralized architecture, multivideo conferencing is text-based and highly feasible compared to previous single communication channels that were hampered by numerous online-based communication restrictions.

Decentralized architecture prioritizes currency storage via technologies such as blockchain and cryptocurrencies. Digital innovations have promoted currency storage technology, which has high scores on safety and reliability. Distributed architec- ture capabilities that leverage nodes that do not depend on a single server make customization easier and integrate more adaptive and flexible network configurations that can support even advanced technologies such as ones of cryptocurrencies and blockchain.

The decentralized structure is now not restricted in real- time communication, and cryptocurrencies, however, are also turning into an increasing number of follower in army agen- cies. A space firm such as NSA, [17] in conjunction with other companies, has expressed a keen interest in exploring blockchain technology, a move that has raised hopes of further advancement of the space industry [17]. The suitability of using a distributed architecture in infrastructure such as the blockchain is made possible by the presence of a large number of autonomously connected nodes with high connection capac- ity, a factor that makes the blockchain framework stronger.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Benefits of Centralized VS Decentralized Networks

1) *Decision-making:* Rising businesses are getting advan- tage from an intersection of control because it makes a difference and speeds up decision-making. A company's structure can in some cases get aggravated input from upper administration when choosing on a matter. Be that as it may, this can be really more viable for non-public companies with a devoted benefit show. Decentralization is more ideal for bigger multinational companies. It may also be better if you're having a business that produces a large range of products that need expertise from different industries/companies to create, modify, sell and market properly. Companies which might be professionals of their subject have a tendency to be extra decentralized due to their scope and performance of manufacturing output.
2) *Authoritative Chain of Command:* The conclusive chain of command that comes with a centralized organizational structure can be accommodating for representatives who might explore for more positive direction in their duties and expectations. A centralized architecture works pretty well to deliver clear headlines to people. Businesses that utilize or contract those with specialized foundations are as a rule superior suited to a top-down administration structure. The vague nature of a decentralized framework may cause perplexity with respect to anticipated workflows, but the expanded autonomy is exceptionally attractive to employees who favor a flexible plan. Companies that have a part of workers working from domestic may utilize a combination of diminished oversight and self-reporting apparatuses to streamline administrative obligations. Decentralization also makes a difference to optimize a company's worldwide establishment by permitting distinctive national branches to oversee their staff and operations.
3) *Stream of Information:* A decentralized organization advances a quicker and smoother stream of data be- tween diverse offices and from upper administration descending. Businesses that depend on a always moving and conflicting showcase advantage from being able to upgrade everybody at will. When you're seeing a part of changes happening in your trade over a brief period, you might consider decentralization endeavors. With a centralized structure, a team may get more cur- rent information by implication through official activities and administrative mandates. This possibly clears out a few representatives ignorant, but a firmly controlled stream of data can increment clarity and decrease the plausibility of clashing elucidations. Companies that depend on exchange insider facts and non-disclosure agreements are too often more than not best suited to a centralized organizational structure.

VI. DECENTRALIZATION PROTOCOLS OF BLOCKCHAIN

By introducing blockchain within these identity Authentication ways, in which a further line of protection is provided within the security ways, blockchain may well be a participant list that records deals between peer-to- peer networks. This medium offers clear tamper- evidence deals that tend to resolve issues like fraud, high haggling costs, and live the particularity of all actors involved. In our analysis, hyperledger and IPFS protocol unit of dimension applied for creating identity-ground authentication and verification in documents. The system begins with a stoner request to the blockchain.Also, network members replied that the blockchain stores the act of information and data throughout a distributed participated data formerly confirmation and acceptance. The history of deals prevents vicious druggies from performing dangerous conduct within the system. It is clear that the blockchain improves the complete system ability to avoid most security pitfalls by migrating, chaining, and distributing the total description. the protection debit of deals or events was formerly Bettered by victimization of the general public blockchain as a decentralized system, due to the stationary history of information. Nothing can change it as a result of everyone carrying a replica of that in their memory. A combination of the immutable security of blockchain school and therefore the fast evolution of recent communications give a motivating stage upon which firms can still introduce for the advantage of society. One such innovation is decentralized applications (DApps). they're go past several users on a decentralized network with trustless protocols (blockchain technology).Designed to avoid any single purpose of failure, DApps generally have commemoratives to award druggies for furnishing calculating power.

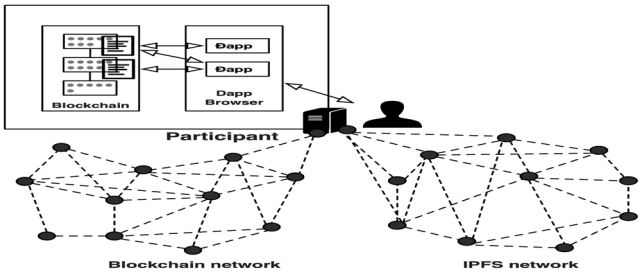


Fig. 4. IPFS File Sharing System on Blockchain

A. Hidden Dangers of Text Messenger Apps

It highlights the issues of safety, privacy and security on social networks and messengers. With doubts revolving around centralized systems like Facebook etc [19], it has become important for the user to pay attention to safeguarding their personal data and when it comes to the intrusion of privacy, as long as we are talking to another person regardless, there is no way our conversations are being kept private.

B. Hyperledger Indy

Hyperledger provides high security by exploiting the decen- tralization and inflexible nature of blockchain. The modules within the Hyper tally are ordering services, class service suppliers, peer-to- see services, and sensible contracts. Deals arrive at agreement on the hyperledger by ordering and sup- porting the deals. By victimization of this, all druggies might have complete operation over their tone- identity. Others can not take over that identity instrument. The credentials area unit is created with the paraphrase name. Additionally, the requested area unit is transferred to the philanthropist with its redistributed symbol (DID). a signal request is entered and a response is going to be transferred for the evidence of a relief paraphrase. Previously more a relief relationship is established with another knot and creates a instrument description, and is submitted to the tally. Eventually, verification is completed by each side in establishment to a holder or holder to a champion. Using this hyperledger for supporting documents, the results easily show the cost effectiveness and high energy.

C. Inter Planetary File System (IPFS)

IPFS could also be a peer-to-peer distributed classification system that uses a DHT to trace data; it is a new model of sharing file distribution. IPFS contains a web application that makes it simple for users to work with it. The IPFS uses hash tables to store a data package. IPFS nodes can offer blocks of knowledge. The IPFS uses Kademlia to search out which nodes have what data. Kademlia could also be a DHT for localized peer-to-peer computer networks designed by Petar Maymounkov and David Mazieres in 2002 [18]. A singular hash could also be the result of saving data without fear of data size inside the IPFS. The IPFS can store the hash therefore parties can use the hash to retrieve the knowledge. Once the data are ready to be featured on the IPFS network, the knowledge will split into many very small chunks. The chunk is thought with its own hash. Then, the chunks square measure attending to be distributed to varied nodes on the network that have their hash nearest to check Id. Once the user requests to retrieve a touch, the retrieve request traverses to nodes where the hash exists by victimizing the DHT. All the chunks unit simply combined to mean the foremost object once visiting all these chunks. However, the distributed part of DHT implies that the complete table unfolds at totally different locations.

VII. FUTURE SCOPE

Developing software that provides all the functionality of current available chat applications and overcomes shortcom- ings such as privacy, phishing, and centralized social networks. The resulting software is safer and more reliable than what is currently available.

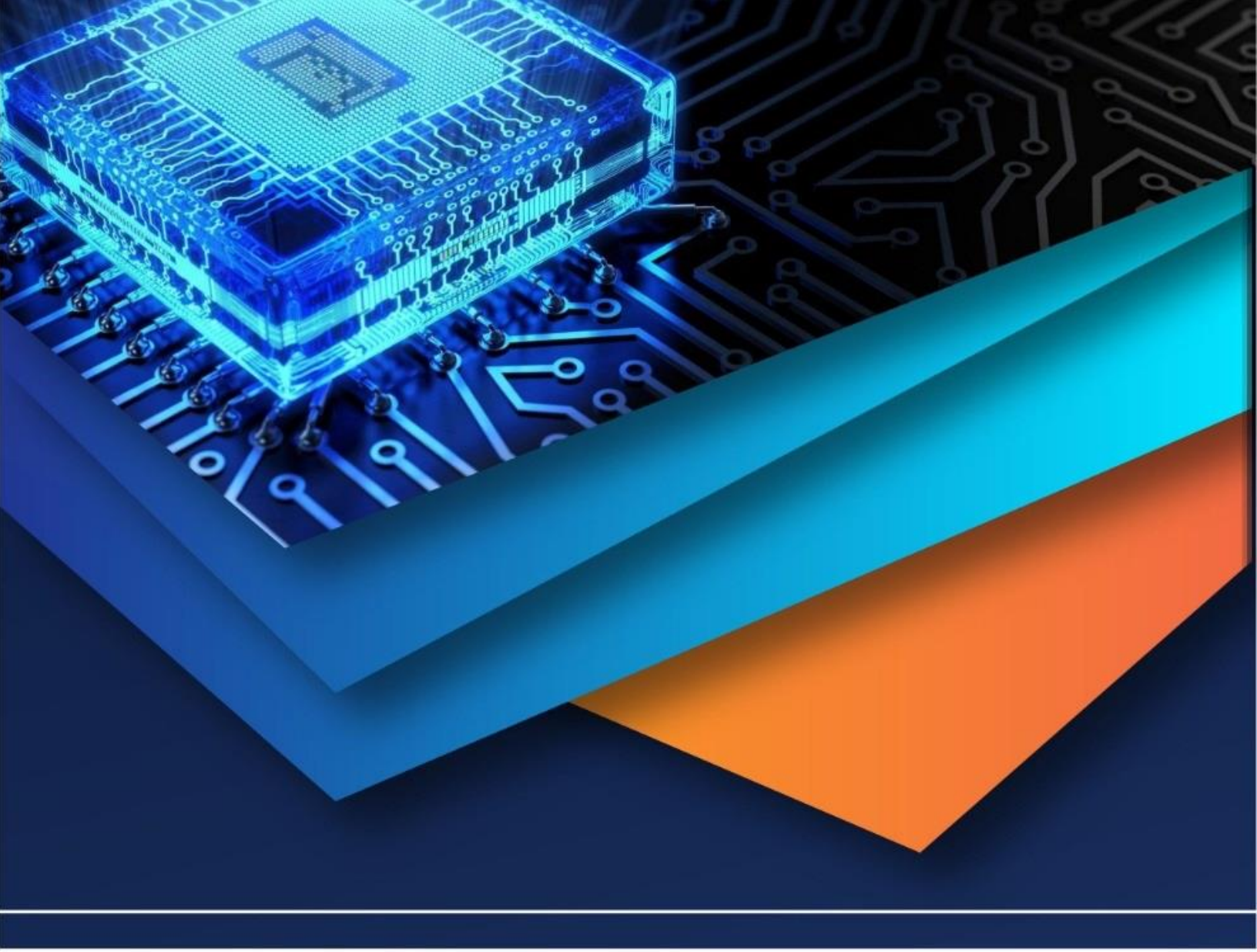
VIII. CONCLUSION

We try to emphasize on the benefits of eliminating the central approach and moving to a decentralized future of the world wide web, specifically in context of real time communication, social media and security threats associated with it. The concept of blockchain, the idea of making every node inaccessible to ensure security and isolation of data, is what makes it very secure and efficient by eliminating any middle devices or the central node. Hence, the future of web and communication is secure, fast and good to rely on.

REFERENCES

[1] Zhang, Q. F., Jin, C. Q., Zhang, Z., Qian, W. N., & Zhou, A. Y. (2018). Blockchain: Architecture and research progress. Chinese Journal of Computers, 041(005), 969–988.
[2] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. http://www.bitcoin.org/bitcoin.pdf
[3] Andoni, Merlinda; Robu, Valentin; Flynn, David; Abram, Simone; Geach, Dale; Jenkins, David; McCallum, Peter; Peacock, Andrew (2019- 02-01). ”Blockchain technology in the energy sector: A systematic review of challenges and opportunities”. Renewable and Sustainable Energy Reviews. 100: 143–174. doi:10.1016/j.rser.2018.10.014. ISSN1364-0321
[4] Johnston, D., Yilmaz, S. O., Kandah, J., Bentenitis, N., Hashemi, F., Gross, R., ... & Mason, S. (2014). The General Theory of Decentralized Applications, DApps.
[5] W örner, 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)

[6] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach and N. Harth, "To- ward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications", IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1256-1270, Nov. 2020
[7] 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
[8] K. Nakayama, R. Moslemi, and R. Sharma, "Transactive Energy Man- agement with Blockchain Smart Contracts for P2P Multi-Settlement Markets," IEEE Power & Energy Society Innovative Smart Grid Tech- nologies Conference (ISGT), 201
[9] Pandarangan, G., Robinson, P. &Trehan, A. —DEX: selfhealing ex- panders. Distrib. Computing. 29, 163–185 (2016)
[10] X. Zhang, Chen, and Ravi Sandhu, "Enhancing data authenticity and integrity in P2P systems," IEEE
[11] 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
[12] 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 (INFO-COM WKSHPS), 2013
[13] Chuan Yen Chiang, Yen-Lin Chen, Pei-Shiun Tsai,Shyan-Ming Yuan, " A Video Conferencing System Based On WebRTC for Seniors", International Conference on trustworthy systems and their application, IEEE, 2014.
[14] Khalid Ibn Zinnah, Nafiz Mahmud, Firoz Hasan, Sabbir Hossain Sagar, 'WebRTC-based P2P Video Conferencing System', International Confer- ence on Electrical, Computer, and Communication Engineering (ECCE), February 2017.
[15] Nayyef, Zinah Amer, Sarah Hussain, and Zena. (2019). Peer-to-Peer Multimedia Real-Time Communication System based on WebRTC Tech- nology. International Journal for the History of Engineering Technol- ogy.2.9. 125-130.
[16] V. W. H. Luk, A. K. S. Wong, C. T. Lea, R. W. Ouyang, RRG: redundancy reduced gossip protocol for real-time N-to-N dynamic group communication, Journal of Internet Services and Applications, 4(1): 14, 2013.
[17] N. Altaf, Space Tech: Transforming satellite launches with blockchain, 2019 [Online] Available: https://www.ibm.com/blogs/blockchain/2019/06/space-tech-transforming-satellite-launches-with h-blockchain/ [Accessed on October 18, 2019]
[18] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer informa- tion system based on the XOR metric," in International Workshop on Peer-to-Peer Systems, pp. 53–65, Springer, 2002.
[19] boyd, d, Ellison, N (2007) Social network sites: definition, history and scholarship. Journal of Computer-Mediated Communication 13(1): 210–230.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)